IBM Security Guardium V10.1

Table des matières

IBM Security Guardium version 10.1

Bienvenue dans la documentation d'IBM Security Guardium, qui contient des informations permettant d'installer, de gérer et d'utiliser IBM Guardium.

Mise en route

Tâches courantes

Identification et résolution des incidents et support

Guardium - Accueil du support
Guardium - Ressources de support
Guardium - Vidéos de support
IBM developerWorks - Réponses pour Guardium

Informations complémentaires

IBM Security Learning Academy
IBM data security and protection
Communauté IBM developerWorks Guardium
Guardium

Présentation du produit

Informations relatives au produit et éditions pour les solutions Guardium.

- IBM Guardium
  IBM Guardium prévient les fuites provenant des bases de données et des environnements big data tels que Hadoop, garantit l'intégrité des informations et automatise les contrôles de conformité dans des environnements hétérogènes.
- Nouveautés de l'édition
  Nouvelles fonctionnalités, fonctions et améliorations.
- Notes sur l'édition
  Découvrez les fonctionnalités et améliorations les plus récentes, la configuration système requise, ainsi que les informations relatives à la mise à niveau, à l'installation et au support.

IBM Guardium

IBM Guardium prévient les fuites provenant des bases de données et des environnements big data tels que Hadoop, garantit l'intégrité des informations et automatise les contrôles de conformité dans des environnements hétérogènes.

Il protège contre les menaces les données structurées et non structurées des bases de données, les environnements big data et les systèmes de fichiers tout en garantissant leur conformité.

Il fournit une plateforme évolutive permettant la surveillance en continu du trafic de données structurées et non structurées, ainsi que l'application des politiques liées à l'accès aux données sensibles à l'échelle de l'entreprise.

Un référentiel d'audit sécurisé et centralisé associé à une plateforme d'automatisation des flux de travaux intégrée rationalise les activités de validation de conformité sur une large gamme de mandats.

Il optimise l'intégration à la gestion informatique ainsi que d'autres solutions de gestion de la sécurité, afin de fournir une protection exhaustive des données dans l'entreprise.

Il est conçu pour activer la surveillance en continu de bases de données et d'infrastructures de partage de documents hétérogènes, ainsi que l'application de vos politiques pour l'accès aux données sensibles dans l'entreprise à l'aide d'une plateforme évolutive. Un référentiel d'audit centralisé conçu pour optimiser la sécurité, associé à une application intégrée d'automatisation des flux de conformité, permet aux produits de rationaliser les activités de validation de conformité sur une large gamme de mandats.

IBM Security Guardium est conçu pour faciliter la protection des données critiques. Guardium est une plateforme de protection des données complète qui permet aux équipes de sécurité d'analyser automatiquement ce qui se passe dans des environnements de données sensibles (bases de données, entrepôts de données, plateformes big data, environnements cloud, systèmes de fichiers, etc.) afin de minimiser les risques, de protéger les données sensibles contre les menaces internes et externes, et de s'adapter de façon homogène aux changements informatiques qui peuvent impacter la sécurité des données. Guardium aide à garantir l'intégrité des informations des centres de données et à automatiser les contrôles.

La solution IBM Security Guardium est proposée en deux versions :

- IBM Security Guardium Database Activity Monitoring (DAM)
- IBM Security Guardium File Activity Monitoring (FAM) - Utilisez la surveillance des activités de fichier Guardium pour étendre les fonctions de surveillance aux serveurs de fichiers.

Les produits IBM Guardium offrent une solution simple et robuste pour prévenir les fuites de données des bases de données et fichiers, aidant ainsi à garantir l'intégrité des informations du centre de données ainsi que l'automatisation des contrôles de conformité.

Les produits Guardium peuvent vous aider à :

- localiser automatiquement des bases de données et effectuer une reconnaissance et un classement des informations sensibles qui s'y trouvent ;
- évaluer automatiquement les vulnérabilités et défauts de configuration d'une base de données ;
- garantir que les configurations sont verrouillées une fois les changements recommandés implémentés ;
- activer une visibilité élevée à un niveau granulaire dans les transactions de base de données impliquant des données sensibles ;
- suivre les activés des utilisateurs finaux qui accèdent indirectement à des données via des applications d'entreprise ;
- surveiller et appliquer une large gamme de politiques, y compris sur l'accès aux données sensibles, le contrôle des changements de base de données et les actions des utilisateurs privilégiés ;
- créer un référentiel d'audit unique et sécurisé pour un grand nombre de systèmes et de bases de données hétérogènes ;
- automatiser le processus complet d'audit de conformité, y compris la création et la distribution de rapports, ou encore la capture des commentaires et des signatures.

La solution Guardium est conçue pour la simplicité d'utilisation et l'évolutivité. Elle peut être configurée pour une base de données unique ou pour des milliers de bases de données hétérogènes, réparties sur l'ensemble de l'entreprise.

Cette solution est disponible sous forme de dispositifs préconfigurés fournis par IBM®, ou en tant que dispositifs logiciels installés sur votre plateforme. Des fonctions facultatives peuvent facilement être ajoutés à votre système après l'installation.

Principales zones fonctionnelles de la solution de sécurité de base de données de Guardium :

- Evaluation des vulnérabilités. Il ne s'agit pas uniquement de détecter les vulnérabilités connues dans des produits de base de données, mais également de fournir une visibilité complète d'infrastructures de base de données complexes, en détectant les erreurs de configuration et en évaluant et réduisant ces risques.
- Reconnaissance et classification des données. Bien que la classification à elle seule ne fournisse aucune protection, elle constitue une première étape cruciale dans la définition de politiques de sécurité appropriées à différentes données en fonction du niveau de criticité et des exigences de conformité.
- Protection des données. Guardium traite le chiffrement de données à l'arrêt et en transit, le masquage de données statiques et dynamiques, ainsi que d'autres technologies destinées à la protection de l'intégrité et de la confidentialité des données.
- Surveillance et analyse. Incluent la surveillance des caractéristiques de performance des bases de données ainsi que la visibilité totale de l'ensemble des actions d'accès et d'administration pour chaque instance. Il est en outre possible d'intégrer l'analyse avancée en temps réel, la détection des anomalies ainsi que l'information sur la sécurité et la gestion des événements (SIEM).
- Prévention des menaces. Fait référence aux méthodes de protection contre les cyberattaques telles que le déni de service distribué (DDoS) ou l'injection SQL, à l'atténuation des vulnérabilités sans correctifs et autres mesures de sécurité spécifiques aux bases de données.
- Gestion des accès. Va au-delà des contrôles basiques d'accès aux instances de base de données. Le processus d'évaluation cible une gestion des accès à base de politiques, plus dynamique et sophistiquée, capable d'identifier et de retirer des droits utilisateur excessifs, de gérer des comptes de service et des comptes partagés, et de détecter et bloquer des activités utilisateur suspectes.
- Audit et conformité. Inclut des mécanismes d'audit avancés dépassant les fonctions natives, la centralisation de l'audit et de la génération de rapports pour des environnements de base de données multiples, contrôlant la répartition des tâches, ainsi que des outils prenant en charge l'analyse conjoncturiste et les audits de conformité.
- Performances et évolutivité. Bien que cela ne constitue pas une fonction de sécurité en soi, il est crucial que toutes les solutions de sécurité de base de données soient capables de faire face à des charges élevées, de réduire la saturation des performances et de prendre en charge les déploiements dans des configurations à haute disponibilité.

Pour plus d'informations sur la famille de produits Guardium, visitez la page http://www.ibm.com/software/data/guardium/.

Rubrique parent : Présentation du produit

Nouveautés de l'édition

Nouvelles fonctionnalités, fonctions et améliorations.

IBM Security Guardium version 10.1.4

Amazon Oracle v11 RDS DBaaS Monitoring utilise Native Audit Integration

Désactivez TLS1.0/1.1, activez TLS1.2

VA (évaluation de vulnérabilité) prend en charge Oracle 12.2

Améliorer l'interface graphique VA (évaluation de vulnérabilité) pour afficher un description courte

Mettre à jour OpenSSL pour Windows/UNIX S-TAP

Support d'EMC ATMOS

Accélérateur GDPR pour z/OS

Amélioration des classificateurs

Déploiement simplifié de S-TAP via GIM

Nouvelle version d'interface graphique du générateur de groupe

Améliorer l'équilibreur de charge d'entreprise pour vérifier que le sniffer est actif avant d'allouer des unités gérées

Autoriser plusieurs tampons K-TAP avec plus de cinq collecteurs

Prioriser les paquets des connexions par rapport aux paquets ordinaires

IBM Security Guardium version 10.1.3

Contrôle de conformité - Démarrage rapide

- Déployer les agents de surveillance - Préparez rapidement la surveillance de base de données via la reconnaissance et l'activation de clients GIM, l'installation d'agents S-TAP, la création de moteurs d'inspection et le mappage des agents S-TAP à des collecteurs.
- Configurer la surveillance de conformité - Vous aide à répondre aux normes de conformité en installant rapidement des politiques, en remplissant des groupes et en exécutant des rapports sur l'activité de surveillance des bases de données.

Cloudera Hadoop - Guardium a été la première solution à fournir une évaluation des vulnérabilités dans l'espace NoSQL avec une prise en charge de MongoDB. Aujourd'hui, Guardium s'étend à l'espace Hadoop/Big Data avec prise en charge de la plateforme Cloudera. L'évaluation des vulnérabilités Guardium (Vulnerability Assessment) permet aux organisations d'utiliser Cloudera en toute confiance en leur donnant les outils pour évaluer et corriger le système afin de s'aligner sur les meilleures pratiques en matière de sécurité. Associé au moniteur d'activités Guardium (Activity Monitor) pour l'analyse d'audit, de conformité et de sécurité en temps réel, Guardium peut fournir une solution de sécurité holistique pour Cloudera ainsi que pour les bases de données et centres de données les plus courants dans des environnements d'entreprise classiques.

Guardium S-TAP for z/OS - IBM Security Guardium étend la sécurité des données aux grands systèmes avec les améliorations suivantes :

- Protection des données afin de bloquer les activités utilisateur DB2 for z/OS non autorisées
- Performances et optimisation afin de réduire les temps système
- Audit et filtrage des fonctions afin d'étendre encore la protection des données et les analyses en temps réel
- Facilité d'emploi et durabilité pour permettre d'accélérer le déploiement et les diagnostics

IBM Security Guardium version 10.1.2

1. Amélioration de la détection des valeurs extrêmes

   Une valeur extrême est définie par le comportement d'une source donnée spécifique (base de données, utilisateur particulier d'une base de données, serveur, utilisateur de système d'exploitation) sur une période donnée qui se trouve hors délai ou portée "normal(e)" de l'activité de cette source particulière. La détection des valeurs extrêmes étend la surveillance de base de données classique en fournissant une détection précoce des attaques possibles en cours de fonctionnement, en analysant les changements de comportement source. Cette version introduit :

   - La prise en charge de FAM
   - S'exécute sur un agrégateur de données provenant de plusieurs collecteurs
   - La page de statut d'analyse des valeurs extrêmes, qui fournit le statut en cours du processus d'analyse des valeurs extrêmes pour l'ensemble des unités gérées et explore les processus avec valeur extrême qui n'ont pas abouti
   - Deux onglets dans la table des résultats du tableau de bord d'investigation : l'onglet Récapitulatif, qui comporte une ligne par source par heure à laquelle une anomalie a été détectée, avec le score d'anomalie et les causes ; l'onglet Détails, qui comporte une ligne par valeur extrême avec le score d'anomalie, la ou les causes de valeur extrême et des détails (programme source, objet, verbe, etc.)

2. Surveillance de l'activité de Hadoop et amélioration de l'intégration de Cloudera 5.7+ / Ranger

   Cette édition étend la prise en charge de Guardium pour la surveillance des données Hadoop avec l'intégration de Cloudera via l'intégration de Cloudera Navigator et Hortonworks à l'aide d'Apache Ranger. Ces intégrations permettent le chiffrement SSL pour les clients qui ont besoin d'accéder à des données Hadoop, et elles sont prises en charge par une nouvelle interface de surveillance Hadoop.

3. Amélioration des classificateurs et nouvelle option de sauvegarde/archivage Cleversafe

   Guardium prend désormais en charge l'exécution simultanée de plusieurs processus de classification. La possibilité d'exécuter plusieurs processus de classification à la fois permet une utilisation plus efficace des ressources d'UC système disponibles.

   Par défaut, les processus de classification Guardium excluent désormais plusieurs bases de données et schémas système utilisés par les fournisseurs de logiciel de base de données. L'exclusion de ces bases de données et tables permet une exécution plus efficace des processus de classification ; elle permet également de renvoyer un moins grand nombre d'erreurs.

   La sauvegarde/archivage Cleversafe prend en charge l'interface Amazon S3 via le même logiciel SDK. L'interface de Guardium pour Cleversafe est analogue à Amazon S3 (également pris en charge par Guardium). La prise en charge cloud de Guardium inclut désormais Cleversafe, SoftLayer et Amazon S3.

4. Vues de la santé de l'entreprise

   Le nouveau tableau de bord de santé du déploiement étend les vues de santé de déploiement existantes en fournissant un récapitulatif global sur les problèmes de santé à partir d'un déploiement Guardium complet. Ce tableau de bord est particulièrement utile pour identifier les modèles et tendances dans les données de santé avant d'examiner des systèmes individuels sur lesquels des problèmes ont été identifiés.

5. Améliorations de FAM - Chaînage d'ID utilisateur et règle multi-action et valeurs extrêmes

   Chaîne d'ID utilisateur pour Windows FAM - Actuellement, l'agent Windows FAM renvoie le nom d'utilisateur pour le processus affecté à un événement de fichier. Désormais, l'agent Windows FAM changera ce nom d'utilisateur unique en une chaîne de noms d'utilisateurs appartenant à l'historique du processus (chaîne d'UID). Exemple : Le processus 1 (utilisateur janedoe) génère le processus 2 (utilisateur johndoe), puis pour les événements de fichier liés au processus n° 2, FAM consigne la chaîne d'UID composée de {janedoe, johndoe}.

   Règle d'actions multiples pour FAM - composée de plusieurs actions, chacune étant associée à une catégorie de commande spécifiée ou à un groupe spécifié. Les commandes dans un contexte de surveillance de l'activité des fichiers sont les suivantes : Lecture, Ecriture, Suppression, Exécution et Opération

de fichier.

6. Optimisation des autorisations

   L'optimisation des autorisations sert de médiateur entre le rôle de l'administrateur de base de données, en fournissant aux utilisateurs les autorisations requises pour exécuter leurs tâches efficacement, et le rôle de sécurité, en conservant ces autorisations aussi précises et minimes que possible afin de prévenir les vulnérabilité du système. Accédez à Optimisation des autorisations en cliquant sur Reconnaître > Autorisations de base de données > Optimisation des autorisations.

7. Support HP Vertica

   HP Vertica est un système big data concurrent de Hadoop. HP Vertica fournit une interface PostgresSQL standard avec ses extensions propriétaires.

   HP Vertica est utilisé pour les entrepôts de données, afin d'assurer des performances de requête particulièrement élevées. HP Vertica est également utilisé pour l'analyse des interactions utilisateur, le suivi publicitaire, les applications de flux de clics, l'évaluation de menace et la prévision financière.

8. Changements apportés aux fichiers RPM UNIX S-TAP

   - Installation sur /opt/guardium (l'emplacement ne peut pas être changé)
   - Configuration par défaut des fichiers RPM

   ktap_installed=1

   Le chargement flexible peut être utilisé en exportant NI_ALLOW_MODULE_COMBOS="Y" avant l'installation des fichiers RPM

   sqlguard_ip défini sur 127.0.0.1

   tap_ip défini sur le nom d'hôte

   Journaux RPM sauvegardés dans /opt/guardium/rpm_logs

   - La mise à jour de production est prise en charge.

   Les mises à jour de demande d'agent K-TAP sont prises en charge via les processus existants (incrémentation de la version de package).

   - Les programmes d'installation de Shell et GIM refusent d'effectuer l'installation si l'installation RPM est détectée.
   - L'agent S-TAP s'exécute après l'installation, mais doit néanmoins être configuré.
   - Un nouveau script, guard-config-update, est fourni pour simplifier la configuration post-installation.

9. Accélérateur GDPR

   La sécurité et la confidentialité des données constituent les principaux soucis auxquels toute organisation doit faire face. Auparavant, au sein de l'Union Européenne, chaque pays exigeait des niveaux de conformité différents ; le tout dernier Règlement général sur la protection des données (General Data Protection Regulation, GDPR) étend et normalise les règles de protection des données pour l'ensemble des pays de l'Union Européenne.

   L'accélérateur Guardium GDPR fournit des rapports prédéfinis basés sur des groupes et politiques GDPR. Pour commencer à utiliser l'accélérateur GDPR, affectez le rôle GDPR à un utilisateur Guardium, puis accédez à Accélérateurs > GDPR avec ce compte utilisateur.

10. Analyse approfondie des données

    L'analyse approfondie des données introduit un paradigme révolutionnaire qui utilise les capacités visuelles humaines pour obtenir une vue globale du flux de données et pour identifier les comportements inattendus. Guardium propose déjà des fonctions d'apprentissage automatique et d'analyse de données en support des audits et pour détecter les attaques, fonctions basées sur le cumul des connaissances et de l'expérience. L'analyse approfondie des données ajoute la flexibilité de la perception visuelle humaine pour repérer des associations et déplacements dans les données brutes, quels que soient les types d'attaques connus, et qui autrement passeraient inaperçus.

    Par exemple, un projet de reconnaissance d'objet permettant d'identifier les nids de poule dans les rues d'une ville serait incapable d'identifier un éléphant errant dans le voisinage. L'oeil humain, en revanche, le remarquerait immédiatement. De la même façon, lors de l'examen de données d'audit sous forme de diagrammes, les utilisateurs recherchent les types de problème connus mais peuvent facilement manquer de nouvelles aberrations (inconnues).

    L'analyse approfondie des données convertit les données d'audit en une visualisation chronologique 3D des sources et destinations de données, représentant les transactions de données sous une forme non compactée, exactement comme elles se sont déroulées.

    L'espace de visualisation comporte deux plans, chacun représentant des entités du domaine d'audit d'un type donné. Chaque entrée des données d'audit est représentée sous la forme d'une "ligne clignotante" qui se déplace d'un objet du plan supérieur (IP client, utilisateur de système d'exploitation, utilisateur de base de données ou programme source) à un objet du plan inférieur (base de données, objet ou serveur). La ligne clignotante entre la source et la destination laisse une trace (ligne en pointillés) qui indique la présence d'une interaction entre les source et destination spécifiées, trace qui s'atténue progressivement vers l'arrière-plan. Les traces forment une vue d'ensemble de l'interaction entre les sources et les destinations pour la période sélectionnée. Les sources sont situées à proximité de leurs destination, ainsi que d'autres sources similaires. La taille de l'entité de destination est proportionnelle au volume des transactions par rapport aux autres entités de destination. Il existe de nombreuses façons de modifier l'affichage, notamment celles-ci : code couleur en haut de l'entité (la couleur change lorsque des détails de la source de données changent), filtre du graphique d'analyse approfondie des données, ou encore facettes du tableau de bord d'investigation. Vous pouvez également afficher l'analyse approfondie des données à l'aide d'un casque de réalité virtuelle.

    Pour accéder à l'analyse approfondie des données : Depuis le Tableau de bord d'investigation, cliquez sur Ajouter un graphique > Graphique d'analyse approfondie des données.

IBM Security Guardium version 10.1

- Infrastructure et plateforme
  - Renforcement des plateformes à l'aide des améliorations étendues de sécurité, globalisation et accessibilité
  - Prise en charge d'un dispositif Guardium s'exécutant dans un environnement Hyper-V. Hyper-V est une solution de virtualisation de Microsoft.
- Prise en charge et gestion améliorées du déploiement Guardium :

    - La stabilité et la fiabilité sont étendues pour les agents S-TAP et l'analyse syntaxique des collections.
    - La vue de santé de Central Manager fournit un tableau de bord centralisé permettant d'évaluer le statut des composants Guardium déployés.
    - Le programme de surveillance S-TAP Watchdog (guard_monitor) pour UNIX/Linux et Windows est un processus conçu pour surveiller les performances et la réactivité des agents S-TAP. Si l'utilisation de l'UC S-TAP dépasse le seuil configuré, ou si l'agent S-TAP ne répond pas à une demande de la console, les actions suivantes peuvent être prises :
        - Exécuter automatiquement guard_diag
        - Arrêter automatiquement le processus S-TAP
        - Effectuer automatiquement un cliché du processus core et arrêter le processus S-TAP
- Les améliorations apportées en matière de disponibilité pour l'entreprise rendent les composants Guardium plus faciles à déployer et à utiliser dans les environnements de grande taille, notamment :
    - Mises à jour apportées à l'équilibrage de charge automatique afin d'améliorer les demandes de granularité et de rééquilibrage
    - Génération de rapports sur les alertes de progression pour les travaux à exécution longue
    - Accès à granularité plus fine à la console de l'interface utilisateur afin d'aider les clients à répartir les rôles et accès Guardium
    - Configurations de profil et modèle pour simplifier le déploiement et le contrôle depuis Central Manager
    - Agrégation sélective pour rationaliser la génération de rapports sur les environnements de grande taille
    - Support pour les tuples à 7 éléments - Un tuple permet la combinaison de plusieurs attributs pour former un membre composite unique. Exemple de tuple à 7 éléments : IP client/Application source/Utilisateur de la base de données/IP serveur/Nom de service/Utilisateur de système d'exploitation/Nom de base de données
- Extension de la couverture des sources de données :
    - Reprise en ligne, chiffrement et génération de rapports améliorés depuis l'agent S-TAP sous System i
    - Filtrage, chaînage d'UID et convivialité étendus pour les agents S-TAP pour les sources de données z/OS
    - Fonctions de sécurité des données supplémentaires pour les plateformes big data : masquage des données dynamiques pour MongoDB, blocage pour HortonWorks et intégration à la plateforme de sécurité Ranger, ainsi que Cassandra Kerberos
        - Intégration Ranger - Ranger fournit une infrastructure de sécurité centralisée permettant de gérer un contrôle d'accès à granularité fine via Hadoop et les composants associés (Hive, HBase, HDFS, Yarn). A l'aide de la console d'administration Ranger, les utilisateurs peuvent aisément gérer des politiques concernant l'accès à une ressource (fichier, dossier, base de données, table, colonne, etc.) pour un ensemble spécifique d'utilisateurs et/ou de groupes et appliquer les politiques au sein de Hadoop. Ils peuvent également activer le suivi d'audit et l'analyse de politique pour un contrôle plus approfondi de l'environnement.
    - Prise en charge pour l'agent S-TAP de l'architecture RedHat 7.1 on Power 8 (big et little endian). Le terme "Endianness" fait référence à l'ordre des octets, formant un mot numérique, dans la mémoire d'ordinateur. Les mots peuvent être représentés au format big endian ou little endian. Le format little endian stocke l'octet de poids faible dans l'adresse mémoire la plus basse, l'octet de poids fort étant stocké dans l'adresse mémoire la plus élevée.
    - Nouvelle prise en charge pour DB2 Analytics Accelerator for z/OS
    - Prise en charge du chiffrement PostgreSQL 9.4 et SSL
    - Pour DB2 UDB et MS SQL, Guardium prend en charge count_big(*).
- Intégration de sécurité fournissant des cas d'utilisation en synergie pour les problèmes de sécurité représentant un défi, sur des silos IT :
    - Protection contre les menaces intérieures. Optimise l'intégration à IBM Security Privileged Identity Manager afin de reconnaître les menaces intérieures.
    - Système de protection contre les menaces. Fonctionne conjointement avec IBM Security QRadar et IBM Security XGS pour détecter les menaces avant qu'elles n'atteignent la source de données, pour prévenir les atteintes à la protection des données ou décupler la vigilance de surveillance.
- Aperçu technique pour les outils supplémentaires d'analyse d'accès aux données :
    - Le centre d'investigation fournit un espace central pour exécuter un suivi scientifique basé sur les enregistrements d'audit.

IBM Security Guardium Vulnerability Assessment version 10.1

- Mise à jour de la reconnaissance de sécurité avec le nouvel événement de sécurité commun (Common Vulnerability Event (CVE)) et d'autres tests de vulnérabilité
- Infrastructure commune partagée pour l'évaluation de vulnérabilité depuis la couche application jusqu'à l'infrastructure d'arrière-plan, avec un intégration à IBM Security AppScan

IBM Security Guardium for Files (FAM) version 10.1

- Evolutivité et performances améliorées pour soutenir le déploiement dans les organisations de grande taille
- Amélioration des performances de reconnaissance du moniteur File Activity Monitor (FAM)
- Support pour la reconnaissance FAM sous AIX 6.1 et Aix 7.1 (pas de classification). Support pour la reconnaissance et la classification des unités partagées sur le moteur d'exploration FAM.

Rubrique parent : Présentation du produit

Notes sur l'édition

Découvrez les fonctionnalités et améliorations les plus récentes, la configuration système requise, ainsi que les informations relatives à la mise à niveau, à l'installation et au support.

Description des fonctions nouvelles et des améliorations

La toute dernière version de Guardium comporte de nombreuses fonctions nouvelles ou améliorations de fonctionnalités existantes. Passez en revue les liens suivants pour connaître le détail des notes sur l'édition :

- Guardium version 10.1.4 - Notes sur l'édition
- Guardium version 10.1.3 - Notes sur l'édition
- Guardium version 10.1.2 - Notes sur l'édition
- Guardium version 10.1 - Notes sur l'édition

Annonce

Reportez-vous à l'annonce de l'édition IBM Guardium pour les informations suivantes :

- Description détaillée du produit, notamment des nouvelles fonctionnalités
- Positionnement du produit
- Informations de conditionnement et de commande
- Informations sur la compatibilité internationale

Configuration système requise

Pour la configuration système de Guardium version 10.1 et des informations sur les plateformes prises en charge, voir http://www-01.ibm.com/support/docview.wss?uid=swg27047801.

Mise à niveau de Guardium

Voir Mise à niveau de votre système Guardium pour des informations sur la mise à niveau vers la version la plus récente de Guardium.

Installation de Guardium

Voir Installation de votre système Guardium pour des informations sur l'installation de la version la plus récente de Guardium.

Problèmes connus

Les problèmes connus sont documentés et accessibles via le site Web du support IBM.

Quand des problèmes recensés sont résolus, le site Web du support IBM est mis à jour. Effectuez une recherche sur le site Web du support IBM afin de rapidement trouver des solutions palliatives ou des solutions aux problèmes, ainsi que d'autres documents comme les téléchargements ou la configuration système détaillée.

Cycle de vie du support

Si vous utilisez une version plus ancienne du logiciel Guardium, envisagez de prendre le temps d'effectuer des mises à niveau. Vous pouvez trouver des informations sur les dates de fin de prise en charge des produits IBM sur le site Web IBM Software Support Lifecycle.

Rubrique parent : Présentation du produit

Mise en route

- Initiation à l'interface utilisateur
  Apprenez les principes de base de l'interface utilisateur Guardium, notamment votre première connexion, les menus de la bannière et de navigation et la recherche de données et d'outils dans l'interface utilisateur.
- Personnalisation de l'interface utilisateur
  Guardium prend en charge la personnalisation du menu de navigation pour des utilisateurs et les rôles spécifiques.
- Configuration rapide de la surveillance et de la conformité
  Découvrez comment déployer des agents de surveillance sur vos serveurs de bases de données et comment configurer la surveillance des bases de données afin de maintenir la conformité aux normes de sécurité et réglementations en vigueur.
- Vue du système
  La Vue du système est celle qui s'affiche en premier pour nombre d'utilisateurs. Elle leur permet de prendre connaissance d'éléments clés témoignant de l'état du système.
- Surveillance de l'activité des données
  Description des concepts de sécurité clés sur lesquels repose la surveillance de l'activité des données dans Guardium.
- Surveillance de l'activité des fichiers
  La surveillance de l'activité des fichiers découvre les données sensibles sur vos serveurs, classifie les contenus sur la base de définitions préconfigurées ou créées par l'utilisateur et configure les règles et les politiques s'appliquant aux accès aux données ainsi que les actions à entreprendre lorsque les conditions des règles sont remplies.
- Concepts clés et outils
  Informations sur les concepts clés relatifs à l'administration de Guardium.

Information associée:
Présentation, architecture et interface utilisateur de Guardium (vidéo)

Initiation à l'interface utilisateur

Apprenez les principes de base de l'interface utilisateur Guardium, notamment votre première connexion, les menus de la bannière et de navigation et la recherche de données et d'outils dans l'interface utilisateur.

Navigation

Lorsque vous vous connectez pour la première fois à l'interface utilisateur Guardium, vous voyez deux menus principaux : celui de la bannière et le menu de navigation.

Vous pouvez déployer ou escamoter le menu de navigation en cliquant sur l'icône  . Vous pouvez aussi le masquer entièrement en cliquant sur l'icône  .

L'agencement initial de votre écran est fonction de la licence en vigueur, de l'accès que vous octroient vos rôles, du type de machine et d'un facteur de visibilité. Exemples de rôles : utilisateur, administrateur, gestionnaire des accès, CLI (interface de ligne de commande). Les rôles sont attribués aux utilisateurs et aux applications pour accorder aux utilisateurs des privilèges d'accès spécifiques.

Navigateurs web pris en charge

Internet Explorer 9 (IE9) et versions suivantes sous Windows 7. Précautions à prendre si vous utilisez IE9 - (1) vérifiez que le site web de votre société n'est pas listé dans la sélection Affichage de compatibilité d'Internet Explorer ; (2) Lors de l'exportation de fichiers, le téléchargement est bloqué par l'option "Ne pas enregistrer les pages chiffrées sur le disque", qui est cochée dans IE9. Décochez cette option afin que les opérations d'exportation et de téléchargement fonctionnent comme prévu.

Firefox ESR 24 et versions suivantes

Chrome 28 et versions suivantes

Résolution d'écran minimum : 1366 x 768

Menu de la bannière

La bannière contient les éléments suivants :

Élément	Description
Horloge système	Temps universel sur votre système Guardium.
Liste des tâches 	Contient la Liste des tâches du processus d'audit, qui peut être filtrée par utilisateur, et les Processus sans résultats en attente.
Aide 	Ouvrez l'aide du produit en cliquant sur Aide > Aide Guardium. Pour obtenir des informations sur votre système Guardium, telles que son numéro de version, cliquez sur Aide > A propos de Guardium. Pour afficher l'aide spécifique d'un écran ou d'une fonction avec laquelle vous travaillez, cliquez sur la petite icône d'aide incorporée dans le panneau concerné. Remarque : Les deux icônes d'aide vous mènent au même centre de documentation, dans lequel vous avez accès à l'intégralité de l'aide en ligne.
Recherche d'éléments de l'interface utilisateur / de données / de fichiers	Permet de rechercher une partie ou une fonction de l'interface utilisateur, une donnée ou un fichier. Par exemple, pour trouver le Générateur de politique, faites passer le type de recherche à Interface utilisateur et commencez à taper le terme `générateur de politique`. Cliquez sur l'un des résultats pour accéder à cette partie de l'interface utilisateur.
Type de compte	Indique quel type de compte vous avez. Vous pouvez aussi éditer les détails de votre compte (par exemple, changer votre mot de passe ou votre nom), personnaliser l'agencement de l'interface utilisateur et vous déconnecter proprement de Guardium.
Type de machine	Indique le type de machine sur lequel vous êtes connecté. Par exemple, autonome, unité gérée, gestionnaire central ou agrégateur.

Le menu de la bannière contient également des messages de démarrage importants : mémoire devenant insuffisante, quantité de mémoire et capacité processeur (nombre de coeurs) requises par la fonction Recherche rapide, expiration de certificat, échec de la gestion centrale, SSLv3 activé ou désactivé et absence de licence.

Remarque : Guardium recommande que SSLv3 soit désactivé. Cependant, avec les anciennes versions de Guardium, si SSLv3 est désactivé, la fonctionnalité de gestion centralisée sera amoindrie entre le gestionnaire central et les unités gérées.

Menu de navigation

Chaque icône du menu de navigation représente une phase particulière du cycle de vie de sécurité Guardium. Cliquez sur une icône pour révéler les composants de la phase correspondante. Le menu de navigation centré sur le cycle de vie est l'un des moyens dont vous disposez pour naviguer dans l'interface utilisateur. Par souci d'homogénéité, il se retrouve dans tous les rôles. Sa composition peut être personnalisée et certains éléments peuvent apparaître ou non selon votre rôle.

Phase	Description
Configuration 	Permet de configurer vos paramètres réseau, de vérifier l'état de vos services et de créer des définitions de sources de données, des groupes, des alias et des alertes.
Gestion 	Permet de gérer la santé générale de votre environnement, les S-TAP, les données, les modules, la maintenance et les rapports.
Reconnaissan	Permet de découvrir automatiquement les nouvelles bases de données introduites dans votre environnement, d'identifier les données sensibles et de

ce 	les classifier.
Renforcement 	Evalue les points faibles de votre environnement avec Vulnerability Assessment (VA) et surveille les changements qu'il subit avec Configuration Auditing System (CAS).
Examen 	Permet de surveiller les activités des bases de données et d'enquêter sur les activités suspectes dans n'importe quelle partie de votre environnement.
Protection 	Permet de protéger votre environnement avec des politiques de sécurité bloquant les activités suspectes et prévenant tout accès non autorisé aux données. Pour plus d'informations sur les politiques, consultez Politiques.
Conformité 	Initiatives de mise en conformité avec des processus d'audit et des rapports à granularité variable.
Rapports 	Créez votre propre rapport ou utilisé l'un des nombreux rapports prédéfinis pour obtenir un compte rendu sur n'importe quelle partie de votre environnement. Pour plus d'informations sur les rapports, consultez Rapports.
Mes tableaux de bord 	Créez vos propres tableaux de bord afin de consulter facilement les rapports qui sont d'un intérêt capital pour vous. Pour plus d'informations sur les tableaux de bord, consultez Création de tableaux de bord.

Icônes communes

Ce jeu d'icônes est commun à nombre d'applications de recherche et de construction ou génération dans Guardium.

Icône	Description
Nouveau 	Crée un nouvel élément tel qu'un groupe ou une définition de source de données.
Modifier 	Modifie un élément. Remarque : Lorsque vous voulez modifier un élément, mieux vaut en faire une copie (le cloner) et apporter les modifications au clone plutôt qu'à l'élément d'origine.
Cloner 	Permet de cloner un élément afin d'en créer une copie.
Supprimer 	Supprime un élément.

Rubrique parent : Mise en route

Personnalisation de l'interface utilisateur

Guardium prend en charge la personnalisation du menu de navigation pour des utilisateurs et les rôles spécifiques.

Les outils Personnaliser le menu de navigation et Personnaliser utilisateur/rôle vous permettent de changer facilement le contenu et l'organisation du menu de navigation. Ils sont accessibles en plusieurs endroits :

- Tous les utilisateurs peuvent personnaliser leur propre menu de navigation en ouvrant le menu Utilisateur dans la bannière de Guardium et en sélectionnant Personnaliser.
- Les utilisateurs administratifs peuvent personnaliser le menu de navigation pour le compte d'autres utilisateurs et rôles en ouvrant le menu Utilisateur et en choisissant Personnaliser utilisateur/rôle ou en accédant à Configurer > Outils et vues > Personnaliser utilisateur/rôle.
- Les utilisateurs connectés en tant que *accessmgr* peuvent personnaliser le menu de navigation pour le compte d'autres utilisateurs et rôles en allant à Accès > Gestion des accès, en choisissant Navigateur de rôles, puis en cliquant sur le lien Personnaliser le menu de navigation.

L'outil fournit à tous les utilisateurs une expérience de personnalisation cohérente et homogène.

La liste Menu de navigation reflète l'organisation et le contenu du système de navigation de Guardium. Sélectionnez outils et rapports dans la liste Outils et rapports disponibles et utilisez l'icône  pour ajouter des entrées à la liste Menu de navigation. Retirez des entrées de la liste Menu de navigation en cliquant sur l'icône  en regard de chaque entrée concernée. Pour réorganiser les entrées de la liste Menu de navigation, faites-les glisser ou utilisez les icônes adéquates.

Vous pouvez définir une nouvelle page d'accueil Guardium (première page vue par l'utilisateur lorsqu'il se connecte au système) en choisissant l'entrée voulue dans la liste Menu de navigation et en cliquant sur l'icône  .

Dès que vous cliquez sur le bouton OK, le menu de navigation de Guardium est mis à jour pour refléter les changements que vous avez entrepris dans la liste Menu de navigation.

L'utilisation de ces outils est soumise aux limitations suivantes :

- Vous ne pouvez pas supprimer le groupe Mes tableaux de bord. Vous pouvez en revanche supprimer individuellement des tableaux de bord dans ce groupe.
- Les nouveaux groupes ne seront pas sauvegardés s'ils sont vides.
- Les groupes vides visibles dans la liste Menu de navigation n'apparaîtront pas dans le menu de navigation de Guardium.

Rubrique parent : Mise en route
Information associée:
Gestion des rôles et des autorisations

Configuration rapide de la surveillance et de la conformité

Découvrez comment déployer des agents de surveillance sur vos serveurs de bases de données et comment configurer la surveillance des bases de données afin de maintenir la conformité aux normes de sécurité et réglementations en vigueur.

Pourquoi et quand exécuter cette tâche

La configuration rapide de la surveillance et de la mise en conformité s'appuie sur les deux outils suivants :

Déploiement d'agents de surveillance

Utilisez l'outil Déploiement d'agents de surveillance pour activer automatiquement les clients GIM, installer des S-TAP et commencer à surveiller le trafic des bases de données.

L'outil de déploiement d'agents de surveillance simplifie le processus de déploiement d'une installation Guardium. S'appuyant sur l'infrastructure existante de Guardium Installation Manager (GIM), cet outil vous aide à trouver rapidement les serveurs de bases de données, à installer des agents de surveillance (S-TAP) et à configurer des moteurs d'inspection (Guardium Inspection Engine) pour vos bases de données. Il offre en outre une vue centralisée grâce à laquelle vous pouvez suivre et passer en revue le statut de déploiement.

Surveillance de conformité

Après avoir déployé vos agents de surveillance (S-TAP), utilisez l'outil Surveillance de conformité pour surveiller votre environnement et s'assurer qu'il respecte des normes de sécurité et des réglementations spécifiques.

Guardium fournit plusieurs modèles de surveillance de conformité--groupes, politiques de sécurité et rapports correspondant à différentes normes et réglementations spécifiques--notamment les suivants :

- Basel Committee on Banking Supervision (Comité de Bâle sur le contrôle bancaire) (BASEL II)
- General Data Protection Regulation (Règlement général sur la protection des données) (GDPR)
- General Data Protection Regulation pour Db2 for z/OS (GDPR pour Db2 for z/OS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Security Standard (Norme de sécurité de l'industrie des cartes de paiement) (PCI)
- Personally Identifiable Information (Données personnelles identifiables) (PII)
- Sarbanes-Oxley Compliance (Conformité à la Loi Sarbanes-Oxley) (SOX)

Ces modèles de surveillance de conformité permettent aux organisations d'être rapidement opérationnelles. A ce titre, ils sont particulièrement utiles à celles qui ont peu de temps pour se mettre en conformité avec l'une des normes ou réglementations couvertes. Une fois les politiques de sécurité installées, l'outil de surveillance de conformité guide les administrateurs ou "compliance officers" à travers la création de groupes qu'ils doivent ensuite remplir avec les informations spécifiques de l'organisation, telles que les adresses IP des clients et les ID utilisateur titulaires de privilèges particuliers. L'outil vérifie également votre environnement Guardium à intervalles réguliers afin d'identifier les nouvelles bases de données susceptibles d'être mises sous surveillance avec les modèles de surveillance de conformité.

Procédure

1. Passez en revue les informations suivantes pour commencer à vous familiariser avec les outils.
   - Déploiement rapide d'agents de surveillance
   - Configuration rapide de la surveillance de conformité
2. Déployez des agents de surveillance pour vos serveurs de bases de données.
   a. Vérifiez que vous remplissez les conditions préalables à l'utilisation de l'outil de déploiement d'agents de surveillance : Prérequis pour le déploiement d'agents de surveillance.
   b. Déployez des agents de surveillance sur vos serveurs de bases de données : Déploiement d'agents de surveillance.
3. Configurez la surveillance de conformité pour vos serveurs de bases de données.
   a. Vérifiez que vous remplissez les conditions préalables à l'utilisation de l'outil de surveillance de conformité : Prérequis pour la surveillance de conformité
   b. Configurez la surveillance de conformité : Configuration de la surveillance de conformité.
   c. Identifiez les utilisateurs et les applications autorisés à accéder à vos bases de données en les ajoutant aux groupes : Remplissage de groupes.
   d. Fournissez les données d'identification qui permettront à Guardium d'accéder à vos bases de données pour découvrir et classifier les données sensibles : Activer la recherche de données sensibles

Résultats

Une fois les agents de surveillance correctement déployés, la surveillance de conformité étant en place pour vos serveurs de bases de données, Guardium commence à surveiller les échanges avec vos bases de données.

Pour plus d'informations sur l'interprétation de ce que vous voyez sur la page de surveillance de conformité, consultez Comprendre les vues de surveillance de conformité.

Rubrique parent : Mise en route

Vue du système

La Vue du système est celle qui s'affiche en premier pour nombre d'utilisateurs. Elle leur permet de prendre connaissance d'éléments clés témoignant de l'état du système.

Trois onglets rattachés à la Vue du système affichent différents types d'informations d'état :

- L'onglet Moniteur d'état S-TAP affiche une synthèse des agents de surveillance S-TAPs déployés dans votre environnement. L'état général de chaque S-TAP est représenté par différentes icônes. Vous pouvez obtenir une vue plus détaillée sur les moteurs d'inspection d'un S-TAP en cliquant sur celui-ci.
- L'onglet Utilisation d'unités affiche des informations sur l'utilisation de chaque système Guardium.
- L'onglet Moniteur système affiche des détails régulièrement actualisés sur les données entrantes, l'utilisation d'UC (processeur) et d'autres informations.

Rubrique parent : Mise en route

Surveillance de l'activité des données

Description des concepts de sécurité clés sur lesquels repose la surveillance de l'activité des données dans Guardium.

- Politiques et règles
  Une politique de sécurité contient un ensemble ordonné de règles à appliquer au trafic observé entre clients et serveurs de bases de données. Chaque règle peut s'appliquer à une demande d'un client ou à une réponse d'un serveur. Plusieurs politiques peuvent être définies et installées en même temps sur un système Guardium.
- Flux de travaux
  Un flux de travaux réunit plusieurs tâches de surveillance des activités des bases de données, notamment la découverte des actifs, l'évaluation des vulnérabilités et la recommandation de mesures de durcissement, la surveillance des activités des bases de données et la production de rapports d'audit, la distribution des rapports, l'acceptation (aval) par les parties prenantes et l'escalade.
- Audit
  Guardium fournit des fonctions d'audit qui permettent de suivre les changements apportés aux valeurs dans les tables de base de données.
- Classification
  Guardium permet de découvrir et classifier les données sensibles, autorisant ainsi la création et la mise en application de politiques d'accès efficaces.

Rubrique parent : Mise en route

Politiques et règles

Une politique de sécurité contient un ensemble ordonné de règles à appliquer au trafic observé entre clients et serveurs de bases de données. Chaque règle peut s'appliquer à une demande d'un client ou à une réponse d'un serveur. Plusieurs politiques peuvent être définies et installées en même temps sur un système Guardium.

Chaque règle dans une politique définit une action conditionnelle. La condition peut être un simple test, par exemple un contrôle visant à détecter tout accès par une adresse IP de client qui ne figure pas dans le groupe IP client autorisées du serveur. Il peut aussi s'agir d'un test complexe, dans lequel sont évalués plusieurs attributs de message et de session tels que l'utilisateur de base de données, le programme source, le type de commande, l'heure, etc. Les règles peuvent aussi être sensibles au nombre de fois où telle ou telle condition se vérifie en un laps de temps déterminé.

L'action déclenchée par la règle peut être une notification (e-mail envoyé à un ou plusieurs destinataires, par exemple), un blocage (la session du client peut être déconnectée) ou la simple consignation de l'événement comme violation de la politique en vigueur. Des actions personnalisées peuvent être développées pour exécuter toute tâche nécessaire en réponse à certaines conditions qui peuvent être propres à un environnement ou une application donnés.

Rubrique parent : Surveillance de l'activité des données

Flux de travaux

Un flux de travaux réunit plusieurs tâches de surveillance des activités des bases de données, notamment la découverte des actifs, l'évaluation des vulnérabilités et la recommandation de mesures de durcissement, la surveillance des activités des bases de données et la production de rapports d'audit, la distribution des rapports, l'acceptation (aval) par les parties prenantes et l'escalade.

Les flux de travaux visent à transformer l'activité manuelle périodique de gestion de la sécurité des bases de données en un processus continuellement automatisé, prenant en compte les besoins en matière de confidentialité et de gouvernance de l'entreprise, par exemple la conformité à des normes ou réglementations telles que PCI-DSS (Norme de sécurité de l'industrie des cartes de paiement), SOX (Loi Sarbanes-Oxley), Data Privacy et HIPAA (Loi Health Insurance Portability Accountability Act). Les flux de travaux se prêtent également à l'exportation des résultats d'audit vers des référentiels externes en vue d'une analyse légale complémentaire. Cette exportation peut se faire par l'intermédiaire de Syslog, de fichiers CSV/CEF ou de flux externes.

Par exemple, un processus d'automatisation du flux de travail de conformité pourrait tenter de répondre aux questions suivantes : de quel type de rapport, d'évaluation, de piste d'audit ou de classification a-t-on besoin, à qui ces informations doivent-elles être communiquées et comment les acceptations sont-elles prises en charge, et quel est le calendrier de livraison ?

Rubrique parent : Surveillance de l'activité des données

Audit

Guardium fournit des fonctions d'audit qui permettent de suivre les changements apportés aux valeurs dans les tables de base de données.

Pour chaque table dans laquelle les changements doivent être suivis, vous pouvez choisir quelles commandes SQL de changement de valeur (insert, update, delete) sont à surveiller. Les valeurs avant et après traitement sont capturées chaque fois qu'une telle commande est exécutée sur une table sous surveillance. Ces activités de changement sont transférées à Guardium selon un horaire planifié, après quoi toutes les fonctions de reporting et d'alerte de Guardium peuvent être utilisées.

Les données sur les changements de valeurs sont consultables dans le rapport par défaut Valeurs changées. Vous pouvez aussi créer vos propres rapports en utilisant le domaine Suivi des changements de valeurs.

Rubrique parent : Surveillance de l'activité des données

Classification

Guardium permet de découvrir et classifier les données sensibles, autorisant ainsi la création et la mise en application de politiques d'accès efficaces.

Une politique de classification est en ensemble de règles conçues pour découvrir et étiqueter les éléments de données sensibles. Des actions peuvent être définies pour chaque règle d'une politique de classification. Il peut s'agir, par exemple, de générer une alerte par e-mail ou d'ajouter un membre à un groupe Guardium. Les politiques de classification peuvent être configurées pour être exécutées à horaires fixes, sur des sources de données spécifiées ou en tant que tâches d'un flux de travaux.

Les routines de découverte et de classification prennent de l'importance à mesure que l'organisation croît et que des informations sensibles telles que numéros de cartes de crédit et données financières personnelles deviennent présentes en plusieurs endroits, souvent sans que les administrateurs en charge de ces données n'en ait connaissance. Cela arrive fréquemment dans le contexte de fusions et d'acquisitions d'entreprises ou encore lorsque d'anciens systèmes survivent à leurs premiers propriétaires. Guardium découvre de telles données sensibles et les étiquette de manière à leur appliquer des politiques d'accès appropriées.

Rubrique parent : Surveillance de l'activité des données

Surveillance de l'activité des fichiers

La surveillance de l'activité des fichiers découvre les données sensibles sur vos serveurs, classifie les contenus sur la base de définitions préconfigurées ou créées par l'utilisateur et configure les règles et les politiques s'appliquant aux accès aux données ainsi que les actions à entreprendre lorsque les conditions des règles sont remplies.

La surveillance de l'activité des fichiers se compose des capacités suivantes :

- La reconnaissance inclut la collecte des métadonnées et des autorisations pour les fichiers et les dossiers.
- La classification utilise des *plans de décision* afin d'identifier les données sensibles dans les fichiers, telles que des informations de carte de crédit ou des informations identifiant la personne.
- Surveillance et collecte des règles de politique et des informations d'audit, et alertes en temps réel ou blocage des connexions ou utilisateurs suspect(e)s.

Surveillance de l'activité des fichiers :

- Conformité aux réglementations avec un bon rapport coût-efficacité
    - Automatise et centralise les contrôles, fournit une trace d'audit.
    - Maintient la conformité aux diverses lois et normes telles que HIPAA (Loi Health Insurance Portability Accountability Act), PCI-DSS (Norme de sécurité de l'industrie des cartes de paiement) et aux différentes réglementations régionales et nationales sur la confidentialité.
- Évolue avec l'accroissement des volumes de données et les besoins d'expansion de l'entreprise
- Fournit un support étendu et hétérogène couvrant tous les systèmes populaires

Cas d'utilisation 1

Des fichiers d'applications critiques peuvent être modifiés, voire détruits suite à un accès en arrière-plan au serveur d'applications ou de bases de données

Solution : la surveillance de l'activité des fichiers peut découvrir et placer sous surveillance vos fichiers de configuration, fichiers journaux, codes source et autres fichiers sensibles puis, lorsqu'un utilisateur ou un processus non autorisé tente d'y accéder, vous alerter ou lui barrer l'accès.

Cas d'utilisation 2

Vous avez besoin de protéger des fichiers contenant des informations identifiant les personnes ou des informations confidentielles sans impacter l'activité au quotidien.

Solution : la surveillance de l'activité des fichiers peut découvrir vos documents sensibles stockés sur de nombreux systèmes de fichiers et surveiller leurs accès. Elle agrégera les données, vous donnera un vue de l'activité et vous alertera en cas d'accès suspect ; elle vous permettra également de barrer l'accès à une sélection de fichiers et de dossiers, pour une sélection d'utilisateurs.

Scénario d'utilisation 3

Vous avez besoin de bloquer les accès en arrière-plan aux documents gérés par votre application.

Solution : la surveillance de l'activité des fichiers peut découvrir vos documents normalement accessibles à travers un frontal d'application (par exemple, un portail web), les placer sous surveillance et bloquer leur accès en arrière-plan.

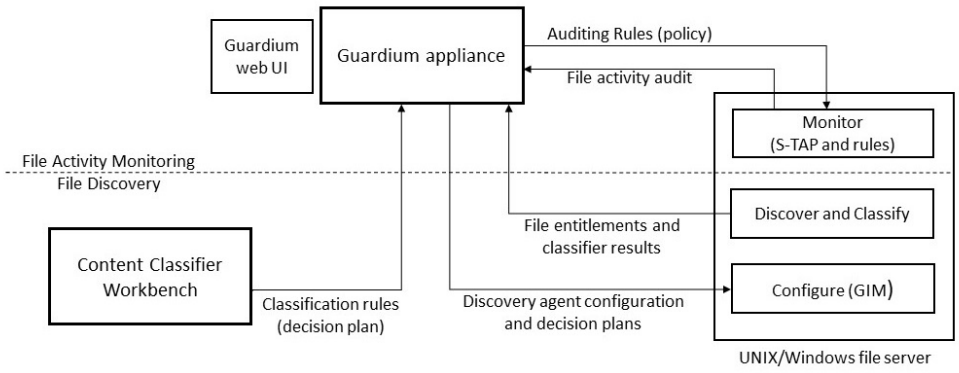
- Présentation et concepts de la surveillance de l'activité des fichiers
- Prérequis pour la surveillance de l'activité des fichiers
- Flux de travaux général pour la surveillance de l'activité des fichiers
  Utilisez ce flux de travaux général pour planifier et mettre en place une surveillance des activités des fichiers.

Rubrique parent : Mise en route
Information associée:
Surveillance de l'activité des fichiers avec Guardium (vidéo)

Présentation et concepts de la surveillance de l'activité des fichiers

La surveillance de l'activité des fichiers comprend les fonctions suivantes :

- La reconnaissance inclut la collecte des métadonnées et des autorisations pour les fichiers et les dossiers.
- La classification utilise des *plans de décision* afin d'identifier les données sensibles dans les fichiers, telles que des informations de carte de crédit ou des informations identifiant la personne.
- Surveillance et collecte des règles de politique et des informations d'audit, et alertes en temps réel ou blocage des connexions ou utilisateurs suspect(e)s.



Reconnaissance et classification

L'examen de **reconnaissance** de base identifie la liste de dossiers et de fichiers, leur propriétaire, leurs droits d'accès, leur taille, ainsi que la date et l'heure de la dernière mise à jour. Il identifie également les droits d'utilisateur et les droits de groupe. Le processus de reconnaissance prend en charge tous les types de fichier. La **classification** est définie par des *plans de décision*. Chaque plan de décision contient des règles visant à réorganiser un certain type de données. (Les plans de décision pour la surveillance de l'activité des fichiers sont identiques aux politiques de classification de la surveillance de l'activité des données.) La classification inclut la prise en charge d'un grand nombre de types de fichier, notamment Texte brut, HTML Office, PDF. Des plans de décision par défaut existent pour HIPAA, PCI, SOX et Source Code. Vous pouvez changer les entités de classification des rapports obtenus/du tableau de bord d'investigation à l'aide des plans de décision par défaut. De plus, vous pouvez créer de nouveaux plans ou modifier des plans existants à l'aide du classifieur de contenus, une application Windows que vous téléchargez sur votre dispositif de collecteur. Pour connaître les prérequis pour IBM Content Classification version 8.8, voir la note technique IBM http://www-01.ibm.com/support/docview.wss?uid=swg27020838. Des plans sont activés et configurés via Guardium Installation Manager (GIM).

La reconnaissance et la classification sont gérées par un agent de reconnaissance, appelé moteur d'exploration des fichiers. Le moteur d'exploration des fichiers envoie les métadonnées et les fichiers de données issues de ses processus de reconnaissance et de classification au système Guardium. La planification d'examen est configurable. D'autres examens (incrémentiels), exécutés après la reconnaissance et la classification initiales, identifient les changements incrémentiels apportés aux fichiers nouveaux et modifiés uniquement. Installez et configurez le moteur d'exploration des fichiers à l'aide de Guardium Installation Manager (GIM), comme vous le feriez pour n'importe quel autre bundle.

Surveillance, audit et blocage

La surveillance de l'activité des fichiers est implémentée par l'agent S-TAP, qui s'exécute sur le serveur de fichiers. (La surveillance de l'activité ne nécessite pas le bundle FAM utilisé par le processus de reconnaissance et de classification.) Pour les volumes NFS, il est important qu'un agent S-TAP soit installé et configuré sur toutes les machines qui ont accès à ces volumes. L'agent S-TAP gère les actions de surveillance, de création d'alertes et de blocage effectuées en continu pour l'accès aux fichiers en fonction des règles de politique Guardium. Les règles spécifient les serveurs de fichiers et les fichiers à surveiller, ainsi que les actions à exécuter si des règles de politique sont violées, par exemple, consigner la violation, l'alerte ou le blocage d'un accès. Les opérations surveillées sont les suivantes : Lecture, Ecriture, Exécution, Suppression, Changement de propriétaire, Droits, Propriétés. Toute activité qui correspond aux critères des règles de politique de sécurité est envoyée au collecteur Guardium où elle est stockée dans le référentiel Guardium. (Dans le cadre de la surveillance de l'activité de base de données, l'agent S-TAP envoie l'activité de toutes les données à Guardium, où elle est surveillée.) Tous les événements enregistrés dans le référentiel Guardium sont des événements audités.

Etant donné que les règles de surveillance des fichiers sont activées dans l'agent S-TAP, un blocage se produit immédiatement. Les données demandées par l'utilisateur ne sont jamais lues à partir du disque ; l'agent S-TAP bloque et empêche l'opération. L'accès aux fichiers peut aussi être bloqué, même s'il est autorisé par les droits du système d'exploitation.

Les activités surveillées sont présentées dans les rapports prédéfinis : Privilèges des utilisateurs, Privilèges sur les fichiers, Nombre d'activités par utilisateur, Nombre d'activités par client, Fichiers ouverts au "public", Utilisateurs dormants, Fichiers dormants, etc., dans le rapport d'accès FAM (journal de l'ensemble des activités surveillées) dans le tableau de bord d'investigation.

Important : Les activités de l'administrateur Windows et de l'utilisateur racine Linux ne sont pas surveillées ni bloquées par la surveillance de l'activité des fichiers.

Un agent S-TAP gère la surveillance de l'activité de serveur de fichiers et de base de données. Si vous possédez des licences pour ces deux fonctions, vous pouvez utiliser le même agent S-TAP pour la surveillance de l'activité des fichiers et de la base de données. Installez et configurez l'agent S-TAP à l'aide de Guardium Installation Manager (GIM), comme vous le feriez pour n'importe quel bundle.

Rubrique parent : Surveillance de l'activité des fichiers

Prérequis pour la surveillance de l'activité des fichiers

Installez les composants suivants pour exécuter la surveillance de l'activité des fichiers :

- Client GIM sur tous les serveurs de fichiers
- Agent S-TAP
- Clés de licence
- Agent de reconnaissance FAM (également appelé bundle FAM ou agent FAM, obligatoire pour le processus de reconnaissance et de classification)
- Serveur IBM Content Classification (facultatif) pour les plans de décision non définis par défaut (http://www-01.ibm.com/support/docview.wss?uid=swg27020838)

La surveillance de l'activité des fichiers prend en charge la chaîne d'ID utilisateur : l'agent FAM remplace un nom d'utilisateur en une chaîne de noms d'utilisateur appartenant à l'historique du processus (chaîne d'ID utilisateur). Par exemple, si le processus 1 (utilisateur janedoe) crée le processus 2 (utilisateur johndoe), pour les événements de fichiers liés au processus #2, l'agent FAM signale la chaîne d'ID utilisateur {janedoe, johndoe}.

La surveillance de l'activité des fichiers ne prend pas en charge :

- Le stockage en réseau (NAS)

La surveillance de l'activité des fichiers prend en charge les serveurs suivants :

Version de plateforme	Surveillance FAM	Reconnaissance FAM	Classification FAM

Version de plateforme	Surveillance FAM	Reconnaissance FAM	Classification FAM
aix-7.1-aix-powerpc	Oui	Oui	Non
aix-6.1-aix-powerpc	Oui	Oui	Non
Red Hat 4 PowerPC	Oui	Non	Non
Red Hat 5 S390X	Oui	Non	Non
rhel-4-linux-i686	Oui	Non	Non
rhel-4-linux-ia64	Non	Non	Non
rhel-4-linux-x86_64	Oui	Non	Non
rhel-5-linux-i686	Oui	Oui	Oui
rhel-5-linux-ia64	Non	Non	Non
rhel-5-linux-ppc64	Oui	Non	Non
rhel-5-linux-x86_64	Oui	Oui	Oui
rhel-6-linux-i686	Oui	Oui	Oui
rhel-6-linux-ppc64	Oui	Non	Non
rhel-6-linux-s390x	Oui	Non	Non
rhel-6-linux-x86_64	Oui	Oui	Oui
rhel-7-linux-x86_64	Oui	Oui	Oui
suse-10-linux-i686	Oui	Oui	Oui
SharePoint 2013	Non	Non	Oui
suse-10-linux-ppc64	Oui	Non	Non
suse-10-linux-s390x	Oui	Non	Non
suse-10-linux-x86_64	Oui	Oui	Oui
suse-11-linux-i686	Oui	Oui	Oui
suse-11-linux-s390x	Oui	Non	Non
suse-11-linux-x86_64	Oui	Oui	Oui
suse-12-linux-x86_64	Oui	Oui	Non
Ubuntu 10 x86/64	Oui	Oui	Non
Ubuntu 12 x86/64	Oui	Oui	Oui
Ubuntu 14 x86/64	Oui	Oui	Non
Windows 2008 Server	Oui	Oui	Oui
Windows 2012 Server	Oui	Oui	Oui

Rubrique parent : Surveillance de l'activité des fichiers

Flux de travaux général pour la surveillance de l'activité des fichiers

Utilisez ce flux de travaux général pour planifier et mettre en place une surveillance des activités des fichiers.

Flux de travaux général pour la surveillance de l'activité des fichiers

1. Installation et activation des composants de surveillance de l'activité des fichiers sur tous les serveurs de fichiers.
2. Reconnaissance et classification de données sensibles dans des serveurs de fichiers.
3. Optionnel : Personnalisation des plans de décision FAM. Vous pouvez utiliser les plans de décision par défaut ou créer vos propres plans en utilisant IBM Content Classification.
4. Surveillance et audit
   - L'activité des fichiers peut être incluse dans les rapports, notamment dans les rapports prédéfinis suivants : Privilèges des utilisateurs, Privilèges sur les fichiers, Nombre d'activités par utilisateur, Nombre d'activités par client, Fichiers ouverts au “public”, Utilisateurs dormants, Fichiers dormants, etc.
   - Pour les investigations et analyses continues, utilisez les Tableaux de bord d'investigation, qui incluent des capacités de recherche de texte et de mise en évidence des valeurs extrêmes ainsi que des fonctions de visualisation évoluées. Voir :
     - Tableau de bord d'investigation pour les fichiers
     - Interprétation des valeurs extrêmes pour l'activité de fichier
5. Protection : créez et appliquez des politiques pour une surveillance et une protection continues. Voir Politiques et règles relatives à l'activité des fichiers.

- UNIX : le niveau de débogage est configuré par tap_debug_output_level. Les journaux d'erreurs et de débogage FAM ont pour nom guard_stap.fam.txt. L'emplacement par défaut dans UNIX est \tmp, et est configuré par tap_log_dir
- Windows : le fichier journal de l'agent FAM s'appelle StapAT.ctl et se trouve dans le dossier C:\Program Files\IBM\Windows S-TAP\Logs.

Rubrique parent : Surveillance de l'activité des fichiers

Concepts clés et outils

Informations sur les concepts clés relatifs à l'administration de Guardium.

- Requêtes et rapports
  Les requêtes Guardium décrivent un ensemble d'informations à obtenir des données recueillies. Les rapports définissent de quelle manière les données obtenues

par une requête Guardium sont présentées.

- Contrôle d'accès
  Guardium s'appuie sur le principe de cartes d'accès pour représenter les accès aux données entre clients et serveurs de bases de données.
- Rôles d'utilisateur
  Un rôle définit un groupe d'utilisateurs Guardium ayant les mêmes privilèges d'accès.
- Groupes
  Guardium permet de grouper divers éléments pour simplifier la création et la gestion des politiques ainsi que pour clarifier la présentation des rapports.
- Archivage et purge des données
  L'opération Archivage des données sauvegarde les données qui ont été capturées par un système Guardium. Lorsque vous la configurez, vous pouvez aussi spécifier les critères de purge des données.
- Guardium Installation Manager
  Guardium Installation Manager (GIM) sert à installer et tenir à jour les composants de Guardium sur les systèmes gérés.

Rubrique parent : Mise en route

Requêtes et rapports

Les requêtes Guardium décrivent un ensemble d'informations à obtenir des données recueillies. Les rapports définissent de quelle manière les données obtenues par une requête Guardium sont présentées.

Les requêtes Guardium décrivent un ensemble d'informations obtenues à partir des données recueillies. Elles comprennent trois éléments : les entités, les champs et les conditions. Les entités définissent la portée de la requête, les champs dressent la liste des colonnes de données à retourner par la requête et les conditions définissent les tests à appliquer aux données (supérieur à, inférieur à, contient, etc.) pour déterminer si elles correspondent à ce que l'on recherche.

Un rapport définit de quelle manière sont présentées les données recueillies par une requête. Le rapport par défaut est un tableau (rapport tabulaire) reflétant la structure de la requête, chaque attribut étant affiché dans une colonne à part. Tous les paramètres d'exécution et composants de présentation d'un rapport tabulaire peuvent être personnalisés.

Rubrique parent : Concepts clés et outils

Contrôle d'accès

Guardium s'appuie sur le principe de cartes d'accès pour représenter les accès aux données entre clients et serveurs de bases de données.

L'accès aux données par les applications et les outils peut être catégorisé en de nombreuses dimensions, exprimant notamment à quelles données ces applications et outils accèdent, de quelle manière ils y accèdent et combien d'appels SQL ils émettent. Dans un environnement d'entreprise, il est très important d'avoir une bonne maîtrise de l'accès aux bases de données. Cette exigence peut résulter de l'obligation de comprendre et de sécuriser l'accès à la base de données en raison d'initiatives de mise en conformité, voire en raison de la nécessité d'ajuster et d'optimiser votre environnement de base de données. Comme ce dernier peut comprendre de nombreuses bases de données et un très grand nombre de clients de base de données, il peut être difficile de maîtriser tous les chemins d'accès aux données.

Les vues de la table et de la topologie de santé du déploiement présentent les relations de flux de données entre les systèmes de votre environnement. Ces vues facilitent l'identification des systèmes présentant des problèmes et l'examen des problèmes sous-jacents. Vous pouvez accéder à la vue de topologie via Gérer > Vue système > Topologie de santé du déploiement. Vous pouvez accéder à la table via Gérer > Vue système > Table de santé du déploiement.

Rubrique parent : Concepts clés et outils

Rôles d'utilisateur

Un rôle définit un groupe d'utilisateurs Guardium ayant les mêmes privilèges d'accès.

Lorsqu'un rôle est associé à un composant tel qu'une application ou la définition d'un élément (par exemple, une requête spécifique), seuls les utilisateurs Guardium auxquels ce rôle est affecté peuvent accéder au composant en question. Si aucun rôle de sécurité n'est associé à un composant (par exemple, un rapport), ce dernier n'est accessible qu'à l'utilisateur qui l'a défini et à l'utilisateur administrateur.

A l'installation, Guardium est configuré avec un ensemble par défaut de rôles et un ensemble par défaut de comptes d'utilisateur. Le gestionnaire des accès Guardium peut créer de nouveaux rôles et modifier les rôles existants selon nécessité.

Rubrique parent : Concepts clés et outils

Groupes

Guardium permet de grouper divers éléments pour simplifier la création et la gestion des politiques ainsi que pour clarifier la présentation des rapports.

Les processus de création des politiques et des définitions de requêtes peuvent être simplifiés par le groupement des éléments qui les composent. Il est souvent utile de grouper les éléments du même type. La présentation des informations dans les rapports s'en trouve alors simplifiée. Les groupes sont utilisés par tous les sous-systèmes. Tous les utilisateurs partagent un même ensemble de groupes.

A titre d'exemple, supposons que votre société ait à gérer 25 objets de données séparés, contenant des informations sensibles sur ses employés. Vous avez besoin de créer un rapport rendant compte de tous les accès à ces objets. Vous pourriez à cet effet formuler une très longue requête testant chacun des 25 objets. Mais vous pourriez aussi définir un unique groupe nommé infos sensibles employés, contenant ces 25 objets. Ainsi, dans vos définitions de requêtes et de règles, vous n'auriez plus qu'à tester si un objet est membre de ce groupe.

Un autre avantage des groupes est qu'ils facilitent la maintenance des données et rendent les choses plus simples lorsque leur composition vient à changer. Pour continuer avec l'exemple précédent, si votre société décidait que deux autres objets doivent être ajoutés au groupe 'infos sensibles employés', vous n'auriez qu'à mettre à jour la définition de ce groupe et non celle des requêtes, rapports et politiques qui y font référence.

Rubrique parent : Concepts clés et outils

Archivage et purge des données

L'opération Archivage des données sauvegarde les données qui ont été capturées par un système Guardium. Lorsque vous la configurez, vous pouvez aussi spécifier les critères de purge des données.

Il y a deux opérations d'archivage : Archivage des données et Archivage des résultats. Le chemin menant à ces opérations est Gérer > Gestion des données > Archivage des données ou Archivage des résultats (audit).

Archivage des données
: Avec cette opération, les données capturées quotidiennement sont généralement archivées en fin de journée, ce qui garantit qu'en cas de catastrophe, seules les données du jour sont perdues. La purge des données dépend quant à elle de l'application ainsi que des besoins de l'entreprise et des exigences de conservation aux fins d'audit, mais dans la plupart des cas, les données peuvent être conservées sur les machines pendant plus de six mois.

Archivage des résultats
: Cette opération sauvegarde les résultats des tâches d'audit (par exemple, les rapports, les tests d'évaluation, la trace d'audit des entités, les jeux de confidentialité et les processus de classification), ainsi que les traces de revue et d'acceptation et les commentaires adaptés des processus du flux de travaux. Les ensembles de résultats sont supprimés (purgés) du système en fonction de la définition des processus du flux de travaux.

Dans un environnement d'agrégation, les données peuvent être archivées à partir du collecteur, de l'agrégateur ou des deux. Il est cependant plus courant qu'elles ne soient archivées que d'un seul de ces deux endroits, celui-ci variant selon les besoins du client.

Rubrique parent : Concepts clés et outils

Guardium Installation Manager

Guardium Installation Manager (GIM) sert à installer et tenir à jour les composants de Guardium sur les systèmes gérés.

Le composant GIM inclut un serveur (le serveur GIM), qui est installé avec les autres composants du système Guardium, et un client (le client GIM), que vous devez installer sur chaque serveur hébergeant une base de données et sur chaque serveur de fichiers que vous voulez surveiller. Une fois installé, le client GIM fonctionne de pair avec le serveur GIM pour l'exécution des tâches suivantes :

- Vérifier s'il y a des mises à jour à appliquer au logiciel installé
- Transférer et installer le nouveau logiciel
- Désinstaller le logiciel
- Mettre à jour les paramètres du logiciel

Si votre environnement inclut un système Guardium configuré comme gestionnaire central (CM), vous devez décider quels systèmes Guardium doivent être utilisés en tant que serveurs GIM. Vous pouvez soit gérer tous vos clients GIM depuis un seul système Guardium, tel que le gestionnaire central, soit les gérer en groupes, à partir des différents systèmes Guardium. Si vous optez pour la gestion de tous les clients GIM depuis un même système Guardium, tous seront visibles et gérables depuis la même interface. Si vous choisissez de les gérer en groupes, à partir de différents systèmes Guardium, vous pourrez utiliser chacun de ces systèmes pour gérer les clients GIM du groupe correspondant, mais vous n'aurez pas de vision globale de l'ensemble des clients de votre environnement.

Rubrique parent : Concepts clés et outils

Reconnaissance

La reconnaissance fait référence aux processus visant à rechercher et identifier les objets de votre environnement devant faire l'objet d'un suivi pour des raisons de sécurité et de conformité.

La reconnaissance correspond au processus visant à rechercher des objets importants, tels que des utilisateurs privilégiés, des données sensibles et des sources de données. La classification correspond au processus visant à identifier de manière appropriée les éléments reconnus pour des raisons de sécurité et de conformité. Ces processus de reconnaissance et de classification sont essentiels dans vos organisations de grande taille où les fusions, les acquisitions et les systèmes existants introduisent de manière non structurée et imprévisible de nouveaux objets dans votre environnement. Guardium vous aide à incorporer ces objets dans votre environnement afin que vous puissiez imposer des politiques de sécurité efficaces et assurer la conformité.

Un scénario courant implique la reconnaissance des données sensibles. Les données sensibles font notamment référence à des informations réglementées, telles que des numéros de carte de crédit, des données financières personnelles, des numéros de sécurité sociale et d'autres informations nécessitant un traitement spécial. Guardium prend en charge deux approches différentes pour reconnaître des données sensibles, à savoir l'utilisation du générateur de flux de travaux de reconnaissance des données sensibles ou l'utilisation du générateur de politiques avec d'autres outils Guardium. Le générateur de flux de travaux de reconnaissance des données sensibles est conçu comme un outil global permettant d'établir des processus de reconnaissance et de classification pour des données sensibles. Utilisez-le afin de spécifier des règles pour la reconnaissance, définir les actions à exécuter sur les données reconnues, spécifier les sources de données à examiner, distribuer des rapports et exécuter le flux de travaux selon une planification automatisée. Pour les utilisateurs plus expérimentés, le générateur de politiques prend en charge des règles de reconnaissance et de classification dont le niveau de granularité est plus élevé et qui sont facilement incorporables dans des processus existants et dans des applications Guardium.

- Sources de données
  Les sources de données stockent des informations sur votre base de données ou référentiel, comme le type de base de données, l'emplacement du référentiel ou les données d'identification qui peuvent lui être associées. Vous devez définir une source de données pour l'utiliser avec des applications Guardium.
- Protection de service de base de données cloud
  La protection de base de données cloud fournit des processus de classification, d'évaluation de vulnérabilité et d'audit d'objet sur les bases de données cloud.
- Reconnaissance automatique de base de données
  L'application de reconnaissance automatique examine et analyse vos serveurs à la recherche de ports ouverts afin d'empêcher toute connexion inconnue ou indésirable avec votre réseau. Vous pouvez exécuter des processus de reconnaissance automatique à la demande ou planifier leur exécution sur une base périodique.
- Classification
  Les politiques et processus de classification définissent la manière dont Guardium reconnaît et traite des données sensibles, telles que des numéros de carte de crédit, des numéros de sécurité sociale et des données financières personnelles.
- Reconnaissance des données sensibles
  Créez un scénario de bout en bout pour reconnaître et classifier des données sensibles.
- Expressions régulières
  Des expressions régulières peuvent être utilisées pour rechercher sur le trafic des modèles complexes dans les données.
- Reconnaissance et classification de données sensibles dans des serveurs de fichiers
  La surveillance de l'activité des fichiers garantit l'intégrité et la protection des données sensibles sur les serveurs de fichiers UNIX et Windows.

- Optimisation des autorisations
  Le dispositif Optimisation des autorisations propose un arbitrage entre le rôle de l'administrateur de base de données visant à fournir aux utilisateurs les autorisations requises pour effectuer leur travail de manière efficace, et le rôle de sécurité visant à maintenir un niveau d'autorisation d'utilisation le plus précis et plus bas possible afin d'empêcher les vulnérabilités du système.

Sources de données

Les sources de données stockent des informations sur votre base de données ou référentiel, comme le type de base de données, l'emplacement du référentiel ou les données d'identification qui peuvent lui être associées. Vous devez définir une source de données pour l'utiliser avec des applications Guardium.

- Création d'une définition de source de données
  Utilisez le panneau Générateur de source de données pour créer des définitions de source de données à utiliser avec les applications Guardium.
- Gestion des sources de données existantes
  Après avoir créé une définition de source de données, vous pouvez la cloner, la modifier ou la supprimer.
- Génération de rapports sur les sources de données
  Guardium fournit des rapports sur les sources de données présentes dans votre environnement, ainsi que sur les modifications qui leur ont été apportées.
- Définition d'une source de données à l'aide d'un nom de service
  Vous pouvez définir une source de données qui permet à vos utilisateurs de se connecter à une base de données Oracle en utilisant le nom de service dans une URL personnalisée.
- Gestion des définitions de centre de distribution de clés
  Si votre source de données requiert l'authentification à l'aide de Kerberos, vous pouvez spécifier les informations nécessaires à Guardium pour obtenir un ticket Kerberos avant d'établir la connexion.

Rubrique parent : Reconnaissance

Création d'une définition de source de données

Utilisez le panneau Générateur de source de données pour créer des définitions de source de données à utiliser avec les applications Guardium.

Pourquoi et quand exécuter cette tâche

Vous pouvez créer une définition de source de données via deux processus généraux. Vous pouvez commencer par ajouter une définition de source de données à partir du panneau Générateur de source de données, puis spécifier l'application pour laquelle vous souhaitez utiliser la source de données. Ensuite, vous pouvez accéder à l'application que vous souhaitez utiliser, puis créer une source de données dans cette application. La navigation pour l'ajout d'une définition de source de données au sein d'une application varie en fonction de celle-ci ou du type de base de données sélectionné. Par exemple, si vous souhaitez créer une base de données d'audit, accédez à Renforcer > Configuration Change Control (CAS Application) > Création de base de données d'audit des changements de valeur et cliquez sur Ajouter une source de données .

Procédure

- Ouvrez le panneau Générateur de source de données en accédant à Configuration > Définitions de source de données.
- Cliquez sur  pour ajouter une définition de source de données.
- Utilisez la boîte de dialogue Créer une source de données pour fournir des informations sur la source de données que vous souhaitez stocker pour une utilisation ultérieure. La boîte de dialogue varie en fonction de l'application et du type de base de données que vous sélectionnez, ainsi que du type de source de données que vous utilisez.
  1. Sélectionnez un élément dans le champ Type d'application.
  2. Entrez un nom unique dans le champ Nom pour la source de données.
  3. Dans le menu Type de base de données, sélectionnez la base de données ou le type de fichier. Pour certaines applications, la source de données doit être une base de données et ne peut pas être un fichier texte. En fonction du type de base de données que vous sélectionnez, certaines zones du panneau sont désactivées ou leur libellé change. Par exemple, le champ Affecter des données d'identification peut être facultatif ou obligatoire. Si ce champ est obligatoire, il est désactivé et les champs Nom d'utilisateur et Mot de passe sont obligatoires. Si le champ Affecter des données d'identification est facultatif, les champs Nom d'utilisateur et Mot de passe sont désactivés tant que vous ne le sélectionnez pas.
  4. Sélectionnez Partager la source de données pour partager la définition de source entre toutes les applications. Si vous ne partagez pas la source de données, la définition que vous créez ne peut être utilisée qu'avec l'application que vous avez choisie.
  5. Vous pouvez éventuellement configurer des données d'identification supplémentaires.
     - Utiliser SSL. Sélectionnez cette option pour utiliser SSL. Ensuite, sélectionnez éventuellement Importer le certificat SSL du serveur, puis cliquez sur Ajouter un certificat pour sélectionner le certificat.
     - Utiliser LDAP. Sélectionnez cette option pour utiliser LDAP. Ensuite, cliquez sur Affecter des données d'identification, puis renseignez les champs Nom d'utilisateur et Mot de passe.
     - Utiliser Kerberos. Sélectionnez cette option pour utiliser une configuration Kerberos prédéfinie. Sélectionnez Configuration Kerberos, puis renseignez les champs Domaine et KDC. La source de données compare ces informations avec son propre centre de distribution de clés et son propre domaine pour s'assurer qu'ils correspondent.
  6. Sélectionnez Sauvegarder le mot de passe pour sauvegarder et chiffrer vos données d'authentification sur le dispositif Guardium. Le champ Sauvegarder le mot de passe est obligatoire si vous définissez une source de données avec une application qui s'exécute en tant que tâche planifiée (et non pas à la demande). Lorsque le champ Sauvegarder le mot de passe est sélectionné, le nom de connexion et le mot de passe sont obligatoires.
  7. Entrez vos données d'identification dans les champs Nom de connexion et Mot de passe.
  8. Entrez le nom d'hôte ou l'adresse IP pour la source de données dans le champ Nom d'hôte/IP.
  9. Utilisez le tableau pour renseigner le champ Port en fonction du type de source de données.
     Tableau répertoriant les types de source de données et les numéros de port

Type de base de données	Numéro de port
Aster Data	2046
DB2	50000 Pour DB2 UDB, Guardium prend en charge count_big(*). Sur des tableaux de très grande taille, une valeur count(*) standard peut provoquer une erreur.
DB2 for i	446

Type de base de données	Numéro de port
DB2 for z/OS	446
GreenplumDB	5432
Hadoop	21000 - 21050
Informix	1526
MS SQL Server (ports dynamiques) et MS SQL Server (DataDirect - ports dynamiques)	Numéro de port grisé. L'utilisation de cette source de données permet à un client sans valeur de port définie ou sur lequel la fonction dynamique est activée à partir du serveur de base de données MS SQL Server de se connecter dynamiquement à une base de données MS SQL Server. Pour définir un port dynamique, accédez au serveur de base de données MS SQL Server et affectez la valeur 0 au type de port dynamique, puis retirez TCP/IP (port 1433 défini par défaut). L'affectation de la valeur 0 au port dynamique et le redémarrage des services permettent de configurer une adresse IP dynamique. Pour MS SQL, Guardium prend en charge count_big(*). Sur des tableaux de très grande taille, une valeur count(*) standard peut provoquer une erreur. Pilote DataDirect pour MS SQL Server Auparavant, le pilote jTDS devait être téléchargé pour permettre la prise en charge de l'authentification Windows à l'aide de NTLM et NTLMv. A présent, cette prise en charge est assurée par le pilote Guardium DataDirect. Paramètres Si l'utilisateur Guardium souhaite utiliser l'authentification Windows, ajoutez ce paramètre à la propriété de connexion : domain=domain_name;AuthenticationMethod=ntlmjava Si vous utilisez NTLMv2 pour l'authentification Windows, ajoutez ce paramètre à la propriété de connexion : domain=domain_name;AuthenticationMethod=ntlm2java AuthenticationMethod Objectif Détermine la méthode d'authentification utilisée par le pilote lors de l'établissement d'une connexion. Si la méthode d'authentification spécifiée n'est pas prise en charge par le serveur de base de données, la connexion échoue et le pilote émet une exception. Valeurs valides auto | kerberos | ntlm | ntlmjava | ntlm2java | userIdPassword Remarques Si vous spécifiez AuthenticationMethod=ntlmjava alors que le niveau LMCompatabilityLevel est limité à NTLMv2, une erreur est renvoyée. Si le niveau LMCompatabilityLevel est limité à NTLMv2, le paramètre AuthenticationMethod doit avoir pour valeur ntlm2java. Si vous spécifiez AuthenticationMethod=ntlmjava ou AuthenticationMethod=ntlm2java, vous devez indiquer le nom du serveur de domaine qui administre la base de données. Vous pouvez indiquer le serveur de domaine à l'aide de la propriété de domaine. Si la propriété de domaine n'est pas spécifiée, le pilote tente de déterminer le serveur de domaine à partir de la propriété d'utilisateur. Si le pilote ne peut pas déterminer le nom du serveur de domaine, il émet une exception. La propriété d'utilisateur fournit l'ID utilisateur. La propriété de mot de passe indique le mot de passe. Les valeurs type4, type2 et none sont dépréciées, mais reconnues pour la compatibilité avec les versions antérieures. Utilisez à la place les valeurs kerberos, ntlm et userIdPassword, respectivement. L'authentification NTLM requiert Microsoft SQL Server 2000, Service Pack 3 ou ultérieur. Si l'utilisateur Guardium utilise un jeu de caractères unicode de base de données non standard, tel que Azeri_Cyrillic_100_CI_AS ou Chinese_Hong_Kong_Stroke_90_CI_AS, ajoutez le paramètre suivant à la propriété de connexion : CodePageOverride=UTF-8 Si vous utilisez SSL (Forcer le chiffrement=Oui), ajoutez : encryptionMethod=SSL;validateServerCertificate=false
MS SQL Server (DataDirect)	1433
MongoDB	27017
MySQL	3306

Type de base de données	Numéro de port
Netezza	5480
Oracle (DataDirect)	1521
PostgreSQL	5432
Sybase	4100
Sybase IQ	2638
Teradata	1025
Text	0
Text:HTTP	8000
Text:FTP	21
Text:SAMBA	445
Text:HTTPS	8443
N_A	0
MS SQL Server (open source) (Utiliser Renforcer > Vulnerability Assessment > Téléchargements client pour télécharger ces pilotes JDBC. Voir Téléchargement de groupes abonnés.)	1433
Oracle (open source) (Utiliser Renforcer > Vulnerability Assessment > Téléchargements client pour télécharger ces pilotes JDBC. Voir Téléchargement de groupes abonnés.)	1521
HIVE, HiveServer2	10000
HADOOP, interface CLI Hive dépréciée	9083
HIVE, pour Impala à partir de Hue	21050
HADOOP, Impala shell	21000
HUE, back end Oracle Hue	1521
HUE, back end MySQL Hue	3306
HUE, backend PostgreSQL Hue	5432
WEBHDFS	50070

Remarque : Lorsque vous tentez de vous connecter à l'aide d'une source de données SSL pour la première fois, l'erreur suivante peut s'afficher lors du test de la connexion :

```
error
Connection unsuccessful
Could not connect to: 'jdbc:db2://su11u1x64t-va:55000/VA_DB' for user: '(DELETE ME) db2 10.1 SSL_DB2(Security
Assessment)'. DataSourceConnectException: Could not connect to: 'DB2 (DELETE ME) db2 10.1 SSL 9.70.146.39:55000' for
user: 'db2inst1'. Exception: com.ibm.db2.jcc.am.DisconnectNonTransientConnectionException: [jcc][t4][2030][11211]
[4.15.134] A communication error occurred during operations on the connection's underlying socket, socket input stream,
```

Cela est dû au fait que l'interface graphique ne comporte pas le fichier de clés approprié pour le certificat chargé en mémoire. Pour remédier à cela, redémarrez l'interface graphique. Cette erreur disparaîtra et la connexion aboutira.

10. Selon le type de source de données, la boîte de dialogue diffère légèrement pour les zones situées après le port.
    - Pour DB2, entrez le nom de base de données.
    - Pour DB2 iSeries ou Oracle, entrez le nom de service.
    - Pour Informix, entrez le nom de serveur Informix.
    - Pour un type de base de données autre que Texte, dans la zone Base de données, entrez le nom de base de données (Informix, Sybase, MS SQL Server, PostgreSQL ou Teradata uniquement). Si la zone est vide pour Sybase ou MS SQL, master est la valeur par défaut. Pour une base de données Sybase, la zone de texte Base de données doit contenir le nom de base de données ou prendre la valeur par défaut master si elle est vide (cela fonctionne pour Entitlement Reports and Classifier), pour VA, utilisez le nom d'instance de base de données).
    - Pour DB2, DB2 iSeries ou Oracle, entrez un nom de schéma valide dans la zone Schéma à utiliser.
    - Pour un type de base de données Fichier texte, dans la zone Nom de fichier, entrez le nom du fichier.
11. Utilisez la zone Propriété de connexion uniquement si des propriétés de connexion supplémentaires doivent être incluses sur l'URL JBDC pour établir une connexion JDBC avec cette source de données. Le format obligatoire est propriété=valeur, où chaque paire propriété-valeur est séparée de la suivante par une virgule.
    - Pour une base de données Sybase avec un jeu de caractères par défaut Roman8, entrez la propriété suivante : charSet=utf8.
    - Pour une connexion chiffrée Oracle, vous devez définir une propriété de connexion comme suit : oracle.net.encryption_client=REQUIRED;oracle.net.encryption_types_client=RC4_40 (Remplacement par un algorithme de chiffrement requis par l'instance surveillée, quel que soit son type.)
    - Notez que le chiffrement 3DES168 pose problème. Une source de données définie pour utiliser le chiffrement 3DES168 émet incorrectement une erreur de protocole ORA-17401 ou une erreur de total de contrôle ORA-17002 lorsqu'elle trouve une erreur SQL. Par conséquent, la connexion ne fonctionnera tout simplement pas tant qu'elle ne sera pas fermée, puis rouverte.
    - Pour une connexion chiffrée DB2, vous devez définir une propriété de connexion comme suit : securityMechanism=13
    - Pour une connexion chiffrée DB2 iSeries, définissez une propriété de connexion comme suit : property1=com.ibm.as400.access.AS400JDBCDriver;translate binary=true
    - Pour une source de données DB2 z/OS, ajoutez une propriété de connexion afin d'améliorer les performances de la base de données : resultSetHoldability=2
    - Dans l'environnement Oracle, sys est un utilisateur Oracle par défaut, propriétaire de l'instance de base de données, et dispose des droits de superutilisateur qui s'apparentent aux droits root en environnement Unix. SYSDBA est un rôle qui dispose des privilèges d'administration requis pour

effectuer de nombreuses opérations administratives de haut niveau, comme le démarrage et l'arrêt de la base de données, mais aussi l'exécution d'opérations, telles que la sauvegarde et la récupération. Ce rôle (SYSDBA) peut aussi être accordé à d'autres utilisateurs. La phrase `sys as SYSDBA` fait référence à la méthode de connexion requise pour se connecter en tant qu'utilisateur sys.

- Pour les valeurs de moniteur pour Oracle 10 (sys as SYSDBA) (s'applique au pilote open source d'Oracle), entrez : internal_logon=sysdba
- Pour DataDirect (pilote Oracle), entrez : SysLoginRole=sysdba
- De plus, si vous utilisez CRYPTO_CHECKSUM_TYPES dans votre sqlnet.ora, utilisez les exemples suivants :
- oracle.net.encryption_client=aes256;oracle.net.crypto_checksum_types_client=SHA1
- oracle.net.encryption_client=rc4_256;oracle.net.crypto_checksum_types_client=MD5
- oracle.net.encryption_client=aes256;oracle.net.crypto_checksum_types_client=MD5
- oracle.net.encryption_client=rc4_256;oracle.net.crypto_checksum_types_client=SHA1
- Exemple : Utilisez les données d'authentification pour Oracle LDAP, appelées ID objet. Les valeurs requises sont les suivantes : l'hôte ou l'adresse IP de serveur LDAP, le port de serveur LDAP, le nom d'instance et le domaine Oracle. L'URL personnalisée doit être correctement saisie : jdbc:guardium:oracle:@ldap://wi3ku2x32t4:389/on0maver,cn=OracleContext,dc=vguardium,dc=com

12. Si nécessaire, entrez une chaîne de connexion à la source de données dans le champ URL personnalisée. Si le champ URL personnalisée est vide, la connexion est établie avec les propriétés entrées dans les autres champs de définition de source de données (par exemple hôte, port, instance, etc.).
    Important :
    - Si vous renseignez un champ URL personnalisée au format open source d'Oracle, spécifiez `jdbc:guardium:oracle://;SID=<SID>`.
    - Si vous créez une source de données pour une base de données Oracle alors que la sécurité avancée d'Oracle est activée, spécifiez `EncryptionLevel=required` dans le champ URL personnalisée de la définition de source de données.
    -
13. Cliquez sur Afficher les options avancées pour afficher les rôles et les options de CAS (système d'audit de configuration).
14. Cliquez éventuellement sur Rôles afin d'affecter des rôles pour la source de données. L'ajout d'un rôle à une source de données permet aux utilisateurs d'afficher la configuration de source de données. Seuls les propriétaires et les administrateurs sont autorisés à modifier et supprimer la source de données.
15. Entrez éventuellement des informations de CAS

    a. Les fournisseurs offrent de la souplesse lors de l'installation, par conséquent, les utilisateurs doivent être sollicités pour déterminer les deux zones obligatoires sur la définition de source de données.

    CAS a besoin de deux éléments d'informations : un compte d'instance de base de données pour exécuter certains des outils de base de données sous Unix, et le nom du répertoire d'instance de base de données afin de trouver les fichiers qui doivent être surveillés. En général, si le compte d'instance de base de données et le répertoire ne sont pas correctement saisis dans la définition de source de données, des messages `Aucune donnée CAS` s'affichent pour les tests pour indiquer que CAS n'a pas pu trouver de données.

    Renseignez les champs Compte d'instance de base de données (propriétaire de logiciel) et Répertoire d'instance de base de données (répertoire dans lequel le logiciel de base de données a été installé) qui seront utilisés par CAS.

    Voici des suggestions relatives à la recherche des renseignements nécessaires pour saisir les informations CAS pour les sources de données. Ces informations peuvent varier d'une installation à l'autre. L'une des méthodes utilisées sous Unix consiste à afficher le fichier /etc/passwd pour des installations de base de données spécifiques qui peuvent être utilisées afin d'identifier le compte d'instance de base de données et le répertoire d'instance. Parfois, lors de l'installation, une variable d'environnement est définie dans le compte d'instance de base de données pour identifier le répertoire d'instance, par exemple ORACLE_HOME. En l'occurrence, entrez $ORACLE_HOME dans le champ Répertoire d'instance de base de données du formulaire de définition de source de données. La variable sera développée et vous pourrez y trouver le nom de répertoire approprié sur le serveur de base de données.
    Remarque : Pour lancer une recherche dans plusieurs répertoires, vous pouvez définir plusieurs chemins de fichier pour Répertoire d'instance de base de données. Pour consulter un exemple, voir la ligne MongoDB.

Tableau 1. Instances de base de données

Type de base de données	Compte d'instance de base de données	Répertoire d'instance de base de données/Suggestions supplémentaires
Db2	Souvent db2inst1	Répertoire de base de db2inst1 ou C:\Program Files\IBM\SQLLIB sous Windows Le programme db2cmd.exe doit figurer dans le chemin de système ou dans le sous-répertoire bin du répertoire d'instance de base de données.
Informix	Souvent informix	Quelque chose comme /opt/IBM/informix sous Unix, ou C:\Program Files\IBM\Informix. Une variable d'environnement INFORMIXDIR peut être définie. Le programme <servicename>.cmd doit figurer dans le chemin de système où <servicename> est la valeur de serveur Informix saisie dans la définition de source de données.

Type de base de données	Compte d'instance de base de données	Répertoire d'instance de base de données/Suggestions supplémentaires
MongoDB	Souvent mongodb ou mongos	Avec MongoDB, vous devez spécifier plusieurs chemins pour le répertoire d'instance de base de données. Indiquez un chemin séparé à l'aide d'une barre verticale "|" et des espaces. Par exemple, /var/lib/mongo | MongoBinary=/usr/bin | dbpath=/var/lib/mongo | logpath=/var/log/mongodb | keytab=/home/keytab | dbdumppath=/opt/backup | sslpath=/etc/ssl | keyfile=/home/mongod/mongo_server.keyfile. Le chemin /var/lib/mongo est requis, car il s'agit du chemin de base pour l'utilisateur mongo. MongoBinary=/usr/bin est le chemin d'accès à la bibliothèque mongo. Vous devez spécifier la variable (sensible à la casse), puis le chemin. dbpath=/var/lib/mongo est le chemin d'accès aux fichiers de données. En l'occurrence, il se trouve qu'il est identique au répertoire de base MongoDB. logpath=/var/log/mongodb est le chemin d'accès au journal MongoDB. keytab=/home/keytab est le chemin d'accès au fichier de clés MongoDB. dbdumppath=/opt/backup est le chemin d'accès au cliché de sauvegarde MongoDB. sslpath=/etc/ssl est le chemin d'accès aux fichiers SSL MongoDB. keyfile=/home/mongod/mongo_server.keyfile pointe vers le fichier de clés MongoDB. Vous n'avez pas besoin de définir tous les chemins répertoriés. Les chemins non définis ne seront pas analysés.
Oracle	Souvent Oracle ou une version spécifique, telle que oracle9 ou oracle10	Par exemple, /home/oracle9 sous Unix ou C:\oracle\product\10.2.0\db_1 sous Windows. Une variable d'environnement ORACLE_HOME peut être définie. Sous Windows, les variables d'environnement PERL5LIB et ORACLE_HOME doivent être définies, et le programme opatch.bat doit figurer sur le chemin système.
SQL Server	Non nécessaire sauf si l'authentification Windows est utilisée. Dans ce cas, il doit être au format acceptable pour l'authentification Windows, DOMAIN/Username.	Il existe deux scénarios possibles lors du remplissage du nom du répertoire d'instance de base de données pour l'utilisation de CAS dans SQL Server. Si la source de données est utilisée pour des tests d'évaluation de vulnérabilité, le répertoire de base d'instance de base de données doit figurer dans cette colonne. Exemples MSSQL2000, instance Nom sur un serveur 64 bits. C:\Program Files (x86)\Microsoft SQL Server\MSSQL$MSSQL2000 MSSQL2000, instance par défaut sur un serveur 32 bits. C:\Program Files\Microsoft SQL Server\MSSQL MSSQL2005 C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL MSSQL2008 C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL Si la source de données n'est pas utilisée pour des tests d'évaluation de non vulnérabilité, mais pour des fichiers ou registre de surveillance CAS, cette colonne contiendra le répertoire Microsoft SQL Server avec des fichiers programme. Exemples : C:\Program Files (x86)\Microsoft SQL Server ou C:\Program Files\Microsoft SQL Server Remarque : vous devez disposer de deux sources de données si vous souhaitez effectuer des tests d'évaluation de vulnérabilité et de la surveillance de fichier CAS.
Sybase	Souvent "sybase"	Pour Unix, /home/sybase ou C:\sybase pour Windows. Une variable d'environnement SYBASE peut être définie.

Type de base de données	Compte d'instance de base de données	Répertoire d'instance de base de données/Suggestions supplémentaires
MySQL		Une variable d'environnement MYSQL_HOME peut être définie. Remarque : Une source de données MySQL avec un nom de base de données Unicode n'est pas prise en charge. Le nom de source de données dans MYSQL doit être composé de caractères ASCII.
Teradata		Non nécessaire. Toutes les installations se ressemblent.
Netezza		Non nécessaire. L'installation se trouve au même emplacement sur toutes les machines.
PostgreSQL		Il s'agit de l'installation la plus flexible. L'utilisateur doit définir deux variables d'environnement sur le serveur de base de données Postgres : PostgreSQL_BIN doit être l'emplacement des binaires pour l'installation et PostgreSQL_DATA doit être l'emplacement des données.

Remarque : Si une variable d'environnement doit être utilisée dans le champ Répertoire d'instance de base de données, elle doit être définie sur le serveur de base de données.

b. Sélectionnez un élément dans la zone Classification des niveaux de gravité (niveau d'impact) pour la source de données. Vous pouvez utiliser une classification de gravité pour trier, filtrer ou mettre en évidence des sources de données lors de l'affichage de rapports et de résultats.
c. Cliquez sur Sauvegarder pour sauvegarder la définition de source de données (vous ne pouvez pas ajouter de rôles ou de commentaires tant que la définition n'a pas été sauvegardée).
d. Cliquez éventuellement sur Ajouter des commentaires pour ajouter des commentaires à la définition.
e. Cliquez éventuellement sur Tester la connexion pour tester la connectivité de la source de données définie.
f. Cliquez sur Fermer lorsque vous en avez terminé avec la définition.

Rubrique parent : Sources de données

Gestion des sources de données existantes

Après avoir créé une définition de source de données, vous pouvez la cloner, la modifier ou la supprimer.

Procédure

- Ouvrez Générateur de source de données en accédant à Configuration > Définitions de source de données.
- Le menu Sélection d'application répertorie toutes les applications avec lesquelles vous pouvez utiliser une définition de source de données. Choisissez l'application pour laquelle la source de données que vous souhaitez modifier a été créée, puis cliquez sur Suivant, ce qui vous conduit au panneau Localiseur de source de données.

Rubrique parent : Sources de données

Clonage d'une source de données

Procédure

- Sélectionnez la source de données que vous souhaitez cloner à partir de la sous-fenêtre Localiseur de source de données, puis cliquez sur Cloner.
- Les informations que vous avez saisies lors de la création de la définition de source de données apparaissent dans la boîte de dialogue Définition de source de données, avec le préfixe "Copie de" devant le nom initial de la source de données. Modifiez les zones de votre choix.
- Cliquez sur Appliquer pour sauvegarder la source de données clonée.

Modification d'une source de données

Procédure

- Sélectionnez la source de données que vous souhaitez modifier à partir de la sous-fenêtre Localiseur de source de données, puis cliquez sur Modifier.
- Les informations que vous avez saisies lors de la création de la définition de source de données apparaissent dans la boîte de dialogue Définition de source de données. Modifiez les zones de votre choix.
- Cliquez sur Appliquer pour sauvegarder les modifications que vous avez apportées à la source de données.

Retrait d'une source de données

Procédure

Sélectionnez la source de données que vous souhaitez modifier à partir de la sous-fenêtre Localiseur de source de données, puis cliquez sur Supprimer.

Génération de rapports sur les sources de données

Guardium fournit des rapports sur les sources de données présentes dans votre environnement, ainsi que sur les modifications qui leur ont été apportées.

Procédure

- Ouvrez le rapport Sources de données en accédant à Rapports > Outils de configuration de rapport > Sources de données. Le tableau qui s'affiche répertorie toutes les sources de données, ainsi que les informations qui sont stockées dans chaque définition de source de données.
- Cliquez avec le bouton droit de la souris dans n'importe quelle cellule du tableau. Deux options apparaissent : Historique des versions de la source de données et Appeler.
  - Cliquez sur Historique des versions de la source de données pour visualiser les modifications apportées à la définition de source de données.
  - Cliquez sur Appeler pour sélectionner et exécuter l'une des API disponibles pour la source de données.

Remarque : Vous pouvez personnaliser les paramètres d'exécution et de présentation du rapport Sources de données en cliquant sur l'icône représentant un crayon.

Rubrique parent : Sources de données
Concepts associés:
GuardAPI Datasource Functions

Définition d'une source de données à l'aide d'un nom de service

Vous pouvez définir une source de données qui permet à vos utilisateurs de se connecter à une base de données Oracle en utilisant le nom de service dans une URL personnalisée.

Pourquoi et quand exécuter cette tâche

Vous devez entrer le nom d'hôte, le port et le nom de service, ainsi que l'URL personnalisée.

Procédure

1. Déterminez le nom de service Oracle. Vous pouvez utiliser des commandes, telles que celles décrites ci-dessous :

   ```
   SQL> set line size 5000;
   SQL> select host_name, instance_name from v$instance;
   SQL> select name from v$database;
   SQL> show parameter service
   ```

   Utilisez le nom qui apparaît dans la colonne VALUE.
2. Chargez le pilote fin JDBC Oracle approprié sur le système Guardium.
   a. Trouvez et téléchargez le pilote pour votre base de données Oracle à l'adresse suivante : http://www.oracle.com/technetwork/database/enterprise-edition/jdbc-112010-090769.html
   b. Ouvrez la fenêtre Téléchargements client en accédant à Renforcer > Vulnerability Assessment > Téléchargements client.
   c. Localisez la section intitulée Télécharger le pilote JDBC Oracle. Cliquez sur Parcourir et accédez à l'emplacement où vous souhaitez télécharger le fichier. Cliquez sur Utiliser un pilote open source pour tout.
   d. Redémarrez l'interface utilisateur Guardium une fois le téléchargement terminé.
3. Définissez la source de données de cette base de données.
   a. Ouvrez Générateur de source de données en accédant à Configuration > Définitions de source de données.
   b. Le menu Sélection d'application répertorie toutes les applications avec lesquelles vous pouvez utiliser une définition de source de données. Choisissez l'application pour laquelle la source de données que vous souhaitez modifier a été créée, puis cliquez sur Suivant, ce qui vous conduit au panneau Localiseur de source de données.
   c. Entrez le nom de service dans le champ Nom de service. Dans le champ URL personnalisée, entrez `jdbc:oracle:thin@//hostname:port/svcname`, où hostname et port sont les valeurs standard pour la base de données et svcname est le nom de service, la même valeur que celle que vous avez indiquée dans le champ Nom de service.

Rubrique parent : Sources de données

Gestion des définitions de centre de distribution de clés

Si votre source de données requiert l'authentification à l'aide de Kerberos, vous pouvez spécifier les informations nécessaires à Guardium pour obtenir un ticket Kerberos avant d'établir la connexion.

Pourquoi et quand exécuter cette tâche

A compter de Guardium V. 10.1.3, vous pouvez affecter un centre de distribution de clés à une source de données spécifique ou à un groupe d'unités géré, afin de fournir l'authentification Guardium pour les bases de données Mongo et Hive. Le dispositif obtient un ticket via la connexion JDBC, par conséquent, les utilisateurs n'ont pas besoin d'obtenir eux-mêmes des tickets. Notez que cela n'a rien à voir avec ce que la configuration du dispositif proprement lui permet d'utiliser.

Vous pouvez définir jusqu'à 5 centres de distribution de clés Kerberos sur un gestionnaire central et un centre de distribution de clés kerberos sur un système Guardium autonome. Pour ajouter un centre de distribution de clés à Guardium, vous spécifiez :

- realm: nom de domaine en lettres majuscules
- KDC: nom d'hôte du serveur Kerberos
- Type de chiffrement pour les tickets Kerberos
  - des-cbc-md5
  - des-cbc-crc
  - rc4-hmac
  - des3-cbc-sha1
  - aes128-cts-hmac-sha1-96
  - aes256-cts-hmac-sha1-96

  La valeur par défaut est aes256-cts-hmac-sha1-96, ce qui représente le type de chiffrement le plus sécurisé.

Procédure

1. Cliquez sur Configuration > Outils et vues > Configuration Kerberos
2. Cliquez sur l' pour créer une nouvelle configuration.
3. Renseignez les champs Nom, KDC et Domaine.
4. Renseignez le champ Type de chiffrement. La valeur par défaut est aes256-cts-hmac-sha1-96.
5. Cliquez sur Sauvegarder.

Que faire ensuite

Après avoir créé un centre de distribution de clés Kerberos, vous pouvez le sélectionner lorsque vous configurez votre source de données.

Rubrique parent : Sources de données

Protection de service de base de données cloud

La protection de base de données cloud fournit des processus de classification, d'évaluation de vulnérabilité et d'audit d'objet sur les bases de données cloud.

Dès lors que vous avez configuré la connexion entre Guardium et le cloud, vous pouvez effectuer les opérations suivantes :

- Reconnaître les instances de base de données et les cataloguer dans Guardium.
- Affecter des sources de données cataloguées à un processus de classification ou créer un processus. Le processus de classification s'exécute sur les bases de données cloud et identifie des objets en fonction des règles définies.
- Affecter des sources de données cataloguées à un processus d'évaluation de vulnérabilité ou créer un processus (une licence d'évaluation de vulnérabilité valide est requise). Le processus d'évaluation de vulnérabilité s'exécute sur les bases de données cloud et utilise les données des rapports Guardium.
- Activer l'audit de base de données. Des données d'audit standard d'Oracle sont extraites du cloud pour des rapportsGuardium, en fonction des politiques installées. (Voir Définitions Oracle dans https://docs.oracle.com/cd/B28359_01/server.111/b28337/tdpsg_auditing.htm#TDPSG50051.)
- Activer l'audit d'objet (trace d'audit d'Oracle). Passez en revue les résultats de la classification et sélectionnez des objets pour audit. (La fonction d'audit de base de données doit être activée.) L'audit d'objet effectue le suivi de toutes les activités effectuées sur les objets. Guardium utilise ces données pour des rapports, le tableau de bord d'investigation, etc. Vous pouvez configurer Guardium pour que les objets soient automatiquement ajoutés, source de données par source de données. Vous pouvez également définir une valeur par défaut pour chaque compte, dont toutes les sources de données héritent. Cette option est particulièrement utile pour les bases de données pour lesquelles un audit d'objet doit être effectué sans aucune autre évaluation. Définissez une limite raisonnablement élevée pour les résultats que le processus de classification devra trouver. Vous souhaiterez également empêcher qu'un dépassement d'objets ne se produise si votre classification contient une erreur. Par conséquent, ne définissez pas une limite trop élevée. (Un dépassement pourrait affecter les performances de base de données.)

Des autorisations AWS sont requises pour l'exécution de fonctions Guardium dans la base de données cloud. Voir Définition AWS IAM.

Dans les bases de données sur site, l'agent S-TAP installé dans la base de données envoie tout le trafic de base de données au système Guardium. Dans l'environnement cloud, Guardium extrait des fichiers journaux de la base de données cloud et traite les données semblables aux données S-TAP. La différence réside dans le fait que l'agent S-TAP enregistre toutes les activités de base de données, tandis que dans l'environnement cloud, seules les tables que vous sélectionnez font l'objet d'un audit. De plus, il peut y avoir un léger décalage lors de l'extraction de données depuis le cloud.

L'activité sur les bases de données et les objets soumis à un audit est enregistrée dans les journaux de base de données. Le volume d'activité enregistré augmente avec le nombre d'éléments surveillés. Une volume d'activité enregistré élevé peut avoir un impact sur les performances de base de données. Vous devez prendre soin de capturer toutes les données pertinentes mais sans surcharger le système.

Vous pouvez exécuter la protection de service de base de données cloud dans un environnement CM et sur un collecteur Guardium autonome.

Dans le contexte de la protection de service de base de données cloud, le terme "base de données" fait référence à la base de données présente sur le cloud et le terme "source de données" fait référence à la base de données cataloguée dans Guardium.

Un seul système Guardium peut être propriétaire de l'audit de base de données et de l'audit d'objet d'une base de données. Les autres systèmes Guardium peuvent accéder au même compte cloud et voir les détails de base de données, mais ils ne peuvent pas désactiver l'audit de base de données ni accéder aux données de l'audit d'objet. Vous pouvez transmettre la propriété d'un système Guardium à un autre, par exemple si un système s'arrête sans possibilité de reprise.

La reconnaissance, la classification et l'évaluation des vulnérabilités (VA) sont prises en charge pour tous les moteurs de base de données AWS RDS.

Limitations relatives à l'audit de base de données

- Vous devez conserver une définition RDS à jour, qui reflète par exemple les suppressions d'instance de base de données ou la modification des données d'identification.
- Guardium v10.1.4 prend en charge uniquement les bases de données Oracle V.11 sur un cloud AWS.
- Les règles d'extrusion ne sont pas prises en charge, y compris l'expurgation et le test de modèles dans les données renvoyées.
- Les données renvoyées ne sont pas prises en charge, y compris les enregistrements affectés et la journalisation des valeurs de variable de liaison.
- Les actions de règle qui interagissent avec S-TAP ne sont pas prises en charge. Exemple : Arrêt par S-GATE, Ignorer, et la réécriture de requête.
- Les échecs de connexion ne sont pas capturés par l'audit natif d'Oracle ; par conséquent, ils ne sont pas transmis à Guardium.
- Les instructions ne sont pas capturées par l'audit natif d'Oracle ; par exemple, les instructions avec des erreurs de syntaxe ne peuvent pas être surveillées.

- Flux de travaux de protection de service de base de données cloud
- Définition AWS IAM
  Cette rubrique explique comment définir votre politique IAM, selon les autorisations requises.
- Création, modification et suppression de comptes cloud
  Créez un compte de service de base de données cloud avec vos données d'identification de base de données, ou modifiez ou supprimez le compte cloud.
- Reconnaissance de bases de données cloud
  Cette rubrique explique comment reconnaître des bases de données dans le compte cloud en sélectionnant les régions sur lesquelles la recherche doit porter.
- Catalogage et gestion de bases de données
  Cette rubrique explique comment cataloguer des bases de données afin de créer les sources de données dans Guardium, modifier des utilisateurs et des mots de passe et mettre à jour la configuration de base de données.
- Gestion de la classification et de l'évaluation des vulnérabilités
  Cette rubrique explique comment affecter des sources de données à un processus de classification ou d'évaluation des vulnérabilité existant ou comment créer de nouveaux processus.
- Configuration de l'audit de base de données
  Cette rubrique explique comment activer l'audit sur la base de données de sorte que les données d'audit d'objet puissent être extraites par Guardium. Modifiez le nombre limite d'objets ajoutés automatiquement au processus de classification, ainsi que le collecteur.
- Gestion de l'audit d'objet
  Cette rubrique vous explique comment afficher les objets sensibles potentiellement identifiés par les processus de classification dans les bases de données que vous gérez et activer l'audit d'objet sur certains objets sélectionnés afin de surveiller toutes les activités effectuées sur ces objets.

Rubrique parent : Reconnaissance

Flux de travaux de protection de service de base de données cloud

Pourquoi et quand exécuter cette tâche

Il s'agit d'un flux de travaux général. Votre flux de travaux dépend de ce que vous souhaitez effectuer avec l'audit de base de données cloud.

Procédure

1. Créez un compte cloud.
2. Lancez la reconnaissance de ses instances de base de données.
3. Cataloguez les bases de données dont vous souhaitez gérer. Le catalogage crée une source de données dans Guardium, de sorte que vous pouvez gérer les fonctions Guardium de base de données cloud sur la base de données spécifique.
4. Ajoutez éventuellement la source de données à un processus d'évaluation de vulnérabilité nouveau ou existant (une licence d'évaluation de vulnérabilité valide est requise).
5. Ajoutez éventuellement la source de données à un processus de classification nouveau ou existant.
6. Activez éventuellement l'audit de base de données sur les bases de données pertinentes et redémarrez les bases de données soit immédiatement à partir de l'interface utilisateur Guardium soit ultérieurement à partir de la console de base de données. Une fois activé, l'audit de base de données effectue un audit Oracle standard. Lorsque vous activez l'audit de base de données, votre système Guardium devient l'unique propriétaire de l'audit de base de données sur cette base de données. Aucun autre système Guardium ne peut modifier l'audit de base de données ou l'audit d'objet. Pour voir les résultats de la classification, exécutez une fois le processus de classification (Exécuter une fois maintenant) après avoir activé la base de données d'audit, ou attendez la prochaine exécution planifiée. (La source de données doit être affectée à un processus de classification.)
7. Passez en revue les résultats de la classification pour vos sources de données (un processus de classification et un audit de base de données sont requis) :
   - Affichez les objets, regroupés par le processus d'objet ou de classification qui les ont identifiés, en utilisant des filtres pour affiner davantage les résultats.
   - Activez ou désactivez l'audit d'objet individuellement ou par table.
   - Effectuez une exploration en aval à partir du regroupement d'objets pour ouvrir une liste de toutes les bases de données qui contiennent l'objet sélectionné dans leurs résultats de classification. Vous pouvez également activer et désactiver l'audit d'objet à partir de cette vue.
8. Répétez régulièrement les étapes 2 à 7.
9. Passez en revue les sources de données régulièrement : recherchez les éventuels nouveaux objets et si vous le souhaitez, ajoutez ou retirez des objets de l'audit d'objet. Par exemple, vous pouvez retirer des objets si les objets ajoutés automatiquement incluent des objets qui ne nécessitent pas d'audit, ou si une base de données rencontre des problèmes de performance. Ou bien, vous pouvez identifier un objet suspect qui n'est pas audité et l'ajouter à l'audit d'objet.

Rubrique parent : Protection de service de base de données cloud

Définition AWS IAM

Cette rubrique explique comment définir votre politique IAM, selon les autorisations requises.

Les autorisations IAM minimales requises incluent l'affichage de la configuration et la modification des balises. Elles n'incluent pas l'activation de l'audit de base de données ni le redémarrage d'une base de données. Le code JSON ci-après définit les autorisations minimales sans lesquelles vous ne pouvez pas assurer la protection de service de base de données cloud.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "rds:DescribeDBParameters",
                "rds:DescribeDBInstances",
                "rds:DescribeDBParameterGroups",
                "rds:DownloadDBLogFilePortion",
                "rds:DescribeDBLogFiles",
                "rds:ListTagsForResource",
                "rds:RemoveTagsFromResource",
                "rds:AddTagsToResource",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcs"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Le droit complet est activé avec ces paramètres.

Activer et désactiver l'audit de base de données dans l'instance
: Si ce droit n'est pas configuré, les boutons Activer l'audit de base de données et Désactiver l'audit de base de données sont grisés et vous devez demander à l'administrateur de base de données d'activer ou de désactiver l'instance de base de données dans la console AWS.

```
"rds:CopyDBParameterGroup",
"rds:CreateDBParameterGroup",
"rds:ModifyDBInstance",
"rds:ModifyDBParameterGroup",
```

Redémarrer l'instance de base de données
: Si ce droit n'est pas configuré, les boutons Redémarrer sont grisés et vous devez demander à l'administrateur de base de données de redémarrer l'instance de base de données dans la console AWS.

```
"rds:RebootDBInstance",
```

Gérer le groupe de sécurité lorsque la plateforme prise en charge est EC2
: Lorsque ce droit n'est pas configuré, l'administrateur de base de données doit ajouter l'adresse IP de Guardium au groupe de sécurité. S'il est configuré, Guardium ajoute son adresse IP au groupe de sécurité de l'instance de base de données. Si le système Guardium ne parvient pas à identifier sa propre adresse IP en raison de la configuration de réseau, l'administrateur de base de données doit ajouter l'adresse IP dans la console AWS.

```
 "rds:ModifyDBInstance"
"rds:AuthorizeDBSecurityGroupIngress",
"rds:CreateDBSecurityGroup",
```

Gérer le groupe de sécurité lorsque la plateforme prise en charge est VPC

Lorsque ce droit n'est pas configuré, l'administrateur de base de données doit ajouter l'adresse IP de Guardium au groupe de sécurité. S'il est configuré, Guardium ajoute son adresse IP au groupe de sécurité de l'instance de base de données. Si le système Guardium ne parvient pas à identifier sa propre adresse IP en raison de la configuration de réseau, l'administrateur de base de données doit ajouter l'adresse IP dans la console AWS.

```
 "rds:ModifyDBInstance"
"ec2:AuthorizeSecurityGroupIngress",
"ec2:CreateSecurityGroup",
```

Lors de la configuration de ces paramètres, Guardium crée une règle entrante dans le groupe de sécurité de l'instance RDS, avec le masque CIDR d'IP publique de collecteur 24.

Rubrique parent : Protection de service de base de données cloud

Création, modification et suppression de comptes cloud

Créez un compte de service de base de données cloud avec vos données d'identification de base de données, ou modifiez ou supprimez le compte cloud.

Rubrique parent : Protection de service de base de données cloud

Création d'un compte cloud

Pourquoi et quand exécuter cette tâche

Prérequis : définissez la politique AWS IAM (voir Définition AWS IAM).

Conseil : Si vous gérez un grand nombre de bases de données dans ce compte, envisagez de définir un processus de classification par défaut. Cela vous évitera d'avoir à définir les propriétés de chaque base de données reconnue.

Procédure

1. Accédez à Reconnaître > Reconnaissance de base de données > Protection de service de base de données cloud.
2. Cliquez sur pour ouvrir la sous-fenêtre Création de définition de compte de service de base de données cloud.
3. Définissez le compte.
   - Nom de compte unique
   - Fournisseur
   - ID de clé d'accès unique et ID de clé d'accès secrète tels que fournis par votre fournisseur de service de cloud. La clé secrète de compte fonctionne comme un mot de passe. La clé d'accès et le titre doivent être uniques pour éviter que plusieurs noms de compte soient associés au même ID d'accès.
   - Limiter les objets ajoutés automatiquement (facultatif) : nombre maximal d'objets détectés par Classification, qui peuvent être activés automatiquement pour l'audit d'objet lorsque l'option Audit de base de données est activée. Vous pouvez modifier ce paramètre, par base de données, une fois que chaque base de données a été reconnue. Les objets activés automatiquement apparaissent à l'état Activé dans la fenêtre des objets gérés. Si vous souhaitez que des objets soient automatiquement ajoutés par Guardium, définissez une limite raisonnablement élevée pour les résultats que le processus de classification devra trouver. Vous souhaiterez également empêcher qu'un dépassement d'objets ne se produise si votre classification contient une erreur. Par conséquent, ne définissez pas une limite trop élevée. (Un dépassement pourrait affecter les performances de base de données.) La valeur zéro (0) signifie qu'aucun objet n'est automatiquement activé pour l'audit d'objet. Si le nombre d'objets audités plus le nombre d'objets nouvellement classifiés dépassent cette limite, aucun nouvel objet n'est activé pour l'audit d'objet. Par exemple, si la valeur 15 est définie et que 5 objets sont identifiés lors de la première exécution du processus de classification, une trace d'audit est affectée à ces 5 objets. Si la valeur 15 est définie et que 5 objets sont déjà activés pour l'audit d'objet, si 16 objets sont identifiés lors du processus de classification suivant, aucun nouvel objet n'est activé pour l'audit d'objet. Si la valeur 15 est définie et que 5 objets sont déjà activés pour l'audit d'objet, si 5 objets sont identifiés lors du processus de classification suivant, ces 5 nouveaux objets sont activés pour l'audit d'objet.
4. Définissez éventuellement la classification par défaut. Ce processus de classification est affecté à toutes les bases de données cataloguées sur ce compte. Vous pouvez modifier le processus de classification, par base de données, une fois que chacune des bases de données a été reconnue.
5. Testez l'accès au cloud.
   a. Cliquez sur Tester l'accès. Guardium tente d'accéder au cloud.
   b. Si Guardium ne parvient pas à accéder au cloud : assurez-vous que votre système Guardium a accès à Amazon et vérifiez les clés que vous avez indiquées.
6. Cliquez sur Créer.
   Le compte est créé et la liste Comptes de service de base de données cloud est mise à jour avec le nouveau compte cloud, dont les détails apparaissent dans la sous-fenêtre de droite.

Que faire ensuite

Découvrez les bases de données et cataloguez-les, configurez le processus de classification et d'évaluation des vulnérabilités, ainsi que l'audit d'objet.

Modification d'un compte cloud

Tous les paramètres peuvent être modifiés, à l'exception du fournisseur.

Procédure

1. Sélectionnez le compte cloud sous Comptes de service de base de données cloud, puis cliquez sur dans le volet droit.
2. Modifiez la configuration.
3. Si des données d'identification ont été modifiées, testez l'accès au cloud en cliquant sur Tester l'accès.
4. Cliquez sur Sauvegarder.

Suppression d'un compte cloud

La suppression d'un compte entraîne la désactivation de l'audit d'objet et de l'audit de base de données sur toutes les bases de données appartenant à l'environnement en cours.

Procédure

1. Sélectionnez le compte dans la sous-fenêtre Comptes de service de base de données cloud, cliquez sur  , puis confirmez.
2. Redémarrez la base de données à partir de la console de base de données. Si vous ne disposez pas d'un accès Amazon à la base de données, demandez à votre administrateur de base de données de désactiver l'audit de base de données et de redémarrer la base de données. Il est très important d'arrêter l'audit et de redémarrer la base de données de sorte que celle-ci cesse d'enregistrer des données dans les fichiers journaux utilisés par Guardium.

Reconnaissance de bases de données cloud

Cette rubrique explique comment reconnaître des bases de données dans le compte cloud en sélectionnant les régions sur lesquelles la recherche doit porter.

Pourquoi et quand exécuter cette tâche

La table Bases de données est remplie et mise à jour lorsque vous exécutez le processus de reconnaissance. Dès lors qu'une base de données est reconnue, elle est conservée dans la table, qu'elle soit toujours présente ou non dans le cloud.

Chaque fois que vous accédez à Reconnaissance > Reconnaissance de bases de données > Protection de service de base de données cloud, Guardium vous envoie un message si le statut d'audit de base de données dans le cloud est différent de celui indiqué dans l'interface utilisateur. Ce message qui apparaît au-dessus de la table Bases de données est le suivant : `Le statut d'audit de base de données a changé pour plusieurs bases de données. Cliquez sur Actualiser pour mettre à jour la table`. Lorsque ce message s'affiche, cliquez sur Actualiser pour actualiser l'affichage de la table.

Vous pouvez également effectuer cette vérification à la demande en cliquant sur Extraire le statut. L'extraction peut prendre quelques minutes. Une fois qu'elle est terminée, un message apparaît uniquement si l'un des statuts d'audit de base de données a changé. Si des changements sont survenus, cliquez sur Actualiser.

Vous pouvez également télécharger des définitions de base de données cloud via un fichier CSV. Les paramètres requis sont répertoriés sur la page GuardAPI Cloud Datasource Functions ; le paramètre d'API cloudTitle doit être remplacé par le paramètre environmentTitle (leur fonction est identique mais leurs noms sont différents). Suivez la procédure de téléchargement dans la section sur la création d'une source de données pour le fichier CSV téléchargé via le menu Télécharger un fichier CSV dans la rubrique Téléchargements client, en sélectionnant Renforcement > Evaluation des vulnérabilités > Téléchargements client pour télécharger votre fichier.

Procédure

1. Accédez à Reconnaissance > Reconnaissance de base de données > Protection de service de base de données cloud, puis cliquez sur le nom de compte de service. Lorsque vous créez un compte cloud, le table Afficher la reconnaissance des bases de données s'affiche avec une liste répertoriant toutes les régions et leurs noeuds finaux RDS.
2. Lorsque vous accédez à cette page par la suite, la table se referme. Cliquez sur Afficher la reconnaissance des bases de données. La table s'ouvre avec les régions.
3. Sélectionnez la ligne correspondant à chaque région dont vous souhaitez reconnaître les bases de données. Utilisez le filtre, le cas échéant.
4. Cliquez sur Reconnaître. Guardium lance des recherches dans les régions et ajoute à la table Bases de données les bases de données qui n'avaient pas encore été reconnues.

Rubrique parent : Protection de service de base de données cloud

Catalogage et gestion de bases de données

Cette rubrique explique comment cataloguer des bases de données afin de créer les sources de données dans Guardium, modifier des utilisateurs et des mots de passe et mettre à jour la configuration de base de données.

Pourquoi et quand exécuter cette tâche

Le catalogage entraîne la création dans Guardium des sources de données utilisées pour la classification, l'évaluation des vulnérabilités, l'audit et les rapports. Les bases de données qui ne sont pas cataloguées sont associées à une icône de couleur rouge dans la colonne Source de données Guardium de la table Base de données.

Procédure

1. Cataloguez les bases de données dont vous souhaitez effectuer un audit.
   a. Sélectionnez une ou plusieurs bases de données dans la table Bases de données.
   b. Cliquez sur Source de données > Cataloguer la source de données.
   c. Entrez le nom d'utilisateur et le mot de passe de base de données sensible à la casse qui vous a été fourni par votre administrateur de base de données. Si vous avez sélectionné plusieurs bases de données, assurez-vous qu'elles doivent toutes utiliser la même paire nom d'utilisateur/mot de passe.
   d. Le cas échéant, sélectionnez, modifiez ou effacez le processus de classification par défaut.
   e. Cliquez sur Cataloguer.

   Le nom de source de données Guardium apparaît dans la table Bases de données.
2. Mettez à jour le nom d'utilisateur ou le mot de passe.
   a. Sélectionnez une ou plusieurs sources de données dans la table Bases de données.
   b. Cliquez sur Source de données > Mettre à jour l'utilisateur et le mot de passe et modifiez les détails. Les deux champs doivent être renseignés.
   c. Cliquez sur Cataloguer.
3. Modifiez une définition de source de données.
   a. Sélectionnez la source de données et cliquez sur Source de données > Ouvrir une définition de source de données.
   b. Effectuez des modifications, le cas échéant. Voir les détails des paramètres dans Création d'une définition de source de données.
   c. Le cas échéant, testez la connectivité à la base de données en cliquant sur Tester la connexion.
   d. Cliquez sur Sauvegarder.

Rubrique parent : Protection de service de base de données cloud

Gestion de la classification et de l'évaluation des vulnérabilités

Cette rubrique explique comment affecter des sources de données à un processus de classification ou d'évaluation des vulnérabilité existant ou comment créer de nouveaux processus.

Pourquoi et quand exécuter cette tâche

Le menu Evaluation des vulnérabilités n'est disponible que si vous possédez une licence d'évaluation des vulnérabilités valide.

Une fois que vous avez affecté un processus de classification à une source de données, des données de classification sont collectées et traitées de la même manière que les données d'une base de données sur site. Vous pouvez affecter une classification lorsque vous n'êtes pas le propriétaire, mais vous devez devenir propriétaire pour pouvoir activer l'audit d'objet et afficher les résultats.

Une icône de couleur verte indique que le processus est en cours d'exécution. Une icône jaune indique qu'aucun planning n'est défini pour le processus. Une icône de couleur rouge dans la colonne Processus de classification ou Evaluation des vulnérabilités indique qu'aucune classification ou évaluation des vulnérabilités n'a été définie, ou une erreur. Consultez les erreurs d'évaluation des vulnérabilités dans Renforcement > Evaluation des vulnérabilités > Générateur d'évaluation > Afficher les résultats. Consultez les erreurs de classification dans Reconnaissance > Scénarios de bout en bout > Reconnaissance des données sensibles > ruban Réviser le rapport > Journal des processus.

Si vous recevez une erreur de classification `Fichier bdump-file-listing dans BDUMP introuvable. Impossible d'extraire les résultats pour :'RDSADMIN.TRACEFILE_`, ajoutez `RDSADMIN` au groupe de schémas prédéfini `Excluded Classification schemas - Oracle` dans le générateur de groupe.

Procédure

1. Affectez une ou plusieurs sources de données à un processus de classification existant.
   a. Sélectionnez une ou plusieurs sources de données.
   b. Cliquez sur Classification > Ajouter à la classification.
   c. Sélectionnez le processus de classification et cliquez sur Sauvegarder.
   d. Si vous le souhaitez, cliquez sur Editer/Afficher pour modifier ou exécuter le processus de classification.
   e. Si vous voulez que l'audit d'objet soit activé automatiquement pour les objets trouvés par le processus de classification, ouvrez ce dernier en cliquant sur **Editer/Afficher** et, dans le ruban Où rechercher, cochez la case Activer l'audit d'objet pour les bases de données sur le cloud.
   f. Vous pouvez aussi exécuter la classification : cliquez sur Exécuter maintenant dans le ruban Exécuter la reconnaissance accessible via Reconnaissance > Scénarios de bout en bout > Reconnaissance des données sensibles.
2. Créez un nouveau processus de classification et affectez-lui une ou plusieurs sources de données.
   a. Sélectionnez une ou plusieurs sources de données.
   b. Cliquez sur Classification > Créer une classification.
   c. Suivez la procédure décrite dans Reconnaissance des données sensibles. L'option Activer l'audit d'objet pour les bases de données sur le cloud est sélectionnée par défaut. Ne la désélectionnez pas.
   d. Exécutez la classification : après avoir indiqué où effectuer la recherche, cliquez sur Exécuter maintenant, ou après avoir sauvegardé le processus, cliquez sur Exécuter maintenant dans le ruban Exécuter la reconnaissance.
3. Affectez une ou plusieurs sources de données à une évaluation de vulnérabilité existante.
   a. Sélectionnez une ou plusieurs sources de données.
   b. Cliquez sur Evaluation des vulnérabilités > Ajouter à l'évaluation de vulnérabilité.
   c. Sélectionnez le processus Evaluation des vulnérabilités, puis cliquez sur Sauvegarder.
   d. Exécutez le processus : accédez à Renforcement > Evaluation des vulnérabilités > Générateur d'évaluation, sélectionnez le processus, puis cliquez sur Exécuter une fois maintenant.
4. Créez une nouvelle évaluation de vulnérabilité et affectez-lui une ou plusieurs sources de données.
   a. Sélectionnez une ou plusieurs sources de données.
   b. Cliquez sur Evaluation des vulnérabilités > Créer une évaluation des vulnérabilités.
   c. Entrez une description de l'évaluation des vulnérabilités ; entrez une ou plusieurs adresses e-mail, séparées par une virgule, auxquelles envoyer les résultats dans le cadre d'un processus d'audit que vous définissez.
   d. Cliquez sur Sauvegarder.
   Le processus d'évaluation des vulnérabilités est créé avec tous les tests, les sources de données sélectionnées et les récepteurs que vous avez définis.
   e. Exécutez le processus : accédez à Renforcement > Evaluation des vulnérabilités > Générateur d'évaluation, sélectionnez le processus, puis cliquez sur Exécuter une fois maintenant.

Rubrique parent : Protection de service de base de données cloud

Configuration de l'audit de base de données

Cette rubrique explique comment activer l'audit sur la base de données de sorte que les données d'audit d'objet puissent être extraites par Guardium. Modifiez le nombre limite d'objets ajoutés automatiquement au processus de classification, ainsi que le collecteur.

Pourquoi et quand exécuter cette tâche

La table Bases de données contient divers détails relatifs aux bases de données reconnues. Vous pouvez utiliser les indicateurs de couleur dans la table pour voir le statut d'une source de données d'un simple regard. Le rouge indique qu'il n'existe aucune configuration. Par exemple, la base de données n'est pas cataloguée ou la source de données n'a pas été affectée à un processus de classification ou d'évaluation de vulnérabilité. Des infobulles associées aux indicateurs de couleur relatifs au statut fournissent des informations supplémentaires sur la couleur rouge ou jaune. Utilisez la liste de filtres prédéfinis pour filtrer n'importe quelle colonne comportant les indicateurs de couleur relatifs au statut ou le filtre de texte libre pour d'autres valeurs.

Si un collecteur est défini pour la source de données, il apparaît dans la colonne Collecteur actif, si vous êtes le propriétaire. Sinon, la colonne est vide.

Le propriétaire de l'audit de base de données correspond au nom d'hôte CM dans un environnement CM. Dans un système autonome, la valeur correspond au nom d'hôte du collecteur.

La colonne Audit de base de données comporte l'une des valeurs suivantes :

- Activé. Suivie de la mention redémarrage en attente, cette valeur indique que le statut prendra effet au redémarrage de l'instance.
- Désactivé. Suivie de la mention redémarrage en attente, cette valeur indique que le statut prendra effet au redémarrage de l'instance.
- La configuration ne correspond pas aux exigences. (La trace d'audit de paramètre AWS n'est pas configurée en fonction des exigences XML, EXTENDED de Guardium. Demandez à l'administrateur de votre base de données de modifier cette valeur.) Suivie de la mention redémarrage en attente, cette valeur indique que le statut prendra effet au redémarrage de l'instance.
- Pas pris en charge pour ce moteur de base de données. La surveillance des activités n'est pas prise en charge actuellement par Guardium.

Si vous êtes le propriétaire de l'instance, qu'un processus de classification est affecté et qu'un audit de base de données est activé, les résultats sont affichés dans la colonne Objets. Le total est le nombre d'objets identifiés par les processus de classification affectés à cette instance ; la valeur Nombre d'éléments audités correspond au

nombre de ces objets qui sont activés pour l'audit d'objet ; la valeur Nombre de nouveaux éléments correspond au nombre d'objets qui ont été trouvés par un processus de classification mais qui n'ont pas été activés automatiquement. Ces objets requièrent une révision. Voir Gestion de l'audit d'objet.

Les résultats doivent apparaître dans la colonne `Objets` si un processus de classification est affecté à la source de données, le processus a été exécuté depuis l'activation de l'audit de base de données et vous êtes le propriétaire. Si vous ne voyez pas ces objets, vérifiez le processus de classification et réexécutez-le.

Rubrique parent : Protection de service de base de données cloud

Modification du nombre limite d'objets ajoutés automatiquement et du collecteur

Vous pouvez modifier le nombre limite d'objets ajoutés automatiquement et le collecteur sur une ou plusieurs bases de données simultanément. Les champs restés vides ne sont pas modifiés.

Procédure

1. Sélectionnez une ou plusieurs bases de données.
2. Cliquez sur Audit de base de données > Configuration d'audit de base de données.
3. Modifiez la valeur indiquée pour le champ Limiter les objets ajoutés automatiquement. nombre maximal d'objets détectés par Classification, qui peuvent être activés automatiquement pour l'audit d'objet lorsque l'option Audit de base de données est activée. Vous pouvez modifier ce paramètre, par base de données, une fois que chaque base de données a été reconnue. Les objets activés automatiquement apparaissent à l'état Activé dans la fenêtre des objets gérés. Si vous souhaitez que des objets soient automatiquement ajoutés par Guardium, définissez une limite raisonnablement élevée pour les résultats que le processus de classification devra trouver. Vous souhaiterez également empêcher qu'un dépassement d'objets ne se produise si votre classification contient une erreur. Par conséquent, ne définissez pas une limite trop élevée. (Un dépassement pourrait affecter les performances de base de données.) La valeur zéro (0) signifie qu'aucun objet n'est automatiquement activé pour l'audit d'objet. Si le nombre d'objets audités plus le nombre d'objets nouvellement classifiés dépassent cette limite, aucun nouvel objet n'est activé pour l'audit d'objet. Par exemple, si la valeur 15 est définie et que 5 objets sont identifiés lors de la première exécution du processus de classification, une trace d'audit est affectée à ces 5 objets. Si la valeur 15 est définie et que 5 objets sont déjà activés pour l'audit d'objet, si 16 objets sont identifiés lors du processus de classification suivant, aucun nouvel objet n'est activé pour l'audit d'objet. Si la valeur 15 est définie et que 5 objets sont déjà activés pour l'audit d'objet, si 5 objets sont identifiés lors du processus de classification suivant, ces 5 nouveaux objets sont activés pour l'audit d'objet.
4. Le collecteur s'affiche et est obligatoire pour un environnement Central Manager. Sélectionnez un collecteur dans la liste déroulante de tous les collecteurs dans l'environnement CM. Il s'agit du collecteur qui extrait les données d'audit (activités) de la base de données.
5. Cliquez sur Appliquer.

Activation de l'audit sur une base de données

Cette rubrique explique comment activer l'audit de base de données sur une base de données à la fois.

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer le paramètre Limiter les objets ajoutés automatiquement ou le collecteur avec n'importe quel niveau de droits. Les autres modifications nécessitent des droits de base de données. Vos clés d'accès peuvent ou non inclure ces droits. Les instructions ci-dessous couvrent tous les niveaux de droits.

Lorsque vous activez l'audit de base de données, votre système Guardium devient l'unique propriétaire de l'audit de base de données sur cette base de données. Aucun autre système Guardium ne peut modifier l'audit de base de données ou l'audit d'objet. Un autre système peut utiliser la force pour devenir propriétaire en cliquant sur Devenir le propriétaire de l'audit de base de données.

Exécutez la classification au moins une fois après l'activation de l'audit de base de données pour voir et gérer les objets sur lesquels effectuer un audit. Si aucun objet n'est trouvé, vérifiez vos politiques.

ATTENTION :
Lorsque vous commencez à gérer la base de données, la balise RDS Amazon IBM Guardium IP est créée avec la valeur de votre nom d'hôte Guardium. Cette balise ne doit pas être modifiée ni retirée.

Procédure

1. Sélectionnez la ligne correspondant à la base de données.
2. Cliquez sur Audit de base de données > Configuration d'audit de base de données.
3. Modifiez éventuellement le nombre d'objets ajoutés automatiquement à l'audit d'objet.
4. Dans l'environnement CM, si aucun collecteur n'est défini, sélectionnez-en un dans la liste déroulante et cliquez sur Appliquer. La boîte de dialogue est actualisée et les boutons sont activés.
5. Si l'option Activer l'audit de base de données est activée, cliquez dessus. La boîte de dialogue et la table sont actualisées pour indiquer que vous êtes désormais le propriétaire de l'audit de base de données. La boîte de dialogue est actualisée. Cliquez sur Redémarrer pour redémarrer immédiatement la base de données (un message de confirmation s'affiche) ou cliquez sur Prochain redémarrage manuel, par exemple, pour attendre une fenêtre de maintenance. Si vous choisissez Prochain redémarrage manuel, vous devrez accéder directement à la console de cloud ultérieurement. Si vous cliquez sur Redémarrer et que vous ne disposez pas des droits d'accès suffisants, un message d'erreur s'affiche. Demandez à votre administrateur de base de données de configurer une **trace d'audit** avec la valeur XML, EXTENDED et redémarrez l'instance.
6. Si l'option Activer l'audit de base de données n'est pas activée, cliquez sur Etre propriétaire de l'audit de base de données. La boîte de dialogue est actualisée. Cliquez sur Prochain redémarrage manuel et demandez à votre administrateur de base de données de configurer la **trace d'audit** avec la valeur XML, EXTENDED, puis redémarrez l'instance.
7. Si vous avez changé le statut d'audit de base de données, cliquez sur Extraire le statut, attendez que le message indiquant que le statut a changé s'affiche, puis cliquez sur Actualiser. La colonne Propriétaire de l'audit de base de données contient le nom d'hôte du gestionnaire central ou du collecteur dans une instance Guardium autonome, et l'icône de l'audit de base de données devient verte.

Désactivation de l'audit sur une base de données

Cette rubrique explique comment désactiver l'audit de base de données sur une base de données à la fois. Lorsque vous désactivez l'audit de base de données, vous renoncez du même coup la propriété sur l'audit de base de données.

Pourquoi et quand exécuter cette tâche

Lorsque vous cessez d'être le propriétaire de l'audit de base de données ou que vous désactivez cette fonction, l'ensemble de l'audit d'objet est également désactivé et la liste des objets sur lesquels un audit peut être effectué (issus des résultats de la classification) est supprimée.

Procédure

1. Sélectionnez la ligne correspondant à la base de données.
2. Cliquez sur Audit de base de données > Configuration d'audit de base de données.
3. Cliquez sur Désactiver l'audit de base de données, puis cliquez sur Prochain redémarrage manuel, par exemple, pour attendre une fenêtre de maintenance, ou cliquez sur Redémarrer pour redémarrer immédiatement la base de données. Si vous choisissez d'attendre le prochain redémarrage manuel, vous devrez accéder directement à la console de cloud ultérieurement. Si vous n'êtes pas autorisé à modifier la configuration, cliquez sur Ne plus être propriétaire de l'audit de base de données et demandez à votre administrateur de base de données de désactiver l'audit de base de données sur cette instance.
4. Cliquez sur Extraire le statut pour actualiser l'affichage avec le statut le plus récente à partir du cloud.

Résultats

Si des changements sont survenus, le message suivant s'affiche : `Le statut d'audit de base de données a changé pour plusieurs bases de données. Cliquez sur Actualiser pour mettre à jour la table.` Cliquez sur Actualiser. Le statut devient Désactivé ou Désactivé, redémarrage en attente, l'icône de l'audit de base de données devient rouge et la colonne Propriétaire de l'audit de base de données est vide.

Comment devenir et cesser d'être propriétaire d'un audit de base de données

Pourquoi et quand exécuter cette tâche

Vous pouvez modifier le statut de propriété de la base de données pour une seule base de données à la fois.

Si vous êtes propriétaire de l'audit de base de données, vous disposez de droits exclusifs sur les définitions d'audit de base de données et d'audit d'objet, et vous avez accès aux données de l'audit d'objet (voir Gestion de l'audit d'objet). D'autres systèmes Guardium peuvent accéder au même compte cloud, mais ne peuvent visualiser que les détails de la base de données.

Grâce aux droits d'accès complet dont vous disposez, lorsque vous activez l'audit de la base de données, vous devenez également propriétaire de cette dernière. Si vos clés d'accès ne fournissent pas de droits d'accès complet, vous devenez propriétaire sans activer l'audit de base de données. Lorsque l'audit de base de données est activé (par l'administrateur de base de données), vous avez accès aux données d'audit. A l'inverse, lorsque vous désactivez l'audit de base de données, vous renoncez du même coup à la propriété. Si vos clés d'accès ne fournissent pas de droits d'accès complet, vous cessez d'être le propriétaire de l'audit de base de données et vous demandez à l'administrateur de base de données de désactiver l'audit de base de données.

Vous pouvez transférer la propriété d'un système Guardium à un autre.

Si vous transférez la propriété d'un système en ligne à un autre, enlevez d'abord la propriété de l'audit de base de données à son propriétaire du moment, puis prenez-la sur le second système Guardium. Tout l'audit est arrêté lorsque l'un des systèmes Guardium abandonne la propriété. Vous devez ensuite définir le processus d'audit sur le nouveau système Guardium : affectez la base de données à une classification, exécutez le processus et ajoutez des objets à l'audit d'objets.
ATTENTION :
Cédez la propriété de l'audit de base de données sur un avant de l'approprier sur le second. Sinon, les données iront au précédent collecteur ainsi qu'au nouveau collecteur. Les deux collecteurs, avec des politiques (CM) différentes, recevront les mêmes activités, mais produiront des résultats différents et incomplets.

Si vous transférez la propriété d'un système Guardium qui s'est arrêté sans espoir de récupération, vous pouvez commencer à posséder l'audit de base de données depuis un autre système Guardium tout en maintenant les définitions d'audit. Seule l'appartenance de l'audit change. Dans ce scénario, arrêtez le système Guardium d'origine de posséder l'audit de base de données dans la console DB.

Procédure

1. Dans la table Bases de données, sélectionnez la ligne correspondant à la base de données.
2. Pour ne plus être propriétaire d'un audit de base de données, cliquez sur Audit de base de données > Configuration d'audit de base de données > Ne plus être propriétaire de l'audit de base de données.
3. Pour devenir propriétaire d'un audit de base de données, cliquez sur Audit de base de données > Configuration d'audit de base de données > Devenir propriétaire de l'audit de base de données.

Gestion de l'audit d'objet

Cette rubrique vous explique comment afficher les objets sensibles potentiellement identifiés par les processus de classification dans les bases de données que vous gérez et activer l'audit d'objet sur certains objets sélectionnés afin de surveiller toutes les activités effectuées sur ces objets.

Pourquoi et quand exécuter cette tâche

Prérequis : vous devez activer et devenir propriétaire de l'audit de base de données, et la classification doit être exécutée au moins une fois sur cette source de données.

Les nouveaux objets sont des objets qui ont été trouvés par les processus de classification et qui n'ont pas été activés à des fins d'audit. Vous pouvez filtrer tous les nouveaux objets, puis les activer pour l'audit d'objet ou désélectionner l'indicateur `Nouveau`. Si aucun nouvel objet n'est trouvé, cela signifie que vous êtes à jour concernant l'évaluation des nouveaux objets. N'oubliez pas que Guardium peut recevoir de nouvelles données chaque fois que le processus de classification est exécuté. Lorsque le processus trouve de nouveaux objets qui n'ont pas été ajoutés automatiquement à l'audit d'objet, un message indiquant que `des nouveaux objets ont été trouvés` s'affiche.

La colonne `Trouvé par classification` répertorie tous les processus de classification qui ont identifié l'objet.

Lorsque la colonne Statut d'audit d'objet indique le statut Mixte, cela signifie que l'audit d'objet est activé dans certaines sources de données et désactivé dans d'autres sources de données.

L'activation et la désactivation de l'audit de l'objet est un processus très lourd, qui peut prendre quelques minutes. Une icône d'attente apparaît pendant le traitement des changements d'audit par le cloud.

Vous pouvez passer en revue les objets trouvés dans une ou plusieurs sources de données en sélectionnant les lignes correspondant aux sources de données concernées dans la table Bases de données. La fenêtre d'audit d'objet présente tous les objets trouvés par tous les processus de classification sur la ou les base(s) de données sélectionnée(s).

- Gestion de l'audit d'objet dans une base de données
- Gestion de l'audit d'objet dans plusieurs bases de données

Rubrique parent : Protection de service de base de données cloud

Gestion de l'audit d'objet dans une base de données

Pourquoi et quand exécuter cette tâche

La fenêtre Objets dans la source de données <nom> répertorie tous les objets trouvés par les processus de classification exécutés sur cette source de données. Des objets peuvent être trouvés par plus d'un processus de classification.

Lorsque des objets sont identifiés par le processus de classification mais n'ont pas été activés automatiquement pour l'audit d'objet, le message `Nouveaux objets trouvés` apparaît au-dessus de la table des objets. Cliquez sur Nouveau uniquementt pour filtrer tous les nouveaux objets trouvés nécessitant d'être traités. De nouveaux objets peuvent être trouvés chaque fois qu'un processus de classification est exécuté. Si aucun nouvel objet n'est trouvé, cela signifie que vous êtes à jour concernant l'évaluation des nouveaux objets.

Passez en revue les sources de données régulièrement : recherchez les éventuels nouveaux objets et si vous le souhaitez, ajoutez ou retirez des objets de l'audit d'objet. Par exemple, vous pouvez retirer des objets si les objets ajoutés automatiquement incluent des objets qui ne nécessitent pas d'audit, ou si une base de données rencontre des problèmes de performance. Ou bien, vous pouvez identifier un objet suspect qui n'est pas audité et l'ajouter à l'audit d'objet.

Utilisez le filtre de classification pour les objets pour lesquels vous savez qu'un audit doit être effectué. Sélectionnez tous les objets dans la vue filtrée et activez l'audit d'objet.

Procédure

1. Si vous avez affecté le processus de classification **avant** d'activer l'audit de base de données, exécutez une fois le processus de classification immédiatement et attendez quelques minutes (ou attendez la prochaine exécution planifiée) que le système Guardium identifie des objets.
2. Sélectionnez une source de données. Envisagez d'utiliser le filtreNouveaux objets trouvés pour identifier les sources de données comportant de nouveaux objets.
3. Sélectionnez Audit de base de données > Gérer l'audit d'objet. La fenêtre Gérer l'audit d'objet s'ouvre avec tous les objets trouvés par les processus de classification auxquels cette source de données a été affectée.
4. Envisagez d'utiliser le filtre Nouveau uniquement pour identifier tous les objets classifiés comme nouveaux.
5. Sélectionnez un ou plusieurs objets (lignes) dans la table.
6. Pour activer une trace d'audit, sélectionnez Actions > Activer l'audit. Le système répond en indiquant que l'opération a abouti ou échoué.
7. Pour désélectionner l'indicateur Nouveau, cliquez sur Actions > Effacer l'indicateur Nouveau.
8. Pour désactiver une trace d'audit, sélectionnez Actions > Désactiver l'audit. Le système répond en indiquant que l'opération a abouti ou échoué.

Rubrique parent : Gestion de l'audit d'objet

Gestion de l'audit d'objet dans plusieurs bases de données

Pourquoi et quand exécuter cette tâche

Cette vue répertorie tous les objets trouvés par les processus de classification exécutés sur les sources de données sélectionnées. Des objets peuvent être trouvés par plus d'un processus de classification. Affichez les objets regroupés par objet (par défaut) ou par classification. La colonne Trouvé par classification répertorie tous les processus de classification qui ont identifié l'objet.

Lorsque des objets sont identifiés par le processus de classification mais n'ont pas été activés automatiquement pour l'audit d'objet, le message Nouveaux objets trouvés apparaît au-dessus de la table des objets. Cliquez sur Nouveau uniquement pour filtrer tous les nouveaux objets trouvés nécessitant d'être traités. Examinez les nouveaux objets et activez l'audit d'objet ou désélectionnez l'indicateur Nouveau.

De nouveaux objets peuvent être trouvés chaque fois qu'un processus de classification est exécuté. Si aucun nouvel objet n'est trouvé, cela signifie que vous êtes à jour concernant l'évaluation des nouveaux objets.

Passez en revue les sources de données régulièrement : recherchez les éventuels nouveaux objets et si vous le souhaitez, ajoutez ou retirez des objets de l'audit d'objet. Par exemple, vous pouvez retirer des objets si les objets ajoutés automatiquement incluent des objets qui ne nécessitent pas d'audit, ou si une base de données rencontre des problèmes de performance. Ou bien, vous pouvez identifier un objet suspect qui n'est pas audité et l'ajouter à l'audit d'objet.

Regrouper par objet : pour afficher tous les nouveaux objets trouvés, entrez Nouveau dans le filtre de texte.

Pour activer ou désactiver l'audit d'objet sur un objet dans toutes les sources de données sélectionnées, sélectionnez la ou les lignes, puis cliquez sur Action > Activer/Désactiver.

Pour effectuer une action par source de données, cliquez sur Présent dans # sources de données afin de visualiser toutes les sources de données dont les processus de classification ont identifié l'objet sélectionné.

Regrouper par classification est une option particulièrement utile lorsque vous avez des politiques de classification ou des sources de données presque identiques pour lesquelles un audit d'objet doit être effectué sans aucune autre évaluation, par exemple, GDPR.

Procédure

1. Si vous avez affecté le processus de classification **avant** d'activer l'audit de base de données, exécutez le processus de classification une fois (ou attendez la prochaine exécution planifiée) et attendez quelques minutes que le système Guardium identifie des objets.
2. En cas de regroupement par objet :
    a. Sélectionnez plusieurs sources de données pour lesquelles de nouveaux objets figurent dans la colonne Objets de la table Bases de données. Utilisez le filtre Nouveaux objets trouvés pour identifier ces sources de données.
    b. Cliquez sur Audit de base de données > Gérer l'audit d'objet. La fenêtre Gérer l'audit d'objet s'ouvre.
    c. Si l'objet doit toujours faire l'objet d'un audit dans toutes les sources de données, sélectionnez la ou les lignes, puis cliquez sur Actions > Activer l'audit. Le système répond en indiquant que l'opération a abouti ou échoué.
    d. SI vous voulez activer l'audit d'objet sur des bases de données individuelles, cliquez sur le nombre dans la colonne Présent dans (nombre) sources de données sur la ligne correspondant à l'objet afin d'ouvrir la fenêtre Sources de données contenant l'<objet>. Cette fenêtre affiche toutes les sources de données dont les processus de classification ont identifié l'objet sélectionné. Sélectionnez une ou plusieurs lignes de source de données, puis cliquez sur Actions > Activer l'audit.

3. Pour un processus de classification dont les objets identifiés doivent toujours faire l'objet d'un audit sans autre évaluation, cliquez sur le bouton d'option Classification (au-dessus de la table), sélectionnez une ou plusieurs lignes de processus de classification, puis cliquez sur Actions > Activer l'audit.

Rubrique parent : Gestion de l'audit d'objet

Reconnaissance automatique de base de données

L'application de reconnaissance automatique examine et analyse vos serveurs à la recherche de ports ouverts afin d'empêcher toute connexion inconnue ou indésirable avec votre réseau. Vous pouvez exécuter des processus de reconnaissance automatique à la demande ou planifier leur exécution sur une base périodique.

Présentation du processus de reconnaissance automatique de base de données

Il existe de nombreux scénarios dans lesquels des bases de données peuvent exister sans être détectées sur votre réseau, ce qui représente un risque potentiel pour celui-ci. D'anciennes bases de données peuvent avoir été oubliées et laissées sans surveillance, ou une nouvelle base de données peut avoir été ajoutée en même temps qu'un package d'applications. Il peut aussi arriver qu'un administrateur de base de données non autorisé crée une nouvelle instance d'une base de données afin d'exercer des activités malveillantes en dehors des bases de données surveillées.

La reconnaissance automatique utilise des travaux d'analyse et d'examen pour s'assurer qu'il n'existe aucune base de données non détectée dans votre environnement.

- Un travail d'*examen* parcourt chaque hôte spécifié (ou les hôtes d'un sous-réseau spécifié) et compile une liste des ports ouverts spécifiés pour cet hôte.
- Un travail d'*analyse* utilise les résultats de l'examen pour déterminer si des services de base de données sont en cours d'exécution sur les ports ouverts. Un travail d'analyse ne peut pas aboutir s'il n'est pas précédé d'un travail d'examen. Affichez les résultats de ce travail dans le rapport prédéfini intitulé Bases de données reconnues.

Avant de commencer, vous devez télécharger et installer le correctif de l'application de reconnaissance automatique. Ce correctif est disponible sur le site IBM Fix Central.

Procédez comme suit pour utiliser l'application de reconnaissance automatique :

1. Créez un processus de reconnaissance automatique pour rechercher des ports ouverts sur des adresses IP ou des sous-réseaux spécifiques.
2. Exécutez le processus de reconnaissance automatique à la demande ou de manière planifiée.
3. Affichez les résultats du processus avec des rapports de reconnaissance automatique ou créez des rapports personnalisés.

La reconnaissance automatique a ses propres processus. Ils sont indépendants des processus d'audit, mais fonctionnent exactement de la même manière.

Lors d'un examen, vous ne pouvez entrer que des adresses IP, et pas de noms d'hôte, mais Guardium détecte des noms d'hôte dans le cadre du rapport. Guardium ne tronque pas les noms d'hôte dans le produit Guardium. Toutefois, il peut s'avérer nécessaire de configurer le rapport avec des colonnes plus larges.

Le processus de reconnaissance automatique de Guardium ne peut pas deviner quelle sera la base de données qui apparaîtra lors d'une analyse. Si le processus de reconnaissance automatique de Guardium indique qu'elle a trouvé une base de données, elle est certaine à 100 % de l'identité de la base de données.

Remarque : Le processus de reconnaissance ne détecte que des bases de données actives. Les bases de données devront être démarrées si vous prévoyez d'utiliser la reconnaissance lors de l'installation. Etant donné la manière dont l'interception AIX KTAP fonctionne, les bases de données doivent être redémarrées après la première exécution de l'agent S-TAP. Dans le cas contraire, une partie de l'interception ne fonctionnera pas.

Création d'un processus de reconnaissance automatique

Spécifiez l'hôte et les ports explorés par le processus de reconnaissance automatique.

1. Configurez la reconnaissance automatique en cliquant sur Reconnaître > Reconnaissance de base de données > Configuration de la reconnaissance automatique.
2. Cliquez sur Nouveau pour créer un nouveau processus et ouvrir la fenêtre Générateur de processus de reconnaissance automatique.
3. Renseignez le champ Nom de processus en indiquant un nom qui est unique sur votre système Guardium.
4. Pour exécuter un travail d'analyse immédiatement après le travail d'examen, cochez la case Exécuter la vérification après l'examen.
5. Pour chaque hôte ou sous-réseau à explorer, entrez un nom d'hôte et un port, puis cliquez sur Ajouter examen. Chaque fois que vous ajoutez un examen, il est ajouté à la liste de tâches.
   Remarque :
   - Les caractères génériques sont activés. Par exemple, pour sélectionner toutes les adresses commençant par 192.168.2, utilisez 192.168.2.*.
   - Indiquez une plage de ports en séparant le premier et le dernier numéros de port par un tiret. Par exemple : 4100-4102.
   - Après avoir ajouté une analyse, modifiez le nom d'hôte ou le port en tapant par dessus. Cliquez sur Appliquer pour sauvegarder la modification.
   - Si vous avez une configuration de double pile, vous devrez configurer un examen portant à la fois sur les adresses IPV4 et sur les adresses IPV6.
   - Pour retirer un examen, cliquez sur l'icône Supprimer cette tâche pour cet examen. Si des résultats d'examen dépendent d'une tâche, l'examen ne peut pas être supprimé.
6. Lorsque vous avez terminé d'ajouter des examens, cliquez sur Appliquer et exécutez le travail ou planifiez le travail ultérieurement.

Si vous avez besoin d'aide pour définir un planning, consultez Plannification.

Exécution ou planification d'un processus de reconnaissance automatique

Exécutez ou planifiez des travaux d'examen et d'analyse dans le cadre du processus de reconnaissance automatique.

1. Cliquez sur Reconnaître > Reconnaissance de base de données > Configuration de la reconnaissance automatique.
2. Sélectionnez dans la liste Sélecteur de processus de reconnaissance automatique le processus à exécuter, puis procédez de l'une des façons suivantes :
3.
   - Pour exécuter immédiatement un travail, cliquez sur Exécuter une fois maintenant.
   - Pour planifier un travail ultérieurement, cliquez sur Modifier le planning (si vous avez besoin d'aide pour définir un planning, consultez Planification).
     Remarque : Un travail d'analyse ne peut pas être exécuté sans les résultats du travail d'examen. Vous pouvez planifier les deux travaux pour qu'ils s'exécutent individuellement ou configurer le travail d'analyse pour qu'il s'exécute après le travail d'examen en modifiant un processus, puis en cochant la case Exécuter la vérification après l'examen.
4. Après avoir démarré ou planifié un travail, vous pouvez cliquer sur Progression/Récapitulatif pour afficher le statut de ce processus.

Rapports de reconnaissance automatique

Ouvrez les rapports de reconnaissance automatique en cliquant sur Reconnaître > Rapports et en sélectionnant l'un des rapports disponibles.

Vous pouvez créer des rapports personnalisés à l'aide de la fenêtre Générateur de requête de reconnaissance automatique. Ouvrez la fenêtre Générateur de requête de reconnaissance automatique en cliquant sur Reconnaître > Reconnaissance de base de données > Générateur de requête de reconnaissance automatique.

Rapport sur les bases de données reconnues

Ouvrez le rapport Bases de données reconnues en cliquant sur Reconnaître > Rapports > Bases de données reconnues.

La principale entité pour ce rapport est le port reconnu. Il existe une ligne spécifique dans le rapport pour chaque port individuel reconnu. Les colonnes du rapport sont les suivantes : Heure de l'analyse, Adresse IP de serveur, Nom d'hôte de serveur, Type de base de données, Port, Type de port (généralement TCP) et Nombre d'occurrences.

Il n'existe aucun paramètre d'exécution spécial pour ce rapport, mais celui-ci exclut les ports reconnus avec une base de données dont le type est inconnu.

Lorsque la définition d'un processus de reconnaissance automatique est modifiée, les statistiques de ce processus sont réinitialisées.

Domaine de suivi de la reconnaissance automatique

Le domaine de suivi de la reconnaissance automatique contient toutes les données signalées par les processus de reconnaissance automatique. Cliquez sur un nom d'entité pour en afficher les attributs.

Entités du domaine de suivi de la reconnaissance automatique

- Le champ d'examen de la reconnaissance automatique contient un horodatage pour chaque opération d'examen.
- Le champ Hôte reconnu fournit l'adresse IP et le nom d'hôte de chaque hôte reconnu.
- Le champ Port reconnu fournit une valeur d'horodatage, identifie le port et contient le type de base de données pour chaque port reconnu qui est ouvert.

Rubrique parent : Reconnaissance

Classification

Les politiques et processus de classification définissent la manière dont Guardium reconnaît et traite des données sensibles, telles que des numéros de carte de crédit, des numéros de sécurité sociale et des données financières personnelles.

L'importance des processus de reconnaissance et de classification grandit à mesure que la taille d'une organisation augmente et que des données sensibles, telles que des numéros de carte de crédit et des données financières personnelles, deviennent de plus en plus nombreuses, souvent à l'insu des administrateurs chargés de gérer ces données. Cela se produit souvent dans le contexte de fusions et d'acquisitions, ou lorsque des systèmes existants ont survécu à leurs propriétaires initiaux. La création de flux de travaux pour la reconnaissance des données sensibles vous permet d'identifier ce type de données dans votre environnement et d'entreprendre les actions appropriées, par exemple, appliquer des politiques d'accès.

Les *processus de classification* sont constitués de politiques de classification qui ont été associées à une ou plusieurs sources de données. Ils peuvent être soumis pour s'exécuter une fois ou, si des données d'identification de connexion ont été stockées pour toutes les sources de données utilisées dans le processus, être planifiés pour s'exécuter périodiquement dans le cadre d'un processus d'automatisation de flux de travaux de conformité.

Les *politiques de classification* sont constituées de règles de classification et d'actions de règle de classification conçues pour rechercher et baliser des données sensibles dans des sources de données spécifiées.

Les *règles de classification* utilisent des expressions régulières, des algorithmes de Luhn et d'autres critères pour définir les règles de mise en correspondance de contenu dans le cadre de l'application d'une politique de classification.

Les *actions de règle de classification* spécifient un ensemble d'actions à exécuter pour chacune des règles définies dans une politique de classification. Par exemple, une action peut générer une alerte e-mail ou ajouter un objet à un groupe Guardium. Chaque fois qu'une règle est satisfaite, l'événement correspondant est consigné et, par conséquent, peut faire l'objet d'un rapport (sauf si l'option Ignorer est spécifiée comme action à entreprendre, auquel cas, aucune consignation n'est effectuée pour cette règle).

- Performances du processus de classification
  Les processus de classification sont gérés avec des routines d'échantillonnage et des paramètres de délai d'attente afin de garantir un impact minimal sur les performances des serveurs de base de données.
- Gestion des règles de classification
  Les règles de classification sont gérées en fonction de critères de mise en correspondance et de regroupement flexibles.
- Gestion des processus de classification
  Créez, exécutez et visualiser des processus de classification à l'aide de l'application Générateur de processus de classification.
- Gestion des politiques de classification
- Gestion des règles de classification
- Gestion des actions de règle de classification

Rubrique parent : Reconnaissance

Performances du processus de classification

Les processus de classification sont gérés avec des routines d'échantillonnage et des paramètres de délai d'attente afin de garantir un impact minimal sur les performances des serveurs de base de données.

Lorsque vous exécutez le classificateur, vous avez la possibilité de spécifier la façon dont il échantillonne les enregistrements. Par défaut, il prend un échantillonnage aléatoire de lignes à l'aide d'une instruction appropriée pour la plateforme de base de données concernée. Par exemple, le classificateur crée des échantillons en utilisant une instruction rand() pour les bases de données SQL. L'autre comportement est l'échantillonnage séquentiel au cours duquel les lignes sont lues, dans l'ordre, jusqu'à ce que la taille d'échantillon spécifiée soit atteinte. L'échantillonnage aléatoire est le comportement par défaut. Il est généralement recommandé car il fournit des résultats plus représentatifs. Toutefois, comparé à l'échantillonnage séquentiel, l'échantillonnage aléatoire peut altérer légèrement les performances. Pour l'échantillonnage aléatoire et pour l'échantillonnage séquentiel, la taille d'échantillon par défaut correspond à 2 000 lignes ou au nombre total de lignes disponibles (la valeur la moins élevée des deux). Il est possible de spécifier des tailles d'échantillon supérieures ou inférieures.

Pour minimiser davantage l'impact des processus de classification sur le serveur de base de données, les requêtes de longue durée seront annulées, consignées et le restant du tableau sera ignoré. Toute ligne obtenue jusqu'à ce point sera utilisée lors de l'évaluation des règles pour la table. De même, si un processus de classification

s'exécute pendant une longue période et n'aboutit pas, l'ensemble du processus est arrêté, consigné avec les statistiques de processus, et le processus de classification suivant est démarré. Cela est assez rare et ne se produit que sur les serveurs qui connaissent déjà des problèmes de performances.

Périodiquement, le classificateur passe lui-même au ralenti de manière à ne pas surcharger le serveur de base de données de demandes. Si de nombreuses règles de classification échantillonnent des données, la charge sur le serveur de base de données doit rester constante, mais l'exécution du processus peut prendre plus de temps.

Le classificateur gère les faux résultats positifs en utilisant des groupes exclus pour le schéma, le tableau et les colonnes de tableau. Auparavant, il pouvait s'avérer complexe de configurer Guardium afin qu'il ignore les faux résultats positifs pour les examens de classification suivants. Aujourd'hui, lorsque vous passez en revue les résultats du classificateur, vous pouvez facilement ajouter des faux résultats positifs à un groupe d'exclusion, puis ajouter celui-ci à la politique de classification, de sorte que ces résultats soient ignorés pour les examens suivants.

Rubrique parent : Classification

Gestion des règles de classification

Les règles de classification sont gérées en fonction de critères de mise en correspondance et de regroupement flexibles.

Marqueur "Déclencher uniquement avec"

Le marqueur "Déclencher uniquement avec" permet de regrouper les types de règle de classification de même nom. De plus, toutes les règles renvoyées à l'aide d'un repère doivent renvoyer des données sur la base du même nom de table. Si deux règles, ou plus, sont définies avec le même repère, elles se déclenchent en même temps, de telle sorte que si ces deux règles sont déclenchées sur la même table, elles sont toutes les deux consignées et leurs actions appelées. En revanche, si une seule de ces deux règles se déclenche sur une table, aucune d'elles n'est consignée et aucune de leurs actions n'est appelée. Le déclenchement de plusieurs règles en même temps est indispensable si vous voulez que vos données sensibles apparaissent conjointement dans la même table. Par exemple, vous souhaiterez peut-être être averti lorsqu'une table comporte à la fois un numéro de sécurité sociale et un permis de conduire du Massachusetts.

Le marqueur "Déclencher uniquement avec" correspond à une valeur constante, quelle qu'elle soit, qui doit être rigoureusement identique dans toutes les règles que vous souhaitez regrouper. Cela signifie que si une règle comporte un repère ABC, l'autre règle avec laquelle vous souhaitez la regrouper doit également comporter un repère ABC. Si la valeur de repère est différente, les règles ne sont plus regroupées.

Vous devez utiliser au moins deux règles de n'importe quelle valeur basées sur la recherche de données dans le même nom de table.

Continuer en cas de correspondance

Le marqueur "Déclencher uniquement avec" est également basé sur le paramètre Continuer en cas de correspondance. Par exemple, si les règles suivantes ont été définies de telle manière que la règle 3 ne corresponde pas au paramètre Continuer en cas de correspondance, aucun résultat n'est renvoyé sauf si les trois règles de repère étaient positives. Cela est dû au fait que vous n'avez pas pu l'occasion d'exécuter la règle 4 et que le regroupement ne se déclenchera pas car tous les marqueurs "Déclencher uniquement avec" doivent s'exécuter avec des résultats positifs.

Règle 1. Règle ABC avec repère de déclenchement (continuer en cas de correspondance)

Règle 2. Règle ABC avec repère de déclenchement (continuer en cas de correspondance)

Règle 3. Type de règle sans repère de déclenchement (continuer en cas de correspondance)

Règle 4. Règle ABC avec repère de déclenchement (continuer en cas de correspondance)

Avec des colonnes sans correspondance uniquement

Utilisez cette option pour réduire la granularité des résultats de données. Certaines organisations souhaiteront peut-être sonder leurs données afin de reconnaître quelles sont les tables et colonnes qui contiennent des données sensibles, sans avoir nécessairement besoin de trouver chaque type de données sensibles dans les colonnes concernées. Une nouvelle option pour le paramètre Continuer en cas de correspondance, intitulée Avec des colonnes sans correspondance uniquement, signifie que dès que le classificateur trouve une correspondance pour cette colonne, il ignore cette dernière et poursuit son traitement.

Tableau 1. Récapitulatif des options de traitement disponibles pour le processus de classification

Continuer en cas de correspondance	Avec des colonnes sans correspondance uniquement	Granularité des résultats
Non	Non applicable	Table. Le traitement des règles par le classificateur cesse après la première occurrence trouvée dans la table.
Oui	Oui	Table et colonne. Le classificateur enregistre la première occurrence pour n'importe quelle colonne donnée, puis ignore cette dernière pour le traitement des règles suivantes.
Oui	Non	Détail. Le classificateur enregistre les occurrences de toutes les colonnes pour toutes les règles.

Classification avec algorithme de Luhn

Lorsqu'un nom de règle commence par guardium://CREDIT_CARD et que le champ d'expression de recherche contient un modèle de numéro de carte de crédit valide, la politique de classification utilise l'algorithme de Luhn (algorithme largement utilisé pour valider des numéros d'identification, tels que les numéros de carte de crédit), en plus de la mise en correspondance de modèle standard. L'algorithme de Luhn est un contrôle supplémentaire et ne remplace pas le contrôle de modèle. Un numéro de carte de crédit valide est une chaîne de 16 chiffres ou quatre groupes de quatre chiffres, chaque groupe étant séparé par un espace. La zone d'expression de recherche doit obligatoirement contenir le nom de règle guardium://CREDIT_CARD et un nombre [0-9]{16} valide pour que l'algorithme de Luhn puisse être utilisé dans le cadre de cette mise en correspondance de modèle.

Rubrique parent : Classification

Gestion des processus de classification

Créez, exécutez et visualiser des processus de classification à l'aide de l'application Générateur de processus de classification.

Procédure

Ouvrez le panneau Générateur de processus de classification en accédant à Reconnaître > Classifications > Générateur de processus de classification.
Rubrique parent : Classification

Création d'un processus de classification

Procédure

1. Sur le panneau Générateur de processus de classification, cliquez sur l'icône afin d'ouvrir le panneau Définir un processus de classification.
2. Entrez un nom pour le processus dans le champ Description de processus.
3. Sélectionnez une politique de classification dans la liste. Vous pouvez cliquer sur Modifier pour visualiser et éditer la politique si nécessaire.
4. Vous pouvez éventuellement désélectionner la case Echantillonnage aléatoire. Ce dispositif s'applique uniquement lorsque le nombre d'enregistrements dans un tableau dépasse la taille de l'échantillon. L'échantillonnage aléatoire effectue une recherche aléatoire d'un certain nombre d'enregistrements dans le tableau jusqu'à ce que la taille d'échantillon définie soit atteinte. Il s'agit d'une recherche de haute qualité car les résultats obtenus sont plus représentatifs des données. Lorsque la case Echantillonnage aléatoire est désélectionnée, la recherche des enregistrements dans le tableau s'effectue de manière séquentielle jusqu'à ce que la taille d'échantillon définie soit atteinte. Une recherche séquentielle peut être plus rapide qu'une recherche aléatoire, mais il se peut que les résultats obtenus ne soient pas aussi représentatifs de toutes les données disponibles.
5. Entrez une taille d'échantillon lorsque vous recherchez des données (voir les rubriques Définition de règles de politique de classification/Définition d'une recherche de règle dans des données). Si le nombre d'enregistrements dans un tableau est <= à "taille de l'échantillon", la recherche d'une correspondance porte sur tous les enregistrements. Lorsque le nombre d'enregistrements dans un tableau dépasse la taille de l'échantillon, l'échantillonnage peut être utilisé.
6. Cliquez sur le bouton Ajouter une source de données pour ajouter une ou plusieurs sources de données.
7. Cliquez sur Sauvegarder. La procédure de définition du processus de classification est à présent terminée.
8. Vous pouvez éventuellement ajouter des commentaires à la définition. Voir la rubrique sur les commentaires dans le fichier d'aide relatif aux outils communs.
9. Vous pouvez éventuellement ajouter des rôles de sécurité. Voir la rubrique sur les rôles de sécurité dans le fichier d'aide relatif à la gestion des accès.
10. Vous pouvez éventuellement soumettre le processus de classification pour exécution. Voir la rubrique Exécution d'un processus de classification.
11. Cliquez sur Terminé lorsque vous avez terminé.

Exécution d'un processus de classification

Pourquoi et quand exécuter cette tâche

Il existe trois façons d'exécuter des processus de classification :

- A la demande, à partir du panneau Générateur de processus de classification, comme expliqué dans cette rubrique.
- En tant que tâche au sein d'un *processus d'automatisation de flux de travaux de conformité*, comme expliqué dans une autre rubrique.
- Dans le cadre d'un *flux de travaux de reconnaissance des données sensible*, comme expliqué dans une autre rubrique.

Procédure

1. Depuis le panneau Générateur de processus de classification, sélectionnez le processus à exécuter, puis cliquez sur Modifier pour ouvrir le panneau Générateur de processus de classification.
2. Cliquez sur le bouton Exécuter une fois maintenant pour soumettre le travail. Le processus est ainsi placé dans la file d'attente de travaux Guardium à partir de laquelle le système Guardium exécute un travail à la fois. Vous pouvez afficher le statut du travail à l'aide du panneau File d'attente de travaux Guardium.
3. Cliquez sur le bouton Terminé lorsque vous avez terminé.

Affichage des résultats de classification

Procédure

1. Sur le panneau Générateur de processus de classification, cliquez sur le bouton Afficher les résultats. Les résultats s'affichent dans une fenêtre distincte.
2. Sur n'importe quelle ligne du journal d'exécution de processus, cliquez sur Détails pour afficher d'autres informations.
3. Le cas échéant, si l'option de sécurité pour les données de l'utilisateur est activée, vous pouvez par l'intermédiaire du profil global afficher des cases à cocher permettant aux utilisateurs de contrôler l'affichage ou non de lignes dans l'ensemble de résultats conformément aux paramètres de filtrage qui ont été définis.
4. Cliquez sur Fermer cette fenêtre lorsque vous avez terminé d'afficher les résultats. En outre, il existe un rapport journal de processus de classification contenant le statut du processus de classification.

Affichage de la file d'attente de travaux

Avant de commencer

La file d'attente de travaux Guardium est disponible uniquement à partir du portail d'administration.

Procédure

Pour afficher le rapport, ouvrez le panneau File d'attente de travaux Guardium en accédant à Reconnaître > Classifications > File d'attente de travaux Guardium.

Gestion des politiques de classification

Procédure

Ouvrez le panneau Générateur de politique de classification en accédant à Reconnaître > Classifications > Générateur de politique de classification.
Rubrique parent : Classification

Création d'une politique de classification

Procédure

1. Cliquez sur Nouveau pour ouvrir le panneau Définition de politique de classification.
2. Entrez un nom unique dans le champ Nom.
3. Entrez une catégorie dans le champ Catégorie et une classification dans le champ Classification. Ces deux champs sont obligatoires. Ils sont tous les deux utilisés pour regrouper et organiser des données dans les rapports.
4. Entrez une description (facultatif).
5. Vous pouvez éventuellement entrer des commentaires. Vous pouvez le faire à tout moment, une fois la politique sauvegardée. Consultez Commentaires.
6. Cliquez sur Editer les règles pour définir des règles et les actions qui leur sont associées. Pour obtenir des instructions détaillées, voir la rubrique Définition de règles de politique de classification. Il est recommandé d'utiliser le scénario de reconnaissance des données sensibles (Reconnaître > Scénario de bout en bout > Reconnaissance des données sensibles) pour modifier des politiques de classification existantes. Utilisez le même scénario de reconnaissances des données sensibles pour créer des groupes de politiques de classification. De plus, si des groupes ont été créés, ils doivent être sélectionnés de manière explicite.

Modification d'une politique de classification

Procédure

1. Sélectionnez la politique de classification à modifier, puis procédez de l'une des façons suivantes :
   - Pour modifier des règles de politique, cliquez sur Editer les règles et reportez-vous à la rubrique Définition de règles de politique de classification.
   - Pour modifier n'importe quel autre élément de la définition, cliquez sur le bouton Modifier.
2. Modifiez (par écrasement) les éléments appropriés.
3. Cliquez sur Sauvegarder pour sauvegarder vos modifications, puis cliquez sur Terminé lorsque vous avez terminé.

Clonage d'une politique de classification

Procédure

1. Sélectionnez la politique de classification à cloner, puis cliquez sur le bouton Cloner.
2. Modifiez (par écrasement) les éléments appropriés pour la politique clonée. Nous vous recommandons de remplacer le nom par défaut du clone. Il s'agit du nom de la politique sélectionnée précédé de Copie de.
3. Cliquez sur le bouton Sauvegarder le clone pour sauvegarder la nouvelle politique de classification. La politique réapparaîtra dans le panneau Définition de politique de classification.
4. Pour savoir comment modifier les composants de la nouvelle définition de politique de classification, voir la rubrique Modification d'une politique de classification.

Gestion des règles de classification

Procédure

1. Ouvrez la boîte de dialogue Règles de politique de classification à partir du panneau Localiseur de politique de classification en accédant à Reconnaître > Classifications > Générateur de politique de classification.
2. Il est recommandé d'utiliser le scénario de reconnaissance des données sensibles (Reconnaître > Scénario de bout en bout > Reconnaissance des données sensibles) pour modifier des politiques de classification existantes. Utilisez le même scénario de reconnaissance des données sensible pour créer des groupes de politiques de classification. De plus, si des groupes ont été créés, ils doivent être sélectionnés de manière explicite.

Rubrique parent : Classification

Ajout d'une nouvelle règle de politique de classification

Procédure

1. Cliquez sur le bouton Ajouter une règle pour ouvrir le panneau Définition de règle de classification.
2. Entrez un nom de règle.
3. Vous pouvez éventuellement entrer une nouvelle catégorie et/ou classification pour la règle. Les valeurs par défaut sont tirées de la définition de politique de classification pour la politique.
4. Si la règle suivante dans la politique de classification doit être évaluée après la mise en correspondance de cette règle, cochez la case Continuer en cas de correspondance. Par défaut, l'évaluation des règles cesse dès lors qu'une règle est mise en correspondance.
5. Sélectionnez un type de règle. Pour une nouvelle règle, aucun type de règle n'est sélectionné. Dès lors qu'un type de règle est sélectionné, le panneau se développe pour inclure les zones nécessaires pour définir ce type de règle. Pour obtenir des instructions spécifiques à la définition de chaque type de règle, consultez l'une des sections suivantes :
   - Définition d'une règle de recherche dans un catalogue. Permet de rechercher un nom de table ou de colonne dans le catalogue de base de données.
   - Définition d'une recherche de règle dans des données. Permet de faire correspondre des valeurs ou des modèles spécifiques dans les données. Remarque : L'authentification vis-à-vis de la base de données (utilisateur/mot de passe) définie dans la définition de source de données utilisée doit disposer de droits d'accès appropriés pour la règle/recherche définie. Par exemple, dans Oracle, un utilisateur disposant du rôle approprié (par exemple, SYSTEM ou DBA) peut rechercher un droit d'accès dans le catalogue de base de données. Cette remarque s'applique à la case à cocher Table système lors de l'utilisation de l'option Rechercher le type de règle de données. Ne cochez pas la case Table système si l'utilisateur ne possède pas le rôle SYSTEM.
   - Définition d'une recherche de règle de données non structurées. Permet de faire correspondre des valeurs ou des modèles spécifiques dans un fichier de données non structurées (CSV, Text, HTTP, HTTPS, Samba).
6. Cliquez sur le bouton Nouvelle action pour ajouter une action à exécuter lorsque cette règle est mise en correspondance. Voir la rubrique sur l'ajout d'une action de règle de classification.
7. Cliquez sur Accepter pour ajouter la règle à la politique.

Définition d'une règle de recherche dans un catalogue

Pourquoi et quand exécuter cette tâche

Une règle de recherche dans un catalogue recherche dans le catalogue de base de données les noms de table et/ou de colonne correspondant à des modèles spécifiés. Les caractères génériques sont autorisés : % pour zéro à n'importe quel nombre de caractères, ou _ (trait de soulignement) pour un seul caractère.

Procédure

1. Sur la ligne Type de table, marquez au moins un type de table à rechercher : Synonyme, Table ou Vue. (Table est le type sélectionné par défaut.)
2. Vous pouvez éventuellement entrer un nom spécifique ou un modèle générique dans la zone Nom de table comme. Si ce champ est omis, tous les noms de table seront sélectionnés.
3. Vous pouvez éventuellement entrer un nom spécifique ou un modèle générique dans la zone Nom de colonne comme. Si ce champ est omis, tous les noms de colonne seront sélectionnés.
4. Cliquez sur le bouton Accepter lorsque vous avez terminé.

Définition d'une recherche de règle dans des données

Pourquoi et quand exécuter cette tâche

Une recherche de règle dans des données recherche des valeurs de données spécifiques dans une ou plusieurs colonnes. Les caractères génériques sont autorisés : % pour zéro à n'importe quel nombre de caractères, ou _ (trait de soulignement) pour un seul caractère. Par exemple, la zone Type de règle contient Recherche de données, la zone Type de table contient Table et la zone Nom de table comme contient CREDIT%.

Procédure

1. Sur la ligne Type de table, marquez au moins un type de table à rechercher : Synonyme, Table ou Vue. (Table est le type sélectionné par défaut.)
2. Sur la ligne Nom de table comme, vous pouvez éventuellement entrer un nom spécifique ou un modèle générique. Si ce champ est omis, tous les noms de table seront sélectionnés.
3. Sur la ligne Type de données, sélectionnez un ou plusieurs types de données à rechercher.
4. Sur la ligne Nom de colonne comme, vous pouvez éventuellement entrer un nom spécifique ou un modèle générique. Si ce champ est omis, tous les noms de colonne seront sélectionnés.
5. Vous pouvez éventuellement entrer une longueur minimale. Si ce champ est omis, il n'y a aucune limite.
6. Vous pouvez éventuellement entrer une longueur maximale. Si ce champ est omis, il n'y a aucune limite.
7. Dans le champ Recherche avec la clause LIKE, vous pouvez éventuellement entrer une valeur spécifique ou un modèle générique. Si ce champ est omis, toutes les valeurs seront sélectionnées.
8. Dans le champ Expression de recherche, vous pouvez éventuellement entrer une expression régulière afin de définir le modèle pour la correspondance. Pour tester une expression régulière, cliquez sur le bouton Expression régulière afin d'ouvrir le panneau Générer une expression régulière dans une fenêtre distincte. Pour des informations détaillées sur l'utilisation d'expressions régulières, consultez Expressions régulières.
9. Dans le champ Nom d'évaluation, vous pouvez éventuellement entrer un nom de classe Java™ qualifié complet qui a été créé et téléchargé. Cette classe Java sera ensuite utilisée pour déclencher et évaluer la chaîne. Il n'y a aucune validation visant à vérifier que le nom de classe saisi a été chargé et qu'il est conforme à l'interface. Pour plus d'informations sur la création et le téléchargement de fichiers de classe Java, voir la rubrique sur la personnalisation de l'évaluation et la gestion des classes personnalisées.
10. Vous pouvez éventuellement entrer un nom dans la zone Marqueur "Déclencher uniquement avec". Voir la rubrique sur le champ Marqueur "Déclencher uniquement avec".
11. Dans le champ Pourcentage de correspondances, vous pouvez éventuellement entrer un pourcentage de données correspondantes à atteindre pour que cette règle se déclenche. Des données sont renvoyées si le pourcentage de données correspondantes examinées est supérieur ou égal (>=) à la valeur de pourcentage saisie, indiquant ainsi qu'une entrée vide signifie qu'il ne s'agit pas d'une condition et que cela n'affectera pas le déclenchement ou non de la règle et le renvoi des données sur l'écran. Un pourcentage égal à 0 provoque le déclenchement de la règle pour cette condition et le renvoi des données sur l'écran, et un pourcentage égal à 100 indique que toutes les règles doivent correspondre.
12. Dans le champ Comparer aux valeurs dans le code SQL, vous pouvez éventuellement entrer une instruction SQL. Cette instruction SQL, qui doit être basée sur le renvoi d'informations à partir d'une seule et même colonne, sera ensuite utilisée comme groupe de valeurs pour la recherche dans les tables et/ou les colonnes sélectionnées. S'il est utilisé, le champ Comparer aux valeurs dans le code SQL doit être conforme aux règles suivantes :
    - L'instruction SQL doit commencer par SELECT.
    - L'instruction SQL ne DOIT PAS utiliser le point-virgule (;).
    - L'instruction SQL saisie DOIT spécifier un nom de valeur de schéma afin de renvoyer des résultats précis.
    - Exemples conformes :

      ```
      SELECT ename FROM scott.emp
      select EMPNUMBER from SYSTEM.EMP where EMPNUMBER in(5555,4444)
      select DNAME from SCOTT.DEPT where DNAME like 'A%G'
      SELECT ZIP from SCOTT.FOO where ZIP in (SELECT ZIP FROM SCOTT.FOO)
      ```

13. Dans le champ Comparer aux valeurs dans le groupe, vous pouvez éventuellement sélectionner un groupe. Le groupe ainsi sélectionné est ensuite utilisé comme groupe de valeurs pour la recherche dans les tables et/ou les colonnes sélectionnées. Dès lors que l'une des valeurs d'un groupe, qu'il s'agisse d'un groupe public ou d'un groupe de classificateur, est mise en correspondance, la règle de valeur renvoie des données.
14. Cochez la case Afficher les valeurs uniques pour ajouter à la zone de commentaires des détails concernant les valeurs qui ont été mises en correspondance avec les règles de politique de classification et déclenchées. Utilisez les expressions régulières du champ Masque de valeur unique pour expurger les valeurs uniques. Par exemple, cochez la case Afficher les valeurs uniques et utilisez ([0-9]{2}-[0-9]{3})-[0-9]{4} dans le champ Masque de valeur unique pour consigner les quatre derniers chiffres et expurger les chiffres qui composant le préfixe.

Définition d'une recherche de règle de données non structurées

Pourquoi et quand exécuter cette tâche

Une recherche de règle de données non structurées examine un fichier autre qu'un fichier de base de données.

Procédure

1. Dans le champ Recherche avec la clause LIKE, vous pouvez éventuellement entrer une valeur spécifique ou un modèle générique. Si ce champ est omis, toutes les valeurs seront sélectionnées.
2. Dans le champ Expression de recherche, vous pouvez éventuellement entrer une expression régulière afin de définir le modèle pour la correspondance. Pour tester une expression régulière, cliquez sur l'icône RE pour ouvrir le panneau Générer une expression régulière dans une fenêtre distincte. Pour des informations détaillées sur l'utilisation d'expressions régulières, consultez Expressions régulières.
3. Vous pouvez éventuellement entrer un nom de repère.

Gestion des actions de règle de classification

Procédure

1. Après avoir sauvegardé une règle, cliquez sur le bouton Personnaliser pour cette règle afin de revenir au panneau définition de règles à partir duquel vous pouvez ajouter une ou plusieurs actions de règle.
2. Cliquez sur le bouton Nouvelle action pour ouvrir le panneau Action.
3. Entrez un nom d'action.
4. Entrez une description (facultatif).
5. Sélectionnez un type d'action dans la liste. Le jeu de zones qui apparaît sur le panneau varie en fonction de l'action que vous avez sélectionnée.
    - Pour les actions Ignorer et Consigner le résultat, aucune autre information n'est requise.
        - Ignorer - Ne pas consigner la correspondance ni exécuter aucune action supplémentaire.
        - Consigner le résultat - Consigner la correspondance et exécuter aucune action supplémentaire.
    - Pour toutes les autres actions, davantage de zones apparaîtront sur le panneau et vous devrez entrer des informations supplémentaires.
        - Action Ajouter à un groupe d'objets/de champs
        - Action Ajouter à un groupe d'objets
        - Action Créer une règle d'accès
        - Action Créer un jeu de confidentialité
        - Action Consigner une violation de politique
        - Action Envoyer une alerte
6. Une fois que des actions ont été ajoutées dans le panneau Classification Rule, les contrôles de la table peuvent être utilisés pour modifier les actions définies.
7. Cliquez sur Accepter lorsque vous avez terminé de gérer la définition de règles.

Rubrique parent : Classification

Action Ajouter à un groupe d'objets/de champs

Pourquoi et quand exécuter cette tâche

Chaque fois que la règle de classification est mise en correspondance, un membre est ajouté au groupe Groupe objet-champ sélectionné sur le système Guardium. Vous avez la possibilité de remplacer tous les membres ou d'en ajouter de nouveaux.

Pour un fichier de base de données, le composant d'objet du membre sera le nom de la table de base de données et le composant de zone sera le nom de la colonne.

Pour un fichier de données non structurées, le composant d'objet du membre sera le nom du fichier (entre guillemets) et le composant de zone sera le nom de la colonne, mais si les noms de colonne ne peuvent pas être déterminés, les colonnes seront nommées column1, column2, etc.

Procédure

1. Effectuez l'une des actions suivantes :
    - Sélectionnez un groupe Groupe objet-champ dans la liste, ou
    - cliquez sur le bouton Groupes, définissez un nouveau groupe à l'aide de l'outil Générateur de groupe, puis sélectionnez ce groupe dans la liste.
2. Vous pouvez éventuellement cocher la zone Remplacer le contenu de groupe pour remplacer complètement l'appartenance du groupe sélectionné par les membres renvoyés par cette règle. Par défaut, cette case n'est pas cochée, ce qui signifie que de nouveaux membres seront ajoutés au groupe, mais qu'aucun membre ne sera supprimé. Pour un travail qui s'exécute à la demande, cette case est ignorée et vous avez la possibilité d'ajouter ou de remplacer des membres sur le panneau d'affichage des résultats.
3. Cliquez sur le bouton Sauvegarder pour ajouter l'action à la définition de règles, fermez le panneau Action et revenez au panneau de définition de règles.

Action Ajouter à un groupe d'objets

Pourquoi et quand exécuter cette tâche

Chaque fois que la règle de classification est mise en correspondance, un membre est ajouté au groupe Objet sélectionné sur le système Guardium.

Pour un fichier de base de données, le nom du membre sera le nom de la table de base de données. Pour un type de fichier non structuré, le nom du membre sera le nom du fichier.

Vous avez la possibilité de remplacer toutes les entrées ou d'en ajouter de nouvelles.

Procédure

1. Effectuez l'une des actions suivantes :
    - Sélectionnez un groupe Objet dans la liste, ou
    - cliquez sur le bouton Groupes, définissez un nouveau groupe à l'aide de l'outil Générateur de groupe, puis sélectionnez ce groupe dans la liste. Remarque : Pour utiliser des alias avec des groupes générés à partir du classificateur, ouvrez l'outil Générateur de groupe, sélectionnez le groupe Objet généré par le classificateur, puis cliquez sur Modifier. Cliquez sur le bouton Alias dans le bouton Groupe pour modifier le nom du groupe Objet.
2. Vous pouvez éventuellement cocher la zone Remplacer le contenu de groupe pour remplacer complètement l'appartenance du groupe sélectionné par les membres renvoyés par cette règle. Par défaut, cette case n'est pas cochée, ce qui signifie que de nouveaux membres seront ajoutés au groupe, mais qu'aucun membre ne sera supprimé. Pour un travail qui s'exécute à la demande, cette case est ignorée et vous avez la possibilité d'ajouter ou de remplacer des membres sur le panneau d'affichage des résultats.
3. Dans Contenu réel du membre, sélectionnez la convention d'attribution de nom qui sera utilisée pour ajouter le membre au groupe où l'option 'Complète' correspond à schema.tablename et l'option 'Nom' correspond à tablename.
4. Cliquez sur Sauvegarder pour ajouter l'action à la définition de règles, fermez le panneau Action et revenez au panneau de définition de règles.

Action Créer une règle d'accès

Pourquoi et quand exécuter cette tâche

Chaque fois que la règle de classification est mise en correspondance, une règle d'accès est insérée dans une définition de politique de sécurité existante. La politique de sécurité mise à jour ne sera pas installée (cette tâche est effectuée séparément, généralement par un administrateur Guardium).

Procédure

1. Sélectionnez une politique d'accès dans la liste. Vous devez être autorisé à accéder à cette politique.
2. Entrez un nom de règle dans la zone Description de règle.
3. Sélectionnez une action dans la liste Action de règle d'accès.
4. Vous pouvez éventuellement sélectionner un groupe Commandes ou cliquer sur le bouton Groupes, définir un nouveau groupe Commandes à l'aide de l'outil Générateur de groupe, puis sélectionner ce groupe Commandes dans la liste.
5. Pour consigner des valeurs de champ séparément, cochez la case Inclure le champ. Sinon, seule la table sera enregistrée (par défaut).
6. Pour inclure l'adresse IP de serveur, cochez la case Inclure IP serveur.
7. Si vous avez sélectionné une action d'alerte, une ligne Récepteur apparaît sur le panneau et vous devez ajouter au moins un récepteur pour l'alerte. Cliquez sur Modifier les récepteurs pour ajouter un ou plusieurs récepteurs.
8. Cliquez sur Accepter pour ajouter l'action à la définition de règles, fermez le panneau Action et revenez au panneau de définition de règles.

Action Créer un jeu de confidentialité

Pourquoi et quand exécuter cette tâche

Chaque fois que la règle de classification est mise en correspondance, la liste Objet-champ d'un jeu de confidentialité est remplacée.

Pour un fichier de base de données, le composant d'objet du jeu de confidentialité sera le nom de la table de base de données et le composant de zone sera le nom de la colonne.

Pour un fichier de données non structurées, le composant d'objet du jeu de confidentialité sera le nom du fichier (entre guillemets) et le composant de zone sera le nom de la colonne, mais si les noms de colonne ne peuvent pas être déterminés, les colonnes seront nommées column1, column2, etc.

Procédure

1. Sélectionnez le jeu de confidentialité précédemment défini dont vous souhaitez remplacer le contenu.
2. Cliquez sur le bouton Accepter pour ajouter l'action à la définition de règles, fermez le panneau Action et revenez au panneau de définition de règles.

Action Consigner une violation de politique

Pourquoi et quand exécuter cette tâche

Chaque fois que la règle de classification est mise en correspondance, une violation de politique est consignée. Cela signifie que les violations de politique de classification seront consignées (et pourront être signalées) en même temps que les violations de politique d'accès (et éventuellement les alertes de corrélation) qui pourront avoir été générées.

Procédure

1. Sélectionnez un code de gravité dans la liste.
2. Cliquez sur le bouton Accepter pour ajouter l'action à la définition de règles, fermez le panneau Action et revenez au panneau de définition de règles.

Action Envoyer une alerte

Pourquoi et quand exécuter cette tâche

Cliquez sur le bouton Accepter pour ajouter l'action à la définition de règles, fermez le panneau Action et revenez au panneau de définition de règles.

Procédure

1. Sélectionnez un type de notification dans la liste.
2. Cliquez sur le bouton Modifier les récepteurs pour ajouter un ou plusieurs récepteurs. Le récepteur spécifié recevra un e-mail par source de données par règle par action. Par conséquent, si une source de données comporte trois règles et chaque règle comporte deux actions (pour lesquelles il existe au moins une correspondance), l'utilisateur recevra 2 * 3 = 6 e-mails.
3. Cliquez sur le bouton Accepter pour ajouter l'action à la définition de règles, fermez le panneau Action et revenez au panneau de définition de règles.

Reconnaissance des données sensibles

Créez un scénario de bout en bout pour reconnaître et classifier des données sensibles.

Pourquoi et quand exécuter cette tâche

L'importance des processus de reconnaissance et de classification grandit à mesure que la taille d'une organisation augmente et que des données sensibles, telles que des numéros de carte de crédit et des données financières personnelles, se propagent à différents emplacements. Cela se produit souvent dans le contexte de fusions et d'acquisitions, ou lorsque des systèmes existants ont survécu à leurs propriétaires initiaux. Par conséquent, des données sensibles peuvent exister sans que la personne qui les possède ne le sache. Il s'agit d'un scénario courant, mais néanmoins extrêmement vulnérable, dans la mesure où vous ne pouvez protéger des données sensibles que si vous savez qu'elles existent.

Les scénarios de reconnaissance des données sensibles couvrent trois aspects critiques de la sécurité d'entreprise :

- Reconnaissance : recherche des données sensibles partout dans votre environnement
- Protection : surveillance et alerte en cas d'accès à des données sensibles
- Mise en conformité : création de traces d'audit pour passer en revue les résultats des processus de reconnaissance des données sensibles

Le générateur de scénario de bout en bout Reconnaissance des données sensibles rationalise les processus de reconnaissance, de protection et de mise en conformité en intégrant plusieurs outils Guardium dans une seule interface conviviale.

Tableau 1. Mappe des outils de reconnaissance de données sensibles

Valeur	Tâche de scénario	Description	Résultat

Valeur	Tâche de scénario	Description	Résultat
Reconnaître	Nom et description	Indiquez un nom et une description pour le scénario et les processus et politiques qui lui sont associés.	Un processus de classification et une politique de classification sont créés. De nouvelles définitions de source de données sont éventuellement créées.
	Elément à reconnaître	Créez des règles et des actions de règle pour la reconnaissance et la classification des données.	
	Où rechercher	Identifiez les sources de données à analyser.	
	Exécuter la reconnaissance	Exécutez le scénario, vérifiez les résultats et définissez les actions d'alerte et de regroupement ad hoc.	
Protection	Rapport de révision		Une politique d'accès est créée.
Conformité	Audit	Définissez les récepteurs, une séquence de distribution et passez en revue les options.	Un processus d'audit est créé.
	Planification	Créez une planification qui sera exécutée à intervalles définis.	

Cette série de tâches vous guide à travers les processus de création d'un nouveau scénario de reconnaissance. Cela inclut de créer des *politiques de classification* constituées de règles et d'actions de règle pour la reconnaissance des données sensibles, de créer des *processus de classification* en identifiant les sources de données à examiner pour rechercher des données sensibles, de définir des politiques ad hoc (pour le regroupement et l'alerte, par exemple) et de créer des *processus d'audit* qui distribuent les résultats aux différentes parties prenantes à intervalles définis.

Si un scénario de reconnaissance des données sensibles crée des politiques et des processus sous-jacents accessibles à l'aide d'autres outils Guardium (par exemple, le panneau Générateur de politique de classification ou des commandes GuardAPI), il n'existe aucune commande GuardAPI permettant de créer ou modifier un scénario de reconnaissance.

1. Scénarios de reconnaissance
   Créez un nouveau scénario de reconnaissance ou sélectionnez un scénario de reconnaissance existant à copier ou éditer.
2. Nom et description
   Indiquez un nom et une description pour votre scénario de reconnaissance.
3. Elément à détecter
   Créez des politiques constituées de règles et d'actions de règle pour la reconnaissance et la classification des données sensibles.
4. Où rechercher
   Identifiez les sources de données à examiner dans le cadre de la recherche de données sensibles.
5. Exécution du processus de reconnaissance et révision de rapport
   Vous pouvez éventuellement exécuter votre scénario de reconnaissance et examiner les résultats.
6. Effectuer un audit
   Vous pouvez éventuellement créer un processus d'audit en définissant des récepteurs, une séquence de distribution, puis examiner les options relatives au rapport de reconnaissance et de classification.
7. Planification
   Vous pouvez éventuellement activer le processus d'audit en planifiant son exécution à des intervalles définis.

Que faire ensuite

Passez à la section suivante et indiquez un nom et une description pour votre scénario de reconnaissance et de classification.
Rubrique parent : Reconnaissance

Scénarios de reconnaissance

Créez un nouveau scénario de reconnaissance ou sélectionnez un scénario de reconnaissance existant à copier ou éditer.

Procédure

1. Accédez à Reconnaître > Scénarios de bout en bout > Reconnaissance des données sensibles.
2. Créez, copiez ou éditez un scénario de reconnaissance.
   - Cliquez sur l'icône pour créer un nouveau scénario.
   - Cliquez sur l'icône pour copier un scénario ou un modèle existant.
   - Cliquez sur un nom de scénario existant dans la liste Scénarios de reconnaissance pour commencer à éditer ce scénario.

   Certains scénarios ou modèles de reconnaissance sont fournis par défaut, notamment les suivants :

   GDPR [modèle]
   : Le scénario GDPR [modèle] fournit l'ensemble de règles de reconnaissance et le support de langue les plus récents pour votre stratégie de conformité GDPR. Les modèles peuvent être copiés ou édités et sauvegardés sous un autre nom, et le scénario GDPR [modèle] recevra toujours les règles de reconnaissance et le support de langue GDPR les plus récents.

   GDPR
   : Le scénario GDPR fournit un ensemble de base de règles de reconnaissance pouvant être utilisées dans le cadre d'une stratégie de conformité GDPR. Vous pouvez éditer et sauvegarder des modifications dans le scénario GDPR, mais celui-ci ne recevra jamais les règles ou le support de langue mis à jour au fil du temps.
     Avertissement : Si le scénario GDPR [modèle] est disponible, l'utilisation de l'ancien scénario GDPR n'est pas recommandée car il ne reçoit pas les mises à jour.

Rubrique parent : Reconnaissance des données sensibles
Rubrique suivante : Nom et description

Nom et description

Indiquez un nom et une description pour votre scénario de reconnaissance.

Pourquoi et quand exécuter cette tâche

Le nom fourni pour le scénario de reconnaissance sera également utilisé pour nommer les politiques et processus sous-jacents.

Au cours de cette étape, vous pouvez également spécifier des *rôles de sécurité* qui peuvent accéder au scénario de reconnaissance.

Procédure

1. Ouvrez la section Nom et description et indiquez ou éditez le nom et une description facultative du scénario. Le nom que vous indiquez ici sera également utilisé pour nommer les processus et politiques de classification sous-jacents créés par le scénario de reconnaissance.
   Exemple : Un scénario de reconnaissance nommé "Find PCI" va créer un *processus de classification* nommé "Find PCI" et une *politique de classification* nommée "Find PCI Classification Policy" (suivis d'une date et d'un horodatage).
2. Indiquez les libellés de catégorie et de classification pour le balisage des violations. "Sensitive" est la valeur par défaut pour les libellés de catégorie et de classification.
3. Cliquez éventuellement sur le bouton Rôles pour spécifier des *rôles de sécurité* pouvant accéder au scénario de reconnaissance.

Que faire ensuite

Passez à la section suivante du scénario de reconnaissance, intitulée Elément à détecter.
Rubrique parent : Reconnaissance des données sensibles
Rubrique précédente : Scénarios de reconnaissance
Rubrique suivante : Elément à détecter

Elément à détecter

Créez des politiques constituées de règles et d'actions de règle pour la reconnaissance et la classification des données sensibles.

Pourquoi et quand exécuter cette tâche

Les *politiques de classification* contiennent un ensemble ordonné de règles et d'actions de règle qui identifient et exécutent des actions sur des données sensibles. Chaque règle d'une politique définit une action conditionnelle qui doit être exécutée lorsqu'une correspondance est trouvée pour la règle. Le test conditionnel peut être simple, par exemple, une chaîne générique trouvée n'importe où dans la table, ou un test complexe qui prend en compte plusieurs conditions. Pour les scénarios de reconnaissance des données sensibles, l'action déclenchée par une règle peut être une action de regroupement qui ajoute l'objet à un groupe spécifié ou une action d'alerte qui déclenche une notification lorsqu'une correspondance est trouvée pour les règles. Il est possible de combiner et d'ordonner plusieurs actions de regroupement et d'alerte afin de créer des réponses sophistiquées à des règles pour lesquelles une correspondance est trouvée.

Cette tâche vous guide à travers les processus de création et d'édition de règles de classification et d'actions de règle pour votre scénario de reconnaissance.

Procédure

1. Ouvrez la section Elément à détecter pour définir des règles de reconnaissance de données.
2. Utilisez le menu Langue pour filtrer des modèles de règle en fonction de la langue sélectionnée et des pays où elle est parlée. Des modèles pour certains motifs universels tels que numéros de carte de crédit et adresses e-mail sont affichés pour toutes les sélections du menu Langue.
3. Ajoutez des règles à votre scénario de reconnaissance en procédant de l'une des façons suivantes :
   - Cliquez sur l'icône pour créer une nouvelle règle.
   - Sélectionnez des règles dans la table Modèles de règle de classification, puis cliquez sur l'icône pour ajouter des règles prédéfinies.
4. Définissez une nouvelle règle ou éditez un modèle de règle en sélectionnant celui-ci et en cliquant sur l'icône .
   a. Sélectionnez un type de règle en fonction du type de recherche effectué.
      - Recherche de données, permet de faire correspondre des valeurs ou des modèles spécifiques dans les données.
      - Recherche dans le catalogue, permet de faire correspondre des noms de table ou de colonne dans le catalogue de base de données.
      - Recherche de données non structurées, permet de faire correspondre des valeurs ou des modèles spécifiques dans un fichier de données non structurées, par exemple, CSV, TXT ou CEF.
   b. Indiquez un nom et une description lorsque vous spécifiez un *test de modèle spécial* (facultatif) au début du champ Nom. Le nom de règle sera également utilisé pour nommer la règle associée à la politique de classification dans le panneau Générateur de politique de classification. Si vous avez besoin d'un test de modèle spécial, il est recommandé de gérer le modèle qui lui correspond (par exemple, utilisez Carte bancaire - Numéro de carte de crédit pour les numéros de carte de crédit).
   c. Ouvrez la section Critères de règle afin de définir une *expression régulière* et d'autres critères de recherche pour la règle. Si vous gérez un modèle de règle, une *expression régulière* appropriée est fournie par défaut.
      Avertissement : Pour les règles créées dans le scénario de reconnaissance des données sensibles, le champ Type de données renseigné par défaut contient à la fois les valeurs Nombre et Texte.
   d. Ouvrez la section Actions et définissez les *actions de règle* à exécuter lorsque des correspondances sont trouvées pour des règles.
   e. Lorsque vous définissez plusieurs *actions de règle*, vous pouvez éventuellement cliquer sur l'icône et utiliser les icônes et pour changer l'ordre dans lequel les actions sont exécutées.
   f. Cliquez sur Sauvegarder lorsque vous avez terminé d'ajouter ou d'éditer des définitions de règle afin de revenir à la section Elément à détecter du scénario de reconnaissance.
5. Vous pouvez éventuellement cliquer sur l'icône et utiliser les icônes et pour modifier l'ordre dans lequel les règles sont appliquées. L'ordre des règles est important, car, par défaut, l'exécution des règles cesse après la première correspondance trouvée, sauf si l'option Continuer en cas de correspondance est sélectionnée sous Critères de règle.
6. Lorsque vous avez terminé de gérer les règles, cliquez sur Suivant pour passer à la section suivante du scénario de reconnaissance.

Que faire ensuite

Passez à la section suivante du scénario de reconnaissance, intitulée Où rechercher.
Rubrique parent : Reconnaissance des données sensibles

Rubrique précédente : Nom et description
Rubrique suivante : Où rechercher
Concepts associés:
Expressions régulières
Tâches associées:
Gestion des actions de règle de classification
Référence associée:
Contenu réel du membre
Critères de règle
Tests de modèle spéciaux

Critères de règle

Tableau 1.

Attribut	Description
Type de table	Sélectionnez un ou plusieurs types de table pour la recherche : Synonyme, Table ou Vue. Le type Table est sélectionné par défaut.
Type de données	Sélectionnez un ou plusieurs types de données pour la recherche : Nombre, Texte ou Date. Les types Nombre et Texte sont sélectionnés par défaut.
Expression de recherche	Vous pouvez éventuellement entrer une expression régulière afin de définir un modèle de recherche pour la correspondance. Pour tester une expression régulière, cliquez sur le bouton ER pour ouvrir l'éditeur d'expression régulière.
Nom de table comme	Vous pouvez éventuellement entrer un nom spécifique ou un modèle générique. Si cette zone est omise, tous les noms de table sont sélectionnés.
Nom de colonne comme	Vous pouvez éventuellement entrer un nom spécifique ou un modèle générique. Si cette zone est omise, tous les noms de colonne sont sélectionnés.
Continuer en cas de correspondance	Si la règle suivante dans la politique de classification doit être évaluée après la mise en correspondance de cette règle, cochez la case Continuer en cas de correspondance. Par défaut, l'évaluation des règles cesse dès lors qu'une règle est mise en correspondance.
Caractère générique de recherche	Vous pouvez éventuellement entrer une valeur spécifique ou un modèle générique. Si cette zone est omise, toutes les valeurs sont sélectionnées.
Longueur minimale	Vous pouvez éventuellement entrer une longueur minimale. Si cette zone est omise, il n'y a aucune limite.
Longueur maximale	Vous pouvez éventuellement entrer une longueur maximale. Si cette zone est omise, il n'y a aucune limite.
Nom d'évaluation	Vous pouvez éventuellement entrer un nom de classe Java™ qualifié complet qui a été créé et téléchargé. Cette classe Java sera ensuite utilisée pour déclencher et évaluer la chaîne. Remarque : Il n'y a aucune validation visant à vérifier que le nom de classe saisi a été chargé et qu'il est conforme à l'interface.
Marqueur "Déclencher uniquement avec"	Le marqueur "Déclencher uniquement avec" permet de regrouper des règles de classification. Les règles ayant le même repère sont déclenchées en même temps. De plus, toutes les règles renvoyées à l'aide d'un repère doivent renvoyer des données sur la base du même nom de table. Si deux règles, ou plus, sont définies avec le même repère, elles se déclenchent en même temps, de telle sorte que si ces deux règles sont déclenchées sur la même table, elles sont toutes les deux consignées et leurs actions appelées. En revanche, si une seule de ces deux règles se déclenche sur une table, aucune d'elles n'est consignée et aucune de leurs actions n'est appelée. Le déclenchement de plusieurs règles en même temps est indispensable si vous voulez que vos données sensibles apparaissent conjointement dans la même table. Par exemple, vous souhaiterez peut-être être averti lorsqu'une table comporte à la fois un numéro de sécurité sociale et un permis de conduire du Massachusetts. Le marqueur "Déclencher uniquement avec" correspond à une valeur constante, quelle qu'elle soit, qui doit être rigoureusement identique dans toutes les règles que vous souhaitez regrouper. Cela signifie que si une règle comporte un repère ABC, l'autre règle avec laquelle vous souhaitez la regrouper doit également comporter un repère ABC. Le marqueur "Déclencher uniquement avec" interagit également avec l'indicateur Continue on Match. Par exemple, si les règles suivantes ont été définies de telle manière que la règle 3 ne corresponde pas au paramètre Continuer en cas de correspondance, aucun résultat n'est renvoyé sauf si les trois règles de repère étaient positives. Cela est dû au fait que vous n'avez pas eu l'occasion d'exécuter la règle 4 et que le regroupement ne se déclenchera pas car tous les marqueurs "Déclencher uniquement avec" doivent s'exécuter avec des résultats positifs. Règle 1. Règle "ABC" avec repère de déclenchement (continuer en cas de correspondance) Règle 2. Règle "ABC" avec repère de déclenchement (continuer en cas de correspondance) Règle 3. Type de règle sans repère de déclenchement (continuer en cas de correspondance) Règle 4. Règle "ABC" avec repère de déclenchement (continuer en cas de correspondance)
Pourcentage de correspondances	Vous pouvez éventuellement entrer un pourcentage de données correspondantes à atteindre pour que cette règle se déclenche. Des données sont renvoyées si le pourcentage de données correspondantes examinées est supérieur ou égal (>=) à la valeur de pourcentage saisie, indiquant ainsi qu'une entrée vide signifie qu'il ne s'agit pas d'une condition et que cela n'affectera pas le déclenchement ou non de la règle et le renvoi des données sur l'écran. Un pourcentage égal à 0 entraîne le déclenchement de la règle pour cette condition et le renvoi des données sur l'écran. Un pourcentage égal à 100 indique que toutes les règles doivent correspondre.

Attribut	Description

Comparer aux valeurs dans le code SQL	Vous pouvez éventuellement entrer une instruction SQL. Cette instruction SQL, qui doit être basée sur le renvoi d'informations à partir d'une seule et même colonne, sera ensuite utilisée comme groupe de valeurs pour la recherche dans les tables et les colonnes sélectionnées.
	Remarque : Si elle utilisée, le champ Comparer aux valeurs dans le code SQL doit être conforme aux règles suivantes :
	• L'instruction SQL doit commencer par `SELECT`.
	• L'instruction SQL ne DOIT PAS utiliser le point-virgule (`;`).
	• L'instruction SQL saisie DOIT spécifier un nom de valeur de schéma afin de renvoyer des résultats précis.
	• Exemples conformes :
	`SELECT ename FROM scott.emp`
	`select EMPNUMBER from SYSTEM.EMP where EMPNUMBER in(5555,4444)`
	`select DNAME from SCOTT.DEPT where DNAME like 'A%G'`
	`SELECT ZIP from SCOTT.FOO where ZIP in (SELECT ZIP FROM SCOTT.FOO)`

Comparer aux valeurs dans le groupe	Vous pouvez également sélectionner un groupe. Le groupe ainsi sélectionné est ensuite utilisé comme groupe de valeurs pour la recherche dans les tables et les colonnes sélectionnées. Dès lors que l'une des valeurs d'un groupe, qu'il s'agisse d'un groupe public ou d'un groupe de classificateur, est mise en correspondance, la règle de valeur renvoie des données.
Afficher les valeurs uniques	Cochez la case Afficher les valeurs uniques pour ajouter au champ de commentaires du rapport obtenu des détails concernant les valeurs qui ont été mises en correspondance avec les règles de politique de classification.
Masque de valeur unique	Utilisez les expressions régulières du champ Masque de valeur unique pour expurger les valeurs uniques. Par exemple, cochez la case Afficher les valeurs uniques et utilisez `([0-9]{2}-[0-9]{3})-[0-9]{4}` dans le champ Masque de valeur unique pour consigner les quatre derniers chiffres et expurger les chiffres qui composant le préfixe.

Rubrique parent : Elément à détecter

Contenu réel du membre

Utilisez le champ Contenu réel du membre pour définir la façon dont les objets sont libellées par l'action de règle Ajouter au groupe d'objets.

Tableau 1.

Sélection Contenu réel du membre	Valeur du groupe
Nom d'objet uniquement	tableName
Like Name%	tableName%
Like %Name	%tableName
Like %Name%	%tableName%
%/%.Name	%%.tableName
Nom qualifié complet	schemaName.tableName
Like Full%	schemaName.tableName%
Like %Full	%schemaName.tableName
Like %Full%	%schemaName.tableName%
%/Full	%%.schemaName.tableName
Read/%.Name	Read/%.tableName
Change/%.Name	Change/%.tableName
Lecture globale	Read/schemaName.tableName
Changement global	Change/schemaName.tableName

Si vos règles renvoient le nom de table `JJ_CREDIT_CARD` depuis le schéma `DB2INST1` et que vous avez spécifié une action Ajouter au groupe d'objets, les sélections Contenu réel du membre se comportent comme suit :

- La sélection de Nom qualifié complet permet d'ajouter `DB2INST1.JJ_CREDIT_CARD` au groupe sélectionné.
- La sélection de Nom d'objet uniquement permet d'ajouter `JJ_CREDIT_CARD` au groupe sélectionné.
- La sélection de Changement global permet d'ajouter `Change/DB2INST1.JJ_CREDIT_CARD` au groupe sélectionné.

Rubrique parent : Elément à détecter

Où rechercher

Identifiez les sources de données à examiner dans le cadre de la recherche de données sensibles.

Pourquoi et quand exécuter cette tâche

Les sources de données stockent des informations sur votre base de données ou référentiel, comme le type de base de données, l'emplacement du référentiel ou les données d'authentification qui peuvent lui être associées. L'ajout de sources de données à un scénario de reconnaissance entraîne la création d'un *processus de classification* dans lequel des *politiques de classification* sont appliquées aux sources de données sélectionnées.

Dans le cadre de cette tâche, vous allez identifier les sources de données dans lesquelles vous souhaitez rechercher des données sensibles.

Procédure

1. Ouvrez la section Où rechercher pour identifier les sources de données dans lesquelles vous souhaitez rechercher des données sensibles.

2. Ajoutez des sources de données à votre scénario de reconnaissance en procédant de l'une des façons suivantes :
   - Cliquez sur l'icône pour ouvrir la boîte de dialogue Créer une source de données et ajoutez une nouvelle définition de source de données.
   - Sélectionnez des sources de données dans le tableau Sources de données disponibles et cliquez sur l'icône pour ajouter des sources de données existantes.
3. Définissez une nouvelle source de données ou éditez une source de données existante en sélectionnant cette dernière, puis en cliquant l'icône . Les nouvelles sources de données définies via le scénario de reconnaissance peuvent également être affichées ou éditées via l'outil Définitions de source de données.
   a. Entrez ou éditez le nom de la source de données.
   b. Sélectionnez le type de base de données approprié dans le menu Type de base de données et indiquez les informations demandées pour terminer la définition de source de données. Les zones disponibles varient en fonction du type de base de données sélectionné.
   c. Lorsque vous avez terminé d'éditer la définition de source de données, cliquez sur Sauvegarder pour sauvegarder votre travail et cliquez éventuellement sur Tester la connexion pour vérifier la connexion à la source de données.
   d. Lorsque vous avez terminé de gérer la définition de source de données, cliquez sur Fermer pour fermer la boîte de dialogue.
4. Si vous utilisez également ce processus de classification pour des bases de données cloud, sélectionnez Activer l'audit d'objet pour les bases de données sur le cloud.
5. Lorsque vous avez terminé d'ajouter des sources de données, cliquez sur Suivant pour passer à la section suivante du scénario de reconnaissance.

Résultats

Un *processus de classification* est créé après que des sources de données ont été ajoutées à votre scénario de reconnaissance et que celui-ci a été sauvegardé. Pour afficher ou éditer ce processus directement, utilisez le panneau Générateur de processus de classification.

Que faire ensuite

Passez à la section suivante du flux de travaux de reconnaissance, intitulée Exécuter la reconnaissance.
Rubrique parent : Reconnaissance des données sensibles
Rubrique précédente : Elément à détecter
Rubrique suivante : Exécution du processus de reconnaissance et révision de rapport
Concepts associés:
Sources de données
Tâches associées:
Création d'une définition de source de données

Exécution du processus de reconnaissance et révision de rapport

Vous pouvez éventuellement exécuter votre scénario de reconnaissance et examiner les résultats.

Pourquoi et quand exécuter cette tâche

Après avoir défini des politiques de reconnaissance de données sensibles et identifié les sources de données à rechercher, vous pouvez exécuter le *processus de classification* et examiner les résultats. L'exécution du processus et l'examen des résultats vous permettent d'affiner vos politiques, par exemple, en spécifiant des critères de recherche supplémentaires si vous trouvez que les résultats sont trop vastes. Il peut s'avérer nécessaire de passer par plusieurs itérations d'affinement de politiques, d'exécution du processus et d'évaluation des résultats avant d'obtenir les résultats souhaités.

Procédure

1. Ouvrez la section Exécuter la reconnaissance pour tester votre scénario de reconnaissance.
2. Cliquez sur Exécuter maintenant pour commencer.
   Avertissement :
   - Selon les politiques que vous avez spécifiées et le nombre de sources de données que vous avez sélectionnées pour la recherche, le processus d'identification des données sensibles peut durer plusieurs minutes ou plus. Le statut du processus apparaît en regard du bouton Exécuter maintenant, ou vous pouvez surveiller le processus à l'aide de File d'attente de travaux Guardium.
   - Vous pouvez aussi exécuter le *processus de classification* en accédant au panneau Générateur de processus de classification, en sélectionnant votre *processus de classification* et en cliquant sur Exécuter une fois maintenant.
3. Lorsque l'exécution du scénario de reconnaissance est terminée, ouvrez la section Rapport de révision pour voir les résultats.
4. Tout en examinant les résultats, vous pouvez définir d'autres règles et actions en fonction de ces résultats. Utilisez le filtre pour affiner les résultats (le filtrage n'est pas pris en charge avec plus de 10 000 résultats).
   a. Sélectionnez la ou les ligne(s) contenant des données contre lesquelles vous souhaitez définir des actions.
   b. Cliquez sur Ajouter au groupe pour définir une action de regroupement ou cliquez sur Actions avancées pour définir d'autres actions, comme Alerter, Consigner ou Ignorer.
   c. Une fois que vous avez renseigné la boîte de dialogue pour définir une action, cliquez sur OK pour revenir au rapport de résultats.
      Avertissement :
      - Les actions ajoutées à partir du tableau de résultats sont considérées comme des actions ad hoc qui ne sont exécutées que lorsqu'elles sont appelées à partir du tableau de résultats. Ces actions n'apparaissent pas dans la section Elément à détecter > Editer la règle > Actions de votre scénario de reconnaissance, et elles ne seront pas exécutées automatiquement dans le cadre du scénario de reconnaissance ou des *processus de classification* connexes.
      - Utilisez la fenêtre Générateur de politique pour examiner, éditer, et installer des actions d'alerte et des règles d'accès.
      - Utilisez la fenêtre Générateur de groupe pour examiner et éditer des actions de regroupement.
      - Utilisez la fenêtre Générateur de jeux de confidentialité pour examiner les actions de révision de jeu de confidentialité.
      - Utilisez l'outil Gestion des incidents pour examiner les actions de consignation de politique.
5. Lorsque vous avez terminé d'examiner le rapport de résultats, cliquez sur Suivant pour passer à la section suivante du scénario de reconnaissance.

Résultats

Après avoir exécuté la recherche de données sensibles, surveillez son statut en regard du bouton Exécuter maintenant ou en utilisant File d'attente de travaux Guardium. Vous pouvez utiliser le panneau Générateur de groupe pour examiner n'importe quelle action de regroupement ou le panneau Générateur de politique pour examiner et installer n'importe laquelle des actions d'alerte qui ont été ajoutées à partir du tableau de résultats.

Que faire ensuite

Passez éventuellement à la section suivante du scénario de reconnaissance, intitulée Effectuer l'audit.
Rubrique parent : Reconnaissance des données sensibles
Rubrique précédente : Où rechercher
Rubrique suivante : Effectuer un audit

Effectuer un audit

Vous pouvez éventuellement créer un processus d'audit en définissant des récepteurs, une séquence de distribution, puis examiner les options relatives au rapport de reconnaissance et de classification.

Pourquoi et quand exécuter cette tâche

Vous pouvez définir n'importe quel nombre de récepteurs pour les résultats d'un flux de travaux de reconnaissance et vous pouvez contrôler l'ordre de réception de ces résultats par ces récepteurs. De plus, vous pouvez spécifier des options de contrôle de processus, par exemple, si un récepteur doit valider les résultats pour que ceux-ci puissent être envoyés au récepteur suivant.

Le *processus d'audit* créé en ajoutant des récepteurs au scénario de reconnaissance hérite du nom de celui-ci. Par exemple, si des récepteurs sont ajoutés à un scénario de reconnaissance nommé "Find PCI", un *processus d'audit* nommé "Find PCI Audit process" et suivi d'une date et d'un horodatage est créé.

Procédure

1. Ouvrez la section Effectuer un audit dans le but de définir des récepteurs pour les rapports de reconnaissance.
2. Ajoutez des récepteurs à votre scénario de reconnaissance n cliquant sur l'icône  et en définissant des options relatives à la distribution des rapports.
   - Si vous envoyez le rapport à des utilisateurs, rôles ou groupes Guardium, vous devrez définir des options de contrôle de processus.
   - Si vous envoyez le rapport à des récepteurs d'e-mail, indiquez leur adresse e-mail et filtrez le rapport en indiquant un nom d'utilisateur Guardium approprié pour le récepteur d'e-mail.
3. Cliquez sur OK pour ajouter le récepteur au flux de travaux de reconnaissance. Continuez d'ajouter des récepteurs au scénario si nécessaire.
4. Vous pouvez éventuellement cliquer sur l'icône  et utiliser les icônes  et  pour modifier l'ordre dans lequel les rapports sont distribués aux récepteurs. Cette action est importante lorsque vous utilisez une distribution *séquentielle* car cela permet d'identifier les récepteurs qui doivent examiner ou signer le rapport avant l'envoi de celui-ci aux récepteurs suivants.
5. Lorsque vous avez terminé d'ajouter, d'éditer et de réorganiser les récepteurs, cliquez sur Nouveau pour passer à la section suivante du scénario de reconnaissance.

Résultats

Un *processus d'audit* est créé une fois que des récepteurs sont définis et que le scénario de reconnaissance est sauvegardé. Pour afficher, éditer ou exécuter ce processus directement, utilisez le panneau Générateur de processus d'audit.

Le *processus d'audit* demeure inactif jusqu'à ce qu'il soit planifié à l'aide de la section Planification du scénario de reconnaissance ou du panneau Générateur de processus d'audit. Vous pouvez également exécuter le *processus d'audit* en accédant au panneau Générateur de processus d'audit, en sélectionnant le *processus d'audit*, puis en cliquant sur Exécuter une fois maintenant.

Que faire ensuite

Vous pouvez éventuellement passer à la section suivante du flux de travaux de reconnaissance, intitulée Planification.
Rubrique parent : Reconnaissance des données sensibles
Rubrique précédente : Exécution du processus de reconnaissance et révision de rapport
Rubrique suivante : Planification
Concepts associés:
Construction de processus d'audit

Planification

Vous pouvez éventuellement activer le processus d'audit en planifiant son exécution à des intervalles définis.

Pourquoi et quand exécuter cette tâche

Une planification devient partie intégrante d'un *processus d'audit* de même que les récepteurs spécifiés dans la section Effectuer l'audit du scénario de reconnaissance. Le fait de définir une planification permet d'exécuter le *processus d'audit* à des intervalles spécifiés et de s'assurer que les résultats du *processus de classification* associé sont régulièrement distribués et examinés.

Procédure

1. Ouvrez la section Planification pour définir une planification de reconnaissance de données.
2. Utilisez le menu Planification par afin de définir des intervalles quotidiens ou mensuels pour le *processus d'audit*.
3. Utilisez les cases à cocher Démarrer la planification à et Répéter toutes les pour définir le nombre de fois par jour et le nombre de fois par heure que le *processus d'audit* doit être exécuté.
4. Utilisez la case à cocher Date et heure de début pour planifier explicitement une date et une heure de début.
5. Désélectionnez la case Activer la planification pour désactiver le *processus d'audit* tout en conservant les informations de planification afin de les utiliser ultérieurement. La case Activer la planification est cochée par défaut, ce qui signifie que le processus d'audit devient actif après la sauvegarde de la planification.
6. Une fois que vous avez défini une planification, cliquez sur Sauvegarder pour terminer l'édition, puis fermez l'éditeur de flux de travaux.

Résultats

Un *processus d'audit* est créé une fois qu'une planification est définie et que le scénario de reconnaissance est sauvegardé. Pour afficher ou éditer ce processus d'audit directement, utilisez le panneau Générateur de processus d'audit. Examinez le rapport Travaux planifiés pour voir le statut, l'heure de début et l'heure de déclenchement suivante des tâches d'audit planifiées.

Rubrique parent : Reconnaissance des données sensibles
Rubrique précédente : Effectuer un audit
Concepts associés:
Construction de processus d'audit

Expressions régulières

Des expressions régulières peuvent être utilisées pour rechercher sur le trafic des modèles complexes dans les données.

L'implémentation par IBM Guardium d'expressions régulières est conforme à POSIX 1003.2. Pour plus d'informations, voir le site Web Open Group : www.opengroup.org. Des expressions régulières peuvent être utilisées pour rechercher sur le trafic des modèles complexes dans les données. Voir les exemples dans la rubrique sur les politiques.

Cette rubrique d'aide fournit des instructions relatives à l'utilisation de l'outil Build Regular Expression, ainsi que plusieurs tableaux de caractères spéciaux et constructions couramment utilisés. Elle ne décrit pas de façon détaillée la construction ou l'utilisation des expressions régulières. Pour plus d'informations détaillées, voir le site Web Open Group.

Ce qu'il faut retenir au sujet de la mise en correspondance de modèle ou de la mise en correspondance XML à l'aide d'expressions régulières est que la recherche d'une correspondance commence au début d'une chaîne et s'arrête lorsque la première séquence correspondant à l'expression est trouvée. Des expressions régulières différentes ou identiques peuvent être utilisées en même temps pour la mise en correspondance de modèle et la mise en correspondance XML.

Remarque : IBM Guardium ne prend pas en charge les expressions régulières pour les langues autres que l'anglais.

Utilisation de l'outil Build Regular Expression

Lorsqu'une zone d'entrée requiert une expression régulière, vous pouvez utiliser l'outil Build Regular Expression pour coder et tester une expression régulière. L'icône Générer une expression régulière est située dans le Générateur de politique, sous Ajouter une règle.

Pour ouvrir l'outil Build Regular Expression, cliquez sur l'icône RE en regard de la zone qui contiendra l'expression régulière. Si vous avez déjà saisi des informations dans la zone, elles seront copiées dans la zone Expression régulière du panneau Générer une expression régulière.

1. Sélectionnez une catégorie d'expressions régulières dans la liste déroulante.
2. Sélectionnez un modèle dans la liste déroulante.
3. Entrez ou modifiez l'expression dans la zone Expression régulière.
4. Pour tester l'expression, entrez un texte dans la zone Texte dans lequel rechercher des correspondances, puis cliquez sur le bouton Tester :
   - Si l'expression contient une erreur (une accolade fermante manquante, par exemple), vous en serez informé par un message Erreur de syntaxe.
   - Le message Correspondance trouvée indique que votre expression régulière a trouvé une correspondance dans le texte que vous avez saisi.
   - Si aucune correspondance n'est trouvée, le message `Aucune correspondance trouvée` s'affiche.
5. Nous vous recommandons de répéter l'étape un certain nombre de fois pour vérifier que votre expression régulière correspond et ne correspond pas, selon vos attentes.
6. Pour entrer un caractère spécial à la fin de votre expression, vous pouvez la sélectionner dans la liste de sélection d'éléments. Pour entrer un caractère spécial n'importe où ailleurs, vous devez la saisir ou la copier à cet endroit précis
7. Lorsque vous avez terminé d'effectuer des modifications et des tests, cliquez sur Accepter pour fermer le panneau Générer une expression régulière et copiez l'expression régulière dans le panneau de définition.

Caractères spéciaux et constructions

Le tableau suivant contient un récapitulatif des caractères spéciaux et des constructions les plus couramment utilisés.

Tableau 1. Caractères spéciaux et constructions

Caractère	Comment faire pour...	Exemple	Correspondances	Pas de correspondance
littéral	Faire correspondre une séquence exacte de caractères (sensibles à la casse), sauf pour les caractères spéciaux décrits ci-dessous	can	can	Can cab caN
. (dot)	Faire correspondre n'importe quel caractère, y compris des caractères de retour chariot ou de retour à la ligne (\n)	ca.	can cab	c cb
*	Faire correspondre zéro ou davantage d'instances du ou des caractère(s) précédent(s)	Ca*n	Cn Can Caan	Cb Cabn
^	Faire correspondre une chaîne commençant par le(s) caractère(s) suivant(s)	^C.	Ca	ca a
$	Faire correspondre une chaîne se terminant par le(s) caractère(s) précédent(s)	C.n$	Can Cn	Cab
+	Faire correspondre une ou davantage d'instances du ou des caractère(s) précédent(s)	^Ca+n	Can Caan	Cn
?	Faire correspondre zéro ou une instance du ou des caractère(s) précédent(s)	Ca?n	Cn Can	Caan
|	Faire correspondre le modèle précédent ou suivant	Can|cab	Can cab	Cab
(x ...)	Faire correspondre la séquence placée entre parenthèses	(Ca)*n	Can XaCan	Cn CCnn
{n}	Faire correspondre exactement n instances du ou des caractère(s) précédent(s)	Ca{3}n	Caaan	Caan Caaaan

Caractère	Comment faire pour...	Exemple	Correspondances	Pas de correspondance
{n,}	Faire correspondre n ou davantage d'instances du ou des caractère(s) précédent(s)	Ca{2,}n	Caan Caaaan	Can Cn
{n,m}	Faire correspondre n à m instances du ou des caractère(s) précédent(s)	Ca{2,3}n	Caan Caaan	Can Caaaan
[a-ce]	Faire correspondre un seul caractère du jeu de caractères, où le tiret indique une séquence contiguë ; par exemple, [0-9] correspond à n'importe quel chiffre	[C-FL]an	Can Dan Lan	Ban
[^a-ce]	Faire correspondre n'importe quel caractère qui ne figure PAS dans le jeu de caractères spécifié	[^C-FL]an	aan Ban	Can Dan
[[.char.]]	Faire correspondre le caractère délimité ou le caractère nommé issu du tableau de caractères nommés	[[.~.]]an ou [[.tilde.]]an	~an	@an
[[:class:]]	Faire correspondre n'importe quel caractère de la classe de caractères spécifiée issue du tableau de classes de caractères	[[:alpha:]]+	abc	ab3

Tableau de caractères nommés (anglais)

Le tableau suivant décrit les noms de caractère standard qui peuvent être utilisés dans des paires de crochets d'expression régulière ([[.char]]). Les noms de caractère sont spécifiques aux emplacements, par conséquent, les versions non anglaises de Guardium peuvent utiliser un autre jeu de noms de caractères.

- NUL \0
- SOH \001
- STX \002
- ETX \003
- EOT \004
- ENQ \005
- ACK \006
- BEL \007
- alert \007
- BS \010
- Espacement arrière \b
- HT \011
- Onglet \t
- LF \012
- Retour à la ligne \n
- VT \013
- Onglet vertical \v
- FF \014
- Alimentation papier \f
- CR \015
- Retour chariot \r
- SO \016
- SI \017
- DLE \020
- DC1 \021
- DC2 \022
- DC3 \023
- DC4 \024
- NAK \025
- SYN \026
- ETB \027
- CAN \030
- EM \031
- SUB \032
- ESC \033
- IS4 \034
- FS \034
- IS3 \035
- GS \035
- IS2 \036
- RS \036
- IS1 \037
- US \037
- Espace ' '
- Point d'exclamation !
- Guillemet "
- Signe dièse #
- Symbole du dollar $
- Symbole du pourcentage %
- Perluète &
- Apostrophe \'
- Parenthèse gauche (
- Parenthèse droite)
- Astérisque *
- Signe plus +

- Virgule ,
- Trait d'union -
- Point .
- Point .
- Barre oblique /
- Barre oblique /
- Zéro 0
- Un 1
- Deux 2
- Trois 3
- Quatre 4
- Cinq 5
- Six 6
- Sept 7
- Huit 8
- Neuf 9
- Deux-points :
- Point-virgule ;
- Signe inférieur à <
- Signe égal à =
- Signe supérieur à >
- Point d'interrogation ?
- Signe arobas @
- Crochet gauche [
- Crochet droit]
- Barre oblique inversée \
- Barres obliques inverses \\
- Circonflexe ^
- Accent circonflexe ^
- Trait de soulignement _
- Ligne inférieure _
- Accent grave `
- Accolade gauche {
- Bracket gauche {
- Accolade droite }
- Bracket droit
- Ligne verticale |
- Tilde ~
- DEL 177
- NULL 0

Tableau de classes de caractères nommés (anglais)

Le tableau suivant décrit les classes de caractères standard qui peuvent être utilisées dans des paires de crochets d'expression régulière ([[:class]]). Notez que les classes de caractères sont spécifiques aux emplacements, par conséquent, les versions non anglaises de Guardium peuvent utiliser un autre jeu de noms de caractères.

- alnum - Alphanumérique (a-z, A-Z, 0-9)
- alpha - Alphabétique (a-z, A-Z)
- blank - Blanc (blanc, saut de ligne, retour chariot)
- cntrl - Contrôle
- digit - 0-9
- graph - Graphique
- lower - Alphabétique minuscule (a-z)
- print - Caractères imprimables
- punct - Caractères de ponctuation
- space - Espace, tabulation, retour à la ligne et retour chariot
- upper - Alphabétique majuscule
- xdigit - Caractère hexadécimal (0-9, a-f)

Exemples d'expression régulière

Vous pouvez copier et coller n'importe lesquelles des expressions dans une zone qui nécessite une expression régulière. Lorsque vous utilisez n'importe lequel de ces exemples, nous vous recommandons fortement de l'expérimenter en l'utilisant dans l'outil Générer une expression régulière, en saisissant une variété de valeurs correspondantes et non correspondantes, de manière à comprendre exactement ce qui est mis en correspondance par l'expression.

Exemples d'expression régulière

Numéro de sécurité sociale (doit comporter des traits d'union) [0-9]{3}-[0-9]{2}-[0-9]{4}

Numéro de téléphone (numéro de téléphone - correspond à 3334445555, 333.444.5555, 333-444-5555, 333 444 5555, (333) 444 5555, et à toutes les combinaisons qui en résultent) \(?[0-9]{3}\)?[-.]?[0-9]{3}[-.]?[0-9]{4}

Code postal - (Canada) [ABCEGHJKLMNPRSTVXY][0-9][A-Z] [0-9][A-Z][0-9]

Code postal - (UK) [A-Z]{1,2}[0-9][A-Z0-9]? [0-9][ABD-HJLNP-UW-Z]{2}

Code postal (US) (5 chiffres requis, trait d'union suivi de quatre chiffres (facultatif)) [0-9]{5}(?:-[0-9]{4})?

Numéros de carte de crédit [0-9]{4}[-,]?[0-9]{4}[-,]?[0-9]{4}[-,]?[0-9]{4}

Rubrique parent : Reconnaissance

Reconnaissance et classification de données sensibles dans des serveurs de fichiers

La surveillance de l'activité des fichiers garantit l'intégrité et la protection des données sensibles sur les serveurs de fichiers UNIX et Windows.

- Installation et activation des composants de surveillance de l'activité des fichiers
  Installez le client GIM sur le serveur de fichiers, puis utilisez-le pour installer l'agent S-TAP et l'agent de reconnaissance FAM.
- Paramètres GIM pour la reconnaissance et la classification de fichiers
  Utilisez ces paramètres GIM afin de configurer la reconnaissance et la classification de fichiers pour chaque collecteur.
- Personnalisation des plans de décision FAM
  Les plans de décision sont utilisés pour identifier un contenu sensible dans des fichiers. L'agent de reconnaissance FAM Guardium fournit des plans de décision par défaut pour HIPAA, PCI, SOX et le code source. Vous pouvez modifier les entités de classification dans le tableau de bord de rapports obtenus/d'investigation à l'aide des plans de décision. Vous pouvez également créer de nouveaux plans ou modifier des plans existants à l'aide d'IBM Content Classifier Workbench.

Rubrique parent : Reconnaissance
Information associée:
Surveillance de l'activité des fichiers avec Guardium (vidéo)

Installation et activation des composants de surveillance de l'activité des fichiers

Installez le client GIM sur le serveur de fichiers, puis utilisez-le pour installer l'agent S-TAP et l'agent de reconnaissance FAM.

Avant de commencer

- Des clés de licence doivent être installées. Consultez Installation des clés de licence :
- L'agent S-TAP doit être installé. Requis pour la surveillance des fichiers et l'application des politiques.
- L'agent de reconnaissance FAM (également appelé bundle FAM ou agent FAM) doit être accessible. Requis pour la reconnaissance et la classification des fichiers.

Conseil : Pour installer l'agent de reconnaissance FAM sous AIX, il est recommandé de définir une taille illimitée pour les données de processus en modifiant les lignes suivantes dans le fichier /etc/security/limits : default: data = -1

Pourquoi et quand exécuter cette tâche

Procédure

1. Installez le client GIM sur le serveur de fichiers. Voir Guardium Installation Manager.
2. Téléchargez les bundles S-TAP et FAM et sauvegardez-les sur une unité accessible. Choisissez le module approprié pour le système d'exploitation de votre serveur de fichiers. Le nom du bundle UNIX est similaire au nom suivant : guard-bundle-FAM_r*****_trunk_*****.gim. Le nom du bundle Windows est similaire au nom suivant : guard-FAM-guardium_r*****Windows-Server-x86_x64_ia64.gim.
3. Sur le gestionnaire central, le cas échéant, à défaut, sur un dispositif, téléchargez et importez le module S-TAP et le bundle FAM :
   a. Accédez à Gérer > Installation de module > Téléchargement des modules.
   b. Sous Télécharger un module, cliquez sur Parcourir, puis accédez au bundle S-TAP et sélectionnez-le. Cliquez sur Télécharger.
   c. Cliquez sur Parcourir et accédez au bundle FAM. Cliquez sur Télécharger.
   d. Sous Importer les modules téléchargés, sélectionnez l'agent S-TAP et le bundle FAM, puis cliquez sur Installer/Mettre à jour.
4. Installez le module S-TAP :
   a. Installez le module S-TAP sur le serveur de fichiers. Suivez le trajet Gérer > Installation de module > Configuration par client (Legacy). Pour voir tous les clients enregistrés, cliquez sur Rechercher.
   b. Sélectionnez votre serveur de fichiers, ou vos serveurs, puis cliquez sur Suivant. Il n'existe aucun paramètre S-TAP spécifique pour les composants FAM.
   c. Cliquez sur Appliquer à la sélection, puis sur Installer/Mettre à jour. Vous pouvez effectuer l'installation maintenant ou planifier son exécution ultérieurement.
   d. Assurez-vous que le module S-TAP a été correctement installé en consultant le rapport Guardium, le moniteur d'état S-TAP (ajout du rapport à partir de l'application Mes tableaux de bord). Recherchez l'hôte S-TAP doté du suffixe :FAM.
5. Installez et configurez le bundle FAM :
   a. Suivez le trajet Gérer > Installation de module > Configuration par client (Legacy). Pour voir tous les clients enregistrés, cliquez sur Rechercher.
   b. Sélectionnez votre serveur de fichiers, puis cliquez sur Suivant.
   c. Choisissez le module FAM que vous avez téléchargé. (Pour Windows, vous devrez peut-être désélectionner la case Afficher uniquement les bundles.)
   d. Remarque : Vous pouvez aussi configurer les paramètres GIM à l'aide de la commande grdapi : gim_update_client_params.
   Configurez les paramètres pour l'agent de reconnaissance FAM, y compris SOURCE_DIRECTORIES pour les répertoires que vous souhaitez examiner. Par défaut, l'agent ne fera qu'une analyse de base pour les informations d'autorisation d'utilisation. Pour activer l'analyse en fonction de plans de décision, tels que SOX ou HIPAA, vous devez affecter la valeur true à FAM_IS DEEP_ANALYSIS. L'agent utilise implicitement tous les plans de décision par défaut. Vous pouvez spécifier les plans de décision que vous souhaiter le voir utiliser. Par défaut, l'analyse est planifiée pour s'exécuter toutes les 12 heures et pour commencer à l'issue de la configuration. Vous pouvez modifier cela à l'aide des paramètres GIM FAM_SCHEDULER_HOUR_TIME_INTERVAL, FAM_SCHEDULER_START et FAM_SCHEDULER_REPEAT. Voir la liste complète de paramètres dans Paramètres GIM pour la reconnaissance et la classification de fichiers.
   e. Cliquez sur Appliquer à la sélection, puis sur Installer/Mettre à jour. Vous pouvez effectuer l'installation maintenant ou planifier son exécution ultérieurement.
6. Assurez-vous que l'agent de reconnaissance FAM a été correctement installé en consultant le rapport Guardium, le moniteur d'état S-TAP (ajout du rapport à partir de l'application Mes tableaux de bord). Recherchez le suffixe FAM_Agent dans l'adresse IP de l'hôte S-TAP.
7. Pour déclencher une nouvelle reconnaissance de fichiers ultérieurement sans avoir à désinstaller, puis à réinstaller le bundle FAM :
   a. Retirez les fichiers sous le répertoire de travail. Si Guardium est installé dans le répertoire par défaut, les fichiers à retirer se trouvent dans le répertoire suivant sur le serveur de fichiers : /usr/local/IBM/modules/FAM/current/files/work
   b. Modifiez les paramètres FAM dans GIM, par exemple, en faisant passer l'intervalle de temps de 5 à 10.
   c. Cliquez sur Appliquer à la sélection, puis sur Installer/Mettre à jour.

Résultats

Résultats du processus de reconnaissance et de classification : lorsque l'installation de l'agent de reconnaissance FAM (moteur d'exploration des fichiers) est terminée, une exécution de base du moteur d'exploration des fichiers commence en utilisant le chemin initial que vous avez spécifié lors de l'installation. Chaque fois que le moteur

d'exploration termine une exécution, il envoie un message de statut qui est inclus dans le rapport Configuration du moteur d'exploration de fichiers. Ce processus collecte la liste de dossiers et de fichiers, leur propriétaire, les droits d'accès, la taille et la date et l'heure de la dernière mise à jour.

Rubrique parent : Reconnaissance et classification de données sensibles dans des serveurs de fichiers
Information associée:
Fonctions de surveillance de l'activité des fichiers dans GuardAPI
Fonctions de surveillance de l'activité des fichiers dans GuardAPI

Paramètres GIM pour la reconnaissance et la classification de fichiers

Utilisez ces paramètres GIM afin de configurer la reconnaissance et la classification de fichiers pour chaque collecteur.

Configurez une reconnaissance et une classification de fichiers par collecteur. Ces paramètres peuvent être configurés lors de l'installation, ou ultérieurement avec GIM (Gérer > Installation de module > Configuration par client) ou à l'aide de la commande GuardAPI gim_update_client_params. Vous ne pouvez mettre à jour qu'un collecteur à la fois lorsque vous utilisez la commande GuardAPI.

Paramètre GIM	Description	Interface graphique	gr dapi
FAM_CLASSIFICATION_LANGUAGES	Interne. Par défaut, le paramètre FAM_CLASSIFICATION_LANGUAGES a pour valeur Anglais. Affectez la valeur GenericLanguage à ce paramètre pour configurer une détection de langue automatique. Pour Linux, assurez-vous que le support de langue requis est installé sur votre serveur Linux. Par exemple, pour assurer la prise en charge de la classification de documents en chinois, le support de la langue chinoise doit être installé sous Linux. Pour plus d'informations sur les langues prises en charge pour IBM Content Classification, voir http://www-01.ibm.com/support/knowledgecenter/SSBRAM_8.8.0/com.ibm.classify.workbench.doc/c_WBG_available_languages.htm%23wp9000332?lang=en	X	
FAM_DEBUG	0=OFF (désactivé) 1=ON (activé) Les journaux du serveur de fichiers sont collectés et envoyés au dispositif Guardium.	X	
FAM_ENABLED	0 = L'agent de reconnaissance FAM est désactivé 1 = L'agent de reconnaissance FAM est activé Par défaut 2 = Redémarrer l'agent de reconnaissance FAM Dans les installations GIM, à compter de la v10.1.4, la valeur par défaut est "Désactivé". Dans les installations S-TAP shell, la valeur par défaut est "Activé". Mettez à 2 le paramètre FAM_ENABLED dans l'interface graphique GIM et appliquez cette modification aux clients en cliquant sur Installer/Mettre à jour. **Unix :** l'ID de processus du service FAM dans le serveur de fichiers doit changer pour indiquer qu'il a été redémarré (ps -ef | grep fam), et une nouvelle entrée est générée dans le rapport d'interface graphique prédéfini intitulé "Configuration du moteur d'exploration de fichiers". La valeur 1 est rétablie dans la configuration dans l'interface graphique GIM pour vous permettre de redémarrer à nouveau en répétant le processus. **Windows :** le service FAM redémarre, comme illustré dans l'afficheur d'événements (Journaux Windows > Système `Le service FAM d'IBM Guardium est passé à l'état Arrêté` et `Le service FAM d'IBM Guardium est passé à l'état En cours`). **Aucune** nouvelle entrée n'est générée dans le rapport d'interface graphique prédéfini intitulé "Configuration du moteur d'exploration de fichiers" et la valeur 2 est conservée dans la configuration dans l'interface graphique GIM. Pour le redémarrage suivant, changez le paramètre à 1.	X	

Paramètre GIM	Description	Interface graphique	grdapi
FAM_ICM_CLASS_DECISION_PLANS	Activez les plans de décision en incluant leurs noms et leurs entités de classification. DecisionPlanName1{Entity1.1,Entity1.2,..}:DecisionPlanName2{Entity2.1,Entity2.2,..} Définissez une liste de plans de décision délimités par des point-virgule et des listes d'entités pour chaque plan de décision. Format : Entités indiquées entre des accolades et délimitées par des deux-points. Lorsque le contenu entre accolades est vide ou manquant pour certains plans de décision, toutes les entités de classification sont présentées dans les résultats de classification, dans le rapport FAM/tableau de bord d'investigation. Exemples de contenu entre accolades vide/manquant : DecisionPlanName1{}:DecisionPlanName2{} DecisionPlanName1:DecisionPlanName2"~		
FAM_ICM_CLASS_THREAD_COUNT	Nombre d'unités d'exécution à utiliser par le classificateur. La valeur par défaut, également recommandée, est 5.	X	
FAM_ICM_URL	L'URL du serveur IBM Content Classification Server. La valeur par défaut est http://localhost:18087	X	
FAM_INSTALLER	Windows uniquement. Chemin d'accès au package du programme d'installation.		
FAM_INSTALL_DIR	Windows uniquement. Emplacement où est installé le logiciel FAM (surveillance de l'activité des fichiers).		
FAM_IS_DEEP_ANALYSIS	Valeur False : la classification est désactivée. Examen de base de métadonnées et droits d'accès uniquement. Valeur True : la classification est activée en fonction du contenu de fichier. Si aucun plan de décision n'est activé (le paramètre FAM_ICM_CLASS_DECISION_PLANS n'est pas défini), seul un examen de base est effectué.	X	
FAM_SCAN_EXCLUDE_DIRECTORIES	Répertoires à exclure du processus de reconnaissance et de classification. Les caractères génériques ne sont pas pris en charge. Format : Chemin d'accès complet au répertoire.	X	
FAM_SCAN_EXCLUDE_REMOTE_DIRECTORIES	True/false. La valeur par défaut est true. Pour examiner des répertoires distants, indiquez la valeur false. Répertoires distants à exclure du processus de reconnaissance et de classification. Les caractères génériques ne sont pas pris en charge. Sous Windows, définissez une valeur semblable à la suivante : \\\\RemoteMachine\sharefolder\directoryA	X	
FAM_SCAN_EXCLUDE_EXTENSIONS	Exclut la ou les extension(s) de fichier spécifiée(s) ou les documents sans extensions de l'examen FAM. S'applique à Windows et à Linux. Format : Liste délimitée par des point-virgule. Le paramètre est sensible à la casse. Exemples d'extensions exclues : pdf;txt;doc. Pour exclure les documents sans extension, spécifiez "NO_EXTENSION".	X	
FAM_SCAN_EXCLUDE_FILES	Fichiers à exclure du processus de reconnaissance et de classification. Format : Nom de fichier valide. Les caractères génériques ne sont pas pris en charge.	X	
FAM_SCAN_MAX_DEPTH	Limitez la profondeur de l'examen par rapport aux répertoire de début spécifiés (FAM_SOURCE_DIRECTORIES).	X	
FAM_SCHEDULER_HOUR_TIME_INTERVAL	Fréquence horaire de l'exécution de l'examen de reconnaissance et de classification Format : Entier. La valeur par défaut est 12 heures.	X	

Paramètre GIM	Description	Interface graphique	grdapi
FAM_SCHEDULER_MINUTE_TIME_INTERVAL	Associé à l'intervalle horaire, cela représente l'intervalle de temps entre les analyses. Par exemple, si vous souhaitez que les analyses se déroulent à 12 heures et 30 minutes d'écart, spécifiez 12 pour l'heure et indiquez 30 ici pour les minutes. Format : Entier.	X	
FAM_SCHEDULER_REPEAT	Valeur True : répéter le processus de reconnaissance à intervalles définis. Valeur False : ne pas répéter l'examen.	X	
FAM_SCHEDULER_START_TIME	Heure de l'activation initiale des processus de reconnaissance et de classification. Format : MM-JJ-AAAA HH:mm Par exemple, si vous entrez 01-02-2016 18:00, l'examen débute à 18 heures le 2 janvier 2016. Pour un intervalle horaire de 12 heures, le processus est exécuté tous les jours à 18 heures et à 6 heures.	X	
FAM_SERVER_PORT	Port de collecteur Guardium, 16022.	X	
FAM_SOURCE_DIRECTORIES	Répertoire(s) à partir duquel ou desquels débute l'analyse. Les caractères génériques ne sont pas pris en charge. Exemple : /home/test. Format : Liste de répertoires source FAM délimités par des point-virgule. Exemple : %IBM_FAM_HOME%/test/dir1;%IBM_FAM_HOME%/test/dir2 ~ Utilisez FILE_SYSTEM_ROOTS pour balayer tous les fichiers du serveur. (Déconseillé, en particulier si le serveur contient de nombreux fichiers.)	X	

Rubrique parent : Reconnaissance et classification de données sensibles dans des serveurs de fichiers
Information associée:
GIM - Interface graphique
GIM - Interface de ligne de commande

Personnalisation des plans de décision FAM

Les plans de décision sont utilisés pour identifier un contenu sensible dans des fichiers. L'agent de reconnaissance FAM Guardium fournit des plans de décision par défaut pour HIPAA, PCI, SOX et le code source. Vous pouvez modifier les entités de classification dans le tableau de bord de rapports obtenus/d'investigation à l'aide des plans de décision. Vous pouvez également créer de nouveaux plans ou modifier des plans existants à l'aide d'IBM Content Classifier Workbench.

Avant de commencer

Installez IBM Content Classification 8.8 sur un poste de travail Windows qui peut être connecté à votre environnement Guardium.

Lors de l'exécution de la surveillance de l'activité des fichiers, l'utilisateur de l'installation GIM doit configurer le paramétrage du plan de décision ICM sur la page de configuration GIM de la surveillance de l'activité des fichiers.

L'utilisateur doit configurer la liste de plans de décisions (catégories) avec des entités (zones NVP) pour chaque plan de décision délimité par des deux-points.

Cette configuration est utilisée par la surveillance de l'activité des fichiers pour la classification de contenu.

Le client doit être en mesure de configurer toutes les entités possibles pour chacun des modèles de plan de décision disponibles lors de l'installation de la fonction de surveillance de l'activité des fichiers.

La classification de plan de décision apparaît uniquement lorsque le fichier est sensible et que la classification n'est pas vide.

Après l'installation de la fonction de surveillance de l'activité des fichiers, quatre modèles de plan de décision sont disponibles :

- HIPAA, PCI, SOX, Source
- Plan de décision HIPAA utilisé pour trouver des informations médicales
- PCI utilisé pour trouver des numéros de carte de crédit
- SOX utilisé pour les documents financiers

Le plan de décision "Source" fait référence à deux bases de connaissances (CodeKB et DocumentTypeKB) qui sont chargées par défaut une fois que le plan de décision source est configuré.

Voici la liste des entités possibles pour chaque plan de décision fourni prêt à l'emploi avec la surveillance de l'activité des fichiers et configurable via GIM.

HIPAA

SSN, Name, License, GovermentID, PassportContext, BankAccount, Address, IPAddress, EmailAddress, URL, Phone, CreditCard, possibleHealthPlan, Confidential_match, HIPAA_match

PCI

SSN, Name, License, GovermentID, PassportContext, BankAccount, Address, IPAddress, EmailAddress, URL, Phone, BankAccountContext, CreditCard, CreditContext, containCardIssuer, PCI_match, Confidential

SOX

SSN, Name, License, GovermentID, PassportContext, BankAccount, Address, IPAddress, EmailAddress, URL, Phone, BankAccountContext, CreditCard, CreditContext, containCardIssuer, piiMatch, Confidential, SOXContext, SOX_match

Source

containDate,hasSSN, hasBirthDate, containCardIssuer, hasCreditCard, PCIViolation, HIPAA_Match, ConfidentialMatch, Source_match

Un plan de décision est une collection de règles que vous pouvez configurer pour déterminer la façon dont IBM Classification Module classifie les objets de contenu. Les règles sont constituées de déclencheurs et d'actions. Un déclencheur détermine les conditions qui doivent être remplies pour initier une action. Une action détermine la façon dont le document doit être classifié. Un plan de décision fait également référence à une ou plusieurs bases de connaissances pour combiner une classification de règles basée sur des mots clés avec une classification de statistiques basée sur du texte.

Une base de connaissances est un ensemble de données collectées qui est utilisé pour analyser et catégoriser des objets de contenu. La base de connaissances reflète le type de données que le système s'attend à gérer. Avant que la base de connaissances puisse analyser du texte, elle doit être entraînée avec un nombre suffisant d'exemples d'objets de contenu correctement classifiés dans des catégories. Une base de connaissances entraînée peut calculer une mesure numérique de la pertinence d'un objet pour chaque catégorie.

Remarque : ICM n'est pas mesure de gérer des plans de décision avec des noms chinois. Les documents de contenu et les règles de plan de décision en chinois sont pris en charge, mais pas les noms de plan de décision en chinois.
Remarque : La distribution des plans de décision à partir du gestionnaire central sur des unités gérées n'est pas prise en charge.
Remarque : Les résultats de classification pour chaque plan de décision doivent être spécifiés par des entités correctement configurées et reconnues. La classification n'apparaît que lorsque le fichier est sensible et que la classification n'est pas vide. Pour le niveau de débogage, il existe une documentation relative aux défaillances de plan de décision et aux erreurs ICM.

Pourquoi et quand exécuter cette tâche

Pour les besoins de cette description, imaginons que votre société possède un projet confidentiel nommé "ProjectA". Vous souhaitez identifier et surveiller tous les fichiers qui contiennent cette chaîne.

Procédure

1. Utilisez le menu Démarrer de Windows pour ouvrir le plan de travail de classification IBM Content Classification 8.8.
2. Dans la boîte de dialogue Open Project, cliquez sur New....
3. Dans la boîte de dialogue New Project, choisissez Decision Plan comme type de projet. Entrez un nom pour ce plan de décision, par exemple, `ProjectA_DP`. Entrez éventuellement une description.
4. Dans la boîte de dialogue New Project Options, sélectionnez Create an empty project.
5. Dans l'explorateur de projets, cliquez sur Word and string list files. Dans la boîte de dialogue Word and string list files, cliquez sur New... pour créer un nouveau fichier. Dans la boîte de dialogue New File, choisissez Word list pour le type de fichier et choisissez un nom pour le fichier. Dans cet exemple, nous appellerons le fichier `Names`. Wordlist_Names.txt apparaît dans la liste de fichiers.
6. Cliquez deux fois sur le nom de fichier pour l'éditer. Insérez une ligne avec la chaîne `~ProjectA~` et sauvegardez le fichier.
7. Dans l'explorateur de projets, cliquez sur DecisionPlan > New Group > New Rule. Remplacez le nom de la règle par `ProjectA`.
8. Dans la boîte de dialogue New Rule, ouvrez l'onglet Trigger. Cliquez sur condition.
9. Choisissez Trigger when fields contains specific words or phrases. Choisissez Word list file. Cliquez sur OK.
10. Ouvrez l'onglet Action. Cliquez sur Add new rule.
11. Sélectionnez Advanced Actions dans la liste Action Type. Choisissez l'action Set content field. Ce champ de contenu est créé lorsque le déclencheur spécifié est mis en application. Le champ de contenu peut être consulté dans des rapports FAM.
12. Dans la boîte de dialogue Add action, entrez `ProjectA_match` comme nom de champ de contenu et tapez `found` dans le champ Value.
13. Importez le contenu dans le projet de plan de décision.
    a. Créez un document texte contenant la chaîne "ProjectA."
    b. Dans l'explorateur de projets, développez le projet ProjectA_DP. Cliquez avec le bouton droit de la souris sur Content Set et choisissez Import Content Set.
    c. Cliquez sur Files from a file system folder. Accédez au fichier que vous avez créé à l'étape a. Cliquez successivement sur Next, Next, Next et Finish.
14. Vérifiez que votre définition a abouti.
    a. Dans l'explorateur de projets, ouvrez l'onglet Content Set. Cliquez avec le bouton droit de la souris sur votre fichier et choisissez Run Item through Decision Plan.
    b. Dans la boîte de dialogue Analyzed item, développez le plan de décision et le groupe. Assurez-vous que [Triggered] apparaît pour la règle ProjectA.
    c. Cliquez sur Content Fields.... Dans la boîte de dialogue Select Content Fields, vérifiez que la mention "ProjectA_match" apparaît dans le champ Changed fields, et que la mention "found" est affichée dans le champ de contenu.
15. Dans l'explorateur de projets, cliquez sur Project > Save pour sauvegarder le projet ProjectA_DP.
16. Dans l'explorateur de projets, cliquez sur Project > Export pour exporter le projet ProjectA_DP dans un fichier dpn.
17. Utilisez GIM pour envoyer par commande push le fichier dpn sur les serveurs de fichiers où vous souhaitez utiliser le plan de décision.

Rubrique parent : Reconnaissance et classification de données sensibles dans des serveurs de fichiers

Optimisation des autorisations

Le dispositif Optimisation des autorisations propose un arbitrage entre le rôle de l'administrateur de base de données visant à fournir aux utilisateurs les autorisations requises pour effectuer leur travail de manière efficace, et le rôle de sécurité visant à maintenir un niveau d'autorisation d'utilisation le plus précis et plus bas possible afin d'empêcher les vulnérabilités du système.

Le dispositif Optimisation des autorisations est introduit à partir de Guardium V10.1.2.

Certaines situations qui se présentent naturellement lors de la gestion quotidienne du système génèrent des vulnérabilités, par exemple :

- Un accès surgénéralisé
- Un privilège qui a été accordé à un utilisateur pour une utilisation unique et qui n'a pas été révoqué ensuite
- Des changements d'utilisateurs et de tables au fil du temps, générant des utilisateurs et des tableaux dormants
- Des privilèges qui sont transmis d'un utilisateur à un autre

Les autorisations nécessitent une vigilance constante. Par exemple, les menaces APT (Advanced Persistent Threat) se propagent généralement dans le système au moyen de l'une de ses portes dérobées.

Le dispositif Optimisation des autorisations analyse les privilèges et les actions des utilisateurs et génère des recommandations qui identifient des actions spécifiques visant à réduire l'accès utilisateur uniquement aux parties du système qui sont requises. L'analyse est entièrement effectuée par le système. L'administrateur passe en revue les résultats, examine chaque cas et exécute les actions appropriées, par exemple, il retire les privilèges d'un utilisateur de base de données ou supprime les rôles dormants.

Vous pouvez également rechercher les changements d'autorisation d'utilisation qui se sont produits au cours de la semaine précédente, examiner une liste complète d'utilisateurs et de rôles, passer en revue des privilèges de source de données et leur utilisation réelle et vérifier une justification simulée d'une combinaison utilisateur-rôle spécifique. Ces vues fournissent des informations appropriées pour les recommandations et constituent également des points de départ pour d'autres investigations.

Comparée aux rapports Guardium, le dispositif Optimisation des autorisations présente l'avantage de consolider des informations pour tous les types de base de données (qui apparaissent dans plusieurs rapports Guardium) et d'ajouter de nouvelles analyses dans ses propres rapports complets et consolidés, simplifiant ainsi la gestion de l'autorisation d'utilisation et du même coup, renforçant la sécurité du système.

Le dispositif Optimisation des autorisations prend en charge les types de base de données Microsoft SQL Server et Oracle. Elle ne prend pas en charge les bases de données SQL Contained. (Les rapports Guardium sont générés pour chaque type de base de données.)

La surveillance des activités exercée dans le cadre du dispositif Optimisation des autorisations est limitée aux données actuellement surveillées par Guardium. L'exactitude du rapport Recommandations, de la fonction Parcourir les autorisations et des analyses Simulation dépend de la pertinence des données surveillées. Pour optimiser le potentiel de cet outil, configurez les paramètres userScope et objectScope et envisagez de modifier la politique de sécurité.

Les utilisateurs qui sont dormants depuis le début de la surveillance exercée à l'aide du dispositif Optimisation des autorisations ne sont pas inclus dans les rapports générés par cette dernière. Pour observer un utilisateur spécifique qui fait l'objet d'une surveillance mais pour lequel il n'existe aucune recommandation, vérifiez manuellement son activité en parcourant les autorisations ou en utilisant n'importe lequel des autres outils de surveillance d'activités Guardium. Les outils disposent de toutes les informations si la politique est correctement définie.

L'analyse Autorisations s'effectue pour chaque collecteur et ne s'applique qu'aux sources de données configurées à l'aide de grdapi.

Le dispositif must gather prend en charge l'Optimisation des autorisations. Voir Informations de base pour le support IBM.

Accédez au dispositif Optimisation des autorisations à partir de Reconnaître > Autorisations de base de données > Optimisation des autorisations.

- Activation et configuration du dispositif Optimisation des autorisations
  Utilisez ces commandes grdapi pour activer et configurer le dispositif Optimisation des autorisations.
- Dispositif Optimisation des autorisations - Nouveautés
  L'onglet Nouveautés récapitule les ajouts et les modifications apportés au système pour la semaine calendaire.
- Dispositif Optimisation des autorisations - Utilisateurs et rôles
  L'onglet Utilisateurs et rôles répertorie tous les utilisateurs, et les rôles qui leur sont associés, pour toutes les sources de données pour lesquelles le dispositif Optimisation des autorisations est activé sur ce collecteur.
- Dispositif Optimisation des autorisations - Recommandations
  Les recommandations identifient des actions spécifiques visant à réduire l'accès utilisateur uniquement aux parties du système qui sont requises.
- Dispositif Optimisation des autorisations - Parcourir les autorisations
  Utilisez les vues et les filtres de cette fenêtre pour voir le niveau d'activité des autorisations et leur lignée.
- Dispositif Optimisation des autorisations - Simulation
  L'onglet Simulation affiche la justification probable d'une autorisation d'utilisation pour un utilisateur spécifique avec un ou plusieurs verbes spécifiques sur un objet donné (que l'autorisation d'utilisation existe ou non).

Rubrique parent : Reconnaissance

Activation et configuration du dispositif Optimisation des autorisations

Utilisez ces commandes grdapi pour activer et configurer le dispositif Optimisation des autorisations.

Toutes les commandes sont exécutées sur le collecteur et utilisent les sources de données Guardium déjà définies. Vous commencez par activer le dispositif sur le collecteur, puis vous spécifiez les sources de données et activez les fonctions spécifiques.

Les résultats les plus précis sont obtenus en réglant les données qui sont incluses dans le dispositif Optimisation des autorisations.

Les fonctions Utilisateurs et rôles et Parcourir les autorisations sont activées par défaut, cependant, vous devez affecter aux paramètres extractActivity et extractEntitlement la valeur `true` pour extraire les données pertinentes. Les trois autres fonctions (Nouveautés, Recommandations, Simulation) sont activées individuellement. Par exemple, vous pouvez activer la fonction Recommandations tout en laissant la fonction Simulation désactivée.

La fonction Recommandations utilise un sous-ensemble de données, filtré au moyen des paramètres userScope et objectScope. La fonction Parcourir les autorisations utilise le paramètre userScope pour filtrer les données. Les deux paramètres spécifient un ou plusieurs groupes Guardium. Plus généralement, vous créerez des groupes spécifiques que vous utiliserez dans ce but. Définissez les groupes pour extraire uniquement les données que vous souhaitez, afin de minimiser le stockage et le traitement. L'option d'audit complet doit être définie pour les groupes, de sorte que l'analyse porte sur toutes les données et les résultats soient probants. Lorsque vous utilisez des groupes pour lesquels l'option d'audit complet est définie, la fonction Parcourir les autorisations affiche tous les droits de tous les utilisateurs, quelle que soit leur activité. Un utilisateur qui ne figure pas dans la définition userScope apparaît dans la fenêtre, mais la mention "inconnu" est indiquée pour son comptage d'activité.

Il est recommandé d'évaluer et de concevoir minutieusement votre schéma de collecte de données de manière à éviter de le changer trop souvent. En effet, à chaque fois que vous modifiez la configuration, il faut compter une semaine pour générer les données des rapports ; les données sont comparées aux données des 3 précédentes semaines, et lorsque vous modifiez la définition de données, la comparaison est moins significative que pour les 3 premières semaines.

Des données apparaissent sur chaque onglet le premier dimanche qui suit l'activation de la fonction individuelle.

Voir les informations complètes sur les commandes dans la rubrique GuardAPI Entitlement Optimization Functions.

Prérequis

- La fonction de recherche rapide est activée. (Requise pour les fonctions Simulation et Recommendations et pour la mise à jour des activités dans la fonction Parcourir les autorisations.)
- L'utilisateur qui configure le dispositif Optimisation des autorisations doit disposer de droits sur toutes les métadonnées et tous les tableaux de schémas présents dans les sources de données configurées.

Activation du dispositif Optimisation des autorisations sur le collecteur

Vous pouvez activer le dispositif Optimisation des autorisations sur le collecteur.

Syntaxe :

grdapi enable_entitlement_optimization

Désactivation du dispositif Optimisation des autorisations sur le collecteur

Vous pouvez désactiver le dispositif Optimisation des autorisations sur le collecteur.

Syntaxe :

grdapi disble_entitlement_optimization

Ajout d'une source de données au dispositif Optimisation des autorisations

Vous pouvez ajouter une ou plusieurs sources de données au dispositif Optimisation des autorisations et activer des analyses individuelles.

Syntaxe :

grdapi add_datasource_to_entitlement_optimization datasourceName=[datasource] isEnabled=[true/false] userScope=[USER SCOPE] objectScope=[OBJECT SCOPE] extractActivity=[true/false] extractEntitlement=[true/false] generateRoleClusters=[true/false] generateNews=[true/false] generateRecommendations=[true/false]

Utilisez ce tableau pour déterminer les extractions dont vous avez besoin, par fonction :

Tableau 1. Paramètres d'activation du dispositif Optimisation des autorisations requis par type d'analyse

	Nouveautés (generateNews)	**Utilisateurs et rôles**	**Recommandations (generateRecommendations)**	**Parcourir les autorisations**	**Simulation (generateRoleClusters)**
extractActivity				X	X
extractEntitlement	X	X	X	X	

Retrait d'une source de données du dispositif Optimisation des autorisations

Vous pouvez retirer une ou plusieurs sources de données du dispositif Optimisation des autorisations de sorte qu'aucune donnée ne soit collectée.

remove_datasource_from_entitlement_optimization datasourceName=[datasource name]

Modification des paramètres de source de données pour le dispositif Optimisation des autorisations

Vous pouvez modifier les paramètres d'une source de données qui est déjà activée pour le dispositif Optimisation des autorisations.

Syntaxe :

grgapi set_entitlement_datasource_parameter datasourceName=[datasource name] parameterName=[value] parameterName=[value]

où les valeurs possibles pour parameterName sont les suivantes :

isEnabled

userScope

objectScope

extractActivity

extractEntitlement

generateRoleClusters

generateNews

generateRecommendations

filterTempObjects

filterIgnoreVerbs

Affichage des informations d'optimisation

Syntaxe :

grdapi get_entitlement_optimization_info

Sortie standard :

```
Le dispositif Optimisation des autorisations est activé
==================================
Datasource: SCALE-DB16
==================================
isEnabled: true
userScope:
objectScope:
extractActivity: true
extractEntitlement: true
generateRoleClusters: true
generateNews: true
generateRecommendations: true
filterTempObjects: true
filterIgnoreVerbs: true
```

Rubrique parent : Optimisation des autorisations

Dispositif Optimisation des autorisations - Nouveautés

L'onglet Nouveautés récapitule les ajouts et les modifications apportés au système pour la semaine calendaire.

Des données apparaissent sur l'onglet le premier dimanche qui suit l'activation de la fonction.

L'onglet Nouveautés contient les informations suivantes :

- Le nombre de nouveaux utilisateurs, rôles et objets, ainsi que le nombre de bases de données associées à ces ajouts.
- Le nombre de nouveaux receveurs d'autorisation et de donneurs d'autorisation, ainsi que le nombre d'octrois d'autorisation.

Que faut-il rechercher ?

Recherchez les tendances actuelles, par exemple, en descendant dans la hiérarchie pour trouver :

- Un type ou un nombre inhabituels de modifications dans les autorisations
- Les receveurs d'autorisation/donneurs d'autorisation les plus actifs

Cliquez sur Détails dans n'importe quelle rubrique pour ouvrir un tableau détaillé des ajouts. Par exemple, les détails sur les nouveaux utilisateurs sont le nom de serveur et de service.

Rubrique parent : Optimisation des autorisations

Dispositif Optimisation des autorisations - Utilisateurs et rôles

L'onglet Utilisateurs et rôles répertorie tous les utilisateurs, et les rôles qui leur sont associés, pour toutes les sources de données pour lesquelles le dispositif Optimisation des autorisations est activé sur ce collecteur.

Des données apparaissent sur l'onglet le premier dimanche qui suit l'activation de la fonction.

Cet onglet est basé sur le rapport des utilisateurs et des rôles Guardium standard qui ne présente des données que pour un seul type de données. L'onglet Utilisateurs et rôles comporte les champs suivants :

- Hôte
- Nom de service
- Type de base de données
- Bénéficiaire
- Type de bénéficiaire
- Rôle

Vous pouvez utiliser les fonctions de générateur de rapport standard, accessibles via les icônes situées au-dessus du tableau.

Rubrique parent : Optimisation des autorisations

Dispositif Optimisation des autorisations - Recommandations

Les recommandations identifient des actions spécifiques visant à réduire l'accès utilisateur uniquement aux parties du système qui sont requises.

Des données apparaissent sur l'onglet le premier dimanche qui suit l'activation de la fonction.

Le système évalue continuellement les utilisateurs et les privilèges. Le rapport hebdomadaire de recommandations d'autorisation d'utilisation est basé sur les 3 dernières semaines de données (par défaut) de sorte que chaque nouveau rapport chevauche les données du précédent rapport. L'onglet Recommandations équivaut au rapport Recommandations de l'application Rapports, activé en tant que rapport réparti.

Si vous avez personnalisé le paramètre userScope, les recommandations incluent uniquement les utilisateurs du groupe d'utilisateurs spécifié. Les paramètres userScope et objectScope sont utilisés pour définir de manière explicite la portée des recommandations. Pour optimiser l'exactitude des recommandations concernant les utilisateurs et les objets, l'option d'audit complet doit être activée pour les utilisateurs et les objets appartenant aux groupes spécifiés.

Toutes les recommandations doivent être examinées de manière approfondie par l'administrateur en descendant dans la hiérarchie à la recherche d'un serveur, d'une base de données, d'un objet et d'un type de recommandation spécifique avant implémentation.

La partie supérieure de l'onglet contient un graphique circulaire représentant les recommandations par type. Les recommandations sont répertoriées dans un tableau situé dans la partie inférieure de l'onglet. Vous pouvez modifier le rapport des recommandations à l'aide des icônes de rapports standard, exporter le rapport en cliquant sur Exporter et effectuer un mappage vers une API en cliquant sur Actions.

Les types de recommandation sont les suivants :

Tableau 1. Types de recommandation

Type	Chaîne	Détails
ANOMAL USER	Examiner le comportement anormal de l'utilisateur {object} au sein du rôle {source}.	Le nombre d'activités d'utilisateur pour un rôle spécifique est anormal. Cela signifie que l'utilisateur est beaucoup trop actif ou beaucoup moins actif que les autres utilisateurs.
ALERT ACTIVITY (Ad-hoc user)	L'utilisateur {source} a utilisé le privilège verb}-{object} mais aucune autorisation n'a été trouvée.	Un utilisateur ad hoc typique s'accorde lui-même des droits, effectue une action, puis retire les droits. Les utilisateurs peuvent être identifiés par erreur comme étant des utilisateurs ad hoc en raison des écarts de temps entre les modifications apportées aux autorisations et leurs activités. Utilisez les outils de surveillance d'activités Guardium pour déterminer si le privilège est justifié ou non.
DORMANT_USER	Retirer l'utilisateur inactif ou vide {object}	Aucun privilège n'a été affecté à l'utilisateur ou aucune activité n'a été enregistrée pour ce dernier au cours de l'intervalle défini.
DORMANT_ROLE	Retirer le rôle inactif ou vide {role}	Aucun utilisateur, aucune activité enregistrée pour aucun utilisateur ou privilèges vides.
REVOKE_FROM_USER	Révoquer {verb}-{object} pour l'utilisateur {source}	L'utilisateur n'a effectué aucune activité sur le bloc de données objet/verbe concerné.
REVOKE _FROM_ROLE	Révoquer {verb}-{object} pour le rôle {source}	Aucun des utilisateurs associés au rôle spécifique n'a effectué d'activité sur le bloc de données objet/verbe.
REMOVE_FROM_ROLE	Retirer l'utilisateur {object} du rôle {source}	L'utilisateur n'a utilisé aucun des privilèges qui lui ont été accordés par le rôle.
INACTIVE DATABASE	La base de données n'a aucune activité	Si la base de données inutilisée ne peut pas être justifiée, retirez-la.

Rubrique parent : Optimisation des autorisations

Dispositif Optimisation des autorisations - Parcourir les autorisations

Utilisez les vues et les filtres de cette fenêtre pour voir le niveau d'activité des autorisations et leur lignée.

Des données apparaissent sur l'onglet le premier dimanche qui suit l'activation de la fonction. Ensuite, les activités sont quotidiennement mises à jour.

Ces informations sont utiles pour l'examen général de l'autorisation d'utilisation et pour évaluer davantage les recommandations du rapport Recommandations. Par défaut, cette fenêtre présente un diagramme à barres illustrant les sources de données avec les taux les plus élevés de privilèges inutilisés.

L'onglet Parcourir les autorisations affiche toutes les autorisations des sources de données définies dans grdAPI pour lesquelles extractEntitlement est disponible. Cela s'applique lorsque la collecte d'activités est désactivée et que les paramètres userScope et objectScope sont définis. Vous pouvez toujours rechercher et voir les droits de tous les utilisateurs.

Les résultats du champ Comptage d'activité sont affectés par le paramètre userScope, comme suit :

- Utilisateurs qui sont inclus dans la portée définie par le paramètre userScope :
-
    - Les utilisateurs actifs apparaissent en vert et des résultats numériques leur sont associés dans la colonne Comptage d'activité.
    - Les utilisateurs non actifs apparaissent en rouge et le comptage d'activité indique "Non actif".
- Utilisateurs qui ne sont pas inclus dans la portée définie par le paramètre userScope :
    - Les utilisateurs actifs apparaissent en vert et des résultats numériques leur sont associés dans le comptage d'activité.
    - Les utilisateurs non actifs apparaissent en gris et le comptage d'activité indique "inconnu".

Examens typiques :

- Identifier les objets sur lesquels un utilisateur dispose de droits et déterminer si celui-ci utilise effectivement ces objets.
- Déterminer si un utilisateur a utilisé ses droits sur un objet au moment où il était autorisé à le faire.
- Certains droits sont-ils utilisés plus souvent que prévu ?
- Certains droits sont-ils utilisés plus d'une fois ?
- Quelle est la lignée des droits qui ont été utilisés de manière inhabituelle : explicites, implicites, hérités d'un rôle parent ou issus d'une hiérarchie de rôles ?

Pour obtenir plus d'informations sur la façon d'utiliser un privilège spécifique, avec des instructions SQL complètes, vous pouvez faire une recherche sur Activité de données (Examen > Recherche d'activité de données), cliquer avec le bouton droit de la souris sur Utilisateur de base de données ou Programme source dans la table de résultats et sélectionner SQL complet par utilisateur de base de données.

Les autorisations inutilisées sont principalement :

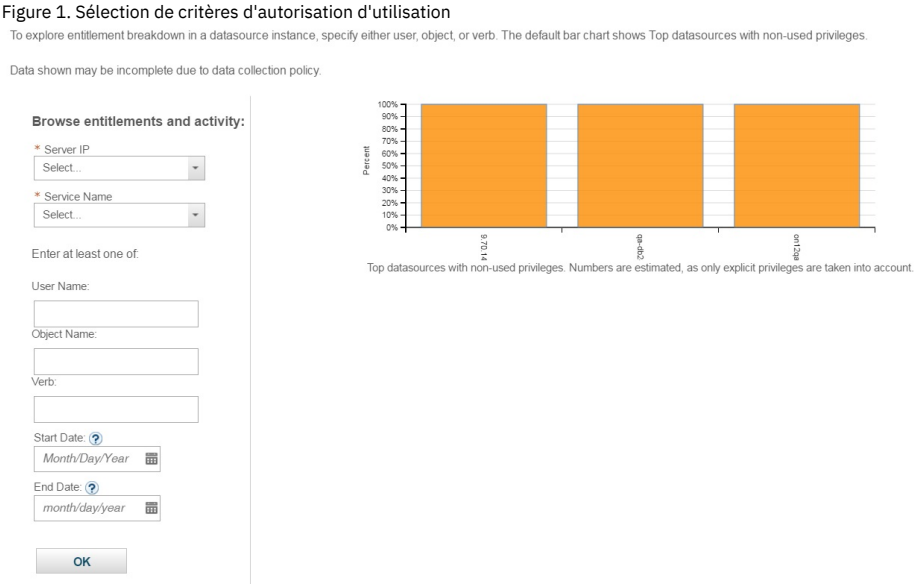
- Action rarement effectuée, mais autorisation d'utilisation valide, par exemple lors de la génération d'un rapport trimestriel
- Autorisation d'utilisation inutilisée et donc, non justifiée (point de vulnérabilité)

Pour afficher l'utilisation des autorisations pour un service ou un serveur spécifique :

1. Sur le côté gauche, sélectionnez une adresse IP de serveur et un service.

2. Procédez à un filtrage par nom et/ou par nom d'objet.
3. Le cas échéant, entrez un verbe ou une plage de dates.

Figure 1. Sélection de critères d'autorisation d'utilisation



La table présente les informations suivantes : Type de bénéficiaire, Bénéficiaire, Verbe, Nom, Comptage d'activité et Lignée. Un utilisateur peut avoir plusieurs lignées de privilèges : explicites, implicites, hérités d'un rôle parent ou issus d'une hiérarchie de rôles.

Rubrique parent : Optimisation des autorisations

Dispositif Optimisation des autorisations - Simulation

L'onglet Simulation affiche la justification probable d'une autorisation d'utilisation pour un utilisateur spécifique avec un ou plusieurs verbes spécifiques sur un objet donné (que l'autorisation d'utilisation existe ou non).

Des données apparaissent sur cet onglet le premier dimanche qui suit l'activation de la fonction.

Guardium analyse le comportement d'utilisateurs similaires pour produire la justification probable, laquelle, dans certains cas, fournit des informations extrêmement pertinentes. L'analyse peut s'avérer utile lorsque vous examinez des autorisations inutilisées et la recommandation REVOKE_FROM_USER. Cette analyse donne une indication d'ordre général et doit être utilisée avec d'autres fonctions d'optimisation des autorisations.

Renseignez les champs suivants et cliquez sur OK pour générer la probabilité :

- Nom d'utilisateur
- Nom d'objet
- Verbe (un ou plusieurs)
- Adresse IP serveur
- Nom de service

Les réponses possibles sont les suivantes :

- La probabilité que cet utilisateur de base de données utilise ce privilège est de **n%**. Une probabilité de 100 % indique que l'utilisateur a utilisé l'activité au moins une fois.
- La source de données est introuvable sur le serveur.
- L'objet et l'utilisateur de base de données sont hors de la portée.
- Aucun indice suffisant n'a été trouvé pour l'utilisateur de base de données et le privilège : soit l'utilisateur/l'objet/le verbe n'existe pas dans la base de données sélectionnée, soit aucune activité n'a été trouvée pour l'utilisateur ou aucune activité n'a été trouvée pour le tuple objet, verbe. Correctifs possibles : attendez que la collecte d'activités soit exécutée ; assurez-vous que les données ont été correctement saisies.

Rubrique parent : Optimisation des autorisations

Protection

Après avoir identifié les bases de données et les systèmes de fichiers qui contiennent des données sensibles, vous pouvez effectuer plusieurs opérations pour protéger ces données. Les options de protection permettent notamment d'inclure des données de masquage, d'alerter le personnel sur la base de l'accès aux données et d'établir des politiques visant à renforcer les restrictions d'accès.

- Bases de référence
  Une base de référence est un profil des commandes d'accès exécutées par le passé, destiné à vous permettre d'identifier des activités normales et des comportements anormaux (incohérents ou différents par rapport aux comportements habituels, normaux ou attendus).
- Politiques
  Une politique de sécurité contient un ensemble ordonné de règles à appliquer au trafic observé entre des clients et des serveurs de base de données. Chaque règle peut s'appliquer à une demande d'un client ou à une réponse d'un serveur. Plusieurs politiques peuvent être définies et plusieurs politiques peuvent être installées en même temps sur un dispositif Guardium.
- Alertes de corrélation
  Une alerte est un message indiquant qu'une exception ou une violation de règle de politique a été détectée.
- Comment indiquer des événements via des alertes de corrélation
  Déclenchez une alerte de corrélation si plus de quinze erreurs SQL émanant d'un utilisateur d'application ont été détectées au cours des trois dernières heures.

- Gestion des incidents
  L'application IIM (Integrated Incident Management) fournit une interface pour utilisateur métier avec des flux de travaux automatisés pour le suivi et la résolution des incidents liés à la sécurité de la base de données.
- Comment gérer la révision de plusieurs incidents de sécurité de base de données
  Gestion des incidents : Apprenez à suivre et résoudre les incidents de sécurité de base de données.
- Réécriture de requête
  La fonctionnalité de réécriture de requête fournit un contrôle d'accès à granularité fine pour les bases de données en interceptant des requêtes de base de données et en les réécrivant en fonction des critères définis dans les politiques de sécurité.
- Politiques et règles relatives à l'activité des fichiers
  La surveillance de l'activité des fichiers garantit l'intégrité et la protection des données sensibles sur les serveurs de fichiers UNIX et Windows.

Bases de référence

Une base de référence est un profil des commandes d'accès exécutées par le passé, destiné à vous permettre d'identifier des activités normales et des comportements anormaux (incohérents ou différents par rapport aux comportements habituels, normaux ou attendus).

L'outil Générateur de base de référence génère une base de référence en examinant les activités précédemment consignées et actuellement disponibles sur le système Guardium.

Lorsqu'elle est incluse dans une politique de sécurité, la base de référence devient une règle de base de référence, qui autorise tous les accès de base de données ayant été inclus dans la base de référence.

Une règle de base de référence incluse dans une politique présente les caractéristiques suivantes :

- Il ne peut exister qu'une seule règle de base de référence.
- L'action associée à la règle de base de référence est toujours Autoriser, ce qui consiste à accepter la commande et à ne pas passer à la règle suivante dans la politique.
- Lorsque la règle de base de référence est ajoutée à la politique, elle est positionnée en premier dans la liste de règles. Elle peut être déplacée n'importe où dans l'ensemble de règles (évaluées de manière séquentielle), en fonction de la politique.
- Une fois incluse dans une politique, la règle de base de référence ne peut pas en être retirée.

Avertissement : Le générateur de base de référence et la fonctionnalité connexe sont dépréciées depuis Guardium version 10.1.4.

L'outil Générateur de politique peut générer des règles de politique recommandées à partir de la base de référence. Les règles recommandées peuvent être éditées et incluses dans la politique avant la règle de base de référence, de sorte que des actions alternatives (par exemple, des alertes) puissent être exécutées pour certaines commandes observées pendant la période de base de référence. De plus, un examen des règles recommandées fournit des informations utiles sur les modèles de trafic réellement observés (types de commande et fréquence).

L'outil Générateur de base de référence offre plusieurs façons de contrôler ce qui est inclus dans la base de référence :

- En spécifiant un seuil correspondant au nombre de fois qu'une commande doit être observée avant d'être incluse dans la règle. Si la valeur de seuil est un, chaque commande observée est incluse dans la règle, et si la valeur de seuil est 1 000, seules les commandes observées au moins 1 000 fois sont ajoutées à la règle.
- En contrôlant la sensibilité à un ou plusieurs attributs. Par exemple, si la base de référence est sensible à l'utilisateur de base de données, elle inclura uniquement des commandes pour certains utilisateurs. Les utilisateurs qui n'ont pas exécuté la commande pendant la période de référence de base ne seront pas autorisés par la règle de base de référence.
- En limitant les connexions incluses dans les sous-ensembles d'adresses IP de serveur et de client. La base de référence indique toujours un masque de réseau client unique et un masque de réseau serveur unique. Chaque masque peut être aussi inclusif ou exclusif que nécessaire.
- En fusionnant des données de différentes périodes. Il peut s'avérer nécessaire d'inclure dans la base de référence du trafic enregistré pendant des périodes non contiguës. Vous pouvez fusionner les données de n'importe quel nombre de périodes dans une seule et même base de référence. En outre, les données peuvent être filtrées pour des adresses client et serveur spécifiques.

A propos de la sensibilité à la base de référence

La sensibilité à la base de référence peut reposer sur n'importe quelle combinaison des éléments suivants (chacun de ces éléments est décrit ultérieurement) :

- Utilisateur de base de données
- Protocole de base de données
- Version du protocole de base de données
- Période
- Programme source
- Séquence

La sensibilité à la base de référence dépend d'un seuil spécifié, lequel définit le nombre minimum de fois qu'une commande doit être observée durant la période de base de référence avant d'être incluse dans la base de référence.

Si aucune sensibilité n'est sélectionnée, chaque commande dont le nombre d'occurrences dépasse le seuil indiqué sera incluse dans la base de référence.

Si un seul type de sensibilité est sélectionné, un comptage distinct de chaque commande est géré pour chaque valeur du type de sensibilité (utilisateur de base de données, par exemple).

Si plusieurs types de sensibilité sont sélectionnés, des comptages distincts de chaque commande sont gérés pour chaque combinaison de valeurs pour chaque type sélectionné (pour chaque combinaison de base de données utilisateur et de programme source, par exemple). Par conséquent, pour chaque type de sensibilité inclus, le nombre de combinaisons peut augmenter de manière significative.

A propos de la sensibilité à la séquence

Si la base de référence est sensible à la séquence de commandes, lorsqu'elle est incluse dans une politique, la règle de base de référence autorise uniquement les séquences de commandes observées durant la période de base de référence. Voici un exemple d'illustration très simple : si les deux seules séquences de commandes observées au cours de la période de base de référence sont A-B et B-C, le tableau ci-dessous indique les séquences de commandes autorisées par cette règle de base de référence.

Tableau 1. A propos de la sensibilité à la séquence

Séquence de commandes	Autorisée
A - B	O
A - toute autre lettre	N
B - C	O
B - toute autre lettre	N
Tout sauf A	N

A propos de la sensibilité à la période

Lorsque la base de référence est sensible à la période, des comptages distincts sont gérés pour chaque période définie. Si des périodes de chevauchement sont définies (situation classique), une commande est comptabilisée plus d'une fois, dans la période la plus restrictive au cours de laquelle elle se produit. Si la période n'est pas contiguë, par exemple, de 00h00 à 08h00 chaque jour de la semaine, un seul segment contigu de la période est pris en compte (en l'occurrence, huit heures).

Pour illustrer la façon dont l'outil Générateur de référence affecte des demandes à des périodes, imaginons que Samedi est inclus dans trois périodes :

- 24x7 (24 heures, 7 jours sur 7)
- Samedi (24 heures uniquement)
- Fin de semaine (48 heures, Samedi + Dimanche)

Etant donné que la période nommée Samedi est la plus restrictive (24 heures uniquement), toutes les demandes dont l'horodatage correspond à Samedi seront comptabilisés dans cette période et non dans les périodes nommées Fin de semaine ou 7x24, plus inclusives.

A propos des bases de référence dans les environnements d'agrégation et de gestionnaire central

S'il existe plusieurs dispositifs Guardium dans un environnement d'agrégation et/ou de gestionnaire central, le point important suivant doit être pris en considération lors de la génération et de l'utilisation de bases de référence :

Une base de référence est générée en utilisant uniquement les données disponibles sur le dispositif qui la génère.

Cela signifie que :

- Une base de référence générée sur un collecteur sera créée à l'aide du trafic disponible uniquement sur cette unité.
- Une base de référence construite sur un agrégateur sera créée à partir des données disponibles sur celui-ci, généralement envoyées par plusieurs collecteurs sur une période donnée.
- Une base de référence générée sur un gestionnaire central qui ne fait pas également office d'agrégateur sera vide, car un gestionnaire central ne collecte pas de données (sauf s'il fait également office d'agrégateur).
- Dans un environnement de gestion centralisée, une base de référence générée sur une unité gérée est créée uniquement à l'aide des données issues de cette unité, mais elle est stockée sur le gestionnaire central et peut être utilisée sur n'importe quelle autre unité.
- Dans un environnement de gestion centralisée, une seule base de référence peut être générée à partir de plusieurs unités gérées. Pour cela, elle est créée à l'aide des données issues du premier dispositif géré, puis fusionnée à l'aide des données issues des autres dispositifs, sélectionnés un par un.

A propos des règles recommandées

Lorsqu'une base de référence est incluse dans une politique, l'outil Générateur de politique peut générer des règles recommandées à partir de cette base de référence. Il génère le nombre minimum de règles nécessaires pour représenter tout ce qui est inclus dans la base de référence. Vous pouvez alors accepter certaines ou l'ensemble des règles recommandées et les modifier si besoin. Hormis le fait qu'il s'agit d'un moyen très pratique de générer une politique explicite (au lieu d'une politique implicite basée uniquement sur une base de référence), vous pouvez ainsi vérifier que la base de référence ne comporte aucune activité malveillante ou erronée susceptible de s'être produite pendant la période de base de référence, ce qui constitue une étape importante.

Vous souhaiterez peut-être modifier les règles recommandées si vous reconnaissez une activité qui s'est produite durant la période de base de référence et que vous souhaitez surveiller cette activité ou lui associer une alerte. Il vous suffit de personnaliser la règle appropriée recommandée à partir de la base de référence et de lui affecter l'action de votre choix. Par défaut, les règles recommandées sont positionnées avant la règle de base de référence, par conséquent, l'action spécifiée sera effectuée avant que la règle de base de référence ne soit exécutée afin d'autoriser cette commande sans test supplémentaire des règles.

Remarque : L'outil Générateur de politique peut également générer des règles à partir de la liste de contrôle d'accès de base de données. Pour plus d'informations, voir Politiques.

A propos des groupes d'objets recommandés

Lorsqu'il génère des règles recommandées à partir de la base de référence ou de la liste de contrôle d'accès de base de données, l'outil Générateur de politique réduit le nombre de règles recommandées en créant des groupes d'objets recommandés. Imaginons par exemple une base de référence incluant une commande spécifique qui fait référence à seulement trois objets, AAA, BBB et CCC, et qu'il n'existe pour l'instant aucun groupe d'objets composé uniquement de ces trois objets. L'outil Générateur de politique va créer un groupe d'objets recommandés correspondant à ces objets et générer une règle unique pour la commande faisant référence au groupe d'objets recommandés.

Vous pouvez afficher l'appartenance d'un groupe d'objets recommandés et vous avez la possibilité d'accepter ou de refuser chaque groupe. Dans l'exemple précédent, si vous rejetez le groupe d'objets recommandés, la règle unique qui lui fait référence sera remplacée par trois règles recommandées (une pour AAA, une pour BBB et une pour CCC).

Création d'une base de référence

1. Cliquez sur Protection > Politiques de sécurité > Générateur de base de référence pour ouvrir le panneau Localiseur de base de référence.
2. Cliquez sur Nouveau pour ouvrir le panneau Générateur de base de référence.
3. Entrez un nom de base de référence unique dans le champ Description de base de référence. Vous ne devez pas ajouter d'apostrophe dans la description de la base de référence.
4. Dans la sous-fenêtre Sensibilité de base de référence, cochez chaque élément auquel la base de référence sera sensible. Plus la base de référence sera sensible, plus le test effectué lors de la création de la base de référence et, plus important encore, lors de l'inspection du trafic, sera complexe. Pour plus d'informations sur la sensibilité à la base de référence, voir la rubrique Présentation du produit.

5. Dans la sous-fenêtre Seuil de base de référence, entrez le nombre minimum d'occurrences d'une commande durant la période de base de référence pour que cette commande soit incluse dans la base de référence. Si une ou plusieurs cases de sensibilité ont été cochées, ce comptage s'applique à la combinaison de valeurs de sensibilité.

   Si l'approche que vous choisissez pour créer votre politique de sécurité consiste à toujours autoriser les commandes les plus couramment exécutées dans le passé, augmentez ce nombre, conformément au niveau approprié. En revanche, si vous souhaitez vous assurer que la base de référence est exhaustive, conservez la valeur 1. Dans les deux cas, vous obtiendrez les règles recommandées à partir de la base de référence par le générateur de politique. Les règles recommandées sont triées par ordre décroissant de fréquence au cours de la période de base de référence ; ainsi, vous pouvez décider à quel moment inclure ou modifier des règles pour chaque commande unique exécutée.

6. Utilisez la sous-fenêtre Informations réseau de base de référence pour identifier les serveurs et les clients à inclure dans la base de référence. La méthode utilisée dans le but de sélectionner les adresses IP à utiliser pour construire la base de référence est la même que pour les serveurs et les clients.

   Pour chaque adresse trouvée dans les données de base de référence, l'appartenance à un groupe balisé éventuellement est prise en compte en premier. Un groupe balisé est une liste spécifique d'adresses IP pour lesquelles des enregistrements de base de référence seront générés. Si un groupe balisé est sélectionné et si une adresse IP détectée dans les données de base de référence est incluse dans le groupe balisé correspondant, cet élément sera inclus dans la base de référence pour cette adresse IP spécifique. Imaginons par exemple que le groupe d'adresses IP client balisées nommé ZoneAGroup ait été sélectionné et que ce groupe comporte l'adresse client 192.162.14.33. Si le générateur de base de référence trouve la commande SELECT abc FROM xyz à partir de cette adresse IP, cette commande est comptabilisée pour cette adresse spécifique.

   En revanche, si aucun groupe balisé n'est sélectionné, ou si une adresse IP détectée dans les données de base de référence n'est pas incluse dans le groupe balisé sélectionné, cette commande peut être comptabilisée avec des commandes identiques à partir d'autres adresses IP, comme indiqué par le masque de réseau correspondant.

   Le masque de réseau est requis pour regrouper des adresses IP client et serveur. Les options incluent toutes les différentes variations de masques de sous-réseau de 255.255.255.255 (les quatre octets doivent tous correspondre) à 0.0.0.0 (il peut s'agir de n'importe quels octets).

   Vous devez toujours :

   - entrer un masque de sous-réseau dans le champ Masque de réseau serveur ;
   - entrer un masque de sous-réseau dans le champ Masque de réseau client.

   Pour illustrer la façon dont le générateur de base de référence utilise des masques de réseau pour regrouper des adresses, imaginons les hypothèses suivantes :
   - Le masque de réseau client est 255.255.0.0, autrement dit, les deux premiers octets doivent être identiques, ce qui n'est pas le cas des deux octets suivants.
   - Dans les données de base de référence, une demande avec l'adresse IP client 192.168.3.211 est trouvée.
   - L'adresse IP client ne figure pas dans le groupe d'adresses IP client balisées sélectionné (ou aucun groupe d'adresses IP client balisées n'est sélectionné).
   - La commande est SELECT abc FROM xyz.

   Lors de la génération de la base de référence, cette commande sera incluse dans le comptage de toutes les commandes SELECT abc FROM xyz pour toutes les adresses IP client à partir du sous-réseau 192.168.0.0.

7. Cliquez sur Sauvegarder pour vérifier que la définition de la base de référence est valide et la sauvegarder. Si vous avez omis des champs obligatoires ou saisi des valeurs incorrectes, la définition n'est pas sauvegardée et vous devez résoudre ces problèmes avant de tenter de la sauvegarder à nouveau.
8. Cliquez éventuellement sur Rôles afin d'affecter des rôles pour la politique.
9. Cliquez éventuellement sur Commentaires pour ajouter des commentaires à la définition.
10. Une fois qu'une base de référence a été sauvegardée, les sous-fenêtres Génération de base de référence et Consignation de base de référence apparaissent sur le panneau.
11. Cliquez n'importe où dans le titre de la sous-fenêtre Génération de base de référence pour développer cette dernière.
12. Renseignez les champs Date de début et Date de fin pour définir la période à partir de laquelle la base de référence doit être générée. Il existe différentes façon d'entrer les dates. Pour plus d'informations, consultez Dates et horodatages. Si vous avez indiqué des minutes ou des secondes, elles ne seront pas prises en compte.
13. Cliquez sur le bouton Générer pour générer la base de référence. Si vous avez modifié la définition de la base de référence, vous serez invité à la sauvegarder avant de générer la base de référence.

Remarque : Une fois la base de référence générée pour la première fois, d'autres champs apparaissent dans le panneau Génération de base de référence. Ces champs vous permettent de fusionner les données issues de périodes supplémentaires dans la base de référence et de limiter les adresses IP client et serveur utilisées au cours de chaque période supplémentaire.

Fusion des informations de base de référence

Pour fusionner des informations de base de référence (dans le but d'inclure des informations issues de périodes supplémentaires et/ou de différents groupes de clients et serveurs, par exemple) :

1. Cliquez sur Protection > Politiques de sécurité > Générateur de base de référence pour ouvrir le panneau Localiseur de base de référence.
2. Dans la liste Définition de base de référence, sélectionnez la base de référence dans laquelle vous souhaitez fusionner des informations de base de référence supplémentaires.
3. Cliquez sur Modifier pour ouvrir le panneau Editer la base de référence.
4. Ne modifiez pas les sélections effectuées pour la sensibilité à la base de référence. Si vous modifiez la sensibilité à la base de référence, vous êtes invité à générer une toute nouvelle base de référence qui viendra remplacer l'existante.
5. Facultatif. Définissez le nombre minimum d'occurrences en plus de la valeur de la base de référence dans la sous-fenêtre Seuil de base de référence. La valeur saisie ici n'a aucun impact sur les informations déjà incluses dans la base de référence. Une information qui a été ajoutée à la base de référence n'est pas retirée lors d'une opération de fusion.
6. Facultatif. Entrez d'autres informations relatives au réseau dans la sous-fenêtre Informations réseau de base de référence. Les valeurs affichées proviennent de la dernière opération de génération ou de fusion. Si les informations fusionnées proviennent du même jeu de serveurs et/ou clients, ne les modifiez pas. Sinon, effectuez les modifications appropriées dans cette sous-fenêtre pour sélectionner le trafic à inclure dans la base de référence.
7. Cliquez n'importe où dans le titre de la sous-fenêtre Génération de base de référence pour développer cette dernière.
8. Renseignez les champs Date de début et Date de fin pour définir la période à partir de laquelle la base de référence doit être générée. Il existe différentes façon d'entrer les dates. Pour plus d'informations, consultez Dates et horodatages. Si vous avez indiqué des minutes ou des secondes, elles ne seront pas prises en compte.
9. Sélectionnez le bouton d'option Fusionner.
10. Facultatif. Dans la sous-fenêtre Sélection de filtre, limitez la génération de base de référence à certaines adresses IP client et/ou serveur en entrant une adresse IP suivie d'un masque de réseau. Par exemple, pour sélectionner toutes les adresses IP client depuis le sous-réseau 192.168.9.x, entrez 192.168.9.1 in dans la

première zone Adresse IP client, puis 255.255.255.0 dans la seconde zone. Pour inclure d'autres adresses, cliquez sur le bouton Ajouter, puis entrez les informations d'adresse supplémentaires.

11. Cliquez sur Générer pour générer la base de référence. Si vous avez modifié la définition de la base de référence, vous serez invité à la sauvegarder avant de générer la base de référence.

Modification d'une base de référence

Attention : avant de modifier la définition d'une base de référence, vous devez être certain de bien avoir compris ce qu'implique cette modification, en particulier si la base de référence dont vous souhaitez modifier et régénérer la définition est utilisée dans une politique installée. Si vous modifiez et régénérez une base de référence contenue dans une politique installée, lorsque vous réinstallez cette dernière, elle utilise la nouvelle base de référence. Pour la rétromigration des bases de référence utilisées par des politiques installées, envisagez plutôt de cloner ces bases de référence et ces politiques et de modifier et générer les définitions clonées. Pour plus d'informations, voir la section Clonage d'une base de référence.

1. Cliquez sur Protection > Politiques de sécurité > Générateur de base de référence pour ouvrir le panneau Localiseur de base de référence.
2. Dans la liste Définition de base de référence, sélectionnez la base de référence à modifier. Cliquez sur Modifier pour ouvrir le panneau Editer la base de référence. A l'exception de son titre, ce panneau est identique au panneau Ajouter une base de référence. Pour savoir comment utiliser ce panneau, voir la section Création d'une base de référence.

Clonage d'une base de référence

Dans un certain nombre de situations, vous souhaiterez peut-être définir une nouvelle base de référence à partir d'une base de référence existante, sans modifier la définition d'origine. Voir la rubrique Attention.

1. Cliquez sur Protection > Politiques de sécurité > Générateur de base de référence pour ouvrir le panneau Localiseur de base de référence.
2. Dans la liste Définition de base de référence, sélectionnez la base de référence à cloner.
3. Cliquez sur Cloner pour ouvrir le panneau Cloner une base de référence.
4. Entrez un nom unique pour la nouvelle base de référence dans le champ Nouvelle description de base de référence. Vous ne devez pas ajouter d'apostrophe dans la description de la nouvelle base de référence.
5. Pour cloner les enregistrements de base de référence (principalement, les commandes) qui ont été générés pour la base de référence qui fait l'objet d'un clonage, cochez la case Cloner enregistrements.
6. Cliquez sur Accepter pour sauvegarder la nouvelle base de référence. Vous pouvez alors ouvrir et éditer la nouvelle base de référence à l'aide du panneau Localiseur de base de référence.

Retrait d'une base de référence

1. Cliquez sur Protection > Politiques de sécurité > Générateur de base de référence pour ouvrir le panneau Localiseur de base de référence.
2. Dans la liste Définition de base de référence, sélectionnez la base de référence à retirer.
3. Cliquez sur Supprimer. Vous êtes invité à confirmer l'action.

Rubrique parent : Protection

Politiques

Une politique de sécurité contient un ensemble ordonné de règles à appliquer au trafic observé entre des clients et des serveurs de base de données. Chaque règle peut s'appliquer à une demande d'un client ou à une réponse d'un serveur. Plusieurs politiques peuvent être définies et plusieurs politiques peuvent être installées en même temps sur un dispositif Guardium.

Chaque règle d'une politique définit une action conditionnelle. La condition testée peut être un simple test, par exemple, il peut s'agir de vérifier les accès à partir d'une adresse IP client qui n'appartient pas à un groupe d'adresses IP client autorisées. Ou, la condition testée peut être un test complexe qui prend en compte plusieurs attributs de message et de session (utilisateur de base de données, programme source, type de commande, heure du jour, etc.),et elle peut être sensible au nombre de fois que la condition est satisfaite dans un délai spécifié.

L'action déclenchée par la règle peut être une action de notification (e-mail envoyé à un ou plusieurs récepteurs, par exemple), une action de blocage (la session client peut être déconnectée), ou l'événement peut simplement être consigné en tant que violation de politique. Des actions personnalisées peuvent être développées dans le but d'effectuer les tâches nécessaires pour des conditions qui peuvent être uniques pour un environnement ou une application spécifique. Pour obtenir la liste complète des actions, voir la présentation des actions associés aux règles.

Une violation de politique est consignée chaque fois qu'une action d'alerte ou de consignation uniquement est déclenchée. Eventuellement, le code SQL ayant déclenché la règle (y compris des valeurs de données) peut être enregistré avec la violation de politique. Des violations de politique peuvent être affectées à des incidents, automatiquement par un processus ou manuellement par des utilisateurs autorisés (voir l'onglet Gestion des incidents de l'interface graphique Guardium). Pour plus d'informations, voir Gestion des incidents.

Remarque : Des alertes de corrélation peuvent aussi être écrites sur le domaine de violations de politique (voir Alertes de corrélation).

Outre la consignation des violations, des règles de politique peuvent affecter la consignation du trafic client, consigné sous la forme d'enregistrements et d'instances d'enregistrement.

- A la base, les enregistrements sont des prototypes de demandes détectés par Guardium dans le trafic. Les combinaisons de commandes, d'objets et de champs inclus dans un enregistrement peuvent être très complexes, mais chaque enregistrement représente principalement un type très spécifique de demande d'accès. Le processus de détection et de consignation de nouveaux enregistrements commence lorsque le moteur d'inspection démarre, et, par défaut, se poursuit (sauf comme indiqué) indépendamment des règles de politique de sécurité.
- Chaque instance d'un enregistrement détecté dans le trafic est également consignée, et chaque instance est associée à une session client-serveur spécifique. Aucun code SQL n'est stocké pour une instance d'enregistrement, sauf lorsqu'une règle de politique demande la consignation de SQL pour cette instance, ou pour une session client-serveur spécifique d'instances (avec ou sans valeurs).

Outre le contrôle de l'inclusion de code SQL dans des instances d'enregistrement client, une règle de politique de sécurité peut désactiver la consignation d'enregistrements et d'instances pour le reste d'une session.

Dans le cas de volumes importants, l'analyse syntaxique et l'agrégation d'informations dans des enregistrements et des instances peuvent être différées à l'aide de l'option Consigner données brutes (processus Flat Log). Lorsque cette option est utilisée, la production d'alertes et de rapports est retardée jusqu'à ce que les informations consignées soient agrégées. Voir la section Consigner données brutes ultérieurement dans cette rubrique.

Pour contrôler entièrement le trafic client qui est consigné, une politique peut être définie en tant que politique Trace d'audit sélectif. Dans ce type de politique, des règles Effectuer l'audit uniquement et un modèle facultatif identifient tout le trafic client à consigner. Voir la section Utilisation de la trace d'audit sélectif ultérieurement dans cette rubrique.

Outre l'installation de nouvelles politiques à partir de l'écran Programme d'installation de politique de la console d'administration/d'installation de politique :

- Une nouvelle politique peut être installée à partir de l'écran Localiseur de politique.
- A partir de l'écran Définition de politique, une politique installée peut être réinstallée, sans qu'il soit nécessaire de réinstaller d'autres politiques installées.
- A partir de l'écran Règles de politique, une règle de politique installée peut être réinstallée, sans qu'il soit nécessaire de réinstaller toute la politique.

Sur les nouvelles installation uniquement (non sur les mises à niveau), il existe une politique par défaut. Elle ne comporte pas de règles, mais la case Audit sélectif est cochée (cela signifie que le système Guardium ne collectera aucun trafic via la politique par défaut). La politique par défaut sur un système Guardium 64 bits (nouvelle installation) est Valeur par défaut - Ignorer l'activité des données pour les connexions inconnues.

Principes de règle de politique

Au sein d'une politique, les règles sont évaluées dans l'ordre où elles apparaissent, à mesure que chaque élément de trafic est analysé.

Il existe trois types de règles :

- Une règle d'accès s'applique aux demandes client. Par exemple, elle peut tester les commandes UPDATE exécutées à partir d'un groupe spécifique d'adresses IP.
- Une règle d'exception évalue les exceptions renvoyées par le serveur (réponses). Par exemple, elle peut tester cinq échecs de connexion dans un délai d'une minute.
- Une règle d'intrusion évalue les données renvoyées par le serveur (dans les réponses aux demandes). Par exemple, elle peut tester les données renvoyées pour des modèles numériques qui peuvent être des numéros de sécurité sociale ou de carte de crédit.

Catégorie, classification et gravité

Pour chaque règle, une catégorie et/ou une classification peut éventuellement être affectée. La catégorie et la classification permettent de regrouper des violations de politique à la fois pour la génération de rapports et pour la gestion des incidents.

Nombre minimum et intervalles de réinitialisation

Certaines activités sont normales et acceptables lorsqu'elles sont inférieures à un certain taux d'occurrence. Mais, ces mêmes activités peuvent nécessiter une certaine attention lorsque leur taux d'occurrence dépasse un seuil tolérable. Par exemple, si un accès interactif à une base de données est autorisé, on peut s'attendre à un taux cohérent mais relativement bas d'échecs de connexion, tandis qu'un taux nettement plus élevé peut indiquer qu'une attaque est en train de se produire.

Pour gérer des seuils, un nombre minimum et un intervalle de réinitialisation peuvent être spécifiés pour chaque règle de politique. Cela peut être utilisé, par exemple, pour déclencher l'action associée à la règle lorsque plus de 100 échecs de connexion (nombre minimum) sont enregistrés dans un délai d'une minute (intervalle de réinitialisation). Si ces valeurs sont omises, par défaut, l'action associée à la règle est exécutée à chaque fois que la règle est satisfaite.

Case à cocher Passer à la règle suivante

Par défaut, l'évaluation de règles d'accès et d'exception pour une unité de trafic se termine lorsqu'une règle est déclenchée, à condition que la règle ne comporte pas plusieurs actions. Lorsqu'il est nécessaire d'exécuter plusieurs actions pour des conditions identiques ou semblables, cochez la case Passer à la règle suivante pour cette règle.

Remarque : La case à cocher Passer à la règle suivante s'applique aux règles d'accès qui suivent des règles d'accès et aux règles d'exception qui suivent des règles d'exception, mais pas à une règle d'exception qui suit une règle d'accès ni à une règle d'accès qui suit une règle d'exception.

Une règle d'extrusion est traitée quelle que soit la fin d'une règle d'accès ou d'exception qui la précède. Pour savoir comment exclure la consignation d'une réponse qui a déjà été sélectionnée pour être consignée par une précédente règle de la politique, voir les règles d'extrusion revoke dans le tableau de référence des définitions de règle à la fin de cette rubrique.

Case à cocher Enregistrer les valeurs avec la violation de politique

Lorsque cette case est cochée, l'enregistrement réel qui satisfait à la règle est consigné dans l'attribut de chaîne SQL et est disponible dans les rapports. Si cette case n'est pas cochée, aucune instruction SQL n'est consignée. Pour inclure les valeurs complètes dans la violation de politique, cochez la case $$Rec. Vals pour cette règle.

Remarque : L'instruction SQL complète avec des valeurs sera disponible uniquement dans l'enregistrement de violation de politique sur le domaine de génération de rapports de violations de politique. Elle ne sera pas disponible dans le journal du trafic client ni dans les rapports du domaine d'accès aux données. Pour inclure l'instruction SQL complète (avec ou sans valeurs de données) dans le journal du trafic client, utilisez les actions de règle Consigner la chaîne SQL complète.

Pour plus d'informations sur la gestion des règles, voir les rubriques suivantes :

- Affichage des règles définies dans la politique installée
- Spécification de valeurs et/ou de groupes de valeurs dans des règles
- Filtrage de règles pour afficher uniquement un sous-ensemble
- Copie de règles
- Utilisation de règles recommandées à partir de la liste de contrôle d'accès de la base de données
- Ajout ou édition de règles
- Utilisation du simulateur de politique

Spécification de valeurs et/ou de groupes de valeurs dans des règles

Pour un grand nombre d'attributs de règle, vous pouvez spécifier une valeur unique et/ou une valeur de groupe en utilisant des contrôles tels que ceux illustrés pour l'utilisateur de l'application.

Sachez qu'un membre de groupe peut contenir des caractères génériques (%), par conséquent, chaque membre d'un groupe peut correspondre à plusieurs valeurs réelles.

Lorsqu'un groupe est sélectionné, sachez qu'il peut contenir des caractères génériques.

- **Règle négative** : cochez la case Non pour créer une règle négative. Par exemple, pour exclure l'utilisateur d'application spécifié ou les membres du groupe sélectionné ou exclure à la fois l'utilisateur d'application spécifié et les membres du groupe sélectionné.
- Valeur vide : entrez la valeur spéciale guardium://empty pour rechercher la présence d'une valeur vide dans le trafic. Cela n'est autorisé que dans les champs suivants : Nom de base de données, Utilisateur de base de données, Utilisateur d'application, Utilisateur de système d'exploitation, Application source, Type d'événement, Nom d'utilisateur d'événement et Texte d'événement.
- Pour définir un nouveau groupe à tester, cliquez sur le bouton Groupes afin de définir un nouveau groupe, pus sélectionnez ce groupe dans la liste Groupe.
- Faire correspondre n'importe quelle valeur : laissez la zone de valeur vide et ne sélectionnez rien dans la liste Groupe (vérifiez que la ligne de tirets est sélectionnée, comme dans l'exemple).
- Faire correspondre uniquement une valeur spécifique : entrez cette valeur dans la zone de valeur et ne sélectionnez rien dans la liste Groupe.
- Faire correspondre n'importe quel membre d'un groupe : laissez la zone de valeur vide et sélectionnez le groupe dans la liste. Si le nombre minimum est supérieur à 1, il n'y aura qu'un seul compteur et il sera incrémenté chaque fois qu'une correspondance sera trouvée pour un membre du groupe.
- Faire correspondre une valeur individuelle ou n'importe quel membre d'un groupe : entrez une valeur spécifique dans la zone de valeur et sélectionnez un groupe dans la liste. Si le nombre minimum est supérieur à 1, il n'y aura qu'un seul compteur et il sera incrémenté chaque fois qu'une correspondance sera trouvée pour la valeur individuelle ou un membre du groupe.
- Si le nombre minimum est supérieur à 1, comptabilisez chaque valeur individuelle séparément : entrez un point (.) dans la zone de valeur et ne sélectionnez rien dans la liste Groupe. Notez que l'option de point ne peut pas être utilisée pour les zones Nom de service ou Protocole réseau. Si le nombre minimum est supérieur à 1, comptabilisez chaque membre d'un groupe séparément : entrez un point (.) dans la zone de valeur et sélectionnez un groupe dans la liste. Notez que l'option de point ne peut pas être utilisée pour les zones Nom de service ou Protocole réseau.

Mise en correspondance de modèles à l'aide d'expressions régulières

Outre des tests de modèle spéciaux, des expressions régulières peuvent être utilisées pour rechercher sur le trafic des modèles complexes dans les données. L'implémentation d'expressions régulières par Guardium est conforme à POSIX 1003.2 et diffère de l'implémentation d'expressions régulières par UNIX. Les expressions régulières sont autorisées dans tous les champs qui sont suivis par le bouton Générer une expression régulière.

Remarque : Vous pouvez également utiliser des expressions régulières dans les champs Utilisateur de base de données, Utilisateur d'application, Application source, Nom de champ, Objet et Texte de valeurs d'événement d'application en tapant la valeur spéciale guardium://regexp/(regular expression) dans la zone de texte correspondant à ces champs.
Remarque : IBM Security Guardium ne prend pas en charge d'expressions régulières pour les langues autres que l'anglais.
Pour des informations détaillées sur l'utilisation d'expressions régulières, consultez Expressions régulières.

- Tests de modèle spéciaux
  Vous pouvez utiliser ces tests de modèle spéciaux pour identifier les données sensibles contenues dans le trafic entre le serveur de base de données et le client.
- Actions associées à des règles
  Un certain nombre de facteurs doivent être pris en compte pour sélectionner l'action à entreprendre lorsqu'une règle est satisfaite.
- Création de politiques
  Vous pouvez non seulement créer des politiques, mais également les modifier, les cloner ou les retirer.
- Installation de politiques
  Utilisez cette rubrique pour installer la politique sur le collecteur Guardium et modifier le planning.
- Champs de définition de règle
  Vous pouvez utiliser ces champs lorsque vous définissez des règles de politique.
- Comment intégrer des règles personnalisées à une politique Guardium
  Cette section explique comment modifier/dériver automatiquement une politique Guardium à partir d'un système d'autorisation d'utilisation personnalisé.
- Comment utiliser l'action Ignorer appropriée
  Cette rubrique explique en détail de quelle façon les données sont gérées lorsque des actions Ignorer sont utilisées dans les règles de politique.
- Jeux de caractères
  Vous pouvez utiliser des codes de jeux de caractères dans des règles d'extrusion.

Rubrique parent : Protection

Tests de modèle spéciaux

Vous pouvez utiliser ces tests de modèle spéciaux pour identifier les données sensibles contenues dans le trafic entre le serveur de base de données et le client.

Chaque règle de politique inclut un test de modèle spécial. Pour utiliser l'un de ces tests, faites débuter le nom de la règle avec l'un des noms de test de modèle spéciaux, suivi d'un espace et d'un ou de plusieurs caractères supplémentaires, afin de rendre le nom de la règle unique. Par exemple, si vous recherchez les numéros de sécurité sociale de vos employés, vous pouvez nommer la règle comme suit : `guardium://SSEC_NUMBER employee`. Vous pouvez toujours indiquer tous les autres composants de la règle, tels que des adresses IP serveur et client spécifiques.

Ces tests correspondent à une trame de caractère, mais cette correspondance ne garantit pas que l'élément suspecté, par exemple, un numéro de sécurité sociale, a été trouvé. Des faux positifs peuvent être présents dans un grand nombre de cas, en particulier si des séquences de valeurs numériques plus longues sont concaténées dans les données.

guardium://CREDIT_CARD

Ce test permet de détecter les modèles de numéro de carte de crédit. Une chaîne de 16 chiffres ou quatre groupes de quatre chiffres, chaque groupe étant séparé par un espace, sont testés. Ce test de modèle spécial fonctionne également avec les modèles de numéro de carte de crédit American Express composés de 15 chiffres (premier groupe de chiffres 3 et second groupe de chiffres 4 ou 7). Par exemple : `1111222233334444` ou `1111 2222 3333 4444`

Lorsqu'un nom de règle commence par "guardium://CREDIT_CARD" et qu'un modèle de numéro de carte de crédit valide figure dans le champ Modèle de données, la politique utilise l'algorithme de Luhn, largement utilisé pour valider les numéros d'identification, tels que des numéros de carte de crédit, en plus de la correspondance de modèles standard. L'algorithme de Luhn est une vérification supplémentaire et ne se substitue pas à la vérification de modèle. Un numéro de carte de crédit valide est une chaîne de 16 chiffres ou quatre groupes de quatre chiffres, chaque groupe étant séparé par un espace. La zone d'expression de recherche doit obligatoirement contenir le nom de règle guardium://CREDIT_CARD et un nombre [0-9]{16} valide pour que l'algorithme de Luhn puisse être utilisé dans le cadre de cette mise en correspondance de modèle.

guardium://PCI_TRACK_DATA

Ce test permet de détecter deux modèles de données de piste magnétique. Le premier modèle est constitué d'un point-virgule (;), de 16 chiffres, d'un signe égal (=), de 20 chiffres et d'un point d'interrogation (?), par exemple :

```
;1111222233334444=11112222333344445555?
```

Le second modèle est constitué d'un symbole de pourcentage (%), du caractère B, de 16 chiffres, d'un carat (^), d'une chaîne de caractères de longueur variable terminée par une barre oblique (/), d'une seconde chaîne de caractères de longueur variable terminée par un carat (^), de 31 chiffres et d'un point d'interrogation (?), par exemple :

```
%B1111222233334444^xxx/xxxx x^11112222333344445555666677778888?
```

guardium://SSEC_NUMBER

Ce test permet de détecter des numéros dans un format de numéro de sécurité sociale : trois chiffres, un tiret (-), deux chiffres, un tiret (-), quatre chiffres, par exemple, `123-45-6789`. Les tirets sont requis.

guardium://CPF

Ce test correspond à Cadastro de Pessoas Físicas (CPF), un numéro d'identification personnel brésilien. Il contient 11 chiffres au format `nnn.nnn.nnn-nn`, les deux derniers chiffres étant des chiffres clés. Les chiffres clés sont calculés à partir des neuf chiffres d'origine et permettent de vérifier que le nombre est valide. Les caractères de formatage au sein de l'expression sont facultatifs. S'il existe une correspondance dans l'expression, les chiffres clés sont validés.

guardium://CNPJ

Ce test correspond à Cadastro Nacional de Pessoas Jurídicas (CNPJ), un numéro d'identification utilisé pour les sociétés brésiliennes. Il contient 14 chiffres au format `00.000.000/0001-00`, où :

- Les huit premiers numéros indiquent l'enregistrement.
- Les quatre numéros suivants identifient la branche de l'entité. 0001 est la valeur par défaut utilisée pour désigner les sièges sociaux.
- Les deux derniers numéros sont les chiffres clés.

Les caractères de formatage au sein de l'expression sont facultatifs. S'il existe une correspondance dans l'expression, les chiffres clés sont validés.

Rubrique parent : Politiques

Actions associées à des règles

Un certain nombre de facteurs doivent être pris en compte pour sélectionner l'action à entreprendre lorsqu'une règle est satisfaite.

Actions de blocage (S-TAP/S-GATE)

Cette section décrit l'action ARRET PAR S-TAP et les actions S-GATE.

Action ARRET PAR S-TAP

L'action ARRET PAR S-TAP met fin à une connexion de base de données (une session) et empêche l'exécution d'autres demandes sur cette session. Cette action est disponible dans S-TAP, que l'agent S-GATE soit utilisé ou non.

Remarque : Avec l'action ARRET PAR S-TAP, la demande de déclenchement n'est généralement pas bloquée, mais les autres demandes émises à partir de cette session sont bloquées (à un rythme soutenu, il peut arriver que plus d'une demande soit acceptée avant la fin de la session).

Actions S-GATE

S-GATE fournit la protection de base de données via S-TAP pour la connexion réseau et la connexion locale.

Lorsque S-GATE est disponible, toutes les connexions de base de données (sessions) sont évaluées et balisées pour être surveillées dans l'un des modes S-GATE suivants :

- Attached (valeur "on" définie pour S-GATE) – S-TAP est en mode de pare-feu pour cette session. Il contient les demandes de base de données et attend un verdict sur chaque demande avant de publier ses réponses. Lorsque ce mode est utilisé, un temps d'attente est prévu. Toutefois, il permet d'assurer que les demandes corrompues seront bloquées.
- Detached (valeur "off" définie pour S-GATE) - S-TAP est en mode de surveillance normal pour cette session. Il transmet les demandes au serveur de base de données sur-le-champ. Lorsque ce mode est utilisé, aucun temps d'attente n'est prévu.

La configuration de l'agent S-GATE définie dans le fichier "guard_tap.ini" spécifie le mode S-GATE par défaut ("associé" ou "dissocié") pour toutes les sessions, ainsi que les autres valeurs par défaut liées aux verdicts S-GATE lorsque le collecteur ne répond pas. Hormis avec sa configuration par défaut, l'agent S-GATE est contrôlé via le mécanisme de politique en temps réel utilisant les actions associées aux règles de politique S-GATE suivantes :

- ASSOCIATION DE L'AGENT S-GATE : affecte la valeur "Attached" au mode S-GATE pour une session spécifique.

  Destinée à être utilisée lorsque certains critères nécessitant de surveiller de plus près (et, le cas échéant, de bloquer) le trafic sur cette session sont remplis.
- DISSOCIATION DE L'AGENT S-GATE : affecte la valeur "Detached" au mode S-GATE pour une session spécifique.

  Destinée à être utilisée sur des sessions considérées comme "sécurisées" ou des sessions qui ne tolèrent aucun temps d'attente.
- ARRET PAR S-GATE : n'a d'effet que si la session est associée. Elle supprime la réponse de la demande bloquée derrière un pare-feu, ce qui met fin à la session sur certaines bases de données. La règle de politique ARRET PAR S-GATE provoque la fin anticipée d'une session précédemment surveillée.

Remarque :

- L'action d'arrêt par S-GATE/S-TAP ne fonctionne pas sur un groupe d'IP client dont les membres comportent des caractères génériques. L'action d'arrêt par S-GATE/S-TAP fonctionne uniquement avec une seule adresse IP. Les caractères génériques doivent être pris en charge par des groupes si le client souhaite utiliser plusieurs entrées IP. Le client peut créer des groupes d'utilisateurs/de clients approuvés ou non approuvés pour répondre à leurs besoins métier dans les politiques.
- Pour les agents A-TAP et S-GATE, des limites s'appliquent aux noyaux Linux de niveau inférieur. En fait, pour l'agent S-TAP 10.1.2 et plus, l'agent S-GATE est pris en charge partout, sauf sous Linux, lorsque l'agent A-TAP et les noyaux sont de niveau inférieur à 2.6.36.
- Pour les bases de données MySQL, il convient de noter que la connexion à la ligne de commande par défaut de MySQL est 'mysql -u<user> -p<pass> <dbname>'

  Lorsque ce mode est activé, MySQL mappe d'abord tous les objets et champs de cette base de données afin de prendre en charge la saisie automatique (avec la touche de tabulation).Lorsqu'une règle de fin est appliquée à un objet ou un champ impliqué dans ce mappage, elle désactive automatiquement la session de connexion. Pour éviter cela, connectez-vous à MySQL en utilisant l'indicateur "-A", ce qui aura pour conséquence de désactiver la fonction de saisie semi-

automatique et de ne pas déclencher la règle de fin. Une autre option consiste à ajuster la règle et à ne mettre fin à aucun des accès à ces objets/champs et à trouver une critère plus restreint qui ne déclenchera pas la règle dans la séquence de connexion.

Actions d'alerte

Les actions d'alerte envoient des notifications à un ou plusieurs récepteurs.

Pour chaque action d'alerte, plusieurs notifications peuvent être envoyées, et ces dernières peuvent être une combinaison d'un ou de plusieurs des types de notification suivants :

- Des e-mails, qui doivent être adressés aux utilisateurs Guardium et qui seront envoyés via le serveur SMTP configuré pour Guardium. Les autres récepteurs pour la notification par e-mail en temps réel sont l'auteur de l'appel (utilisateur qui a initié la commande SQL ayant déclenché la politique) et le propriétaire (propriétaire(s) de la base de données). L'auteur de l'appel et le propriétaire sont identifiés en procédant à l'extraction des ID utilisateur (basé sur IP) configurés via les API Guardium. L'option Association util-BD pour la sécurité des données (disponible via accessmgr) affiche le mappage (semblable à ce qui s'affiche si la commande d'API Guardium "list_db_user_mapping" est exécutée).
- Des alertes SNMP, qui seront envoyées à la communauté d'interception configurée pour le dispositif Guardium.
- Des messages Syslog, qui seront consignés dans syslog.
- Des notifications personnalisées, gestionnaires de notification écrits par l'utilisateur, implémentées en tant que classes Java™.

Remarque : La définition et la notification d'alertes ne sont pas soumis à la sécurité au niveau des données. Les raisons à cela sont notamment les suivantes : les alertes ne sont pas évaluées dans le contexte d'utilisateur, l'alerte peut être liée aux bases de données associées à plusieurs utilisateurs et pour éviter que personne ne reçoive la notification d'alerte.

Des modèles de message sont utilisés pour générer des alertes. Plusieurs modèles de message nommés sont créés et modifiés à partir du profil global. Il existe plusieurs types d'action d'alerte, chacun d'eux étant approprié pour un type de situation spécifique.

- L'action Alerter quotidiennement envoie des notifications uniquement la première fois que la règle est satisfaite chaque jour.
- L'action Alerter une fois par session envoie des notifications une seule fois pour chaque session dans laquelle la règle est satisfaite. Cette action peut être appropriée lorsque vous souhaitez savoir qu'un événement en particulier s'est produit, mais pas pour toutes les instances de cet événement au cours d'une session. Par exemple, vous souhaiterez peut-être qu'une notification soit envoyée lorsqu'un objet sensible en particulier est mis à jour. Or, si un programme met à jour des milliers d'instances de cet objet dans une session, il y a fort à parier que vous ne souhaiterez pas que des milliers de notifications soient envoyées aux récepteurs de l'alerte.
- Alerter uniquement - Pour cette action, avec le type syslog, le message est directement envoyé dans /var/log/messages. Pour les autres types de l'action Alerter uniquement, le message est envoyé dans le tableau MESSAGE. L'action Alerter uniquement n'envoie pas de notification relative aux violations de politique.
- L'action Alerter par correspondance envoie des notifications chaque fois que la règle est satisfaite. Cela convient pour une condition qui requiert systématiquement de l'attention.
- L'action Alerter par granularité temporelle envoie des notifications une fois par période de granularité de consignation. Par exemple, si la valeur affectée à la granularité de la consignation est Une heure, des notifications seront envoyées chaque heure, uniquement pour la première correspondance de la règle. (L'administrateur Guardium définit la granularité de la consignation sur le panneau Configuration de moteur d'inspection.)

Actions Consigner ou Ignorer

Ces actions contrôlent le niveau de consignation, basé sur le trafic observé.

Les commandes Consigner et Ignorer sont la plupart du temps toujours disponibles, mais l'action Effectuer l'audit uniquement est disponible uniquement pour une politique Trace d'audit sélectif. Les actions associées aux règles d'accès, aux règles d'exception et aux règles d'extrusion sont différentes. Cliquez sur le bouton Ajouter une action pour connaître les offres.

- Effectuer l'audit uniquement : disponible uniquement pour une politique Trace d'audit sélectif. Consigner l'événement qui a déclenché la règle. Pour une politique Trace d'audit sélectif, aucun enregistrement n'est consigné par défaut. Par conséquent, utilisez cette sélection pour indiquer ce qui est consigné. Avec l'API des événements d'application, vous devez utiliser cette action pour forcer la consignation des noms d'utilisateur de base de données, si vous souhaitez que ces informations soient disponibles pour la génération de rapports (sinon, dans ce cas, le champ Nom d'utilisateur n'est pas renseigné).
- Autoriser : en cas de correspondance, une violation de politique n'est pas consignée. Si l'action "Autoriser" est sélectionnée, aucune autre action ne peut être ajoutée à la règle. Les enregistrements sont consignés.
- Alerter et effectuer l'audit FAM (deux actions associées à des règles) - Alerter (en cas d'événement de mise en correspondance, déclencher une alerte (à l'aide du récepteur et du modèle))et Effectuer l'audit (consigner l'événement qui a déclenché la règle).
- Effectuer l'audit FAM uniquement - consigner l'événement qui a déclenché la règle.
- Ignorer FAM - ne pas consigner cet événement.
- Consigner uniquement les violations d'accès FAM - consigner les violations d'accès FAM.
- Consigner uniquement : consigner uniquement la violation de politique. Nous faisons référence au fait que la règle a été déclenchée en tant que violation de politique. A l'exception de l'action Autoriser, une violation de politique est consignée chaque fois qu'une règle est déclenchée (sauf si cette action supprime la consignation).
- Consigner les détails masqués : consigner l'ensemble de la chaîne SQL pour cette demande en remplaçant les valeurs par des points d'interrogation (???). Cette action est disponible pour les règles d'accès et les règles d'extrusion.
- Consigner l'ensemble des détails : consigner l'ensemble de la chaîne SQL et les données d'horodatage exactes pour cette demande. Voir les remarques dans la section Discussion plus approfondie et exemples.
- Consigner l'ensemble des détails avec les valeurs : semblable à l'action Consigner l'ensemble des détails, à ceci près que chaque valeur est stockée en tant qu'élément distinct (faire l'analyse syntaxique des valeurs et les consigner dans une table distincte dans la base de données). Cette action de consignation utilise davantage de ressources système car elle consigne les valeurs spécifiques des commandes pertinentes. Utilisez cette action de consignation uniquement lorsque vous devez générer des rapports contenant des conditions spécifiques sur ces valeurs. L'activation de cette action de consignation n'est pas disponible sans avoir préalablement consulté les services techniques (administrateur/Outils/Maintenance de la prise en charge).
- Consigner l'ensemble des détails par session : consigner l'ensemble de la chaîne SQL et les données d'horodatage exactes pour cette demande et pour le reste de la session.
- Consigner l'ensemble des détails avec les valeurs par session : voir les descriptions des actions Consigner l'ensemble des détails avec les valeurs et Consigner l'ensemble des détails par session. L'activation de cette action de consignation n'est pas disponible sans avoir préalablement consulté les services techniques (administrateur/Outils/Maintenance de la prise en charge).
- Ignorer la consignation : en cas de correspondance, ne pas consigner une violation de politique et cesser de consigner les enregistrements. Cette action est similaire à l'action Autoriser, mais en plus, elle arrête la consignation des enregistrements. Cette action supprime la consignation des enregistrements pour les demandes reconnues comme sans intérêt. GDM_CONSTRUCT est consigné dans certains cas, car l'analyse syntaxique/la consignation des enregistrements se produit avant que la règle ne soit appliquée. Toutefois, l'enregistrement n'est pas inclus dans la session. Cette fonction s'applique également aux règles d'exception

pour les codes d'erreur de base de données uniquement. Cela permet aux utilisateurs de ne pas consigner d'erreurs lorsqu'une application génère une importante quantité d'erreurs et que les utilisateurs n'ont pas les moyens de les arrêter.

- Ignorer les réponses par session : les réponses pour le reste de la session sont ignorées. Cette action ne consigne pas une violation de politique, mais elle cesse d'analyser les réponses pour le reste de la session. Cette action s'avère utile lorsque vous savez que la réponse de base de données sera sans intérêt. Cette action fonctionne lors de l'utilisation d'un sniffer pour les données d'un agent S-TAP. Cette action ne fonctionne pas lors de l'utilisation d'un sniffer pour les données d'un port SPAN.
  Remarque : Concernant l'action Ignorer les réponses par session, dans la mesure où le sniffer est ignoré ou ne reçoit aucune réponse pour la requête, les valeurs pour COUNT_FAILED et SUCCESS correspondent à ce qui est indiqué par défaut dans la table, en l'occurrence, COUNT_FAILED=0 et SUCCESS=1.
- Ignorer la session : La demande en cours et le reste de la session sont ignorées. Cette action ne consigne pas les violations de politique, mais elle interrompt la consignation des enregistrements, et elle ne recherche pas les violations de politique, quel que soit leur type, dans le reste de la session. Cette action peut s'avérer utile si, par exemple, la base de données comporte une région de test et qu'il n'est pas nécessaire d'appliquer des règles de politique à cette région de la base de données. Les règles Ignorer la session fournissent la méthode la plus efficace pour filtrer le trafic. Avec une règle Ignorer la session, les activités depuis des sessions individuelles sont supprimées par l'agent S-TAP ou complètement ignorées par le sniffer.Remarque : les informations de session (connexion/déconnexion) sont toujours consignées, même si la session est ignorée.
- Ignorer la session S-TAP : la demande en cours et le reste de la session S-TAP sont ignorées. Cette action est exécutée en même temps que sont spécifiés sur l'écran de menu du générateur de politique de certains systèmes, les utilisateurs ou les applications qui produisent un volume élevé de trafic réseau. Cette action s'avère utile lorsque vous savez que la réponse de base de données provenant de la session S-TAP sera sans intérêt. Deux options sont possibles pour l'action Ignorer la session S-TAP : IGNORE_ENTIRE_STAP_SESSION, action Ignorer de type physique qui ne peut pas être révoquée, et IGNORE_STAP_SESSION (REVOCABLE), action Ignorer de type logique qui permet de renvoyer le trafic de session sans avoir à se reconnecter à la base de données. Remarque concernant ignore_stap_session (revocable) - la révocation de la commande Ignorer la session S-TAP est permanente pour l'hôte S-TAP dans un processus sniffer. Les nouvelles sessions ouvertes après la révocation de la commande Ignorer pour l'hôte S-TAP ne seront PAS ignorées (même si la règle IGNORER LA SESSION S-TAP (REVOCABLE) est déclenchée). Commande REVOKE Ignore - Les sessions qui ont été ignorées par l'action "IGNORER LA SESSION S-TAP (REVOCABLE)" seront reprises, ce qui signifie que le trafic sera envoyé au système Guardium après que la commande "REVOKE Ignore" aura été reçue par l'agent S-TAP. (Cette commande peut être envoyée à partir du contrôle S-TAP -->commande Send.)
- Ignorer SQL par session : aucune chaîne SQL n'est consignée pour le reste de la session. Les exceptions seront toujours consignées, mais il se peut que les chaînes correspondantes ne soient pas capturées par le système.
- Consigner le compteur d'extrusion : disponible uniquement pour les règles d'extrusion, cette action met à jour le compteur, mais ne consigne pas les données renvoyées. Cette action permet d'économiser de l'espace disque lorsque la valeur de compteur est la plus importante et que les valeurs renvoyées sont les moins importantes.
- Consigner le compteur d'extrusion masqué : disponible uniquement pour les règles d'extrusion, cette action met à jour le compteur, consigne la demande SQL, en remplaçant les valeurs par des points d'interrogation, ne consigne pas les données renvoyées (réponse).
- Mettre en quarantaine : disponible pour les règles d'accès, d'exception et d'extrusion, cette action a pour objectif d'empêcher un utilisateur de se connecter à un serveur pendant une période donnée. Il existe un élément de validation : vous ne pouvez pas avoir une règle associée à une action METTRE EN QUARANTAINE si vous n'avez pas indiqué la période pendant laquelle l'utilisateur est mis en quarantaine. Voir la section sur l'option Quarantaine pour (minutes) pour définir la période de mise en quarantaine. Si la session est surveillée (scénario S-GATE), envoyez un verdict de suppression. Si la session n'est pas surveillée (scénario ARRET PAR S-TAP), faites en sorte que l'agent S-TAP arrête la session. Prenez l'heure en cours et ajoutez-la au nombre de minutes dans le champ Intervalle de réinitialisation. Vous obtenez un nouvel horodatage. Dans une nouvelle structure, vous conservez une liste triée (triée par cet horodatage). Outre la valeur d'horodatage, chaque élément comporte une adresse IP de serveur, un type de serveur, un nom d'utilisateur de base de données, un nom de service et un indicateur spécifiant s'il s'agissait ou non d'une session surveillée.
- Aucune analyse : ne pas faire une analyse syntaxique de l'instruction SQL.
- Analyse rapide - aucun champ : ne pas faire une analyse syntaxique des champs contenus dans l'instruction SQL. Les règles d'analyse rapide sont toutes appliquées uniquement si la chaîne SQL comporte plus de 100 caractères.
- Analyse rapide - éléments natifs : utilisé uniquement pour Guardium S-TAP for DB2 on z/OS. Utilisez cette action de règle lorsqu'un trafic élevé surcharge le processus sniffer. L'utilisation de cette règle d'action doit permettre d'améliorer les performances de l'agent S-TAP for DB2 on z/OS.
- Analyse rapide : s'applique uniquement aux règles d'accès. Pour le reste de la session, ne pas faire une analyse syntaxique de l'instruction SQL. Cela réduit le temps d'analyse syntaxique. Dans ce mode, tous les objets consultés peuvent être identifiés (dans la mesure où les objets apparaissent avant la clause WHERE), mais les instances d'objet spécifiquement affectées ne sont pas connues, car c'est la clause WHERE qui permet d'obtenir cette information.
- Expurger : s'applique uniquement aux règles d'extrusion. Cette fonction permet à un client de masquer certaines parties d'un résultat de requête de base de données (par exemple, des numéros de carte de crédit) dans les rapports destinés à certains utilisateurs. L'option Caractère de remplacement dans la section Modèle de données du menu de règle d'extrusion définit le caractère de masquage. Si la sortie produite par la règle d'extrusion correspond à l'expression régulière du modèle de données, les parties qui correspondent aux sous-expressions placées entre parenthèses "(" et ")" seront remplacées par le caractère de masquage. Des expressions régulières prédéfinies (expression régulière rapide) peuvent également être utilisées. Consultez Modèle de données dans Champs de définition de règle pour plus d'informations.
  Restriction :
  - L'expurgation ne fonctionne pas sur les sessions ouvertes après une mise à niveau "live" des agents S-TAP.
  - La fonction d'expurgation ne fonctionne pas sur les tables créées avec un type de champ et de numéro.
  - Modèle SQL n'est pas pris en charge pour les règles d'expurgation.
- Enregistrer les valeurs séparément/Ne pas enregistrer les valeurs séparément : cette action est une règle d'accès basée sur une session. Utilisée dans la fonction de réexécution pour distinguer les différentes transactions.
- Marquer en indiquant que la validation automatique est activée/Marquer en indiquant que la validation automatique est désactivée : cette action est une règle d'accès basée sur une session. Utilisée dans la fonction de réexécution en raison de différents modèles de validation automatique pour différentes bases de données.
- Audit z/OS : utilisée spécifiquement pour les règles de politique de profil de collecte z/OS (IMS, jeux de données et Db2), qui sont utilisées pour spécifier le trafic qui doit être collecté sur le serveur z/OS. Cette action indique que le trafic qui répond aux critères de filtrage est envoyé au collecteur. Il s'agit de la seule et unique action pouvant être spécifiée sur une règle de profil de collecte.

Remarque :

La fonction d'expurgation (nettoyage) sur Linux est prise en charge à compter de la version 9.1. Pour toutes les plateformesUNIX, la fonction de nettoyage est prise en charge uniquement avec des jeux de caractères ANSI.

Les règles d'expurgation (nettoyage) doivent être définies au niveau session (autrement dit, les règles de déclenchement sur les attributs de session, tels que Adresses IP, Utilisateurs, etc.) et non au niveau/sur les attributs SQL (par exemple, OBJECT_NAME ou VERB), car si vous définissez la règle de nettoyage sur la chaîne SQL qui doit être nettoyée, il faudra quelques millisecondes aux instructions de nettoyage pour atteindre l'agent S-TAP et par conséquent, certains résultats pourront être transmis non masqués.

Pour s'assurer que toutes les chaînes SQL sont nettoyées, affectez la valeur "attach" au mode par défaut de l'agent S-TAP (S-GATE) pour toutes les sessions (dans guard_tap.ini). Ainsi, aucune commande ne sera transmise sans être inspectée par le moteur de règles et retenir chaque demande et attendre le verdict de la politique sur la demande.Ce déploiement introduit un certain temps d'attente, mais il permet de garantir que 100 % des données sont nettoyées.

Pour la base de données Informix, lorsque Char est utilisé comme type de données, aucune chaîne ne se termine par un caractère Null à la fin de chaque colonne. Par conséquent, les quatre colonnes sont capturées en même temps dans l'appel système sendmsg. L'agent K-TAP essaiera toujours d'expurger les données qu'il capture, quelles qu'elles soient. Cette limitation s'applique lors de l'utilisation de la fonction d'expurgation et de la base de données Informix.

Remarque :

Pour la prise en charge HTTP, il existe des limitations qui s'appliquent aux actions de politique. Les actions de politique suivantes ne sont pas prises en charge pour HTTP : Arrêt par S-TAP et Ignorer la consignation.

HTTP ne prend pas en charge les autres actions suivantes :

- Ignorer les réponses par session, car HTTP ne prend pas en charge les règles d'exception et d'extrusion.
- Ignorer SQL par session, car HTTP ne contient pas de chaînes SQL.
- Mettre en quarantaine : cette action est utilisée pour mettre un utilisateur en quarantaine, mais HTTP ne prend pas en charge DBUser et OSUser.
- Analyse rapide : cette action s'applique aux instructions SQL de consignation.
- Arrêt par SGate : cette action n'est pas prise en charge pour Hadoop - aucune des actions d'arrêt ne fonctionne pour HTTP.

Pour les conditions de politique : ces conditions ne sont pas prises en charge pour HTTP :

MAC client, Nom de base de données, Utilisateur de base de données, Utilisateur d'application, Utilisateur de système d'exploitation, Application source, Modèle de masquage, Caractère de remplacement, Quarantaine pour minutes, Seuil des enregistrements affectés, Modèle XML, Type d'événement, Nom d'utilisateur d'événement, Texte de valeurs d'événement d'application, Groupe de texte de valeurs d'événement d'application, Texte et groupe de valeurs d'événement d'application, Numérique, Date.

Discussion plus approfondie et exemples

Consigner l'ensemble des détails

Par défaut, le collecteur Guardium masque toutes les valeurs lors de la consignation d'une chaîne SQL. Par exemple,

```
insert into tableA (name,ssn,ccn) values ('Bob Jones', '429-29-2921','29249449494949494')
```

est consigné comme suit : `insert into tableA (name,ssn,ccn) values (?, ?,?)`. Les raisons de ce comportement par défaut sont les suivantes :

1. Les valeurs ne doivent pas être consignées par défaut car elles peuvent contenir des informations sensibles.
2. La consignation sans spécifier de valeurs peut fournir des performances système accrues et une période de conservation de données prolongée au sein du dispositif. Très souvent, le trafic de base de données correspond à un grand nombre de demandes SQL, identiques en tout point, à l'exception de leurs valeurs, répétées des centaines, des milliers ou des millions de fois par heure. En masquant les valeurs, Guardium peut agréger ces demandes SQL répétées en une seule demande, appelée "enregistrement". Lorsque des enregistrements sont consignés, au lieu d'être consignée séparément, chaque demande/enregistrement SQL est consignée une fois par heure (par session) avec le nombre de fois où l'enregistrement a été exécuté. Cela permet d'économiser une quantité significative d'espace disque car au lieu de créer des centaines (ou des millions) de lignes dans la base de données, une seule nouvelle ligne est ajoutée.

Avec l'action Consigner l'ensemble des détails, Guardium consigne les données avec les valeurs non masquées et chaque demande distincte. L'action Consigner l'ensemble des détails fournit des données d'horodatage exactes, tandis que la consignation sans les détails indique l'horodatage le plus récent d'un enregistrement au sein de la période de granularité de la consignation (généralement, une heure).

Ignorer la session S-TAP - avec cette action, le collecteur envoie à l'agent S-TAP un signal lui indiquant qu'il doit arrêter d'envoyer du trafic, sauf pour les notifications de déconnexion pour certaines sessions. Par exemple, si vous possédez une règle indiquant `where DBUserName?=scott, Ignore S-TAP Session` :

- Lorsque Scott se connecte au serveur de base de données, l'agent S-TAP envoie les informations de connexion au collecteur.
- Le collecteur consigne la connexion. Les informations de session (connexion/déconnexion) sont toujours consignées.
- Le collecteur envoie un signal à l'agent S-TAP pour lui demander de cesser d'envoyer du trafic à partir de cette session spécifique. Cela signifie que les commandes exécutées par Scott sur le serveur de base de données et les réponses (ensembles de résultats, erreurs SQL, etc.) envoyées par le serveur de base de données seront supprimées par l'agent S-TAP et n'atteindront jamais le collecteur.
- Lorsque Scott se déconnecte du serveur de base de données, l'agent S-TAP envoie ces informations au collecteur (les informations de connexion/déconnexion font toujours l'objet d'un suivi même si la session est ignorée).
- Lorsque Scott se reconnecte, ces étapes sont répétées. La logique selon laquelle les sessions doivent être ignorées est maintenue par le collecteur et non par l'agent S-TAP.

Attention, il est toujours très important d'inclure des règles Ignorer la session dans la politique même s'il s'agit d'une politique Trace d'audit sélectif. Les règles Ignorer la session diminuent considérablement la charge sur un collecteur car en filtrant les informations au niveau de l'agent S-TAP, le collecteur ne les reçoit jamais et n'a pas besoin de consommer des ressources en analysant du trafic qui en définitive ne sera pas consigné. Si une politique Trace d'audit sélectif ne comporte pas de règle Ignorer la session, tout le trafic sera envoyé depuis le serveur de base de données vers le collecteur, amenant ainsi ce dernier à analyser chaque commande et ensemble de résultats générés par le serveur de base de données.

Utilisation d'instructions par lots MS-SQL ou Sybase dans une application Guardium

Limitation

La réussite ou l'échec des commandes SQL dans les instructions par lots MS-SQL ou Sybase peut ne pas s'afficher correctement.

Les instructions par lots MS-SQL ou Sybase sont principalement utilisées pour la création de procédures complexes.

Si vous exécutez des instructions SQL séparément, le statut de chacune d'elles fait l'objet d'un suivi spécifique et la valeur de succès ou d'échec appropriée s'affiche.

Lorsque des instructions SQL (dans MS-SQL ou Sybase) sont exécutées par lots, le statut renvoyé correspond à la dernière instruction du lot.

Exemple Guardium

[Start of SQL batch]

SQL 1 statement - failed

SQL 2 statement - failed

SQL 3 statement - success

[End of SQL batch]

Dans l'application Guardium, seule l'indication de succès ou de réussite de la dernière instruction SQL est signalée dans une instruction par lots MS-SQL ou Sybase. Dans ce cas, la réussite est indiquée pour l'instruction par lots MS-SQL ou Sybase, même si SQL 1 et SQL 2 ont échoué.

Définir le jeu de caractères

Vous pouvez utiliser une action dans le cadre d'une règle d'extrusion de politique afin d'associer des jeux de caractères de remplacement à la session.

Règles de modèle spécial avec des jeux de caractères

Exemple de règle d'extrusion (avec suggestion) :

Jeu de caractères EUC-JP (code 274).

Modèle de règle d'extrusion : `guardium://char_set?hint=274`

Résultat : une règle d'extrusion est associée à la session et l'analyseur utilisera EUC-JP dans la session, s'il n'existe aucun autre jeu de caractères.

Exemple de règle d'extrusion (avec contrainte) :

Jeu de caractères EUC-JP (code 274).

Modèle de règle d'extrusion : `guardium://char_set?force=274`

Résultat : une règle d'extrusion est associée à la session et l'analyseur utilisera systématiquement le jeu de caractères EUC-JP dans la session. Le jeu de caractères utilisé précédemment sera remplacé par EUC-JP.

Gardez à l'esprit que les règles d'extrusion sont généralement associées à la session avec un certain délai. Par conséquent, les sessions courtes ou le début de la session ne sont pas immédiatement affectés par un changement de jeu de caractères. Le schéma fonctionne pour Oracle, Sybase, MY SQL et MS SQL.

Règles d'analyseur

Certaines règles peuvent être appliquées au niveau analyseur. Exemples de règles d'analyseur : jeux de caractères définis par l'utilisateur, changements de programme source et émission de verdicts de surveillance pour le mode pare-feu. Dans les éditions précédentes, les politiques et les règles étaient appliquées à la fin du traitement de la requête, au niveau de l'état de consignation. Dans certains cas, cela retardait la prise de décisions basées sur ces règles. Lorsque les règles sont appliquées au niveau de l'analyseur, les décisions peuvent être prises à un stade moins avancé.

Consigner données brutes

L'option Consigner données brutes indiquée dans la définition de politique ou le générateur de politique permet au dispositif Guardium de consigner des informations sans en faire immédiatement une analyse syntaxique.

Cela permet d'économiser des ressources de traitement et, ainsi, de prendre en charge un trafic plus important. L'analyse syntaxique et la fusion de ces données sur la base de données interne de Guardium peuvent être effectuées ultérieurement, soit sur un collecteur, soit sur un agrégateur.

Lorsque l'option Consigner données brutes (processus Flat Log) est cochée :

- Les données ne sont pas soumis à une analyse syntaxique en temps réel
- Les processus Flat Log sont visibles dans un rapport Liste Flat Log attribué
- Le processus hors ligne pour l'analyse syntaxique des données et leur fusion sur des domaines d'accès standard peut être configuré via les options Gestion > Surveillance des activités > Processus Flat Log.

Règles sur données brutes

Cette section décrit les différences en termes d'utilisation de l'action Règles sur données brutes.

Lorsque l'option Règles sur données brutes est cochée :

- Les règles de niveau session sont examinées en temps réel
- Aucune règle n'est évaluée lorsque le traitement hors ligne s'effectue

Lorsque l'option Règles sur données brutes n'est pas cochée :

- Les règles de politique se déclenchent lors du traitement à l'aide de la politique installée

Remarque : L'action Règles sur données brutes ne fonctionne pas avec des règles de politique impliquant un champ, un objet, un verbe SQL (commande), un groupe d'objets/de commandes et un groupe d'objets/de champs. Dans le processus Flat Log, "flat" signifie qu'un arbre de syntaxe n'est pas généré. En l'absence d'arbre de syntaxe, les champs, les objets et les verbes SQL ne peuvent pas être déterminés.

Les actions suivantes ne fonctionnent pas avec des règles sur des politiques non hiérarchiques : LOG_FULL_DETAILS, LOG_FULL_DETAILS_PER_SESSION, LOG_FULL_DETAILS_VALUES, LOG_FULL_DETAILS_VALUES_PER_SESSION, LOG_MASKED_DETAILS.

Utilisation de l'option Trace d'audit sélectif

Utilisez l'option Trace d'audit sélectif dans la section Définition de politique de la sous-fenêtre Générateur de politique pour limiter la quantité de données consignées sur le dispositif Guardium.

ce choix est approprié lorsque le trafic d'intérêt constitue un pourcentage relativement faible du trafic accepté par les moteurs d'inspection ou lorsque tout le trafic pour lequel vous pourriez souhaiter générer un rapport peut être complètement identifié.

Lorsque l'option Trace d'audit sélectif n'est pas cochée, le dispositif Guardium consigne tout le trafic accepté par les moteurs d'inspection. Chaque moteur d'inspection sur le dispositif ou sur un agent S-TAP est configuré pour surveiller un protocole de base de données spécifique (Oracle, par exemple) sur un ou plusieurs ports. De plus, le moteur d'inspection peut être configuré pour accepter le trafic provenant de sous-réseaux de connexions client-serveur. Cette situation tend à capturer davantage d'informations que lorsque la case à cocher Trace d'audit sélectif est cochée, mais peut obliger le dispositif Guardium à traiter et stocker beaucoup plus d'informations que nécessaire afin de répondre à vos exigences en matière de sécurité et de réglementation.

Lorsqu'une politique Trace d'audit sélectif est installée, seul le trafic demandé par la politique est consigné, et il existe deux façons d'identifier ce trafic :

- En spécifiant une chaîne qui peut être utilisée pour identifier le trafic d'intérêt, dans le champ Modèle d'audit du panneau Définition de politique. Cela peut permettre d'identifier une base de données ou un groupe de tables de base de données, par exemple. Notez qu'un modèle d'audit est un modèle appliqué (via une correspondance d'expressions régulières) à chaque chaîne SQL que le consignateur traite pour voir si elles correspondent. Ce modèle de correspondance est uniquement une correspondance de chaînes. Il ne fonctionne pas avec les variables de session (nom de base de données, etc.) comme c'est le cas pour les règles de politique.
- Ou, en spécifiant l'option Effectuer l'audit uniquement ou n'importe laquelle des actions Consigner (Consigner uniquement, Consigner l'ensemble des détails, etc.) pour une ou plusieurs des règles de politique dans un panneau Définition de règle. L'utilisation de règles de politique vous permet d'être très précis, en spécifiant des valeurs exactes, des groupes ou des modèles à mettre en correspondance avec chaque type d'attribut imaginable (Type de base de données, Nom de base de données, Nom d'utilisateur, etc.)..

Si l'option Trace d'audit sélectif est activée pour la politique de sécurité Guardium et qu'une règle a été créée sur un groupe d'objets, la chaîne sur chaque élément du groupe est vérifiée. Si une correspondance est trouvée, la décision est prise de consigner les informations et de poursuivre. Si l'option Trace d'audit sélectif est activée pour la politique de sécuritéGuardium et qu'une règle a été créée sur un groupe d'objets avec une condition NON sur celui-ci, il est toujours nécessaire de vérifier la chaîne sur chaque élément du groupe et de décider de consigner les informations et de poursuivre uniquement si aucune correspondance n'est trouvée pour les éléments. Les règles incluant une condition NON se comportent comme des règles normales lorsqu'elles sont utilisées avec l'option Trace d'audit sélectif.

Cela inclut :

- Des situations OU, par exemple, des règles basées sur plusieurs objets ou commandes
- Des situations avec deux conditions NON (par exemple, la partie NON d'un groupe d'objets et la partie NON d'un groupe de commandes), et
- Des situations avec une condition NON et une condition OUI (par exemple, la partie NON d'un groupe d'objets et la partie OUI d'un groupe de commandes

Remarque : Les instructions SELECT comportant des indices de requête, par exemple, SELECT /*+ ORDERED USE_MERGE(m) */ SELECT /*+ ORDERED */ SELECT /*+ all_rows */ etc., sont autorisées à passer par l'analyseur syntaxique et sont consignées quelle que soit la définition de règle utilisée pour les ignorer (au moins avec le mode d'audit sélectif). Cela est dû au fait qu'une politique d'audit sélectif ne doit pas empêcher la consignation de certaines chaînes SQL qui peuvent être nécessaires pour d'autres fonctions, comme la conversion d'utilisateur d'application.

Option Trace d'audit sélectif et API d'événements d'application

Lorsqu'une politique Trace d'audit sélectif est utilisée et que des utilisateurs ou des événements d'application sont définis via l'API d'événements d'application, la politique doit inclure une règle Effectuer l'audit uniquement qui se déclenche chaque fois qu'un événement de définition/d'effacement d'application ou une commande de définition/d'effacement d'utilisateur d'application sont détectés. Consultez Identification des utilisateurs via une API pour des informations sur la définition de l'utilisateur d'application via l'API Evénements d'application.

Option Trace d'audit sélectif et conversion d'utilisateur d'application

Lorsqu'une politique Trace d'audit sélectif est utilisée, une conversion d'utilisateur d'application est également utilisée :

- La politique ignore tout le trafic qui ne répond pas à la règle de conversion d'utilisateur d'application (par exemple, qui ne provient pas du serveur d'applications).
- Seules les chaînes SQL qui correspondent au modèle défini pour cette politique seront disponibles pour les rapports de conversion d'utilisateur d'application spéciaux.

Option Trace d'audit sélectif et spécification d'un groupe vide

Un groupe de tuples vide associé à une règle NE provoque PAS la mise en correspondance d'une action associée à la règle.

Rubrique parent : Politiques

Création de politiques

Vous pouvez non seulement créer des politiques, mais également les modifier, les cloner ou les retirer.

création d'un politique

Utilisez cette section pour créer une politique. Les étapes de cette procédure sont décrites après les champs de menu de l'écran Générateur de politique.

Procédez comme suit :

1. Cliquez sur Configuration > Générateur de politique pour ouvrir le panneau Localiseur de politique ou cliquez sur Protection > Politiques de sécurité > Générateur de politique pour ouvrir le panneau Localiseur de politique.
2. Une série de politiques prédéfinies (disponibles pour clonage) avec des règles d'accès, d'exception et d'extrusion a été créée pour les événements de base de données démontrant que des tentatives visant à mettre en échec les mécanismes de protection ont eu lieu. Les événements de ce type, qui génèrent des actions de journal ou des alertes, sont les suivants : échecs de connexion et erreurs SQL de la part de certains groupes ou serveurs, accès à certains objets de base de données par certains utilisateurs ou groupes, tentatives de changement de commandes SQL GRANT, etc. Ces politiques prédéfinies facilitent et accélèrent la création de politiques de conformité. Par exemple, GDPR, Basel II et PCI.
   Avertissement : Si une version [modèle] d'une politique prédéfinie est disponible, il est déconseillé d'utiliser l'ancienne version (non marquée [modèle]), car elle ne sera plus mise à jour. Clonez la version [modèle] et personnalisez-la selon nécessité.
3. Clonez une politique prédéfinie ou cliquez sur Nouveau pour ouvrir le panneau Définition de politique.
4. Entrez un nom unique pour la politique dans le champ Description de politique. Vous ne devez pas ajouter d'apostrophe dans la description.
5. Facultatif. Entrez une catégorie dans le champ Catégorie. Une catégorie est un libellé arbitraire pouvant servir à regrouper des violations de politique à des fins de génération de rapports. La catégorie spécifiée ici sera utilisée comme catégorie par défaut pour chaque règle (et pourra être remplacée dans la définition de règle).
6. Facultatif. Sélectionnez une base de référence à utiliser à partir de la liste Base de référence de politique. Assurez-vous que la base de référence sélectionnée a été générée. Si tel n'est pas le cas, l'outil Générateur de politique ne pourra pas suggérer de règles à partir de cette base de référence. Si la base de référence que vous

souhaitez utiliser ne s'affiche pas dans la liste, cela signifie qu'aucun rôle de sécurité autorisé à utiliser cette base de référence n'a été affecté à votre ID utilisateur Guardium. Pour plus d'informations, prenez contact avec votre administrateur Guardium.

Si la politique comporte une base de référence, au départ, sa définition ne contiendra que la base de référence, et l'action associée à une base de référence consiste à toujours autoriser la commande sans passer à la règle suivante.

Lorsque vous ajoutez une base de référence à une politique existante, elle est ajoutée en tant que première règle. Vous pouvez déplacer la règle de la base de référence vers n'importe quel emplacement dans la politique. (Notez que si vous déplacez la base de référence en tant que dernière règle, elle n'a aucun effet.)

Avertissement : Le générateur de base de référence et la fonctionnalité connexe sont dépréciées depuis Guardium version 10.1.4.

7. Vous pouvez éventuellement cocher la case Consigner données brutes pour indiquer que Guardium doit consigner des données, mais pas analyser et agréger les données dans la base de données interne.
8. Si la case Consigner données brutes est cochée, vous pouvez éventuellement cocher la case Règles sur données brutes pour appliquer les règles de politique aux données de consignation brute (par opposition aux données agrégées).
9. Vous pouvez éventuellement cocher la case Trace d'audit sélectif pour limiter les informations consignées lorsque cette politique est installée :
    - Lorsque cette case est cochée, seul le trafic demandé par cette politique est consigné. Cela convient lorsque le trafic d'intérêt représente un pourcentage relativement faible du trafic observé par les moteurs d'inspection. Lorsque cette case est cochée, il existe deux manières de signaler le trafic qui doit être consigné : en spécifiant une chaîne qui peut être utilisée pour identifier le trafic d'intérêt, dans le champ Modèle d'audit, ou en spécifiant l'option Effectuer l'audit uniquement ou n'importe laquelle des actions de consignation pour une ou plusieurs règles de politique (les actions associée aux règles sont décrites ultérieurement).
    - Lorsque cette case n'est pas cochée (par défaut), le dispositif Guardium consigne tout le trafic observé par les moteurs d'inspection. Vous disposez ainsi de fonctions de trace d'audit complètes, mais cela peut entraîner la capture et l'analyse de plus d'informations que nécessaire.
    - Pour plus d'informations, voir Utilisation de la trace d'audit sélectif.
10. Cliquez sur Sauvegarder pour sauvegarder la définition de politique.
11. Cliquez éventuellement sur Rôles afin d'affecter des rôles pour la politique.
12. Cliquez éventuellement sur Commentaires pour ajouter des commentaires à la définition.

Etapes suivantes

Après avoir créé une nouvelle définition de politique, utilisez le panneau Localiseur de politique pour accéder à cette définition. Créez la définition de politique en effectuant une ou plusieurs des tâches suivantes :

- Créez des règles de politique manuellement. Voir Ajout ou édition de règles.
- Si la politique comporte une base de référence, faites en sorte que le générateur de politique suggère des règles à partir de cette base de référence. Vous pouvez éventuellement accepter ou personnaliser les règles générées, en fonction de vos besoins. Voir la section Utilisation de règles recommandées à partir de la base de référence.
- Faites en sorte que le générateur de politique suggère des règles à partir de la liste de contrôle d'accès définie pour cette base de données. Vous pouvez rejeter ou accepter et éventuellement personnaliser chaque règle, selon vos besoins. Voir la section Utilisation de règles recommandées à partir de la liste de contrôle d'accès de la base de données.

Modification/Clonage/Retrait d'une politique

Cette section décrit la procédure à suivre pour modifier, cloner ou retirer une politique.

Modification d'une politique

Attention, avant de modifier une définition de politique, assurez-vous d'avoir bien compris ce qu'implique la modification d'une politique en cours d'utilisation. Si la politique existante doit être réinstallée avant la fin de toutes les révisions, il se peut que cette installation échoue ou que les résultats que vous obtenez après la réinstallation de la politique ne soient pas conformes à vos attentes. Par conséquent, il est préférable de cloner la politique, de sorte que l'original puisse toujours être réinstallé.

1. Cliquez sur Configuration > Générateur de politique pour ouvrir le panneau Localiseur de politique ou cliquez sur Protection > Politiques de sécurité > Générateur de politique pour ouvrir le panneau Localiseur de politique.
2. Dans la liste Description de politique, sélectionnez la politique à modifier.
3. Effectuez l'une des actions suivantes :
    - Pour éditer les paramètres de politique globaux (catégorie, option Consigner données brutes, etc.), cliquez sur Modifier. Pour changer l'un de ces paramètres, voir la section Création d'une politique.
    - Pour éditer les règles uniquement, cliquez sur Editer les règles. Pour modifier des composants des définitions de règle, voir la section Ajout ou édition de règles.

clonage d'une politique

Dans un certain nombre de situations, vous souhaiterez peut-être définir une nouvelle politique à partir d'une politique existante, sans modifier la définition d'origine.

1. Cliquez sur Configuration > Générateur de politique pour ouvrir le panneau Localiseur de politique ou cliquez sur Protection > Politiques de sécurité > Générateur de politique pour ouvrir le panneau Localiseur de politique.
2. Dans la liste Description de politique, sélectionnez la politique à cloner.
3. Cliquez sur Cloner pour ouvrir le panneau Cloner une politique.
4. Entrez un nom unique pour la nouvelle politique dans le champ Nouveau nom. N'incluez pas d'apostrophe.
5. Pour cloner les enregistrements de base de référence (principalement, les commandes) qui ont été générés pour la base de référence qui fait l'objet d'un clonage, cochez la case Cloner enregistrements.
6. Cliquez sur Sauvegarder pour sauvegarder la nouvelle politique. Vous pouvez alors ouvrir et éditer la nouvelle politique à l'aide du panneau Localiseur de politique. Voir la section Modification d'une politique.

Retrait d'une politique

1. Cliquez sur Configuration > Générateur de politique pour ouvrir le panneau Localiseur de politique ou cliquez sur Protection > Politiques de sécurité > Générateur de politique pour ouvrir le panneau Localiseur de politique.
2. Dans la liste Description de politique, sélectionnez la politique à cloner.
3. Cliquez sur le bouton Supprimer. Vous êtes invité à confirmer l'action.

Ajout ou édition de règles

Cette section explique comment ajouter ou éditer des règles dans une politique.

1. Cliquez sur Configuration > Générateur de politique pour ouvrir le panneau Localiseur de politique ou cliquez sur Protection > Politiques de sécurité > Générateur de politique pour ouvrir le panneau Localiseur de politique.
2. Dans la liste Description de politique, sélectionnez la politique à éditer.
3. Cliquez sur le bouton Editer les règles pour ouvrir le panneau Règles de politique.
4. Effectuez l'une des actions suivantes :
   - Pour éditer une règle, cliquez sur le bouton Editer cette règle de manière individuelle.
   - Pour ajouter une nouvelle règle, cliquez sur l'un des boutons suivants :

     Ajouter une règle d'accès

     Ajouter une règle d'exception

     Ajouter une règle d'extrusion Rule (ce bouton n'est disponible que si l'utilisateur administrateur a indiqué l'option Inspecter les données renvoyées pour la configuration du moteur d'inspection).

     Les correspondances d'extrusion permettent à l'utilisateur d'indiquer le nombre d'enregistrements mis en correspondance qui seront regroupés lorsqu'ils seront consignés et signalés dans un rapport par Guardium. Aux règles d'extrusion doivent être associés une action Consigner l'ensemble des détails et un nom de règle qui inclut guardium://(some text)?split=(number), où (some text) correspond à n'importe quel texte ou à l'un des mots prédéfinis, tels que CREDIT CARD, et (number) est le nombre d'enregistrements de données renvoyés par enregistrement de journal Guardium.
5. Les attributs qui peuvent être testés dans chaque type de règle varient, mais, quel que soit le type de règle, chaque définition de règle commence par les quatre éléments suivants :
   - Description de règle : entrez un nom descriptif et court pour la règle. Pour utiliser un test de modèle spécial, entrez le nom du test de modèle spécial, suivi d'un espace et d'un ou de plusieurs caractères supplémentaires afin de créer un nom de règle unique, par exemple `guardium://SSEC_NUMBER employee`.
   - Catégorie : la catégorie est consignée avec les violations et est utilisée à des fins de regroupement et de génération de rapports. Si aucune catégorie n'est indiquée, la catégorie par défaut de la politique est utilisée.
   - Classification : entrez éventuellement une classification dans le champ Classification. A l'instar de la catégorie, la classification est consignée avec les exceptions et peut être utilisée à des fins de regroupement et de génération de rapports.
   - Gravité : sélectionnez l'un des codes de gravité suivants : Info, Faible, Moyen ou Elevé (Info est le code de gravité par défaut).
6. Utilisez les autres champs du panneau Définition de règles pour spécifier le mode de mise en correspondance de la règle. De nombreux champs sont communs aux règles d'accès, d'exception et d'extrusion et certains champs sont disponibles uniquement après que d'autres options ont été sélectionnées. Pour obtenir une liste classée par ordre alphabétique de tous les champs disponibles sur les panneaux de définition de règles, voir la rubrique Référence de définition de règle. De même, pour savoir comment utiliser des combinaisons de groupes et de valeurs individuelles, voir la section Spécification de valeurs et/ou de groupes de valeurs dans des règles.
7. Pour chaque type de règle, vous pouvez entrer une ou plusieurs expressions régulières dans un champ Modèle, afin de les mettre en correspondance avec des chaînes du trafic. Entrez l'expression manuellement ou cliquez sur l'icône RE pour ouvrir l'outil Générer une expression régulière qui vous permet d'entrer et de tester des expressions régulières.
8. Pour les règles d'exception uniquement, sélectionnez dans le champ Type d'exception un type d'exception auquel la règle sera sensible. Le nombre de règles est incrémenté uniquement lorsque le type d'exception sélectionné est détecté.
9. Lorsqu'une action associée à une règle est sélectionnée, les deux champs suivants sont activés :
   - Nb min. : entrez le nombre minimum de correspondances qui doit être trouvé pour la règle pour que l'action associée à la règle se déclenche. Le nombre de mises en correspondance de la règle est réinitialisé chaque fois que l'action est déclenchée ou lorsque l'intervalle de réinitialisation arrive à expiration. La valeur par défaut, zéro, équivaut à 1, ce qui signifie que chaque fois que la règle est mise en correspondance, l'action correspondante se déclenche.
   - Intervalle de réinitialisation (minutes) : utilisé uniquement lorsque le nombre minimum est supérieur à zéro, et est obligatoire dans ce cas. Entrez le nombre de minutes au terme desquelles le compteur de règle est remis à zéro. Le compteur est également remis à zéro chaque fois que l'action associée à la règle est déclenchée.
10. Cochez la case Passer à la règle suivante pour indiquer que lorsque cette règle est satisfaite et son action déclenchée, les tests portant sur la même demande, la même exception ou les mêmes résultats doivent continuer avec la règle suivante. Cela signifie que plusieurs règles peuvent être satisfaites et plusieurs actions exécutées à partir d'une seule demande ou exception. Si cette case n'est pas cochée (par défaut), aucune règle supplémentaire n'est testée lorsque cette règle est satisfaite. Si cette case est cochée, les tests de règle continuent avec la règle suivante, que cette règle soit satisfaite ou non.
11. Lorsque la case Val. enreg. est cochée, l'enregistrement réel qui satisfait à la règle est consigné dans l'attribut de chaîne SQL et est disponible dans les rapports. Si cette case n'est pas cochée, aucune instruction SQL n'est consignée.
12. Des modèles de message sont utilisés pour générer des alertes. Plusieurs modèles de message nommés sont créés et modifiés à partir du profil global.
13. Sélectionnez l'action à exécuter lorsque la règle est satisfaite.
14. Si une action d'alerte est spécifiée, la sous-fenêtre Notification s'ouvre, et au moins un type de notification doit être défini. Pour savoir comment ajouter des notifications, consultez Notifications.
15. Cliquez sur Sauvegarder pour sauvegarder la règle. Le panneau Définition de règle se referme et le panneau Règles de politique s'affiche.

Filtrage de règles pour afficher uniquement un sous-ensemble

Lorsqu'une politique contient un grand nombre de règles, il peut être utile d'afficher un sous-ensemble de règles ayant des attributs communs.

Pour ce faire, vous pouvez utiliser le champ Filtrer du panneau Définition de règle. La procédure de définition d'un filtre est semblable à la procédure de définition d'une règle.

1. Cliquez sur Configuration > Générateur de politique pour ouvrir le panneau Localiseur de politique ou cliquez sur Protection > Politiques de sécurité > Générateur de politique pour ouvrir le panneau Localiseur de politique.
2. Dans la liste Description de politique, sélectionnez la politique à afficher ou modifier.
3. Cliquez sur Editer les règles.
4. Dans le champ Filtrer, effectuez l'une des actions suivantes :
   - Sélectionnez un filtre dans la liste de filtres.
   - Cliquez sur Editer pour modifier une définition de filtre.
   - Cliquez sur Nouveau pour définir un nouveau filtre.

   Une fois que l'ensemble de règles filtré apparaît, vous pouvez effectuer n'importe laquelle des actions décrites dans cette section sur les règles affichées.

Copie de règles

Cette procédure vous permet de copier les règles sélectionnées d'une politique vers une autre ou vers un autre emplacement dans la même politique.

Toutes les règles copiées sont copiées vers un seul emplacement, après la règle 3, par exemple. Pour copier des règles vers différents emplacements dans la politique cible, effectuez plusieurs opérations de copie ou copiez toutes les règles en une seule fois, puis éditez la politique cible afin de déplacer les règles si besoin est.

1. Cliquez sur Configuration > Générateur de politique pour ouvrir le panneau Localiseur de politique ou cliquez sur Protection > Politiques de sécurité > Générateur de politique pour ouvrir le panneau Localiseur de politique.
2. Dans la liste Description de politique, sélectionnez la politique à partir de laquelle vous souhaitez copier une ou plusieurs règles.
3. Cliquez sur Editer les règles.
4. Cochez la case pour chaque règle à copier.
5. Cliquez sur Copier des règles.
6. Dans la liste Copier les règles sélectionnées dans la politique, sélectionnez la politique destinée à recevoir les règles copiées.
7. Dans la liste Insérer après la règle, sélectionnez la règle après laquelle les règles copiées doivent être insérées, ou sélectionnez Haut pour insérer les règles copiées au début de la liste.
8. Cliquez sur Copier. Vous serez tenu informé de la réussite de l'opération.
9. Vous devez à présent éditer la politique vers laquelle vous avez copié les règles, afin de vérifier que vous avez copié les bonnes règles vers le bon emplacement.

Utilisation de règles recommandées à partir de la base de référence

Utilisez le générateur de politique pour suggérer des règles à partir de la base de référence incluse dans la politique.

1. Cliquez sur Configuration > Générateur de politique pour ouvrir le panneau Localiseur de politique ou cliquez sur Protection > Politiques de sécurité > Générateur de politique pour ouvrir le panneau Localiseur de politique.
2. Dans la liste Description de politique, sélectionnez la politique à gérer. (Elle doit comporter une base de référence.)
3. Cliquez sur Editer les règles.
4. Définissez une valeur pour Nombre minimum pour jeu de règles. Il s'agit du nombre minimum de commandes like que le système doit trouver afin de suggérer une règle. La valeur par défaut est zéro. Plus le nombre saisi est petit, plus le nombre de règles recommandées par le système est élevé. (Sachez que le nombre qui s'affiche dans le panneau des règles recommandées ne reflète pas cette valeur.)
5. Définissez une valeur pour Nombre minimum pour groupe d'objets, afin de déterminer combien d'instances d'un groupe d'objets doivent être trouvées par le système afin de générer un groupe d'objets recommandés. La valeur par défaut est un. Plus le nombre saisi est petit, plus le nombre de groupes d'objets recommandés est élevé.
6. Cliquez sur le bouton Recommander des règles. Les règles recommandées s'affichent dans une fenêtre distincte, sur le panneau Règles recommandées.
7. Les règles recommandées sont triées par ordre décroissant du nombre d'occurrences au cours de la période de base de référence, pour chaque règle recommandée. Si vous sélectionnez une ou plusieurs des règles recommandées et que vous cliquez sur Sauvegarder, elles sont insérées dans le même ordre, juste avant la règle BASE DE REFERENCE dans le panneau Règles de politique. Vous pouvez ensuite changer l'ordre des règles recommandées ou les éditer si nécessaire, à partir du panneau Règles de politique.
8. Développez les règles et vérifiez l'appartenance des groupes d'objets recommandés. Dans la colonne Objet du panneau Règles recommandées, si des groupes d'objets recommandés ont été créés, leur nom commence par les mots Groupe d'objets recommandé et s'affiche sous la forme de liens hypertexte. Pour savoir comment afficher, accepter ou rejeter des groupes d'objets recommandés, voir la section Utilisation de groupes d'objets recommandés.
9. Cochez la case Sélectionner pour chaque règle recommandée à inclure dans la politique.
10. Cliquez sur Sauvegarder pour accepter les règles sélectionnées.
11. Vous pouvez désormais éditer ou modifier les règles recommandées comme vous le feriez pour n'importe quelle règle que vous avez ajoutée manuellement.

Utilisation de groupes d'objets recommandés

Le générateur de règle peut suggérer des règles à partir de la base de référence incluse dans la politique et de la politique de sécurité de base de données (interne au système de gestion de base de données) définie pour un serveur.

Dans les deux cas, il tente de générer l'ensemble minimal de règles en regroupant des objets de base de données (tables, procédures ou vues) dans des groupes d'objets recommandés. Vous pouvez accepter ou rejeter des groupes d'objets recommandés.

Avant d'accepter un groupe d'objets recommandés, vous pouvez éditer le champ Description de groupe généré (Groupe d'objets recommandé603-25 11:54, par exemple) afin de fournir un nom plus significatif. Après avoir accepté un groupe d'objets recommandés, vous pouvez afficher son appartenance. Vous pouvez rejeter l'utilisation de ce groupe dans n'importe quelle règle recommandée, mais vous ne pouvez pas éditer l'appartenance de ce groupe.

Si vous rejetez un groupe d'objets recommandés, la règle recommandée pour ce groupe est remplacée par une règle recommandée distincte pour chaque membre du groupe rejeté. Vous pouvez accepter ou rejeter chacune de ces règles recommandées séparément. Après avoir accepté une règle recommandée, vous pouvez l'éditer.

Affichage de groupes d'objets recommandés

Les groupes d'objets recommandés s'affichent dans la colonne Objet du panneau Règles recommandées sous la forme de liens hypertexte commençant par les mots Groupe d'objets recommandé.

Pour afficher l'appartenance d'un groupe d'objets recommandés, cliquez sur le lien hypertexte pour ce groupe. Si le groupe n'a pas encore été accepté, l'appartenance au groupe s'affiche dans le panneau Editer le groupe. Si le groupe a déjà été accepté, il s'affiche dans le panneau Afficher un groupe.

Acceptation de groupes d'objets recommandés

Pour accepter une groupe d'objets recommandés :

1. Entrez un nom significatif dans le champ Description de groupe sur le panneau Editer un groupe. (Cela n'est pas obligatoire, mais vivement recommandé.) Vous ne devez pas ajouter d'apostrophe dans le nom. C'est la seule occasion qui vous est offerte de nommer ce groupe. Si vous ne nommez pas le groupe, il prend un nom commençant par les mots Groupe d'objets recommandé, suivis d'un nombre, comme indiqué précédemment.
2. Cliquez sur Sauvegarder afin d'accepter le groupe édité pour la règle recommandée ou cliquez sur Sauvegarder pour tout afin d'accepter le groupe édité pour toutes les règles recommandées dans lesquelles il apparaît. Le nouveau nom d'objet remplace l'ancien nom d'objet dans la règle.

Rejet de groupes d'objets recommandés

Lorsque vous rejetez un groupe d'objets recommandés, l'utilisation de ce groupe est remplacé par une ou plusieurs règles recommandées. Pour rejeter un groupe d'objets recommandés, effectuez l'une des actions suivantes :

- Afin de rejeter le groupe pour cette règle recommandée uniquement, cliquez sur le bouton Rejeter.
- Afin de rejeter le groupe pour toutes les règles recommandées, cliquez sur le bouton Rejeter pour tout.

Remarque : Si vous acceptez un groupe d'objets recommandés dans une règle, ouvrez ce même groupe d'objets recommandés une nouvelle fois à partir d'une autre règle, puis cliquez sur le bouton Rejeter pour tout. Ce groupe sera conservé dans toutes les règles où il a été accepté de manière explicite, mais il sera rejeté dans les autres règles où il a été utilisé.

Utilisation de règles recommandées à partir de la liste de contrôle d'accès de la base de données

Pour un serveur de base de données spécifié, le générateur de politique peut suggérer des règles d'accès à l'aide de la politique de sécurité définie en interne par le système de gestion de base de données.

Pour ce faire, le générateur de politique examine les droits accordés aux groupes d'utilisateurs et aux objets de base de données (tables, procédures et vues) dans le système de gestion de base de données, puis regroupe les objets de base de données dans des groupes d'objets recommandés de manière à réduire le nombre total de règles recommandées. Vous pouvez accepter ou rejeter les groupes d'objets recommandés (voir la section Utilisation de groupes d'objets recommandés). Vous pouvez accepter ou rejeter des règles recommandées.

Pour faire en sorte que le générateur de politique suggère des règles à partir de la liste de contrôle d'accès de la base de données :

Remarque : Lors de la suggestion des règles à partir de la liste de contrôle d'accès de la base de données, le système n'utilise pas les champs Nombre minimum de règles ou Nombre minimum de groupes d'objets. Ces champs sont utilisés uniquement lorsque des règles sont recommandées à partir de la base de référence.

1. Cliquez sur Recommander des règles à partir de la base de données pour ouvrir le panneau Définition de base de données dans une fenêtre de navigateur distincte.
2. Cliquez sur Ajouter une source de données pour sélectionner la base de données à partir de laquelle vous souhaitez accéder à la liste de contrôle d'accès de la base de données.
   Remarque : Si vous ajoutez une source de données Oracle, DB2 ou DB2 for z/OS pour accéder à la liste de contrôle d'accès de la base de données, la section Paramètres de requête dans la fenêtre en incrustation Définition de base de données est désactivée.
3. Cliquez sur Recommander des règles pour générer les règles. Le panneau Règles recommandées s'ouvre dans une fenêtre distincte (comme indiqué précédemment pour les règles recommandées à partir de la base de référence). Si vous sélectionnez une ou plusieurs des règles recommandées et que vous cliquez sur Sauvegarder, elles sont insérées dans le même ordre dans la liste de règles sur le panneau Règles de politique, juste avant la règle BASE DE REFERENCE. S'il n'existe aucune règle BASE DE REFERENCE, elles sont insérées au début de la liste. Une fois que les règles recommandées ont été insérées dans le panneau Règles de politique, vous pouvez changer leur ordre ou les éditer, si nécessaire.
4. Vérifiez l'appartenance des groupes d'objets recommandés. Dans la colonne Objet, le nom des groupes d'objets recommandés qui ont été créés commence par les mots Groupe d'objets recommandé et s'affiche sous la forme de liens hypertexte (surlignés en bleu). Pour savoir comment afficher, éditer, accepter ou rejeter des groupes d'objets recommandés, voir la section Utilisation de groupes d'objets recommandés.
5. Cochez la case Sélectionner pour chaque règle recommandée à inclure dans la politique. Cliquez sur Sauvegarder pour accepter les règles sélectionnées.

Utilisation du simulateur de politique

Utilisez le simulateur de politique pour tester les règles d'accès sans avoir à installer la politique.

Il ne teste pas les règles d'exception ni les règles d'extrusion. Le simulateur réexécute le trafic réseau consigné et applique toutes les règles d'accès dans la politique. Il génère un rapport spécial dans une fenêtre distincte qui répertorie les chaînes SQL ayant déclenché les actions d'alerte ou de consignation uniquement. Le rapport comporte les colonnes suivantes : Horodatage, Nom de catégorie, Description de règle d'accès, Adresse IP client, Adresse IP serveur, Nom d'utilisateur de base de données, Chaîne SQL complète, Description de gravité et Nombre de violations de règle de politique. Utilisez la commande CLI store allow_simulation pour activer le bouton Simulateur de politique dans l'interface graphique.

Le simulateur de politique peut être utilisé pour tester uniquement les types d'actions de règle d'accès suivants :

- Consigner uniquement
- N'importe quelle action d'alerte : Alerter quotidiennement, Alerter une fois par session, Alerter par correspondance, Alerter par granularité temporelle.

Le simulateur de politique ne produit aucun résultat si la politique inclut des actions de consignation autres que Consigner uniquement. Afin d'utiliser le simulateur pour une politique de ce type, remplacez temporairement toutes les actions de consignation par Consigner uniquement.

Pour utiliser le simulateur de politique :

1. Cliquez sur Configuration > Générateur de politique pour ouvrir le panneau Localiseur de politique ou cliquez sur Protection > Politiques de sécurité > Générateur de politique pour ouvrir le panneau Localiseur de politique.
2. Dans la liste Description de politique, sélectionnez la politique à gérer.
3. Cliquez sur Editer les règles.
4. Cliquez sur le bouton Simulateur de politique pour ouvrir le panneau Simulateur de politique.
5. Renseignez les champs Date de début et Date de fin pour définir la période à utiliser pour la simulation.
   Remarque : Les données d'historique peuvent être archivées et purgées à partir de votre dispositif Guardium selon une planification définie par votre administrateur Guardium. Assurez-vous que les données de la période que vous spécifiez sont disponibles (et n'ont pas été purgées).
6. Cliquez sur Tester. Lorsque le test démarre et pendant qu'il s'exécute, le message * en cours d'exécution s'affiche dans le panneau Simulateur de politique. Lorsque le test est terminé, un rapport spécial s'ouvre dans une fenêtre distincte qui répertorie toutes les mises en correspondances de règles qui ont été consignées. Si aucune règle d'alerte ou de consignation uniquement n'a été déclenchée, un message `Aucune donnée trouvée pour le rapport d'exploration en aval demandé` s'affiche. Dans ce dernier cas, il se peut que vous n'ayez pas inclus suffisamment de données dans la période de test.

Rubrique parent : Politiques
Information associée:
Création et installation d'une politique (vidéo)
Groupes et politiques Guardium (vidéo)

Installation de politiques

Utilisez cette rubrique pour installer la politique sur le collecteur Guardium et modifier le planning.

Prise en charge de plusieurs politiques

1. Cliquez sur Configuration > Générateur de politique pour ouvrir le panneau Localiseur de politique ou cliquez sur Protection > Politiques de sécurité > Installation de politique pour ouvrir le panneau Programme d'installation de politique.
2. Sélectionnez la politique à installer à partir du champ Description de politique.

3. Effectuez l'une des actions suivantes :
    - Cliquez sur Installer pour installer la politique immédiatement.
    - Cliquez sur Modifier la planification pour ouvrir l'utilitaire de planification ordinaire et planifier l'installation de la politique.

Affichage des règles définies dans la politique installée

Plusieurs politiques installées peuvent cohabiter. Des actions peuvent être exécutées sur toutes les politiques installées. Il existe deux restrictions : les politiques définies en tant que politiques d'audit sélectif ne peuvent pas être utilisées en même temps que des politiques qui ne sont pas définies en tant que politiques d'audit sélectif, et les politiques définies en tant que consignation brute ne peuvent pas être utilisées en même temps que des politiques qui ne sont pas définies en tant que consignation brute. Si vous essayez de combiner des politiques de types différents, un message d'erreur s'affiche lorsque vous tentez de les installer.

Il est possible de contrôler l'ordre d'apparition des politiques durant leur installation, par exemple, en premier, en dernier, ou quelque part entre la première et la dernière politiques. En revanche, l'ordre d'apparition ne peut pas être édité ultérieurement.

En outre, il est possible de retirer une politique précédemment installée, à l'aide d'un bouton Désinstaller la politique.

La première politique installée a une signification particulière, car elle définit la valeur des paramètres de politique globaux. Ces paramètres sont les suivants : Modèle global, S'agit-il d'une politique d'audit sélectif, Masque de réseau client, Masque de réseau serveur, Client balisé et IP groupe de serveurs.

La prise en charge de plusieurs politiques est disponible via l'interface graphique (Configuration > Outils et vues > Installation de politique) et via GuardAPI.

Affichage des règles définies dans la politique installée

A partir du panneau Politiques actuellement installées, n'importe quel utilisateur peut afficher les règles de la politique installée, et, en outre, les utilisateurs autorisés peuvent ouvrir la politique afin de l'éditer.

1. Cliquez sur Configuration > Générateur de politique pour ouvrir le panneau Localiseur de politique ou cliquez sur Protection > Politiques de sécurité > Installation de politique pour ouvrir le panneau Programme d'installation de politique.
2. Cliquez sur la lien Politique installée pour afficher les règles de politique. Un bouton supplémentaire, Editer politique installée, est disponible pour les utilisateurs autorisés et leur permet d'ouvrir la politique afin de l'éditer dans le générateur de politique.

Planificateur de dépendances de travaux

Le collecteur Guardium comporte de nombreuses tâches, telles que Installation de politique, Processus d'audit, Mises à jour de groupe, etc., planifiées pour s'exécuter périodiquement. La fonction Dépendances de travaux recherche tous les travaux qui ont une relation et un impact directs sur la réussite de l'exécution de la tâche que vous essayez de planifier. sauf si vous trouvez les travaux qui sont définis en tant que prérequis pour le travail que vous essayez de planifier, il est possible que la tâche se réfère à des données inexactes, ce qui peut générer des résultats erronés.

Caractéristiques du dispositif

- L'utilisateur balise un travail planifié pour rechercher et exécuter des dépendances lors de l'exécution.
- Lorsque le planificateur exécute le travail, il cherche automatiquement tous les travaux subordonnés et les exécute dans l'ordre.
- Il existe une séquence de nouvelle tentative en cas d'échec.

Recherche des dépendances

- Identifiez les scénarios qui nécessitent des dépendances.
- Identifiez les travaux exécutables et ceux qui ne sont pas exécutables.
- Calculez les dépendances de travaux prédéfinies.

Travail	Travail prérequis préconisé	Motif
Installation de politique	Groupes qui sont définis dans n'importe quelle politique (à installer) et dont le remplissage par le mécanisme Remplir à partir d'une requête est planifié ou non.	Les règles de politique qui utilisent des groupes doivent comporter des données de groupe à jour avant d'être installées.
Installation de politique	Processus d'audit qui incluent une tâche d'audit de classification dans laquelle la tâche de classification est associée à une action Ajouter à un groupe d'objets, Ajouter à un groupe d'objets/de champs ou Ajouter à une règle d'accès.	Les règles de politique qui utilisent des groupes doivent comporter des données de groupe à jour avant d'être installées.
Processus d'audit	Travaux de téléchargement de tables personnalisées dans lesquels une tâche d'audit de type Rapport fait référence (dans la clause "from") au nom d'une table personnalisée.	Les tables personnalisées auxquelles une tâche d'audit de type Rapport fait référence doivent être remplies de données à jour pour permettre la planification de l'exécution d'un processus d'audit.
Processus d'audit	Groupes qui sont définis dans une condition d'une tâche d'audit de type Rapport et dont le remplissage par le mécanisme Remplir à partir d'une requête est planifié ou non.	Les groupes auxquels une condition de requête fait référence doivent être remplis de données à jour pour permettre l'exécution d'une tâche d'audit de type Rapport.
Remplir à partir d'une requête	Tables de téléchargement personnalisées qui contiennent n'importe laquelle des entités de la requête utilisée pour remplir un groupe.	
Processus d'audit	Importation	S'applique à un regroupeur uniquement. Ce prérequis garantit que des informations sont importées depuis toutes les unités agrégées avant l'exécution d'un processus d'audit.

Améliorations apportées au planificateur

- Recherche des dépendances de travaux lors de l'exécution d'un travail planifié
- Exécution des dépendances de travaux dans un ordre donné

Des travaux exécutables peuvent être planifiés, ce qui n'est pas le cas des travaux non exécutables.

Un groupe est un travail non exécutable.

Le travail de remplissage à partir d'une requête sur un groupe est exécutable.

Les dépendances directes sont des objets qui sont liés les uns aux autres par une définition, par exemple, une politique dépend d'une règle et une règle dépend de groupes.

Les dépendances indirectes sont des objets qui sont liés les uns aux autres de manière logique, par exemple, exécutez des processus d'audit avant d'installer des politiques.

Interface graphique prise en charge

1. Cochez la case Exécution automatique des travaux dépendants après avoir sélectionné Créer une planification dans Installation de politique.
2. Cliquez sur Sauvegarder pour planifier le processus. Cela permet d'informer l'utilisateur sur le statut des dépendances.

Commandes GuardAPI prises en charge

Commandes de dépendances de travaux GuardAPI :

CLI> grdapi add_job_dependency

Paramètres de fonction :

dependOnJobExecutedWithin - Chaîne

dependOnTrigger - Chaîne - Obligatoire

intervalBetweenRetries - Entier

jobRetries - Entier

jobTrigger - Chaîne - Obligatoire

runIfDependOnJobReturns - Chaîne

api_target_host - Chaîne

Utilisez la commande GuardAPI suivante pour lancer l'exécution automatique des dépendances :

> grdapi auto_execute_suggested_dependencies jobTrigger=*<nom de déclencheur du travail planifié>*

CLI> grdapi auto_execute_suggested_dependencies

Paramètres de fonction :

jobTrigger - Chaîne - Obligatoire

api_target_host - Chaîne

CLI> grdapi delete_job_dependencies

Paramètres de fonction :

dependOnTrigger - Chaîne

jobTrigger - Chaîne - Obligatoire

api_target_host - Chaîne

CLI> grdapi disable_auto_execute_suggested_dependencies

Paramètres de fonction :

jobTrigger - Chaîne - Obligatoire

api_target_host - Chaîne

CLI> grdapi list_job_dependencies_tree

Paramètres de fonction :

jobTrigger - Chaîne - Obligatoire

api_target_host - Chaîne

Pour obtenir une liste de tous les travaux/déclencheurs planifiés, exécutez la commande GuardAPI suivante :

> grdapi list_scheduler_jobs

CLI> grdapi list_suggested_job_dependencies

Paramètres de fonction :

jobTrigger - Chaîne - Obligatoire

api_target_host - Chaîne

CLI> grdapi list_existing_job_dependencies

Paramètres de fonction :

jobTrigger - Chaîne - Obligatoire

api_target_host - Chaîne

CLI> grdapi modify_job_dependency

Paramètres de fonction :

dependOnJobExecutedWithin - Chaîne

dependOnTrigger - Chaîne - Obligatoire

intervalBetweenRetries - Entier

jobRetries - Entier

jobTrigger - Chaîne - Obligatoire

runIfDependOnJobReturns - Chaîne

api_target_host - Chaîne

CLI> grdapi show_job_dependency_execution_profile

Paramètres de fonction :

dependOnTrigger - Chaîne - Obligatoire

jobTrigger - Chaîne - Obligatoire

api_target_host - Chaîne

Planificateur d'exécution

Le planificateur recherche les éventuelles dépendances de travaux lorsqu'un travail doit être exécuté.

Les dépendances sont exécutées dans l'ordre inverse.

Exemple d'arborescence de dépendances :

Installation de politique (travail exécutable)						
	Processus d'audit (travail exécutable/dépendance indirecte)					
		Tâche d'audit				
			Processus de classification			
				Politique de classification		
					Action de politique de classification	
						Groupe (travail exécutable/dépendance directe - remplir à partir de la requête)

L'ordre d'exécution sera : Remplir à partir du groupe de requêtes → Processus d'audit → Installation de politique

Le planificateur exécutera chacune des dépendances et attendra qu'elle se termine.

L'exécution de toute une arborescence de dépendances peut prendre un certain temps, mais elle permet de garantir que toutes les dépendances sont exécutées dans le bon ordre.

Traitement des erreurs

Si l'une des dépendances échoue, le travail en cours d'exécution par le planificateur n'est pas lancé.

Si un échec se produit, un message d'erreur est généré dans le rapport Exceptions des travaux planifiés.

Le nombre de nouvelles tentatives pour les dépendances sur les travaux précédents peut être défini. La valeur par défaut est 3. Une valeur valide est ≥ 0. Le nombre de minutes entre chaque nouvelle tentative peut être défini. La valeur par défaut est 3. Une valeur valide est ≥ 0.

Rubrique parent : Politiques

Champs de définition de règle

Vous pouvez utiliser ces champs lorsque vous définissez des règles de politique.

Tableau 1. Table de référence des champs de définition de règle

Champ	Description
Action	Indique l'action à entreprendre lorsque la règle a pour valeur true. Pour obtenir une description complète des actions associées aux règles, voir la présentation des actions de règle.
L'événement d'application existe	Faire correspondre un événement d'application uniquement. Voir la remarque sur l'événement d'application.
Valeurs d'événement d'application	Faire correspondre le texte, le numéro ou la date d'événement d'application spécifiés. De plus, permettre la sélection d'un groupe pour la chaîne d'événement en tant qu'option. Voir la remarque sur l'événement d'application.
(Application) Type d'événement	Faire correspondre l'événement d'application spécifié. Voir la remarque sur l'événement d'application.
(Application) Nom d'utilisateur d'événement	Faire correspondre le nom d'utilisateur d'événement d'application spécifié uniquement. Voir la remarque sur l'événement d'application.
Remarque sur l'événement d'application	Les champs d'événement d'application ne peuvent pas être utilisés lorsque la case Flat Log est cochée.
Utilisateur d'application	Utilisateur d'application. Voir la section Spécification de valeurs et/ou de groupes de valeurs dans des règles.
Catégorie	Libellé arbitraire pouvant servir à regrouper des violations de politique à des fins de génération de rapports. Une catégorie par défaut peut être spécifiée dans la définition de politique, mais la valeur par défaut peut être remplacée pour chaque règle.
Classification	Libellé arbitraire pouvant servir à regrouper des violations de politique à des fins de génération de rapports. Une classification par défaut peut être spécifiée dans la définition de politique, mais la valeur par défaut peut être remplacée pour chaque règle.
Infos sur le client	Infos sur le client DB2 : pour les règles d'accès uniquement. Pour z/OS uniquement, un champ INFOS SUR LE CLIENT (et CLIENT_INFO_GROUP_ID) sera visible si DB_TYPE a pour valeur DB2, DB2 COLLECTION Profile ou VSAM COLLECTION Profile. Le type d'informations pouvant être placées dans ce champ est USER=x; WKSTN=y; APPL=z.
Adresse IP client	Désélectionnez la case Non pour inclure ou sélectionnez la case Non pour exclure : • N'importe quel client : Laissez tous les champs de client vides. Le nombre est incrémenté chaque fois qu'un client satisfait à la règle. (Vous ne pouvez pas laisser tous les champs vides si la case Non est sélectionnée.) • Tous les clients sélectionnés par une adresse et un masque IP : Entrez une adresse IP client dans la première zone et un masque de réseau dans la seconde zone. Le nombre est incrémenté chaque fois que l'un des clients spécifiés satisfait à la règle. Par exemple, pour sélectionner tous les clients dans le sous-réseau 192.168.9.x, entrez 192.168.9.1 dans la première zone et 255.255.255.0 dans la seconde zone. Pour plus d'informations sur la sélection des adresses IP, voir la rubrique sur la sélection d'adresses IP à l'aide d'un masque. • Un groupe de clients : Sélectionnez un groupe d'adresses IP client dans la liste déroulante Groupe ou cliquez sur le bouton Groupes afin de définir un nouveau groupe, pus sélectionnez ce groupe. Le nombre est incrémenté chaque fois que l'un des membres du groupe sélectionné satisfait à la règle. • Tous les clients sélectionnés par une adresse et un masque IP ET un groupe de clients : Utilisez les champs Adresse IP client et Groupe. Le nombre est incrémenté chaque fois que l'un des clients spécifiés à l'aide de cette méthode satisfait à la règle. Autorisez un caractère générique dans l'adresse IP. Le caractère générique % est autorisé dans une politique pour un groupe IP client.
Adresse IP client/Programme source/Utilisateur de base de données/Adresse IP serveur/Nom de service	Groupe 7 tuples - Adresse IP client/Application source/Utilisateur de base de données/Adresse IP serveur/Nom de service/ Utilisateur de système d'exploitation/Base de données Type de groupe 5 tuples disponible pour les règles d'accès, d'exception et d'extrusion. Un tuple admet la combinaison de plusieurs attributs pour former un membre de groupe unique. Un tuple accepte l'utilisation d'une barre oblique et d'un caractère générique (%). Il n'accepte pas l'utilisation de double barres obliques. Le caractère générique % est autorisé dans une politique pour un groupe Adresse IP client/Programme source/Utilisateur de base de données/Adresse IP serveur/Nom de service.
MAC client	Pour rendre la règle sensible à une adresse MAC client unique, entrez l'adresse au format nn:nn:nn:nn:nn:nn, où n est un chiffre hexadécimal (0-F), OU entrez un point (.) dans la zone MAC client pour indiquer qu'un nombre distinct doit être maintenu pour chaque adresse MAC client OU laissez la zone MAC client vide pour ignorer les adresses MAC client.
Commande	Commande. Voir la section Spécification de valeurs et/ou de groupes de valeurs dans des règles si un groupe de commandes ne peut pas être édité et que le libellé et/ou groupe devient Collecter uniquement, indiquant que seules les commandes issues du groupe sélectionné seront sélectionnées. Si la case Chaque est cochée, chaque champ de l'instruction SQL doit être un membre du groupe.
Passer à la règle suivante	Si cette case est cochée, les tests de règle continuent avec la règle suivante, que cette règle soit satisfaite ou non. Cela signifie que plusieurs règles peuvent être satisfaites (et plusieurs actions exécutées) par une seule instruction ou exception SQL. Si cette case n'est pas cochée (par défaut), aucune règle supplémentaire n'est testée pour la transaction en cours lorsque cette règle est satisfaite.
Modèle de données	Si un modèle de données est facultatif pour les règles d'accès et les règles d'exception, en revanche, il est obligatoire pour les règles d'extrusion. Utilisation lors de la définition de règles d'extrusion - Expression régulière à mettre en correspondance, dans la zone Modèle de données. Cliquez sur le bouton Expression régulière pour ouvrir l'outil Générer une expression régulière, ce qui vous permet d'entrer et de tester des expressions régulières. Cela permet d'activer des modèles de masquage plus complexes. Placer entre parenthèses la section à masquer. Utilisez cette fonction pour masquer les données extraites de la base de données. Exemple :

Champ	Description
	Windows S-TAP : ([0-9][0-9][0-9][0-9[-,]?[0-9][0-9][0-9][0-9][-,]?[0-9][0-9][0-9][0-9][-,]?)[0-9][0-9][0-9][0-9] Unix S-TAP: ([0-9]{4}[-,]?[0-9]{4}[-,]?[0-9]{4}[-,]?)[0-9]{4}[ ]{0,20} Autres expressions régulières destinées à être utilisées uniquement dans les modèles de données avec l'option Expurger (Purger) : Windows S-TAP Nom : Modèle : Masqué comme suit : SCRUB_SSN_ANSI AAA-AA-AAAA ***-***-AAAA SCRUB_SSN_UNICODE UUU-UU-UUUU ***-***-UUUU SCRUB_CC_SPACES_ANSI AAAA AAAA AAAA AAAA **** **** **** AAAA SCRUB_CC_SPACES_UNICODE UUUU UUUU UUUU UUUU **** **** **** UUUU SCRUB_CC_SOLID_ANSI AAAAAAAAAAAAAAAA ************AAAA SCRUB_CC_SOLID_UNICODE UUUUUUUUUUUUUUUU ************UUUU SCRUB_CC_AX_SOLID_ANSI AAAAAAAAAAAAAAA ***********AAAA SCRUB_CC_AX_SOLID_UNICODE UUUUUUUUUUUUUUU ***********UUUU UNIX S-TAP Nom : Modèle : Masqué comme suit : SCRUB_SSN_ANSI AAA-AA-AAAA ***-***-AAAA SCRUB_SSN_UNICODE UUU-UU-UUUU ***-***-UUUU SCRUB_CC_SPACES_ANSI AAAA AAAA AAAA AAAA A*** **** **** 1234 SCRUB_CC_SPACES_UNICODE UUUU UUUU UUUU UUUU U*** **** **** **** SCRUB_CC_SOLID_ANSI AAAAAAAAAAAAAAAA A*************** SCRUB_CC_SOLID_UNICODE UUUUUUUUUUUUUUUU U*************** SCRUB_AMEX_SOLID_ANSI AAAAAAAAAAAAAAAA A*************** SCRUB_AMEX_SOLID_UNICODE UUUUUUUUUUUUUUUU U*************** Utilisation d'expressions régulières avec l'option Expurger - Les expressions régulières dans la solution IBM Security Guardium (y compris le masquage dans la politique) sont exécutées sur le dispositif et activent des fonctions d'expression régulière avancées. Toutefois, la bibliothèque d'expressions régulières à utiliser avec l'option Expurger est exécutée dans le noyau du serveur de base de données et est limitée aux expressions régulières de base. Seuls les modèles d'expressions régulières de base peuvent être utilisés avec l'option Expurger. Par exemple, la nomenclature d'expression régulière [0-9]* ne peut pas être utilisée pour indiquer n'importe quel nombre de chiffres. Il est nécessaire d'utiliser la nomenclature d'expression régulière de base [0-9]-[0-9]-[0-9]... pour spécifier une séquence de chiffres. Remarque : S-TAP acceptera uniquement les noms de modèle SCRUB prédéfinis ; tout autre nom sera ignoré. Règle d'accès, modèle de données et caractère de remplacement - L'utilisation d'un modèle de données, par exemple, [a-z,2]{3}([_][0-9]{1,2}), avec le caractère de remplacement * permet de changer les valeurs situées entre parenthèses dans le modèle de données et de les remplacer par ***. Utilisez cette fonction pour masquer des valeurs. Jeux de caractères définis par l'utilisateur Disponibles uniquement pour Oracle, Sybase, MySQL et MSSQL et les règles d'extrusion. Les utilisateurs peuvent influencer le jeu de caractères utilisé en définissant des règles d'extrusion spéciales. Ces règles de politique de jeu de caractères sont utilisées uniquement pour définir le jeu de caractères dans lequel un utilisateur souhaite convertir le trafic. Il est inutile de définir une action. Pour qu'une action soit associée à ce trafic, l'utilisateur doit définir d'autres règles après cette règle de jeu de caractères. Deux exemples de définition d'une règle de jeu de caractères sont possibles (avec suggestion ou contrainte), comme illustré ci-dessous : Exemple de règle d'extrusion (avec suggestion) Conversion du trafic par jeu de caractères, conformément à ce qui est indiqué dans la règle d'extrusion de la politique installée UNIQUEMENT si la conversion régulière a échoué. Jeu de caractères EUC-JP (code 274). Modèle de règle d'extrusion : guardium://char_set?hint=274 Exemple de règle d'extrusion (avec contrainte) Conversion du trafic par jeu de caractères, conformément à ce qui est indiqué dans la règle d'extrusion de la politique installée pour TOUTES les données. Jeu de caractères EUC-JP (code 274). Modèle de règle d'extrusion : guardium://char_set?force=274 Voir la section Liste de codes de jeux de caractères possibles à la fin de cette rubrique. Remarque : Gardez à l'esprit que les règles d'extrusion sont généralement associées à la session avec un certain délai. Par conséquent, des sessions courtes ou le début d'une session peuvent ne pas être affectés immédiatement par un changement de jeu de caractères.
Nom de base de données	Nom de la base de données. Voir la section Spécification de valeurs et/ou de groupes de valeurs dans des règles.

Champ	Description
Type de base de données	Types de base de données pris en charge Pour les règles d'accès : Cassandra, CIFS, CouchDB, DB2, DB2 COLLECTION PROFILE* (uniquement pour une utilisation avec z/OS), FTP, GreenPlumDB, Hadoop, HTTP, IBM® INFORMIX (DRDA), IBM iSeries, IMS, IMS COLLECTION PROFILE (uniquement pour des utilisations avec z/OS, Informix, MongoDB, MS SQL SERVER, MYSQL, NETEZZA, Oracle, PostgreSQL, Sybase, TERADATA, VSAM ou VSAM COLLECTION PROFILE* (uniquement pour une utilisation avec z/OS). Pour les règles d'exception et d'extrusion : Cassandra, CIFS, CounchDB, DB2, FTP, GreenPlumDB, Hadoop, IBM INFORMIX (DRDA), IBM iSeries, Informix, MongoDB, MS SQL SERVER, MYSQL, NETEZZA, Oracle, PostgreSQL, Sybase ou TERADATA. Remarque : Informix prend en charge deux protocoles SQLEXEC (protocole Informix natif) ou DRDA (protocole IBM). Ces protocoles sont automatiquement identifiés pour le trafic Informix, sans paramètres supplémentaires. L'attribut Type de serveur affiche INFORMIX (pour le protocole SQLEXEC) et IBM INFORMIX (DRDA) (pour le protocole DRDA). Remarque : TERADATA dispose d'une connexion silencieuse et permet aux clients de se reconnecter automatiquement. Pour bloquer les instructions de téradonnées dans une politique, utilisez la fonction de pare-feu S-TAP avec l'état par défaut ON et ne surveillez pas les utilisateurs qui ne présentent aucun risque.
Utilisateur de base de données	Utilisateur de la base de données. Voir la section Spécification de valeurs et/ou de groupes de valeurs dans des règles.
Code d'erreur	Code d'erreur (pour une exception). Voir la section Spécification de valeurs et/ou de groupes de valeurs dans des règles.
Type d'exception	Type d'exception (sélectionnée dans la liste). Remarque : Lorsqu'une session est fermée suite à un dépassement de délai d'attente d'interface graphique, avec une règle d'exception, aucune erreur de session (Session_Error) n'est générée.
Nom de champ	Nom du champ. Voir la section Spécification de valeurs et/ou de groupes de valeurs dans des règles. Si la case Chaque est cochée, chaque champ de l'instruction SQL doit être un membre du groupe.
Nb min.	Nombre minimum de correspondances qui doit être trouvé pour la condition contenue dans la règle pour que celle-ci soit satisfaite (sujette à l'intervalle de réinitialisation).
Protocole réseau	Protocole de réseau. Voir la section Spécification de valeurs et/ou de groupes de valeurs dans des règles.
Objet	Nom de l'objet. Voir la section Spécification de valeurs et/ou de groupes de valeurs dans des règles. Pour Sybase et MS SQL Server, il existe deux groupes, MASKED_SP_EXECUTIONS_SYBASE et MASKED_SP_EXECUTIONS_MS_SQL_SERVER, incluant respectivement des noms de procédures mémorisées. Si une procédure incluse est exécutée, tout sera masqué. Si la case Chaque est cochée, chaque champ de l'instruction SQL doit être un membre du groupe.
Groupe d'objets/de commandes	Faites correspondre un membre du groupe d'objets/de commandes sélectionné.
Groupe d'objets/de champs	Faites correspondre un membre du groupe d'objets/de champs sélectionné.
Utilisateur de système d'exploitation	Utilisateur du système d'exploitation. Voir la section Spécification de valeurs et/ou de groupes de valeurs dans des règles.
Modèle	Expression régulière qui doit être mise en correspondance, spécifiée dans la zone Modèle. Vous pouvez entrer une expression régulière manuellement ou cliquer sur le bouton Expression régulière pour ouvrir l'outil Générer une expression régulière qui vous permet d'entrer et de tester des expressions régulières.
Période	Pour rendre la règle sensible à une période unique, sélectionnez une période prédéfinie dans la liste Période ou cliquez sur le bouton Période pour définir une nouvelle période.
Val. enreg.	Lorsque cette case est cochée, l'enregistrement réel qui satisfait à la règle est consigné dans l'attribut de chaîne SQL et est disponible dans les rapports. Pour une violation de politique uniquement, si cette case n'est pas cochée, aucune instruction SQL n'est consignée.
Seuil des enregistrements affectés	Règle d'accès uniquement. Définissez une valeur de seuil pour les enregistrements mis en correspondance. Par exemple, laissez 1000 instances s'exécuter avant d'effectuer une action. Ce champ affecte la sortie de la règle et non pas la définition de la règle (par exemple, ce qui se produit lorsqu'elle est déclenchée et non pas quand elle doit se déclencher). La valeur du champ Seuil des enregistrements affectés est basée sur les règles et les sessions. Il s'agit des lignes cumulées renvoyées par toutes les requêtes qui satisfont à la condition de règle. Une fois que tous les enregistrements affectés cumulés atteignent le seuil, la règle se déclenche et les enregistrements affectés sur l'instruction (avec l'action Consigner l'ensemble des détails) correspondent à la valeur cumulée des enregistrements affectés.
Caractère de remplacement	Définissez un caractère de masquage. Si la sortie produite par la règle d'extrusion correspond à l'expression régulière, les parties qui correspondent aux sous-expressions placées entre parenthèses '(' et ')' seront remplacées par le caractère de masquage
Intervalle de réinitialisation	Utilisé uniquement si la valeur du champ Nb min. est supérieure à zéro. Cette valeur est le nombre de minutes au terme desquelles le compteur de conditions remplies est remis à zéro.
Révoquer	Cette case à cocher apparaît uniquement sur les règles d'extrusion. Elle vous permet d'exclure de la consignation une réponse qui a déjà été sélectionnée pour la consignation par une règle précédente définie dans la politique. Dans la plupart des cas, vous pouvez obtenir le même résultat plus simplement en définissant une seule règle avec une ou plusieurs conditions NOT afin d'exclure les réponses non souhaitées, tout en consignant les autres réponses qui satisfont à la règle. (La case à cocher Révoquer est antérieure aux conditions NOT et est principalement fournie à des fins de compatibilité avec les versions antérieures afin de permettre la prise en charge des politiques existantes.)

Champ	Description
Description de règle	Nom de la règle. Pour utiliser un test de modèle spécial dans la règle, entrez le nom du test de modèle spécial, suivi d'un espace et d'un ou de plusieurs caractères supplémentaires afin de créer un nom de règle unique, par exemple, guardium://SSEC_NUMBER employee. (Pour plus d'informations, voir la section Tests de modèle spéciaux.) Lorsqu'il est affiché, le nom de la règle est précédé du numéro de celle-ci et du libellé Règle d'accès, Règle d'exception ou Règle d'extrusion, afin d'identifier le type de règle. Si la règle a été générée à l'aide de la fonction Recommander à partir de la base de données, le format du nom généré est le suivant : Règle recommandée <n>_mm-jj hh:mm, dont les composants sont les suivants : n est le numéro de séquence pour la règle générée mm-jj correspond au mois et au jour de génération de la règle hh:mm correspond à l'heure de génération de la règle
Adresse IP serveur	Désélectionnez la case Non pour inclure ou sélectionnez la case Non pour exclure : • N'importe quel serveur : Laissez tous les champs de serveur vides. Le nombre est incrémenté chaque fois qu'un serveur satisfait à la règle. (Vous ne pouvez pas laisser tous les champs vides si la case Non est sélectionnée.) • Tous les serveurs sélectionnés par une adresse et un masque IP : Entrez une adresse IP de serveur dans la première zone et un masque de réseau dans la seconde zone. Le nombre est incrémenté chaque fois que l'un des serveurs spécifiés satisfait à la règle. Par exemple, pour sélectionner tous les serveurs dans le sous-réseau 192.168.3.x, entrez 192.168.3.1 dans la première zone et 255.255.255.0 dans la seconde zone. • Un groupe de serveurs : Sélectionnez un groupe d'adresses IP de serveur dans la liste déroulante Groupe ou cliquez sur le bouton Groupes afin de définir un nouveau groupe, pus sélectionnez ce groupe. Le nombre est incrémenté chaque fois que l'un des membres du groupe spécifié satisfait à la règle. • Tous les serveurs sélectionnés par une adresse et un masque IP ET un groupe de serveurs : Utilisez les champs Adresse IP client et Groupe. Le nombre est incrémenté chaque fois que l'un des serveurs spécifiés à l'aide de cette méthode satisfait à la règle. Autorisez un caractère générique dans l'adresse IP. Le caractère générique % est autorisé dans une politique pour un groupe d'IP serveur.
Nom de service	Nom du service. Voir la section Spécification de valeurs et/ou de groupes de valeurs dans des règles.
Gravité	Sélectionnez l'un des codes de gravité suivants : INFO, FAIBLE, AUCUN, MOYEN ou ELEVE. Si le code ELEVE est sélectionné et que des alertes e-mail sont envoyées par cette règle, l'e-mail est signalé comme Urgent.
Modèle SQL	Expression régulière qui doit être mise en correspondance, spécifiée dans la zone Modèle. Vous pouvez entrer une expression régulière manuellement ou cliquer sur le bouton Expression régulière pour ouvrir l'outil Générer une expression régulière qui vous permet d'entrer et de tester des expressions régulières. Restriction : Modèle SQL n'est pas pris en charge pour les règles d'expurgation.
Application source	Programme source d'application. Voir la section Spécification de valeurs et/ou de groupes de valeurs dans des règles.
Déclencher une fois par session	Ne lancez pas d'analyse de session pour la même règle après la première correspondance trouvée. Particulièrement efficace pour les politiques d'audit sélectif.
Modèle XML	Expression régulière qui doit être mise en correspondance, spécifiée dans la zone Modèle. Vous pouvez entrer une expression régulière manuellement ou cliquer sur le bouton Expression régulière pour ouvrir l'outil Générer une expression régulière qui vous permet d'entrer et de tester des expressions régulières. Une expression régulière qui doit être mise en correspondance peut être utilisée dans cette zone. L'expression régulière doit être entrée manuellement.
Valeurs de retour Full_SQL à l'aide de MSSQL	En MSSQL, les procédures mémorisées sprocsp_cursoropen et sp_cursorfetch sont utilisées pour les requêtes de base de données SELECT. Sp_cursoropen contient l'instruction d'origine, tandis que la valeur de retour FULL_SQL dans la règle d'extrusion apparaît sous la forme sp_cursorfetech et non pas sous la forme Select * from _____.

Rubrique parent : Politiques

Comment intégrer des règles personnalisées à une politique Guardium

Cette section explique comment modifier/dériver automatiquement une politique Guardium à partir d'un système d'autorisation d'utilisation personnalisé.

L'exemple ci-dessous illustre un modèle de table Oracle (CUSTOM_ENTITLEMENT) comme données d'autorisation d'utilisation personnalisées, utilise un script Oracle pour sélectionner des données dans cette table, puis génère un fichier à l'aide de commandes GuardAPI. Le fichier comportera des commandes pour la création de nouvelles règles de politique ou la modification de règles de politique existantes, le changement d'un ordre de règles de politique et la réinstallation de la politique. Nous verrons ensuite comment exécuter le script généré et afficher les changements de politique dans l'interface graphique Guardium.

Valeur ajoutée : l'API Guardium permet d'accéder à la fonctionnalité Guardium à partir de la ligne de commande ou du script. Cela permet d'automatiser les tâches répétitives, ce qui est particulièrement utile pour les implémentations plus importantes. Le fait d'appeler ces fonctions GuardAPI permet à un utilisateur d'effectuer rapidement des opérations, comme la maintenance de la politique Guardium.

Procédez comme suit :

1. Définissez une structure de règle qui consigne tous les détails pour toutes les commandes DML (manipulation de base de données). Elle sera utilisée comme modèle pour la création de nouvelles règles. La règle appartiendra à la politique de modèle.
2. Créez le script Oracle qui générera un fichier à l'aide des commandes GuardAPI suivantes :
    - copy_rule, qui permet d'ajouter de nouvelles règles aux politiques installées en tant que copie de modèle de règle.

- update_rule, qui permet de mettre à jour les règles copiées avec les données appropriées issues de la table Oracle CUSTOM_ENTITLEMENT.
- update_rule, qui permet de mettre à jour la règle existante avec les données issues de cette table.
- change_rule_order, qui permet de changer la position d'une règle.
- policy_install, reinstall_policy, qui permettent d'installer/de réinstaller une politique.

3. Exécutez le script généré.
4. Affichez les changements apportés aux politiques installées.

Etapes :

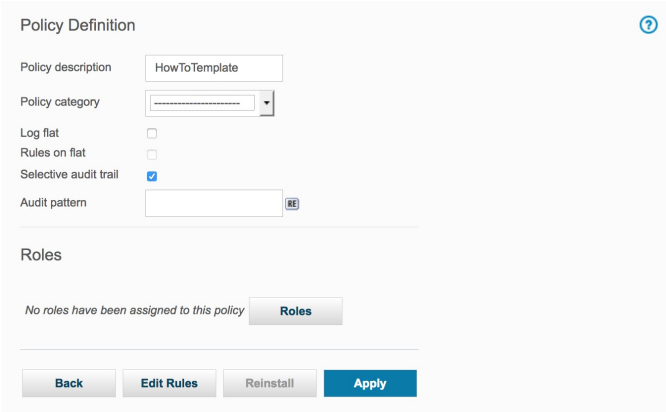
1. Définissez un modèle de règle.

   Comme de nombreuses actions sont autorisées pour une règle de politique donnée, il devient très difficile de définir la structure hiérarchique complexe d'une règle à l'aide de l'API Guard. Toutefois, dans la plupart des cas, les règles varient en fonction des conditions, ce qui fait que les structures d'action/de récepteur font généralement partie d'un petit ensemble de différentes options. Par conséquent, les API sont basées sur le clonage d'une règle existante qui fait office de modèle de règle. Cela permet de définit la structure d'action/de récepteur, et les conditions peuvent être changées à l'aide d'API.

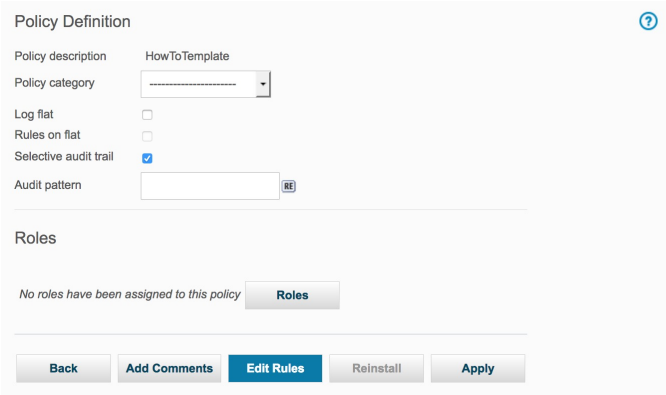
   Ici, nous allons créer un modèle de règle (HowToTemplate), qui inclut une définition d'action de règle et qui sera cloné, puis mis à jour chaque fois qu'une nouvelle règle de ce type devra être ajoutée à une politique.

   Cliquez sur Protection > Politiques de sécurité > Générateur de politique pour ouvrir le panneau Localiseur de politique et créer une politique de modèle.

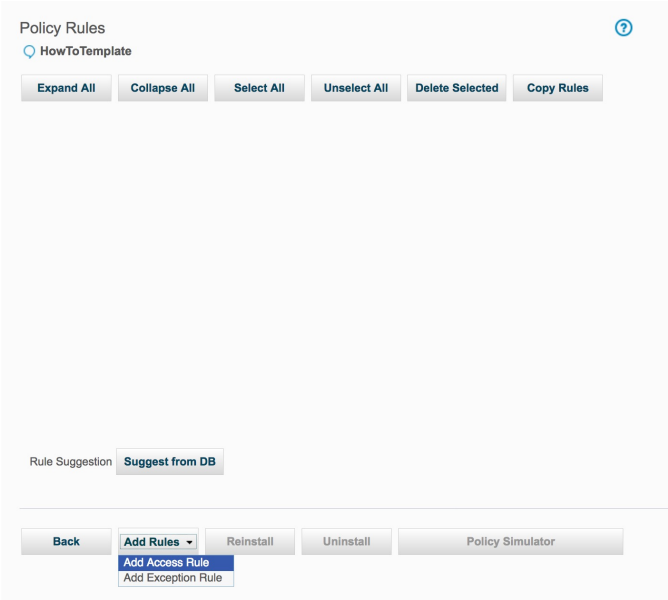
   Cliquez sur Nouveau pour créer la politique de modèle. Entrez une description de politique, cochez la case Trace d'audit sélectif, puis cliquez sur le bouton Sauvegarder.



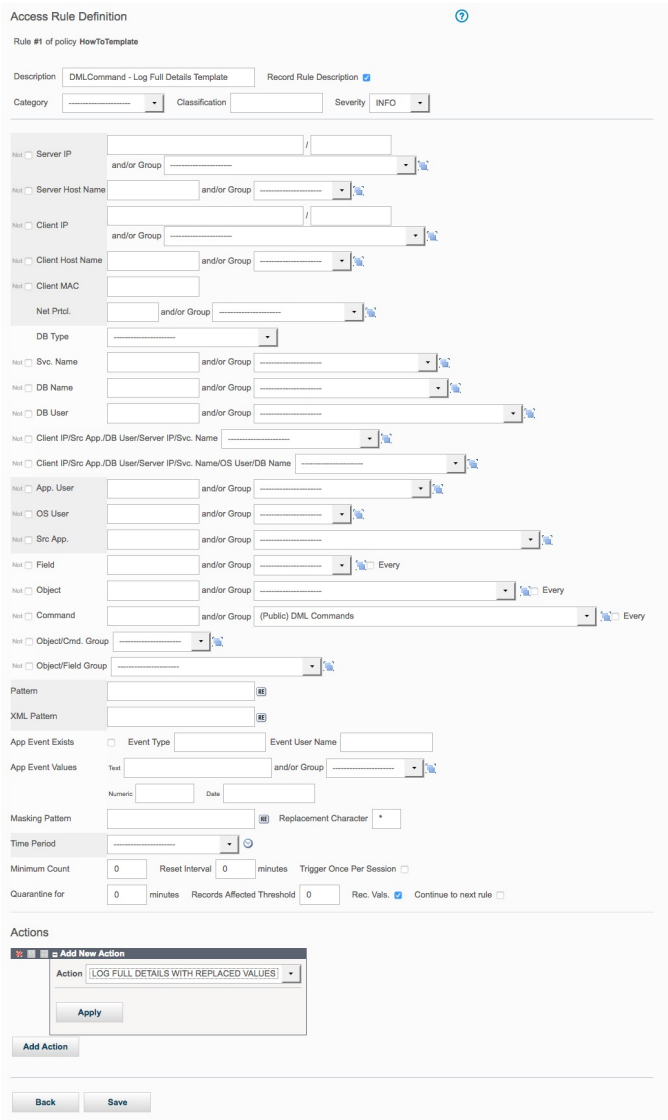
   Cliquez sur le bouton Editer les règles pour ajouter une règle de modèle à cette politique.

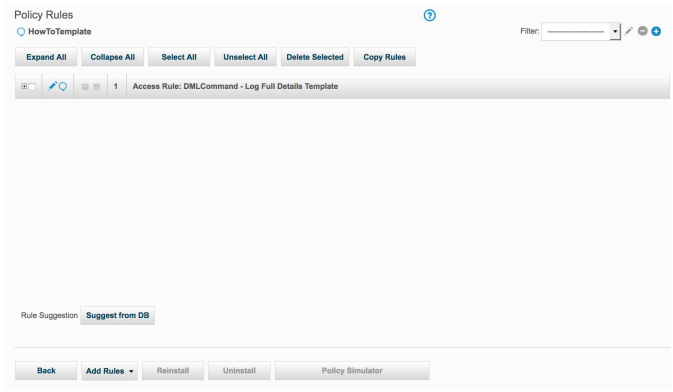


   Cliquez sur le bouton **Ajouter une règle d'accès** pour afficher le panneau Définition de règle d'accès et ajouter une règle.



Pour ajouter la règle, entrez **Commande DML - Modèle Consigner l'ensemble des détails** dans le champ Description, choisissez **(Public) Commandes DML** dans le champ Commandes, mettez en évidence **CONSIGNER L'ENSEMBLE DES DETAILS AVEC LES VALEURS** dans la section Action, puis cliquez sur le bouton **Sauvegarder**.





2. Créez le script Oracle qui générera un fichier à l'aide de commandes GuardAPI.

   Ce que vous devez savoir avant d'écrire le script :

   - GuardAPI est un ensemble de commandes CLI, qui commencent toutes par le mot clé **grdapi**. Pour répertorier toutes les commandes GuardAPI disponibles, entrez la commande 'grdapi' sans arguments. Pour afficher les paramètres d'une commande spécifique, entrez la commande suivie de '--help=yes'.

   Par exemple

   CLI>grdapi copy_rule --help=yes

   ID=0

   Paramètres de fonction :

   fromPolicy - obligatoire

   ruleDesc - obligatoire

   toPolicy - obligatoire

   ok

   - Les composants de mot clé et de valeur des paramètres sont sensibles à la casse.
   - Si une valeur de paramètre contient un ou plusieurs espaces, elle doit être placée entre guillemets. Par exemple :

```
grdapi copy_rule ruleDesc="DMLCommand - Log Full Details Template" ...
```

   - Il n'est pas nécessaire d'utiliser tous les paramètres disponibles pris en charge par une fonction. Outre les paramètres obligatoires, utilisez les paramètres que vous souhaitez changer.
   - Les scripts, qui appellent GuardAPI, peuvent contenir des informations sensibles, comme des mots de passe de sources de données. Pour garantir le chiffrement permanent des informations sensibles, la commande **grdapi** prend en charge la transmission d'un paramètre chiffré à une fonction d'API. Ce chiffrement est effectué à l'aide du secret partagé du système, qui est défini par l'administrateur et qui peut être partagé par un grand nombre de systèmes et entre toutes les unités d'un gestionnaire central et/ou d'un cluster d'agrégation. Ainsi, les scripts contenant des paramètres chiffrés peuvent être exécutés sur des machines qui possèdent le même secret partagé. Pour plus d'informations à ce sujet, voir l'aide Guardium.
   - Si plusieurs politiques sont installées, la commande d'installation de politique (**policy_install**) doit inclure toutes les descriptions de politiques installées délimitées par une barre verticale. Cela s'applique même si une seule politique a subi des changements. Les descriptions de politiques doivent être indiquées dans l'ordre où vous souhaitez installer les politiques.

   Exemple de commande d'installation des politiques HowTo 1 et HowTo 2 :

```
grdapi policy_install policy="HowTo 1|HowTo 2"
```

   Pour illustrer la logique sous-jacente à l'écriture du script, changez la politique actuellement installée, HowTo, en procédant comme suit :

   a. Pour chacun des enregistrements de la table CUSTOM_ENTITLEMENT auxquels la valeur '1' est associée à IS_NEW_FLAG, une nouvelle règle d'accès avec une description sauvegardée dans la colonne RULE_DESC sera ajoutée à la politique "HowTo". La règle consigne tous les détails pour l'ensemble des commandes DML depuis l'utilisateur de système d'exploitation (OS_USER), l'adresse IP client (CLIENT_IP), l'adresse IP serveur (SERVER_IP), avec le nom de service (SERVICE_NAME).

   b. Si IS_NEW_FLAG a pour valeur '0', la règle avec une description équivaut à la valeur de la colonne RULE_DESC et sera changée en fonction des données appropriées issues de l'enregistrement de la table.

   c. Rule3 sera défini comme première règle, afin de montrer comment utiliser la fonction **change_rule_order**.

   d. La politique sera réinstallée afin que tous les changements soient pris en compte.

   Données de la table custom_entitlement

Tableau 1. Table CUSTOM_ENTITLEMENT

os_user	client_ip	server_ip	rule_desc	service_name	is_new_rule	seq
User1	192.168.7.101	192.168.7.201	Rule1	PROD1	1	1
User2	192.168.7.102	192.168.7.202	Rule2	PROD2	1	2

os_user	client_ip	server_ip	rule_desc	service_name	is_new_rule	seq
User3	192.168.7.103	192.168.7.203	Rule3	PROD3	1	3
User4	192.168.7.104	192.168.7.204	Rule2	PROD4	0	4

Les changements, basés sur la logique et sur les données de la table, peuvent être décrits comme suit :

a. Ajoutez une nouvelle règle d'accès : Rule1. La règle consigne tous les détails pour l'ensemble des commandes DML depuis l'utilisateur "user1" et l'adresse IP client "192.168.7.101" vers la base de données Oracle, sur le serveur "192.168.7.201", avec le nom de service "PROD1".

b. Ajoutez une nouvelle règle d'accès : Rule2. La règle consigne tous les détails pour l'ensemble des commandes DML depuis l'utilisateur "user2" et l'adresse IP client "192.168.7.102" vers la base de données Oracle, sur le serveur "192.168.7.202", avec le nom de service "PROD2".

c. Ajoutez une nouvelle règle d'accès : Rule3. La règle consigne tous les détails pour l'ensemble des commandes DML depuis l'utilisateur "user3" et l'adresse IP client "192.168.7.103" vers la base de données Oracle, sur le serveur "192.168.7.203", avec le nom de service "PROD3".

d. Changez Rule2 – affectez "user4" au champ d'utilisateur de système d'exploitation, "192.168.7.104" au champ d'adresse IP client, "192.168.7.204" au champ d'adresse IP serveur et "PROD4" au champ de nom de service.

e. Définissez Rule3 comme première règle de la politique.

f. Pour que tous les changements soient pris en compte, réinstallez la politique.

Script Oracle

```
SET LINESIZE 2000
SET TERMOUT OFF
SET FEEDBACK OFF

SET SERVEROUTPUT ON SIZE 1000000
spool update_policy.txt

declare cursor CUSTOM_TABLE is
select OS_USER,CLIENT_IP,SERVER_IP,SERVICE_NAME,RULE_DESC,IS_NEW_RULE
  from CUSTOM_ENTITLEMENT order by SEQ;
S_RULE_DESC VARCHAR2(100);
BEGIN
    FOR CUR_W IN CUSTOM_TABLE
    LOOP
        IF NVL(CUR_W.IS_NEW_RULE,'0') = '1' THEN
           -- copy rule
           DBMS_OUTPUT.PUT_LINE('grdapi copy_rule ruleDesc="DMLCommand - Log Full Details Template" fromPolicy=HowToTemplate
toPolicy=HowTo ');
           S_RULE_DESC := 'DMLCommand - Log Full Details Template';
        ELSE
           S_RULE_DESC := CUR_W.RULE_DESC;
        END IF;
        -- update rule
        DBMS_OUTPUT.PUT_LINE(
        'grdapi update_rule ruleDesc="'||S_RULE_DESC||'"'||
        ' fromPolicy=HowTo newDesc="'|| CUR_W.RULE_DESC ||'" clientIP='||CUR_W.CLIENT_IP ||
        ' clientNetMask=255.255.255.0 serverIP='||CUR_W.SERVER_IP||' serverNetMask=255.255.255.0 '||
        ' serviceName='||CUR_W.SERVICE_NAME ||' osUser='||CUR_W.OS_USER||' dbType=ORACLE');
    END LOOP;
    -- set Rule3 to be the first one
    DBMS_OUTPUT.PUT_LINE('grdapi change_rule_order ruleDesc=Rule3 fromPolicy=HowTo order=1');
    -- reinstall policy
    DBMS_OUTPUT.PUT_LINE('grdapi policy_install policy=HowTo');
END;
/
spool off
```

Script généré à l'aide de commandes GuardAPI

Lorsque le script Oracle est exécuté en SQL*Plus et, par conséquent, placé en fichier spoule, un fichier (update_policy.txt) semblable à celui présenté ci-dessous est généré :

```
grdapi copy_rule ruleDesc="DMLCommand - Log Full Details Template" fromPolicy=HowToTemplate toPolicy=HowTo
grdapi update_rule ruleDesc="DMLCommand - Log Full Details Template" fromPolicy=HowTo newDesc="Rule1" clientIP=192.168.7.101
clientNetMask=255.255.255.0 serverIP=192.168.7.201 serverNetMask=255.255.255.0  serviceName=PROD1 osUser=user1 dbType=ORACLE
grdapi copy_rule ruleDesc="DMLCommand - Log Full Details Template" fromPolicy=HowToTemplate toPolicy=HowTo
grdapi update_rule ruleDesc="DMLCommand - Log Full Details Template" fromPolicy=HowTo newDesc="Rule2" clientIP=192.168.7.102
clientNetMask=255.255.255.0 serverIP=192.168.7.202 serverNetMask=255.255.255.0  serviceName=PROD2 osUser=user2 dbType=ORACLE
grdapi copy_rule ruleDesc="DMLCommand - Log Full Details Template" fromPolicy=HowToTemplate toPolicy=HowTo
grdapi update_rule ruleDesc="DMLCommand - Log Full Details Template" fromPolicy=HowTo newDesc="Rule3" clientIP=192.168.7.103
clientNetMask=255.255.255.0 serverIP=192.168.7.203 serverNetMask=255.255.255.0  serviceName=PROD3 osUser=user3 dbType=ORACLE
grdapi update_rule ruleDesc="Rule2" fromPolicy=HowTo newDesc="Rule2" clientIP=192.168.7.104 clientNetMask=255.255.255.0
serverIP=192.168.7.204 serverNetMask=255.255.255.0  serviceName=PROD4 osUser=user4 dbType=ORACLE
grdapi change_rule_order ruleDesc=Rule3 fromPolicy=HowTo order=1
grdapi policy_install policy=HowTo
```

Remarque : La dernière commande grdapi réinstalle la politique pour appliquer les règles au système.

3. Exécutez le script généré.

Pour exécuter ce script, utilisez la structure de commande suivante :

ssh cli@[nom de dispositif Guardium] < [nom de script]

Par exemple, pour exécuter le script update_policy.txt sur l'hôte 192.168.12.5 (vous serez invité à taper votre mot de passe) :

ssh cli@192.168.12.5 <update_policy.txt

Exemple de résultat :

192.168.12.5> ok

ID=20002

192.168.12.5> 192.168.12.5> ok

ID=20015

192.168.12.5> 192.168.12.5> ok

ID=20002

192.168.12.5> 192.168.12.5> ok

ID=20016

192.168.12.5> 192.168.12.5> ok

ID=20002

192.168.12.5> 192.168.12.5> ok

ID=20017

192.168.12.5> 192.168.12.5> ok

ID=20016

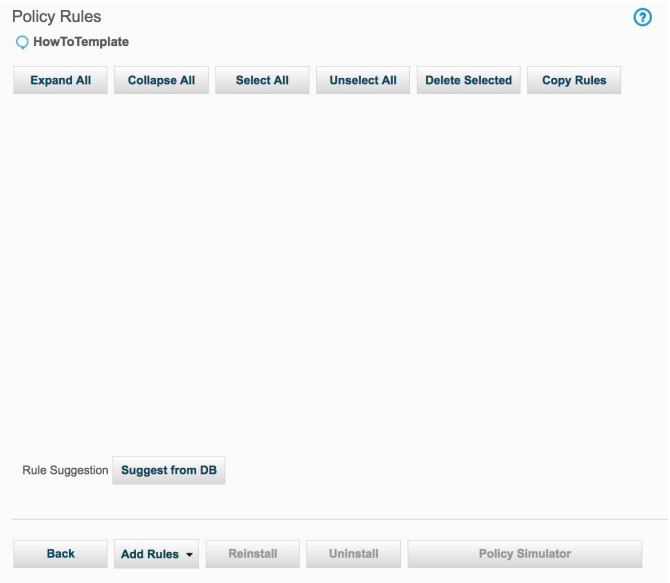
192.168.12.5> 192.168.12.5> ok

ID=20002

192.168.12.5> 192.168.12.5>

4. Affichez les changements apportés aux politiques installées.

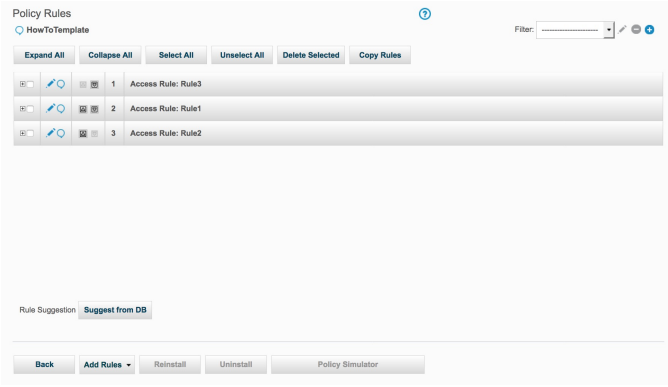
   Avant d'exécuter le script, aucune règle n'était définie dans la politique HowTo, comme illustré ci-dessous.



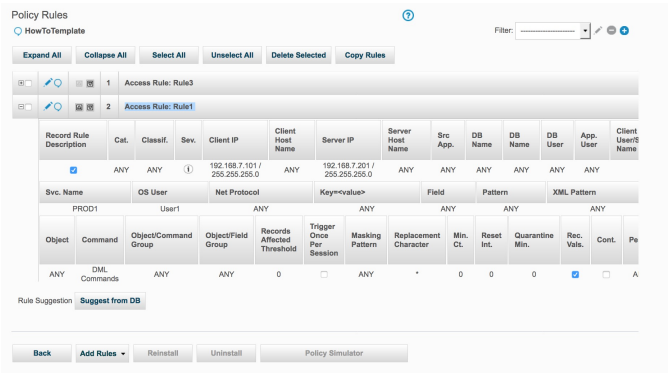
   Après l'exécution du script :

   Suite à l'exécution de la commande **copy_rule**, la politique HowTo comporte désormais trois règles d'accès.

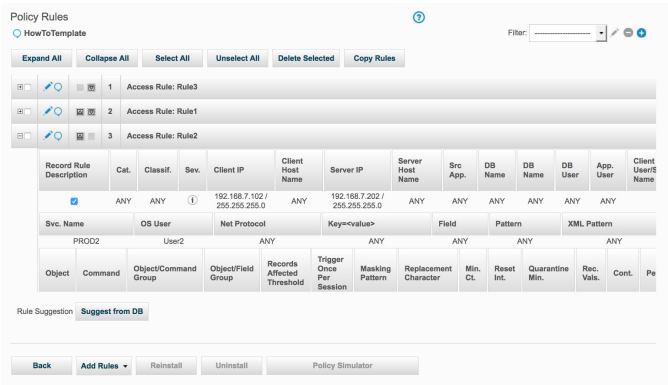
   Suite à l'exécution de la commande **change_rule_order**, Rule3 apparaît désormais en premier.



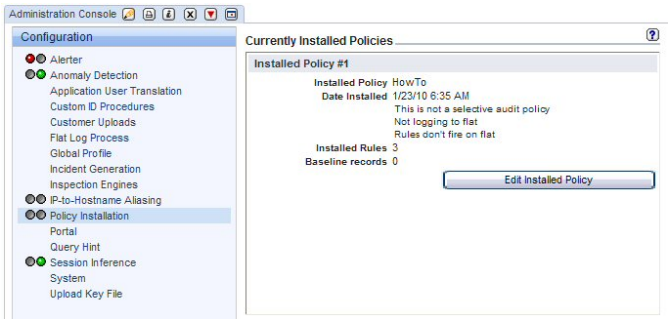
En détaillant une règle de politique, en l'occurrence, Rule1, nous pouvons vérifier les différents champs qui ont été modifiés à l'aide des commandes **update_rule**.



Suite à l'exécution de la commande **update_rule**, Rule2 a été changé.



Et, suite à l'exécution de la commande **policy_install**, la politique actuellement installée est désormais HowTo avec trois règles installées.



Rubrique parent : Politiques

Comment utiliser l'action Ignorer appropriée

Cette rubrique explique en détail de quelle façon les données sont gérées lorsque des actions Ignorer sont utilisées dans les règles de politique.

Valeur ajoutée : permet de clarifier ce qu'il se passe lorsque certaines options sont choisies dans les règles de politique pour les actions Consigner ou Ignorer, qui contrôlent le niveau de consignation en fonction du trafic observé.

Pour plus d'informations, voir la rubrique Politiques.

Ignorer la session

La demande en cours et le reste de la session sont ignorées. Cette action ne consigne pas les violations de politique, mais elle interrompt la consignation des enregistrements, et elle ne recherche pas les violations de politique, quel que soit leur type, dans le reste de la session. Cette action peut s'avérer utile si, par exemple, la base de données comporte une région de test et qu'il n'est pas nécessaire d'appliquer des règles de politique à cette région de la base de données.

Tableau 1. Ignorer la session

Données consignées ou ignorées entre le client et le serveur de base de données/S-TAP	**Données envoyées depuis le serveur de données/S-TAP au collecteur**	**Données depuis le port SPAN/TAP réseau vers le collecteur**
Ignorer les commandes SQL, les erreurs SQL, les ensembles de résultats	Se connecter/Se déconnecter Sniffer vers S-TAP - Un signal est transmis à l'agent S-TAP pour cesser l'envoi de l'activité relative à cette session. Si d'autres informations d'activité sont envoyées par l'agent S-TAP, elles sont ignorées au niveau du sniffer uniquement. Ignorer les commandes SQL Ignorer les erreurs SQL Ignorer les ensembles de résultats	Ignorer les commandes SQL, les erreurs SQL, les ensembles de résultats Les commandes et erreurs SQL qui proviennent d'un port SPAN ou d'un TAP réseau sont filtrées au niveau du sniffer.

Ignorer la session S-TAP

La demande en cours et le reste de la session S-TAP sont ignorées. Cette action est exécutée en même temps que sont spécifiés sur l'écran de menu du générateur de politique de certaines machines, les utilisateurs ou les applications qui produisent un volume élevé de trafic réseau. Cette action s'avère utile lorsque vous savez que la réponse de base de données provenant de la session S-TAP sera sans intérêt.

Tableau 2. Ignorer la session S-TAP

Données consignées ou ignorées entre le client et le serveur de base de données/S-TAP	**Données envoyées depuis le serveur de données/S-TAP au collecteur**	**Données depuis le port SPAN/TAP réseau vers le collecteur**
Ignorer les commandes SQL, les erreurs SQL, les ensembles de résultats	Se connecter/Se déconnecter Sniffer vers S-TAP - Un signal est transmis à l'agent S-TAP pour cesser l'envoi de l'activité relative à cette session. D'autres signaux sont transmis à l'agent S-TAP our cesser l'envoi de l'activité relative à cette session.	Non applicable Lorsqu'il est nécessaire d'ignorer le trafic entre un port SPAN/TAP réseau, utilisez plutôt l'action Ignorer la session.

Ignorer les réponses par session

Les réponses pour le reste de la session seront ignorées. Cette action consigne les violations de politique, mais elle cesse d'analyser les réponses pour le reste de la session. Cette action s'avère utile lorsque vous savez que la réponse de base de données sera sans intérêt.

Remarque : Concernant l'action Ignorer les réponses par session, dans la mesure où le sniffer est ignoré ou ne reçoit aucune réponse pour la requête, les valeurs pour COUNT_FAILED et SUCCESS correspondent à ce qui est indiqué par défaut dans la table, en l'occurrence, COUNT_FAILED=0 et SUCCESS=1.

Tableau 3. Ignorer les réponses par session

Données consignées ou ignorées entre le client et le serveur de base de données/S-TAP	**Données envoyées depuis le serveur de données/S-TAP au collecteur**	**Données depuis le port SPAN/TAP réseau vers le collecteur**
Consigner - Commandes SQL, Ignorer - Erreurs SQL, ensembles de résultats	Se connecter/Se déconnecter Commandes SQL Sniffer vers S-TAP - Un signal est transmis à l'agent S-TAP pour cesser l'envoi de l'activité relative à cette session. D'autres signaux sont transmis à l'agent S-TAP our cesser l'envoi de l'activité relative à cette session.	Non applicable Cette action de règle concerne uniquement les implémentations S-TAP uniquement.

Ignorer SQL par session

Aucune chaîne SQL n'est consignée pour le reste de la session. Les exceptions seront toujours consignées, mais il se peut que les chaînes correspondantes ne soient pas capturées par le système.

Tableau 4. Ignorer SQL par session

Données consignées ou ignorées entre le client et le serveur de base de données/S-TAP	**Données envoyées depuis le serveur de données/S-TAP au collecteur**	**Données depuis le port SPAN/TAP réseau vers le collecteur**

Données consignées ou ignorées entre le client et le serveur de base de données/S-TAP	Données envoyées depuis le serveur de données/S-TAP au collecteur	Données depuis le port SPAN/TAP réseau vers le collecteur
Ignorer - Commandes SQL Consigner - Erreurs SQL, ensembles de résultats	Se connecter/Se déconnecter Sniffer vers S-TAP - Un signal est transmis à l'agent S-TAP pour cesser l'envoi de l'activité relative à cette session. Si d'autres informations d'activité sont envoyées par l'agent S-TAP, elles sont ignorées au niveau du sniffer uniquement. Consigner les commandes SQL Consigner les erreurs SQL Consigner les ensembles de résultats, si des règles d'extrusion sont utilisées	Ignorer - Commandes SQL Consigner - Erreurs SQL, ensembles de résultats Les commandes SQL sont filtrées au niveau du sniffer.

Trace d'audit sélectif

Utilisez une politique Trace d'audit sélectif pour limiter la quantité de consignation sur le dispositif. Cela s'avère approprié lorsque le trafic d'intérêt représente un pourcentage relativement faible du trafic accepté par les moteurs d'inspection ou lorsque tout le trafic sur lequel vous pourriez souhaiter générer des rapports peut être complètement identifié.

Attention, il est toujours très important d'inclure des règles Ignorer la session dans la politique même s'il s'agit d'une politique Trace d'audit sélectif. Les règles Ignore la session diminuent considérablement la charge sur un collecteur car en filtrant les informations au niveau de l'agent S-TAP, le collecteur ne les reçoit jamais et n'a pas besoin de consommer des ressources en analysant du trafic qui en définitive ne sera pas consigné. Si une politique Trace d'audit sélectif ne comporte pas de règle Ignorer la session, tout le trafic sera envoyé depuis le serveur de base de données vers le collecteur, amenant ainsi ce dernier à analyser chaque commande et ensemble de résultats générés par le serveur de base de données.

Tableau 5. Trace d'audit sélectif

Données consignées ou ignorées entre le client et le serveur de base de données/S-TAP	Données envoyées depuis le serveur de données/S-TAP au collecteur	Données depuis le port SPAN/TAP réseau vers le collecteur
Ignorer - Commandes SQL Consigner - Erreurs SQL, ensembles de résultats	Se connecter/Se déconnecter Ignorer les commandes SQL, sauf pour celles qui sont définies avec les règles Effectuer l'audit uniquement ou Consigner l'ensemble des détails. Consigner les erreurs SQL Consigner les ensembles de résultats, si des règles d'extrusion sont utilisées	Ignorer - Commandes SQL Consigner - Erreurs SQL, ensembles de résultats Les commandes SQL sont filtrées au niveau du sniffer.

Rubrique parent : Politiques

Jeux de caractères

Vous pouvez utiliser des codes de jeux de caractères dans des règles d'extrusion.

Liste de codes de jeux de caractères possibles

ANSI_X3.4-1968 - 1
ANSI_X3.4-1986 - 2
ASCII - 3
CP367 - 4
IBM367 - 5
ISO-IR-6 - 6
ISO646-US - 7
ISO_646.IRV:1991 - 8
US - 9
US-ASCII - 10
CSASCII - 11
UTF-8 - 12
ISO-10646/UCS2 - 13
UCS-2 - 14
CSUNICODE - 15
UCS-2BE - 16
UNICODE - 17
UNICODEBIG - 18
TSCII - 19
UCS-2LE - 20
UNICODELITTLE - 21
ISO-10646/UCS4 - 22
UCS-4 - 23
CSUCS4 - 24
UCS-4BE - 25
UCS-4LE - 26
UTF-16 - 27
UTF-16BE - 28
UTF-16LE - 29

UTF-32 - 30
UTF-32BE - 31
UTF-32LE - 32
UTF7 - 33
UTF-7 - 34
UTF-8 - 35
UCS2 - 36
UCS2 - 37
UCS4 - 38
UCS4 - 39
UTF8 - 40
UTF8 - 41
CP819 - 42
IBM819 - 43
ISO-8859-1 - 44
ISO-IR-100 - 45
ISO8859-1 - 46
ISO_8859-1 - 47
ISO_8859-1:1987 - 48
L1 - 49
LATIN1 - 50
CSISOLATIN1 - 51
ISO-8859-2 - 52
ISO-IR-101 - 53
ISO8859-2 - 54
ISO_8859-2 - 55
ISO_8859-2:1987 - 56
L2 - 57
LATIN2 - 58
CSISOLATIN2 - 59
ISO-8859-3 - 60
ISO-IR-109 - 61
ISO8859-3 - 62
ISO_8859-3 - 63
ISO_8859-3:1988 - 64
L3 - 65
LATIN3 - 66
CSISOLATIN3 - 67
ISO-8859-4 - 68
ISO-IR-110 - 69
ISO8859-4 - 70
ISO_8859-4 - 71
ISO_8859-4:1988 - 72
L4 - 73
LATIN4 - 74
CSISOLATIN4 - 75
CYRILLIC - 76
ISO-8859-5 - 77
ISO-IR-144 - 78
ISO8859-5 - 79
ISO_8859-5 - 80
ISO_8859-5:1988 - 81
CSISOLATINCYRILLIC - 82
ARABIC - 83
ASMO-708 - 84
ECMA-114 - 85
ISO-8859-6 - 86
ISO-IR-127 - 87
ISO8859-6 - 88
ISO_8859-6 - 89
ISO_8859-6:1987 - 90
CSISOLATINARABIC - 91
ECMA-118 - 92
ELOT_928 - 93
GREEK - 94
GREEK8 - 95
ISO-8859-7 - 96
ISO-IR-126 - 97
ISO8859-7 - 98
ISO_8859-7 - 99
ISO_8859-7:1987 - 100
CSISOLATINGREEK - 101
HEBREW - 102
ISO-8859-8 - 103
ISO-IR-138 - 104
ISO8859-8 - 105
ISO_8859-8 - 106
ISO_8859-8:1988 - 107
CSISOLATINHEBREW - 108
ISO-8859-9 - 109

ISO-IR-148 - 110
ISO8859-9 - 111
ISO_8859-9 - 112
ISO_8859-9:1989 - 113
L5 - 114
LATIN5 - 115
CSISOLATIN5 - 116
ISO-8859-10 - 117
ISO-IR-157 - 118
ISO8859-10 - 119
ISO_8859-10 - 120
ISO_8859-10:1992 - 121
L6 - 122
LATIN6 - 123
CSISOLATIN6 - 124
ISO-8859-13 - 125
ISO-8859-13 - 126
ISO-8859-13 - 127
ISO-8859-13 - 128
L7 - 129
LATIN7 - 130
ISO-8859-14 - 131
ISO-CELTIC - 132
ISO-IR-199 - 133
ISO8859-14 - 134
ISO_8859-14 - 135
ISO_8859-14:1998 - 136
L8 - 137
LATIN8 - 138
ISO-8859-15 - 139
ISO-IR-203 - 140
ISO8859-15 - 141
ISO_8859-15 - 142
ISO_8859-15:1998 - 143
ISO-8859-16 - 144
ISO-IR-226 - 145
ISO8859-16 - 146
ISO_8859-16 - 147
ISO_8859-16:2000 - 148
KOI8-R - 149
CSKOI8R? - 150
KOI8U? - 151
KOI8R? - 152
CP1250 - 153
MS-EE - 154
WINDOWS-1250 - 155
CP1251 - 156
MS-CYRL - 157
WINDOWS-1251 - 158
CP1252 - 159
MS-ANSI - 160
WINDOWS-1252 - 161
CP1253 - 162
MS-GREEK - 163
WINDOWS-1253 - 164
CP1254 - 165
MS-TURK - 166
WINDOWS-1254 - 167
CP1255 - 168
MS-HEBR - 169
WINDOWS-1255 - 170
CP1256 - 171
MS-ARAB - 172
WINDOWS-1256 - 173
CP1257 - 174
WINBALTRIM - 175
WINDOWS-1257 - 176
CP1258 - 177
WINDOWS-1258 - 178
850 - 179
CP850 - 180
IBM850 - 181
CSPC850MULTILINGUAL? - 182
862 - 183
CP862 - 184
IBM862 - 185
CSPC862LATINHEBREW? - 186
866 - 187
CP866 - 188
IBM866 - 189

CSIBM866 - 190
MAC - 191
MACINTOSH - 192
MACUK - 193
CSMACINTOSH - 194
MACIS - 195
MAC - 196
MAC - 197
MAC - 198
MAC - 199
MACUKRAINIAN - 200
MAC - 201
MAC - 202
MAC - 203
MAC - 204
MAC - 205
HP-ROMAN8 - 206
R8 - 207
ROMAN8 - 208
HPROMAN8 - 209
ROMAN8 - 210
ARMSCII-8 - 211
GEORGIAN-ACADEMY - 212
GEORGIAN-PS - 213
KOI8-T - 214
KOI8-T - 215
CP1133 - 216
IBM-CP1133 - 217
ISO-IR-166 - 218
TIS-620 - 219
TIS620 - 220
TIS620-0 - 221
TIS620.2529-1 - 222
TIS620.2533-0 - 223
TIS620.2533-1 - 224
CP874 - 225
WINDOWS-874 - 226
VISCII - 227
VISCII - 228
VISCII - 229
TCVN - 230
TCVN-5712 - 231
TCVN5712-1 - 232
TCVN5712-1:1993 - 233
ISO-IR-14 - 234
ISO646-JP - 235
JIS_C6220-1969-RO - 236
JP - 237
CSISO14JISC6220RO? - 238
JISX0201-1976 - 239
JIS_X0201 - 240
X0201 - 241
CSHALFWIDTHKATAKANA - 242
ISO-IR-87 - 243
JIS0208 - 244
JIS_C6226-1983 - 245
JIS_X0208 - 246
JIS_X0208-1983 - 247
JIS_X0208-1990 - 248
X0208 - 249
CSISO87JISX0208? - 250
ISO-IR-159 - 251
JIS_X0212 - 252
JIS_X0212-1990 - 253
JIS_X0212.1990-0 - 254
X0212 - 255
CSISO159JISX02121990? - 256
CN - 257
GB_1988-80 - 258
ISO-IR-57 - 259
ISO646-CN - 260
CSISO57GB1988? - 261
CHINESE - 262
GB_2312-80 - 263
ISO-IR-58 - 264
CSISO58GB231280? - 265
CN-GB-ISOIR165 - 266
ISO-IR-165 - 267
ISO-IR-149 - 268
KOREAN - 269

KSC_5601 - 270
KS_C_5601-1987 - 271
KS_C_5601-1989 - 272
CSKSC56011987 - 273
EUC-JP - 274
EUCJP - 275
EXTENDED_UNIX_CODE_PACKED_FORMAT_FOR_JAPANESE - 276
CSEUCPKDFMTJAPANESE - 277
MS_KANJI - 278
SHIFT-JIS - 279
SHIFT_JIS - 280
SJIS - 281
CSSHIFTJIS - 282
CP932 - 283
ISO-2022-JP - 284
CSISO2022JP? - 285
ISO-2022-JP-1 - 286
ISO-2022-JP-2 - 287
CSISO2022JP2? - 288
CN-GB - 289
EUC-CN - 290
EUCCN - 291
GB2312 - 292
CSGB2312 - 293
CP936 - 294
GBK - 295
GB18030 - 296
ISO-2022-CN - 297
CSISO2022CN? - 298
ISO-2022-CN-EXT - 299
HZ - 300
HZ-GB-2312 - 301
EUC-TW - 302
EUCTW - 303
CSEUCTW - 304
BIG-5 - 305
BIG-FIVE - 306
BIG5 - 307
BIGFIVE - 308
CN-BIG5 - 309
CSBIG5 - 310
CP950 - 311
BIG5-HKSCS - 312
BIG5HKSCS? - 313
EUC-KR - 314
EUCKR - 315
CSEUCKR - 316
CP949 - 317
UHC - 318
CP1361 - 319
JOHAB - 320
ISO-2022-KR - 321
CSISO2022KR? - 322
IBM037 - 323
IBM038 - 324
IBM256 - 325
IBM273 - 326
IBM274 - 327
IBM275 - 328
IBM277 - 329
IBM278 - 330
IBM280 - 331
IBM281 - 332
IBM284 - 333
IBM285 - 334
IBM290 - 335
IBM297 - 336
IBM367 - 337
IBM420 - 338
IBM423 - 339
IBM424 - 340
IBM437 - 341
IBM500 - 342
IBM775 - 343
IBM813 - 344
IBM819 - 345
IBM848 - 346
IBM850 - 347
IBM851 - 348
IBM852 - 349

IBM855 - 350
IBM856 - 351
IBM857 - 352
IBM860 - 353
IBM861 - 354
IBM862 - 355
IBM863 - 356
IBM864 - 357
IBM865 - 358
IBM866 - 359
IBM866NAV? - 360
IBM868 - 361
IBM869 - 362
IBM870 - 363
IBM871 - 364
IBM874 - 365
IBM875 - 366
IBM880 - 367
IBM891 - 368
IBM903 - 369
IBM904 - 370
IBM905 - 371
IBM912 - 372
IBM915 - 373
IBM916 - 374
IBM918 - 375
IBM920 - 376
IBM922 - 377
IBM930 - 378
IBM932 - 379
IBM933 - 380
IBM935 - 381
IBM937 - 382
IBM939 - 383
IBM943 - 384
IBM1004 - 385
IBM1026 - 386
IBM1046 - 387
IBM1047 - 388
IBM1089 - 389
IBM1124 - 390
IBM1129 - 391
IBM1132 - 392
IBM1133 - 393
IBM1160 - 394
IBM1161 - 395
IBM1162 - 396
IBM1163 - 397
IBM1164 - 398
MSCP949 - 399
EUC-JISX0213 - 400
UJIS - 401
CP852 - 402
EUCJP-MS - 403
IBM902 - 404
IBM921 - 405
WINDOWS-31J - 406
IBM1025 - 407
IBM1140 - 408
IBM1137 - 409
IBM1122 - 410
IBM1141 - 411
IBM1142 - 412
IBM1143 - 413
IBM1144 - 414
IBM1145 - 415
IBM1146 - 416
IBM1147 - 417
IBM1148 - 418
IBM1149 - 419
IBM1153 - 420
IBM1155 - 421
IBM1157 - 422
EBCDICUS - 423
IBM1112 - 424
IBM1158 - 425
437 - 426
500g - 427
500V1g - 428
851g - 429

852g - 430
855g - 431
856g - 432
857g - 433
860g - 434
861g - 435
863g - 436
864g - 437
865g - 438
866NAVg - 439
869g - 440
874g - 441
904g - 442
1026g - 443
1046g - 444
1047g - 445
8859_1g - 446
8859_2g - 447
8859_3g - 448
8859_4g - 449
8859_5g - 450
8859_6g - 451
8859_7g - 452
8859_8g - 453
8859_9g - 454
10646-1:1993g - 455
10646-1:1993/UCS4/ - 456
ANSI_X3.4g - 457
ANSI_X3.110-1983g - 458
ANSI_X3.110g - 459
ARABIC7g - 460
ASMO_449g - 461
BALTICg - 462
BIG-5g - 463
BIG-FIVEg - 464
BIG5-HKSCSg - 465
BIG5g - 466
BIG5HKSCSg? - 467
BIGFIVEg - 468
BS_4730g - 469
CAg - 470
CN-BIG5g - 471
CN-GBg - 472
CNg - 473
CP-ARg - 474
CP-GRg - 475
CP-HUg - 476
CP037g - 477
CP038g - 478
CP273g - 479
CP274g - 480
CP275g - 481
CP278g - 482
CP280g - 483
CP281g - 484
CP282g - 485
CP284g - 486
CP285g - 487
CP290g - 488
CP297g - 489
CP420g - 490
CP423g - 491
CP424g - 492
CP437g - 493
CP500g - 494
CP737g - 495
CP775g - 496
CP803g - 497
CP813g - 498
CP851g - 499
CP852g - 500
CP855g - 501
CP856g - 502
CP857g - 503
CP860g - 504
CP861g - 505
CP863g - 506
CP864g - 507
CP865g - 508
CP866NAVg? - 509

CP868g - 510
CP869g - 511
CP870g - 512
CP871g - 513
CP875g - 514
CP880g - 515
CP891g - 516
CP901g - 517
CP902g - 518
CP903g - 519
CP904g - 520
CP905g - 521
CP912g - 522
CP915g - 523
CP916g - 524
CP918g - 525
CP920g - 526
CP921g - 527
CP922g - 528
CP930g - 529
CP932g - 530
CP933g - 531
CP935g - 532
CP936g - 533
CP937g - 534
CP939g - 535
CP949g - 536
CP950g - 537
CP1004g - 538
CP1008g - 539
CP1025g - 540
CP1026g - 541
CP1046g - 542
CP1047g - 543
CP1070g - 544
CP1079g - 545
CP1081g - 546
CP1084g - 547
CP1089g - 548
CP1097g - 549
CP1112g - 550
CP1122g - 551
CP1123g - 552
CP1124g - 553
CP1125g - 554
CP1129g - 555
CP1130g - 556
CP1132g - 557
CP1137g - 558
CP1140g - 559
CP1141g - 560
CP1142g - 561
CP1143g - 562
CP1144g - 563
CP1145g - 564
CP1146g - 565
CP1147g - 566
CP1148g - 567
CP1149g - 568
CP1153g - 569
CP1154g - 570
CP1155g - 571
CP1156g - 572
CP1157g - 573
CP1158g - 574
CP1160g - 575
CP1161g - 576
CP1162g - 577
CP1163g - 578
CP1164g - 579
CP1166g - 580
CP1167g - 581
CP1361g - 582
CP1364g - 583
CP1371g - 584
CP1388g - 585
CP1390g - 586
CP1399g - 587
CP4517g - 588
CP4899g - 589

CP4909g - 590
CP4971g - 591
CP5347g - 592
CP9030g - 593
CP9066g - 594
CP9448g - 595
CP10007g - 596
CP12712g - 597
CP16804g - 598
CPIBM861g - 599
CSA7-1g - 600
CSA7-2g - 601
CSA_T500-1983g - 602
CSA_T500g - 603
CSA_Z243.4-1985-1g - 604
CSA_Z243.4-1985-2g - 605
CSA_Z243.419851g - 606
CSA_Z243.419852g - 607
CSDECMCSg - 608
CSEBCDICATDEg - 609
CSEBCDICATDEAg - 610
CSEBCDICCAFRg - 611
CSEBCDICDKNOg - 612
CSEBCDICDKNOAg - 613
CSEBCDICESg - 614
CSEBCDICESAg - 615
CSEBCDICESSg - 616
CSEBCDICFISEg - 617
CSEBCDICFISEAg - 618
CSEBCDICFRg - 619
CSEBCDICITg - 620
CSEBCDICPTg - 621
CSEBCDICUKg - 622
CSEBCDICUSg - 623
CSEUCKRg - 624
CSEUCPKDFMTJAPANESEg - 625
CSGB2312g - 626
CSIBM037g - 627
CSIBM038g - 628
CSIBM273g - 629
CSIBM274g - 630
CSIBM275g - 631
CSIBM277g - 632
CSIBM278g - 633
CSIBM280g - 634
CSIBM281g - 635
CSIBM284g - 636
CSIBM285g - 637
CSIBM290g - 638
CSIBM297g - 639
CSIBM420g - 640
CSIBM423g - 641
CSIBM424g - 642
CSIBM500g - 643
CSIBM803g - 644
CSIBM851g - 645
CSIBM855g - 646
CSIBM856g - 647
CSIBM857g - 648
CSIBM860g - 649
CSIBM863g - 650
CSIBM864g - 651
CSIBM865g - 652
CSIBM868g - 653
CSIBM869g - 654
CSIBM870g - 655
CSIBM871g - 656
CSIBM880g - 657
CSIBM891g - 658
CSIBM901g - 659
CSIBM902g - 660
CSIBM903g - 661
CSIBM904g - 662
CSIBM905g - 663
CSIBM918g - 664
CSIBM921g - 665
CSIBM922g - 666
CSIBM930g - 667
CSIBM932g - 668
CSIBM933g - 669

CSIBM935g - 670
CSIBM937g - 671
CSIBM939g - 672
CSIBM943g - 673
CSIBM1008g - 674
CSIBM1025g - 675
CSIBM1026g - 676
CSIBM1097g - 677
CSIBM1112g - 678
CSIBM1122g - 679
CSIBM1123g - 680
CSIBM1124g - 681
CSIBM1129g - 682
CSIBM1130g - 683
CSIBM1132g - 684
CSIBM1133g - 685
CSIBM1137g - 686
CSIBM1140g - 687
CSIBM1141g - 688
CSIBM1142g - 689
CSIBM1143g - 690
CSIBM1144g - 691
CSIBM1145g - 692
CSIBM1146g - 693
CSIBM1147g - 694
CSIBM1148g - 695
CSIBM1149g - 696
CSIBM1153g - 697
CSIBM1154g - 698
CSIBM1155g - 699
CSIBM1156g - 700
CSIBM1157g - 701
CSIBM1158g - 702
CSIBM1160g - 703
CSIBM1161g - 704
CSIBM1163g - 705
CSIBM1164g - 706
CSIBM1166g - 707
CSIBM1167g - 708
CSIBM1364g - 709
CSIBM1371g - 710
CSIBM1388g - 711
CSIBM1390g - 712
CSIBM1399g - 713
CSIBM4517g - 714
CSIBM4899g - 715
CSIBM4909g - 716
CSIBM4971g - 717
CSIBM5347g - 718
CSIBM9030g - 719
CSIBM9066g - 720
CSIBM9448g - 721
CSIBM12712g - 722
CSIBM16804g - 723
CSIBM11621162g - 724
CSISO4UNITEDKINGDOMg? - 725
CSISO10SWEDISHg? - 726
CSISO11SWEDISHFORNAMESg? - 727
CSISO15ITALIANg? - 728
CSISO16PORTUGESEg? - 729
CSISO17SPANISHg? - 730
CSISO18GREEK7OLDg? - 731
CSISO19LATINGREEKg? - 732
CSISO21GERMANg? - 733
CSISO25FRENCHg? - 734
CSISO27LATINGREEK1g? - 735
CSISO49INISg? - 736
CSISO50INIS8g? - 737
CSISO51INISCYRILLICg? - 738
CSISO58GB1988g? - 739
CSISO60DANISHNORWEGIANg? - 740
CSISO60NORWEGIAN1g? - 741
CSISO61NORWEGIAN2g? - 742
CSISO69FRENCHg? - 743
CSISO84PORTUGUESE2g? - 744
CSISO85SPANISH2g? - 745
CSISO86HUNGARIANg? - 746
CSISO88GREEK7g? - 747
CSISO89ASMO449g? - 748
CSISO90g - 749

CSISO92JISC62991984Bg? - 750
CSISO99NAPLPSg? - 751
CSISO103T618BITg? - 752
CSISO111ECMACYRILLICg? - 753
CSISO121CANADIAN1g? - 754
CSISO122CANADIAN2g? - 755
CSISO139CSN369103g? - 756
CSISO141JUSIB1002g? - 757
CSISO143IECP271g? - 758
CSISO150g - 759
CSISO150GREEKCCITTg? - 760
CSISO151CUBAg? - 761
CSISO153GOST1976874g? - 762
CSISO646DANISHg? - 763
CSISO2022CNg? - 764
CSISO2022JPg? - 765
CSISO2022JP2g? - 766
CSISO2022KRg? - 767
CSISO2033g - 768
CSISO5427CYRILLICg? - 769
CSISO5427CYRILLIC1981g? - 770
CSISO5428GREEKg? - 771
CSISO10367BOXg? - 772
CSKSC5636g - 773
CSNATSDANOg - 774
CSNATSSEFIg - 775
CSN_369103g - 776
CSPC8CODEPAGE437g? - 777
CSPC775BALTICg? - 778
CSPCP852g - 779
CSSHIFTJISg - 780
CSUCS4g - 781
CSWINDOWS31Jg? - 782
CUBAg - 783
CWI-2g - 784
CWIg - 785
DEg - 786
DEC-MCSg - 787
DECg - 788
DECMCSg - 789
DIN_66003g - 790
DKg - 791
DS2089g - 792
DS_2089g - 793
E13Bg? - 794
EBCDIC-AT-DE-Ag - 795
EBCDIC-AT-DEg - 796
EBCDIC-BEg - 797
EBCDIC-BRg - 798
EBCDIC-CA-FRg - 799
EBCDIC-CP-AR1g - 800
EBCDIC-CP-AR2g - 801
EBCDIC-CP-BEg - 802
EBCDIC-CP-CAg - 803
EBCDIC-CP-CHg - 804
EBCDIC-CP-DKg - 805
EBCDIC-CP-ESg - 806
EBCDIC-CP-FIg - 807
EBCDIC-CP-FRg - 808
EBCDIC-CP-GBg - 809
EBCDIC-CP-GRg - 810
EBCDIC-CP-HEg - 811
EBCDIC-CP-ISg - 812
EBCDIC-CP-ITg - 813
EBCDIC-CP-NLg - 814
EBCDIC-CP-NOg - 815
EBCDIC-CP-ROECEg - 816
EBCDIC-CP-SEg - 817
EBCDIC-CP-TRg - 818
EBCDIC-CP-USg - 819
EBCDIC-CP-WTg - 820
EBCDIC-CP-YUg - 821
EBCDIC-CYRILLICg - 822
EBCDIC-DK-NO-Ag - 823
EBCDIC-DK-NOg - 824
EBCDIC-ES-Ag - 825
EBCDIC-ES-Sg - 826
EBCDIC-ESg - 827
EBCDIC-FI-SE-Ag - 828
EBCDIC-FI-SEg - 829

EBCDIC-FRg - 830
EBCDIC-GREEKg - 831
EBCDIC-INTg - 832
EBCDIC-INT1g - 833
EBCDIC-IS-FRISSg - 834
EBCDIC-ITg - 835
EBCDIC-JP-Eg - 836
EBCDIC-JP-KANAg - 837
EBCDIC-PTg - 838
EBCDIC-UKg - 839
EBCDIC-USg - 840
EBCDICATDEg - 841
EBCDICATDEAg - 842
EBCDICCAFRg - 843
EBCDICDKNOg - 844
EBCDICDKNOAg - 845
EBCDICESg - 846
EBCDICESAg - 847
EBCDICESSg - 848
EBCDICFISEg - 849
EBCDICFISEAg - 850
EBCDICFRg - 851
EBCDICISFRISSg - 852
EBCDICITg - 853
EBCDICPTg - 854
EBCDICUKg - 855
EBCDICUSg - 856
ECMA-128g - 857
ECMA-CYRILLICg - 858
ECMACYRILLICg - 859
ESg - 860
ES2g - 861
EUC-CNg - 862
EUC-JISX0213g - 863
EUC-JP-MSg - 864
EUC-JPg - 865
EUC-KRg - 866
EUC-TWg - 867
EUCCNg - 868
EUCJP-MSg - 869
EUCJP-OPENg - 870
EUCJP-WINg - 871
EUCJPg - 872
EUCKRg - 873
EUCTWg - 874
FIg - 875
FRg - 876
GBg - 877
GB2312g - 878
GB13000g - 879
GB18030g - 880
GBKg - 881
GB_1988-80g - 882
GB_198880g - 883
GOST_19768-74g - 884
GOST_19768g - 885
GOST_1976874g - 886
GREEK-CCITTg - 887
GREEK7-OLDg - 888
GREEK7g - 889
GREEK7OLDg? - 890
GREEKCCITTg - 891
HUg - 892
IBM-803g - 893
IBM-856g - 894
IBM-901g - 895
IBM-902g - 896
IBM-921g - 897
IBM-922g - 898
IBM-930g - 899
IBM-932g - 900
IBM-933g - 901
IBM-935g - 902
IBM-937g - 903
IBM-939g - 904
IBM-943g - 905
IBM-1008g - 906
IBM-1025g - 907
IBM-1046g - 908
IBM-1047g - 909

IBM-1097g - 910
IBM-1112g - 911
IBM-1122g - 912
IBM-1123g - 913
IBM-1124g - 914
IBM-1129g - 915
IBM-1130g - 916
IBM-1132g - 917
IBM-1133g - 918
IBM-1137g - 919
IBM-1140g - 920
IBM-1141g - 921
IBM-1142g - 922
IBM-1143g - 923
IBM-1144g - 924
IBM-1145g - 925
IBM-1146g - 926
IBM-1147g - 927
IBM-1148g - 928
IBM-1149g - 929
IBM-1153g - 930
IBM-1154g - 931
uIBM-1155g - 932
IBM-1156g - 933
IBM-1157g - 934
IBM-1158g - 935
IBM-1160g - 936
IBM-1161g - 937
IBM-1162g - 938
IBM-1163g - 939
IBM-1164g - 940
IBM-1166g - 941
IBM-1167g - 942
IBM-1364g - 943
IBM-1371g - 944
IBM-1388g - 945
IBM-1390g - 946
IBM-1399g - 947
IBM-4517g - 948
IBM-4899g - 949
IBM-4909g - 950
IBM-4971g - 951
IBM-5347g - 952
IBM-9030g - 953
IBM-9066g - 954
IBM-9448g - 955
IBM-12712g - 956
IBM-16804g - 957
IBM037g - 958
IBM038g - 959
IBM256g - 960
IBM273g - 961
IBM274g - 962
IBM275g - 963
IBM277g - 964
IBM278g - 965
IBM280g - 966
IBM281g - 967
IBM284g - 968
IBM285g - 969
IBM290g - 970
IBM297g - 971
IBM420g - 972
IBM423g - 973
IBM424g - 974
IBM437g - 975
IBM500g - 976
IBM775g - 977
IBM803g - 978
IBM813g - 979
IBM848g - 980
IBM851g - 981
IBM852g - 982
IBM855g - 983
IBM856g - 984
IBM857g - 985
IBM860g - 986
IBM861g - 987
IBM863g - 988
IBM864g - 989

IBM865g - 990
IBM866NAVg? - 991
IBM868g - 992
IBM869g - 993
IBM870g - 994
IBM871g - 995
IBM874g - 996
IBM875g - 997
IBM880g - 998
IBM891g - 999
IBM901g - 1000
IBM902g - 1001
IBM903g - 1002
IBM904g - 1003
IBM905g - 1004
IBM912g - 1005
IBM915g - 1006
IBM916g - 1007
IBM918g - 1008
IBM920g - 1009
IBM921g - 1010
IBM922g - 1011
IBM930g - 1012
IBM932g - 1013
IBM933g - 1014
IBM935g - 1015
IBM937g - 1016
IBM939g - 1017
IBM943g - 1018
IBM1004g - 1019
IBM1008g - 1020
IBM1025g - 1021
IBM1026g - 1022
IBM1046g - 1023
IBM1047g - 1024
IBM1089g - 1025
IBM1097g - 1026
IBM1112g - 1027
IBM1122g - 1028
IBM1123g - 1029
IBM1124g - 1030
IBM1129g - 1031
IBM1130g - 1032
IBM1132g - 1033
IBM1133g - 1034
IBM1137g - 1035
IBM1140g - 1036
IBM1141g - 1037
IBM1142g - 1038
IBM1143g - 1039
IBM1144g - 1040
IBM1145g - 1041
IBM1146g - 1042
IBM1147g - 1043
IBM1148g - 1044
IBM1149g - 1045
IBM1153g - 1046
IBM1154g - 1047
IBM1155g - 1048
IBM1156g - 1049
IBM1157g - 1050
IBM1158g - 1051
IBM1160g - 1052
IBM1161g - 1053
IBM1162g - 1054
IBM1163g - 1055
IBM1164g - 1056
IBM1166g - 1057
IBM1167g - 1058
IBM1364g - 1059
IBM1371g - 1060
IBM1388g - 1061
IBM1390g - 1062
IBM1399g - 1063
IBM4517g - 1064
IBM4899g - 1065
IBM4909g - 1066
IBM4971g - 1067
IBM5347g - 1068
IBM9030g - 1069

IBM9066g - 1070
IBM9448g - 1071
IBM12712g - 1072
IBM16804g - 1073
IEC_P27-1g - 1074
IEC_P271g - 1075
INIS-8g - 1076
INIS-CYRILLICg - 1077
INISg - 1078
INIS8g - 1079
INISCYRILLICg - 1080
ISIRI-3342g - 1081
ISIRI3342g - 1082
ISO-2022-CN-EXTg - 1083
ISO-2022-CNg - 1084
ISO-2022-JP-2g - 1085
ISO-2022-JP-3g - 1086
ISO-2022-JPg - 1087
ISO-2022-KRg - 1088
ISO-8859-9g - 1089
ISO-8859-10g - 1090
ISO-8859-11g - 1091
ISO-8859-16g - 1092
ISO-10646g - 1093
ISO-10646/UTF-8/ - 1094
ISO-10646/UTF8/ - 1095
ISO-IR-4g - 1096
ISO-IR-8-1g - 1097
ISO-IR-9-1g - 1098
ISO-IR-10g - 1099
ISO-IR-11g - 1100
ISO-IR-15g - 1101
ISO-IR-16g - 1102
ISO-IR-17g - 1103
ISO-IR-18g - 1104
ISO-IR-19g - 1105
ISO-IR-21g - 1106
ISO-IR-25g - 1107
ISO-IR-27g - 1108
ISO-IR-37g - 1109
ISO-IR-49g - 1110
ISO-IR-50g - 1111
ISO-IR-51g - 1112
ISO-IR-54g - 1113
ISO-IR-55g - 1114
ISO-IR-57g - 1115
ISO-IR-60g - 1116
ISO-IR-61g - 1117
ISO-IR-69g - 1118
ISO-IR-84g - 1119
ISO-IR-85g - 1120
ISO-IR-86g - 1121
ISO-IR-88g - 1122
ISO-IR-89g - 1123
ISO-IR-90g - 1124
ISO-IR-92g - 1125
ISO-IR-98g - 1126
ISO-IR-99g - 1127
ISO-IR-103g - 1128
ISO-IR-111g - 1129
ISO-IR-121g - 1130
ISO-IR-122g - 1131
ISO-IR-127g - 1132
ISO-IR-139g - 1133
ISO-IR-141g - 1134
ISO-IR-143g - 1135
ISO-IR-150g - 1136
ISO-IR-151g - 1137
ISO-IR-153g - 1138
ISO-IR-155g - 1139
ISO-IR-156g - 1140
ISO-IR-166g - 1141
ISO-IR-193g - 1142
ISO-IR-197g - 1143
ISO-IR-209g - 1144
ISO/TR_11548-1/ - 1145
ISO646-CAg - 1146
ISO646-CA2g - 1147
ISO646-CNg - 1148
ISO646-CUg - 1149

ISO646-DEg - 1150
ISO646-DKg - 1151
ISO646-ESg - 1152
ISO646-ES2g - 1153
ISO646-FIg - 1154
ISO646-FRg - 1155
ISO646-FR1g - 1156
ISO646-GBg - 1157
ISO646-HUg - 1158
ISO646-ITg - 1159
ISO646-JP-OCR-Bg - 1160
ISO646-KRg - 1161
ISO646-NOg - 1162
ISO646-NO2g - 1163
ISO646-PTg - 1164
ISO646-PT2g - 1165
ISO646-SEg - 1166
ISO646-SE2g - 1167
ISO646-YUg - 1168
ISO2022CNg? - 1169
ISO2022CNEXTg? - 1170
ISO2022JPg? - 1171
ISO2022JP2g? - 1172
ISO2022KRg? - 1173
ISO6937g - 1174
ISO8859-11g - 1175
ISO11548-1g - 1176
ISO88591g - 1177
ISO88592g - 1178
ISO88593g - 1179
ISO88594g - 1180
ISO88595g - 1181
ISO88596g - 1182
ISO88597g - 1183
ISO88598g - 1184
ISO88599g - 1185
ISO885910g - 1186
ISO885911g - 1187
ISO885913g - 1188
ISO885914g - 1189
ISO885915g - 1190
ISO885916g - 1191
ISO_2033-1983g - 1192
ISO_2033g - 1193
ISO_5427-EXTg - 1194
ISO_5427g - 1195
ISO_5427:1981g - 1196
ISO_5427EXTg - 1197
ISO_5428g - 1198
ISO_5428:1980g - 1199
ISO_6937-2g - 1200
ISO_6937-2:1983g - 1201
ISO_6937g - 1202
ISO_6937:1992g - 1203
ISO_8859-7:2003g - 1204
ISO_8859-16:2001g - 1205
ISO_9036g - 1206
ISO_10367-BOXg - 1207
ISO_10367BOXg - 1208
ISO_11548-1g - 1209
ISO_69372g - 1210
ITg - 1211
JIS_C6229-1984-Bg - 1212
JIS_C62201969ROg - 1213
JIS_C62291984Bg - 1214
JOHABg - 1215
JP-OCR-Bg - 1216
JSg - 1217
JUS_I.B1.002g - 1218
KOI-7g - 1219
KOI-8g - 1220
KOI8g - 1221
KSC5636g - 1222
L10g - 1223
LATIN-9g - 1224
LATIN-GREEK-1g - 1225
LATIN-GREEKg - 1226
LATIN10g - 1227
LATINGREEKg - 1228
LATINGREEK1g - 1229

MAC-CYRILLICg - 1230
MAC-ISg - 1231
MAC-SAMIg - 1232
MAC-UKg - 1233
MACCYRILLICg - 1234
MIKg - 1235
MS-MAC-CYRILLICg - 1236
MS932g - 1237
MS936g - 1238
MSCP949g - 1239
MSCP1361g - 1240
MSMACCYRILLICg - 1241
MSZ_7795.3g - 1242
MS_KANJIg - 1243
NAPLPSg - 1244
NATS-DANOg - 1245
NATS-SEFIg - 1246
NATSDANOg - 1247
NATSSEFIg - 1248
NC_NC0010g - 1249
NC_NC00-10g - 1250
NC_NC00-10:81g - 1251
NF_Z_62-010g - 1252
NF_Z_62-010_(1973)g - 1253
NF_Z_62-010_1973g - 1254
NF_Z_62010g - 1255
NF_Z_62010_1973g - 1256
NOg - 1257
NO2g - 1258
NS_4551-1g - 1259
NS_4551-2g - 1260
NS_45511g - 1261
NS_45512g - 1262
OS2LATIN1g? - 1263
OSF00010001g - 1264
OSF00010002g - 1265
OSF00010003g - 1266
OSF00010004g - 1267
OSF00010005g - 1268
OSF00010006g - 1269
OSF00010007g - 1270
OSF00010008g - 1271
OSF00010009g - 1272
OSF0001000Ag? - 1273
OSF00010020g - 1274
OSF00010100g - 1275
OSF00010101g - 1276
OSF00010102g - 1277
OSF00010104g - 1278
OSF00010105g - 1279
OSF00010106g - 1280
OSF00030010g - 1281
OSF0004000Ag? - 1282
OSF0005000Ag? - 1283
OSF05010001g - 1284
OSF100201A4g? - 1285
OSF100201A8g? - 1286
OSF100201B5g? - 1287
OSF100201F4g? - 1288
OSF100203B5g? - 1289
OSF1002011Cg? - 1290
OSF1002011Dg? - 1291
OSF1002035Dg? - 1292
OSF1002035Eg? - 1293
OSF1002035Fg? - 1294
OSF1002036Bg? - 1295
OSF1002037Bg? - 1296
OSF10010001g - 1297
OSF10020025g - 1298
OSF10020111g - 1299
OSF10020115g - 1300
OSF10020116g - 1301
OSF10020118g - 1302
OSF10020122g - 1303
OSF10020129g - 1304
OSF10020352g - 1305
OSF10020354g - 1306
OSF10020357g - 1307
OSF10020359g - 1308
OSF10020360g - 1309

OSF10020364g - 1310
OSF10020365g - 1311
OSF10020366g - 1312
OSF10020367g - 1313
OSF10020370g - 1314
OSF10020387g - 1315
OSF10020388g - 1316
OSF10020396g - 1317
OSF10020402g - 1318
OSF10020417g - 1319
PTg - 1320
PT2g - 1321
PT154g - 1322
RK1048g - 1323
RUSCIIg - 1324
SEg - 1325
SE2g - 1326
SEN_850200_Bg - 1327
SEN_850200_Cg - 1328
SHIFT-JISg - 1329
SHIFT_JISg - 1330
SHIFT_JISX0213g - 1331
SJIS-OPENg - 1332
SJIS-WINg - 1333
SJISg - 1334
SS636127g - 1335
STRK1048-2002g - 1336
ST_SEV_358-88g - 1337
T.61-8BITg - 1338
T.61g - 1339
T.618BITg - 1340
TS-5881g - 1341
UHCg - 1342
UJISg - 1343
UKg - 1344
UTF8g - 1345
UTF16g - 1346
UTF16BEg? - 1347
UTF16LEg? - 1348
UTF32g - 1349
UTF32BEg? - 1350
UTF32LEg? - 1351
WCHAR_Tg - 1352
WIN-SAMI-2g - 1353
WINDOWS-31Jg - 1354
WINDOWS-936g - 1355
WINSAMI2g - 1356
WS2g - 1357
YUg - 1358

Rubrique parent : Politiques

Alertes de corrélation

Une alerte est un message indiquant qu'une exception ou une violation de règle de politique a été détectée.

Les alertes sont déclenchées de deux manières :

- Une *alerte de corrélation* est déclenchée par une requête qui effectue une recherche en arrière sur une période spécifiée afin de déterminer si le seuil d'alerte a été atteint. Le moteur de détection des anomalies Guardium exécute des requêtes de corrélation de manière planifiée. Par défaut, les alertes de corrélation ne consignent pas les violations de politique, mais il est possible de les configurer pour cela.
- Une *alerte en temps réel* est déclenchée par une règle de politique de sécurité. Le moteur d'inspection Guardium exécute la politique de sécurité lorsqu'il collecte et analyse le trafic de base de données en temps réel.

Quelle que soit la façon dont elles sont déclenchées, Guardium consigne toutes les alertes de la même façon : les informations d'alerte sont consignées dans la base de données interne de Guardium. La quantité et le type d'informations consignées varient selon le type d'alerte spécifique. L'avertisseur Guardium, également exécuté de façon planifiée, traite chaque nouvelle alerte en transmettant les informations consignées pour chaque alerte à n'importe quelle combinaison des mécanismes de notification suivants :

- SMTP – Serveur SMTP (messages sortants). Le composant Alerter transmet des messages standard au serveur SMTP pour lequel il a été configuré.
- SNMP – Serveur SNMP (contrôle et informations réseau). Lorsque la valeur SNMP est sélectionnée pour une notification d'alerte, le composant Alerter transmet tous les messages d'alerte de ce type à la seule communauté d'interception pour laquelle il a été configuré.
- Syslog – L'alerte est consignée dans syslog sur le dispositif Guardium (qui peut être configuré par l'administrateur Guardium pour écrire les messages syslog sur un système distant).
  Remarque : Pour SNMP ou SYSLOG, la longueur maximale du message est de 3 000 caractères. Les messages qui sont plus longs seront tronqués.
- Personnalisé - Classe Java™ écrite par les utilisateurs pour gérer les alertes. Le composant Alerter transmet un message d'alerte et une valeur d'horodatage à la classe d'alerte personnalisée. Il peut y avoir plusieurs classes d'alerte personnalisées, et une classe d'alerte personnalisée peut être une extension d'une autre classe d'alerte personnalisée.

Remarque : La sécurité au niveau des données ne peut pas être appliquée à la définition et la notification d'alertes. Les raisons à cela sont notamment les suivantes : les alertes ne sont pas évaluées dans le contexte d'utilisateur, l'alerte peut être liée aux bases de données associées à plusieurs utilisateurs et pour éviter que personne ne reçoive la notification d'alerte.
Remarque : S'il existe une alerte qui utilise une requête contenant au moins 30 champs (y compris des compteurs), la détection des anomalies échoue et un message d'erreur `Array out of bound exception` est généré. Les requêtes comportant au moins 30 colonnes ne peuvent pas être utilisées pour les alertes. De telles requêtes n'apparaissent pas dans la liste des requêtes disponibles pour les alertes de seuil.

Tâches d'alerte pour les administrateurs

Les administrateurs Guardium effectuent les tâches suivantes :

- Personnaliser le modèle de message d'alerte, à l'aide du profil global
- Configurer et démarrer le composant Alerter, qui distribue des messages à des SMTP, SNMP, Syslog ou des classes d'alerte personnalisées
- Démarrer et arrêter le moteur de détection des anomalies, qui exécute les alertes de corrélation en fonction des planifications définies
- Télécharger des classes d'alerte personnalisées sur le système Guardium

Tâches d'alerte pour les utilisateurs

Les utilisateurs (et administrateurs) Guardium peuvent effectuer les tâches d'alerte de corrélation suivantes :

- Définir des requêtes qui peuvent être utilisées pour des alertes de corrélation
- Définir des alertes de corrélation
- Ecrire des classes d'alerte personnalisées

A propos des requêtes d'alerte de corrélation

Une alerte de corrélation est basée sur une requête dans n'importe lequel des domaines de génération de rapports. Cette requête doit impérativement être définie avant l'alerte. Pour pouvoir être utilisée par une alerte de corrélation, la requête doit contenir au moins un champ de date.

Création d'une alerte de corrélation

1. Cliquez sur Protection > Détection d'intrusion de base de données > Générateur d'alerte pour ouvrir le panneau Localiseur d'alerte.
2. Cliquez sur Nouveau dans le panneau Localiseur d'alerte pour afficher le panneau Ajouter une alerte.
3. Entrez un nom unique pour l'alerte dans le champ Nom. N'ajoutez pas d'apostrophes dans le nom de l'alerte.
4. Entrez une courte description pour l'alerte dans le champ Description.
5. Entrez une catégorie facultative dans le champ Catégorie.
6. Entrez une classification facultative dans le champ Classification.
7. Dans le champ Action recommandée, l'utilisateur peut ajouter un texte libre comme action recommandée pour l'alerte spécifique.
8. Comme dans les alertes en temps réel, l'utilisateur peut choisir un modèle pour le message qui est envoyé en cas de déclenchement de l'alerte de seuil. Le modèle utilise une liste prédéfinie de variables qui sont remplacées par la valeur appropriée pour l'alerte spécifique. La liste de variables et un modèle par défaut sont décrits en détail dans la section Modèles nommés de la rubrique d'aide sur le profil global.
9. Sélectionnez un niveau de gravité dans la liste Gravité. Lorsque la valeur ELEVE est définie pour une alerte e-mail, l'e-mail contient la mention Urgent.
10. Entrez le nombre de minutes entre les exécutions de la requête dans le champ Fréquence d'exécution.
11. Cochez la case Actif pour activer l'alerte ou désélectionnez la case pour sauvegarder la définition d'alerte sans lancer son exécution (elle pourra être activée ultérieurement). Dans un environnement Central Manager, l'alerte est activée (ou arrêtée) sur toutes les unités gérées lorsque cette case à cocher est sélectionnée (ou désélectionnée). Pour désactiver l'alerte sur un dispositif spécifique dans un environnement Central Manager, utilisez le panneau Détection des anomalies de la console d'administrateur.
12. Cochez la case Consigner une violation de politique pour consigner une violation de politique au déclenchement de cette alerte. Par défaut, les alertes de corrélation sont consignées uniquement dans le domaine Suivi des alertes. En cochant cette case, les alertes de corrélation et les alertes en temps réel (émises par la politique de sécurité relative à l'accès aux données) peuvent être visualisées en même temps, dans le domaine Violations de politique.
13. Dans la liste de requêtes sur le panneau Définition d'alerte, sélectionnez la requête à exécuter pour cette alerte. La liste de requêtes affichées inclura toutes les requêtes définies qui :
    - Contiennent au moins un champ de date (horodatage) (un champ d'horodatage est requis)
    - Contiennent un champ Nombre (un champ de comptage est requis)
    - Sont accessibles via votre compte utilisateur Guardium

    Astuces pour l'identification et la résolution des problèmes
    - Si une requête personnalisée a été créée dans n'importe quel générateur de requête dans l'application Générateur de rapport et qu'elle n'apparaît pas dans la liste de requêtes, assurez-vous qu'elle comporte une valeur d'horodatage (champ de date).
    - Après avoir sélectionné une requête dans la liste de requêtes sur le panneau Définition d'alerte de l'écran Ajouter une alerte, si cette requête doit être éditée (icône Editer) et qu'elle n'est pas modifiable, accédez à Générateur de requête (Outils > Générateur de rapport) pour l'éditer.
14. Si la requête sélectionnée contient des paramètres d'exécution, un panneau Paramètres de requête apparaîtra dans la sous-fenêtre Définition d'alerte. Indiquez des valeurs de paramètre selon vos besoins pour votre application.
15. Dans la case Intervalle d'accumulation, entrez la durée de l'intervalle (en minutes) pendant lequel la requête doit examiner le référentiel d'audit, en comptant à rebours à partir de l'heure en cours (par exemple, entrez 10 pour examiner les données correspondant aux 10 dernières minutes).
    Remarque : Les alertes qui s'exécutent sur des regroupeurs sont basées uniquement sur les données avec la période de fusion définie.
16. Cochez la case Consigner l'ensemble des résultats d'une requête pour que le rapport complet soit consigné avec l'alerte.
17. Si la requête sélectionnée contient une ou plusieurs colonnes de données numériques, sélectionnez-en une afin de l'utiliser pour le test. La valeur par défaut, qui sera le dernier élément de la liste, est la dernière colonne pour la requête, et correspond toujours au nombre d'occurrences agrégées dans cette ligne.
18. Dans la sous-fenêtre Seuil d'alerte, définissez le seuil auquel une alerte de corrélation doit être générée, comme suit :
    - Dans le champ Seuil, entrez un nombre correspondant au seuil qui sera appliqué selon les modalités définies dans les autres champs du panneau.
    - Dans la liste Alerter lorsque la valeur est, sélectionnez un opérateur indiquant la façon dont la valeur de rapport doit être associée au seuil pour produire une alerte (supérieur à, inférieur ou égal à, inférieur à, etc.)..
    - Sélectionnez par rapport si le nombre correspondant au seuil s'applique à l'ensemble du rapport ou sélectionnez par ligne si le seuil s'applique à une seule ligne du rapport (le rapport étant la sortie de la requête sélectionnée, exécutez-le en examinant la période d'accumulation spécifiée).

      En l'absence de données durant l'intervalle d'accumulation indiqué :

      Si l'option par rapport est sélectionnée pour le rapport, la valeur de cet intervalle est 0 (zéro), et une alerte est générée si la condition de seuil est remplie (par exemple, si la condition spécifiée est "Alerter lorsque la valeur est < 1").

Si l'option par ligne est sélectionnée, aucune alerte n'est générée, quelle que soit la condition spécifiée (cela est dû au fait que la sortie ne contient pas de ligne).

- Sélectionnez En tant que limite absolue pour indiquer que le seuil saisi est un nombre absolu ou sélectionnez En tant que changement de pourcentage au sein d'une période pour indiquer que le seuil représente un pourcentage de modification au cours de la période identifiée dans les champs Date de début et Date de fin.

  Si l'option En tant que changement de pourcentage au sein d'une période est sélectionnée, utilisez les contrôles du sélecteur de date pour sélectionner les dates de début (champ Date de début) et de fin (champ Date de fin).

  Si l'option En tant que changement de pourcentage pour la même "période d'accumulation" sur un temps relatif est sélectionnée, une date relative sera saisie et l'alerte exécutera la requête pour la période en cours et pour la période relative (à l'aide du même intervalle) et vérifiera les valeurs en tant que pourcentage de la valeur de période de base.
  Remarque : Si une période relative est utilisée, chaque fois que l'alerte est vérifiée, la requête est exécutée deux fois, une fois pour la période en cours et une fois pour la période relative.

19. Indiquez dans le champ Fréquence des notifications le nombre de minutes correspondant à la fréquence à laquelle les récepteurs d'alerte doivent être prévenus que la condition d'alerte a été satisfaite.
20. Cliquez sur Sauvegarder pour sauvegarder la définition d'alerte.
    Remarque : Vous ne pouvez pas affecter des récepteurs ou des rôles, ni saisir des commentaires tant que la définition n'a pas été sauvegardée.
21. Sur le panneau Récepteurs d'alerte, indiquez éventuellement une ou plusieurs personnes ou un ou plusieurs groupes à prévenir lorsque cette condition d'alerte est satisfaite. Pour ajouter un récepteur, cliquez sur le bouton Ajouter un récepteur pour ouvrir le panneau Sélection de récepteur d'alerte.
    Remarque : Si le récepteur d'une alerte est l'administrateur, la valeur E-mail doit être définie pour celui-ci pour que l'alerte se déclenche.
    Remarque : Une autre valeur de récepteur pour les alertes de seuil est Propriétaire (le(s) propriétaire(s) de la base de données). Si la requête associée à l'alerte contient une adresse IP de serveur et un nom de service et si l'alerte est évaluée par ligne, la valeur de récepteur peut être Propriétaire. La notification d'alerte doit comporter les informations suivantes : Type de notification d'alerte : E-mail, ID utilisateur d'alerte : 0, Destination de l'alerte : Propriétaire. Pour connaître les autres récepteurs des alertes en temps réel, voir la section sur les actions d'alerte dans la rubrique Politiques.
22. Cliquez éventuellement sur Rôles afin d'affecter des rôles pour l'alerte.
23. Cliquez éventuellement sur Commentaires pour ajouter des commentaires à la définition.
24. Cliquez sur Appliquer, puis sur Terminé lorsque vous avez terminé.

Modification d'une alerte de corrélation

1. Cliquez sur Protection > Détection d'intrusion de base de données > Générateur d'alerte pour ouvrir le panneau Localiseur d'alerte.
2. Sélectionnez dans le panneau Localiseur d'alerte l'alerte de corrélation que vous souhaitez modifier.
3. Cliquez sur Modifier pour ouvrir le panneau Modifier une alerte.
4. En vous reportant à la rubrique Création d'une alerte de corrélation, modifiez la définition d'alerte.
5. Cliquez sur Sauvegarder.

Retrait d'une alerte de corrélation

1. Cliquez sur Protection > Détection d'intrusion de base de données > Générateur d'alerte pour ouvrir le panneau Localiseur d'alerte.
2. Sélectionnez dans le panneau Localiseur d'alerte l'alerte de corrélation que vous souhaitez retirer.
3. Cliquez sur le bouton Supprimer. Vous êtes invité à confirmer l'action.

Rubrique parent : Protection

Comment indiquer des événements via des alertes de corrélation

Déclenchez une alerte de corrélation si plus de quinze erreurs SQL émanant d'un utilisateur d'application ont été détectées au cours des trois dernières heures.

Pourquoi et quand exécuter cette tâche

Utilisez des alertes de corrélation pour signaler l'accumulation de certains événements dans la durée. Généralement, les applications ne génèrent pas d'erreurs SQL. Une augmentation du nombre d'erreurs SQL dans une application est un avertissement indiquant une possible tentative d'injection SQL. Pour plus d'informations, voir les rubriques d'aide en ligne intitulées Alertes de corrélation et Requêtes.

Prérequis

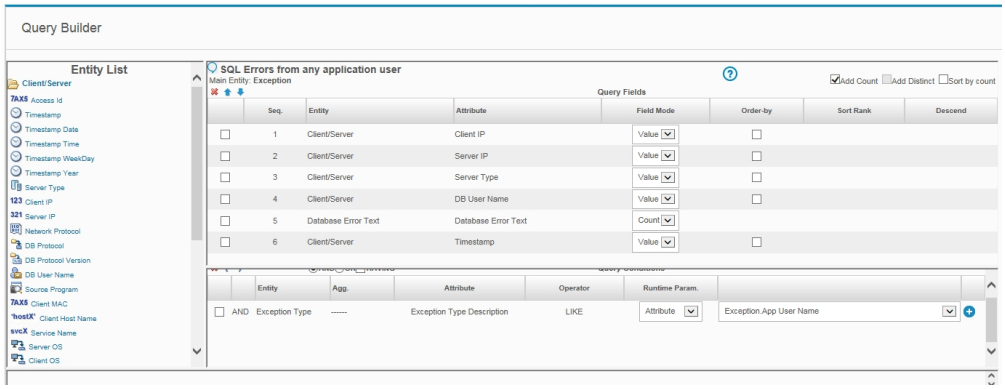
- Configurez le serveur de messagerie (SMTP) (Configuration > Outils et vues > Alerter).
- Après avoir entièrement configuré l'alerte de corrélation, assurez-vous qu'elle est active et fonctionnelle (Configuration > Outils et vues > Détection des anomalies).

Une alerte est un message indiquant qu'une exception (alerte de corrélation) ou une violation de règle de politique (alerte en temps réel) a été détectée.

Une alerte de corrélation est déclenchée par une requête qui effectue une recherche en arrière sur une période spécifiée afin de déterminer si un seuil d'alerte a été atteint.

Présentation des étapes d'alerte de corrélation

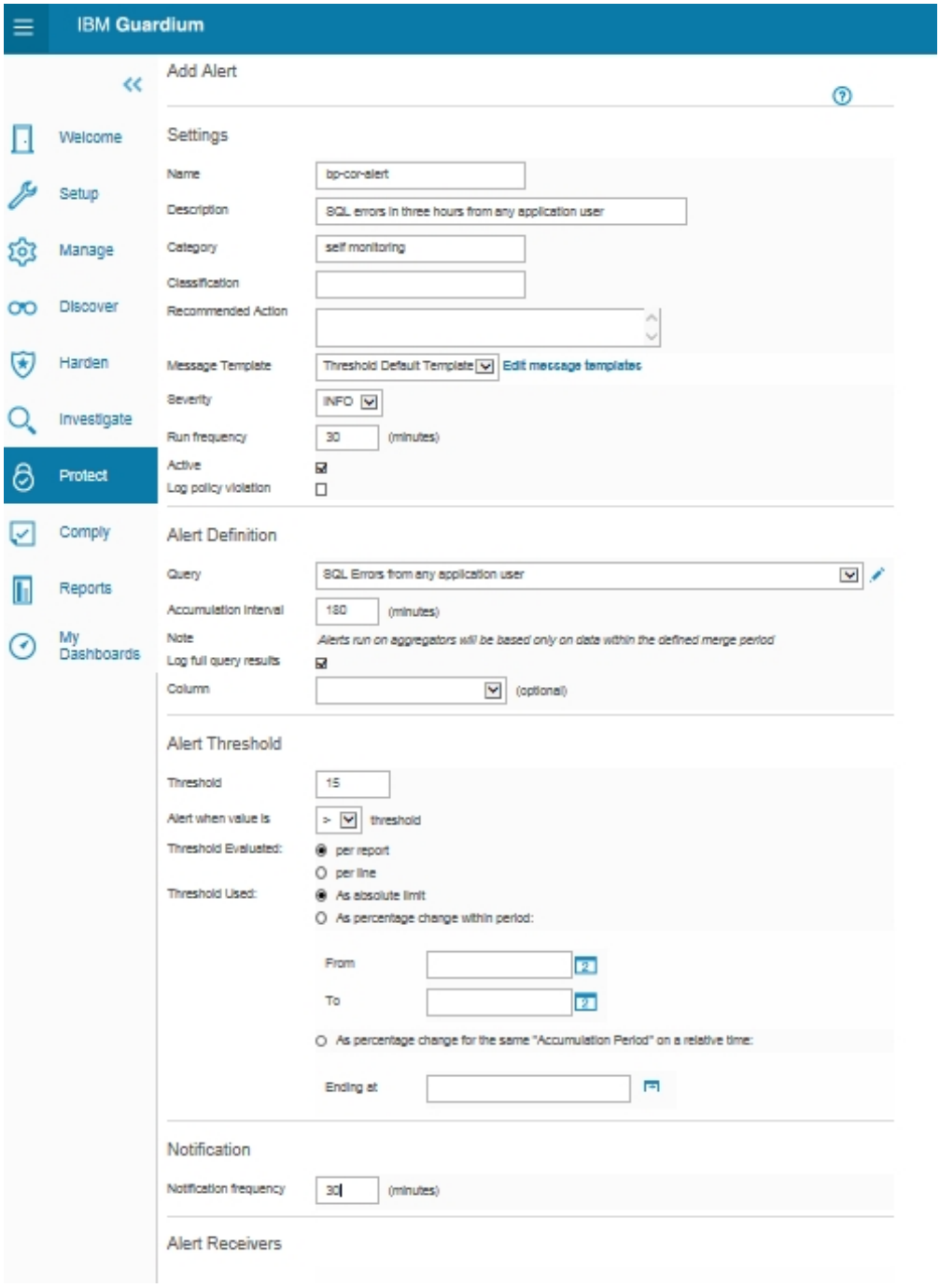
1. Créez une requête personnalisée à partir de l'application Suivi des exceptions avec un champ d'erreurs SQL (avec un comptage) et une condition d'utilisateurs d'application. Pour que cette requête personnalisée puisse être utilisée dans le générateur d'alerte, le champ de date (horodatage) doit être renseigné.
2. Cliquez sur Protection > Détection d'intrusion de base de données > Générateur d'alerte pour ouvrir le panneau Localiseur d'alerte.
3. Cliquez sur Nouveau. Renseignez les champs conformément aux instructions situées après l'écran de menu Générateur d'alerte.
4. Ajoutez un récepteur.



Domaine Exceptions, requête d'erreurs SQL

Procédure

1. Suivi des exceptions - Ouvrez le localiseur de requête
   - Utilisateurs : Sélectionnez Outils > Générateur de rapport, puis le domaine Exceptions uniquement.
2. Ouvrez le menu déroulant Requête. Sélectionnez Erreurs SQL. Un écran de configuration s'affiche avec Erreurs SQL comme titre principal.
3. Clonez cette sélection. Pour cela tapez un nom unique dans la zone de texte pour la requête. Vous ne devez pas ajouter d'apostrophe dans le nom de la requête.
4. Dans votre requête personnalisée, sous Champs de requête, dans la liste d'entités Client/Serveur, ajoutez un champ de date (horodatage) et affectez la valeur Nombre dans la colonne Mode champ pour Texte d'erreur renvoyé par la base de données. Sous Conditions de requête, dans la colonne Param. exécution, remplacez la valeur Exception par Attribut et choisissez Exception.App. User Name.
5. Cliquez sur Sauvegarder. Cette requête personnalisée pour les erreurs SQL de n'importe quel utilisateur d'application est désormais disponible et peut être utilisée dans le générateur d'alerte.



Menu d'écran Générateur d'alerte

6. Générateur d'alerte - Créez une alerte de corrélation
7. Cliquez sur Protection > Détection d'intrusion de base de données > Générateur d'alerte pour ouvrir le panneau Localiseur d'alerte.
8. Cliquez sur le bouton Nouveau dans le panneau Localiseur d'alerte pour afficher le panneau Ajouter une alerte.
9. Entrez un nom unique pour l'alerte dans le champ Nom. N'ajoutez pas d'apostrophes dans le nom de l'alerte.
10. Entrez une courte description pour l'alerte dans le champ Description.
11. Entrez une catégorie facultative dans le champ Catégorie. En l'occurrence, la catégorie Surveillance automatique a été utilisée.
12. Entrez une classification facultative dans le champ Classification.
13. Sélectionnez un niveau de gravité dans la liste Gravité. Lorsque la valeur ELEVE est définie pour une alerte e-mail, l'e-mail contient la mention Urgent.
14. Entrez le nombre de minutes entre les exécutions de la requête dans le champ Fréquence d'exécution.
15. Cochez la case Actif pour activer l'alerte.
16. Cochez la case Consigner une violation de politique pour consigner une violation de politique au déclenchement de cette alerte. Par défaut, les alertes de corrélation sont consignées uniquement dans le domaine Suivi des alertes. En cochant cette case, les alertes de corrélation et les alertes en temps réel (émises par la politique de sécurité relative à l'accès aux données) peuvent être visualisées en même temps, dans le domaine Violations de politique.
17. Dans la liste de requêtes sur le panneau Définition d'alerte, sélectionnez la requête à exécuter pour cette alerte. La liste de requêtes affichées inclura toutes les requêtes définies qui :
    - Contiennent au moins un champ de date (horodatage) (un champ d'horodatage est requis)
    - Contiennent un champ Nombre (un champ de comptage est requis)
    - Sont accessibles via votre compte utilisateur Guardium

Astuce relative au traitement des incidents : si une requête personnalisée a été créée dans n'importe quel générateur de requête dans l'application Générateur de rapport et qu'elle n'apparaît pas dans la liste de requêtes, assurez-vous qu'elle comporte une valeur d'horodatage (champ de date).

Astuce relative au traitement des incidents : après avoir sélectionné une requête dans la liste de requêtes sur le panneau Définition d'alerte de l'écran Ajouter une alerte, si cette requête doit être éditée (icône Editer) et qu'elle n'est pas modifiable, accédez à Générateur de requête (Outils > Générateur de rapport) pour l'éditer.

18. Si la requête sélectionnée contient des paramètres d'exécution, un panneau Paramètres de requête apparaîtra dans la sous-fenêtre Définition d'alerte. Indiquez des valeurs de paramètre selon vos besoins pour votre application.
19. Dans la case Intervalle d'accumulation, entrez la durée de l'intervalle (en minutes) pendant lequel la requête doit examiner le référentiel d'audit, en comptant à rebours à partir de l'heure en cours (par exemple, entrez 10 pour examiner les données correspondant aux 10 dernières minutes).
20. Cochez la case Consigner l'ensemble des résultats d'une requête pour que le rapport complet soit consigné avec l'alerte.
21. Si la requête sélectionnée contient une ou plusieurs colonnes de données numériques, sélectionnez-en une afin de l'utiliser pour le test. La valeur par défaut, qui sera le dernier élément de la liste, est la dernière colonne pour la requête, et correspond toujours au nombre d'occurrences agrégées dans cette ligne.
22. dans la sous-fenêtre Seuil d'alerte, définissez le seuil auquel une alerte de corrélation doit être générée, comme suit :
    - Dans le champ Seuil, entrez un nombre correspondant au seuil qui sera appliqué selon les modalités définies dans les autres champs du panneau.
    - Dans la liste Alerter lorsque la valeur est, sélectionnez un opérateur indiquant la façon dont la valeur de rapport doit être associée au seuil pour produire une alerte (supérieur à, inférieur ou égal à, inférieur à, etc.)..
    - Sélectionnez par rapport si la valeur de seuil s'applique au total d'un rapport.

    Si aucune donnée n'est générée durant l'intervalle d'accumulation spécifié : si la valeur définie pour le seuil est par rapport, la valeur de cet intervalle est 0 (zéro) et une alerte est générée si la condition de seuil est remplie (par exemple, si la condition spécifiée est " Alerter lorsque la valeur est < 1").

23. Indiquez dans le champ Fréquence des notifications le nombre de minutes correspondant à la fréquence à laquelle les récepteurs d'alerte doivent être prévenus que la condition d'alerte a été satisfaite.
24. Cliquez sur le bouton Appliquer pour sauvegarder la définition d'alerte.
    Remarque : Vous ne pouvez pas affecter des récepteurs ou des rôles, ni saisir des commentaires tant que la définition n'a pas été sauvegardée.
25. Sur le panneau Récepteurs d'alerte, indiquez éventuellement une ou plusieurs personnes ou un ou plusieurs groupes à prévenir lorsque cette condition d'alerte est satisfaite. Pour ajouter un récepteur, cliquez sur le bouton Ajouter un récepteur pour ouvrir le panneau Sélection de récepteur d'alerte. Pour plus d'informations sur l'ajout de récepteurs, voir la rubrique Notifications.
26. Cliquez éventuellement sur le bouton Rôles afin d'affecter des rôles pour l'alerte. Voir la rubrique Rôles de sécurité.
27. Cliquez éventuellement sur le bouton Commentaires pour ajouter des commentaires à la définition.
28. Cliquez sur le bouton Appliquer, puis sur le bouton Terminé lorsque vous avez terminé.

    Si plus de quinze erreurs SQL émanant d'un utilisateur d'application ont été détectées au cours des trois dernières heures, une alerte est envoyée au récepteur spécifié.

Rubrique parent : Protection

Gestion des incidents

L'application IIM (Integrated Incident Management) fournit une interface pour utilisateur métier avec des flux de travaux automatisés pour le suivi et la résolution des incidents liés à la sécurité de la base de données.

Elle simplifie la gestion des incidents en permettant aux administrateurs de regrouper une série de violations de politique connexes dans un seul incident et de les affecter de manière individuelle à des personnes spécifiques. Cela réduit le nombre de violations de politique distinctes que les équipes de surveillance doivent passer en revue.

Des processus de génération d'incident peuvent être définis et planifiés pour lire le journal de violations de politique et générer de nouveaux incidents. A partir d'un processus de génération d'incident, chaque incident sélectionné :

- se voit affecter un numéro d'incident unique ;
- est affecté à un utilisateur ;
- se voit affecter un code de gravité ;
- est affecté à une catégorie.

De plus, des violations de politique peuvent être affectées manuellement (par des utilisateurs autorisés) à de nouveaux incidents ou à des incidents existants à partir du rapport Violations de politique/Gestion des incidents.

Dès lors qu'un incident a été généré, les administrateurs et d'autres utilisateurs gèrent les incidents à partir de l'onglet Gestion des incidents figurant sur les portails administrateur et utilisateur. Toutes les autres tâches (affecter des incidents, envoyer des notifications, affecter un statut, etc.) peuvent être effectuées à partir de cet onglet.

Les fonctions de gestion des incidents sont accessibles à partir des menus déroulants des rapports de gestion des incidents. Seul un sous-ensemble de rapports ou de fonctions peut être disponible pour chaque utilisateur, en fonction des rôles de sécurité affectés au compte utilisateur correspondant.

Vous pouvez créer vos propres copies des rapports de gestion des incidents, mais elles ne bénéficieront pas de toutes les fonctions disponibles sur les rapports préconfigurés figurant dans l'onglet Gestion des incidents. Pour affecter des incidents, des codes de gravité, etc., utilisez les rapports figurant dans l'onglet Gestion des incidents.

Définition d'un processus de génération d'incident

Un processus de génération d'incident exécute une requête sur le journal des violations de politique et génère des incidents à partir de cette requête. Par défaut, la définition et la planification de processus de génération d'incident est limité aux utilisateurs dotés du rôle d'administrateur.

1. Cliquez sur Conformité > Outils et vues > Génération d'incident pour ouvrir le panneau Processus de génération d'incident.
2. Cliquez sur Ajouter processus pour ouvrir le panneau Editer un processus de génération d'incident.
3. Sélectionnez une requête dans la liste de requêtes. Plusieurs restrictions s'appliquent aux requêtes utilisées dans un processus de génération d'incident. Nous vous recommandons d'ouvrir une requête dans le générateur de requête pour vérifier qu'elle est conforme aux critères suivants :
    - La requête doit provenir du domaine Violations de politique.
    - La case Ajouter un nombre doit être cochée pour la requête. Pour plus d'informations, consultez Requêtes.
    - La principale entité pour la requête doit être l'entité Violation de règle de politique.
    - Les champs de la requête ne doivent pas comporter de chaîne SQL (issue de l'entité SQL ou de l'attribut Chaîne SQL complète de l'entité Violation de règle de politique).

4. Sélectionnez une gravité pour l'incident (le niveau de gravité par défaut est Info).
5. Entrez éventuellement une catégorie pour l'incident (la catégorie par défaut est aucun).
6. Entrez éventuellement un seuil pour la génération de l'incident. Le valeur de seuil par défaut est un, ce qui signifie que chaque ligne renvoyée par la requête générera un incident.
7. Dans la liste Affecter à un utilisateur, sélectionnez l'utilisateur auquel l'incident sera affecté.
8. Renseignez les champs Date de début et Date de fin pour la requête. Pour une requête planifiée, utilisez des dates relatives (par exemple, maintenant -1 jour et maintenant).
9. Cliquez sur Sauvegarder pour sauvegarder la définition de processus. Vous ne pouvez pas exécuter ou planifier le processus tant qu'il n'a pas été sauvegardé.
10. Pour exécuter la requête maintenant, cliquez sur Exécuter une fois maintenant.
11. Pour planifier l'exécution de la requête, cliquez sur Modifier la planification pour ouvrir l'utilitaire de planification ordinaire.

Affectation/réaffectation à un incident

1. Dans l'un des rapports de gestion des incidents, cliquez deux fois sur la violation de politique à affecter ou réaffecter.
2. Sélectionnez Affecter/réaffecter à l'incident dans le menu déroulant. Lorsque cette option est sélectionnée, ce menu est remplacé par un nouveau menu contenant une liste d'incidents ouverts (par exemple, Affecter à l'incident #123) et une option supplémentaire, Affecter à un nouvel incident.
3. Sélectionnez un incident auquel affecter cette violation ou sélectionnez Affecter à un nouvel incident pour affecter cette violation de politique au numéro d'incident suivant (les incidents sont numérotés l'un après l'autre).

   Un message s'affiche lorsque le changement a été effectué, et le panneau Gestion des incidents est actualisé. Si un nouvel incident a été créé, il est répertorié en premier dans le rapport contenant les incidents ouverts.

Affectation à un utilisateur

1. Dans l'un des rapports de gestion des incidents, cliquez deux fois sur l'incident à affecter à un autre utilisateur.
2. Sélectionnez Affecter à l'utilisateur dans le menu déroulant. Lorsque cette option est sélectionnée, ce menu est remplacé par un nouveau menu contenant une liste d'utilisateurs et une option supplémentaire, Désaffecter.
3. Sélectionnez un utilisateur ou sélectionnez Désaffecter pour retirer l'affectation actuelle à un utilisateur. Lorsqu'un utilisateur est affecté, la description de son statut indique Désaffecté et lorsque l'affectation d'un utilisateur est retirée, la description de son statut indique Ouvert.

   Un message s'affiche lorsque le changement a été effectué, et le panneau Gestion des incidents est actualisé.

Changement de la gravité

1. Dans l'un des rapports de gestion des incidents, cliquez deux fois sur l'incident dont la gravité doit être changée.
2. Sélectionnez Changer la gravité dans le menu déroulant. Lorsque cette option est sélectionnée, ce menu est remplacé par un nouveau menu contenant une liste de codes de gravité : Info, Faible, Moy et Elevé.
3. Sélectionnez le nouveau code de gravité.

   Un message s'affiche lorsque le changement a été effectué, et le panneau Gestion des incidents est actualisé.

Notification

1. Dans l'un des rapports de gestion des incidents, cliquez deux fois sur l'incident pour lequel un utilisateur doit recevoir une notification.
2. Sélectionnez Notifier dans le menu déroulant. Lorsque cette option est sélectionnée, ce menu est remplacé par un nouveau menu contenant une liste d'utilisateurs.
3. Sélectionnez un utilisateur.

   Un message s'affiche lorsque l'utilisateur a reçu une notification.

Changement de statut

1. Dans l'un des rapports de gestion des incidents, cliquez deux fois sur l'incident dont le statut doit être changé.
2. Sélectionnez Changer le statut dans le menu déroulant. Lorsque cette option est sélectionnée, ce menu est remplacé par un menu contenant une liste de codes de statut :
   - DESAFFECTE - Lorsqu'un incident prend ce statut, aucune violation de politique supplémentaire ne peut lui être ajoutée. Pour ajouter des violations de politique, affectez le statut Ouvert à l'incident, ajoutez les violations, puis refaites repasser le statut à Désaffecté.
   - FERME - Lorsqu'un incident a pour statut Fermé, il ne peut pas être modifié et il n'apparaît plus.
   - OUVERT - Statut initial d'un nouvel incident.
3. Sélectionnez le nouveau code de statut.

   Un message s'affiche lorsque le changement a été effectué, et le panneau Gestion des incidents est actualisé.

Ajout de commentaires

1. Dans l'un des rapports de gestion des incidents, cliquez deux fois sur l'incident auquel des commentaires doivent être ajoutés.
2. Sélectionnez Commentaires dans le menu déroulant pour ouvrir la fenêtre Commentaire utilisateur. Pour savoir comment ajouter des commentaires, consultez Commentaires.

Rubrique parent : Protection

Comment gérer la révision de plusieurs incidents de sécurité de base de données

Gestion des incidents : Apprenez à suivre et résoudre les incidents de sécurité de base de données.

Pourquoi et quand exécuter cette tâche

Les administrateurs peuvent regrouper une série de violations de politique connexes dans un seul incident et les affecter de manière individuelle à des personnes spécifiques. Cela réduit le nombre de violations de politique distinctes que les équipes de surveillance doivent passer en revue.

Prérequis

- Créez une politique (voir la rubrique Politiques).
- Démarrez des moteurs d'inspection (voir la rubrique Configuration de moteur d'inspection).

Une politique de sécurité contient un ensemble ordonné de règles à appliquer au trafic observé entre des clients et des serveurs de base de données.

Une violation de politique est consignée chaque fois qu'une règle est déclenchée. Des violations de politique peuvent être affectées à des incidents, automatiquement par un processus ou manuellement par des utilisateurs autorisés (voir la rubrique Gestion des incidents).

Récapitulatif des étapes

1. Cliquez sur Conformité > Outils et vues > Génération d'incident pour ouvrir le panneau Processus de génération d'incident.
2. Editez le processus de génération d'incident (Requête, Gravité, Seuil, Planification).
3. Accédez à l'onglet Gestion des incidents pour les rapports.

Gestion des incidents

L'application Gestion des incidents fournit une interface pour utilisateur métier avec des flux de travaux automatisés pour le suivi et la résolution des incidents liés à la sécurité de la base de données.

Des processus de génération d'incident peuvent être définis et planifiés pour lire le journal de violations de politique et générer de nouveaux incidents. A partir d'un processus de génération d'incident, chaque incident sélectionné :

- se voit affecter un numéro d'incident unique ;
- est affecté à un utilisateur ;
- se voit affecter un code de gravité ;
- est affecté à une catégorie.

De plus, des violations de politique peuvent être affectées manuellement (par des utilisateurs autorisés) à de nouveaux incidents ou à des incidents existants à partir du rapport Violations de politique/Gestion des incidents.

Dès lors qu'un incident a été généré, les administrateurs et d'autres utilisateurs gèrent les incidents à partir de l'onglet Gestion des incidents figurant sur les portails administrateur et utilisateur. Toutes les autres tâches (affecter des incidents, envoyer des notifications, affecter un statut, etc.) peuvent être effectuées à partir de cet onglet.

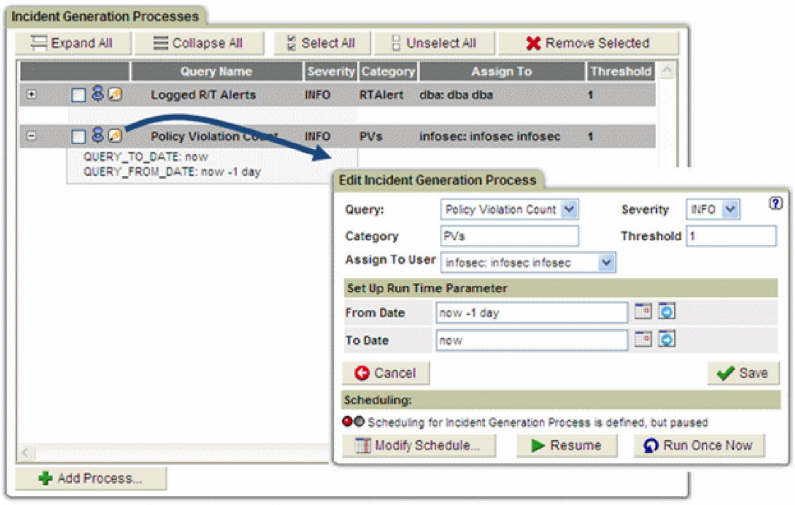
Les fonctions de gestion des incidents sont accessibles à partir des menus déroulants des rapports de gestion des incidents. Seul un sous-ensemble de rapports ou de fonctions peut être disponible pour chaque utilisateur, en fonction des rôles de sécurité affectés au compte utilisateur correspondant.

Définition d'un processus de génération d'incident

Un processus de génération d'incident exécute une requête sur le journal des violations de politique et génère des incidents à partir de cette requête. Par défaut, la définition et la planification de processus de génération d'incident est limité aux utilisateurs dotés du rôle d'administrateur.

Procédure

1. Cliquez sur Conformité > Outils et vues > Génération d'incident pour ouvrir le panneau Processus de génération d'incident.
2. Cliquez sur le bouton Ajouter processus pour ouvrir le panneau Editer un processus de génération d'incident.
3. Sélectionnez une requête dans la liste de requêtes. Plusieurs restrictions s'appliquent aux requêtes utilisées dans un processus de génération d'incident. Ouvrez la requête dans le générateur de requête pour vérifier qu'elle est conforme aux critères suivants :
   - La requête doit provenir du domaine Violations de politique.
   - La case Ajouter un nombre doit être cochée pour la requête. Pour plus d'informations, voir la rubrique Présentation du générateur de requête (Requêtes).
   - La principale entité pour la requête doit être l'entité Violation de règle de politique.
   - Les champs de la requête ne doivent pas comporter de chaîne SQL (issue de l'entité SQL ou de l'attribut Chaîne SQL complète de l'entité Violation de règle de politique).
4. Sélectionnez une gravité pour l'incident (le niveau de gravité par défaut est Info).
5. Entrez éventuellement une catégorie pour l'incident (la catégorie par défaut est aucun).
6. Entrez éventuellement un seuil pour la génération de l'incident. Le valeur de seuil par défaut est un, ce qui signifie que chaque "ligne" renvoyée par la requête générera un incident.
7. Dans la liste Affecter à un utilisateur, sélectionnez l'utilisateur auquel l'incident sera affecté.
8. Renseignez les champs Date de début et Date de fin pour la requête. Pour une requête planifiée, utilisez des dates relatives (par exemple, maintenant -1 jour et maintenant).
9. Cliquez sur Sauvegarder pour sauvegarder la définition de processus. Vous ne pouvez pas exécuter ou planifier le processus tant qu'il n'a pas été sauvegardé.
10. Pour exécuter la requête maintenant, cliquez sur Exécuter une fois maintenant.
11. Pour planifier l'exécution de la requête, cliquez sur Modifier la planification pour ouvrir l'utilitaire de planification. Pour savoir comment utiliser le planificateur, voir la rubrique Planification.

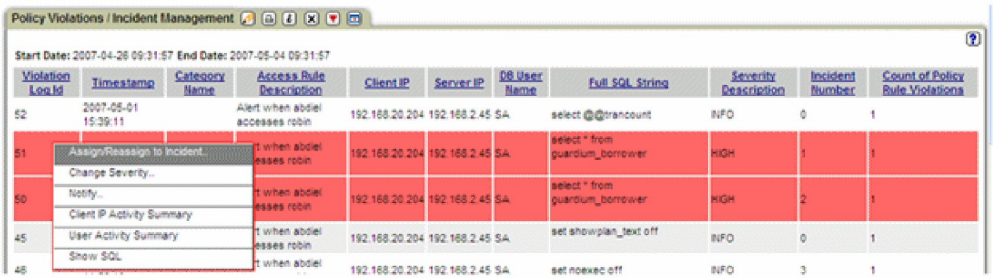


12. Affectez/réaffectez à un incident. Dans l'un des rapports de gestion des incidents, cliquez deux fois sur la violation de politique à affecter ou réaffecter.
13. Sélectionnez Affecter/réaffecter à l'incident dans le menu déroulant. Lorsque cette option est sélectionnée, ce menu est remplacé par un nouveau menu contenant une liste d'incidents ouverts (par exemple, Affecter à l'incident #123) et une option supplémentaire, Affecter à un nouvel incident.
14. Sélectionnez un incident auquel affecter cette violation ou sélectionnez Affecter à un nouvel incident pour affecter cette violation de politique au numéro d'incident suivant (les incidents sont numérotés l'un après l'autre).

    Un message s'affiche lorsque le changement a été effectué, et le panneau Gestion des incidents est actualisé. Si un nouvel incident a été créé, il est répertorié en premier dans le rapport contenant les incidents ouverts.

    Dans le rapport Violations de politique d'incident/Gestion des incidents, les utilisateurs peuvent effectuer les actions suivantes :

    - Affecter/Réaffecter à un incident (créer un incident à partir de cette violation de politique)
    - Changer la gravité de l'incident
    - Avertir un ou plusieurs utilisateurs qu'un incident s'est produit
    - Afficher des rapports récapitulant l'activité IP client, l'activité utilisateur ou les chaînes SQL à partir de l'incident.



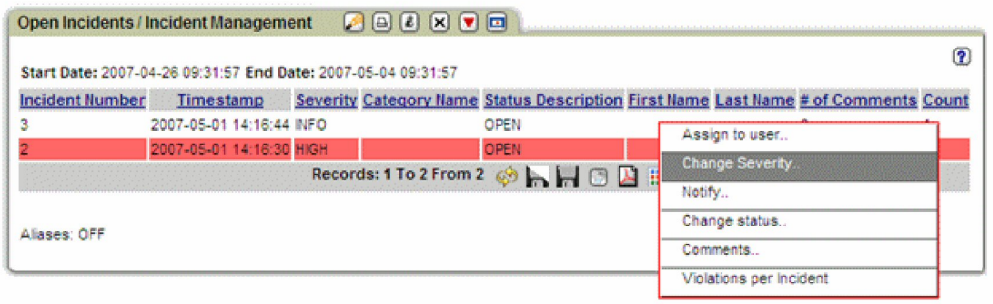
15. Affectez à un utilisateur. Dans l'un des rapports de gestion des incidents, cliquez deux fois sur l'incident à affecter à un autre utilisateur.
16. Sélectionnez Affecter à l'utilisateur dans le menu déroulant. Lorsque cette option est sélectionnée, ce menu est remplacé par un nouveau menu contenant une liste d'utilisateurs et une option supplémentaire, Désaffecter.
17. Sélectionnez un utilisateur ou sélectionnez Désaffecter pour retirer l'affectation actuelle à un utilisateur. Lorsqu'un utilisateur est affecté, la description de son statut indique Désaffecté et lorsque l'affectation d'un utilisateur est retirée, la description de son statut indique Ouvert.

    Un message s'affiche lorsque le changement a été effectué, et le panneau Gestion des incidents est actualisé.

18. Changez la gravité. Dans l'un des rapports de gestion des incidents, cliquez deux fois sur l'incident dont la gravité doit être changée.
19. Sélectionnez Changer la gravité dans le menu déroulant. Lorsque cette option est sélectionnée, ce menu est remplacé par un nouveau menu contenant une liste de codes de gravité : Info, Faible, Moy et Elevé.
20. Sélectionnez le code de gravité souhaité.

    Un message s'affiche lorsque le changement a été effectué, et le panneau Gestion des incidents est actualisé.

    Une fois qu'un violation de politique a été affectée à un incident, celui-ci s'affiche dans le rapport sur les incidents ouverts. Dans le rapport sur les incidents ouverts, les utilisateurs peuvent effectuer les actions affichées :



21. Créez une notification. Dans l'un des rapports de gestion des incidents, cliquez deux fois sur l'incident au sujet duquel un utilisateur doit recevoir une notification.
22. Sélectionnez Notifier dans le menu déroulant. Lorsque cette option est sélectionnée, ce menu est remplacé par un nouveau menu contenant une liste d'utilisateurs.
23. Sélectionnez un utilisateur.

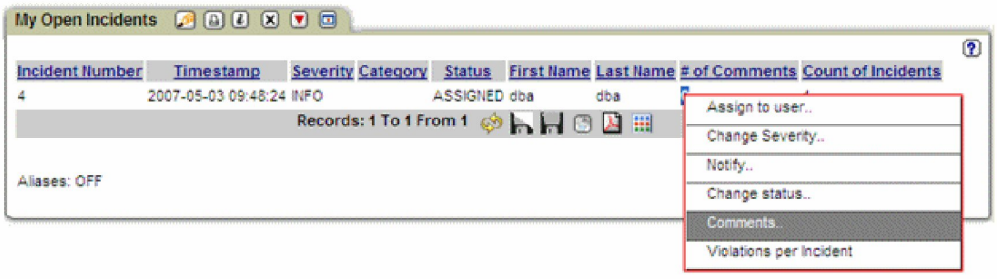
Lorsque l'utilisateur reçoit la notification, un message s'affiche.

24. Changez le statut. Dans l'un des rapports de gestion des incidents, cliquez deux fois sur l'incident dont le statut doit être changé.
25. Sélectionnez Changer le statut dans le menu déroulant. Lorsque cette option est sélectionnée, ce menu est remplacé par un menu contenant une liste de codes de statut :
    - DESAFFECTE - Lorsqu'un incident prend ce statut, aucune violation de politique supplémentaire ne peut lui être ajoutée. Pour ajouter des violations de politique, affectez le statut Ouvert à l'incident, ajoutez les violations, puis refaites repasser le statut à Désaffecté.
    - FERME - Lorsqu'un incident a pour statut Fermé, il ne peut pas être modifié et il n'apparaît plus.
    - OUVERT - Statut initial d'un nouvel incident.
26. Sélectionnez le code de statut souhaité.

    Un message s'affiche lorsque le changement a été effectué, et le panneau Gestion des incidents est actualisé.

27. Ajoutez des commentaires. Dans l'un des rapports de gestion des incidents, cliquez deux fois sur l'incident auquel des commentaires doivent être ajoutés.
28. Sélectionnez Commentaires dans le menu déroulant pour ouvrir la fenêtre Commentaire utilisateur. Pour savoir comment ajouter des commentaires, voir la rubrique sur la mise en commentaire.

    Chaque portail utilisateur affiche un rapport intitulé Incidents ouverts pour cet utilisateur. Dans le rapport Incidents ouverts, les utilisateurs peuvent effectuer les actions affichées :



Rubrique parent : Protection

Réécriture de requête

La fonctionnalité de réécriture de requête fournit un contrôle d'accès à granularité fine pour les bases de données en interceptant des requêtes de base de données et en les réécrivant en fonction des critères définis dans les politiques de sécurité.

La modification des requêtes se fait de manière transparente et impromptue, ainsi, lorsqu'un utilisateur émet des requêtes sans rencontrer de problèmes, il reçoit des résultats basés sur les instructions SQL réécrites.

La fonctionnalité de réécriture de requête est implémentée via une combinaison de définitions de réécriture de requête indiquant de quelle manière les requêtes doivent être changées ou augmentées et un contexte d'exécution indiquant les circonstances spécifiques dans lesquelles les définitions de réécriture de requête s'appliquent.

La réécriture des requêtes de base de données de manière impromptue permet aux administrateurs d'implémenter plusieurs types de contrôle d'accès, comme illustré dans les exemples ci-dessous.

Tableau 1. Exemples de contrôle d'accès à l'aide de la réécriture de requête.

Contrôle d'accès	**Instruction SQL d'origine**	**Instruction SQL réécrite**
Limitation de l'accès aux lignes en ajoutant une clause WHERE	`SELECT C from T`	`SELECT C from T WHERE [valeurs]`
Limitation de l'accès aux colonnes en modifiant la liste SELECT	`SELECT C1 from T`	`SELECT C2 from T`
	`SELECT C1,C2 from T`	`SELECT C2 from T`
Restriction des activités de base de données en réécrivant des instructions SQL pour ne rien faire	`SELECT EMAIL from T`	`SELECT++ EMAIL from T`
Restriction des actions que les utilisateurs peuvent effectuer en modifiant les verbes de requête (SELECT, INSERT, UPDATE, etc.)	`DROP TABLE T`	`UPDATE T SET [valeurs]`
Restriction des actions que les utilisateurs peuvent effectuer en modifiant les objets de requête (TABLE, VIEW, COLUMN, etc.)	`SELECT C from T1`	`SELECT C from T2`

La capacité à réécrire des requêtes de base de données de façon transparente procure une forme de contrôle d'accès extrêmement puissante et flexible permettant aux entreprises de traiter rapidement une grande variété de problématiques de sécurité. Par exemple, les définitions de réécriture de requête peuvent être développées pour réaliser les objectifs suivants :

- imposer la sécurité dans des scénarios d'architecture mutualisée où plusieurs utilisateurs et applications partagent une même base de données, mais où toutes les données ne doivent pas être accessibles à tous ces utilisateurs et applications
- exposer une base de données à un environnement de production à des fins de test sans exposer la totalité de la base de données
- corriger rapidement des vulnérabilités critiques en matière de sécurité tandis que des solutions permanentes sont développées au niveau base de données ou application

Consultez les sections suivantes pour en apprendre davantage sur le fonctionnement de la réécriture de requête et savoir comment configurer cette fonctionnalité afin de l'utiliser dans votre environnement Guardium.

Remarque : Si l'état firewall_default_state=1 est défini pour l'agent S-TAP, l'état par défaut pour la réécriture de requête, grw_default_state=1, ne peut pas être activé en même temps.

- Fonctionnement de la réécriture de requête
  Cette rubrique explique comment Guardium implémente la fonctionnalité de réécriture de requête.
- Utilisation d'une réécriture de requête
  Cette rubrique explique comment activer et utiliser la fonctionnalité de réécriture de requête.

Rubrique parent : Protection

Fonctionnement de la réécriture de requête

Cette rubrique explique comment Guardium implémente la fonctionnalité de réécriture de requête.

Présentation

Une fois la fonctionnalité de réécriture de requête activée sur l'agent S-TAP pour les serveurs de base de données pris en charge (voir Activation d'une réécriture de requête), elle est implémentée via les actions de règle de politique :

- REECRITURE DE REQUETE : ASSOCIER
- REECRITURE DE REQUETE : APPLIQUER LA DEFINITION
- REECRITURE DE REQUETE : DISSOCIER

Ces actions associées aux règles sont installées en tant que règles de politique d'accès. Les règles de politique d'accès contiennent des définitions de réécriture de requête indiquant de quelle façon les requêtes doivent être réécrites, ainsi qu'un contexte d'exécution indiquant à quel moment ces définitions doivent s'appliquer.

Une fois que des règles de réécriture de requête ont été spécifiées, les sessions sont traitées comme suit :

1. Une demande SQL déclenche une règle REECRITURE DE REQUETE : ASSOCIER, et toutes les activités suivantes dans la session sont observées par la réécriture de requête.
2. Tandis que les sessions sont observées par la réécriture de requête, le trafic est mis en attente au niveau de l'agent S-TAP et les informations de session sont vérifiées par rapport aux règles de politique d'accès.
3. Si une requête dans la session observée correspond à la règle REECRITURE DE REQUETE : APPLIQUER LA DEFINITION, la requête est réécrite en fonction de la définition et envoyée à l'agent S-TAP.
4. L'agent S-TAP libère la requête réécrite sur le serveur de base de données.
5. Lorsqu'une règle REECRITURE DE REQUETE : DISSOCIER est déclenchée, la réécriture de requête cesse d'observer les activités pour le reste de la session ou jusqu'à ce qu'une autre règle REECRITURE DE REQUETE : ASSOCIER soit déclenchée.

Exigences et limitations

La réécriture de requête a été conçue pour fonctionner avec les serveurs de base de données suivants :

- Oracle
- DB2 (Linux et Unix uniquement)
- Microsoft SQL

Pour plus d'informations sur les serveurs de base de données pris en charge et les restrictions qui leur sont éventuellement associées, voirPlatforms supported for IBM Guardium 10.1. Pour plus d'informations au sujet du support client de base de données pour la réécriture de requête, contactez le support IBM Guardium.

Important : Lorsque la réécriture de requête observe une session, le sniffer doit envoyer des verdicts de moteur à l'agent S-TAP pour chaque demande SQL présente dans la session. Ce processus est asynchrone et introduit un temps d'attente entre le sniffer et l'agent S-TAP. Créez des conditions de règle de réécriture de requête qui évitent d'établir des associations avec les sessions dans le cas d'applications sensibles aux performances ou sécurisées.
Rubrique parent : Réécriture de requête
Tâches associées:
Activation d'une réécriture de requête

Utilisation d'une réécriture de requête

Cette rubrique explique comment activer et utiliser la fonctionnalité de réécriture de requête.

Pourquoi et quand exécuter cette tâche

Suivez cette séquence de tâches pour activer et commencer à utiliser la fonctionnalité de réécriture de requête.

1. Activation d'une réécriture de requête
   Cette rubrique explique comment configurer un agent S-TAP pour la fonctionnalité de réécriture de requête.
2. Création de définitions de réécriture de requête
   Rubrique expliquant comment créer des définitions de réécriture de requête pour des scénarios de contrôle d'accès et de masquage de données.
3. Test de définitions de réécriture de requête
   Cette rubrique explique comment tester des définitions de réécriture de requête par rapport à un exemple de données entrées et vérifier qu'elles se comportent comme prévu.
4. Définition d'une politique de sécurité pour activer une réécriture de requête
   Cette rubrique explique comment créer des règles de politique d'accès à l'aide de vos définitions de réécriture de requête contenant des requêtes opérationnelles.
5. Création d'un rapport personnalisé pour valider des résultats de réécriture de requête
   Rubrique expliquant comment créer un rapport de suivi des réécritures de requête pour effectuer un audit des activités de réécriture de requête.

Rubrique parent : Réécriture de requête

Activation d'une réécriture de requête

Cette rubrique explique comment configurer un agent S-TAP pour la fonctionnalité de réécriture de requête.

Pourquoi et quand exécuter cette tâche

La fonctionnalité de réécriture de requête est activée uniquement lorsque les deux conditions suivantes sont réunies :

- La fonctionnalité de réécriture de requête est activée dans le fichier guard_tap.ini
- Des règles de politique de réécriture de requête existent et sont déclenchées par le trafic de session

Cette tâche vous guide tout au long des changements que vous devez apporter à votre fichier guard_tap.ini.

Procédure

1. Ouvrez guard_tap.ini dans un éditeur de texte.
2. Localisez le paramètre qrw_installed = 0 et remplacez-le par qrw_installed = 1. Le paramètre qrw_installed doit être défini avec une valeur 1 pour activer la fonctionnalité de réécriture de requête. Définissez le paramètre qrw_installed = 0 pour désactiver la fonctionnalité de réécriture de requête.
3. Sauvegardez vos changements dans guard_tap.ini.
4. Sur le système Guardium, connectez-vous en tant qu'utilisateur CLI et redémarrez le moteur d'inspection à l'aide de la commande CLI restart_inspection_engines.

Résultats

A la fin de cette tâche, la fonctionnalité de réécriture de requête sera activée et répondra aux règles de politique qui contiennent des actions de réécriture de requête.
Rubrique parent : Utilisation d'une réécriture de requête
Rubrique suivante : Création de définitions de réécriture de requête

Création de définitions de réécriture de requête

Rubrique expliquant comment créer des définitions de réécriture de requête pour des scénarios de contrôle d'accès et de masquage de données.

Procédure

1. Ouvrez Protection > Politiques de sécurité > Générateur de réécriture de requête.
2. Indiquez dans le champ Nom un nom unique et significatif pour la définition de réécriture de requête.
3. Créez une requête de modèle et soumettez-la à une analyse syntaxique.
   a. Indiquez une requête de modèle dans le champ Entrer une requête de modèle.

      Par exemple, pour créer une définition de réécriture visant à empêcher l'utilisation des instructions `SELECT * from`, entrez `SELECT * from EMPLOYEE` comme modèle.

   b. Cliquez sur le menu Type de base de données et sélectionnez un analyseur syntaxique SQL à utiliser avec la requête de modèle.
   c. Cliquez sur Faire une analyse syntaxique pour traiter la requête de modèle.

      Votre requête de modèle sera scindée en composants individuels et chaque composant sur lequel une action peut être effectuée sera souligné.

4. Indiquez la façon dont certains composants de la requête de modèle doivent être réécrits.
   a. Cliquez sur un composant souligné de la requête analysée que vous souhaitez réécrire. Une boîte de dialogue s'ouvre afin de vous aider à créer votre définition de réécriture de requête.

      Options :

      - Sélectionner et modifier un verbe, un champ ou un objet individuel dans la requête analysée
      - Ajouter un composant (souligné en gris en regard de la requête analysée) à la requête
      - Réécrire l'ensemble de la requête en cliquant sur la lettre [R] soulignée en gris figurant en regard de la requête analysée

      Dans l'exemple `SELECT * from EMPLOYEE` où vous souhaitez empêcher l'utilisation des instructions `SELECT * from`, cliquez sur * pour fournir un contenu de réécriture.

   a. Le champ Changer à partir de indique ce qui sera réécrit.
   b. Le champ En définit le composant réécrit.

      Par exemple, pour empêcher l'utilisation des instructions `SELECT * from`, remplacez le composant `*` par une liste d'objets spécifiques : `EMPNO, FIRSTNME, MIDINIT, LASTNAME, WORKDEPT, PHONENO, HIREDATE, JOB, EDLEVEL, SEX`.

      Important :

      Les définitions de réécriture sont basées sur la syntaxe, par conséquent, toutes les instructions au format `SELECT * from [OBJECT]` correspondront à l'exemple. Par exemple, les instructions `SELECT * from DEPARTMENT` et `SELECT * from EMPLOYEE` correspondent toutes les deux à notre exemple.

      Les définitions de réécriture de requête peuvent être limitées à certains objets à l'aide de règles de politique d'accès. Pour plus d'instructions, voir la rubrique Définition d'une politique de sécurité pour activer une réécriture de requête.

   c. Cliquez sur Sauvegarder pour sauvegarder la définition de réécriture, puis cliquez sur Retour pour fermer la boîte de dialogue.
5. Vérifiez la sortie de la définition de réécriture de requête à l'aide du champ Aperçu en temps réel et apportez d'éventuels changements.

   Pour reprendre notre exemple, l'instruction `SELECT * from EMPLOYEE` est réécrit sous la forme suivante : `SELECT EMPNO, FIRSTNME, MIDINIT, LASTNAME, WORKDEPT, PHONENO, HIREDATE, JOB, EDLEVEL, SEX from EMPLOYEE`.

6. Lorsque vous êtes satisfait de vos résultats, cliquez sur Sauvegarder pour sauvegarder votre définition de réécriture de requête.

   Votre définition de réécriture de requête est sauvegardée et apparaît dans la liste des définitions de réécriture de requête disponibles dans la sous-fenêtre Générateur de réécriture de requête.

Que faire ensuite

Continuez à gérer vos définitions de réécriture de requête :

- Créez des définitions supplémentaires en cliquant sur Nouveau et en répétant les étapes de cette tâche.
- Editez une définition de réécriture de requête existante en cliquant deux fois sur l'entrée correspondante dans la liste des définitions de réécriture de requête disponibles.
- Copiez et éditez une définition de réécriture de requête existante en sélectionnant l'entrée correspondante dans la liste des définitions de réécriture de requête disponibles et en cliquant sur Cloner.
- Supprimez une définition de réécriture de requête existante en sélectionnant l'entrée correspondante dans la liste des définitions de réécriture de requête disponibles et en cliquant sur Supprimer.

Lorsque vous avez terminé de gérer vos définitions de réécriture de requête, passez à l'étape suivante de cette séquence afin de tester et d'implémenter vos définitions.
Rubrique parent : Utilisation d'une réécriture de requête
Rubrique précédente : Activation d'une réécriture de requête
Rubrique suivante : Test de définitions de réécriture de requête
Tâches associées:
Définition d'une politique de sécurité pour activer une réécriture de requête

Test de définitions de réécriture de requête

Cette rubrique explique comment tester des définitions de réécriture de requête par rapport à un exemple de données entrées et vérifier qu'elles se comportent comme prévu.

Avant de commencer

Pour effectuer cette tâche, vous devez avoir créé une ou plusieurs définitions de réécriture de requête.

Procédure

1. Ouvrez Protection > Politiques de sécurité > Générateur de réécriture de requête.
2. Cliquez sur Configurer un test pour ouvrir une boîte de dialogue et sélectionnez des définitions de réécriture de requête à des fins de test.
    a. Faites glisser et déplacez des éléments du champ Définitions de réécriture de requête disponibles vers le champ Tester les définitions de réécriture de requête.
    b. Faites glisser et déplacez des éléments à l'aide du champ Tester les définitions de réécriture de requête disponibles afin de classer plusieurs définitions, comme vous le feriez dans une politique d'accès.
    c. Cliquez sur Sauvegarder pour fermer la boîte de dialogue lorsque vous avez terminé.
3. Tapez ou collez des requêtes de test dans le champ prévu à cet effet.

    Par exemple, pour tester une définition de réécriture visant à empêcher l'utilisation des instructions `SELECT * from` (voir la rubrique Création de définitions de réécriture de requête), entrez des exemples de requête, tels que les suivants :

    ```
    SELECT * from DEPARTMENT
    SELECT * from EMPLOYEE
    SELECT FIRSTNME, case
    when SALARY > 150000 then 'high'
    when SALARY > 100000 then 'medium'
    when SALARY > 80000 then 'fair'
    else 'poor'
    end from EMPLOYEE
    DELETE from EMPLOYEE where EMPNO=100
    INSERT into TEMP_EMP SELECT * from EMPLOYEE
    ```

4. Cliquez sur Exécuter le test pour traiter les exemples de requête et passez en revue les résultats.

    Par exemple, les exemples de requête fournis à l'étape précédente renvoient les résultats suivants :

Tableau 1. Résultats de test de réécriture de requête

Instruction SQL d'origine	Instruction SQL réécrite	Changé
`SELECT * from DEPARTMENT`	`SELECT EMPNO, FIRSTNME, MIDINIT, LASTNAME, WORKDEPT, PHONENO, HIREDATE, JOB, EDLEVEL, SEX from DEPARTMENT`	YES
`SELECT * from EMPLOYEE`	`SELECT EMPNO, FIRSTNME, MIDINIT, LASTNAME, WORKDEPT, PHONENO, HIREDATE, JOB, EDLEVEL, SEX from EMPLOYEE`	YES
`SELECT FIRSTNME, case when SALARY > 150000 then 'high' when SALARY > 100000 then 'medium' when SALARY > 80000 then 'fair' else 'poor' end from EMPLOYEE`	`SELECT FIRSTNME, case when SALARY > 150000 then 'high' when SALARY > 100000 then 'medium' when SALARY > 80000 then 'fair' else 'poor' end from EMPLOYEE`	NO
`DELETE from EMPLOYEE where EMPNO=100`	`DELETE from EMPLOYEE where EMPNO=100`	NO
`INSERT into TEMP_EMP SELECT * from EMPLOYEE`	`INSERT into TEMP_EMP SELECT * from EMPLOYEE`	NO

Important :

Les définitions de réécriture sont basées sur la syntaxe, par conséquent, toutes les instructions au format `SELECT * from [OBJECT]` correspondront à l'exemple. Par exemple, les instructions `SELECT * from DEPARTMENT` et `SELECT * from EMPLOYEE` correspondent toutes les deux à notre exemple.

Les définitions de réécriture de requête peuvent être limitées à certains objets à l'aide de règles de politique d'accès. Pour plus d'instructions, voir la rubrique Définition d'une politique de sécurité pour activer une réécriture de requête.

5. Continuez de saisir des exemples de requête afin de tester vos définitions de réécriture. Cliquez sur Configurer un test pour réorganiser les définitions de réécriture utilisées pour le test.

Que faire ensuite

Lorsque vous êtes satisfait de vos résultats de test, créez une politique de sécurité et commencez à utiliser vos définitions de réécriture de requête avec des requêtes opérationnelles.
Rubrique parent : Utilisation d'une réécriture de requête
Rubrique précédente : Création de définitions de réécriture de requête
Rubrique suivante : Définition d'une politique de sécurité pour activer une réécriture de requête
Tâches associées:
Définition d'une politique de sécurité pour activer une réécriture de requête
Création de définitions de réécriture de requête

Définition d'une politique de sécurité pour activer une réécriture de requête

Cette rubrique explique comment créer des règles de politique d'accès à l'aide de vos définitions de réécriture de requête contenant des requêtes opérationnelles.

Avant de commencer

Pour effectuer cette tâche, vous devez avoir créé et testé une ou plusieurs définitions de réécriture de requête et vous devez maîtriser la création des politiques de sécurité.

Procédure

1. Ouvrez Protection > Politiques de sécurité > Générateur de politique.
2. Créez une nouvelle politique ou modifiez une politique existante afin d'utiliser vos définitions de réécriture de requête.
   Conseil : Envisagez de créer une nouvelle politique afin de tester vos définitions de réécriture de requête. Ajoutez vos règles de réécriture à des politiques de sécurité existantes une fois que vous êtes satisfait du comportement de la politique de test.
3. Cliquez sur Editer les règles pour commencer à ajouter des règles de réécriture à la politique sélectionnée, puis sélectionnez Ajouter des règles > Ajouter une règle d'accès.
   Remarque : Les règles de réécriture de requête sont toujours classifiées en tant que règles d'accès.
4. Ajoutez une règle à laquelle une action REECRITURE DE REQUETE : ASSOCIER est associée. Prenez soin de cocher la case Passer à la règle suivante. Cette règle identifie les paramètres de session spécifiques qui doivent correspondre pour qu'une session de réécriture de requête se déclenche. Par exemple, un nom d'utilisateur de base de données ou une adresse IP client spécifique.
5. Ajoutez une règle à laquelle une ou plusieurs actions REECRITURE DE REQUETE : APPLIQUER LA DEFINITION sont associées et sélectionnez les définitions de réécriture de requête que vous souhaitez appliquer. Prenez soin de cocher la case Passer à la règle suivante. Cette règle identifie les objets ou commandes spécifiques qui doivent correspondre pour que les définitions de réécriture s'appliquent et que la requête source soit modifiée.

   Par exemple, si la valeur `EMPLOYEE` est affectée au champ Objet, une définition de réécriture `SELECT * from` est limitée aux objets `EMPLOYEE`.

6. Ajoutez une règle à laquelle une action REECRITURE DE REQUETE - DISSOCIER est associée. Cela entraîne la fermeture de la session de réécriture de requête et met fin à la surveillance du trafic de session.
7. Pour installer la nouvelle politique, retournez dans la sous-fenêtre Localiseur de politique, sélectionnez votre politique de sécurité, puis choisissez Sélectionner une action d'installation > Installer et écraser. Cliquez sur OK lorsque vous êtes invité à confirmer l'installation de la politique.
8. Connectez-vous à votre serveur de base de données et exécutez des requêtes de test afin de vérifier que vos règles de réécriture de politique d'accès fonctionnent comme prévu.
   a. Connectez-vous à votre serveur de base de données.
   b. Exécutez des requêtes qui doivent déclencher (ou non) les règles de politique d'accès installées et correspondre aux critères de vos définitions de réécriture de requête.

      Par exemple, exécutez `SELECT * from EMPLOYEE` pour vérifier qu'une définition de réécriture `SELECT * from` est appliquée à l'objet `EMPLOYEE`, puis exécutez `SELECT * from DEPARTMENT` pour vérifier que la même définition n'est pas appliquée à l'objet `DEPARTMENT`.

   c. Vérifiez que les résultats reflètent l'instruction SQL réécrite.

Rubrique parent : Utilisation d'une réécriture de requête
Rubrique précédente : Test de définitions de réécriture de requête
Rubrique suivante : Création d'un rapport personnalisé pour valider des résultats de réécriture de requête
Concepts associés:
Politiques

Création d'un rapport personnalisé pour valider des résultats de réécriture de requête

Rubrique expliquant comment créer un rapport de suivi des réécritures de requête pour effectuer un audit des activités de réécriture de requête.

Avant de commencer

Pour effectuer cette tâche, vous devez avoir créé et installé des règles de politique d'accès qui appliquent des définitions de réécriture de requête et vous devez maîtriser la création de rapports.

Pourquoi et quand exécuter cette tâche

Un rapport de suivi des réécritures de requête vous aide à valider les actions de réécriture de requête dans des environnements de test et de production.

Procédure

1. Ouvrez Rapports > Outils de configuration de rapport > Générateur de requête
2. Sélectionnez Réécriture de requête dans le menu Domaine.

3. Cliquez sur l'icône pour définir une nouvelle requête.
4. Indiquez un nom unique et significatif pour la requête dans le champ Nom de requête.

   Par exemple, `Mon rapport sur les réécritures de requête`

5. Sélectionnez l'une des options disponibles dans le menu Entité principale.

   Les options disponibles sont les suivantes :

   - Journal des réécritures de requête
   - Client-serveur
   - Session
   - Période d'accès

6. Cliquez sur Suivant pour ouvrir le générateur de rapport.
7. Développez les sections dans Liste d'entités et sélectionnez les éléments nécessaires à la génération de votre rapport.
   - Cliquez sur un élément et sélectionnez Ajouter un champ pour ajouter l'élément en tant que colonne dans le rapport.
   - Cliquez sur un élément et sélectionnez Ajouter une condition pour ajouter un filtre conditionnel au rapport.
   - Vous pouvez aussi glisser et déplacer des éléments depuis Liste d'entités vers les tables Champs de requête et Conditions de requête pour les appliquer à votre rapport.

   Ajoutez les éléments suivants comme point de départ d'un rapport sur des réécritures de requête :

   - Client-serveur : horodatage
   - Client-serveur : nom d'utilisateur de base de données
   - Client-serveur : type de serveur
   - Journal des réécritures de requête - noms de définition RQ appliqués
   - Journal des réécritures de requête - instruction SQL en entrée
   - Journal des réécritures de requête - instruction SQL en sortie

8. Cliquez sur Sauvegarder lorsque vous avez terminé de générer votre rapport.
9. Cliquez sur Créer un rapport pour créer le rapport.
10. Cliquez sur Ajouter à Mes rapports personnalisés pour ajouter le rapport à vos rapports personnalisés.
11. Ouvrez Rapports > Mes rapports personnalisés et sélectionnez le rapport que vous avez créé pour afficher un rapport sur les actions de réécriture de requête.

Rubrique parent : Utilisation d'une réécriture de requête
Rubrique précédente : Définition d'une politique de sécurité pour activer une réécriture de requête

Politiques et règles relatives à l'activité des fichiers

La surveillance de l'activité des fichiers garantit l'intégrité et la protection des données sensibles sur les serveurs de fichiers UNIX et Windows.

- Fonctionnalité des politiques et des règles relatives à l'activité des fichiers
  Une politique de surveillance de l'activité des fichiers indique de quelle façon Guardium gère différents événements relatifs à l'activité des fichiers. Chaque politique est constituée d'un ensemble de règles ordonnées. Chaque règle incluse dans une politique définit une action conditionnelle qui est exécutée lorsqu'une correspondance est trouvée pour la règle. Le test conditionnel peut être un test simple, par exemple, un utilisateur accède à un emplacement spécifique, ou un test complexe qui prend en compte plusieurs conditions. L'action peut aller de ne rien faire à bloquer l'événement. Plusieurs actions de regroupement et d'alerte peuvent être combinées et ordonnées afin de créer des réponses sophistiquées à des règles pour lesquelles une correspondance a été trouvée.
- Création d'une politique FAM et de ses règles à partir de zéro
  Configurez la surveillance de l'activité des fichiers en définissant et en gérant des politiques et des règles dans la fenêtre Générateur de politique pour les fichiers.
- Création d'une règle de politique FAM à partir de l'onglet Autorisations du tableau de bord d'investigation
  Vous pouvez utiliser les données surveillées, par exemple, des noms de source de données, des noms d'utilisateur, des actions et des chemins de fichier, dans la table de résultats du tableau de bord d'investigation afin de créer des règles de politique.

Rubrique parent : Protection
Information associée:
Surveillance de l'activité des fichiers avec Guardium (vidéo)

Fonctionnalité des politiques et des règles relatives à l'activité des fichiers

Une politique de surveillance de l'activité des fichiers indique de quelle façon Guardium gère différents événements relatifs à l'activité des fichiers. Chaque politique est constituée d'un ensemble de règles ordonnées. Chaque règle incluse dans une politique définit une action conditionnelle qui est exécutée lorsqu'une correspondance est trouvée pour la règle. Le test conditionnel peut être un test simple, par exemple, un utilisateur accède à un emplacement spécifique, ou un test complexe qui prend en compte plusieurs conditions. L'action peut aller de ne rien faire à bloquer l'événement. Plusieurs actions de regroupement et d'alerte peuvent être combinées et ordonnées afin de créer des réponses sophistiquées à des règles pour lesquelles une correspondance a été trouvée.

Par exemple, vous pouvez définir des politiques pour les cas suivants :

- Consigner une violation de politique si John écrit dans le dossier CONFIDENTIAL
- Empêcher un groupe d'utilisateurs de supprimer le fichier SALARIES.XLS
- Envoyer un e-mail à Krishna si JENNY lit les données de fichiers dont le nom commence par sample*
- Effectuer un audit de tous les accès à des fichiers qui ont été classifiés comme contenant des données sensibles liées à PCI

Groupes : Guardium utilise le concept de groupes pour la création de politique et de rapport.

Des groupes Guardium sont créés et gérés sur le collecteur Guardium ou le gestionnaire central. Ne confondez pas les groupes Guardium avec les groupes de systèmes de fichiers.

Nous vous recommandons d'envisager une stratégie de désignation pour vos groupes, y compris les groupes de sources de données (serveurs de fichiers), les groupes de fichiers (par exemple, par niveau de sensibilité ou par combinaison de niveau de sensibilité et d'application), les groupes d'utilisateurs (liste de tous les utilisateurs connus, des utilisateurs "autorisés", des utilisateurs dotés de privilèges spéciaux).

Guide de bonnes pratiques pour les règles

- Une règle trop étendue (une règle qui surveille un trop grand nombre de fichiers) peut surcharger le système et augmenter le temps de traitement et de réponse.
- Une règle FAM peut comporter plusieurs modèles. Pour protéger à la fois un répertoire et son contenu, définissez une règle avec deux modèles, /FAMtest/* et /FAMtest.
- Un groupe constitué de chemins d'accès aux fichiers : chaque chemin doit être unique quel que soit sa casse. Par exemple, les deux chemins suivants peuvent cohabiter dans un groupe : C:\ABC et C:\abcdef. En revanche, les deux chemins suivants ne peuvent pas coexister dans un groupe : C:\ABC et C:\abc. Le générateur de groupe n'est pas sensible à la casse. Il n'est pas obligatoire de saisir des membres tout en majuscules ou tout en minuscules. Toutefois, dans un environnement UNIX, qui est sensible à la casse, le chemin /IBM/Guardium est différent du chemin /ibm/guardium. Si l'utilisateur souhaite surveiller ces deux chemins, le générateur de groupe en cours est limité et ne peut pas les voir comme deux chemins distincts.
- L'ordre des règles dans la politique de sécurité est très important. Les règles sont envoyées à l'agent S-TAP en tant qu'ensemble et sont traitées dans un ordre strict. Toute activité d'utilisateur donnée est vérifiée par rapport à chaque règle contenue dans la politique dans un ordre spécifique. La première règle qui répond au critère de cet accès de fichier est appliquée et les règles suivantes sont ignorées. Dans la plupart des cas, placez la règle la plus spécifique en premier et la règle la plus générale en dernier. Prenons l'exemple des deux règles suivantes :
  - **Règle A :** *Effectuer l'audit uniquement* pour tous les accès à /data/*
  - **Règle B :** *Bloquer, Consigner la violation et effectuer l'audit* pour l'accès de l'utilisateur 'joe' à /data/salaries

  Si vous placez la règle A en premier et que Joe tente de lire /data/salaries, il n'est pas nécessaire de passer à la règle suivante, et Joe fait l'objet d'un audit. Si vous placez la règle B en premier, l'accès de Joe à /data/salaries est bloqué et il n'est pas nécessaire de passer à la règle suivante.

Comportement de la surveillance de l'activité des fichiers lors de l'utilisation d'un agent S-TAP doté d'une version antérieure à la version 10.1.2 (sans prise en charge d'actions multiples) avec un sniffer doté de la version 10.1.2 ou ultérieure (avec prise en charge d'actions multiples)

- Si vous utilisez un agent S-TAP doté d'une version antérieure à la version 10.1.2 avec une nouvelle interface utilisateur sniffer version 10.1.2 dotée d'une règle d'actions multiples, le blocage est correctement implémenté puisque cette action se trouve côté S-TAP.
- Côté sniffer, les actions cumulent toutes les actions spécifiées.
- Par exemple, si vous sélectionnez Effectuer l'audit uniquement pour la commande READ et Bloquer, Consigner les violations et effectuer l'audit pour la commande DELETE, celle-ci est bloquée, mais pas la commande READ. En revanche, la commande READ et la commande DELETE déclenchent l'audit, la consignation des violations et les alertes même si la règle Effectuer l'audit uniquement était sélectionnée pour la commande READ.
- Dans l'autre instance où l'utilisateur utilise un agent S-TAP 10.1.2 et une interface utilisateur sniffer dotée d'une version antérieure à la version 10.1.2, cela fonctionne bien car il est absolument impossible de définir une règle d'actions multiples (par conséquent, aucune interface utilisateur ou API GuardAPI à prendre en charge).

Attributs de règle

Nom de règle

Nom unique.

Source de données

La source de données peut être :

- une source de données sélectionnée dans une liste déroulante
- un groupe sélectionné dans une liste déroulante
- un groupe créé à partir de groupes sélectionnés dans la fenêtre Créer une règle
- un chemin saisi manuellement

Action de règle

L'action associée à une règle est l'action qui est exécutée lorsque les critères sont remplis. Les actions possibles sont les suivantes :

- Une action pour tout accès à un fichier qui répond aux critères de règle
- Une règle d'actions multiples composée de plusieurs actions, chacune étant associée à une catégorie de commande spécifiée ou à un groupe spécifié Notez que l'action **Passer à la règle suivante** n'est pas prise en charge avec des règles d'actions multiples.

Les actions de règle sont les suivantes :

- Alerter et effectuer l'audit : Envoi d'une alerte directement générée à partir du sniffer avec un comportement spécifique et consignation de l'événement
- Effectuer l'audit uniquement : Consignation de l'événement dans les tables GDM
- Bloquer, Consigner la violation et effectuer l'audit : Blocage de l'accès à l'objet, consignation d'une violation de politique et consignation de l'événement. Une action de blocage requiert également une configuration d'alerte.
- Ignorer : Aucune action n'est exécutée
- Consigner en tant que violation et effectuer l'audit : Consignation en tant que violation de politique et consignation de l'événement

Commandes d'accès : Etant donné qu'il existe des centaines de commandes de système de fichiers, elles sont regroupées dans les catégories suivantes :

- Lecture
- Ecriture
- Exécution
- Suppression
- Opération de fichier, y compris tout appel qui affecte les métadonnées de fichiers, telles qu'un changement d'appartenance de fichier, un changement de droits d'accès à un fichier, et des appels similaires.

Ces catégories sont définies dans le système et ne peuvent pas être changées. Vous pouvez toutefois créer un groupe Guardium contenant n'importe quelle combinaison de catégories, et utiliser ce groupe dans la politique de sécurité. Par exemple, vous pouvez créer un groupe Guardium contenant les catégories Ecriture et Exécution comme membres.

Si vous laissez la commande non spécifiée, toutes les commandes de système de fichiers sont comptabilisées comme une correspondance. Certains appels, tels que l'obtention de l'heure système, n'affectent pas du tout les fichiers et sont ignorés.

Critères de règle

Pour n'importe quel accès à un fichier donné, des critères de règle sont utilisés pour évaluer si une action en particulier doit être exécutée. Pour n'importe quelle source de données ou n'importe quel groupe de sources de données (serveurs de fichiers), les critères de règle que vous pouvez spécifier sont notamment les suivants :

Utilisateur : Utilisateur de système d'exploitation qui accède aux fichiers. Il peut également s'agir d'un groupe d'utilisateurs, conformément à ce qui est défini dans un groupe Guardium. Si ce champ n'est pas renseigné, la règle s'applique à tous les utilisateurs (à l'exception de l'utilisateur racine).

Chemin : Il peut s'agir d'un chemin Windows ou UNIX, d'un chemin individuel ou d'un groupe de chemins, conformément à ce qui est défini dans un groupe Guardium. Ce champ ne peut pas être vide (sauf lorsqu'un support amovible est sélectionné). Vous pouvez également choisir de surveiller les sous-répertoires dans le chemin.

Caractères génériques dans la spécification de nom :

- Le caractère '*' correspond à n'importe quel nombre de caractères
- Le caractère '?' correspond à un seul caractère
- Pour UNIX, utilisez une barre oblique inversée pour mettre en échappement * et ?

Conseil : Les caractères génériques nécessitent un traitement supplémentaire. Une utilisation excessive de caractères génériques nuit aux performances.

UNIX

Syntaxe :

Pour établir une correspondance avec tous les fichiers d'un disque, entrez /*

Pour établir une correspondance avec /tmp/My*File.txt, utilisez /tmp/My*File.txt

Pour établir une correspondance avec n'importe quel fichier portant une extension .txt dans /tmp, utilisez /tmp/*.txt

Exemple : le modèle de règle FAM est : /FAM*

Signification

- Répertoire : /
- Nom de fichier : FAM*

Des sous-répertoires sont sélectionnés pour la règle implémentée : (Subdirs: Yes)

Le fichier consulté est :

/guardium/modules/SUPERVISOR/10.0.0/FAM.output

Une correspondance est trouvée. Le nom de fichier, FAM.output, correspond au nom, FAM, et se trouve dans un sous-répertoire du répertoire donné '/'.

Windows : Pour Windows, vous devez spécifier l'unité, par exemple C:\

Syntaxe :

Pour surveiller tous les fichiers sur l'unité C, entrez C:\ et cochez la case Surveiller les sous-répertoires dans le chemin d'accès aux fichiers.

Pour établir une correspondance avec n'importe quel fichier portant l'extension .txt dans C:\tmp, utilisez C:\tmp*.txt

Exemples GuardAPI : Créez une politique avec deux règles

```
grdapi create_policy ruleSetDesc=policy1 isFam=true
grdapi create_fam_rule policyName=policy1 ruleName=rule1 serverHost="x.x.x.x" filePath="/famtest/*" command="DELETE"
actionName="Alert and Audit" notificationType="SYSLOG"
grdapi create_fam_rule policyName=policy1 ruleName=rule2 serverHost="x.x.x.x" filePath="/famtest/*" command="READ"
actionName="Alert and Audit" notificationType="MAIL"
```

policy1 -> rule1 -> "DELETE" -> "Alert and Audit" -> "SYSLOG"

policy1 -> rule2 -> "READ" -> "Alert and Audit" -> "MAIL"

Exemples GuardAPI : Créez une politique avec une règle d'actions multiples

Règle d'actions multiples pour FAM - composée de plusieurs actions, chacune étant associée à une catégorie de commande spécifiée ou à un groupe spécifié. Les commandes dans un contexte de surveillance de l'activité des fichiers sont les suivantes : Lecture, Ecriture, Suppression, Exécution et Opération de fichier. Si le système ne prend pas en charge les règles d'actions multiples, il ignore la règle et passe à la règle suivante.

```
grdapi create_policy ruleSetDesc=policy1 isFam=true
grdapi create_fam_rule policyName=policy1 ruleName=rule1 serverHost="x.x.x.x" filePath="/famtest/*"
add_action_to_fam_rule policyName=policy1 ruleName=rule1 command="DELETE, READ" actionName="Alert and Audit"
notificationType="SYSLOG"
add_action_to_fam_rule policyName=policy1 ruleName=rule1 command="WRITE" actionName="Alert and Audit" notificationType="MAIL"
```

policy1 -> rule1 -> "DELETE, READ" -> "Alert and Audit" -> "SYSLOG"

policy1 -> rule1 -> "WRITE" -> "Alert and Audit" -> "MAIL"

Ajout d'une autre action à l'aide de commandGroupId, en partant du principe que commandGroupId=20000 existe et qu'il comporte "DELETE, WRITE"

```
add_action_to_fam_rule policyName=policy1 ruleName=rule1 command="READ" commandGroupId=20000 actionName="Ignore"
notificationType=""
```

policy1 -> rule1 -> "READ, DELETE, WRITE" -> "Ignore"

Comportement de la surveillance de l'activité des fichiers avec un agent S-TAP doté d'une version antérieure à la version 10.1.2 et un sniffer doté de la version 10.1.2 ou ultérieure

La règle d'actions multiples pour la surveillance de l'activité des fichiers a été introduite dans la version 10.1.2. L'agent S-TAP doté d'une version antérieure à la version 10.1.2 ne prend pas en charge la règle d'actions multiples pour la surveillance de l'activité des fichiers, tandis que le sniffer doté de la version 10.1.2 ou ultérieure prend en charge cette règle d'actions multiples. Côté sniffer, les actions cumulent toutes les actions spécifiées.

Par exemple, si la politique indique Effectuer l'audit uniquement pour la commande READ et Bloquer, Consigner les violations et effectuer l'audit pour la commande DELETE, celle-ci est bloquée, mais pas la commande READ. En revanche, la commande READ et la commande DELETE déclenchent toutes les deux l'audit, la consignation des violations et les alertes même si la règle Effectuer l'audit uniquement était sélectionnée pour la commande READ.

Rubrique parent : Politiques et règles relatives à l'activité des fichiers

Création d'une politique FAM et de ses règles à partir de zéro

Configurez la surveillance de l'activité des fichiers en définissant et en gérant des politiques et des règles dans la fenêtre Générateur de politique pour les fichiers.

Pourquoi et quand exécuter cette tâche

Une fois que vous avez ouvert la fenêtre Générateur de politique pour les fichiers, ainsi que d'autres vues dans le générateur de politique, vous pouvez passer d'une vue à l'autre en cliquant sur Générateur de politique pour les fichiers, Nouvelle politique et Créer une règle au bas de la page.

Vous pouvez aussi créer des politiques et des règles en utilisant GuardAPI.

Procédure

1. Sur une machine autonome ou MU, accédez au générateur de politique FAM, puis à Protection > Politiques de décurité > Générateur de politique pour les fichiers.
2. Entrez un nom pour la nouvelle politique. (Vous pourrez la sauvegarder dès qu'une règle sera définie.)
3. Pour ajouter des règles existantes à la politique.
   a. Cliquez sur Afficher les modèles. Le tableau Modèles de règle apparaît.
   b. Vous pouvez éventuellement filtrer la liste à l'aide de la fonction de filtrage.
   c. Sélectionnez une ou plusieurs règles, puis cliquez sur la flèche vers la droite 
4. Pour créer une nouvelle règle.
   a. Cliquez sur l'icône  pour ouvrir la fenêtre Créer une règle.
   b. Indiquez un nom pour la règle, définissez ses attributs, puis cliquez sur Sauvegarder.
5. Pour modifier une règle existante et l'ajouter à la politique.
   a. Sélectionnez la règle, puis cliquez sur l'icône  .
   b. Cliquez sur  , changez le nom, modifiez les autres attributs si besoin, puis cliquez sur Sauvegarder.
6. Changez l'ordre des règles à l'aide des flèches 
7. Supprimez une règle en la sélectionnant et en cliquant sur l'icône  .
8. Cliquez sur Sauvegarder pour sauvegarder la politique ou sur Sauvegarder et installer pour installer la politique immédiatement. Voir Installation de politiques.

Rubrique parent : Politiques et règles relatives à l'activité des fichiers
Information associée:
Fonctions de surveillance de l'activité des fichiers dans GuardAPI

Création d'une règle de politique FAM à partir de l'onglet Autorisations du tableau de bord d'investigation

Vous pouvez utiliser les données surveillées, par exemple, des noms de source de données, des noms d'utilisateur, des actions et des chemins de fichier, dans la table de résultats du tableau de bord d'investigation afin de créer des règles de politique.

Avant de commencer

- Le bundle FAM doit être installé et configuré
- Le processus de reconnaissance et de classification doit être activé
- Le tableau de bord d'investigation doit être activé. Voir la rubrique Activation et désactivation du tableau de bord d'investigation.

Pourquoi et quand exécuter cette tâche

Procédure

1. Choisissez Fichier dans la liste déroulante de la bannière du produit et cliquez sur l'icône de recherche pour ouvrir le tableau de bord d'investigation pour les données de fichier.
2. Ouvrez l'onglet Autorisations de la table de résultats. Cliquez sur Détails pour voir les entrées individuelles.
3. Choisissez une ou plusieurs entrées dans les résultats que vous souhaitez utiliser pour remplir une règle. Vous pouvez utiliser la case à cocher Sélectionner tout pour inclure toutes les entrées actuellement affichées (et non toutes les entrées de la base de données).
4. Cliquez avec le bouton droit de la souris et choisissez Ajouter une règle de politique. La boîte de dialogue Générer une règle s'ouvre avec des valeurs issues des entrées que vous avez sélectionnées. Si vous avez sélectionné plusieurs entrées, un groupe contenant les valeurs issues de ces entrées est créé. Vous pouvez créer une règle à ajouter à une politique existante ou créer une nouvelle politique qui inclut votre nouvelle règle.
   Remarque : Une règle trop étendue (une règle qui surveille un trop grand nombre de fichiers) surchargera le système et augmentera le temps de traitement et de réponse.
   Remarque : Une règle FAM peut comporter plus d'un modèle. Pour protéger un répertoire et son contenu, définissez une règle avec deux modèles, /FAMtest/* et /FAMtest.
   Remarque : Lorsque vous utilisez une politique FAM, vous devez tenir compte du respect de la casse lorsque vous définissez un groupe pour spécifier les chemins surveillés. Sinon, le groupe ne peut pas être créé. La solution de contournement consiste à créer deux règles de politique FAM différentes. Clarification - Si les chaînes définies en tant que membres d'un groupe sont différentes sans avoir à tenir compte du respect de la casse, le groupe peut être créé. Par exemple : 1. C:\ABC 2. C:\abcdef. Si les chaînes définies en tant que membres d'un groupe sont identiques sans avoir à tenir compte du respect de la casse, le groupe NE peut PAS être créé. Par exemple : 1. C:\ABC 2. C:\abc Par conséquent, il n'est pas obligatoire de saisir des membres tout en majuscules ou tout en minuscules. Le générateur de groupe n'est pas sensible à la casse. Toutefois, dans un environnement UNIX, qui est sensible à la casse, le chemin /IBM/Guardium est différent du

chemin /ibm/guardium. Si l'utilisateur souhaite surveiller ces deux chemins, le générateur de groupe en cours est limité et ne peut pas les voir comme un seul et même chemin.
5. Choisissez des sources de données, des actions et des critères. Remplacez les valeurs que vous souhaitez changer. Cliquez sur Editer pour modifier chaque champ.
6. Pour créer une nouvelle politique et l'installer, cliquez sur Créer et installer. Pour créer la politique sans l'installer, cliquez sur OK.

Rubrique parent : Politiques et règles relatives à l'activité des fichiers

Surveillance et audit

Une fois que vous avez identifié vos données sensibles et pris les mesures appropriées pour les protéger, vous devez surveiller les activités y accédant. Dans la plupart des cas, vous pouvez utiliser les données générées par la surveillance pour vous conformer aux exigences en matière d'audit, qu'elles soient réglementaires ou internes.

- Construction de processus d'audit
  Rationalisez le processus d'automatisation du flux de travail de conformité en consolidant, en un seul point, les tâches de surveillance des activités de bases de données suivantes : découverte des actifs, évaluation des vulnérabilités et recommandation de mesures de durcissement, surveillance des activités des bases de données et production de rapports d'audit, distribution des rapports, acceptation (signature) par les parties prenantes et escalade.
- Audits et rapports
  Guardium organise les données qu'il collecte en un ensemble de domaines. Chaque domaine contient un type différent d'informations concernant un domaine de préoccupation : accès aux données, exceptions, violations de politique, etc.
- Corrélation des données externes
  Cette rubrique explique comment créer des tables personnalisées pour les informations d'entreprise qui sont requises en plus des données internes Guardium existantes.
- Jeux de confidentialité
  Un jeu de confidentialité est une collection d'éléments utilisables dans le cadre d'une surveillance spéciale.
- Alerte personnalisée
  Des messages d'alerte peuvent être distribués via e-mail, SNMP, syslog ou des classes Java™ écrites par l'utilisateur. La dernière option correspond aux alertes personnalisées.
- Processus Flat Log
  L'option Flat Log est un processus qui permet au dispositif Guardium de consigner des informations sans les analyser immédiatement en temps réel.
- Construction d'une expression dans une condition de requête
  Utilisez l'icône Ajouter une expression associées aux sélections Valeur, Paramètre et Attribut pour entrer des conditions de requête incluant des chaînes définies par l'utilisateur et des expressions mathématiques.
- Rapport sur les autorisations de base de données
  Le processus de révision des autorisations consiste à vérifier que les utilisateurs disposent des privilèges requis pour effectuer leurs tâches.
- Identification de l'utilisateur
  Guardium met à disposition plusieurs méthodes d'identification des utilisateurs d'application, lorsque l'utilisateur de base de données réel n'apparaît pas de façon évidente depuis le trafic de base de données.
- Audit des changements de valeurs
  La fonction Audit des changements de valeurs permet de suivre les changements apportés aux valeurs dans les tables de base de données.
- Création d'une base de données d'audit
  Créez une base de données d'audit et utilisez-la pour vos activités de surveillance des changements de valeurs.
- Surveillance de l'accès aux tables
  Cette fonction ajoute un champ “Last Assessed” dans les tables pertinentes, pour l'interaction avec les produits de gestion du cycle de vie des données Optim Designer.
- Configuration rapide de la surveillance de conformité
  Après avoir déployé vos agents de surveillance (S-TAP), utilisez l'outil Surveillance de conformité pour surveiller votre environnement et s'assurer qu'il respecte des normes de sécurité et des réglementations spécifiques.
- Utilisation de l'accélérateur PCI/DSS pour implémenter la conformité à la norme PCI
  Configurez l'accélérateur PCI/DSS d'IBM Security Guardium et créez une série de politiques et de rapports afin de satisfaire les exigences de la norme PCI/DSS.
- Générateur de flux de travaux
  Le générateur de flux de travaux est utilisé pour définir des flux de travaux personnalisés (étapes, transitions et actions) à utiliser dans le processus d'audit.
- Analytique de détection de menace
  Guardium inclut l'analytique de détection de menace spécialisée, qui permet d'examiner et d'analyser des données auditées afin de détecter des symptômes pouvant indiquer divers types d'attaque de base de données.
- Tableau de bord d'investigation
  Le tableau de bord d'investigation fournit des outils puissants permettant d'identifier et d'évaluer les problèmes pouvant exister dans votre environnement Guardium. Il utilise des données non filtrées locales ou système et fournit de nombreuses options de filtrage pour interroger les données dans un environnement Guardium entier, potentiellement depuis tout collecteur Guardium dans cet environnement.
- Détection des valeurs extrêmes
  Activez et démarrez la détection des valeurs extrêmes en deux étapes simples, en laissant Guardium faire le travail d'identification de tout comportement anormal d'un serveur ou d'un utilisateur, permettant ainsi de détecter au plus vite les attaques possibles.
- Tableau de bord de protection des données
  Le tableau de bord de protection des données Guardium fournit une vue récapitulative des données relatives au risque et à la conformité destinées aux responsables de la sécurité seniors.

Construction de processus d'audit

Rationalisez le processus d'automatisation du flux de travail de conformité en consolidant, en un seul point, les tâches de surveillance des activités de bases de données suivantes : découverte des actifs, évaluation des vulnérabilités et recommandation de mesures de durcissement, surveillance des activités des bases de données et production de rapports d'audit, distribution des rapports, acceptation (signature) par les parties prenantes et escalade.

Automatisez et intégrez les activités d'audit suivantes dans un flux de travail de conformité :

- Possibilité de regrouper plusieurs tâches d'audit (rapports, évaluation des vulnérabilités, etc.) dans un même processus.
- Programmer l'exécution régulière de ces processus.
- Exécuter ces tâches en arrière-plan.
- Inscrire les résultats des tâches dans un fichier au format CSV (valeurs séparées par des virgules) ou ArcSight CEF (Common Event Format) et/ou les transférer à d'autres systèmes en utilisant Syslog.
- Ajouter des commentaires et des notations.

- Attribuer le processus à son auteur pour consultation (il recevra une nouvelle entrée dans sa liste de tâches une fois le résultat prêt).
- Attribuer le processus à d'autres utilisateurs ou à un groupe d'utilisateurs ou à un rôle.
- Créer l'obligation pour ces utilisateurs de signer le résultat.
- Autoriser l'escalade du résultat (l'affecter à une personne étrangère à la trace d'audit d'origine).

Transformez les activités manuelles périodiques de gestion de la sécurité des bases de données en un processus continuel et automatisé, prenant en compte les besoins en matière de confidentialité et de gouvernance de l'entreprise, par exemple la conformité à des normes ou réglementations telles que PCI-DSS (Norme de sécurité de l'industrie des cartes de paiement), SOX (Loi Sarbanes-Oxley), Data Privacy et HIPAA (Loi Health Insurance Portability Accountability Act).

Exportez les résultats d'audit vers des référentiels externes en vue d'une analyse légale complémentaire. Cette exportation peut se faire par l'intermédiaire de Syslog, de fichiers CSV/CEF ou de flux externes.

Le rapport Journal du processus d'audit présente un journal détaillé des activités pour toutes les tâches, avec notamment les heures de début et de fin. Il est à la disposition des utilisateurs administrateurs, qui peuvent y accéder via l'onglet Surveillance de Guardium. Les tâches d'audit comportent des heures de début et de fin. Cependant, le début et la fin des évaluations de sécurité et des classifications (qui vont dans une file d'attente) sont identiques.

Les résultats de chaque processus de flux de travail, y compris la revue, les traces d'acceptation (signature) et les commentaires, peuvent être archivés pour être restaurés et consultés ultérieurement via le centre d'investigation.

Un processus d'automatisation du flux de travail de conformité répond aux questions suivantes :

- De quel type de rapport, d'évaluation, de trace d'audit ou de classification a-t-on besoin ?
- A qui ces informations doivent-elles être communiquées et comment les acceptations sont-elles prises en charge ?
- Quel est le calendrier de livraison ?

Le processus d'automatisation du flux de travail de conformité inclut par ailleurs :

- Une définition de processus
- Un plan de distribution, qui :
  - Définit les récepteurs, qui peuvent être des utilisateurs, des groupes d'utilisateurs ou des rôles. (Voir Récepteurs de processus.)
  - Définit la responsabilité de revue/signature pour chaque récepteur.
  - Définit la séquence de distribution en positionnant l'option Continu.
- Un ensemble de tâches (voir Types de tâche de processus)
- Un planning - Le processus d'audit peut être exécuté immédiatement ou périodiquement, selon un planning défini.

Types de tâche de processus

Un processus de flux de travaux peut contenir un nombre quelconque de tâches d'audit :

- Rapports, personnalisés ou prédéfinis. Guardium fournit des centaines de rapports prédéfinis, dont plus de 100 sont spécifiques aux différentes réglementations.
- Rapport d'évaluation de la sécurité : une application dédiée évalue la sécurité de l'infrastructure des bases de données pour relever les vulnérabilités et fournir un rapport de l'état de santé de la base de données et de son niveau de sécurité, avec des mesures temps réel et passées. Elle confronte l'environnement actuel à un ensemble de tests préconfigurés, basés sur les failles et vulnérabilités connues, groupés par bonnes pratiques de sécurité des bases de données (telles que STIG et CIG1) et complétés par des tests personnalisés. L'application génère un rapport de l'état de santé de la sécurité, avec des métriques pondérées (basées sur les bonnes pratiques) et recommande des plans d'action visant à renforcer la sécurité des bases de données.
- Trace d'audit des entités : un rapport détaillé de l'activité liée à une entité spécifique est produit (il peut porter, par exemple, sur une adresse IP de client ou sur un groupe d'adresses).
- Jeu de confidentialité : production d'un rapport détaillant les accès à un groupe de paires objet-champ (par exemple, un numéro de sécurité sociale et une date de naissance) au cours d'une période donnée.
- Processus de classification : les métadonnées et données des bases de données existantes sont balayées en quête d'informations sensibles telles que numéros de sécurité sociale et numéros de carte de crédit.
- Flux externe : les données peuvent être exportées vers une application spécialisée externe en vue de les soumettre à une analyse légale complémentaire. Remarque : Le composant Flux externe est une tâche d'audit optionnelle dont l'activation se fait au moyen d'une clé de produit. Si la fonctionnalité correspondante n'a pas été activée, la tâche Flux externe n'apparaîtra pas dans la liste de sélection de tâches d'audit et la liste Type de flux sera vide.

Processus de flux de travail, gestion centralisée et agrégation

Sur un gestionnaire central (CM), des rapports peuvent faire référence à des données de sources de données (unités gérées) distantes. Dans ces conditions, les processus d'audit qui utilisent ces rapports ne sont accessibles qu'à partir du gestionnaire central. Ils ne sont pas visibles depuis les unités gérées.

L'automatisation du flux de travail (processus d'audit) pour le serveur agrégateur inclut désormais la possibilité de créer une base de données ad hoc pour chaque tâche de l'agrégateur et de ne spécifier que les jours pertinents pour cette tâche.

Remarque : Les bases de données ad hoc du serveur agrégateur peuvent être conservées dans le système jusqu'à 14 jours (selon la valeur spécifiée dans la commande drop_ad_hoc_audit_db) afin d'être soumises, si besoin est, à une analyse post-exécution par les services d'assistance Guardium.

Lors de la définition d'un rapport dans le processus d'audit, le nombre de jours pris en compte (défini par les champs DE-A) ne doit pas dépasser une certaine limite (un mois, par défaut). En cas de franchissement de cette limite, une erreur se produira à l'exécution si vous tentez d'exécuter la tâche d'audit sur l'agrégateur.

Il est permis de créer une tâche d'audit avec une période DE-A plus longue que ne le permet théoriquement la valeur du paramètre max_audit_reporting (fixée dans l'interface de ligne de commande), car les processus d'audit définis sur l'agrégateur sont susceptibles d'être exécutés sur les collecteurs gérés (lorsque cet agrégateur a le rôle de gestionnaire central). Or les tâches d'audit exécutées sur une unité collecteur n'ont pas de limite de temps (max_audit_reporting).

Il est donc admis de sauvegarder une tâche configurée avec une période dépassant la limite autorisée, mais si cette tâche est ensuite exécutée sur l'agrégateur, vous obtiendrez une exception d'exécution (RuntimeException).

La limite de durée couverte par le rapport d'audit peut être configurée avec la commande show max_audit_reporting ou store max_audit_reporting. Aucun message d'avertissement n'est émis si un rapport est créé avec un intervalle de temps DE-A non valide. Seule une mise en garde est visible dans le panneau Paramètres de tâche de l'écran Processus d'audit (sélectionnez Outils/Générateur de processus d'audit, puis ouvrez Tâches d'audit pour afficher Paramètres de tâche). Cette mise en garde est la suivante :

```
Sur les agrégateurs, seuls les rapports portant sur une durée qui ne dépasse pas la limite de temps (fixée par max_audit_reporting
dans l'interface de ligne de commande) seront exécutés.
```

Remarque : Lors de l'exécution d'une installation de correctif, tous les processus d'audit sont arrêtés.

Arrêter un processus d'audit

L'arrêt d'un processus d'audit ne peut avoir lieu que si les tâches d'audit n'ont pas été exécutées ou sont en cours d'exécution. L'arrêt d'un processus d'audit signifie que les tâches qui n'ont pas encore démarré ne seront pas exécutées. Aucun résultat partiel n'est fourni. Le processus d'audit s'arrête et le seul résultat fourni est un message d'erreur Arrêté. En revanche, si des tâches sont terminées, l'arrêt du processus d'audit n'interrompt pas l'envoi de leurs résultats.

Pour arrêter un processus d'audit, utilisez GuardAPI (placez le curseur sur une ligne et double-cliquez pour approfondir) à partir du rapport Conformité > Outils et vues > Journal du processus d'audit.

Dans le cas d'un utilisateur, le fait d'arrêter un processus d'audit affiche uniquement la ligne qui appartient à cet utilisateur (uniquement les tâches, sans les détails). Un utilisateur administrateur peut voir tous les détails et arrêter les processus d'audit de n'importe quel utilisateur. Un utilisateur ne peut arrêter que ses propres processus d'audit.

Remarque :

Les requêtes utilisant une source distante ne peuvent pas être arrêtées. Les rapports en ligne utilisant une source distante ne peuvent pas être arrêtés.

L'arrêt des processus d'audit ne concerne pas les tâches d'audit Jeu de confidentialité ou Flux externe. Si ces tâches ont commencé, elles vont jusqu'à leur terme, même si le processus est arrêté.

Distribution des résultats

Les récepteurs désignés d'un processus d'audit sont informés par e-mail et/ou via leur liste de tâches de la mise à disposition des résultats. Tout récepteur peut être désigné comme signataire d'un processus, auquel cas les résultats peuvent, en option, être maintenus à ce point de la liste de distribution jusqu'à ce que ce récepteur les signe électroniquement ou les libère sans les signer ni les voir. Les récepteurs peuvent être des utilisateurs, des groupes d'utilisateurs ou des rôles.

Récapitulatif des processus d'audit

Dans l'écran Localiseur de processus d'audit figure un récapitulatif intitulé Statut de processus d'audit. Il contient des informations sur les processus d'audit planifiés, ainsi que les résultats, les récepteurs en attente et les erreurs. Il s'agit d'une consolidation des données de plusieurs rapports de processus d'audit.

Un bouton permet également de supprimer les résultats de n'importe quel processus d'audit. Examinez l'écran Localiseur de processus d'audit. Recherchez le bouton Résultats à côté du bouton Exécuter une fois maintenant (choix Afficher ou Supprimer).

S'il est possible de supprimer les résultats d'un processus d'audit, il faut aussi penser à tracer ou consigner qui les supprime. Le rôle audit-delete (suppression d'audit) permet d'identifier l'auteur de la suppression d'un résultat de processus d'audit (ou de consigner l'occurrence de cette suppression dans le journal). Les utilisateurs ayant le rôle audit-delete peuvent supprimer les rapports. Les utilisateurs administrateurs peuvent aussi supprimer les rapports. Le suivi est réalisé via le rapport Trace d'audit d'activité d'utilisateur.

Remarque : Les processus d'audit issus de sources distantes sont limités à 100.000 résultats. Pour repousser cette limite, utilisez la commande d'interface de ligne de commande store save_result_fetch_size (ou show save_result_fetch_size).

Récepteurs

Dans un processus d'automatisation du flux de travail, vous pouvez définir un nombre quelconque de récepteurs et contrôler dans quel ordre ils reçoivent les résultats. Avec la fonction d'escalade, les récepteurs peuvent aussi envoyer une notification à d'autres récepteurs. Il est également possible d'exécuter un processus d'audit sans récepteurs définis. Il peut s'agir, par exemple, d'un processus qui écrit dans Syslog et dont les résultats n'ont pas besoin d'être passés en revue (ou signés).

Qui peut être récepteur ?

Dans le panneau Définition de processus d'audit, la liste des récepteurs inclut tous les utilisateurs, groupes d'utilisateurs et rôles Guardium (les groupes et les rôles sont libellés comme tels). Lorsqu'un groupe ou un rôle est sélectionné, tous les utilisateurs membres de ce groupe ou titulaires de ce rôle deviennent récepteurs des résultats.

Si un groupe est sélectionné comme récepteur et que l'une des tâches du flux de travail utilise le paramètre d'exécution spécial ./LoggedUser dans une condition d'une requête, cette dernière sera exécutée séparément pour chaque utilisateur du groupe, et chaque utilisateur recevra uniquement les résultats qui lui sont propres.

Prenons par exemple le cas d'une société avec trois administrateurs de base de données (DBA), chacun d'eux étant en charge d'un ensemble différent de serveurs. En vous aidant de la fonction de téléchargement de données personnalisées, vous transférez les secteurs de responsabilités de chaque DBA (avec les IP des serveurs) au système Guardium et vous les corrélez avec le domaine d'activité de base de données, puis vous utilisez un rapport dans ce domaine personnalisé comme tâche d'audit. Si un groupe d'utilisateurs contenant les trois DBA est désigné comme récepteur, chaque DBA recevra un rapport traitant uniquement de l'ensemble de serveurs dont il a la charge.

Si un groupe est sélectionné comme récepteur et que chaque récepteur est tenu de donner son aval (signature), chaque membre du groupe devra signer les résultats séparément (comme expliqué plus haut, chaque membre du groupe peut avoir à examiner un jeu différent de résultats).

Un récepteur peut être une simple adresse e-mail, auquel cas les résultats seront envoyés à cette adresse e-mail. Le nom d'utilisateur entré à cette occasion servira à filtrer les données. Il doit s'agir du même utilisateur que celui qui est connecté ou d'un utilisateur qui en dépend dans la hiérarchie des données.

Si un rôle est sélectionné comme récepteur, un seul utilisateur titulaire de ce rôle aura besoin de signer les résultats. Les autres titulaires du rôle recevront simplement une notification les informant que les résultats ont été signés.

Remarque :

Lorsqu'un événement est créé dans le flux de travail, chaque état par lequel passe cet événement peut être associé à un rôle (ce qui signifie que, pour être visible par un titulaire de ce rôle, l'événement doit être dans cet état).Lorsqu'un événement est affecté à un processus d'audit, il est important que chaque rôle associé à un état de cet événement soit celui d'un récepteur dans le processus d'audit.Autrement, il existe un risque qu'une ligne de résultat d'audit passe à un moment ou un autre par un état tel que plus aucun récepteur ne soit en mesure de la voir ni de changer son état.

Si cela arrive, l'utilisateur administrateur (qui peut voir tous les événements, sans considération de leurs rôles) pourra quand même voir la ligne de résultat et changer son état.En revanche, il est possible qu'il ne puisse la voir si la sécurité au niveau données est active.Il faudra dans ce cas qu'il la désactive (à partir de Profil global) ou qu'il ait

le rôle dataset_exempt. Il est important de configurer le processus d'audit de sorte que tous les rôles amenés à intervenir sur un événement associé à ce processus soient récepteurs des résultats.

Notification par e-mail

En option, la mise à disposition de nouveaux résultats de processus peut être notifiée par e-mail aux récepteurs. Deux possibilités existent :

- Lier uniquement - L'e-mail de notification contient seulement un lien hypertexte aux résultats stockés sur le système Guardium. Pour que le lien fonctionne, l'e-mail doit être ouvert depuis un système qui a accès au système Guardium. Consultez la section suivante pour plus d'informations sur les liens dans les e-mails.
- Résultats complets - Un fichier PDF ou CSV contenant les résultats est joint à l'e-mail, sauf en cas d'escalade spécifiant un récepteur non inclus dans la liste de distribution d'origine, auquel cas aucun fichier PDF ou CSV n'est joint. Lorsque l'option Résultats complets est choisie, la prudence s'impose, car des données sensibles, personnelles ou confidentielles, peuvent figurer dans le fichier PDF ou CSV. Lors de l'exécution d'un processus d'audit, si la notification à un récepteur est configurée avec l'option Résultats complets au format CSV cochée, aucun fichier CSV n'est généré pour les tâches des types Evaluation, Classificateur et Flux externe. Ces tâches ne peuvent pas non plus générer de fichiers CSV/CEF/PDF pour l'exportation. Seules les tâches des types Rapport, Jeu de confidentialité et Trace d'audit d'entité donnent lieu à la génération d'un fichier CSV (et uniquement si la notification au récepteur est configurée avec l'option Résultats complets au format CSV cochée).
  Remarque : Lorsque l'utilisateur destinataire de la notification consulte des résultats d'audit, si le fichier PDF généré existe déjà, un bouton Recréer PDF est présent pour permettre à cet utilisateur de recréer le fichier PDF et de le télécharger.

Liens hypertexte vers les résultats des processus d'audit

Dans les e-mails de notification, il existe des cas où les liens aux résultats des processus sur le système Guardium ne fonctionnent pas. Par exemple :

- Si vous (en tant que destinataire de l'e-mail) accédez à l'e-mail depuis un endroit où vous n'avez pas accès au système Guardium, les liens seront inopérants. Par exemple, si vous êtes à l'extérieur, vous conservez l'accès à vos e-mails via Internet, mais vous n'êtes plus relié au réseau privé de votre société et n'avez donc plus accès au système.
- Si vous (en tant que destinataire de l'e-mail) accédez à l'e-mail une fois passée la période de conservation des résultats, ces derniers ne seront plus disponibles et le lien sera inopérant. Par exemple, si les résultats sont conservés pendant sept jours et que vous avez été en congés pendant deux semaines, l'e-mail que vous ouvrirez à votre retour contiendra un lien à des résultats qui n'existent plus ; ce lien sera donc inopérant.

Listes de récepteurs gelées

Une fois qu'un processus a été exécuté, la liste des récepteurs existants est gelée, ce qui signifie que :

- Vous ne pouvez pas supprimer des récepteurs de la liste.
- Vous ne pouvez pas déplacer des récepteurs existants vers le haut ou vers le bas dans la liste.
- Vous pouvez à tout moment ajouter de nouveaux récepteurs à la fin de la liste et les repositionner à ce moment-là.
- Si le compte d'utilisateur Guardium d'un récepteur figurant sur la liste est supprimé, ce récepteur est remplacé par le compte de l'utilisateur administrateur (qui n'est jamais supprimé). C'est donc l'utilisateur administrateur qui reçoit les e-mails de notification de ce récepteur à présent supprimé et qui doit prendre toutes mesures nécessaires concernant les résultats qui lui étaient destinés.
- Si vous avez besoin de créer un ensemble complètement différent de récepteurs pour un processus existant, désactivez le processus original, faites-en un clone, puis apportez les modifications voulues à la liste des récepteurs dans la version clonée avant de la sauvegarder.

Comment les résultats sont communiqués aux récepteurs

Les résultats sont communiqués aux utilisateurs Guardium figurant sur la liste des récepteurs avec la chronologie suivante, qui varie selon que la case Continu est cochée ou non :

- Si la case Continu est cochée, la distribution se poursuit sans interruption et enchaîne avec le récepteur suivant de la liste.
- Si la case Continu n'est pas cochée, la distribution au récepteur suivant est différée jusqu'à ce que le récepteur en cours effectue l'action requise (revue ou signature).

Par exemple, supposons que vous vouliez définir l'enchaînement suivant :

- Administrateurs de base de données (DBA) - Tous les DBA doivent recevoir en même temps les résultats qui leur reviennent. Chacun reçoit un jeu de résultats différent, qui concerne uniquement les IP des serveurs dont il a la charge.
- Le Responsable DBA ne doit voir les résultats que lorsque tous les DBA les ont signés.
- A leur tour, les auditeurs ne doivent voir les résultats que lorsque le Responsable DBA a publié son rapport.
- Tous les auditeurs doivent recevoir les rapports en même temps, mais un seul d'entre eux (n'importe lequel) a besoin de signer chaque résultat.Les autres seront tenus informés de la signature des résultats.
- Un auditeur peut faire remonter (escalader) un résultat au Responsable de l'audit.

Pour définir ce flux :

- Le groupe des administrateurs de base de données (DBA) sera désigné comme premier récepteur
- Le Responsable DBA sera le suivant sur la liste.
- Le rôle (et non le groupe) Auditeurs sera le suivant sur la liste. N'importe lequel de ces auditeurs pourra signer, les autres recevront alors notification de la signature. En outre, un auditeur quelconque pourra faire remonter (escalader) un ensemble de résultats au Responsable de l'audit.
  Remarque : Les résultats ne seront distribués au récepteur suivant que lorsque le récepteur du moment aura cliqué sur le bouton Continuer. Ce procédé est entièrement séparé de la fonctionnalité de revue/signature et n'en dépend aucunement.
  Remarque : Les résultats de processus exportés sous forme de fichiers CSV ou CEF sont envoyés à un autre emplacement du réseau par le mécanisme Guardium d'archivage et d'exportation. Ces résultats ne sont pas soumis à la liste des récepteurs ni à une quelconque action de signature. Ils sont soumis au planning d'exportation de CSV/CEF Guardium (s'il en est défini un) et sont accessibles conformément aux autorisations d'accès qui ont été accordées sur le répertoire dans lequel ils sont stockés à terme.

Exportation des résultats de tâches d'audit sous forme de fichiers CSV, CEF ou PDF

Les rapports contenant des informations utilisables par d'autres applications, tout comme les rapports qui contiennent de grosses quantités de données, peuvent être exportés dans d'autres formats de fichier. Les données produites par les tâches Rapport, Trace d'audit d'entité et Jeu de confidentialité peuvent être exportées au format CSV (valeurs séparées par des virgules). Les données destinées à la production de rapports d'activité des bases de données peuvent quant à elles être exportées au format de fichier CEF (ArcSight Common Event Format).

Les sorties fichier CEF et CSV peuvent aussi être écrites sur syslog. Si la capacité syslog distant est utilisée, les sorties fichier CEF/CSV sont immédiatement transférées aux emplacements syslog distants. La fonction syslog distant offre la possibilité d'orienter les messages de chaque combinaison d'équipement et de gravité vers un système distant spécifique. Pour plus d'informations, consultez la description de la commande CLI remotelog (syslog).

Chaque enregistrement dans le fichier CSV ou CEF représente une ligne du rapport.

Le fichier exporté est créé en complément de la sortie standard de la tâche, il ne la remplace pas. Ce type de fichier est utile lorsque vous devez :

- Configurer l'intégration avec un système SIEM (Security Incident and Event Manager) existant dans votre infrastructure (Qradar, ArcSight, Network Intelligence, LogLogic, TSIEM, etc.).
- Passer en revue et analyser de très gros ensembles de résultats de tâches de conformité. (Les ensembles de résultats destinés aux présentations web sont limités à 5000 lignes, tandis que les lignes de résultats écrites dans un fichier exporté au format CSV ou CEF ne sont soumises à aucune limite).

Les fichiers CSV et CEF exportés sont stockés sur le système Guardium avec un nom de la forme suivante :

```
processus_tâche_AAAA_MMM_JJ-HHMMSS.<csv | cef>
```

Où processus est un libellé que vous choisissez lors de la définition du processus d'audit, tâche est un libellé de second niveau que vous pouvez définir pour chaque tâche membre du processus, et AAAA_MMM_JJ-HHMMSS est un horodatage marquant le moment où la tâche est exécutée.

Les fichiers CSV ou CEF exportés ne sont pas accessibles directement sur le système Guardium. Il revient à votre administrateur Guardium de les transférer du système Guardium vers un autre endroit du réseau au moyen de la fonction d'exportation adéquate. Pour accéder à ces fichiers, demandez à votre administrateur Guardium de vous indiquer l'endroit où ils ont été copiés.

Le fait que les fichiers exportés soient envoyés à l'extérieur du système Guardium a deux conséquences importantes :

- La publication de ces fichiers est sans rapport avec le plan de distribution des résultats défini pour le processus d'audit. Leur exportation se fait selon un calendrier défini par l'administrateur Guardium.
- Après l'exécution de la fonction d'exportation de fichier CSV/CEF, tous les fichiers exportés sont à la disposition de toute personne (utilisateur Guardium ou non) ayant accès au répertoire de destination défini pour cette fonction. Pour cette raison, il est possible que votre administrateur Guardium programme l'exécution de travaux additionnels (hors système Guardium) afin de copier les jeux de fichiers exportés du répertoire de destination de l'exportation CSV/CEF Guardium vers d'autres répertoires dont l'accès est contrôlé par des autorisations adéquates.

L'activité d'exportation de CSV/CEF est disponible dans le rapport d'activité Agrégation/Archivage.

Remarque : Si la sécurité au niveau des données a été activée, la sortie du processus d'audit (fichiers inclus) sera filtrée de sorte que les utilisateurs ne voient que les informations concernant la base de données dont ils ont la charge. Les fichiers envoyés par e-mail (sous forme de pièces jointes) à un récepteur seront filtrés. En revanche, les fichiers téléchargés localement sur la machine puis transférés ailleurs au moyen de la fonction Exportation des résultats ne seront pas soumis au filtrage de sécurité au niveau des données. Pour davantage d'informations sur l'exportation CSV/CEF, consultez la section "Exportation d'un fichier CSV ou CEF", plus loin dans cette rubrique.

Le tableau suivant fait la synthèse des différents cas de figure correspondant aux différents formats (CSV/CEF/PDF) d'exportation d'un fichier de processus d'audit.

Tableau 1. Exportation des résultats de tâches d'audit sous forme de fichiers CSV, CEF ou PDF

Fonction	Niveau	CSV	CEF	PDF
Joindre à un e-mail	Récepteur	Option Résultats complets --> Case à cocher PDF	N/A	Option Résultats complets --> Case à cocher PDF Les options (boutons radio) sont seulement pour le récepteur PDF.
Exporter un fichier	Tâche	Case à cocher Exporter un fichier CSV	Case à cocher Exporter un fichier CSV	Case à cocher Exporter un fichier CSV
Rapport vide et Approuver si vide = oui	Récepteur	Exportation non affectée (les fichiers vides seront exportés) Pièce jointe, pas de pièce jointe à l'e-mail	Exportation non affectée (les fichiers vides seront exportés) Pièce jointe, pas de pièce jointe à l'e-mail	Exportation non affectée (les fichiers vides seront exportés) Pièce jointe, pas de pièce jointe à l'e-mail
Zipper la pièce jointe	Processus d'audit	Si aucun fichier n'est généré, rien à zipper Fusion de tous les CSV dans un même fichier ZIP	N/A	Si aucun fichier n'est généré, rien à zipper Le PDF n'est pas zippé
Compresser (export)	Tâche	Compressé, fichier séparé pour chaque fichier CSV	Compressé, fichier séparé pour chaque fichier CSV	Le PDF n'est pas compressé

Fonctionnement des options Zipper pour envoi par e-mail et Compresser

L'option Zipper pour envoi par e-mail est le plus haut niveau de contrôle pour l'exportation des résultats d'une tâche d'audit. Elle produit un ensemble de fichiers CSV ou CEF. Les fichiers PDF ne sont jamais zippés ni compressés.

L'option Compresser opère sur des fichiers individuels.

Remarque : Pour les fichiers CSV joints à l'e-mail, lorsque la case Zipper pour envoi par e-mail n'est pas cochée, l'option Compresser peut toujours être appliquée. Le choix de l'option Compresser peut aussi être fixé individuellement pour chaque tâche. Il est donc possible qu'une tâche d'audit particulière envoie un fichier .csv (non zippé, non compressé) et qu'une autre envoie un fichier .csv.gz, le tout dans un même e-mail.

Les options Zipper pour envoi par e-mail et Compresser interagissent comme suit :

- Dès lors que l'option Zipper pour envoi par e-mail est cochée (peu importe que Compresser soit cochée ou non), la pièce jointe est constituée d'un unique fichier zip de fichiers CSV.
- Si Zipper pour envoi par e-mail n'est pas cochée et que Compresser est cochée, la pièce jointe est un ensemble de fichiers csv.gz.
- Si Zipper pour envoi par e-mail n'est pas cochée et que Compresser n'est pas cochée non plus, la pièce jointe est un ensemble de fichiers csv.
- Avec l'option Compresser cochée, Télécharger tous les enregistrements sera csv.gz.

- Avec l'option Compresser non cochée, Télécharger tous les enregistrements sera csv.
- Avec l'option Compresser cochée ou non cochée, Télécharger les enregistrements affichés sera toujours csv.
- Avec l'option Compresser cochée, l'exportation des fichiers CSV/CEF sera gzippée.
- Avec l'option Compresser non cochée, l'exportation des fichiers CSV/CEF ne sera pas gzippée.

Exportation vers SCAP ou AXIS

Dans la Définition de processus d'audit, dans la section Ajouter une nouvelle tâche, lorsque le type de tâche choisi est Evaluation de la sécurité, plusieurs choix apparaissent : Exporter XML AXIS et Exporter XML SCAP. Choisissez l'une de ces options pour sauvegarder les résultats du processus d'audit et transférer le fichier XML vers la destination configurée pour Exportation des résultats (Gérer > Gestion des données > Exportation des résultats (Fichiers)). D'autres choix sont réservés à la configuration du format PDF : Rapport, Différence (Diff.), Rapport et différence (Rapport et diff.).

SCAP est l'acronyme de Security Content Automation Protocol. AXIS signifie Apache EXtensible Interaction System. Il est utilisé par QRadar.

Création ou changement de rapports

Utilisez le Générateur de rapports pour créer ou personnaliser des rapports, notamment pour appliquer des couleurs aux lignes à faire ressortir. Pour ouvrir le Générateur de rapports, suivez le trajet Rapports > Outils de configuration de rapport > Générateur de rapports.

Création d'un processus d'audit

1. Ouvrez le Générateur de processus d'audit en suivant le trajet Conformité > Outils et vues > Générateur de processus d'audit.
2. Cliquez sur le bouton Nouveau pour ouvrir le panneau Définition de processus d'audit, lequel est divisé en trois sections : Général, Récepteurs et Tâches.
3. Allez d'abord à la section Tâches. Vous devez définir au moins une tâche d'audit avant de pouvoir sauvegarder le processus. Parcourez chaque tâche et faites vos choix. Exécutez la procédure adéquate pour chaque tâche d'audit que vous souhaitez inclure dans le processus d'audit. Les choix proposés dans cette section permettent d'effectuer les opérations suivantes :
   - Définir une tâche Rapport
   - Définir une tâche Evaluation de la sécurité
   - Définir une tâche Trace d'audit d'entité
   - Définir une tâche Jeu de confidentialité
   - Définir une tâche Processus de classification
   - Définir une tâche Flux externe
4. Allez à la section Récepteurs. Ouvrez la boîte déroulante et ajoutez les récepteurs du processus. Consultez Ajout de récepteurs. Différentes cases doivent être cochées pour déterminer l'action nécessaire, les ajouts à la liste des tâches, la notification par e-mail et la distribution continue. Là encore, consultez la section Ajout de récepteurs pour des informations complètes sur la définition de ces choix.
5. Allez à la section Général. Entrez un nom dans la zone Description. N'incluez pas d'apostrophe.
6. Cochez la case Actif pour associer un planning à ce processus.
7. Cochez la case Archiver les résultats si vous voulez stocker les résultats hors ligne une fois écoulée leur période de conservation. Les résultats ainsi archivés pourront être restaurés ultérieurement sur le système afin d'être consultés à nouveau.
8. Utilisez l'option Autoriser la purge des résultats avant la révision pour supprimer les résultats d'un processus ad hoc sans attendre que tous les réviseurs les aient passés en revue, que toutes les signatures (acceptations) aient été données et que toutes les activités du flux de travail aient été menées à bien. Cela permet à l'utilisateur de supprimer les résultats sur une période donnée (par exemple, 1 jour), qu'ils aient ou non été passés en revue.
9. Dans les zones Conserver pendant au moins (n) jours ou (n) exécutions, indiquez pendant combien de temps les résultats doivent être conservés. Il peut s'agir d'un nombre de jours (0 par défaut) ou d'un nombre d'exécutions (5 par défaut). Une fois cette période écoulée, les résultats seront archivés (si la case Conserver pendant au moins est cochée) et purgés du système.
   Remarque : Les résultats ne seront affichés que s'il y a des récepteurs pour eux. Ajoutez des récepteurs, lancez une nouvelle exécution et celle-ci sera visible dans la liste déroulante.
10. Si une ou plusieurs tâches créent des fichiers CSV ou CEF, vous pouvez, au besoin, entrer dans la zone Libellé de fichier CSV/CEF un libellé à inclure dans tous les noms de fichier. Vous pouvez aussi choisir de compresser ces fichiers ou de les zipper en cochant la case Zipper pour e-mail.
    Remarque : La taille des fichiers CSV/CEF exportés est limitée à 10240 Mo (soit 10,240 Go). Il est conseillé de cocher la case Zipper pour e-mail.
11. Dans la définition d'un processus d'audit, le contenu du champ Objet de l'e-mail est utilisé dans les e-mails adressés à tous les récepteurs de ce processus. L'objet peut contenir une (ou plusieurs) des variables suivantes, qui seront remplacées à l'exécution :
    - %%ProcessName sera remplacée par la description du processus d'audit.
    - %%ExecutionStart sera remplacée par la date et l'heure de début de la première tâche.
    - %%ExecutionEnd sera remplacée par la date et l'heure de fin de la dernière tâche.

    La donnée entrée dans ce champ est validée : le système vérifie si l'objet contient une variable (code commençant par %%) et s'assure de sa validité.
12. Au besoin, affectez des rôles de sécurité.
13. En option, ajoutez un commentaire.
14. Cliquez sur les boutons appropriés pour programmer le processus d'audit (planifier son exécution) ou l'exécuter immédiatement.
15. Cliquez sur Sauvegarder. Ne quittez pas cet écran pour effectuer une autre tâche de configuration avant d'avoir sauvegardé votre travail. Le travail en cours et inachevé n'est pas conservé si vous quittez cette section pour aller créer quelque chose d'autre pour la tâche d'audit.

    Par exemple, pour définir une tâche d'évaluation dans le Générateur de processus d'audit, vous devez d'abord aller dans le Générateur d'évaluation de sécurité pour créer les tests d'évaluation, puis aller dans Définitions de source de données pour identifier la ou les bases de données à évaluer. Sauvegardez votre travail au moment où vous créez le flux de travail du processus d'audit, puis allez aux autres tâches, ou exécutez celles-ci en premier, puis créez le processus d'audit.

Ajout de récepteurs

1. Dans la colonne Récepteur, faites un choix dans la liste des utilisateurs, groupes ou rôles Guardium. Si vous sélectionnez un groupe ou un rôle, tous les membres de ce groupe ou tous les utilisateurs titulaires de ce rôle recevront les résultats ; si la signature (acceptation) des résultats est requise, un seul de ces membres ou utilisateurs aura besoin de les signer.
2. Dans la colonne Action requise, sélectionnez une option parmi les suivantes :
   - Réviser (choix par défaut) - Indique que ce récepteur n'est pas tenu de signer les résultats.
   - Réviser et valider - Indique que ce récepteur doit signer les résultats (électroniquement, en cliquant sur le bouton Valider résultats lorsqu'il consulte les résultats en ligne).
3. Dans la colonne Liste des tâches, cochez ou décochez la case Ajouter pour indiquer si ce récepteur doit recevoir notification de l'existence de résultats en attente dans sa Liste des tâches du processus d'audit.

Remarque : Pour envoyer les fichiers sur un serveur externe sans envoyer d'e-mail et sans ajouter les résultats à la liste des tâches, définissez un processus d'audit sans récepteurs. Pensez aussi à décocher la case Liste des tâches dans la section Ajout de récepteur et à retirer les éventuels récepteurs de la section Récepteurs afin que les résultats ne soient pas ajoutés à leur liste de tâches.

4. Dans la colonne Notification électronique, sélectionnez une option parmi les suivantes :
   - Non - Aucun e-mail ne sera envoyé au récepteur.
   - Lier uniquement - L'e-mail de notification contiendra un lien hypertexte aux résultats stockés sur le système Guardium.
   - Résultats - L'e-mail contiendra une copie des résultats au format PDF ou CSV. N'oubliez pas que les résultats des tâches Classification ou Evaluation peuvent contenir des informations sensibles.
5. La case à cocher dans la colonne Continu détermine si la distribution des résultats se poursuivra au récepteur suivant (choix par défaut) ou s'interrompra jusqu'à ce que ce récepteur ait pris les mesures appropriées. Si cette case est décochée et que le récepteur concerné est un groupe ou un rôle, lorsqu'un utilisateur membre de ce groupe ou titulaire de ce rôle effectuera l'action sélectionnée, les résultats seront passés au récepteur suivant sur la liste.
   Remarque : Les résultats ne seront distribués au récepteur suivant que lorsque le récepteur du moment aura cliqué sur le bouton Continuer. Ce procédé est entièrement séparé de la fonctionnalité de revue/signature et n'en dépend aucunement.
6. Cliquez sur Ajouter pour ajouter le récepteur à la fin de la liste ; répétez ces étapes pour chaque récepteur voulu. Il faut au moins un récepteur.
7. Il est permis de choisir des récepteurs autres que des utilisateurs. Un récepteur peut être une simple adresse e-mail. Choisissez E-mail, entrez un adresse e-mail et les résultats seront envoyés à cette adresse e-mail. Lorsque l'adresse e-mail n'est pas celle d'un utilisateur, il faut néanmoins entrer un nom d'utilisateur, car il servira à filtrer les données. Il doit s'agir du même utilisateur que celui qui est connecté ou d'un utilisateur qui en dépend dans la hiérarchie. Cet utilisateur sera sauvegardé dans une nouvelle colonne de la section Récepteurs de l'écran.
8. Approuver si vide - Lorsque cette case est cochée, si tous les rapports de la tâche sont vides, cela aura pour conséquences de signer automatiquement le résultat (et/ou de le marquer comme vu), de cliquer automatiquement sur Continuer (le cas échéant), de ne PAS envoyer d'e-mail de notification, de ne PAS ajouter la tâche à la liste des tâches de l'utilisateur concerné et de ne PAS générer de fichiers PDF/CSV/CEF. Même vides, les résultats d'audit seront signés automatiquement et, dans les journaux des résultats d'audit, seront présentés exactement comme d'autres résultats d'audit non vides (vus et signés). Cette action sera appliquée aux rapports vides ainsi qu'aux résultats d'évaluation de sécurité vides. Consultez le tableau récapitulant les actions exécutées lorsque Approuver si vide = OUI, plus haut dans la section Exportation des résultats de tâches d'audit sous forme de fichiers CSV, CEF ou PDF.

Exportation d'un fichier CSV ou CEF

Les données produites par les tâches d'audit Rapport, Trace d'audit d'entité et Jeu de confidentialité peuvent être exportées au format CSV. Les données destinées à la production de rapports d'activité des bases de données peuvent quant à elles être exportées au format de fichier CEF (ArcSight Common Event Format). Sous Tâches d'audit, dans la section Rapport, Trace d'audit d'entité ou Jeu de confidentialité, effectuez les étapes suivantes :

1. Sélectionnez un titre.
2. (optionnel) Entrez un libellé pour le fichier dans la zone Libellé de fichier CSV/CEF. Par défaut, le libellé reprend la Description de la tâche. Ce libellé entrera dans la composition du nom du fichier généré (une autre composante de ce nom sera le libellé défini pour le processus d'automatisation du flux de travail).
3. Cochez l'option Exporter fichier CSV ou Exporter fichier CEF.
   Remarque : L'exportation au format de fichier CEF n'est appropriée que pour les rapports du domaine Accès aux données (par exemple, Accès, Exceptions ou Violations de politique). Les autres domaines tels que ceux de l'autosurveillance Guardium (Agrégation/Archivage, Processus d'audit, Connexions à Guardium, etc.) n'ont pas de lien avec les extensions CEF.
4. Si l'option Exporter fichier CEF a été sélectionnée, au besoin, cochez la case Ecrire dans syslog (journal système) pour écrire les enregistrements CEF dans syslog. Si la fonctionnalité syslog disant est activée, les enregistrements du fichier CEF seront écrits dans le syslog distant.
5. Si la case Compresser est cochée, les fichiers CSV/CEF à exporter seront compressés.
6. Si la case Exporter un fichier PDF est cochée, un fichier PDF (au nom similaire à celui du fichier CSV) sera créé pour cette tâche d'audit et exporté en même temps que les fichiers CSV/CEF.
   Remarque : Le fichier PDF exporté ne sera pas compressé, même si la case Compresser a été cochée à l'étape précédente.

Définir une tâche Rapport

Si vous n'avez pas encore commencé à définir de processus d'automatisation du flux de travail de conformité, créez-en un avant d'effectuer cette procédure. Si le rapport à utiliser n'a pas encore été défini, faites-le d'abord.

1. Si le panneau Ajouter une nouvelle tâche n'est pas ouvert, cliquez sur Ajouter une tâche d'audit.
2. Cliquez sur l'option Rapport.
3. Plusieurs sélections sont à effectuer : Libellé de fichier CSV/CEF, Exporter CSV/CEF, Exporter PDF, Ecrire dans syslog, Compresser. Consultez Exportation d'un fichier CSV ou CEF.
4. La sélection d'options PDF est la suivante : Rapport (résultats du moment), Diff. (différence entre un rapport précédent et un nouveau rapport) et Rapport et diff. (les deux).
   Remarque : La sélection d'options PDF s'applique tant aux pièces jointes PDF qu'aux fichiers exportés au format PDF. Le rapport Diff. s'applique uniquement APRÈS la première exécution de cette tâche.(De toute évidence, il n'est pas possible d'établir de comparaison avec des résultats précédents qui n'existent pas encore.) Le nombre maximum de lignes comparables en une seule fois est de 5000. Si le nombre de lignes de résultats dépasse cette limite, le message

   ```
   (comparer les 5000 premières lignes uniquement)
   ```

   apparaîtra dans le résultat de la comparaison.
5. Entrez des valeurs pour tous les paramètres dans le panneau Paramètres de tâche. La nature de ces paramètres dépendra du type de rapport sélectionné.
6. Cliquez sur Appliquer.

API pour l'exécution automatique

Par défaut, l'application Guardium est livrée avec des données de configuration qui relient nombre de fonctions d'API aux rapports, permettant aux utilisateurs de bénéficier, à travers l'interface graphique, d'appels préconfigurés aux API depuis les données des rapports. Utilisez le panneau Affectation d'API, dans le générateur de rapports, pour lier d'autres fonctions d'API aux rapports Guardium prédéfinis ou à vos rapports personnalisés. L'option de menu API d'exécution automatique apparaîtra dans Ajouter une tâche d'audit : Rapport si le rapport sélectionné (rapport Guardium prédéfini ou rapport personnalisé) contient des champs reliés à des paramètres d'API. C'est le cas, par exemple, des rapports prédéfinis Violations de politique d'accès, Bases de données reconnues et Détails du groupe Guardium.

Générateur de flux de travaux

Vous gérez la séquence formelle de types d'événement créés dans le Générateur de flux de travaux en cliquant sur le bouton Evénement et colonnes supplémentaires dans la fenêtre Tâches d'audit. Ce bouton apparaît après qu'une tâche d'audit a été créée et sauvegardée. Il n'apparaît pas tant que la tâche d'audit n'a pas été sauvegardée. Configurez ces activités du flux de travail lorsque vous ajoutez une tâche d'audit :

1. Créez et sauvegardez une tâche d'audit. Une fois la tâche sauvegardée, un bouton supplémentaire apparaîtra : Evénement et colonnes supplémentaires.

2. Cliquez sur ce bouton additionnel.
3. Dans l'écran suivant, cochez la case Evénement et acceptation. Le flux créé dans le Générateur de flux de travaux apparaîtra comme choix dans Evénement et acceptation.
4. Mettez ce choix en évidence. Appliquez (sauvegardez) votre sélection.
5. Si des informations supplémentaires (comme des codes de société, des intitulés d'unité commerciale etc.) sont requises dans le rapport de flux de travaux, ajoutez-les dans la section Définir des colonnes supplémentaires, puis cliquez sur Appliquer (pour sauvegarder). Pour sélectionner la colonne des groupes prédéfinis ou créés, changez la colonne Type en Groupe. Cela fait, fermez cette fenêtre.
6. Appliquez (sauvegardez) votre tâche d'audit. Appliquez (sauvegardez) la définition entière du processus d'audit.

Ce bouton Evénement et colonnes supplémentaires apparaît dans toutes les tâches d'audit. Lorsque l'utilisateur passe le pointeur dessus, une bulle d'information apparaît, indiquant si la tâche d'audit a une colonne Evénement ou Acceptation liée à la tâche d'audit concernée.

Remarque :

Si la sécurité au niveau des données, pour le niveau de données observé, a été activée, la sortie du processus d'audit est filtrée de sorte que les utilisateurs ne voient que les informations provenant de leurs bases de données.

Le choix de rapports sous Ajouter une tâche d'audit comprend deux rapports procéduraux : Evénements en attente et Transition du statut de l'événement. Ajoutez ces deux rapports à deux nouvelles tâches d'audit pour montrer les détails de tous les événements du flux de travail, avec leurs transitions d'un état à un autre. Ces deux rapports ne seront pas filtrés (le filtrage de sécurité au niveau Observé ne s'appliquera pas). Par défaut, ils ne sont disponibles dans la liste des rapports que pour l'utilisateur administrateur ainsi que pour les utilisateurs titulaires du rôle d'administrateur.

Le bouton Colonnes supplémentaires est désactivé pour les tâches Classification.

Cloner une tâche d'audit - Si vous clonez un processus et que vous modifiez une tâche clonée avant que le processus cloné ne soit sauvegardé, le flux de travail associé à la tâche originale ne sera pas cloné.

La suppression d'un état d'événement n'est permise que s'il ne constitue pas le premier état d'un événement quel qu'il soit et s'il n'est utilisé par aucune action. Le mécanisme de validation fournira la liste des événements/actions interdisant la suppression de l'état concerné.

Le propriétaire/créateur d'un événement du flux de travail a toujours une visibilité de tous les états de cet événement, quels que soient les rôles qui ont été associés à ces états.

Définir une tâche Evaluation de la sécurité

Si vous n'avez pas encore commencé à définir de processus d'automatisation du flux de travail de conformité, créez-en un avant d'effectuer cette procédure. Si l'évaluation à utiliser n'a pas encore été définie, faites-le d'abord.

1. Si le panneau Ajouter une nouvelle tâche n'est pas ouvert, cliquez sur Ajouter une tâche d'audit.
2. Cliquez sur le bouton Evaluation de sécurité.
3. Sélectionnez une évaluation de sécurité dans la liste correspondante.
4. La sélection de contenus PDF est la suivante : Rapport (résultats du moment), Diff. (différence entre un rapport précédent et un nouveau rapport) et Rapport et diff. (les deux).
5. Cliquez sur Appliquer.

Remarque :

Si la sécurité au niveau des données, pour le niveau de données observé, a été activée, la sortie du processus d'audit est filtrée de sorte que les utilisateurs ne voient que les informations provenant de leurs bases de données.

Si une tâche d'évaluation de sécurité est vide (par exemple, une évaluation sans rôles affectés), elle n'apparaîtra pas dans la liste déroulante du Générateur de processus d'audit.

Définir une tâche Trace d'audit d'entité

Si vous n'avez pas encore commencé à définir de processus d'automatisation du flux de travail de conformité, créez-en un avant d'effectuer cette procédure.

1. Si le panneau Ajouter une nouvelle tâche n'est pas ouvert, cliquez sur Ajouter une tâche d'audit.
2. Cliquez sur le bouton Trace d'audit d'entité.
3. Sélectionnez le type d'entité à auditer. Vous devez fournir les informations suivantes, qui varient en fonction du type choisi :
    - Objet : entrez un nom d'objet.
    - Groupe d'objets : sélectionnez un groupe d'objets dans la liste.
    - IP client : entrez une adresse IP de client.
    - Groupe d'IP client : sélectionnez un groupe d'IP de client.
    - IP serveur : entrez une adresse IP de serveur.
    - Nom d'utilisateur d'application : entrez un nom d'utilisateur d'application.
4. Plusieurs sélections sont à effectuer : Libellé de fichier CSV/CEF, Ecrire dans syslog (journal système), Compresser et Exporter PDF. Consultez Exportation d'un fichier CSV ou CEF.
5. Dans le panneau Paramètres de tâche, fournissez les valeurs des paramètres qui serviront à l'exécution (seules les dates et heures de début et de fin de période sont obligatoires).
6. Cliquez sur Appliquer.

Remarque : Si la sécurité au niveau des données, pour le niveau de données observé, a été activée, la sortie du processus d'audit est filtrée de sorte que les utilisateurs ne voient que les informations provenant de leurs bases de données.

Définir une tâche Jeu de confidentialité

Si vous n'avez pas encore commencé à définir de processus d'automatisation du flux de travail de conformité, créez-en un avant d'effectuer cette procédure. Si le jeu de confidentialité à utiliser n'a pas encore été défini, faites-le d'abord.

1. Si le panneau Ajouter une nouvelle tâche n'est pas ouvert, cliquez sur Ajouter une tâche d'audit.
2. Cliquez sur le bouton Jeu de confidentialité.
3. Sélectionnez un jeu de confidentialité dans la liste correspondante.

4. Sélectionnez Rapport par détails des accès ou Rapport par utilisateur d'application pour spécifier comment les résultats doivent être triés et affichés.
5. Plusieurs sélections sont à effectuer : Libellé de fichier CSV/CEF, Ecrire dans syslog (journal système), Compresser et Exporter PDF. Consultez Exportation d'un fichier CSV ou CEF.
6. Entrez les dates de début et de fin pour le rapport dans les zones Début de période et Fin de période.
7. Cliquez sur Appliquer.

Remarque : Si la sécurité au niveau des données, pour le niveau de données observé, a été activée, la sortie du processus d'audit est filtrée de sorte que les utilisateurs ne voient que les informations provenant de leurs bases de données.

Définir une tâche Processus de classification

Si vous n'avez pas encore commencé à définir de processus d'automatisation du flux de travail de conformité, créez-en un avant d'effectuer cette procédure. Si le processus de classification à utiliser n'a pas encore été défini, faites-le d'abord.

1. Si le panneau Ajouter une nouvelle tâche n'est pas ouvert, cliquez sur Ajouter une tâche d'audit.
2. Cliquez sur le bouton Processus de classification.
   Remarque : Un message vous alerte sur le fait que les processus de classification peuvent retourner des données sensibles et que les résultats seront ajoutés aux fichiers PDF ou CSV.
3. Sélectionnez un processus de classification dans la liste correspondante. Cliquez sur Appliquer.

Remarque : Si la sécurité au niveau des données, pour le niveau de données observé, a été activée, la sortie du processus d'audit est filtrée de sorte que les utilisateurs ne voient que les informations provenant de leurs bases de données.

Définir une tâche Flux externe

Ce type de tâche d'automatisation du flux de travail alimente une application externe en données recueillies par Guardium et les mappe vers un format reconnu par cette application. Cette fonctionnalité est une option payante : elle est vendue à part et activée par un module complémentaire (patch).

Remarque : Si cette fonctionnalité est utilisée dans un environnement de gestionnaire central, le module (patch) Flux externe doit être installé sur le gestionnaire central ainsi que sur chaque unité gérée sur laquelle la tâche sera exécutée.

Pour plus d'informations sur la manière dont les données sont mappées entre Guardium et l'application externe, référez-vous à la documentation de l'option qui a été achetée.

Si vous n'avez pas encore commencé à définir de processus d'automatisation du flux de travail de conformité, créez-en un avant d'effectuer cette procédure.

1. Si le panneau Ajouter une nouvelle tâche n'est pas ouvert, cliquez sur Ajouter une tâche d'audit.
2. Cliquez sur Flux externe.
3. Sélectionnez un type de flux dans la liste correspondante.
4. Les contrôles qui apparaissent ensuite dépendent du type de flux sélectionné. Consultez Flux externe optionnel pour davantage d'informations sur chaque type de flux externe.
5. Sélectionnez un type d'événement dans la liste correspondante.
6. Sélectionnez un rapport dans la liste correspondante. Un nombre variable de paramètres apparaît dans le panneau Paramètres de tâche, selon le type de rapport choisi.
7. Dans la zone Retard d'extraction, entrez le nombre d'heures dont le flux doit être retardé ou cochez la case Continu pour inclure les données jusqu'au moment où la tâche d'audit est exécutée.
8. Dans le panneau Sources de données, identifiez une ou plusieurs sources de données pour le flux externe.
9. Entrez des valeurs pour tous les paramètres dans le panneau Paramètres de tâche. La nature de ces paramètres dépendra du type de rapport sélectionné.
10. Cliquez sur Appliquer.

Voir ou signer les résultats

1. Ouvrez les résultats du processus d'automatisation du flux de travail de conformité.
2. Si la signature est requise, cliquez sur le bouton Valider résultats.
3. Optionnel. Pour transférer ces résultats à un autre utilisateur, cliquez sur Escalader et consultez Transférer les résultats à des récepteurs supplémentaires (dans la section Escalade).
4. Cliquez sur le lien Fermer cette fenêtre.

Remarque : Si des événements sont en attente, les résultats ne peuvent être signés ni depuis l'afficheur d'audit ni depuis la liste des tâches. Si vous tentez de signer les résultats alors que des événements sont en attente, le message suivant apparaît :

```
Le processus d'audit ne peut pas être validé car des événements sont en attente.

Mettez à jour tous les événements en attente avant de valider ce résultat.
```

Remarque : Lors de la consultation des résultats d'un processus d'audit, si un résultat a des événements qui lui sont associés, le bouton Valider résultats n'est pas disponible pour ce résultat tant que tous les événements ne sont pas dans l'état Final, ou bien ils ne peuvent pas être vus par l'utilisateur (en raison de la sécurité de niveau données).
Remarque : Ce rapport contient également la mention de la date ou de l'heure de la dernière action dans une colonne située entre Récepteur et Statut. Cela signifie qu'il indique d'une part qui a signé le résultat, d'autre part à quel moment cette signature a eu lieu.

Remettre en circulation les résultats sans les signer ni les voir

1. Ouvrez votre panneau Liste des tâches.
2. Cliquez sur le bouton Continuer pour les résultats que vous souhaitez faire avancer jusqu'au récepteur suivant sur la liste de distribution.
3. Cliquez sur le lien Fermer cette fenêtre.

Voir l'état de distribution des résultats

1. Ouvrez les résultats du processus d'automatisation du flux de travail de conformité.
2. Développez le panneau Statut de distribution en cliquant sur le bouton (Afficher les détails).
3. Cliquez sur le lien Fermer cette fenêtre.

Voir les commentaires ajoutés aux résultats par les récepteurs

1. Ouvrez les résultats du processus d'automatisation du flux de travail de conformité.
2. Développez le panneau Commentaires en cliquant sur le bouton Afficher les détails.
   Remarque : Les commentaires visibles dans ce contexte sont ceux qui étaient déjà associés aux résultats au moment où la page de rapport a été obtenue du système Guardium. Si vous ajoutez ensuite vos propres commentaires ou si d'autres récepteurs ajoutent des commentaires au même moment, vous ne pourrez les voir qu'après avoir actualisé la page (en utilisant la fonction prévue à cet effet dans votre navigateur).
3. Cliquez sur le lien Fermer cette fenêtre.

Escalader les résultats du processus

Un récepteur désigné des résultats du processus peut transférer la notification de mise à disposition de ces résultats à d'autres récepteurs pour revue et/ou acceptation (signature). Si vous transférez (escaladez) les résultats à un récepteur hors audit et trace d'acceptation d'origine et s'ils incluent un fichier CSV, celui-ci ne sera pas joint à la notification.

Un résultat d'audit peut être transféré par escalade à n'importe quel utilisateur dans le système dès lors que la case Escalader le résultat à tous les utilisateurs est cochée dans le menu Configurer > Outils et vues > Profil global. Dans ces circonstances, peu importe qui est récepteur de ce résultat. Lorsque cette case est cochée (elle l'est par défaut), les résultats du processus d'audit peuvent être escaladés à tous les utilisateurs, y compris si la sécurité des données au niveau Observé est activée. Si cette case n'est pas cochée, l'escalade des résultats du processus d'audit ne peut viser que les utilisateurs à un niveau plus haut dans la hiérarchie. Cela signifie que si aucune hiérarchie des utilisateurs n'est définie, aucune escalade n'est permise lorsque cette case est décochée.

Il faut aussi tenir compte du fait que les utilisateurs n'ont pas tous les mêmes autorisations sur les événements. Si, par exemple, l'utilisateur infosec ne peut voir que les événements à l'état 1 et que l'utilisateur dba ne peut voir que les événements à l'état 2, ce dernier recevra un résultat différent de celui que voyait l'utilisateur infosec lorsqu'il a cliqué sur Escalader.Il est par conséquent possible que l'utilisateur infosec escalade à dba et que ce dernier reçoive un résultat d'audit avec 0 ligne.

1. Si les résultats d'automatisation du flux de travail de conformité que vous voulez transférer ne sont pas ouverts, ouvrez-les maintenant.
2. Cliquez sur Escalader.
3. Sélectionnez le récepteur dans la liste correspondante.
4. Dans la colonne Action requise, sélectionnez Réviser (choix par défaut) ou Réviser et valider.
5. Cliquez sur le bouton Escalade pour achever l'opération.

Remarque :

Les résultats d'un processus d'audit ne peuvent pas être escaladés à un groupe d'utilisateurs. Seuls des utilisateurs désignés ou des rôles sont autorisés.

En cas d'escalade d'un résultat à un utilisateur ayant déjà la revue/signature de ce résultat dans sa liste de tâches, un message s'affiche pour vous demander si un autre e-mail doit lui être envoyé. Si vous répondez oui, un autre e-mail sera envoyé à l'utilisateur, mais sa liste de tâches ne sera pas incrémentée.

Programmer l'exécution d'un processus d'automatisation du flux de travail de conformité ou l'exécuter immédiatement

1. Ouvrez le Générateur de processus d'audit en suivant le trajet Conformité > Outils et vues > Générateur de processus d'audit.
2. Sélectionnez le processus voulu dans la liste correspondante.
3. Cliquez sur Modifier pour ouvrir le panneau Définition de processus d'audit.
4. Pour une exécution ponctuelle et immédiate du processus, cliquez sur Exécuter une fois maintenant. Pour définir un planning d'exécution, cliquez sur Modifier le planning.
   Remarque : Lorsqu'un planning est défini pour un processus, ce dernier est exécuté conformément au planning, mais uniquement s'il est marqué actif. Pour activer ou désactiver un processus d'audit, consultez la section suivante.

Activer ou désactiver un processus d'automatisation du flux de travail de conformité

Lorsqu'un planning est défini pour un processus d'audit, ce dernier est exécuté conformément au planning, mais uniquement s'il est marqué actif.

Pour activer ou désactiver un processus d'audit :

1. Ouvrez le Générateur de processus d'audit en suivant le trajet Conformité > Outils et vues > Générateur de processus d'audit.
2. Sélectionnez le processus d'audit dans la liste correspondante.
3. Cliquez sur Modifier.
4. Dans le panneau Définition de processus d'audit, cochez la case Actif pour que le processus soit exécuté conformément au planning ou décochez-la pour empêcher toute exécution (y compris si un planning prévoit son exécution).
   Remarque : Si vous activez le processus alors qu'aucun planning n'est défini, cliquez sur Modifier le planning pour définir un tel planning et permettre ainsi l'exécution du processus au moment voulu.
5. Cliquez sur Sauvegarder.

- Création d'un flux de travaux d'audit
  Créez un flux de travaux de processus d'audit qui génère un rapport prédéfini en fonction d'une planification préconfigurée, affecte le rapport à l'administrateur de base de données pour qu'il le révise et le valide, et facilite l'envoi du rapport révisé à un superviseur pour une nouvelle révision et une nouvelle validation.
- Ouverture des résultats du processus de flux de travaux
  Cliquez sur Afficher pour consulter les résultats du processus de flux de travaux.
- Distribution d'un flux de travaux à des groupes Guardium
  Lorsque le type de récepteur choisi est un groupe, définissez un unique processus d'audit Flux de travaux de conformité qui enverra des résultats différents à divers utilisateurs Guardium en fonction d'un mappage personnalisé prédéfini.
- Liste des tâches du processus d'audit
  Cette rubrique décrit la Liste des tâches du processus d'audit et les étapes requises pour l'ouvrir et l'utiliser.

Rubrique parent : Surveillance et audit

Création d'un flux de travaux d'audit

Créez un flux de travaux de processus d'audit qui génère un rapport prédéfini en fonction d'une planification préconfigurée, affecte le rapport à l'administrateur de base de données pour qu'il le révise et le valide, et facilite l'envoi du rapport révisé à un superviseur pour une nouvelle révision et une nouvelle validation.

Pourquoi et quand exécuter cette tâche

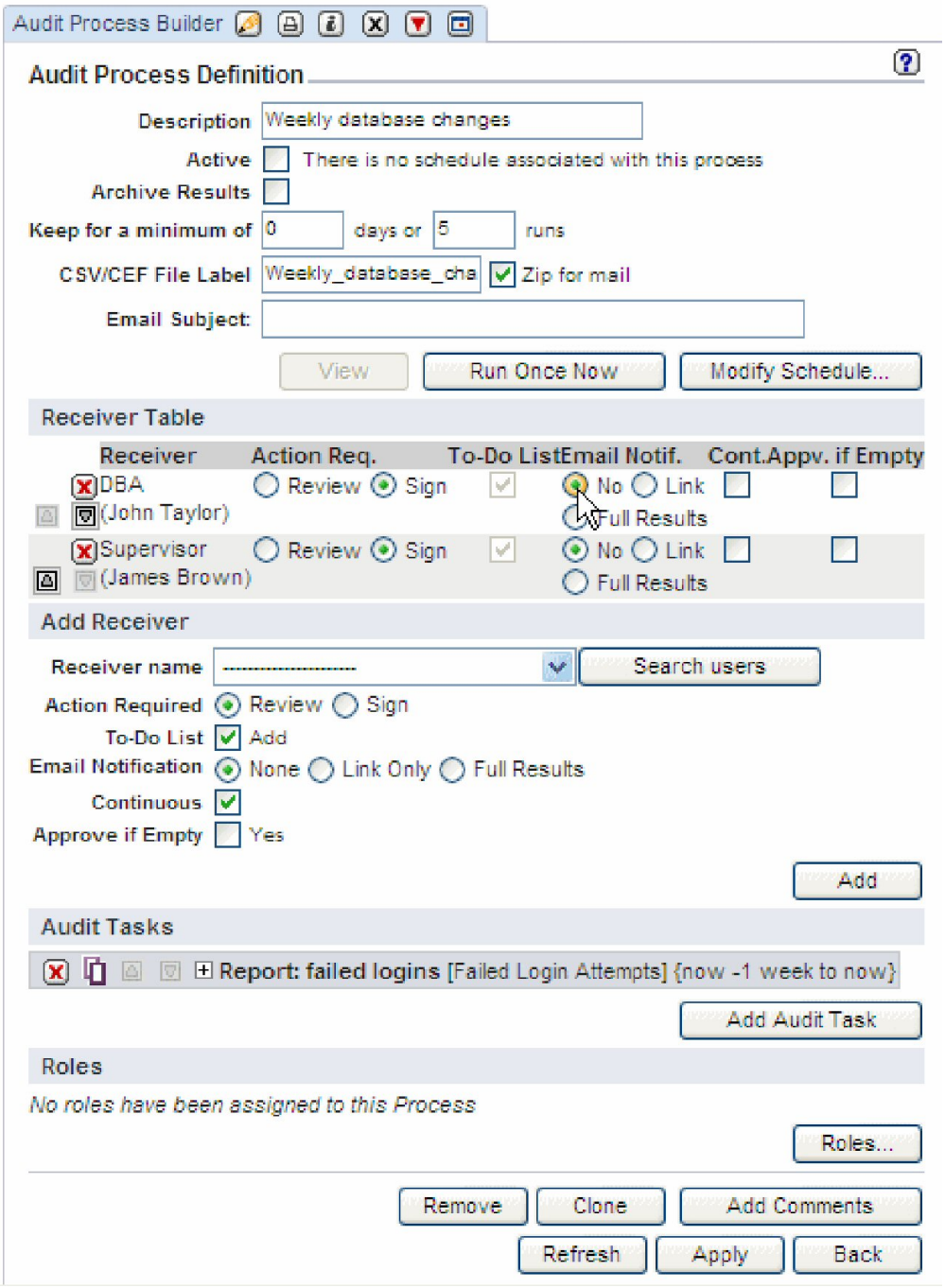
Automatisez les étapes de flux de travaux du processus d'audit du client.

Voir la rubrique Automatisation du flux de travaux de conformité pour plus d'informations à ce sujet.

Procédure

1. Ouvrez le localiseur de processus d'audit en sélectionnant Conformité > Outils et vues > Générateur de processus d'audit.
2. Cliquez sur le bouton Nouveau pour ouvrir le panneau Définition de processus d'audit.

   Le panneau Définition de processus d'audit comporte trois sections : Général, Table de récepteurs et Tâches d'audit.



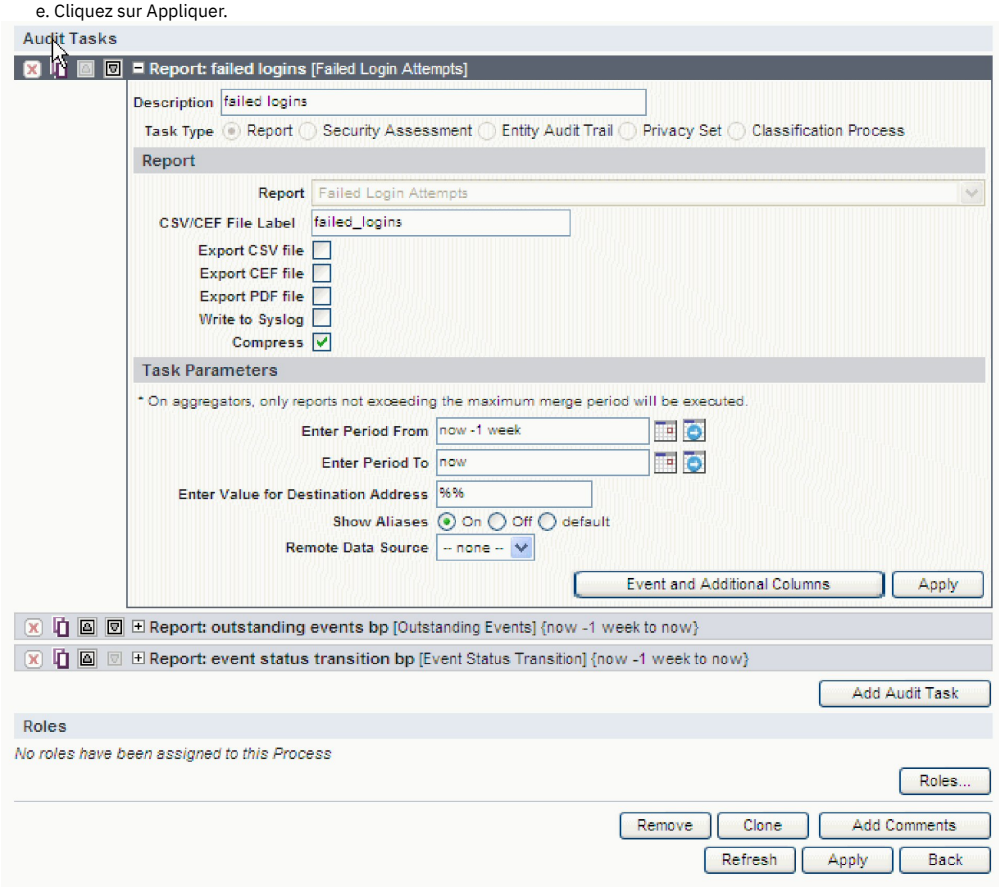
Ecran du menu Générateur de processus d'audit

3. Accédez à la section Général. Entrez un nom dans la zone Description. N'incluez pas d'apostrophe.
4. Sélectionnez la case à cocher Actif afin d'associer une planification au processus. Vous devez définir une tâche d'audit au moins pour pouvoir sauvegarder le processus.
5. Sélectionnez la case à cocher Archiver les résultats si vous voulez stocker les résultats hors ligne à la fin de la durée de conservation. Si des résultats ont été archivés, vous pouvez les restaurer sur le dispositif pour les consulter à nouveau, ultérieurement.
6. Dans les zones Conserver pendant un minimum de (n) jours ou (n) exécutions, spécifiez la durée de conservation des résultats en entrant un nombre de jours (0 par défaut) ou un nombre d'exécutions (5 par défaut). Une fois la durée de conservation écoulée, les résultats seront archivés (si la case à cocher Archiver les résultats est sélectionnée) et purgés sur le dispositif.

7. Si une ou plusieurs tâches créent des fichiers CSV ou CEF, si vous le souhaitez, vous pouvez entrer dans la zone Libellé de fichier CSV/CEF un libellé à inclure dans tous les noms de fichier. Vous pouvez aussi choisir de compresser ces fichiers ou de les zipper en cochant la case Zipper CSV pour e-mail.
8. La zone Objet de l'e-mail dans la définition de processus d'audit est utilisée dans les e-mails pour tous les récepteurs de ce processus d'audit. L'objet peut contenir une ou plusieurs des variables suivantes, qui sont remplacées à l'exécution :
   - %%ProcessName est remplacée par la description du processus d'audit.
   - %%ExecutionStart est remplacée par la date et l'heure de début de la première tâche.
   - %%ExecutionEnd est remplacée par la date et l'heure de fin de la dernière tâche.

   Lorsque vous entrez un objet, le système détermine si des variables (commençant par %%) sont présentes et si elles sont toutes valides.

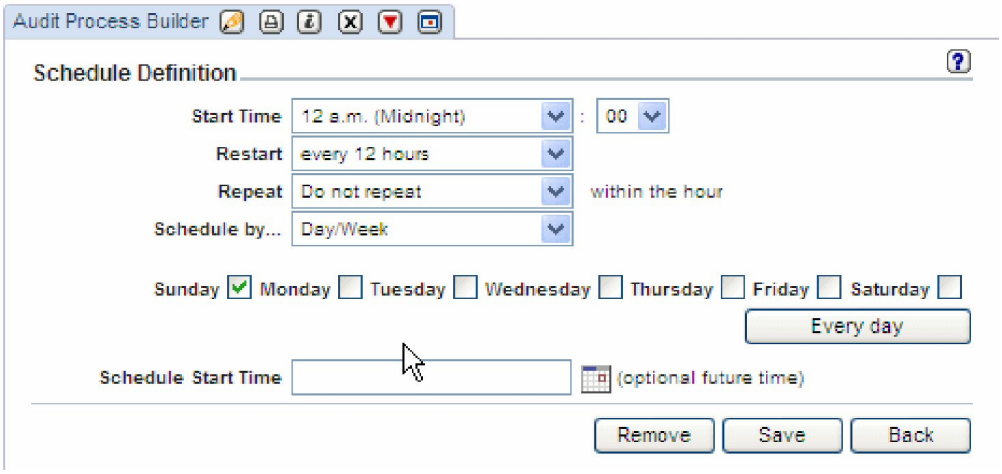
9. Accédez à la section Récepteurs. Ouvrez la zone déroulante et ajoutez les récepteurs pour le processus. Voir Ajout de récepteurs dans la rubrique Automatisation du flux de travaux de conformité pour plus d'informations. Des cases à cocher permettent de définir l'action requise, les ajouts à la liste des tâches, la notification par e-mail et la distribution en continu. Voir Ajout de récepteurs pour des informations complètes relatives à la définition de ces choix. Dans cet exemple, ne sélectionnez pas les cases à cocher pour la distribution en continu pour les récepteurs. Si la case à cocher Cont. est sélectionnée, la distribution continue sur le récepteur suivant dans la liste, sans interruption. Si la case à cocher Cont. n'est pas sélectionnée, la distribution sur le récepteur suivant est mise en attente jusqu'à ce que le récepteur en cours effectue l'action requise (réviser ou valider). Dans cet exemple, l'administrateur de base de données doit réviser et valider le rapport avant sa transmission au superviseur.
10. Accédez à la section Tâches. Vous devez définir une tâche d'audit au moins pour pouvoir sauvegarder le processus.
11. Définissez une tâche de rapport.
    a. Si la sous-fenêtre Ajouter une nouvelle tâche n'est pas ouverte, cliquez sur Ajouter une tâche d'audit (voir l'illustration).
    b. Cliquez sur le bouton Rapport.
    c. Si vous le souhaitez, créez une sortie au format de fichier CSV ou CEF et écrivez les données dans Syslog.
    d. Entrez toutes les valeurs de paramètre dans la sous-fenêtre Paramètres de tâche. Les paramètres sont différents selon le rapport sélectionné.
    e. Cliquez sur Appliquer.



Tâche d'audit – Rapport

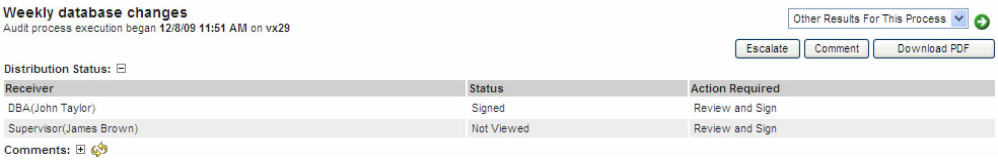
12. Si vous le souhaitez, affectez des rôles de sécurité.
    a. Ouvrez ou sélectionnez l'élément auquel affecter un ou plusieurs rôles de sécurité (par exemple, une définition de rapport).
    b. Cliquez sur le bouton Rôles.
    c. Dans le panneau Affecter des rôles de sécurité, sélectionnez tous les rôles à affecter (vous ne voyez que les rôles qui ont été affectés à votre compte).
    d. Cliquez sur Appliquer.
13. Si vous le souhaitez, ajoutez des commentaires.
14. Cliquez sur les boutons appropriés pour planifier ou exécuter un processus de flux de travaux d'audit (voir lien).
15. Cliquez sur Appliquer.
16. Planifiez ou exécutez un processus d'automatisation de flux de travaux de conformité.
    Ouvrez le localiseur de processus d'audit en sélectionnant Conformité > Outils et vues > Générateur de processus d'audit.
    a. Sélectionnez le processus dans la liste de sélection de processus.
    b. Cliquez sur Modifier pour ouvrir le panneau Définition de processus d'audit.
    c. Pour exécuter le processus une fois, cliquez sur Exécuter une fois maintenant ou bien, pour définir une planification pour le processus, cliquez sur Modifier la planification.

    Remarque : Une fois qu'une planification a été définie pour un processus, le processus s'exécute conformément à cette planification uniquement si la case à cocher Actif est sélectionnée.



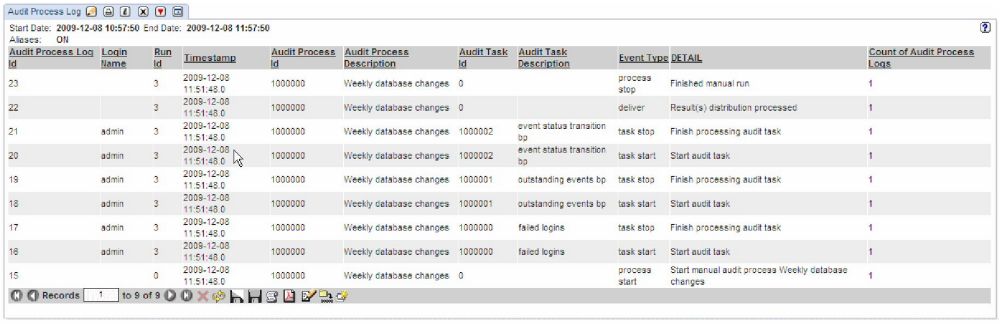
17. Validation et révision d'un rapport

    Une fois que le rapport a été exécuté, le statut de distribution est affiché dans le rapport. Dans l'exemple, l'administrateur de base de données a révisé et validé le rapport, mais pas le superviseur.



    Statut de distribution

    Le rapport Journal du processus d'audit présente un journal d'activité détaillé pour toutes les tâches, avec les heures de début et de fin. Pour y accéder, sélectionnez Rapports > Rapports opérationnels Guardium > Journal du processus d'audit. Les heures de début et de fin des tâches d'audit sont indiquées.



    Exemple de journal de processus d'audit

Rubrique parent : Construction de processus d'audit

Ouverture des résultats du processus de flux de travaux

Cliquez sur Afficher pour consulter les résultats du processus de flux de travaux.

Effectuez l'une des opérations suivantes :

- Ouvrez votre liste des tâches d'automatisation du flux de travaux (voir la liste des tâches de processus d'audit) et cliquez sur Afficher pour l'ensemble de résultats que vous voulez voir ou signer.
- Si vous avez reçu une notification par e-mail contenant des liens hypertexte vers votre liste des tâches ou les résultats, cliquez sur l'un des liens pour ouvrir votre liste des tâches ou les résultats directement depuis l'e-mail. Vous devez avoir accès au système Guardium à l'emplacement depuis lequel vous accédez à votre e-mail (sinon, ces liens ne fonctionnent pas). Si vous n'êtes pas connecté, vous êtes invité à vous connecter au système Guardium.

Remarque : Lorsque vous enregistrez une nouvelle unité gérée auprès d'un gestionnaire central, il se peut que vous ne puissiez pas afficher les résultats d'audit. L'application n'affiche pas les résultats dont l'horodatage est antérieur à l'enregistrement de l'unité gérée auprès du gestionnaire central. L'horodatage de l'enregistrement utilise l'heure du gestionnaire central, et l'horodatage du résultat d'audit utilise l'heure du noeud géré. Par conséquent, si l'heure du gestionnaire central est ultérieure à celle de l'unité centrale, les résultats générés sur l'unité gérée ne sont pas visibles tant que l'unité gérée n'a pas passé l'heure de l'enregistrement, ce qui se produit généralement dans les 24 heures, et parfois moins, selon les emplacements des deux machines. Vous devriez pouvoir consulter les résultats des processus d'audit sur l'unité gérée 24 heures au plus après l'enregistrement.
Rubrique parent : Construction de processus d'audit

Distribution d'un flux de travaux à des groupes Guardium

Lorsque le type de récepteur choisi est un groupe, définissez un unique processus d'audit Flux de travaux de conformité qui enverra des résultats différents à divers utilisateurs Guardium en fonction d'un mappage personnalisé prédéfini.

Avantage : configurez un processus d'audit unique et distribuez les résultats appropriés au responsable approprié. Ainsi, il n'est pas nécessaire de créer des processus d'audit distincts pour des récepteurs distincts.

L'automatisation du flux de travaux de conformité d'IBM Security Guardium distribue automatiquement des rapports, des résultats de classification et des résultats d'évaluation de la sécurité aux utilisateurs Guardium selon une planification. Les destinataires des résultats peuvent être des utilisateurs Guardium, des rôles Guardium ou des groupes d'utilisateurs.

Prenons l'exemple d'une grande organisation comptant quinze responsables d'administrateurs de base de données devant réviser les activités des administrateurs de base de données qu'ils gèrent sans afficher les activités des administrateurs de base de données gérés par les autres responsables. L'une des solutions consiste à configurer quinze processus d'audit distincts, un pour chaque responsable. Cette configuration prend beaucoup de temps et est difficile à gérer : chaque processus d'audit doit être planifié séparément et tout changement global doit être effectué individuellement dans chacun des quinze processus d'audit.

En revanche, la méthode de distribution à des groupes d'utilisateurs permet de ne configurer qu'un seul processus d'audit et de distribuer les résultats appropriés à chaque responsable en fonction d'un mappage responsable/administrateur de base de données. Ce processus nécessite une configuration plus importante en amont, mais réduit le temps consacré à la maintenance. Il suffit de planifier un seul processus d'audit et d'appliquer les changements à un emplacement seulement.

Mappage des utilisateurs

La première étape du processus consiste à mapper les utilisateurs aux éléments de données dans Guardium, qui constitueront la base pour la distribution des rapports. L'exemple présenté dans ce document repose sur des objets, mais vous pouvez appliquer ces concepts à tout élément de données dans Guardium.

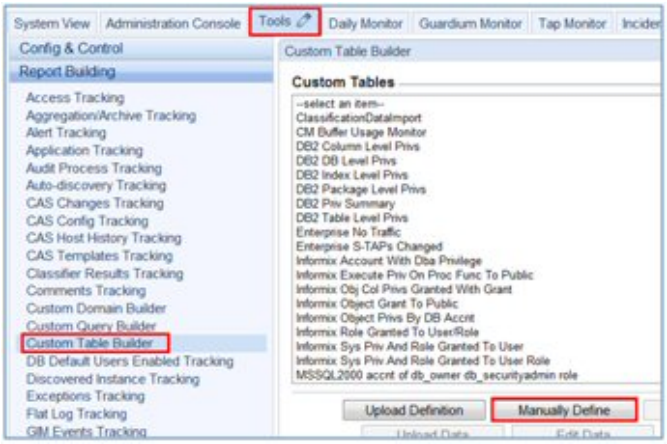
Exemple : trois utilisateurs sont responsables de trois ensembles de tables différents, conformément aux exigences en matière d'audit (PCI, HIPPA et CCI) sur un serveur de base de données, comme suit :

Tableau 1. Utilisateur avec table/objet

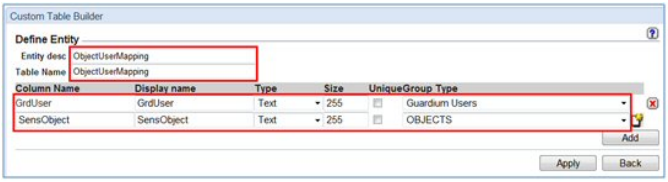
Utilisateur	Table/Objet
Utilisateur01	db2inst1.cc_numbers
Utilisateur01	db2inst1.ccn
Utilisateur02	db2inst1.ADDRESSES
Utilisateur02	db2inst1.SSN_NUMBERS
Utilisateur02	db2inst1.G_CUSTOMERS
Utilisateur02	db2inst1.G_EMPLOYEES
Utilisateur02	db2inst1.G_FUNDS
Utilisateur03	db2inst1.doctor
Utilisateur03	db2inst1.medicare
Utilisateur03	db2inst1.med_history

Cette table doit être ajoutée en tant que table personnalisée dans Guardium, manuellement ou via le téléchargement de données. Les étapes ci-après permettent de créer une table personnalisée manuellement. Les captures d'écran proviennent de l'interface utilisateur “admin”, mais sont également accessibles depuis l'interface utilisateur “utilisateur”.

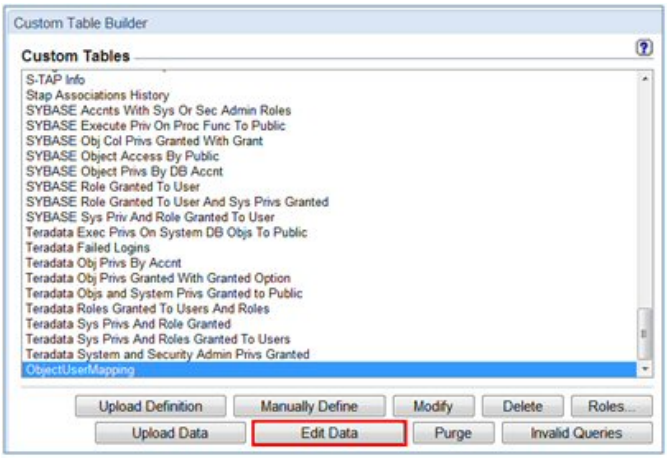
1. Sélectionnez Rapports > Outils de configuration de rapport > Générateur de table personnalisée, puis cliquez sur le bouton **Définition manuelle**.



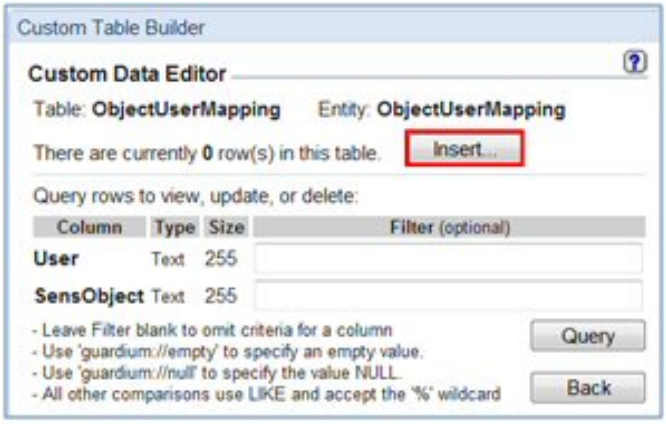
2. Dans l'écran **Générateur de table personnalisée**, définissez la présentation de la table. Assurez-vous que **Type de groupe** correspond à l'élément de données correct dans Guardium. Cliquez sur **Appliquer** et **Précédent** lorsque vous avez terminé.



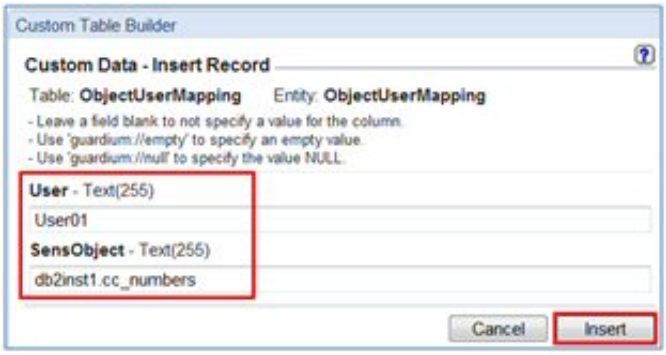
3. Cliquez sur **Editer les données** pour ajouter les enregistrements manuellement. Si vous disposez d'une grande quantité de données, choisissez **Télécharger des données** pour importer les données depuis une source de données externe.



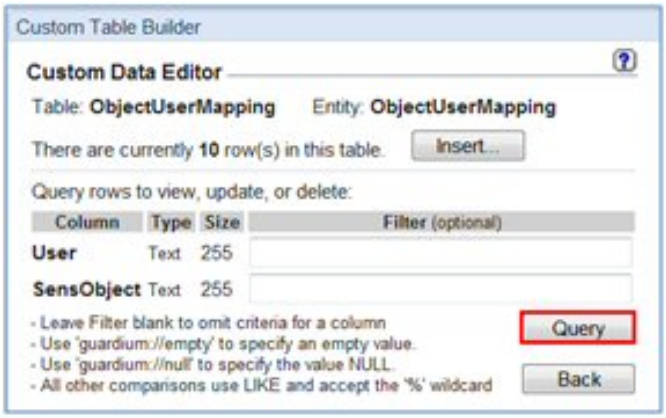
4. Cliquez sur **Insérer**.



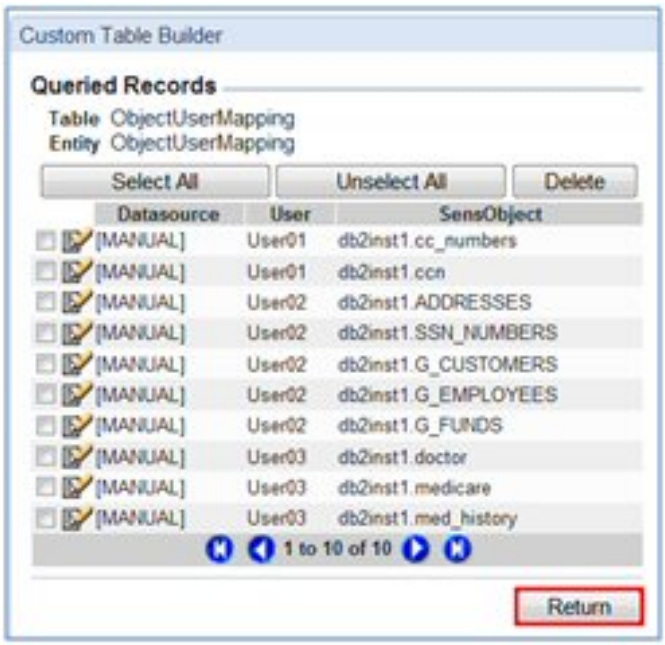
5. Entrez chaque combinaison de valeurs et cliquez sur **Insérer** jusqu'à ce que vous ayez ajouté tous les enregistrements requis.



6. Lorsque vous avez terminé, cliquez sur le bouton **Requête** pour réviser les données.



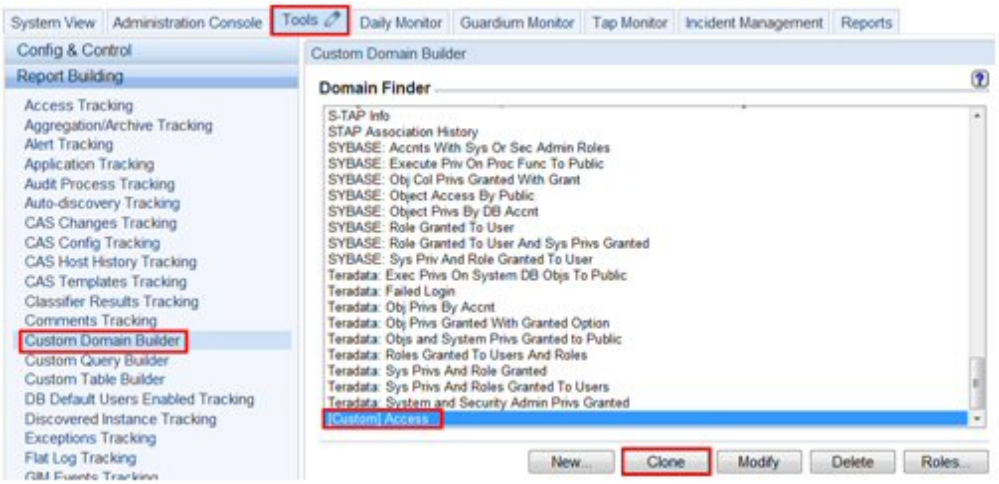
7. Cliquez sur Retour lorsque vous avez terminé.



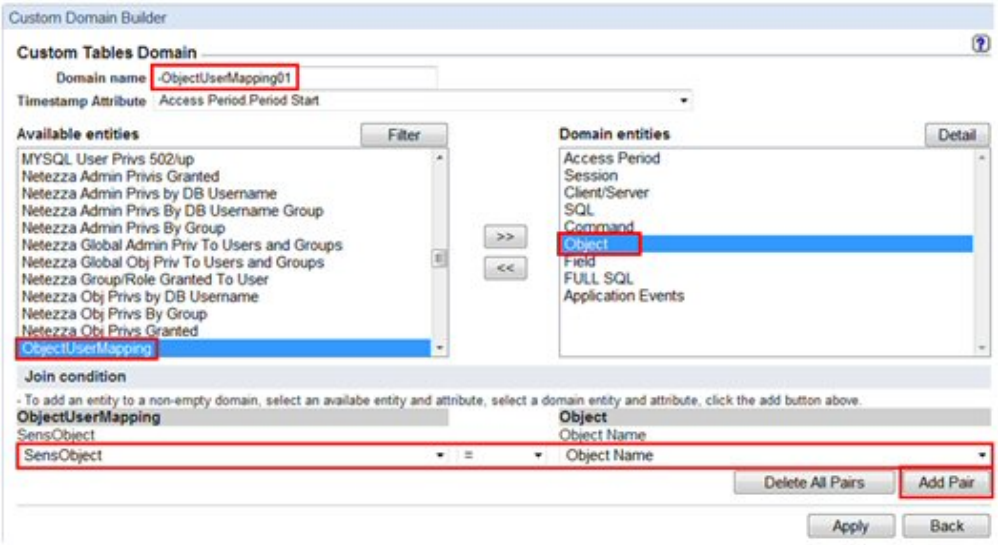
Domaines personnalisés

Ensuite, joignez cette table personnalisée à la structure de table Guardium à l'aide de domaines personnalisés.

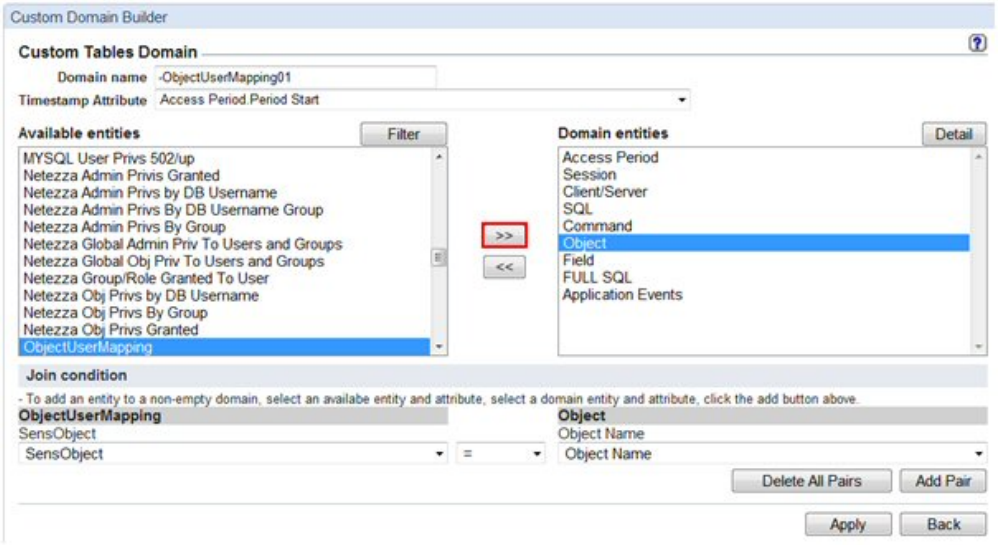
1. Sélectionnez Rapports > Outils de configuration de rapport > Générateur de domaine personnalisé. Mettez en évidence l'*accès [personnalisé]* et cliquez sur **Cloner**.



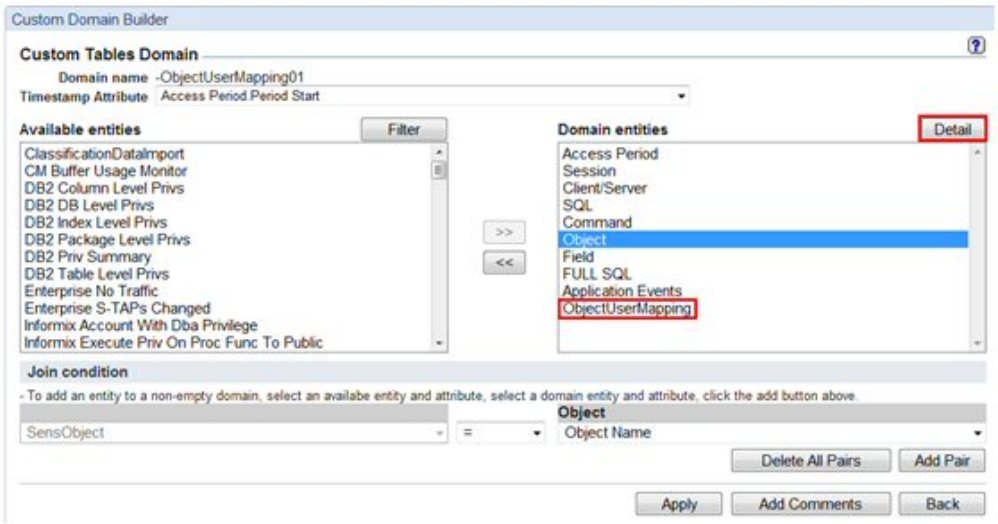
2. Dans le générateur de domaine personnalisé :
   a. Mettez en évidence la nouvelle table créée sous **Entités disponibles**.
   b. Sous **Entités de domaine**, mettez en évidence la table à laquelle vous voulez joindre la table personnalisée.
   c. Sous **Condition de jointure**, choisissez les zones dans chaque table pour laquelle créer la jointure, puis cliquez sur **Ajouter une paire**.



3. Cliquez sur les flèches (>>) pour déplacer la table personnalisée de la liste **Entités disponibles** à la liste **Entités de domaine**.

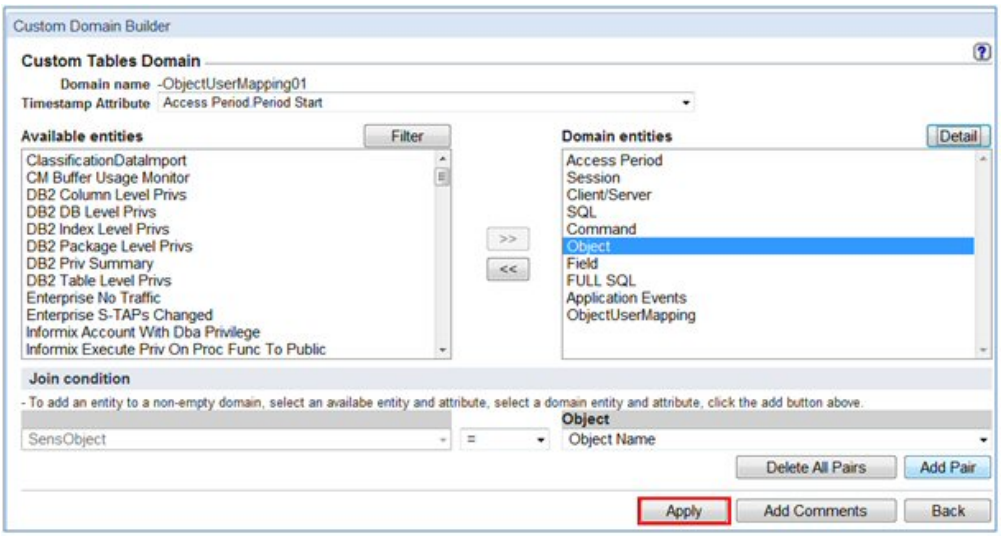


4. Cliquez sur le bouton **Détails** pour réviser les jointures.



5. Vérifiez que les jointures sont correctes, puis cliquez sur **Fermer**.

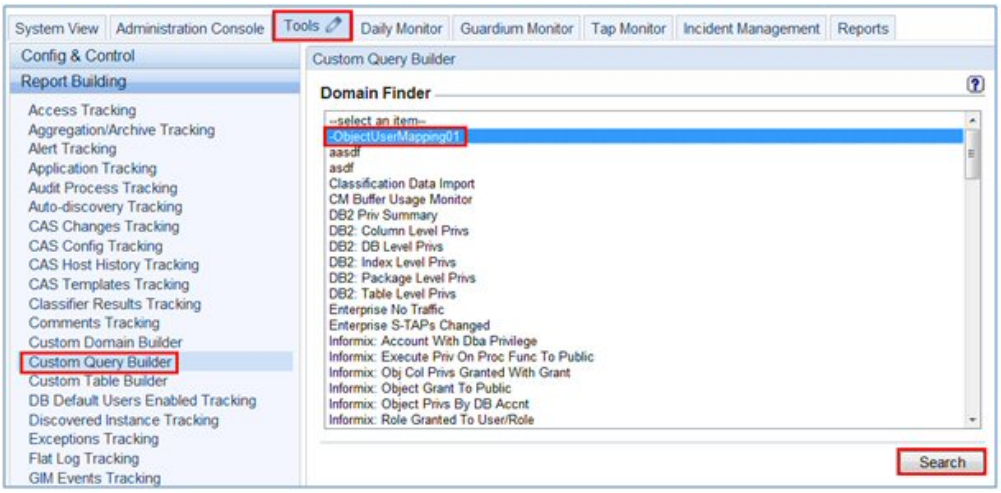
6. Cliquez sur **Appliquer** pour sauvegarder le nouveau domaine personnalisé.



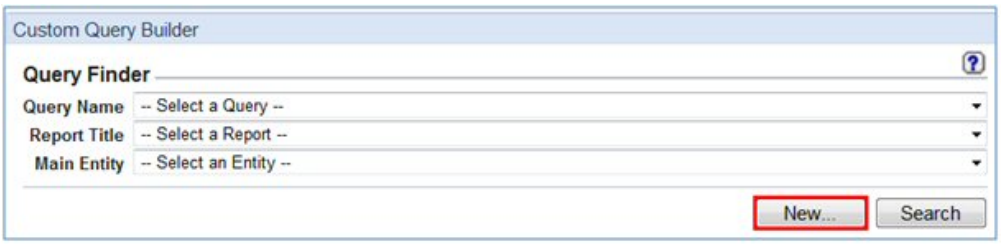
Rapport personnalisé

Ensuite, créez un rapport à distribuer aux utilisateurs.

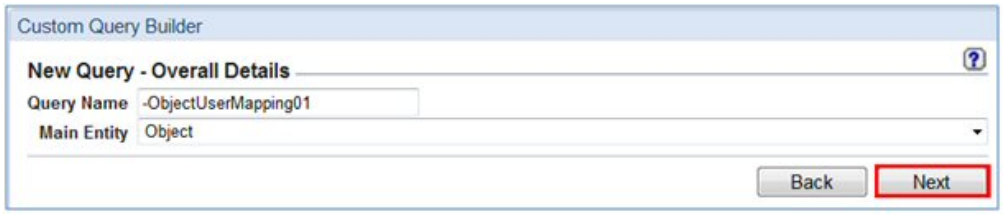
1. Sélectionnez Rapports > Outils de configuration de rapport > Générateur de rapport, puis sélectionnez le nouveau domaine dans le menu déroulant Localiseur de domaine.



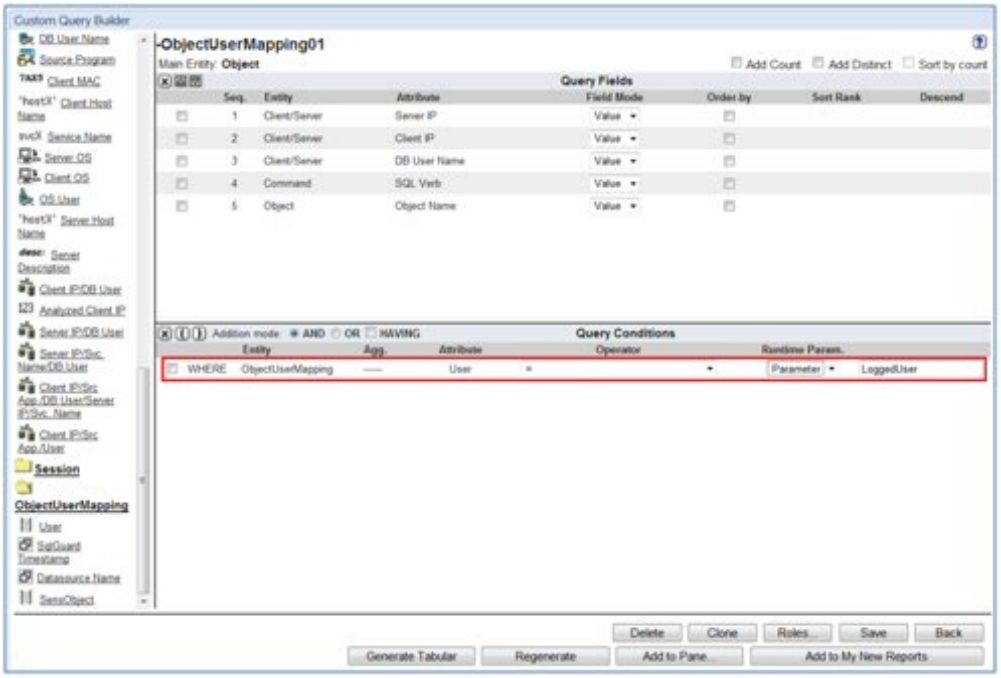
2. Cliquez sur **Nouveau**.



3. Entrez un **nom de requête** et une **entité principale**, puis cliquez sur **Suivant**.



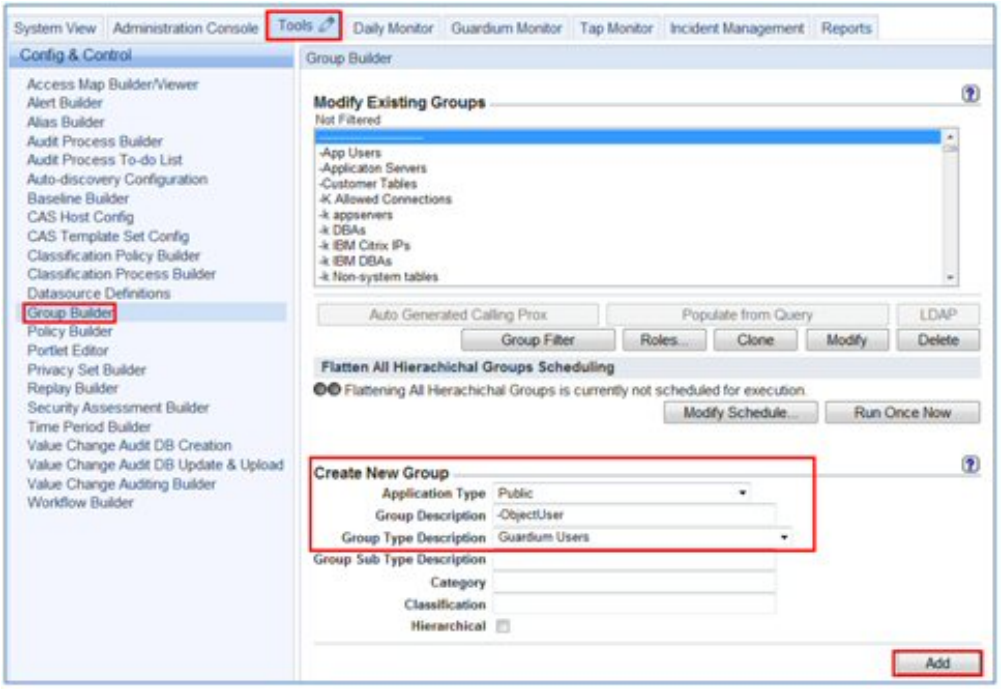
4. Créez un rapport avec un paramètre d'exécution pour la zone d'utilisateur créée dans la table personnalisée.



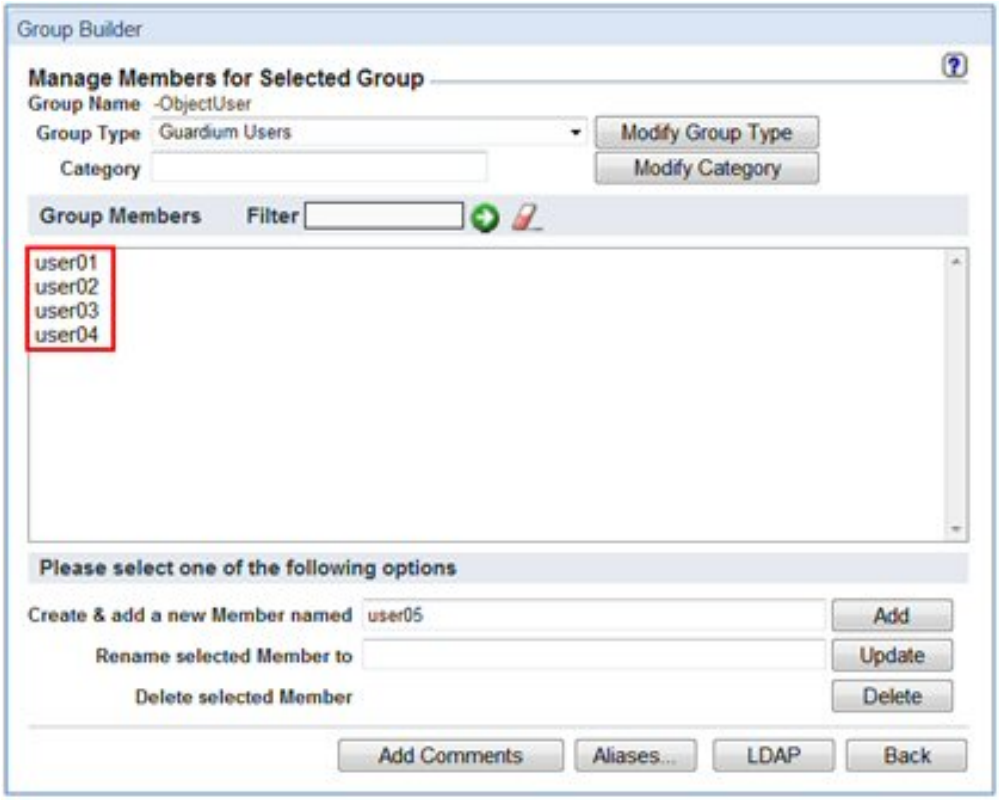
Groupe d'utilisateurs

Créez un groupe d'"utilisateurs Guardium" en fonction de la table personnalisée.

1. Sélectionnez Configuration > Outils et vues > Générateur de groupe et créez un groupe en indiquant **Utilisateurs Guardium** comme **type de groupe**.

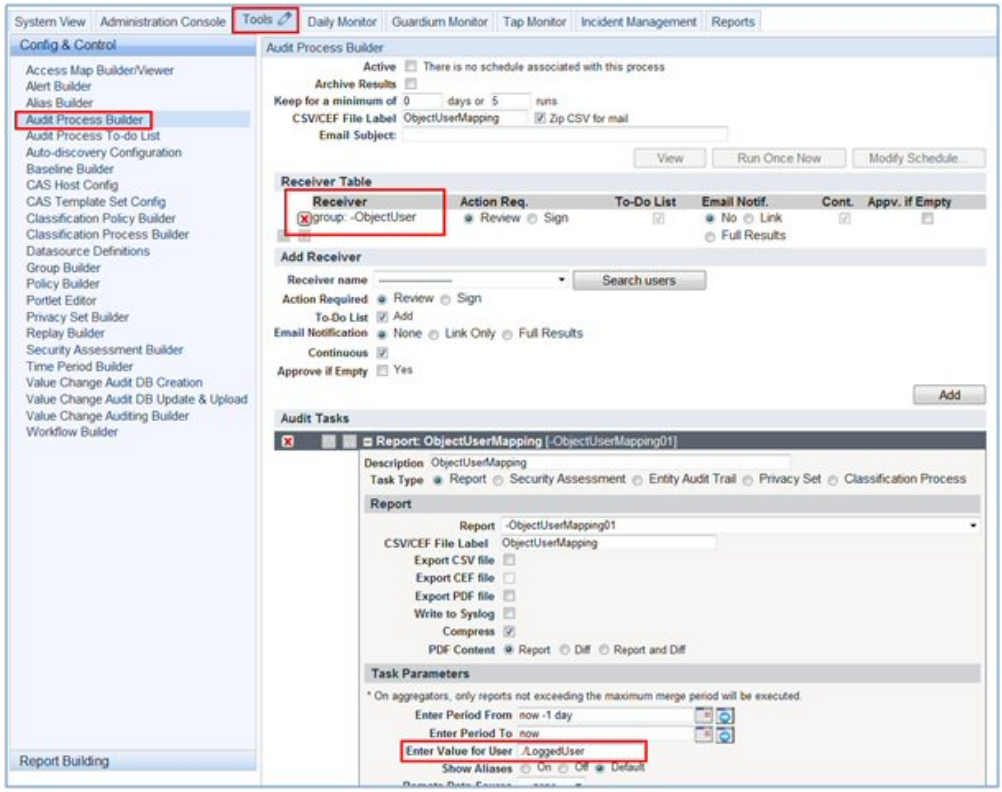


2. Ajoutez tous les utilisateurs depuis la table personnalisée.



Processus d'audit

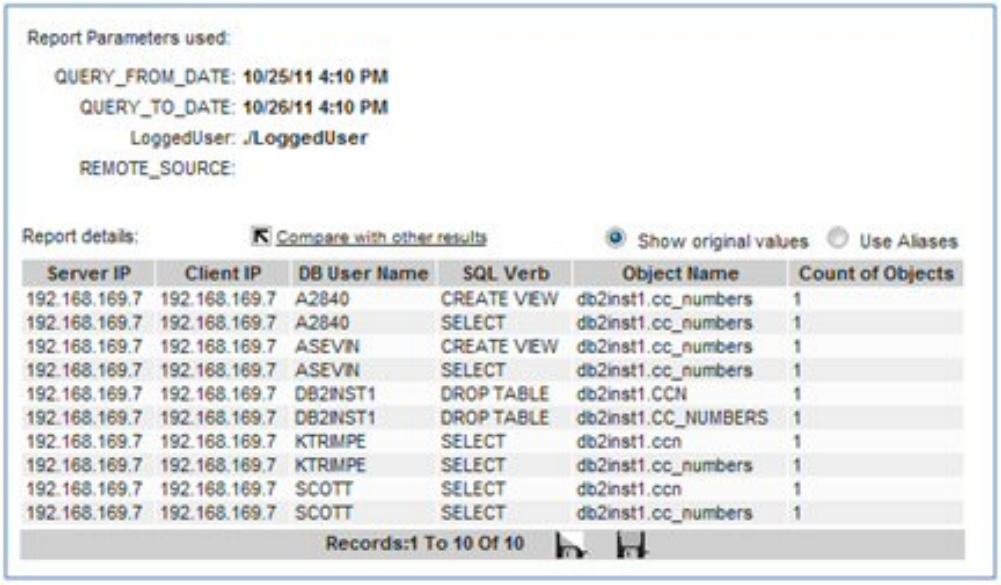
1. Créez un processus d'audit.
2. Pour **Récepteur**, choisissez le groupe que vous avez créé dans Groupe d'utilisateurs.
3. Choisissez le rapport personnalisé que vous avez créé à l'étape 4 comme tâche.
4. Dans le paramètre d'exécution, entrez la balise spéciale “./LoggedUser”. Ainsi, les résultats seront distribués en fonction du mappage personnalisé.
5. Cliquez sur **Exécuter une fois maintenant** pour exécuter le processus d'audit.



Une fois le processus d'audit terminé, chaque récepteur reçoit un ensemble de résultats différent conformément au mappage :

Utilisateurs

Utilisateur01



Report Parameters used:

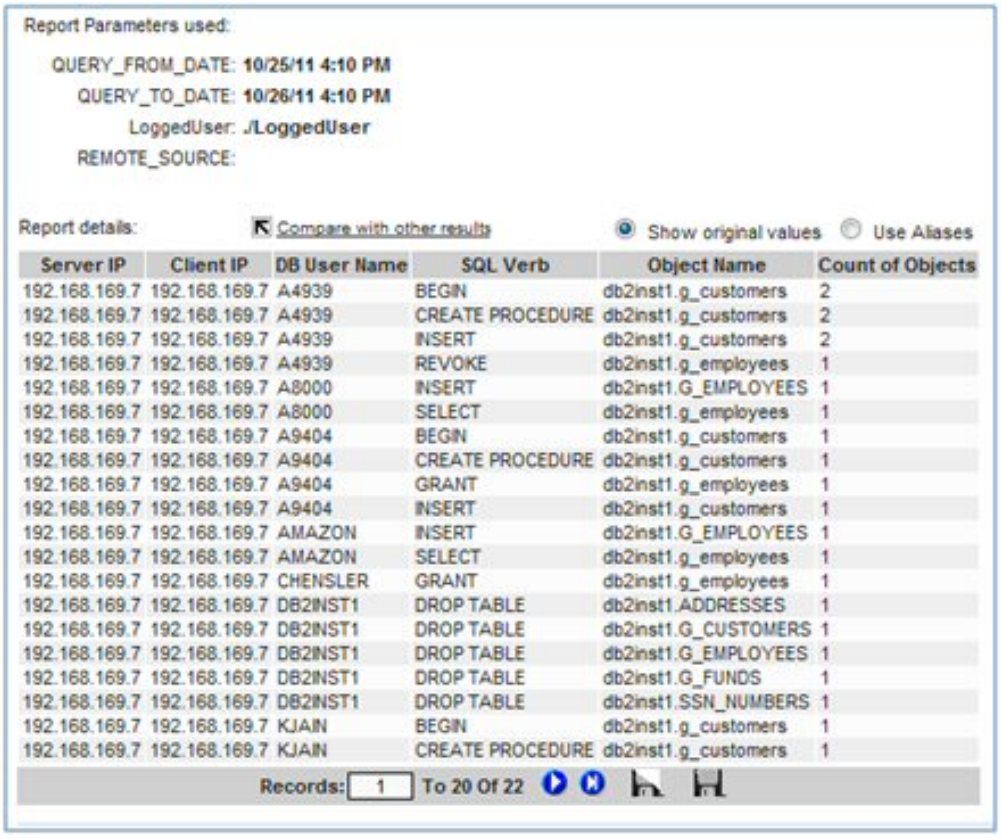
QUERY_FROM_DATE: 10/25/11 4:10 PM
QUERY_TO_DATE: 10/26/11 4:10 PM
LoggedUser: ./LoggedUser
REMOTE_SOURCE:

Report details: Compare with other results — Show original values — Use Aliases

Server IP	Client IP	DB User Name	SQL Verb	Object Name	Count of Objects
192.168.169.7	192.168.169.7	A2840	CREATE VIEW	db2inst1.cc_numbers	1
192.168.169.7	192.168.169.7	A2840	SELECT	db2inst1.cc_numbers	1
192.168.169.7	192.168.169.7	ASEVIN	CREATE VIEW	db2inst1.cc_numbers	1
192.168.169.7	192.168.169.7	ASEVIN	SELECT	db2inst1.cc_numbers	1
192.168.169.7	192.168.169.7	DB2INST1	DROP TABLE	db2inst1.CCN	1
192.168.169.7	192.168.169.7	DB2INST1	DROP TABLE	db2inst1.CC_NUMBERS	1
192.168.169.7	192.168.169.7	KTRIMPE	SELECT	db2inst1.ccn	1
192.168.169.7	192.168.169.7	KTRIMPE	SELECT	db2inst1.cc_numbers	1
192.168.169.7	192.168.169.7	SCOTT	SELECT	db2inst1.ccn	1
192.168.169.7	192.168.169.7	SCOTT	SELECT	db2inst1.cc_numbers	1

Records:1 To 10 Of 10

Utilisateur02



Report Parameters used:

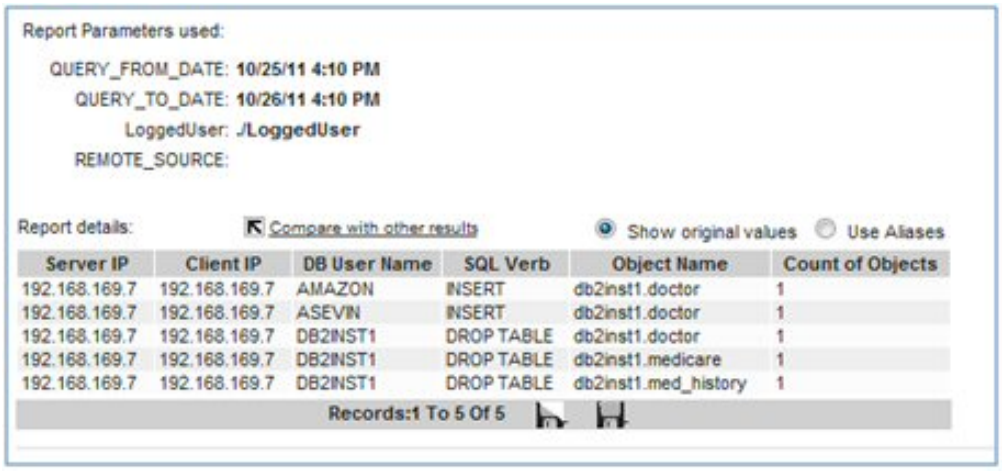
QUERY_FROM_DATE: 10/25/11 4:10 PM
QUERY_TO_DATE: 10/26/11 4:10 PM
LoggedUser: ./LoggedUser
REMOTE_SOURCE:

Report details: Compare with other results — Show original values — Use Aliases

Server IP	Client IP	DB User Name	SQL Verb	Object Name	Count of Objects
192.168.169.7	192.168.169.7	A4939	BEGIN	db2inst1.g_customers	2
192.168.169.7	192.168.169.7	A4939	CREATE PROCEDURE	db2inst1.g_customers	2
192.168.169.7	192.168.169.7	A4939	INSERT	db2inst1.g_customers	2
192.168.169.7	192.168.169.7	A4939	REVOKE	db2inst1.g_employees	1
192.168.169.7	192.168.169.7	A8000	INSERT	db2inst1.G_EMPLOYEES	1
192.168.169.7	192.168.169.7	A8000	SELECT	db2inst1.g_employees	1
192.168.169.7	192.168.169.7	A9404	BEGIN	db2inst1.g_customers	1
192.168.169.7	192.168.169.7	A9404	CREATE PROCEDURE	db2inst1.g_customers	1
192.168.169.7	192.168.169.7	A9404	GRANT	db2inst1.g_employees	1
192.168.169.7	192.168.169.7	A9404	INSERT	db2inst1.g_customers	1
192.168.169.7	192.168.169.7	AMAZON	INSERT	db2inst1.G_EMPLOYEES	1
192.168.169.7	192.168.169.7	AMAZON	SELECT	db2inst1.g_employees	1
192.168.169.7	192.168.169.7	CHENSLER	GRANT	db2inst1.g_employees	1
192.168.169.7	192.168.169.7	DB2INST1	DROP TABLE	db2inst1.ADDRESSES	1
192.168.169.7	192.168.169.7	DB2INST1	DROP TABLE	db2inst1.G_CUSTOMERS	1
192.168.169.7	192.168.169.7	DB2INST1	DROP TABLE	db2inst1.G_EMPLOYEES	1
192.168.169.7	192.168.169.7	DB2INST1	DROP TABLE	db2inst1.G_FUNDS	1
192.168.169.7	192.168.169.7	DB2INST1	DROP TABLE	db2inst1.SSN_NUMBERS	1
192.168.169.7	192.168.169.7	KJAIN	BEGIN	db2inst1.g_customers	1
192.168.169.7	192.168.169.7	KJAIN	CREATE PROCEDURE	db2inst1.g_customers	1

Records: 1 To 20 Of 22

Utilisateur03



Rubrique parent : Construction de processus d'audit

Liste des tâches du processus d'audit

Cette rubrique décrit la Liste des tâches du processus d'audit et les étapes requises pour l'ouvrir et l'utiliser.

Plusieurs techniques permettent d'ouvrir la Liste des tâches du processus d'audit :

- Cliquez sur l'icône dans la bannière de page.
- Suivez le trajet Conformité > Outils et vues > Liste des tâches du processus d'audit.
- Si vous avez reçu une notification par e-mail, cliquez sur le lien Liste des tâches pour ouvrir votre liste de tâches. Vous pouvez aussi cliquer sur le lien du rapport pour ouvrir les résultats. Dans les deux cas, pour que le lien fonctionne, vous devez ouvrir votre e-mail depuis un endroit où le système Guardium est accessible.

Les étapes suivantes décrivent comment utiliser la Liste des tâches du processus d'audit :

1. Sélectionnez l'utilisateur dont vous souhaitez ouvrir la liste de tâches. A cet effet, ouvrez le menu déroulant ou cliquez sur Rechercher des utilisateurs. Si la liste est vide, vous en serez informé.
2. En tant qu'administrateur, vous pouvez effectuer n'importe quelle action sur toute entrée de la liste des tâches. Chaque action est consignée et l'enregistrement du journal indique alors que l'action a été entreprise pour le compte de l'utilisateur par l'administrateur.
3. Les choix disponibles pour chaque entrée de la liste des tâches sont Afficher, Télécharger au format PDF et Valider les résultats affichés.

   La sélection de contenus PDF est la suivante : Rapport (résultats du moment), Diff. (différence entre un rapport précédent et un nouveau rapport) et Rapport et diff. (les deux).

   Remarque : La sélection de contenus PDF s'applique tant aux pièces jointes PDF qu'aux fichiers exportés au format PDF. Le rapport Diff. s'applique uniquement APRÈS la première exécution de cette tâche.(De toute évidence, il n'est pas possible d'établir de comparaison avec des résultats précédents qui n'existent pas encore.) Le nombre maximum de lignes comparables en une seule fois est de 5000. Si le nombre de lignes de résultats dépasse cette limite, le message `comparer les 5000 premières lignes uniquement` apparaîtra dans le résultat de la comparaison.
4. Cliquez sur l'icône d'actualisation de l'ensemble (flèche en cercle).

Remarque : Pour envoyer les fichiers sur un serveur externe sans envoyer d'e-mail et sans ajouter les résultats à la liste des tâches, définissez un processus d'audit sans récepteurs. Pensez aussi à décocher la case Liste des tâches dans la section Ajout de récepteur et à retirer les éventuels récepteurs de la section Récepteurs afin que les résultats ne soient pas ajoutés à leur liste de tâches.

Listes des tâches et Sécurité au niveau données

La liste des tâches comporte un menu déroulant qui permet à son utilisateur de voir la liste des tâches des autres utilisateurs. Contrairement aux utilisateurs titulaires du rôle d'administrateur, les utilisateurs standard ont un menu dans lequel figurent UNIQUEMENT les utilisateurs qui leur sont inférieurs dans la hiérarchie DLS (Data Level Security, sécurité au niveau données). Si toutefois un utilisateur a le rôle 'exempt' (exempté), tous les utilisateurs sont visibles dans son menu déroulant. Les titulaires du rôle d'administrateur peuvent aussi voir tous les utilisateurs dans leur menu.

Lorsqu'un utilisateur accède aux résultats d'un autre utilisateur, les données présentées dans le rapport sont filtrées en fonction de la Sécurité au niveau données (DLS) et du rôle de l'utilisateur sélectionné (par exemple, dans le cas d'un flux de travail personnalisé, les données sont filtrées d'après le rôle de l'utilisateur sélectionné et du statut défini pour ce rôle).

Si un utilisateur titulaire du rôle d'administrateur accède au résultat d'un utilisateur qui lui est INFÉRIEUR dans la hiérarchie, le comportement est tel qu'expliqué dans le paragraphe précédent. S'il accède au résultat d'un utilisateur qui ne lui est PAS inférieur dans la hiérarchie, la visibilité des données est déterminée par la Sécurité au niveau données (DLS) de l'administrateur, pour tous les rôles.

Lorsqu'un résultat est ajouté à la liste des tâches d'un utilisateur en raison d'un changement d'état d'un événement, si ce résultat ne figurait pas déjà dans sa liste, un e-mail est envoyé à cet utilisateur. L'e-mail ne contient pas de PDF, mais seulement une notification et un lien.

Si un utilisateur accède à la liste des tâches d'un autre utilisateur, un message lui indique quel utilisateur détermine le filtrage DLS.

Rubrique parent : Construction de processus d'audit

Audits et rapports

Guardium organise les données qu'il collecte en un ensemble de domaines. Chaque domaine contient un type différent d'informations concernant un domaine de préoccupation : accès aux données, exceptions, violations de politique, etc.

Tous les domaines et leur contenu sont décrits dans les annexes Domaines, Entités et Attributs.

Il y a un générateur de requêtes par domaine, l'accès à chacun étant contrôlé par des rôles de sécurité. Quel que soit le domaine, le même outil générateur de requêtes est utilisé pour créer tous les requêtes. Pour des instructions détaillées sur la manière de construire des requêtes, consultez Requêtes.

Si les domaines standard ne suffisent pas, les utilisateurs peuvent définir leurs propres domaines et les télécharger vers le dispositif Guardium. Par exemple, votre société pourrait créer une table mettant en relation des noms d'utilisateur de base de données génériques (tels que (hr23455 ou qa4872) avec de vrais noms de personnes (Paula Smith, John Doe, etc.). Une fois cette table téléchargée, les vrais noms pourraient être affichés dans les rapports Guardium à partir du domaine personnalisé. Pour des informations plus détaillées sur la manière de définir et d'utiliser des domaines personnalisés, consultez Corrélation avec des données externes.

Rubrique parent : Surveillance et audit

Corrélation des données externes

Cette rubrique explique comment créer des tables personnalisées pour les informations d'entreprise qui sont requises en plus des données internes Guardium existantes.

De nombreux clients possèdent des informations intéressantes dans différentes bases de données, dans leur environnement.Il est extrêmement utile pour un rapport d'audit de corréler les informations pertinentes nécessaires afin de rendre ces rapports faciles à comprendre et intéressants.La corrélation des données externes vous permet de créer des tables personnalisées dans le dispositif Guardium pour les informations d'entreprise qui sont nécessaires en plus des données internes Guardium existantes. Vous pouvez effectuer cette opération manuellement dans l'interface graphique ou en vous appuyant sur une table existante sur un serveur de base de données. Ensuite, vous pouvez créer des requêtes et des rapports pour ces informations, de la même façon que si vous utilisiez des données prédéfinies.

Les tables personnalisées, les domaines personnalisés et les requêtes personnalisées sont des concepts distincts.

Par exemple, imaginez qu'il existe une table sur un serveur de base de données qui contient tous les employés, leurs noms d'utilisateur de base de données et le service auquel ils appartiennent (par exemple Développement, Finances, Marketing, Ressources humaines, etc.).Si vous téléchargez cette table et toutes ses données, vous pouvez la croiser avec les tables internes de Guardium pour déterminer, par exemple, quels sont les employés du service Marketing qui accèdent à la base de données Finances (ce qui peut constituer une activité suspecte).

Pour accéder à l'aide du magasin de données, cliquez sur Magasin de données.

Tables personnalisées

Une table personnalisée contient un ou plusieurs attributs que vous voulez mettre à disposition sur le dispositif Guardium. Par exemple, vous pouvez avoir une table de base de données qui met en correspondance des noms d'utilisateurs codés avec les noms réels. Dans le trafic réseau, seuls les noms codés seront visibles. En définissant une table personnalisées sur le dispositif Guardium et en téléchargeant des données pour cette table depuis la table existante, vous pourrez mettre en correspondance les noms codés et les noms réels.

Avant de définir une table personnalisée, vérifiez que le type des données dont vous avez besoin dans la base de données existante est pris en charge. Un type de données est pris en charge s'il est admis comme l'un des types SQL suivants par le pilote JDBC sous-jacent : INTEGER, BIGINT, SMALLINT, TINYINT, BIT, BOOLEAN, DECIMAL, DOUBLE, FLOAT, NUMERIC, REAL, CHAR, VARCHAR, DATE, TIME, TIMESTAMP. Le tableau ci-dessous présente certains des types de données pris en charge et non pris en charge pour le téléchargement dans une table personnalisée.

Types de données pris en charge et non pris en charge pour les tables personnalisées

Servez-vous de ce tableau pour déterminer quels sont les types de données pris en charge et non pris en charge pour des bases de données spécifiques.

Tableau 1. Types de données pris en charge et non pris en charge pour les tables personnalisées

Bases de données	Types de données pris en charge	Types de données non pris en charge
Oracle	float number char varchar2 date nchar nvarchar2	long clob raw nclob longraw bfile rowid urowid blob
DB2	char varchar bigint integer smallint real double decimal date time timestamp	blob clob longvarchar datalink
Sybase	char nchar varchar nvarchar int smallint tinyint datetime smalldatetime	text binary varbinary image timestamp
MS SQL	bigint bit char datetime decimal float int money nchar numeric nvarchar real smalldatetime smallint tinyint smallmoney varchar unique identifier	text
Informix	char nchar integer smallint decimal smallfloat float serial date money varchar nvarchar datetime	text
MY SQL	bigint decimal int mediumint smallint tinyint double float date datetime timestamp time year char binary enum set	longtext tinyblob tinytext blob text mediumblob mediumtext longblob longtext

Remarque : Une valeur d'objet blob (même de 1 K) peut être capturée dans une instruction SQL dynamique, mais pas dans une instruction SQL statique.

Archivage et restauration d'une table personnalisée

L'écran Générateur de table personnalisée comporte le bouton Purger/Archiver.

L'écran Purge des données de table personnalisée comporte une case à cocher Archiver. Si vous la sélectionnez, les données de la table personnalisée seront incluses dans l'archive de données standard.

Ces données de table personnalisée sont archivées en fonction de la date figurant dans la colonne SQLGUARD_TIMESTAMP de la table personnalisée.

Les données de la table personnalisée peuvent être archivées depuis un collecteur ou un agrégateur.

Les données de la table personnalisée archivées depuis un collecteur peuvent être restaurées sur n'importe quel collecteur ou agrégateur géré par une même instance de Central Manager comme collecteur source (les métadonnées doivent être présentes).

Les données de la table personnalisée archivées depuis un agrégateur peuvent être restaurées sur n'importe quel agrégateur géré par une même instance de Central Manager comme agrégateur source.

Si le fichier archive à restaurer sur un système Guardium n'inclut pas les métadonnées, les données de la table personnalisée ne sont pas restaurées.

Si la structure de la table personnalisée change entre le moment de l'archivage et le moment de la restauration (par exemple, colonnes retirées ou type changé) et qu'une erreur SQL est générée en conséquence, un message d'avertissement apparaît dans le rapport d'activité d'agrégation/archivage et les données ne sont pas restaurées.

Si une table personnalisée doit être purgée par le processus de purge par défaut, les données restaurées sont conservées pendant le nombre de jours spécifié dans l'écran de restauration.

Si la table personnalisée doit écraser les données lors de leur téléchargement, les données restaurées ne sont pas supprimées lors du téléchargement.

Domaines personnalisés

Un domaine personnalisé contient une ou plusieurs tables personnalisées. S'il contient plusieurs tables, vous définissez les relations entre les tables lorsque vous définissez le domaine personnalisé.

Requêtes personnalisées

Une requête personnalisée accède aux données d'un domaine personnalisé. Vous utilisez le générateur de requête personnalisée afin de créer des requêtes pour des domaines personnalisés. Ensuite, vous pouvez utiliser les requêtes personnalisées comme toute autre requête afin de générer des rapports ou des tâches d'audit, de remplir des groupes ou de définir des alias.

Rapports sur les autorisations de base de données

Les rapports sur les autorisations de base de données utilisent la fonction Domaine personnalisé pour créer des liens entre les données externes dans la base de données sélectionnée et les données internes des rapports prédéfinis sur les autorisations. Voir la section Liaison de données externes à des données internes à ce sujet. Voir Rapport sur les autorisations de base de données pour plus d'informations sur l'utilisation de rapports prédéfinis sur les autorisations de base de données. Pour consulter les rapports sur les autorisations, connectez-vous au portail utilisateur et accédez à l'onglet Autorisations de base de données.

Création d'une table personnalisée

Ouvrez le générateur de table personnalisée en sélectionnant l'une des séries d'options suivantes :

- Conformité > Génération de rapports personnalisés > Générateur de table personnalisée
- Rapports > Outils de configuration de rapport > Générateur de table personnalisée

Téléchargement d'une définition de table

Vous pouvez créer une table personnalisée en téléchargeant une définition de table en accédant à ses métadonnées depuis le serveur de base de données sur lequel elles sont définies.

Remarque : Les tables personnalisées téléchargées dans Guardium sont des composants facultatifs activés par la clé de produit. Si ces composants n'ont pas été activés, les choix de table personnalisée répertoriés n'apparaissent pas dans la sélection du générateur de table personnalisée.

1. Ouvrez le générateur de table personnalisée.
2. Cliquez sur Télécharger la définition pour ouvrir le panneau Importer la structure de table. Il n'est pas nécessaire de sélectionner un élément.
3. Entrez une description pour la table dans le champ Description d'entité. Il s'agit du nom que vous utiliserez pour référencer la table lors de la création d'une requête personnalisée.
4. Entrez le nom de table de base de données pour la table dans le champ Nom de table. Il s'agit du nom que vous utiliserez pour créer la table dans la base de données locale.
5. Entrez une instruction SQL valide pour la table dans le champ Instruction SQL. La structure de l'ensemble de résultats renvoyé par l'instruction SQL doit être identique à celle de la table personnalisée définie. Par exemple, si la table personnalisée contient toutes les colonnes de la table appelée my_table, entrez select * from my_table.
   Remarque :

   N'incluez pas de caractère de retour à la ligne dans l'instruction SQL. Toutes les colonnes doivent être nommées explicitement ; utilisez un alias de colonne si nécessaire.

6. Cliquez sur Ajouter une source de données pour ouvrir le localiseur de source de données dans une fenêtre distincte. Ainsi, vous pourrez localiser la base de données externe et identifier les données d'identification nécessaires pour extraire la définition de table et le contenu ultérieurement au cours du processus.
7. Utilisez le localiseur de source de données pour identifier la base de données depuis laquelle la définition de table sera téléchargée.
8. Cliquez sur Extraire pour télécharger la définition de table. Cette action exécute l'instruction SQL et extrait la structure de table. La demande SQL est envoyée à la base de données externe à partir du système Guardium. Gardez à l'esprit que seule la définition est téléchargée et que vous pouvez télécharger les données ultérieurement.

Définition manuelle d'une définition de table

1. Ouvrez le générateur de table personnalisée.
2. Cliquez sur Définition manuelle pour ouvrir le panneau Définir une entité.
3. Entrez une description pour la table dans le champ Description d'entité. Il s'agit du nom que vous utiliserez pour référencer la table lors de la création d'une requête personnalisée.Les caractères spéciaux `\$|&;'`"` ne sont pas admis dans la description de l'entité.
4. Entrez le nom de la table de base de données pour la table dans le champ Nom de table. Il s'agit du nom que vous utiliserez pour créer la table dans la base de données locale.
5. Pour chaque colonne de la table à définir :
   - Entrez un nom dans la zone Nom de la colonne. Ce sera le nom de la colonne dans la table de base de données.
   - Entrez un nom dans la zone Nom d'affichage. Il s'agit du nom que vous utiliserez pour référencer l'attribut dans le générateur de domaine personnalisé et le générateur de requête personnalisée.
   - Sélectionnez un type de données (Texte, Date, Entier, Flottant ou Horodatage).
   - Pour un attribut de type Texte, entrez le nombre maximal de caractères dans la zone Taille. (Celle-ci n'est pas disponible pour les autres types de données.)
   - Si le caractère unique doit être appliqué dans la colonne, cochez la case Unique.
   - Si l'attribut que vous définissez correspond à un type de groupe, sélectionnez ce type de groupe dans la liste Type de groupe.
   - Cliquez sur Ajouter pour ajouter la colonne.
6. Utilisez la liste déroulante Clé d'entité pour identifier la colonne qui sera utilisée comme clé d'entité. La clé d'entité est utilisée dans le générateur de requête lors de la sélection du nombre.

7. Si vous apportez d'autres modifications après avoir cliqué sur le bouton Ajouter, par exemple si vous supprimez une colonne ou changez un attribut, cliquez sur Appliquer pour sauvegarder les modifications.
8. Cliquez sur Terminé une fois que vous avez ajouté toutes les colonnes pour la table.

Modification d'une définition de table

Si vous modifiez la définition d'une table personnalisée, vous risquez d'invalider les rapports existants reposant sur des requêtes qui utilisent cette table. Par exemple, une requête existante peut référencer un attribut qui a été supprimé ou dont le type de données a été changé. Lorsque vous apportez des modifications à une table personnalisée, si des requêtes ont été générées à l'aide d'attributs provenant de cette table, les requêtes sont affichées dans le panneau Liste de requêtes. Remarque : vous pouvez aussi utiliser l'option Modifier pour afficher et valider les structures de table qui ont été importées.

1. Ouvrez le générateur de table personnalisée.
2. Choisissez une table personnalisée en cliquant sur le libellé d'entité et en le mettant en évidence.
3. Cliquez sur Modifier pour ouvrir le panneau Modifier une entité.
4. Voir la section relative à la définition manuelle d'une table pour de l'aide.
5. Lorsque vous apportez des modifications à une table personnalisée, si des requêtes ont été invalidées suite à la modification d'un attribut provenant de cette table, les requêtes sont affichées dans le panneau Liste de requêtes. Utilisez ce dernier pour choisir et changer des requêtes. Il n'est pas nécessaire d'apporter toutes les modifications immédiatement car vous pouvez revenir dans ce panneau ultérieurement et utiliser l'option Requêtes non valides.

Requêtes non valides

Si vous modifiez la définition d'une table personnalisée, vous risquez d'invalider les rapports existants reposant sur des requêtes qui utilisent cette table. Par exemple, une requête existante peut référencer un attribut qui a été supprimé ou dont le type de données a été changé. Il est judicieux de rechercher les éventuelles requêtes non valides après avoir modifié la table.

1. Ouvrez le générateur de table personnalisée.
2. Cliquez sur Requêtes non valides.
3. Les requêtes sont affichées dans le panneau Liste de requêtes. Utilisez ce dernier pour choisir et changer des requêtes.

Purge des données d'une table personnalisée

Les données peuvent être purgées depuis des tables personnalisées sur le serveur Guardium à la demande, ou selon un planning.

1. Ouvrez le générateur de table personnalisée.
2. Choisissez une table personnalisée en cliquant sur son nom et en le mettant en évidence.
3. Cliquez sur Purger pour ouvrir le panneau Purge des données de table personnalisée.
4. Cliquez sur Purger tout pour procéder à la purge maintenant.
   Remarque : L'option de purge Exécuter une fois maintenant vérifie le paramètre de conservation dans la table RESTORED_DATA. L'option Purger tout permet de purger tous les enregistrements supprimés sans vérifier le paramètre de conservation.
5. Dans le panneau de configuration, entrez l'ancienneté des données à purger, c'est-à-dire le nombre de jours, de semaines ou de mois avant la date de l'opération de purge.
6. Cliquez sur Exécuter une fois maintenant pour exécuter une opération de purge planifiée une fois.
7. Cliquez sur Modifier la planification pour ouvrir le panneau Définition de planification standard et planifier une opération de purge.
8. Cliquez sur Terminé pour fermer le panneau.

Téléchargement de données dans une table personnalisée

1. Ouvrez le générateur de table personnalisée.
2. Choisissez une table personnalisée en cliquant sur son nom et en le mettant en évidence.
3. Cliquez sur Télécharger des données pour ouvrir le panneau Importation de données.
4. Dans la zone Instruction SQL, entrez une instruction SQL valide pour la table. La structure de l'ensemble de résultats renvoyé par l'instruction SQL doit être identique à celle de la table personnalisée définie. Par exemple, si la table personnalisée contient toutes les colonnes de la table appelée my_table, entrez `select * from my_table`. Les champs suivants, qui sont internes à Guardium, peuvent être utilisés dans des instructions SQL :
   - ^FromDate?^ et ^ToDate?^, où les valeurs sont égales à la date de téléchargement précédente et à la date de téléchargement en cours, respectivement.
   - ^fromID^ et ^toID^ où, si elles sont utilisées avec le nom de colonne d'ID, les valeurs sont la valeur maximale de la colonne d'ID du téléchargement précédent et la valeur maximale du téléchargement en cours, respectivement.

   Remarque : N'incluez pas de caractère de retour à la ligne dans l'instruction SQL.
5. Si nécessaire, spécifiez un nom de colonne dans Nom de colonne d'ID (depuis la table définie dans la source de données) qui permettra le suivi par ID et qui sera utilisé en conjonction avec les champs Guardium internes ^fromID^ et ^toID^.
6. Dans la commande DML après la zone de téléchargement, entrez une commande DML (ou une instruction SQL de mise à jour ou de suppression) sans point-virgule à exécuter après le téléchargement des données. Remarque : n'incluez pas de caractère de retour à la ligne dans l'instruction SQL.
7. Cochez la case Ecraser par téléchargement si vous voulez purger les données dans la table personnalisée avant le téléchargement. Cochez la case Ecraser par source de données si vous voulez purger les données pour cette source de données avant de les télécharger.
8. Sélectionnez le bouton de purge par défaut (dans l'écran Téléchargement de données personnalisées) pour qu'il fasse partie de l'objet de purge Travail de purge de la table personnalisée par défaut dont l'ancienneté par défaut initiale est de 60 jours. Afin d'ajouter une planification de purge pour cette table, accédez à la page Générateur de table personnalisée initiale, sélectionnez une table personnalisée et cliquez sur Purger pour ouvrir un écran de configuration Purge des données de table personnalisée.
9. Cochez la case Utiliser la planification par défaut si vous téléchargez des tables de versions précédentes de Guardium. Cette case à cocher apparaît uniquement dans les vues Central Manager et seulement pour les tables personnalisées prédéfinies Surveillance de l'utilisation de la mémoire tampon CM, Aucun trafic pour l'entreprise, S-TAP Changes et Informations S-TAP.
10. Cliquez sur Ajouter une source de données pour ouvrir le localiseur de source de données dans une fenêtre distincte. Utilisez cette fenêtre pour identifier une ou plusieurs bases de données depuis lesquelles télécharger les données de table. Vous pouvez ajouter plusieurs sources de données afin d'effectuer un téléchargement depuis plusieurs sources. Remarque : la page Importation de données pour les instances de Central Manager comporte la case à cocher Inclure la source par défaut. Si elle est sélectionnée, l'opération de téléchargement des données effectue une itération sur toutes les unités gérées enregistrées en ligne. Remarque : lorsque vous ajoutez une source de données, vous ne pouvez pas planifier l'exécution de l'application sans spécifier le nom d'utilisateur et le mot de passe pour la source de données sélectionnée.
11. Vous pouvez cliquer sur Vérifier/Réparer pour comparer le schéma de la table personnalisée au schéma des métadonnées. Pour les environnements de gestion centralisée : dans un environnement de gestion centralisée, la définition de table personnalisée se trouve sur le gestionnaire central et la table personnalisée n'existe pas nécessairement dans la base de données (unité gérée) locale. Cliquez sur le bouton Vérifier/Réparer pour vérifier si la table personnalisée existe localement et la créer si tel n'est pas le cas.

12. Cliquez sur Vérifier la source de données pour tester la connexion à la base de données externe. Un écran de confirmation apparaît.
13. Cliquez sur Appliquer.
14. Pour télécharger des données dans cette table personnalisée, effectuez l'une des opérations suivantes :
    - Cliquez sur Exécuter une fois maintenant pour télécharger les données manuellement.
    - Sélectionnez Modifier la planification pour configurer la planification.

Gestion de la table personnalisée

Lorsque vous suivez la procédure de création d'une table personnalisée (détaillée précédemment) et de sélection d'une table personnalisée prédéfinie, cliquez sur Maintenance pour gérer le type de moteur de table et l'index de table. Les types de moteur de table pour les tables personnalisées/les autorisations (InnoDB et MyISAM) apparaissent pour toutes les bases de données personnalisées prédéfinies car les données stockées dans la base de données interne Guardium s'appuient sur MySQL. Les deux types principaux de moteur de stockage de table pour les bases de données MySQL sont InnoDB et MyISAM. Les différences majeures entre ces deux types de moteur de table sont les suivantes :

- InnoDB est plus complexe que MyISAM.
- InnoDB assure une intégrité des données plus stricte que MyISAM.
- InnoDB implémente un verrou au niveau de la ligne pour l'insertion et la mise à jour alors que MyISAM implémente un verrou au niveau de la table.
- InnoDB possède des transactions, au contraire de MyISAM.
- InnoDB possède des clés externes et des contraintes de relation, au contraire de MyISAM.

Remarque : Vous ne pouvez pas changer le type de moteur (la sélection est grisée) si le nombre de lignes dans la table est supérieure à 1M.

Le menu Gérer une table personnalisée contient également l'option Gérer un index de table. Cliquez sur Insérer pour ouvrir la définition d'index de table. L'écran en incrustation suggère l'ajout de colonnes dans la table à des index basés sur les colonnes utilisées dans des domaines personnalisés en tant que conditions de jointure. Sélectionnez les colonnes et procédez à la sauvegarde. Les index seront créés (ou recréés).

Planification de téléchargements de données personnalisés

Une fois qu'une définition de table personnalisée a été créée, les données peuvent être téléchargées dans des tables personnalisées sur le dispositif Guardium selon une planification.

Remarque : Les nouvelles installations ne démarrent pas automatiquement des rapports d'entreprise. Il existe une planification de téléchargement pour chaque table personnalisée. La quantité totale d'espace disque réservée sur le dispositif Guardium pour les tables personnalisées est 4 Go.

1. Ouvrez le générateur de table personnalisée.
2. Choisissez une table personnalisée en cliquant sur le libellé d'entité et en le mettant en évidence.
3. Cliquez sur Télécharger des données pour ouvrir le panneau Importation de données.
4. Sélectionnez la case à cocher Utiliser la planification par défaut pour télécharger cette table en fonction de la planification par défaut. Sinon, cette table personnalisée utilisera sa propre planification de téléchargement des données.
5. Cliquez sur Modifier la planification pour ouvrir le panneau Définition de planification standard et modifier la planification.
6. Cliquez sur Terminé une fois que vous avez fini.

Le téléchargement personnalisé de rapports d'entreprise est similaire à d'autres travaux. Vous pouvez l'activer de deux façons :

- Dans l'interface graphique de téléchargement de table personnalisée (licence requise pour le téléchargement personnalisé).
- En utilisant GuardAPI depuis l'interface de ligne de commande :

```
grdapi add_schedule jobName=CustomTablePurgeJob_CM_SNIFFER_BUFFER_USAGE obGroup=customTableJobGroup Enterprise S-TAPs
Changed: grdapi add_schedule jobName=customTableDataUpload_106 jobGroup=customTableJobGroup CM Buffer Usage Monitor: grdapi
add_schedule jobName=customTableDataUpload_104 jobGroup=customTableJobGroup S-TAP Info: grdapi add_schedule
jobName=customTableDataUpload_80 jobGroup=customTableJobGroup
```

Création d'un domaine personnalisé

Après avoir défini une ou plusieurs tables personnalisées, définissez un domaine personnalisé pour pouvoir effectuer des tâches de requête et de production de rapport en utilisant les données personnalisées. Les informations collectées sont organisées en domaines, qui contiennent chacun un type différent d'informations liées à un sujet spécifique : accès aux données, exceptions, violations de politique, etc. Il existe un outil de génération de requête distinct pour chaque domaine. Les domaines personnalisés admettent les domaines définis par l'utilisateur et peuvent définir toutes les tables de données téléchargées sur le dispositif Guardium. Consultez Domaines personnalisés. Ces domaines d'autorisations (privilèges) personnalisés sont utilisés pour les rapports sur les autorisations que vous pouvez consulter si vous êtes connecté en tant qu'utilisateur. Pour afficher ces rapports, accédez à l'onglet utilisateur Autorisations de base de données.

Remarque : Les domaines d'autorisations de base de données sont des composants facultatifs activés par la clé de produit. Si ces composants n'ont pas été activés, les choix décrits dans la rubrique d'aide Domaines personnalisés n'apparaissent pas dans la sélection du générateur de table personnalisée.

1. Ouvrez le générateur de domaine personnalisé en sélectionnant l'une des séries d'options suivantes :
    - Conformité > Génération de rapports personnalisés > Générateur de domaine personnalisé
    - Rapports > Outils de configuration de rapport > Générateur de domaine personnalisé
    - Configuration > Outils et vues > Générateur de domaine personnalisé
2. Cliquez sur Domaines pour ouvrir le panneau Localiseur de domaine.
3. Cliquez sur Nouveau pour ouvrir le panneau Domaine de tables personnalisées.
4. Entrez un nom de domaine. En général, vous inclurez une table personnalisée unique dans le domaine ; par conséquent, vous pouvez utiliser le même nom pour le domaine.
5. La zone Entités disponibles répertorie toutes les tables personnalisées qui ont été définies (et auxquelles vous avez accès). Sélectionnez une entité. Si vous le souhaitez, cliquez sur l'outil Filtre pour ouvrir Filtre d'entité et entrez une valeur Similaire à afin de ne sélectionner que les entités que vous voulez répertorier, puis cliquez sur Accepter. La fenêtre de filtre se ferme et vous revenez au panneau Domaine de tables personnalisées, qui ne contient plus que les entités qui correspondent à la valeur Similaire à dans la zone Entités disponibles. Sélectionnez l'entité à inclure.
6. Cliquez sur la flèche double >> pour déplacer l'entité sélectionnée de la liste Entités disponibles vers la liste Entités de domaine.
7. Pour ajouter une entité à un domaine comportant déjà une ou plusieurs tables, procédez comme suit. Vous devrez utiliser la condition de jointure pour définir la relation entre les entités.

   Pour chaque entité supplémentaire :

- Depuis la zone Entités de domaine, sélectionnez une entité. Tous les attributs de l'entité sont mis à disposition dans la liste déroulante des champs dans la zone Entités de domaine. Sélectionnez dans la liste l'attribut à utiliser dans l'opération de jointure.
- Dans la liste Entités disponibles, sélectionnez l'entité à ajouter. Tous les attributs de l'entité sont mis à disposition dans la liste déroulante des champs dans la zone Entités disponibles. Sélectionnez dans la liste l'attribut à utiliser dans l'opération de jointure.
- Sélectionnez = (opérateur égal à) si vous voulez que la condition de jointure soit "égal à" (par exemple, domaineA.attributB = domaineC.attributD). Sélectionnez une jointure externe si vous voulez que la condition de jointure soit une jointure externe utilisant les attributs sélectionnés.
- Cliquez sur Ajouter une paire de champs. Vous pouvez utiliser ce bouton pour ajouter d'autres paires d'attributs de ces deux entités à la condition de jointure.
- Répétez les étapes pour toute opération de jointure supplémentaire.

Remarque : Lorsque la sécurité au niveau des données est activée, les entités internes ajoutées au domaine personnalisé ne peuvent pas appartenir à des domaines différents avec des règles de filtrage.

8. Sélectionnez l'attribut Horodatage pour l'entité de domaine personnalisé.
   Remarque : Vous devez utiliser au moins une entité avec un horodatage, car un horodatage est requis pour la sauvegarde d'un domaine personnalisé.
9. Cliquez sur Appliquer.

Modification d'un domaine personnalisé

Le but est de créer une liaison entre des données externes et les données internes.

1. Ouvrez le générateur de domaine personnalisé.
2. Choisissez le domaine personnalisé à cloner.
3. Cliquez sur Modifier pour ouvrir le panneau Domaine de tables personnalisées.
4. Voir la section relative à l'ouverture du générateur de domaine personnalisé et la section relative à la liaison de données externes à des données internes pour de l'aide.
5. Cliquez sur Appliquer pour sauvegarder les modifications.

Retrait d'un domaine personnalisé

1. Ouvrez le générateur de domaine personnalisé.
2. Choisissez le domaine personnalisé à cloner.
3. Cliquez sur Domaines pour ouvrir le panneau Localiseur de domaine.
4. Cliquez sur Supprimer pour retirer le domaine personnalisé.

Clonage d'un domaine personnalisé

1. Ouvrez le générateur de domaine personnalisé.
2. Choisissez la table personnalisée qui se trouve dans le domaine à cloner.
3. Cliquez sur Domaines pour ouvrir le panneau Localiseur de domaine.
4. Cliquez sur Cloner pour ouvrir le panneau Domaine de tables personnalisées.
5. Changez le nom de domaine pour refléter le nouveau domaine.
6. Voir la section relative à l'ouverture du générateur de domaine personnalisé et la section relative à la liaison de données externes à des données internes pour de l'aide.
7. Cliquez sur Appliquer pour sauvegarder les modifications.

Liaison de données externes à des données internes

Le but est de créer une liaison entre des données externes et les données internes.

1. Ouvrez le générateur de domaine personnalisé.
2. Choisissez la table personnalisée contenant vos données externes.
3. Cliquez sur Domaines pour ouvrir le panneau Localiseur de domaine.
4. Cliquez sur Modifier pour ouvrir le panneau Domaine de tables personnalisées.
5. Cliquez sur l'icône Filtre à côté de la liste Entités disponibles.
6. Désélectionnez la case à cocher Personnalisé pour le filtre et si vous le souhaitez, indiquez une condition Similaire à afin de filtrer les noms d'entité et cliquez sur Accepter.
7. Sélectionnez dans la liste Entités disponibles une entité à lier à vos données externes.
8. Sélectionnez le champ qui sera utilisé pour joindre les données à vos données externes.
9. Mettez en évidence la table contenant vos données externes dans la liste Entités de domaine.
10. Sélectionnez le champ qui sera utilisé pour joindre des données aux données internes.
11. Cliquez sur Ajouter une paire de champs pour ajouter la relation.
12. Cliquez sur la flèche double >> pour ajouter la table interne à la liste Entités de domaine.
13. Cliquez sur Appliquer pour sauvegarder les modifications.

Utilisation de requêtes personnalisées

Cette section explique comment ouvrir le générateur de requête personnalisée. Voir la section relative à la génération de requêtes et la section relative à la génération de rapports pour de l'aide lors de la définition d'une requête et de la génération d'un rapport. Utilisez le générateur de requête personnalisée afin de générer des requêtes sur des données provenant de domaines personnalisés, qui contiennent une ou plusieurs tables personnalisées.

1. Ouvrez le générateur de requête personnalisée en sélectionnant Conformité > Génération de rapports personnalisés > Générateur de requête personnalisée.
2. Sélectionnez un domaine personnalisé dans la liste.
3. Cliquez sur Rechercher pour ouvrir le localiseur de requête.
4. Pour afficher, modifier ou cloner une requête existante, sélectionnez-la dans la liste Nom de requête ou sélectionnez un rapport utilisant cette requête dans la liste Titre de rapport.
5. Pour afficher toutes les requêtes définies pour une table personnalisée spécifique, sélectionnez cette table personnalisée dans la liste Entité principale et cliquez sur le bouton Rechercher (seules les tables personnalisées incluses dans le domaine personnalisé sélectionné seront répertoriées).

Interface bidirectionnelle vers et depuis InfoSphere Discovery

IBM Guardium et InfoSphere Discovery peuvent identifier et classer les données sensibles, comme les numéros de sécurité sociale ou les numéros de carte de crédit.

Un client du produit IBM Guardium peut utiliser une interface bidirectionnelle pour transférer les données sensibles identifiées d'un produit à l'autre. Ces clients, qui ont déjà investi leur temps dans l'un des produits InfoSphere, peuvent transférer les informations dans l'autre produit InfoSphere.
Remarque : Dans IBM Guardium, le processus de classification est un processus continu qui s'exécute régulièrement. Dans InfoSphere Discovery, la classification fait partie du processus de reconnaissance qui généralement, ne s'exécute qu'une fois.

Les données sont transférées dans des fichiers CSV.

Récapitulatif des procédures d'exportation et d'importation :

- Exportation depuis Guardium - Exécutez le rapport prédéfini (Exporter les données sensibles vers Discovery) et procédez à l'exportation à l'aide d'un fichier CSV.
- Importation dans Guardium - Procédez au chargement dans une table personnalisée de la source de données CSV ; définissez un rapport par défaut pour cette source de données.

Procédez comme suit :

- Exportation depuis Guardium
- Exportez les données de classification depuis IBM Guardium vers InfoSphere Discovery.

1. En tant qu'administrateur dans l'application Guardium, sélectionnez Outils > Générateur de rapport > Suivi des résultats de classificateur > Sélectionner un rapport > Exporter les données sensibles vers Discovery.
   Remarque : Ajoutez ce rapport à la sous-fenêtre de l'interface utilisateur (il n'y figure pas par défaut).
2. Cliquez sur l'icône Personnaliser dans l'écran Résultat du rapport et spécifiez les critères de recherche afin de filtrer les données des résultats de classification à transférer à Discovery.
3. Exécutez le rapport et cliquez sur Télécharger tous les enregistrements.
4. Procédez à la sauvegarde au format CSV et importez ce fichier dans Discovery conformément aux instructions d'InfoSphere Discovery.

Importation dans Guardium

Importez des données de classification depuis InfoSphere Discovery dans IBM Guardium.

1. Exportez les données de classification au format CSV depuis InfoSphere Discovery conformément aux instructions d'InfoSphere Discovery.
2. Ouvrez le générateur de table personnalisée en sélectionnant l'une des séries d'options suivantes :
   - Conformité > Génération de rapports personnalisés > Générateur de table personnalisée
   - Rapports > Outils de configuration de rapport > Générateur de table personnalisée

   Sélectionnez Importation des données de classification et cliquez sur Télécharger des données.
3. Dans l'écran Télécharger des données, cliquez sur Ajouter une source de données, cliquez sur Nouveau, définissez le fichier CSV importé depuis Discovery comme la nouvelle source de données (Type de base de données = Texte).
   Remarque : Vous pouvez aussi charger les données directement depuis la base de données Discovery si vous savez comment accéder à la base de données Discovery et aux données des résultats de classification.
4. Après avoir défini le fichier CSV comme source de données, cliquez sur Ajouter dans l'écran comportant la liste des sources de données.
5. Dans l'écran Télécharger des données, cliquez sur Vérifier la source de données, puis cliquez sur Appliquer.
6. Cliquez sur Exécuter une fois maintenant pour charger les données depuis le fichier CSV.
7. Accédez au générateur de rapport, sélectionnez le rapport Importation des données de classification, cliquez sur Ajouter à la sous-fenêtre pour l'ajouter à votre portail, puis accédez au rapport.
8. Accédez au rapport, cliquez sur Personnaliser pour définir les dates de début et de fin, et exécutez le rapport.

Le résultat du rapport contient les données de classification importées depuis InfoSphere Discovery. Cliquez deux fois pour appeler les API affectées à ce rapport. Les données importées depuis Discovery peuvent être utilisées pour :

- Ajouter une nouvelle source de données en fonction de l'ensemble de résultats.
- Ajouter/Mettre à jour un groupe de données sensibles.
- Ajouter des règles de politique en fonction des détails sur la source de données et les données sensibles.
- Ajouter un jeu de confidentialité.

Signature d'interface CSV

Reportez-vous au tableau pour des exemples de signatures d'interface CSV utilisées pour le transfert bidirectionnel entre IBM Guardium et InfoSphere Discovery.

Tableau 2. Signature d'interface CSV

Signature d'interface	Exemple
Type	DB2
Hôte	9.148.99.99
Port	50001
Nom de base de données (nom de schéma pour DB2 ou Oracle, nom de base de données pour les autres)	cis_schema
URL de la source de données	
Nom de la table	MK_SCHED
Nom de la colonne	ID_PIN
Nom de la classification	SSN
Description de la règle	Algorithme prêt à l'emploi d'InfoSphere Discovery
Taux de réussite	70 % - non disponible pour l'exportation dans Guardium version 8.2
Seuil utilisé	60 % - non disponible pour l'exportation dans Guardium version 8.2

Rubrique parent : Surveillance et audit

Jeux de confidentialité

Un jeu de confidentialité est une collection d'éléments utilisables dans le cadre d'une surveillance spéciale.

Il consiste en une ou plusieurs paires objet-champ. Par exemple, le champ salaire de la table personnel ou tous les champs de la table de l'historique des salaires. Tous les accès à ces éléments au cours d'une période donnée peuvent être rapportés.

Sélectionnez l'une des rubriques suivantes pour apprendre à exécuter l'opération correspondante sur un jeu de confidentialité.

Ouvrir le Générateur de jeu de confidentialité

Pour accéder à la définition d'un jeu de confidentialité, vous devez posséder un compte d'utilisateur Guardium dont le rôle de sécurité est également affecté à cette définition. Les jeux de confidentialité auxquels vous n'avez pas accès ne sont pas visibles dans la liste des jeux de confidentialité qui vous est présentée.

1. Ouvrez le panneau Identification de jeu de confidentialité en utilisant l'un des trajets suivants :
   - Conformité > Outils et vues > Générateur de jeu de confidentialité
   - Reconnaître > Reconnaissance de base de données > Générateur de jeu de confidentialité
2. Effectuez l'une des opérations suivantes :
   - Cliquez sur le bouton Nouveau pour définir un nouveau jeu de confidentialité (voir Créer un jeu de confidentialité).
   - Sélectionnez un jeu de confidentialité dans la liste et cliquez sur l'un des boutons suivants :
     - Cloner - Voir Cloner un jeu de confidentialité.
     - Modifier - Utilisez ce bouton pour modifier la définition ou pour exécuter un rapport basé sur celle-ci. Consultez Modifier un jeu de confidentialité ou Exécuter un Rapport sur un jeu de confidentialité.
     - Retirer - Voir Retirer un jeu de confidentialité.

Créer un jeu de confidentialité

1. Ouvrez le panneau Identification de jeu de confidentialité en utilisant l'un des trajets suivants :
   - Conformité > Outils et vues > Générateur de jeu de confidentialité
   - Reconnaître > Reconnaissance de base de données > Générateur de jeu de confidentialité
2. Cliquez sur Nouveau pour ouvrir le panneau Définition de jeu de confidentialité.
3. Dans la zone Description de jeu de confidentialité, entrez un nom unique pour le jeu de confidentialité. N'incluez pas d'apostrophe. C'est par ce nom que le jeu de confidentialité sera identifié dans le panneau Identification de jeu de confidentialité.
4. Au besoin, dans la liste Classification de sécurité, choisissez une classification de sécurité pour le jeu de confidentialité.
5. Dans la section Eléments du panneau Jeu de confidentialité, pour chaque paire d'éléments à inclure :
   - Entrez un nom d'objet dans la zone Objet.
   - Entrez un nom de champ dans la zone Champ ou cochez la case N'importe quel champ de cet objet pour inclure tous les champs de l'objet spécifié.
   - Cliquez sur Ajouter cette nouvelle paire objet-champ.
6. Lorsque tous les éléments ont été ajoutés, cliquez sur Sauvegarder.
7. En option, cliquez sur le bouton Rôles pour ajouter des rôles.
8. En option, cliquez sur le bouton Commentaires pour ajouter des commentaires.

Modifier un jeu de confidentialité

1. Ouvrez le jeu de confidentialité à modifier dans le Générateur de jeu de confidentialité. Consultez Ouvrir le Générateur de jeu de confidentialité.
2. Apportez les changements nécessaires à la définition du jeu de confidentialité. Pour une description de toutes les zones, consultez Créer un jeu de confidentialité.
3. Cliquez sur Sauvegarder.
4. Cliquez sur Terminé lorsque vous avez fini.

Cloner un jeu de confidentialité

1. Ouvrez le jeu de confidentialité à cloner dans le Générateur de jeu de confidentialité. Consultez Ouvrir le Générateur de jeu de confidentialité.
2. Le clone du jeu de confidentialité sera nommé Copie de [jeu de confidentialité sélectionné].Il est conseillé de remplacer ce nom par quelque chose de plus significatif. N'incluez pas d'apostrophe.
3. Si nécessaire, apportez tout changement additionnel à la définition du jeu de confidentialité. Pour une description de toutes les zones, consultez Créer un jeu de confidentialité.
4. Cliquez sur Sauvegarder.
5. Cliquez sur Terminé lorsque vous avez fini.

Retirer un jeu de confidentialité

Vous ne pouvez pas retirer un jeu de confidentialité si un processus d'audit est en cours d'exécution. Arrêtez le processus d'audit, puis suivez ces étapes pour retirer le jeu de confidentialité.

1. Dans le panneau Identification de jeu de confidentialité, sélectionnez le jeu de confidentialité à retirer. Consultez Ouvrir le Générateur de jeu de confidentialité.
2. Cliquez sur Supprimer et confirmez l'action.
3. Cliquez sur Terminé.

Exécuter un rapport sur un jeu de confidentialité

Cette procédure décrit comment exécuter ponctuellement un rapport sur un jeu de confidentialité. Pour programmer l'exécution d'un rapport sur un jeu de confidentialité, incluez-le dans un flux de travail de conformité (voir Automatisation du flux de travail de conformité).

1. Dans le Générateur de jeu de confidentialité, ouvrez le jeu de confidentialité sur lequel vous voulez générer un rapport. Consultez Ouvrir le Générateur de jeu de confidentialité.
2. Cliquez sur Exécuter.
3. Dans Paramètres de tâche, entrez les heures de début et de fin de la période à prendre en compte.
4. Sélectionnez Rapport par détails des accès ou Rapport par utilisateur d'application pour spécifier comment les résultats doivent être présentés. La première option est celle qui est active par défaut. Elle consiste à afficher le nombre d'accès pour chaque combinaison d'IP de client, d'IP de serveur, de (nom de) serveur, de type de serveur, de protocole de base de données, de nom de programme source et de nom d'utilisateur de base de données. Si Utilisateur de l'application est sélectionné, le rapport contiendra une colonne du même nom (après la colonne Nom d'utilisateur de la base de données) et la sortie sera complétée de cette information.

5. Cliquez sur Exécuter une fois maintenant. Après son exécution, le rapport apparaîtra dans une fenêtre à part.
6. Cliquez sur Terminé.

Rubrique parent : Surveillance et audit

Alerte personnalisée

Des messages d'alerte peuvent être distribués via e-mail, SNMP, syslog ou des classes Java™ écrites par l'utilisateur. La dernière option correspond aux alertes personnalisées.

Lorsqu'une alerte est déclenchée, une classe d'alerte personnalisée peut effectuer toute action appropriée à la situation ; par exemple, elle peut mettre à jour une page Web et envoyer un message texte à un numéro de téléphone.

Pour créer une classe d'alerte personnalisée, prenez d'abord contact avec le support technique afin de vous procurer le fichier d'interface nécessaire. La rubrique ci-après explique comment implémenter l'interface. Reportez-vous à la section Utilisation de l'interface d'alerte personnalisée ainsi qu'à la section Exemple de classe d'alerte personnalisée, qui contient un exemple.

Une fois la classe compilée, vous devez la télécharger dans le dispositif Guardium. Voir la section relative à la gestion des classes personnalisées.

Pour des instructions de test d'une classe d'alerte personnalisée, reportez-vous à la section Test d'une classe d'alerte personnalisée plus loin dans cette rubrique.

Remarque : Ne récupérez pas ou n'exécutez pas de code personnalisé provenant de sources de données non fiables, afin de réduire le risque de vulnérabilité en matière de sécurité.
Remarque : Ne récupérez pas ou n'exécutez pas de code personnalisé provenant de sources de données non fiables.
Remarque : N'écrivez pas de classe personnalisée obtenant des données d'une source non fiable.

Utilisation de l'interface d'alerte personnalisée

La classe d'alerte personnalisée doit se trouver dans le package com.guardium.custom et doit implémenter l'interface com.guardium.custom.alerts.CustomerDefinedAlertingIfc :

```
package com.guardium.custom
public class YourClassNameHere implements CustomerDefinedAlertingIfc {
       }
```

L'interface contient les cinq méthodes décrites ci-après.

Tableau 1. Méthode processAlert

Méthode 1	
Description	Traitement d'un message d'alerte unique.
Syntaxe	public void processAlert (String message, Date timeStamp)
Paramètres	Chaîne contenant le message généré par l'alerte. Elément java.util.Date pour l'heure de création du message d'alerte.

Tableau 2. Méthode getMessage

Méthode 2	
Description	Renvoi du message d'alerte.
Syntaxe	public String getMessage ()
Paramètres	Chaîne contenant le message d'alerte.

Tableau 3. Méthode getTimeStamp

Méthode 3	
Description	Renvoi de l'horodatage associé au message d'alerte.
Syntaxe	public Date getTimeStamp ()
Paramètres	Elément java.util.Date pour l'heure de création du message d'alerte.

Tableau 4. Méthode setMessage

Méthode 4	
Description	Définition du message d'alerte.
Syntaxe	public void setMessage (String inMessage)
Paramètres	Chaîne contenant le message d'alerte.

Tableau 5. Méthode setTimeStamp

Méthode 5	
Description	Définition de l'horodatage associé au message d'alerte.
Syntaxe	public void setTimeStamp (Date inDate)
Paramètres	Elément java.util.Date pour l'heure de création du message d'alerte.

Exemple de classe d'alerte personnalisée

L'exemple de programme ci-dessous implémente les cinq méthodes décrites dans la section précédente. Pour la méthode processAlert, ce programme affiche simplement le message d'alerte et l'horodatage dans la console système.

```
/*
 * Sample Custom Alerting Class
 *
 */
package com.guardium.custom;
import java.text.DateFormat;
import java.util.Date;
public class HandleAlerts implements CustomerDefinedAlertingIfc {
private String message = "";
private Date timeStamp = null;
public void processAlert(String message, Date timeStamp){
setMessage(message);
setTimeStamp(timeStamp);
System.out.println(getMessage() + " on " +
  DateFormat.getDateInstance(). format(getTimeStamp()));
}
    public void setMessage(String inMessage){
        message = inMessage;
    }
    public String getMessage(){
        return message;
    }
    public void setTimeStamp(Date inDate){
        timeStamp = inDate;
    }
    public Date getTimeStamp(){
        return timeStamp;
    }
}
```

Test d'une classe d'alerte personnalisée

Après avoir compilé une classe d'alerte personnalisée, suivez cette procédure pour la tester.

1. Téléchargez la classe personnalisée dans le dispositif. Il s'agit d'une opération d'administration effectuée depuis la console d'administration. Voir la section relative à la gestion des classes personnalisées.
2. Définissez une alerte de corrélation ou en temps réel qui utilisera la classe d'alerte personnalisée. Quel que soit le type d'alerte qui génère l'alerte, le test est plus facile si vous affectez un deuxième type de notification (e-mail par exemple) auquel vous pouvez comparer les résultats de l'alerte personnalisée.
3. Vérifiez l'environnement en effectuant l'une des opérations suivantes :
    - Pour une alerte de corrélation :
        - Vérifiez que l'intervalle d'interrogation Détection des anomalies est adapté au test et que la détection des anomalies a été démarrée. Si l'intervalle d'interrogation est trop long (30 minutes ou plus), l'attente avant l'exécution de la requête peut être longue.
        - Vérifiez que l'intervalle d'interrogation Avertisseur est adapté au test et que l'avertisseur a été démarré.
        - Vérifiez que l'alerte à tester est active.
    - Pour une alerte en temps réel :
        - Vérifiez que la politique contenant la règle avec l'action d'alerte personnalisée est la politique installée.
        - Vérifiez que le moteur d'inspection a été redémarré après l'installation de la politique mise à jour.
        - Vérifiez que l'intervalle d'interrogation Avertisseur est adapté au test et que l'avertisseur a été démarré.
4. Effectuez toute action nécessaire pour déclencher l'alerte (par exemple, provoquez plusieurs échecs de connexion).

Rubrique parent : Surveillance et audit

Processus Flat Log

L'option Flat Log est un processus qui permet au dispositif Guardium de consigner des informations sans les analyser immédiatement en temps réel.

Ce processus sauvegarde les ressources de traitement, ce qui permet de gérer un trafic plus volumineux. L'analyse syntaxique et la fusion des données dans la base de données interne de Guardium peuvent être effectuées ultérieurement, sur un collecteur ou une unité agrégation.

Remarque : Les règles sur données brutes ne fonctionnent pas avec des règles de politique impliquant un champ, un objet, un verbe SQL (commande), un groupe d'objets/de commandes et un groupe d'objets/de champs. Dans le terme "processus Flat Log", "flat" signifie qu'aucun arbre de syntaxe n'est généré. S'il n'existe pas d'arbre de syntaxe, les champs, objets et verbes SQL ne peuvent pas être déterminés.

Les actions suivantes ne fonctionnent pas avec des politiques de type règles sur données brutes : LOG FULL DETAILS, LOG FULL DETAILS PER SESSION, LOG FULL DETAILS VALUES, LOG FULL DETAILS VALUES PER SESSION, LOG MASKED DETAILS.

La sélection de cette fonction implique le menu Générateur de politique dans Configuration > Outils et vues et le menu Processus Flat Log dans Gestion > Surveillance des activités.

Lorsque la case à cocher Consigner données brutes (Flat Log) qui apparaît dans l'écran Définition de politique du générateur de politique est sélectionnée :

- Les données ne sont pas analysées en temps réel.
- Les processus Flat Log sont répertoriés dans un rapport Liste Flat Log désigné.

1. Accédez à Gestion > Surveillance des activités > Processus Flat Log.
2. Sélectionnez l'activité à effectuer :
    - Traiter - Fusionnez les informations de processus Flat Log dans la base de données interne.
    - Archivage/Agrégation/Purge - Archivez ou agrégez, et si vous le souhaitez, purgez le processus Flat Log.
    - Purger uniquement - Purgez les données Flat Log.
3. Cliquez sur Appliquer pour sauvegarder la configuration.
4. Dans le cadre d'une activité Traiter, si vous le souhaitez, effectuez l'une des opérations suivantes :
    - Cliquez sur Exécuter une fois maintenant pour fusionner immédiatement les informations de processus Flat Log dans la base de données interne.

- Cliquez sur Modifier la planification afin de définir une planification pour cette activité. Vous pouvez sélectionner l'heure de début, la fréquence de redémarrage et la fréquence de répétition. Dans le champ Planifier par..., vous devez sélectionner Jour/Semaine ou Mois. Pour plus d'informations sur la planification, consultez Planification.

Rubrique parent : Surveillance et audit

Construction d'une expression dans une condition de requête

Utilisez l'icône Ajouter une expression associées aux sélections Valeur, Paramètre et Attribut pour entrer des conditions de requête incluant des chaînes définies par l'utilisateur et des expressions mathématiques.

Utilisez cette possibilité lorsque vous devez ajouter une condition basée non pas sur le contenu entier de l'attribut, mais sur une partie de celui-ci, sur une fonction de l'attribut ou sur une fonction combinant plusieurs attributs.

Exemple : `INSTR(:attribute, '150.1') = 5`, qui retournera toutes les instances de l'attribut IP client contenant les cinq caractères listés (avec le premier en position 5). Tapez le caractère 5 dans la boîte d'entrée à côté de l'icône Ajouter une expression. Tapez l'expression `INSTR(:attribute, '150.1')` dans la fenêtre distincte Générer une expression. Testez la validité de l'expression dans cette même fenêtre. Autre exemple : `LENGTH(:attribute) >= 40`, qui retourne la longueur de toute instruction SQL faisant plus de 40 caractères. L'expression peut (ou non) contenir des références à l'attribut lui-même, ainsi que des références à d'autres attributs.

Rubrique parent : Surveillance et audit

Rapport sur les autorisations de base de données

Le processus de révision des autorisations consiste à vérifier que les utilisateurs disposent des privilèges requis pour effectuer leurs tâches.

Avec l'authentification des utilisateurs et la restriction des privilèges d'accès aux données basés sur les rôles, la révision des autorisations, qui consiste à vérifier que les utilisateurs ne disposent que des privilèges requis pour accomplir leurs tâches, doit être effectuée régulièrement. Ce processus est également appelé génération d'attestation des droits d'utilisateur de base de données.

Utilisez les rapports sur les autorisations (privilèges) de base de données prédéfinis (par exemple) pour savoir qui possèdent des privilèges système et qui a octroyé ces privilèges à d'autres utilisateurs et rôles. Les rapports sur les autorisations de base de données sont importants pour les auditeurs qui effectuent le suivi de l'accès aux bases de données et pour garantir qu'aucune faille de sécurité liée à la persistance des comptes ou à des privilèges incorrectement octroyés n'existe.

Des rapports personnalisés sur les autorisations de base de données ont été créés pour une configuration plus rapide et pour faciliter le téléchargement et la génération de rapports sur les données provenant des bases de données suivantes : Oracle, MYSQL, DB2, SYBASE, SYBASE IQ, Informix, MS SQL 2000/2005/2008, Netezza, Teradata et PostgreSQL, DB2 sur z/OS.

Pour les bases de données Microsoft SQL Server et Oracle, vous pouvez aussi utiliser l'Optimisation des autorisations afin d'accéder à ces informations.

Procédez comme suit pour utiliser les rapports sur les autorisations (privilèges) de base de données prédéfinis avec des instantanés à jour des utilisateurs de base de données et des privilèges d'accès :

1. Ajoutez des sources de données/bases de données au dispositif (accédez à Conformité > Génération de rapports personnalisés > Générateur de domaine personnalisé).
2. Affectez des sources de données à des autorisations (accédez à Conformité > Génération de rapports personnalisés > Générateur de table personnalisée). Sélectionnez la liste des tables personnalisées pour votre autorisation. Cliquez sur Télécharger des données. Affectez des sources de données au rapport sur les autorisations dans l'écran du menu Importation de données. Lorsque vous avez terminé, cliquez sur Exécuter une fois maintenant.
3. Pour consulter les rapports sur les autorisations, connectez-vous au portail utilisateur et accédez à l'onglet Autorisations de base de données.

Les rapports sur les autorisations de base de données utilisent la fonction Domaine personnalisé de Guardium pour créer des liens entre les données externes dans la base de données sélectionnée et les données internes des rapports prédéfinis sur les autorisations. Voir Corrélation des données externes pour plus d'informations sur le générateur de domaine personnalisé, le générateur de requête personnalisée ou le générateur de table personnalisée.

Les rapports d'autorisation prédéfinis sont listés dans Rapports sur les autorisations de base de données.

Rubrique parent : Surveillance et audit

Identification de l'utilisateur

Guardium met à disposition plusieurs méthodes d'identification des utilisateurs d'application, lorsque l'utilisateur de base de données réel n'apparaît pas de façon évidente depuis le trafic de base de données.

Certaines applications de base de données ont été conçues pour utiliser ou partager un petit nombre de comptes utilisateur de base de données. Ces applications gèrent leurs utilisateurs indépendamment du système de gestion de base de données, ce qui signifie que lorsque vous observez le trafic depuis l'extérieur de l'application, il peut être difficile de déterminer quel est l'utilisateur d'application qui contrôle une connexion de base de données à un moment donné. Toutefois, lorsque des activités de base de données suspectes surviennent, vous devez lier des actions spécifiques à des individus spécifiques plutôt qu'à un compte partagé par des groupes d'individus. En d'autres termes, vous devez connaître l'utilisateur d'application, et pas seulement l'utilisateur de base de données.

Guardium met à disposition plusieurs méthodes d'identification des utilisateurs d'application, lorsque l'utilisateur de base de données réel n'apparaît pas de façon évidente depuis le trafic de base de données :

- Identification des utilisateurs via la traduction des utilisateurs de l'application : pour certaines des applications commerciales les plus populaires (Oracle EBS, PeopleSoft, SAP, etc.), Guardium peut identifier les utilisateurs automatiquement.
- Identification des utilisateurs via l'API : l'API Application Events vous permet d'avertir Guardium lorsqu'un utilisateur d'application prend ou abandonne le contrôle d'une connexion, ou lorsqu'un autre événement intéressant survient. (Cette méthode ne permet pas que d'identifier des utilisateurs.)
- Identification des utilisateurs via des procédures mémorisées : de nombreuses applications utilisent des procédures mémorisées de base de données pour identifier l'utilisateur d'application. Dans ces cas, les informations utilisateur peuvent généralement être extraites depuis les paramètres de procédure mémorisée.

Dans l'entreprise, il peut être nécessaire d'employer plusieurs méthodes d'identification des utilisateurs, selon les applications utilisées.

- Identification des utilisateurs via la traduction des utilisateurs de l'application
  Certaines applications gèrent un pool de connexions de base de données. Dans ce type d'architecture à trois niveaux, les connexions en pool se connectent toutes

à la base de données au moyen d'un même ID fonctionnel. Tous les utilisateurs de l'application sont ensuite gérés en interne. Lorsqu'une session d'utilisateur a besoin d'accéder à la base de données, elle obtient une connexion du pool, l'utilise, puis la rend au pool. Dans ces conditions, Guardium peut voir comment l'application interagit avec la base de données, mais il ne peut pas attribuer telle ou telle action sur la base de données à tel ou tel utilisateur de l'application.

- Identification des utilisateurs via une API
  Pour certaines applications qui gèrent les utilisateurs en interne, l'utilisateur d'application ne peut pas être identifié à partir du trafic. Dans ce cas, vous pouvez utiliser l'API Guardium Application Events.
- Identification d'utilisateurs via des procédures stockées
  Dans de nombreuses applications existantes, toutes les informations nécessaires à l'identification d'un utilisateur d'application peuvent être obtenues depuis le trafic de base de données existant, à partir d'appels de procédure stockée. Une fois que Guardium sait quels sont les appels à surveiller et quels sont les paramètres qui contiennent le nom d'utilisateur ou d'autres informations intéressantes, les utilisateurs peuvent être identifiés automatiquement.

Rubrique parent : Surveillance et audit

Identification des utilisateurs via la traduction des utilisateurs de l'application

Certaines applications gèrent un pool de connexions de base de données. Dans ce type d'architecture à trois niveaux, les connexions en pool se connectent toutes à la base de données au moyen d'un même ID fonctionnel. Tous les utilisateurs de l'application sont ensuite gérés en interne. Lorsqu'une session d'utilisateur a besoin d'accéder à la base de données, elle obtient une connexion du pool, l'utilise, puis la rend au pool. Dans ces conditions, Guardium peut voir comment l'application interagit avec la base de données, mais il ne peut pas attribuer telle ou telle action sur la base de données à tel ou tel utilisateur de l'application.

Pour certaines applications populaires, Guardium dispose d'un support intégré qui permet d'identifier l'utilisateur final et donc de faire le lien entre activité de la base de données et utilisateur final de l'application.

Pour utiliser cette fonctionnalité, suivez ces procédures :

1. Définissez, pour l'application voulue, une Configuration de traduction des utilisateurs de l'application. Consultez à cet effet Configurer la détection des utilisateurs de l'application.
2. Remplissez les groupes prédéfinis requis pour cette application. Consultez à cet effet Peupler les groupes prédéfinis de l'application.
3. Régénérez les portlets des rapports spéciaux de cette application et placez-les sur une page. Consultez à cet effet Régénérer les portlets des rapports spéciaux de l'application.

Trace d'audit sélective et traduction des utilisateurs de l'application

Si la politique d'accès aux données installée utilise la fonction Trace d'audit sélective pour limiter la quantité de données consignées, deux points importants concernant la traduction des utilisateurs de l'application sont à prendre en considération :

- La politique ignorera tout trafic qui ne remplit pas les conditions de la règle de traduction des utilisateurs de l'application (par exemple, le trafic d'une provenance autre que le serveur d'application).
- Seul le SQL correspondant au motif (pattern) pour cette politique de sécurité sera disponible pour les rapports spéciaux de traduction des utilisateurs de l'application.

Configurer la détection des utilisateurs de l'application

1. Sélectionnez Protéger > Détection des intrusions dans la base de données > Traduction des utilisateurs de l'application. Les détails des configurations de traduction existantes apparaissent en haut de la page.
2. Pour créer une nouvelle configuration, commencez par entrer un code unique dans la zone Code d'application.
   Remarque : Sous Gestion centralisée, vous devez utiliser des codes d'application différents sur les différentes machines gérées. Vous éviterez ainsi tout conflit entre les alias générés pour les utilisateurs. (Sous Gestion centralisée, il n'y a qu'un seul jeu d'alias partagé par toutes les unités gérées.)
3. Sélectionnez le type d'application dans la liste correspondante :
   - BO-WI - Business Objects / Web Intelligence
   - EBS - Oracle E-Business Suite
   - PeopleSoft
   - SAP Observed
   - SAP DB
   - SIEBEL Observed
   - SIEBEL DB
4. Dans la zone Version d'application, entrez le numéro de version de l'application (par exemple, 11).
5. Sélectionnez le type de base de données dans la liste correspondante. Seuls sont proposés les types de base de données convenant à votre sélection de type et de version d'application.
   Remarque : Lorsque le type d'application choisi est EBS, SIEBEL DB ou SAP DB, vous avez la possibilité de sélectionner une source de données parmi les sources préexistantes en cliquant sur le bouton Ajouter une source de données. La source de données doit convenir à l'un des types de base de données supportés pour le type d'application que vous configurez.
6. Dans la zone IP serveur, entrez l'adresse IP que l'application utilise pour se connecter à la base de données.
7. Dans la zone Port, entrez le numéro de port que l'application utilise pour se connecter à la base de données.
8. Dans la zone Nom d'instance, entrez le nom d'instance que l'application utilise pour se connecter à la base de données.
9. Dans la zone Nom de base de données, entrez le nom de base de données pour l'application. (Information indispensable pour certaines applications, inutile pour d'autres.)
10. Cochez la case Actif pour activer la traduction des utilisateurs. Rien n'est traduit tant qu'il n'y a pas eu une première importation de définitions d'utilisateurs.
11. Entrez le nom d'utilisateur que le système Guardium devra utiliser pour accéder à la base de données. Entrez le mot de passe que le système Guardium devra utiliser pour accéder à la base de données.
12. Cochez la case Responsabilité si vous voulez importer les responsabilités (par exemple, Administration) associées aux noms d'utilisateurs. Décochez-la si vous voulez seulement enregistrer les noms d'utilisateur. Si cette case n'est pas cochée, toutes les activités d'un utilisateur seront groupées ensemble, sans considération de la responsabilité de cet utilisateur au moment où ont eu lieu ces activités.
    Remarque : Si le type d'application est EBS (type de base de données Oracle), deux choix supplémentaires apparaissent : Se connecter via IP serveur et Se connecter via nom d'utilisateur.Si vous indiquez une IP de serveur et un nom d'utilisateur dans ces zones, le système les utilisera pour se connecter et récupérer les noms d'utilisateur et les responsabilités associées.
13. Cliquez sur le bouton Ajouter pour sauvegarder la définition de traduction des utilisateurs de l'application.
14. Enchaînez avec les procédures "Peupler les groupes prédéfinis de l'application" et "Régénérer les portlets des rapports spéciaux de l'application".
15. Une fois l'étape précédente effectuée, allez à Gérer > Surveillance des activités > Moteurs d'inspection et cliquez sur Redémarrer les moteurs d'inspection dans le panneau Configuration de moteur d'inspection.

16. Après avoir suivi les tâches des deux procédures citées plus haut, retournez à la configuration de traduction des utilisateurs de l'application et cliquez sur Exécuter une fois maintenant pour importer les définitions d'utilisateurs pour cette application (ainsi que pour les autres applications, le cas échéant).
17. Plus tard, après avoir vérifié le bon fonctionnement de l'opération d'importation des données (voir plus bas), retournez à ce panneau et cliquez sur le bouton Modifier le planning pour programmer l'exécution à intervalles réguliers de cette opération d'importation. Il est en effet souhaitable de programmer l'importation des définitions d'utilisateurs avec une régularité convenant à votre environnement. Lorsqu'un nouvel utilisateur est créé côté application, sa définition n'est pas disponible côté Guardium tant qu'une nouvelle importation des définitions n'a pas eu lieu. L'intervalle entre deux exécutions successives de l'opération d'importation est donc le temps maximum pendant lequel une définition d'utilisateur pourrait ne pas être disponible. Pour savoir comment utiliser le planificateur, consultez Planification.
18. Vous pouvez vérifier que l'importation des données destinées à la traduction des utilisateurs de l'application s'est bien déroulée en consultant les rapports prédéfinis. Par exemple, Accès aux applications SAP. Suivez le trajet Rapports > Outils de configuration de rapport > Générateur de rapports et choisissez le rapport (par exemple, Accès aux applications SAP). Régénérez ce rapport et ajoutez-le à un panneau, puis choisissez une période suffisamment étendue (par exemple, remontez un an en arrière pour les données).

Remarque : Après la mise en place de la traduction des utilisateurs de l'application dans votre environnement, lorsque vous cliquez pour la première fois sur Exécuter une fois maintenant, la date de dernière mise à jour des tables consultées est récupérée.Après quoi, lors des exécutions suivantes, seules les nouvelles données (postérieures à cette date) sont importées. Sans ce procédé, plusieurs années de données seraient inutilement importées et rempliraient de nombreuses tables/bases de données.

Peupler les groupes prédéfinis de l'application

Une fois que la traduction des utilisateurs de l'application a été configurée, vous devez peupler au moins deux groupes prédéfinis avec des informations qui seront spécifiques à votre environnement. Le tableau suivant indique quels groupes doivent être peuplés pour chaque type d'application. Pour des instructions sur la manière de peupler un groupe, consultez Présentation des groupes.

Application	Groupe prédéfini	Type de groupe
EBS	Serveurs d'application EBS	IP client
	Serveurs de base de données EBS	IP serveur
PeopleSoft	Serveurs d'application PSFT	IP client
	Serveurs de base de données PSFT	IP serveur
	Objets PeopleSoft	Objets
Siebel	Serveurs d'application SIEBEL	IP client
	Serveurs de base de données SIEBEL	IP serveur
SAP	Serveurs d'application SAP	IP client
	Serveurs de base de données SAP	IP serveur
	SAP - PCI	Objets

Régénérer les portlets des rapports spéciaux de l'application

Pour certains types d'application, un ou plusieurs portlets pour rapports spéciaux doivent être régénérés. Par exemple, pour EBS, il y a deux rapports prédéfinis. Il y en a également deux pour PeopleSoft. Ces rapports ne sont pas modifiables. Après avoir peuplé les groupes prédéfinis du type d'application concerné, suivez la procédure ci-après pour régénérer les portlets des rapports prédéfinis correspondants et les placer sur une page.

Les exemples utilisés dans cette section concernent les portlets EBS, mais la procédure est la même pour les autres types d'application.

1. Ouvrez le Localiseur de rapport en appliquant l'une des méthodes suivantes : utilisateurs titulaires du rôle d'administrateur : sélectionnez Outils - Générateur de rapports. Tous les autres : sélectionnez Surveillance/Audit - Générateur de rapports.
2. Cliquez sur Rechercher pour ouvrir le panneau Résultats de la recherche de rapport.
3. Sélectionnez un portlet de rapport pour le type d'application concerné (par exemple, Accès aux applications EBS) et cliquez sur Régénérer le portlet. Lorsque le portlet aura été régénéré, vous en serez informé.
4. Répétez l'étape précédente pour chaque autre rapport nécessaire (par exemple, Accès à la base de données des processus EBS ou Accès à la base de données des processus PSFT). A présent, ajoutez un nouvel onglet à votre agencement de panneaux et incorporez-y les deux portlets régénérés.
5. Cliquez sur Personnaliser pour ouvrir le panneau correspondant.
6. Cliquez sur Ajouter une sous-fenêtre pour définir un nouvel onglet.
7. Entrez un nom pour le nouvel onglet (par exemple, Rapports EBS) et cliquez sur Appliquer. Le nouvel onglet apparaît en dernière position dans la liste.
8. Cliquez sur le nom du nouvel onglet pour éditer le panneau associé.
9. Cliquez sur Ajouter un portlet, puis sur Suivant jusqu'à atteindre les rapports voulus (les rapports EBS, par exemple). Cochez la case de chaque rapport à inclure.
10. Cliquez sur Appliquer, puis sur Sauvegarder et appliquer, puis sur Sauvegarder pour sauvegarder le nouvel agencement de panneaux. Le nouvel onglet apparaîtra à la fin de la première rangée d'onglets.
11. Cliquez sur le nom du nouvel onglet pour ouvrir celui-ci.
12. Cliquez sur Personnaliser pour fixer les paramètres d'exécution (par exemple, la plage de dates et Afficher les alias).

Clients réticents à l'idée de donner le mot de passe du DB_USER pour l'application EBS

Dans certains cas, les clients ne souhaitent pas utiliser le DB_USER Oracle EBS pour traduire le trafic EBS. Si vous êtes dans ce cas de figure, il est néanmoins possible de faire fonctionner le mécanisme de traduction des utilisateurs de l'application avec Oracle EBS. Deux possibilités s'offrent à vous :

- Fournissez le nom d'utilisateur et le mot de passe que EBS utilise pour dialoguer avec Oracle (il s'agit souvent de APPS/$passwd).
- Si le client ne souhaite pas fournir/entrer le mot de passe du DB_USER utilisé par EBS pour accéder à Oracle, il demeure possible d'obtenir la traduction des utilisateurs de l'application, mais la procédure est plus compliquée.

1. Créez/choisissez un ID de connexion (login) pour Oracle qui permette d'accéder à la base de données pour recueillir les alias/utilisateurs/responsabilités.Cet utilisateur devra pouvoir accéder à la table [APPLSYS.]FND_USER et à la vue FND_RESPONSIBILITY_VL, cette dernière étant la combinaison de deux tables : APPLSYS.FND_RESPONSIBILITY et APPLSYS.FND_RESPONSIBILITY_TL.

```
(  CREATE VIEW FND_RESPONSIBILITY_VL AS SELECT /* $HEADER$ */ B.ROWID ROW_ID , B.WEB_HOST_NAME ,
B.WEB_AGENT_NAME , B.APPLICATION_ID , B.RESPONSIBILITY_ID ,
B.RESPONSIBILITY_KEY , B.LAST_UPDATE_DATE , B.LAST_UPDATED_BY ,
B.CREATION_DATE , B.CREATED_BY , B.LAST_UPDATE_LOGIN ,
B.DATA_GROUP_APPLICATION_ID , B.DATA_GROUP_ID , B.MENU_ID ,
B.START_DATE , B.END_DATE , B.GROUP_APPLICATION_ID ,
B.REQUEST_GROUP_ID , B.VERSION , T.RESPONSIBILITY_NAME ,
T.DESCRIPTION FROM FND_RESPONSIBILITY_TL T, FND_RESPONSIBILITY B
WHERE B.RESPONSIBILITY_ID = T.RESPONSIBILITY_ID
AND B.APPLICATION_ID = T.APPLICATION_ID
AND T.LANGUAGE = USERENV('LANG')  )
```

2. Exécutez les instructions SQL suivantes directement à partir du système Guardium : select RESPONSIBILITY_ID, RESPONSIBILITY_NAME from FND_RESPONSIBILITY_VL order by RESPONSIBILITY_ID; et SELECT USER_ID, USER_NAME from FND_USER ORDER BY USER_ID;

   Une fois l'utilisateur configuré pour que ces deux instructions soient exécutées correctement, deux entrées de configuration Traduction des utilisateurs de l'application doivent être créées.Toutes les deux doivent avoir les mêmes IP de serveur, numéro de port et nom d'instance (et bien sûr, EBS et Oracle choisis respectivement comme type d'application et comme type de base de données).

   Peu importe que le code d'application soit identique ou non. Une entrée a besoin du nom d'utilisateur que EBS utilise pour se connecter à la base de données (généralement APPS), mais le mot de passe associé que vous entrez peut être volontairement erroné (bidon). La seconde entrée a besoin de la combinaison nom d'utilisateur/mot de passe qui a été créée pour accéder à ces tables.

3. Une fois les deux entrées créées et les cases Actif et Responsabilité cochées, cliquez sur Exécuter une fois maintenant et démarrez ou redémarrez EBS (on suppose ici qu'un moteur d'inspection (S-TAP ou net) observe le trafic). La collecte des données et l'affectation des noms d'utilisateur APPS à ces données pour le trafic EBS sont à présent effectives.

Privilèges Oracle nécessaires pour l'utilisateur d'application Oracle EBS

Traduction :

1. Octroyez (grant) le privilège select sur les tables suivantes à l'utilisateur de base de données personnalisé :

   APPLSYS.FND_USER

   APPLSYS.FND_RESPONSIBILITY

   APPLSYS.FND_RESPONSIBILITY_TL

2. Créez un synonyme privé FND_USER sur APPLSYS.FND_USER pour l'utilisateur de base de données personnalisé.
3. Créez une vue nommée FND_RESPONSIBILITY_VL pour l'utilisateur de base de données personnalisé.Cette vue peut être trouvée sous l'utilisateur APPS et est utilisable comme modèle.

Comment valider la pile SAP pour la traduction des utilisateurs de l'application

Si IBM Guardium doit prendre en charge la traduction des utilisateurs de l'application SAP, certaines différences fondamentales entre les systèmes à pile ABAP et les systèmes à pile Java™ sont à prendre en considération.
Remarque :

Les piles ABAP et Java ont des spécifications de noyau (kernel) différentes.

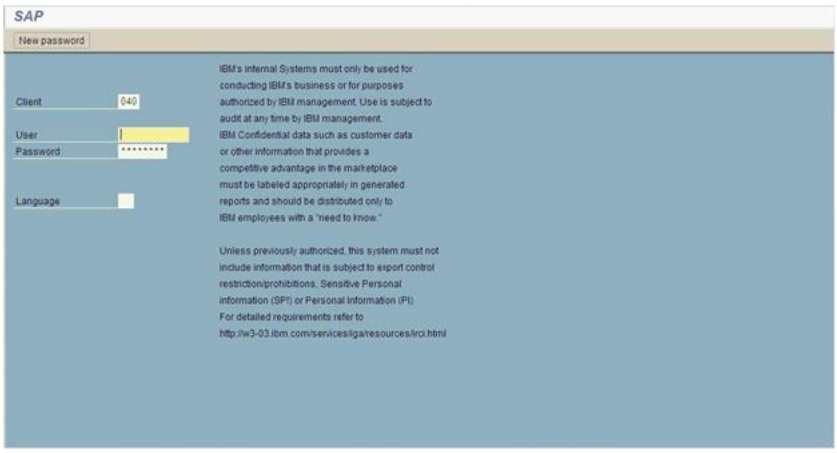
Les systèmes à pile ABAP et les systèmes à pile Java ont des tables différentes.

Pile ABAP

Les systèmes SAP ECC (Enterprise Core Components) traditionnels sont écrits en code ABAP et l'accès à ces systèmes se fait principalement via le client graphique SAP (SAP GUI), même si l'accès web reste possible.

Les systèmes SAP à pile ABAP ont un accès direct (lecture/écriture/mise à jour) aux bases de données SAP traditionnelles. Ces bases de données sont énormes et contiennent toutes les données sensibles. C'est donc avec elles que IBM Guardium révélera tout son potentiel.

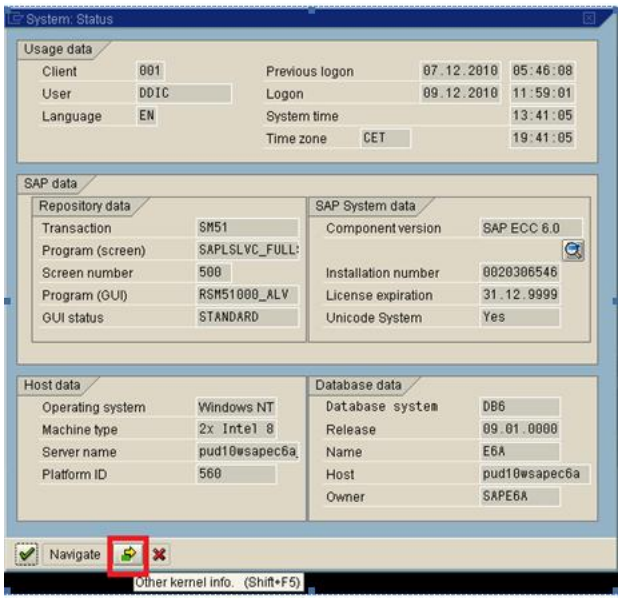
Un écran du type suivant apparaît lorsque vous entrez dans le client graphique SAP GUI (pile ABAP) :



1-SAP GUI (pile ABAP)

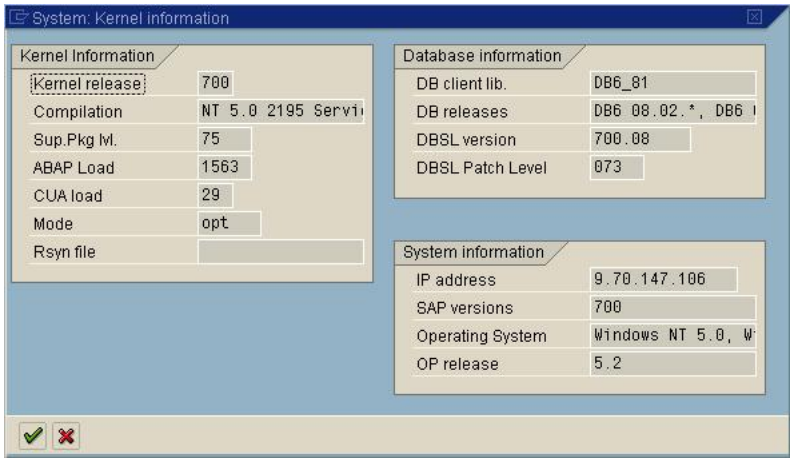
Pour valider le noyau SAP sur pile ABAP par rapport à la traduction des utilisateurs de l'application, suivez ces étapes :

1. Connectez-vous à SAP.
2. Allez à System > Status



2-System Status (pile ABAP)

3. Cliquez sur Other Kernel Info dans l'écran System Status.



3-System Kernel Information (pile ABAP)

Dans cet exemple, la version du noyau est 700.

SAP avec DB2 comme base de données en backend est également disponible pour SAP version de noyau 640, mais l'utilisateur doit dans ce cas configurer DB6_DBSL_ACCOUNTING=1 (dans les versions de noyau 700 et suivantes, DB6_DBSL_ACCOUNTING est déjà réglé à 1 par défaut). SAP avec Oracle en backend requiert un noyau version 710 ou ultérieure.

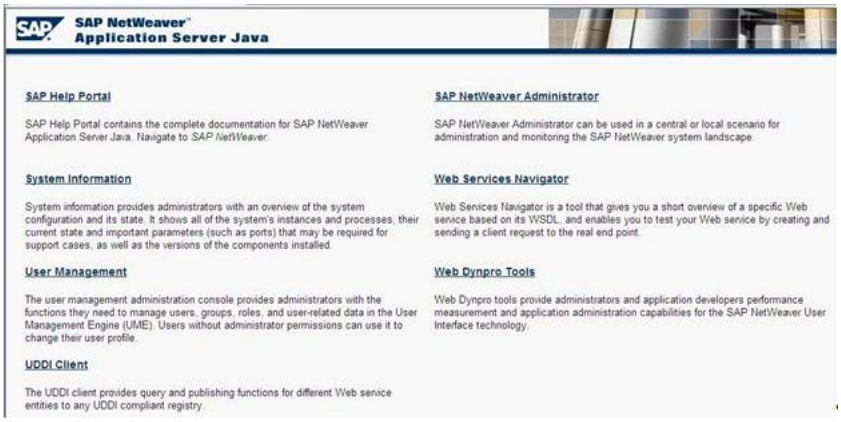
Les données sont placées dans le champ utilisateur d'application et la chaîne d'événements de l'application.

Pile Java

Les systèmes de portail SAP sont écrits en Java. Ce sont des applications web frontales qui exploitent des requêtes prêtes à l'emploi pour afficher les pages web liées à SAP.

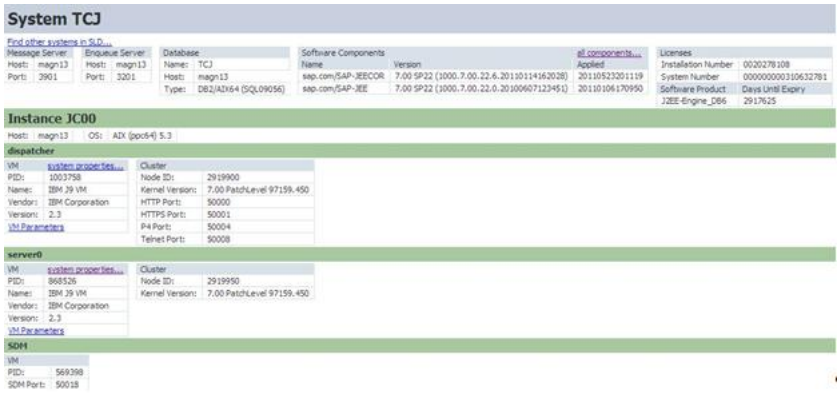
Les systèmes de portail ne sont accessibles que par l'intermédiaire d'un navigateur web. Leurs bases de données sont beaucoup plus petites et ne contiennent que quelques espaces table.

Un écran du type suivant apparaît lorsque vous entrez dans un système de portail SAP (pile Java).



4-Système de portail SAP (pile Java)

Pour valider le noyau SAP sur pile Java par rapport à la traduction des utilisateurs de l'application, suivez ces étapes : 1. Cliquez sur System Information.



5-System TCJ (pile Java)

Dans cet exemple, la version du noyau SAP est 7.00.

SAP pour DB2 ou Oracle requiert un noyau version 7.02 ou supérieure.

Côté client, les propriétés dans la pile Java sont similaires à ce qu'elles étaient dans la pile ABAP.

Rubrique parent : Identification de l'utilisateur

Identification des utilisateurs via une API

Pour certaines applications qui gèrent les utilisateurs en interne, l'utilisateur d'application ne peut pas être identifié à partir du trafic. Dans ce cas, vous pouvez utiliser l'API Guardium Application Events.

L'API Application Events fournit des appels simples pouvant être émis depuis l'application afin de signaler à Guardium qu'un utilisateur acquiert ou libère une connexion, ou tout autre événement intéressant.

Remarque : Si l'option Trace d'audit sélective est activée pour votre politique de sécurité Guardium, les commandes de l'API Application Events qui sont utilisées pour définir et effacer l'utilisateur d'application et/ou des événements d'application sont ignorées par défaut, et les noms d'utilisateur d'application et/ou les événements d'application ne sont pas consignés. Afin de consigner ces éléments de sorte qu'ils soient disponibles pour les rapports ou les exceptions, incluez une règle de politique permettant d'identifier les commandes appropriées, en spécifiant l'action de règle Effectuer l'audit uniquement.

GuardAppUser - Identification des utilisateurs via une API

Utilisez deux déclencheurs prédéfinis afin de définir GDM_CONSTRUCT_INSTANCE.APP_USER_NAME et GDM_APP_EVENT.* pour les noms d'utilisateur d'application et les données d'événement d'application.

Ces déclencheurs prédéfinis sont :

- GuardAppEvent
- GuardAppUser

Ils comportent chacun des déclencheurs de démarrage et d'arrêt, et Event possède des sous-déclencheurs permettant de définir les éléments Type, Username, StrValue, NumValue et Date.

Le système Guardium peut lire les instructions SELECT spéciales pour les détails de nom d'utilisateur d'application et d'événement d'application.

Le format est le suivant :

```
 Select "action" [autres
paramètres] FROM [emplacement].
```

Tableau 1. Options d'action

Syntaxe	Action
GuardAppUser:<nom_utilisateur>	Définir <nom_utilisateur> pour GDM_CONSTRUCT_INSTANCE.APP_USER_NAME
GuardAppUserReleased	Effacer APP_USER_NAME pour les requêtes suivantes
GuardAppEvent:Start	Démarrer un événement GuardAppEvent (recherche les paramètres supplémentaires)
GuardAppEvent:Released	Arrêter un événement GuardAppEvent (efface les informations pour les requêtes suivantes)

Tableau 2. Paramètres supplémentaires (définissant les valeurs dans GDM_APP_EVENT)

Paramètres	Syntaxe
GuardAppEventType: <chaîne_type_événement>	Définir <chaîne_type_événement> pour APP_EVENT_TYPE
GuardAppEventUserName: <nom_utilisateur_évén>	Définir <nom_utilisateur_événement> pour GDM_APP_EVENT.APP_USER_NAME
GuardAppEventStrValue:<valeur_chaîne>	Définir <valeur_chaîne> pour EVENT_VALUE_STR
GuardAppEventNumValue:<nombre>	Définir <nombre> pour EVENT_VALUE_NUM
GuardAppEventDateValue:<date>	Définir <date> pour EVENT_DATE

Voici quelques exemples d'instruction SELECT :

Select guardappuser:tiberius from dual

Select guardappuserreleased from dual

Select GuardAppEvent:Start, GuardAppEventType:Event1, GuardAppEventUserName:Tiberius, GuardAppEventStrValue:abc, GuardAppEventNumValue:123, GuardAppEventDateValue:2016-01-26 15:55:28 from dual

Select GuardAppEvent:Released from dual

La partie FROM de l'instruction varie en fonction du type de base de données.

Oracle : from DUAL

DB2 : from SYSIBM.SYSDUMMY1

Informix : from SYSTABLES

MS-SQL : <rien>

Sybase : <rien>

MySQL : <rien> ou from DUAL

Identification dans Guardium du nom d'utilisateur d'application et des modèles nommés

Dans Guardium, vous pouvez capturer un nom d'utilisateur d'application de plusieurs façons. Guardium possède deux tables Turbine dans lesquelles les valeurs du champ APP_USER_NAME sont stockées, en fonction de la façon dont les données ont été reçues :

GDM_CONSTRUCT_INSTANCE

GDM_APP_EVENT

Le paramètre de modèle nommé %%AppUserName dans Guardium (voir le menu Profil global) est mappé à la table Turbine GDM_CONSTRUCT_INSTANCE. Pour que Guardium puisse l'utiliser dans le modèle nommé, APP_USER_NAME doit être associé à la valeur d'utilisateur d'application dans la table GDM_CONSTRUCT_INSTANCE.

Remplacez la syntaxe de la commande SQL dans l'application par :

SELECT 'GuardAppUser:<valeur>'

Ainsi, les valeurs seront placées dans la table appropriée et la valeur du paramètre %%AppUserName dans le modèle nommé sera remplacée par la valeur appropriée.

Exemple

.....

select 'GuardAppUser:Db2_User' FROM SYSIBM.SYSDUMMY1 ;

select * from AppUser_DB2;

select 'GuardAppUserReleased' FROM SYSIBM.SYSDUMMY1 ;

select * from NoMoreUser_DB2;

.....

Consultez les résultats dans le fichier /var/log/messages :

Jan 24 12:49:41 vx64 guard_sender[28274]: LEEF:1.0|IBM|Guardium|10.0|Alert per match|ruleID=20003|ruleDesc=Alert per match|severity=INFO|devTime=2016-01-24
11:50:39|serverType=DB2|classification=|category=|dbProtocolVersion=3.0|usrName=Db2_User|sourceProgram=DB2JCC_APPLICATION|start=1448383760000|dbUse

r=DB2INST1|dst=9.70.144.126|dstPort=50000|src=9.70.144.126|srcPort=58781|protocol=TCP|type=SQL_LANG|violationID=20|sql=select * from AppUser_DB2 FOR READ ONLY|error=

Définition de l'utilisateur d'application via GuardAppUser

Utilisez cet appel pour indiquer qu'un nouvel utilisateur d'application a pris le contrôle de la connexion. Le nom d'utilisateur d'application fourni sera disponible dans l'attribut Application User de l'entité Access Period. Pour cette session, à partir de là, Guardium attribuera toutes les activités ayant lieu sur la connexion à cet utilisateur d'application, jusqu'à ce qu'il reçoive un autre appel GuardAppUser ou un appel GuardAppUserReleased, entraînant l'effacement du nom d'utilisateur d'application.

Pour signaler l'occurrence d'autres événements (vous pouvez définir les types d'événement en fonction de vos besoins), utilisez l'appel GuardAppEvent décrit dans la section ci-après.

Syntaxe : SELECT 'GuardAppUser:nom_utilisateur' FROM emplacement

nom_utilisateur est une chaîne contenant le nom d'utilisateur d'application. Cette chaîne sera la valeur de l'attribut Application User dans l'entité Access Period.

FROM emplacement est utilisé uniquement pour Oracle, DB2 et Informix. (Omettez ce paramètre pour les autres types de base de données). Il doit être entré exactement comme suit :

- Oracle : FROM DUAL
- DB2 : FROM SYSIBM.SYSDUMMY1
- Informix : FROM SYSTABLES

Effacement de l'utilisateur d'application via GuardAppUserReleased

Utilisez l'appel GuardAppUserReleased pour signaler que l'utilisateur en cours a abandonné le contrôle de la connexion. Guardium effacera le nom d'utilisateur d'application, qui restera vide pour la connexion jusqu'à réception d'un autre appel GuardAppUser.

Syntaxe : SELECT 'GuardAppUserReleased' FROM emplacement

FROM emplacement est utilisé uniquement pour Oracle, DB2 et Informix. (Omettez ce paramètre pour les autres types de base de données). Il doit être entré exactement comme suit :

- Oracle : FROM DUAL
- DB2 : FROM SYSIBM.SYSDUMMY1
- Informix : FROM SYSTABLES

Définition d'un événement d'application via GuardAppEvent

Cet appel permet de signaler de façon plus générique les événements d'application qui surviennent. Vous pouvez définir vos propres types d'événement et fournir des valeurs textuelle, numérique ou de date à stocker avec l'événement, au début et à la fin de l'événement. Vous pouvez utiliser cet appel conjointement avec l'appel GuardAppUser. Guardium attribuera toutes les activités ayant lieu sur la connexion à cet événement d'application jusqu'à réception d'une autre commande GuardAppEvent:Start ou d'une commande GuardAppEvent:Released.

Syntaxe :

SELECT 'GuardAppEvent:Start|Released',

'GuardAppEventType:type',

'GuardAppEventUserName:nom',

'GuardAppEventStrValue:chaîne',

'GuardAppEventNumValue:nombre',

'GuardAppEventDateValue:date' FROM emplacement

Start | Released - Utilisez le mot clé Start pour indiquer que l'événement prend le contrôle de la connexion ou le mot clé Released pour indiquer que l'événement a abandonné le contrôle de la connexion.

type identifie le type d'événement. Il peut s'agir d'une valeur de chaîne, par exemple Connexion, Déconnexion, Crédit, Débit, etc. Dans l'entité Application Events, cette valeur est stockée dans l'attribut Event Type pour un appel Start ou dans l'attribut Event Release Type pour un appel Released.

nom est une valeur de nom d'utilisateur à définir pour cet événement. Dans l'entité Application Events, cette valeur est stockée dans l'attribut Event User Name pour un appel Start et dans l'attribut Event Release User Name pour un appel Released.

chaîne est une valeur de chaîne à définir pour cet événement. Par exemple, pour un événement Connexion, vous pouvez fournir un nom de compte. Dans l'entité Application Events, cette valeur est stockée dans l'attribut Event Value Str pour un appel Start et dans l'attribut Event Release Value Str pour un appel Released.

nombre est une valeur numérique à définir pour cet événement. Par exemple, pour un événement Crédit, vous pouvez indiquer le montant de la transaction. Dans l'entité Application Events, cette valeur est stockée dans l'attribut Event Value Num pour un appel Start et dans l'attribut Event Release Value Num pour un appel Released.

date est une date (avec une heure facultative) fournie par l'utilisateur pour cet événement. Elle doit être au format aaaa-mm-jj hh:mm:ss, où la partie heure (hh:mm:ss) est facultative. Il peut s'agir de la date et de l'heure en cours ou d'une valeur provenant d'une transaction dont vous assurez le suivi. Dans l'entité Application Events, cette valeur est stockée dans l'attribut Event Date pour un appel Start et dans l'attribut Event Release Date pour un appel Released.

FROM emplacement est utilisé uniquement pour Oracle, DB2 et Informix. (Omettez ce paramètre pour les autres types de base de données). Reportez-vous à l'exemple ci-après. Toutefois, tout nom de table factice est acceptable pour une instruction SQL factice.

- Oracle : FROM DUAL
- DB2 : FROM SYSIBM.SYSDUMMY1
- Informix : FROM SYSTABLES

L'appel GuardAppEvent remplit une entité Application Events (voir Entité Application Events dans la section Entités et Attributs des annexes). Lorsque vous créez des requêtes et des rapports Guardium, vous pouvez accéder à l'entité Application Events depuis le domaine Suivi des accès ou Violations de politique.

Si l'un des attributs de l'entité Application Events n'a pas été défini à l'aide de l'appel GuardAppEvent, ces valeurs sont vides.

Concernant les deux attributs de date :

- La date d'événement (Event Date) est définie à l'aide de l'appel GuardAppEvent ou depuis une procédure d'identification personnalisée, comme décrit dans la section ci-après.
- L'horodatage (Timestamp) est la date et l'heure auxquelles Guardium stocke l'instance de l'entité Application Events.

Rubrique parent : Identification de l'utilisateur

Identification d'utilisateurs via des procédures stockées

Dans de nombreuses applications existantes, toutes les informations nécessaires à l'identification d'un utilisateur d'application peuvent être obtenues depuis le trafic de base de données existant, à partir d'appels de procédure stockée. Une fois que Guardium sait quels sont les appels à surveiller et quels sont les paramètres qui contiennent le nom d'utilisateur ou d'autres informations intéressantes, les utilisateurs peuvent être identifiés automatiquement.

Dans le cas le plus simple, une application peut comporter une procédure stockée unique qui définit plusieurs valeurs de propriété, dont l'une est le nom d'utilisateur. Un appel permettant de définir le nom d'utilisateur peut ressembler à :

```
set_application_property('user_name', 'JohnDoe');
```

Dans un mappage de procédure personnalisée (décrit ultérieurement), vous pouvez demander à Guardium de :

- Surveiller une procédure stockée appelée set_application_property, avec la valeur user_name pour le premier paramètre.
- Associer l'utilisateur d'application à la valeur du deuxième paramètre dans l'appel (JohnDoe dans l'exemple).

Plusieurs procédures stockées peuvent exister pour une application : l'une pour démarrer une session d'utilisateur d'application, une autre pour mettre fin à une session, et d'autres pour signaler des événements essentiels propres à cette application. Le mécanisme de procédure d'identification personnalisée de Guardium peut être utilisé pour assurer le suivi des événements d'application que vous voulez surveiller.

Etant donné que chacune de vos applications identifier peut-être les utilisateurs avec une méthode différente, il peut être nécessaire de définir des mappages de procédure d'identification personnalisée distincts pour chaque application. Pour ce faire, procédez comme suit.

Définition d'un mappage de procédure d'identification personnalisée

1. Accédez à Protection > Détection d'intrusion de base de données > Procédures d'identification personnalisées.
2. Pour afficher un mappage existant, placez le pointeur de votre souris sur la colonne En savoir plus pour la ligne contenant la carte à afficher.
3. Pour ajouter un mappage, cliquez sur Ajouter.
4. Dans la zone Nom de carte personnalisée, entrez le nom à utiliser pour ce mappage.
5. Dans la zone Nom de procédure, entrez le nom de la procédure de base de données qui fournira les informations.
6. Sélectionnez Définir ou Effacer dans la liste d'actions pour indiquer si l'appel de procédure définira ou effacera les valeurs d'application. Le champ Position de type d'événement est utilisé de façon particulière lorsque l'action Effacer est sélectionnée.
7. Si les informations de l'application peuvent être obtenues à partir d'un appel de procédure stockée, mais uniquement sous une ou deux conditions :
   - Utilisez une zone d'emplacement de condition pour spécifier quel paramètre d'appel de procédure stockée doit être testé.
   - Utilisez la zone de valeur de condition correspondante afin de spécifier la valeur qui doit être mise en correspondance pour définir les informations de l'application depuis un ou plusieurs des autres paramètres.
   - Par exemple, supposez qu'une procédure stockée appelée set_context est utilisée par une application afin de définir plusieurs valeurs, dont l'une est le nom d'utilisateur. Trois paramètres sont transmis à la procédure : un nom d'application, un nom de propriété et une valeur. Trois appels classiques sont illustrés :
     - set_context('publishing_application', 'role_name', 'manager');
     - set_context('publishing_application', 'user_name', 'jsmith');
     - set_context('publishing_application', 'company', 'guardium');
   - Dans les exemples, la deuxième instruction représente le format de l'appel qui nous intéresse. Le deuxième paramètre (le nom de propriété) est le paramètre à tester ; par conséquent, le chiffre 2 doit être entré dans la zone d'emplacement de Condition1 et user_name doit être entré dans la zone de valeur de Condition1.
   - Si un deuxième format de l'appel définit également le nom d'utilisateur, les zones d'emplacement et de valeur de Condition2 peuvent être utilisées. Par exemple, supposez que le format suivant de l'appel de procédure est parfois utilisé pour définir un nom d'utilisateur :
     - set_context('admin_application', 'admin_name', 'wjones');
   - Pour utiliser cette procédure, afin de définir le nom d'utilisateur d'application, entrez 2 dans la zone d'emplacement de Condition2 et admin_name dans la zone de valeur de Condition2.
     Remarque : Si deux conditions sont utilisées, le nom d'utilisateur ou toute autre information extraite doit se trouver à la même position de paramètre dans les deux types d'appel.
8. Pour une action Effacer :
   - Utilisez uniquement les champs Position de type d'événement et Position de nom d'utilisateur d'application.
   - Effectuez l'une des opérations suivantes :
     - Pour effacer l'événement d'application : définissez 1 pour Position de type d'événement et 0 pour Position de nom d'utilisateur d'application.
     - Pour effacer l'utilisateur d'application : définissez 0 pour Position de type d'événement et 1 pour Position de nom d'utilisateur d'application.
9. Pour une action Définir, utilisez la sous-fenêtre Position de paramètre pour indiquer quels paramètres de procédure stockée et quels attributs d'événement d'application Guardium mapper. Le numéro du premier paramètre de procédure est 1. Utilisez 0 (zéro, par défaut) pour tous les attributs qui ne sont pas définis par l'appel. Position de nom d'utilisateur d'application – Entrez la position de paramètre du nom d'utilisateur d'application à associer à l'activité de base de données à partir de ce point (jusqu'à la réinitialisation, comme décrit précédemment). Position de valeur de chaîne d'événement – Entrez la position de paramètre d'une valeur de chaîne pour un événement (pour une connexion, il peut s'agir d'un nom d'utilisateur ou de compte). Position de valeur numérique d'événement – Entrez la position de paramètre d'une valeur numérique pour l'événement (pour une transaction, il peut s'agir d'un montant en dollars). Position de type d'événement – Entrez la position de paramètre d'un nom pour le type d'événement (Connexion, Déconnexion, Demande de crédit, etc.). Position de date d'événement – Entrez la position de paramètre d'une valeur de date/heure pour l'événement. Le format doit être aaaa-mm-jj hh:mm:ss. La partie heure (hh:mm:ss) est facultative et si elle est omise, est 00:00:00.
10. Dans la sous-fenêtre Informations sur le serveur : sélectionnez le type de serveur de base de données dans la liste Type de serveur. Entrez le nom d'utilisateur de base de données dans la zone Nom d'utilisateur de base de données. Facultatif : entrez un nom de base de données dans la zone Nom de base de données. Si vous l'omettez, toutes les bases de données sont surveillées. Facultatif : identifiez un ou plusieurs serveurs. Si aucun serveur n'est spécifié, tous les serveurs sont

surveillés. Pour sélectionner un serveur spécifique seulement, entrez l'adresse IP du serveur et le masque de réseau dans les zones IP serveur et Masque de réseau serveur ou bien, pour sélectionner un groupe de serveurs, sélectionnez un groupe de serveurs dans la liste Groupe IP serveur ou cliquez sur le bouton Groupes pour définir un nouveau groupe de serveurs.

11. Lorsque vous avez terminé, cliquez sur le bouton Ajouter pour ajouter le mappage à la liste.

Rubrique parent : Identification de l'utilisateur

Audit des changements de valeurs

La fonction Audit des changements de valeurs permet de suivre les changements apportés aux valeurs dans les tables de base de données.

La fonction Audit des changements de valeurs permet de suivre les changements apportés aux valeurs dans les tables de base de données. Pour chaque table dans laquelle les changements doivent être suivis, vous choisissez quelles commandes SQL de changement de valeur (insert, update, delete) sont à surveiller. Chaque fois qu'une telle commande est exécutée sur une table sous surveillance, les valeurs avant et après traitement sont capturées. Les activités de changement sont transférées périodiquement à un système Guardium, sur lequel toutes les fonctions de reporting et d'alerte peuvent être utilisées. L'utilisation de la fonction Audit des changements de valeurs passe par les étapes élémentaires suivantes :

1. Créez une base de données d'audit sur le serveur de base de données. C'est dans cette base de données que seront stockées les données de changement de valeurs en attendant leur transfert au système Guardium. Voir Création d'une base de données d'audit.
2. Identifiez les tables à surveiller et, pour chacune d'elles, sélectionnez les commandes de changement de valeurs (insert, delete, update) dont les occurrences devront être enregistrées. Un déclencheur est créé pour chaque table à surveiller. Il servira à écrire les données de changement de valeurs dans la base de données d'audit. Pour que le déclencheur puisse mettre à jour la base de données d'audit, tous les utilisateurs ayant des privilèges de mise à jour sur la table surveillée reçoivent des privilèges appropriés sur la base de données d'audit. Cela a des conséquences sur les utilisateurs qui n'ont pas encore de privilèges de mises à jour sur cette table et qui les reçoivent plus tard (voir l'étape 4). Pour des instructions détaillées sur la manière de définir les activités de surveillance, consultez la section Définir les activités de surveillance.
3. Programmez les téléchargement visant à transférer les données de changement de valeurs du serveur de bases de données au système Guardium. Consultez la section Programmer les téléchargements des changements de valeurs.
4. Mettez à jour les privilèges d'accès à la base de données d'audit. Après la création du déclencheur associé à une table surveillée, il peut arriver qu'un utilisateur reçoive un accès à cette table qu'il n'avait pas au moment où ce déclencheur a été créé. Si cet utilisateur émet une commande de changement de valeur surveillée, cette commande échouera, car l'utilisateur n'aura pas reçu les privilèges lui permettant de mettre à jour la base de données d'audit. Consultez la section Tenir à jour les listes d'utilisateurs privilégiés.
5. Surveillez les activités de changement depuis la console d'administration ou utilisez le domaine de requête Suivi des changements de valeurs pour créer des rapports personnalisés sur le dispositif (appliance) Guardium. Consultez la section Créer des rapports sur les changements de valeurs.

Définir les activités de surveillance

Après avoir défini une base de données d'audit, utilisez le Générateur d'audit des changements de valeurs pour désigner les tables à surveiller et sélectionner les types de changement (insertions, mises à jour, suppressions) à enregistrer.

1. Ouvrez le Générateur d'audit des changements de valeurs en suivant le trajet Renforcer > Contrôle des changements de configuration (Application CAS) > Générateur d'audit des changements de valeurs.
2. Cliquez sur Ajouter une source de données pour ouvrir le panneau Localiseur de source de données.
3. Sélectionnez une source de données par rapport à laquelle une base de données d'audit est définie. Si aucune base de données d'audit n'est encore définie, consultez Création d'une base de données d'audit.
4. Cliquez sur Ajouter pour fermer le localisateur et ajouter la source de données sélectionnée au panneau Audit des changements de valeurs.
5. Au besoin, entrez un Propriétaire de schéma et/ou un Nom d'objet pour limiter le nombre de tables affichées lorsque vous choisissez les tables à surveiller. Vous pouvez utiliser le caractère générique % (signe pour cent). Par exemple, pour afficher seulement les tables dont le nom commence par la lettre a, entrez `a%` dans la zone Nom d'objet.
6. Cliquez sur Choisir les tables à surveiller pour ouvrir le panneau Définir un audit de données.
7. Cochez la case Sélectionner pour chaque table à surveiller.
   Remarque : Vous ne pouvez pas définir de déclencheur pour une table contenant un ou plusieurs types de données définis par l'utilisateur.

   La colonne Déclencheur défini indique si un déclencheur est déjà défini pour la table. Chacune des cases à cocher Auditer les insertions, Auditer les suppressions et Auditer les mises à jour indique si les déclencheur enregistrera les changements opérés par la commande correspondante (insert, delete et update, respectivement).

   Si la colonne Déclencheur défini ne contient pas de marque pour une table, le fait de cocher la case Sélectionner pour cette table coche automatiquement les trois cases Auditer les insertions, Auditer les suppressions et Auditer les mises à jour. Si vous ne souhaitez pas surveiller l'une de ces commandes, décochez la case correspondante.

8. Cliquez sur Ajouter des sélections pour définir des déclencheurs pour les tables sélectionnées. Vous serez informé des mesures prises.
9. Cliquez sur OK pour fermer la boîte de message et réafficher le panneau Définir un audit de données. Les tables sélectionnées demeurent sélectionnées et la colonne Déclencheur défini est à présent marquée pour ces tables. Notez que dès l'instant où il est défini, le déclencheur associé à une table est actif et déclenche l'enregistrement, dans la base de données d'audit, des changements effectués sur cette table par les commandes sélectionnées. La configuration des déclencheurs est entièrement réalisée sur le serveur de base de données, contrairement à la plupart des autres configurations Guardium, qui sont définies dans la base de données Guardium et sont ensuite activées ou désactivées en tant que tâches séparées.
10. Pour définir d'autres actions, répétez ces étapes. Vous pouvez aussi supprimer un ou plusieurs déclencheurs en cochant leur case Sélectionner et en cliquant sur Supprimer des sélections.
11. Cliquez sur Terminé une fois tous vos changements terminés.
    Remarque : Le bouton Annuler n'inverse pas les changements que vous avez apportés aux déclencheurs en utilisant les boutons Ajouter des sélections et Supprimer des sélections.

Après la définition des activités de surveillance

Si vous avez ajouté pour la première fois des activités de surveillance des changements de valeurs à une source de données, vous devez créer un planning des téléchargements pour celle-ci, car la base de données d'audit associée ne sera vidée que lorsque les données qui y ont été enregistrées auront été transférées au système Guardium. Consultez la section suivante.

Programmer les téléchargements des changements de valeurs

1. Ouvrez le Générateur d'audit des changements de valeurs en suivant le trajet Renforcer > Contrôle des changements de configuration (Application CAS) > Générateur d'audit des changements de valeurs.
2. Sélectionnez la source de données d'audit pour laquelle vous voulez programmer les téléchargements et cliquez sur Planifier le téléchargement pour ouvrir le planificateur de tâches général. Si vous avez besoin d'aide pour définir un planning, consultez la partie correspondante dans le manuel des outils communs.

Tenir à jour les listes d'utilisateurs privilégiés

Lorsque la fonction d'audit des changements de valeurs ajoute un déclencheur à une table de base de données, tous les utilisateurs du moment autorisés à mettre à jour cette table reçoivent l'autorisation de mettre à jour les tables de la base de données d'audit. C'est une nécessité dans la mesure où le déclencheur doit pouvoir mettre à jour la base de données d'audit afin d'y consigner les changements (anciennes et nouvelles valeurs). Or, si un nouvel utilisateur reçoit, après coup, l'autorisation de mettre à jour une table déjà placée sous surveillance et s'il tente une mise à jour sur cette table, elle lui est refusée, car il n'a pas l'autorisation de mettre à jour la base de données d'audit. Dans ces conditions, vous devez actualiser la liste des utilisateurs privilégiés de la base de données d'audit en utilisant le Générateur d'audit des changements de valeurs.

Pour que la liste des utilisateurs privilégiés de la base de données d'audit puisse être actualisée, il faut que l'ID utilisateur de base de données servant à se connecter à la base de données surveillée soit également le créateur de tout rôle auquel les nouveaux utilisateurs ont été ajoutés. Autrement, les membres de ce rôle ne seront pas disponibles.

1. Ouvrez le Générateur d'audit des changements de valeurs en suivant le trajet Renforcer > Contrôle des changements de configuration (Application CAS) > Générateur d'audit des changements de valeurs.
2. Cliquez sur Ajouter une source de données pour ouvrir le panneau Localiseur de source de données, sélectionnez la source de données appropriée dans la liste et cliquez sur Ajouter.
3. Cliquez sur Mettre à jour les utilisateurs privilégiés des tables d'audit. La liste des utilisateurs autorisés à exécuter des déclencheurs pour mettre à jour les tables de la base de données d'audit est alors actualisée et vous êtes informé de l'achèvement de l'opération.
4. Cliquez sur OK pour fermer la boîte de message.

Créer des rapports sur les changements de valeurs

Les données sur les changements de valeurs sont consultables dans le rapport par défaut Valeurs changées. Vous pouvez aussi créer vos propres rapports en utilisant le domaine Suivi des changements de valeurs. Par défaut,, le domaine Suivi des changements de valeurs est limité aux utilisateurs ayant le rôle d'administrateur.

Rapport par défaut Valeurs changées

Un seul rapport par défaut Valeurs changées est disponible. Vous pouvez y accéder en suivant le trajet Rapports > Rapports opérationnels Guardium en temps réel > Valeurs changées.

La principale entité suivie dans le rapport Valeurs changées est l'entité Colonnes changées. Dans la plupart des cas, chaque changement de colonne détecté, pour chaque action auditée (Insert, Update, Delete), fait l'objet d'une ligne de rapport. Cependant, dans le cas d'une base de données MS SQL Server ou Sybase, si la table surveillée n'a pas de clé primaire, chaque changement fait l'objet de deux lignes de rapport, une pour l'ancienne valeur et l'autre pour la nouvelle valeur.

Rubrique parent : Surveillance et audit

Création d'une base de données d'audit

Créez une base de données d'audit et utilisez-la pour vos activités de surveillance des changements de valeurs.

Pour créer une base de données d'audit et l'utiliser pour vos activités de surveillance des changements de valeurs, vous devez posséder un compte d'utilisateur avec les autorisations appropriées pour :

- Créer une base de données sur le serveur
- Créer un compte d'utilisateur de base de données sur le serveur

- Vous connecter à chaque base de données à surveiller - Créer des tables et des déclencheurs sur chaque base de données à surveiller

Avant de définir une base de données d'audit sous Informix ou Sybase

Dans le cas d'un système de gestion de base de données Informix ou Sybase (excepté pour Sybase IQ, qui ne gère pas les déclencheurs) et selon le type de système d'exploitation du serveur de base de données, vous devez effectuer l'une des procédures suivantes avant de définir la base de données d'audit.

Configuration Informix - Localiser un espace de base de données existant ou en créer un nouveau

Cette partie s'applique à Informix (version 9.4 ou ultérieure). Avec Informix, il est fortement déconseillé d'utiliser l'espace de base de données racine par défaut, root_dbs. Cet espace ne peut pas être supprimé (drop) ni réduit en taille.

Vous devez utiliser un autre espace de base de données déjà défini ou créer un nouvel espace. Dans ce dernier cas, appliquez l'une des procédures suivantes (à choisir en fonction du système d'exploitation).

Informix - Créer un espace de base de données Informix sur un serveur Windows Server

Cette procédure se déroule en dehors de l'interface utilisateur de Guardium et s'applique à Informix version 9.4 ou ultérieure.

1. Vérifiez que le serveur de base de données est en ligne et à l'écoute.
2. Créez un fichier de zéro octet nommé guardium_dbs_dat.000 dans le répertoire C:\IFMXDATA\nom_serveur (nom_serveur étant le nom du serveur Informix ou son nom de service). Vous pouvez pour cela sauvegarder un fichier texte vide et le renommer en pensant à remplacer son extension txt par 000.
3. Faites du répertoire suivant le répertoire de travail.

   C:\Program Files\Informix\bin

4. Exécutez la commande suivante :

```
C:\Program Files\Informix\bin>onspaces -c -d guardium_dbs -p C:\IFMXDATA\nom_serveur\guardium_dbs_dat.000 -o 0 -s 150000
```

Si le fichier a été créé correctement, vous devriez voir le message suivant :

```
Verifying physical disk space, please wait ...
Space successfully added.
** WARNING **  A level 0 archive of Root DBSpace will need to be done.
```

5. Redémarrez le serveur Informix et utilisez un outil adapté (par exemple, le client distant Aqua Data Studio) pour vous connecter et vérifier que l'espace nommé guardium_dbs a bien été créé. Il est possible que votre première tentative de connexion échoue et se solde par un message signalant que le serveur fonctionne en mode repos (Quiescent).Si cela arrive, faites une nouvelle tentative de connexion. En cas de nouvel échec, recommencez au moins une fois. La connexion devrait finir par s'établir.
6. Pour vérifier que l'espace de base de données guardium_dbs a été créé, utilisez Aqua Data Studio et regardez sous Storage.

Informix - Créer un espace de base de données Informix sur un serveur Unix

Cette procédure se déroule en dehors de l'interface utilisateur de Guardium et s'applique à Informix version 9.4 ou ultérieure.

1. A partir d'une fenêtre de ligne de commande, entrez les commandes suivantes :

```
su - informix
cd demo/server
vi guardium_dbs
```

2. Sans ajouter aucun texte, sauvegardez le fichier guardium_dbs vide.
3. Entrez les commandes suivantes :

```
chmod 660 guardium_dbs
cd ../../bin
onspaces -c -d guardium_dbs -p /home/informix10/demo/server/guardium_dbs -o 0 -s 100000
```

Configuration Sybase - Initialiser les disques

Cette partie s'applique uniquement aux serveurs Sybase (mais pas à Sybase IQ, qui ne gère pas les déclencheurs). Pour initialiser les disques, effectuez l'une des procédures suivantes, à choisir en fonction du type de système d'exploitation du serveur de base de données.

Sybase - Initialiser les disques sur un serveur Sybase sous Windows

1. Connectez-vous au serveur sur lequel vous comptez créer la base de données d'audit Guardium : guardium_audit.
2. Sous le lecteur c:, créez un dossier nommé guardium_audit.
3. Connectez-vous à la base de données.
4. Exécutez les commandes suivantes :

```
use master
go
disk init name="guardium_auditdev", size=8192
go
disk init name="guardium_auditlog",
physname="c:/guardium_audit/guardium_auditlog", size=8192
go
```

Sybase - Initialiser les disques sur un serveur Sybase sous Unix

1. Connectez-vous à la base de données.
2. Exécutez les commandes suivantes :

```
use master
go
disk init name = 'guardium_auditdev', physname
 ='/home/sybase/data/guardium_auditdev' , size = 8192
go
disk init name = 'guardium_auditlog', physname
 ='/home/sybase/data/guardium_auditlog' , size = 8192
go
```

Créer la base de données

Dans le cas d'un système Informix ou Sybase, assurez-vous d'avoir effectué les tâches préliminaires avant d'aborder cette procédure.

1. Ouvrez le Générateur d'audit des changements de valeurs en suivant le trajet Renforcer > Contrôle des changements de configuration (Application CAS) > Création de base de données d'audit des changements de valeur.
2. Cliquez sur Ajouter une source de données pour ouvrir le panneau Localiseur de source de données. Les sources de données dont la définition provient de l'application Audit des changements de valeurs sont libellées comme sources de surveillance des valeurs. Celles qui ont été définies pour d'autres applications seront libellées différemment (par exemple, Ecouteur ou Analyseur de base de données). Ces sources ne sont peut-être pas configurées avec un jeu d'autorisations d'accès aux données convenant à l'application Audit des changements de valeurs, qui nécessite un compte d'utilisateur ayant l'autorité d'administrateur de base de données. Si aucune source de données adaptée n'est disponible, cliquez sur le bouton Nouveau pour créer une nouvelle source pour la base de données à surveiller (pour des informations détaillées sur la définition de sources de données, consultez Sources de données dans le manuel des outils communs).
   Remarque : Si une base de données GUARDIUM_AUDIT est déjà créée sur ce serveur de bases de données, il n'est pas possible d'en créer d'autre tant que vous n'avez pas supprimé (drop) la combinaison base de données GUARDIUM_AUDIT/utilisateur. Après quoi vous pouvez en créer une nouvelle.
3. Sélectionnez une source de données qui utilise un compte d'administrateur et cliquez sur Ajouter pour l'ajouter au volet Sources de données, dans le panneau Créer une base de données d'audit des changements de valeurs.
4. Entrez un Nom de source de données d'audit. C'est par ce nom que sera identifiée la source de données lors de la définition des tâches de surveillance ainsi que pour le transfert des données. Ne confondez pas ce nom avec celui de la source de données figurant dans le panneau Sources de données.
5. Au besoin, cochez la case Partager la source de données si vous voulez que cette source de données puisse être partagée avec d'autres applications (Classification, par exemple). Par défaut, elle ne l'est pas. Ce type de source de données fonctionnant avec des privilèges d'administrateur, il est peut-être prudent de ne pas la partager avec les autres applications.
   Remarque : Pour partager une source de données avec d'autres utilisateurs, associez-lui des rôles de sécurité.

6. Excepté pour le type de base de données DB2, d'autres champs sont à renseigner dans le panneau Configuration d'audit. Tous sont obligatoires. Entrez les valeurs appropriées en vous référant au tableau suivant.

Tableau 1. Autres champs à renseigner dans la configuration d'audit

Type de base de données	Libellé du champ : description
Informix	**Espace de base de données** : entrez le nom de l'espace de base de données à utiliser. Il peut s'agir d'un espace existant ou de celui que vous avez créé pour la base de données d'audit (et que nous avons appelé guardium_dbs dans l'exemple précédent). Si vous laissez ce champ en blanc, l'espace par défaut root_dbs sera utilisé. Nous déconseillons ce choix.
MS SQL Server	**Nom d'utilisateur d'audit** : entrez un nouveau nom d'utilisateur de base de données qui servira pour l'accès à la base de données d'audit. Cet utilisateur recevra le rôle sysadmin. **Mot de passe d'audit** : entrez un mot de passe. Lorsque la source de données est MSSQL Server (et uniquement dans ce cas), un choix supplémentaire apparaît dans le menu Création de base de données d'audit des changements de valeurs. Mode compatibilité : les choix disponibles sont Valeur par défaut et MSSQL 2000. Le processeur est informé du mode de compatibilité à utiliser lors de la surveillance d'une table. Utilisez la commande GuardAPI grdapi list_compatibility_modes pour afficher la liste des modes disponibles pour MS SQL Server.
Oracle	**Mot de passe d'audit** : entrez le mot de passe de l'utilisateur système, qui sera le compte de base de données utilisé pour accéder à la base de données d'audit. **Espace table par défaut** : entrez un nom pour l'espace table par défaut. **Espace table temp**: entrez un nom pour l'espace table temporaire.
Sybase	**Nom d'utilisateur d'audit** : entrez un nouveau nom d'utilisateur de base de données qui servira pour l'accès à la base de données d'audit. Cet utilisateur recevra le rôle sa_role. **Mot de passe d'audit** : entrez un mot de passe. **Nom d'unité de données** : entrez le nom d'unité que vous avez choisi lors de l'initialisation du disque réservé aux données de la base de données d'audit (dans la procédure d'initialisation des disques décrite précédemment, nous avons choisi le nom guardium_auditdev). **Nom d'unité de consignation** : entrez le nom d'unité que vous avez choisi lors de l'initialisation du disque réservé aux journaux de la base de données d'audit (dans la procédure d'initialisation des disques décrite précédemment, nous avons choisi le nom guardium_auditlog).

7. Cliquez sur Créer une base de données d'audit pour créer la base de données d'audit.
8. Pour accéder aux actions décrites dans le tableau suivant, utilisez la sélection Mise à jour et téléchargement de base de données d'audit des changements de valeurs sous l'onglet Configuration et contrôle.

Action	Description
Supprimer	Cliquez pour retirer la source de données du panneau Sources de données.
Modifier	Cliquez pour éditer cette définition de source de données dans le panneau Définition de source de données.
Planifier le téléchargement	Cliquez pour programmer le transfert de la base de données d'audit associée à cette source de données.

Après la définition de la base de données d'audit

Une fois créée sur un serveur de base de données, la base de données d'audit devient utilisable par le Générateur d'audit des changements de valeurs, outil qui sert à construire des déclencheurs. Voir Audit des changements de valeurs.

Rubrique parent : Surveillance et audit

Surveillance de l'accès aux tables

Cette fonction ajoute un champ “Last Assessed” dans les tables pertinentes, pour l'interaction avec les produits de gestion du cycle de vie des données Optim Designer.

Cette fonction est également appelée “Table Last Referenced”.

Cette fonction utilise le flux externe de Guardium qui est préconfiguré avec les données (une mappe de flux externe prédéfinie), et un processus d'audit pour l'exécuter.

Procédure

1. Créez les tables cible (Optim) dans une base de données Informix. Utilisez le script.
2. Ouvrez le générateur de processus d'audit en sélectionnant Conformité > Outils et vues > Générateur de processus d'audit, puis éditez le processus nommé Table Last Referenced. Ajoutez une source de données à la tâche Flux externe (la source de données Informix contenant les tables) et configurez le paramètre d'exécution pour le groupe de serveurs. Les autres paramètres sont prédéfinis et il n'est pas nécessaire de les changer.
3. Exécutez le processus d'audit (ou planifiez son exécution régulière).

Remarque : La table générée affiche uniquement la dernière exécution. Le nombre de récepteurs correspond au nombre de récepteurs, et non au nombre de résultats d'exécution depuis la dernière exécution seulement.

IBM Guardium peut détecter les références externes à des objets de base de données, notamment des tables. Vous pouvez utiliser cette capacité, en conjonction avec Optim Designer, pour gérer le retrait des tables inactives ou l'archivage avec certaines règles de conservation.

Guardium collecte et gère une liste de tables incluant la date de la dernière référence. Cette liste est générée à l'aide de règles dans Guardium qui régissent l'intervalle pour la dernière référence et la fréquence de mise à jour du contenu de la liste. Les informations capturées par Guardium constituent la liste .dernière référence.. et

répondent aux questions suivantes : Quelles sont les tables qui ne sont plus référencées ? Quelles sont les tendances d'accès aux tables qui existent pour les candidats au retrait ?

Le fait de pouvoir planifier précisément le retrait d'applications vous permet de :

- Planifier le retrait ou le redéploiement de matériel
- Réduire le coût de propriété en déplaçant ou en retirant les ressources prenant en charge les applications (par exemple le matériel, l'administrateur ou les administrateurs de base de données, les propriétaires d'application ou les opérations informatiques telles que les sauvegardes)
- Savoir quelles sont les tables rarement ou jamais consultées

Cette fonctionnalité d'IBM Guardium a été ajoutée directement à l'interface utilisateur d'Optim Designer.

Les informations fournies par Guardium à Optim incluent les attributs suivants pour chaque entrée de table :

Tableau 1. Entrée de la liste d'accès aux tables surveillées

Entrée de liste	Description
Champ	Commentaire
Description de source de données	Description
Adresse IP du serveur	
Nom d'hôte	
Fournisseur de base de données	Par exemple, Oracle, DB2
Nom d'utilisateur	Par exemple, pour Oracle, il définit principalement le schéma
Nom de base de données	
Schéma	
Table	
Date	Date du dernier accès

Script de création de tables Informix dans le produit Optim

Last_referenced_datasource

```
create table last_referenced_datasource (
   id              serial(1) not null,
   datasource_desc    varchar(100),
   server_ip         char(39),
   host_name          varchar(200),
   db_vendor         char(40),
   primary key (id) constraint last_referenced_datasource_pk
);
```

Last_referenced_table

```
create table last_referenced_table (
   id              serial(1) not null,
   datasource_id      int not null,
   user_name         char(32),
   db_name           char(128) not null,
   schema_name        char(128) not null,
   table_name        char(128) not null,
   last_reference     datetime year to second not null,
   primary key (id) constraint last_referenced_table_pk,
   foreign key (datasource_id) references last_referenced_datasource(id) constraint last_referenced_table_fk
);
```

Rubrique parent : Surveillance et audit

Configuration rapide de la surveillance de conformité

Après avoir déployé vos agents de surveillance (S-TAP), utilisez l'outil Surveillance de conformité pour surveiller votre environnement et s'assurer qu'il respecte des normes de sécurité et des réglementations spécifiques.

Guardium fournit plusieurs modèles de surveillance de conformité--groupes, politiques de sécurité et rapports correspondant à différentes normes et réglementations spécifiques--notamment les suivants :

- Basel Committee on Banking Supervision (Comité de Bâle sur le contrôle bancaire) (BASEL II)
- General Data Protection Regulation (Règlement général sur la protection des données) (GDPR)
- General Data Protection Regulation pour Db2 for z/OS (GDPR pour Db2 for z/OS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Security Standard (Norme de sécurité de l'industrie des cartes de paiement) (PCI)
- Personally Identifiable Information (Données personnelles identifiables) (PII)
- Sarbanes-Oxley Compliance (Conformité à la Loi Sarbanes-Oxley) (SOX)

Ces modèles de surveillance de conformité permettent aux organisations d'être rapidement opérationnelles. A ce titre, ils sont particulièrement utiles à celles qui ont peu de temps pour se mettre en conformité avec l'une des normes ou réglementations couvertes. Une fois les politiques de sécurité installées, l'outil de surveillance de conformité guide les administrateurs ou "compliance officers" à travers la création de groupes qu'ils doivent ensuite remplir avec les informations spécifiques de l'organisation, telles que les adresses IP des clients et les ID utilisateur titulaires de privilèges particuliers. L'outil vérifie également votre environnement Guardium à intervalles réguliers afin d'identifier les nouvelles bases de données susceptibles d'être mises sous surveillance avec les modèles de surveillance de conformité.
Une fois le modèle de surveillance de conformité choisi, dès lors que vous avez indiqué les bases de données où ce type de conformité doit être appliqué, l'outil de surveillance de conformité effectue les opérations suivantes :

- Une politique de sécurité est créée et installée pour le type de conformité sélectionné. Dans un environnement à gestion centralisée, la politique est installée sur les collecteurs.
- Un planning d'installation de politique est défini pour une exécution quotidienne à 10:30. Dans un environnement à gestion centralisée, ce planning est exécuté sur les collecteurs.
- Un groupe d'IP de serveur est peuplé avec les adresses IP de serveur des bases de données sélectionnées.
- L'utilisateur en cours se voit attribuer le rôle correspondant au type de conformité sélectionné. Il a ainsi accès aux rapports et accélérateurs associés à partir de la navigation Guardium principale.
- Un scénario de découverte des données sensibles est créé, s'il est pris en charge par le type de conformité.
- Si un scénario de découverte des données sensibles est créé et qu'au moins une des bases de données sélectionnées a une source de données de définie, le scénario est programmé pour être exécuté chaque dimanche à 10:30. Dans un environnement à gestion centralisée, le planning est exécuté sur le gestionnaire central.

Le tableau suivant récapitule les fonctionnalités prises en charge pour chacun des types de conformité :

Tableau 1. Récapitulatif des fonctionnalités prises en charge par l'outil Surveillance de conformité pour chaque type de conformité.

	Basel II	GDPR	HIPAA	PCI	PII	SOX
Politique de sécurité	✓	✓	✓	✓	✓	✓
Rapports	✓	✓		✓	✓	✓
Scénario de découverte des données sensibles		✓		✓	✓	

- Prérequis pour la surveillance de conformité
  Avant de configurer la surveillance de conformité, passez en revue les prérequis et restrictions applicables.
- Configuration de la surveillance de conformité
  Apprenez à créer la configuration initiale de la surveillance de conformité.
- Remplissage de groupes
  Apprenez à remplir des groupes pour la surveillance de conformité.
- Activer la recherche de données sensibles
  Apprenez comment stocker les données d'identification des bases de données et permettre ainsi la découverte et la classification des données sensibles.
- Comprendre les vues de surveillance de conformité
  Apprenez à interpréter les vues de surveillance de conformité et à y répondre.

Rubrique parent : Surveillance et audit
Concepts associés:
Politiques
Sources de données
Tâches associées:
Reconnaissance des données sensibles
Information associée:
Groupes
Accélérateur GDPR de Guardium (vidéo)

Prérequis pour la surveillance de conformité

Avant de configurer la surveillance de conformité, passez en revue les prérequis et restrictions applicables.

L'outil de surveillance de conformité utilise des modèles prêts à l'emploi pour établir rapidement la surveillance de conformité des nouveaux serveurs de bases de données dans votre environnement. Ces modèles sont optimisés pour être utilisés avec les déploiements Guardium nouveaux ou en cours d'évolution. Pour bénéficier des fonctionnalités les plus complètes tout en préservant la simplicité de configuration, vérifiez que les conditions préalables suivantes sont toutes satisfaites :

- Vous êtes un utilisateur Guardium avec des privilèges d'administration exécutant une installation de Guardium version 10.1.3 ou plus récente, configurée comme gestionnaire central ou système autonome.
- Des agents de surveillance S-TAP sont installés et opérationnels sur les nouveaux serveurs de bases de données.
- Les serveurs de bases de données sont pris en charge par les modèles de surveillance de conformité.
- Aucune politique autre que *Par défaut - Ignorer l'activité des données pour les connexions inconnues* n'est installée.
  Avertissement :

  L'installation conjointe de politiques de surveillance de conformité pour déploiement rapide avec vos politiques préexistantes n'est possible que si ces dernières sont configurées comme suit dans leur Définition de politique :

  - Consigner données brutes : désactivé
  - Règles sur données brutes : désactivé

- Trace d'audit sélective : activé

L'installation des politiques de sécurité pour déploiement rapide échouera si l'une quelconque des politiques préexistantes comporte des valeurs incompatibles dans sa définition. Dans le cas d'un déploiement existant, voyez s'il ne serait pas préférable de désinstaller les politiques existantes avant d'utiliser les politiques pour déploiement rapide. Les nouveaux déploiements Guardium ne sont normalement pas concernés par cette mesure.

Les sections suivantes décrivent en détail les prérequis à l'utilisation des modèles de surveillance de conformité pour déploiement rapide.

Déploiement d'agents de surveillance

Avant de commencer à configurer la surveillance de conformité, veillez à ce qu'un agent de surveillance (S-TAP) Guardium soit installé sur chaque serveur de base de données et qu'il soit configuré pour communiquer avec le système Guardium. Pour savoir comment installer et configurer rapidement ces agents, consultez Déploiement d'agents de surveillance.

Pour des informations plus détaillées sur les agents S-TAP, y compris sur d'autres méthodes d'installation, consultez le Guide d'administration des agents S-TAP.

Bases de données prises en charge

Pour détecter les bases de données dans votre environnement Guardium, l'outil de surveillance de conformité se fonde sur les critères suivants :

- Le trafic actif sur un système Guardium.
- Le rapport des instances découvertes (Découvrir > Rapports > Instances découvertes).

La méthode de détection varie en fonction du type de base de données, comme le montre le tableau suivant.

Tableau 1. Types de base de données pris en charge et méthodes de détection.

Base de données	Trafic actif	Instances découvertes
Db2 for Linux, UNIX, and Windows	✓	
Db2 for z/OS	✓ Important : La politique *Valeur par défaut - Ignorer l'activité des données pour les connexions inconnues* ne capture pas le trafic pour les bases de données Db2 for z/OS. Avant d'utiliser l'outil de surveillance de conformité avec les bases de données Db2 for z/OS, vous devez d'abord installer une politique qui répond aux critères de définition de politique et de trafic actif décrits dans cette rubrique.	
Informix	✓	✓
Microsoft SQL Server	✓	✓
MySQL	✓	✓
Netezza	✓	
Oracle	✓	✓
PostgreSQL	✓	
Sybase	✓	✓
Teradata	✓	✓

Pour être considéré comme tel, le trafic actif doit répondre aux critères suivants :

- Le trafic utilise l'un des protocoles suivants :
  - Bases de données Db2 for z/OS : BATCH, CALL, CICS, CTL, DRDA, PRIV, RRSAF, TRAN, TSO ou UTIL.
  - Toutes les autres bases de données : TCP.
- Le trafic n'est pas local (l'IP du serveur est différence de celle du client).
- Les tentatives d'ouverture de session (logins) infructueuses sont ignorées.
- Le trafic n'est pas chiffré.

La recherche de nouvelles bases de données dans le trafic actif a lieu toutes les heures, à 17 minutes passées l'heure. Par exemple, le trafic actif d'une base de données établie à 13:00 sera détecté à 13:17.
Pour être considérées comme telles, les instances découvertes doivent répondre aux critères suivants :

- Les bases de données ne spécifient pas de plage de ports.
- Les bases de données ne nécessitent pas de nom de base de données pour la création de source de données.

Règles d'extrusion et Inspecter les données renvoyées

Plusieurs politiques de surveillance de conformité pour déploiement rapide utilisent des règles d'extrusion. Ces dernières évaluent les données retournées par le serveur en réponse aux demandes. Par exemple, une règle d'extrusion pourrait rechercher un motif numérique particulier faisant penser à des données sensibles telles que des numéros de sécurité sociale ou des numéros de carte de crédit.

Les règles d'extrusion nécessitent que l'option Inspecter les données renvoyées soit activée pour tous les moteurs d'inspection qui utilisent la politique concernée. Pour utiliser les règles d'extrusion incluses avec les modèles de conformité suivants, vous devez autoriser les moteurs d'inspection à inspecter les données retournées :

- GDPR
- HIPAA
- PCI
- PII (confidentialité des données)

Important : Le fait d'activer l'option Inspecter les données renvoyées accroît le trafic réseau.
Le chemin à suivre pour activer l'option Inspecter les données renvoyées est Gérer > Surveillance de l'activité > Moteurs d'inspection. Pour plus d'informations sur l'option Inspecter les données renvoyées, consultez Création de politiques et Configuration des moteurs d'inspection.

Valeurs de définition des politiques

Toutes les politiques de sécurité utilisées pour la surveillance de conformité sont configurées avec les valeurs suivantes dans leur définition :

- Consigner données brutes : désactivé
- Règles sur données brutes : désactivé
- Trace d'audit sélective : activé

Les politiques dont les valeurs Consigner données brutes, Règles sur données brutes ou Trace d'audit sélective sont différentes ne peuvent pas être installées dans le même environnement Guardium. Il n'est donc pas possible d'utiliser les modèles de surveillance de conformité pour déploiement rapide si vous avez installé des politiques configurées différemment.

Avec les nouveaux déploiements Guardium ou les déploiement existants mais dépourvus de politiques définies par l'utilisateur, il est peu probable que vous observiez des conflits avec ces valeurs. Dans le cas de déploiements Guardium existants, si vous recevez un message signalant des *conflits entre définitions de politique* lorsque vous utilisez l'outil Configurer la surveillance de conformité, passez en revue vos définitions de politique.

Pour plus d'informations sur les traces d'audit sélectives, consultez Actions associées à des règles.
Exception : Si elle est la seule à être installée, la politique *Par défaut - Ignorer l'activité des données pour les connexions inconnues* est outrepassée par l'installation des politiques de surveillance de conformité.
Rubrique parent : Configuration rapide de la surveillance de conformité

Configuration de la surveillance de conformité

Apprenez à créer la configuration initiale de la surveillance de conformité.

Avant de commencer

Pour plus d'informations sur les prérequis et les restrictions, consultez Prérequis pour la surveillance de conformité.

Pourquoi et quand exécuter cette tâche

Utilisez l'outil de configuration de la surveillance de conformité pour associer les bases de données à un ou plusieurs modèles de conformité. Cette procédure permet d'installer rapidement une politique de sécurité et de créer des groupes et des rapports ainsi qu'un scénario de découverte des données sensibles lorsqu'il est pris en charge.

Procédure

1. Ouvrez la page Surveillance de conformité en suivant le trajet Configurer > Configuration rapide > Surveillance de conformité.
2. Ouvrez l'outil de configuration de la surveillance de conformité en cliquant sur l'icône dans la vignette Configurer la surveillance de conformité.
3. Dans la section Type de conformité, utilisez le menu Sélectionnez le type de conformité à activer pour choisir le type de surveillance de base de données à configurer. Par exemple, pour activer la surveillance GDPR, sélectionnez General Data Protection Regulation (GDPR). Cliquez sur Suivant pour continuer.
4. Dans la section Bases de données, sélectionnez les bases de données voulues dans la table Bases de données disponibles et cliquez sur l'icône pour les ajouter à la table Bases de données sélectionnées.
   Bon à savoir :
   - Cochez la case Exclure les bases de données surveillées pour masquer les bases de données dont la surveillance de conformité est déjà configurée.
   - Lorsque vous utilisez le type de conformité General Data Protection Regulation pour Db2 for z/OS (GDPR pour Db2 for z/OS), la liste des bases de données disponibles est filtrée pour n'inclure que les bases de données Db2 for z/OS. De même, les bases de données Db2 for z/OS ne sont pas affichées lorsque vous utilisez des types de conformité autres que z/OS.
   - Sélectionnez une base de données dans la table Bases de données sélectionnées et cliquez sur Fournir des données d'identification pour stocker ses données d'identification. Le stockage des données d'identification permet la découverte et la classification des données sensibles pour certains types de conformité. Si la configuration automatisée n'est pas prise en charge, les sources de données créées lorsque vous stockez les données d'identification pourront servir dans vos propres scénarios de découverte des données sensibles.
   - Pour dissocier des bases de données d'un type de conformité, éditez la configuration et supprimez les bases de données concernées de la table Bases de données sélectionnées. Vous pouvez également suivre le trajet Afficher les détails > Bases de données à partir de la vignette du type de conformité et cliquer sur l'icône en regard de chaque base de données à dissocier.
5. Une fois les bases de données à surveiller identifiées, cliquez sur Exécuter la configuration pour installer la politique, peupler le groupe d'IP de serveur et générer les rapports de surveillance de conformité.
6. Dans la boîte de dialogue Actualiser la page pour afficher le nouveau contenu ?, cliquez sur Oui pour régénérer la page et terminer la configuration.

Résultats

Une fois la configuration terminée, le tableau de bord de surveillance de conformité est complété d'une vignette correspondant au modèle de conformité que vous venez de configurer.

Que faire ensuite

Après avoir configuré la surveillance de conformité, vous verrez peut-être plusieurs icônes  affichées dans les vignettes du tableau de bord. Ces icônes indiquent qu'une configuration supplémentaire est nécessaire. Utilisez les liens Remplir un groupe pour peupler des groupes supplémentaires ou le lien Données d'identification de source de données pour fournir les données d'identification de la base de données afin qu'elles puissent servir dans un scénario de découverte des données sensibles.

Important : Lorsque la surveillance est configurée avec l'outil de configuration de la surveillance de conformité, un groupe par défaut est automatiquement créé et peuplé avec les adresses IP des serveurs. Il est cependant important de définir quels utilisateurs et applications seront autorisés à accéder à vos bases de données. Vous devez à cet effet constituer plusieurs groupes supplémentaires. Pour des informations sur le remplissage de groupes à partir de la page de surveillance de conformité, consultez Remplissage de groupes.

Rubrique parent : Configuration rapide de la surveillance de conformité

Concepts associés:

Prérequis pour la surveillance de conformité

Information associée:

Déploiement d'agents de surveillance

Remplissage de groupes

Apprenez à remplir des groupes pour la surveillance de conformité.

Avant de commencer

Installez un modèle de surveillance de conformité en suivant la procédure décrite dans Configuration de la surveillance de conformité.

Pourquoi et quand exécuter cette tâche

Lorsque la surveillance est configurée avec l'outil de configuration de la surveillance de conformité, un groupe par défaut est automatiquement créé et peuplé avec les adresses IP des serveurs. Il est cependant important de définir quels utilisateurs et applications seront autorisés à accéder à vos bases de données. Vous devez à cet effet constituer plusieurs groupes supplémentaires. La procédure suivante décrit comment constituer rapidement des groupes.

Important :

- Un groupe vide n'est pas considéré comme une valeur générique et ne permet pas la capture du trafic.
- Les groupes hiérarchisés ou imbriqués ne sont pas pris en charge.

Procédure

1. Utilisez l'une des méthodes suivantes pour identifier les groupes non peuplés et ouvrir la boîte de dialogue Editer un groupe.
   - Dans la section Surveillance activée d'une vignette du tableau de bord de surveillance de conformité, repérez l'icône  et cliquez sur le lien Remplir un groupe associé.
   - Cliquez sur le lien Afficher les détails d'une vignette du tableau de bord de surveillance de conformité pour ouvrir le panneau correspondant, sélectionnez l'onglet Récapitulatif et cliquez sur l'icône  en regard d'un groupe.
     Conseil : Dans le panneau des détails, les groupes non peuplés sont signalés par une petite icône .

   La vue des détails et la boîte de dialogue Editer un groupe s'ouvrent par-dessus le tableau de bord de surveillance de conformité.
2. Dans la boîte de dialogue Editer un groupe, fournissez éventuellement une Catégorie et une Classification pour le groupe. Les champs Type d'application, Type de groupe et Description (utilisé comme Nom de groupe) sont préremplis en fonction du groupe que vous avez sélectionné à l'étape précédente. Ils ne sont pas éditables.
3. Dans la boîte de dialogue Editer un groupe, utilisez l'une des méthodes suivantes pour commencer à remplir le groupe sélectionné.
   - Cliquez sur l'icône  pour ajouter une entrée à la table Membres et spécifier vous-même le membre du groupe.
   - Cliquez sur Importer > Depuis un fichier CSV pour importer des membres de groupe à partir d'un fichier CSV.
   - Cliquez sur Importer > Depuis un groupe pour importer des membres d'un autre groupe Guardium du même type. Par exemple, vous pourriez peupler un groupe d'*utilisateurs autorisés* en important ses membres d'une autre groupe contenant une liste d'utilisateurs, mais pas d'un groupe constitué d'une liste d'adresses IP.
   - Cliquez sur Importer > Depuis une source de données externe pour importer des membres de groupe d'une source de données externe. Le menu Source de données inclut toutes les sources de données marquées *Partagé* ou du type *Domaine personnalisé*. Pour plus d'informations, consultez Importation à partir de sources de données externes.
4. Lorsque vous avez fini d'ajouter des membres au groupe, cliquez sur OK pour retourner au tableau de bord de surveillance de conformité.

Rubrique parent : Configuration rapide de la surveillance de conformité

Activer la recherche de données sensibles

Apprenez comment stocker les données d'identification des bases de données et permettre ainsi la découverte et la classification des données sensibles.

Avant de commencer

Installez un modèle de surveillance de conformité en suivant la procédure décrite dans Configuration de la surveillance de conformité.

Pourquoi et quand exécuter cette tâche

La procédure suivante décrit comment créer des sources de données en stockant les données d'identification des bases de données à l'aide de l'outil de surveillance de conformité. Le stockage des données d'identification et la création de sources de données permettront à Guardium d'accéder à vos bases de données pour découvrir et classifier les données sensibles.

Procédure

1. Utilisez l'une des méthodes suivantes pour identifier les bases de données pour lesquelles des données d'identification doivent être fournies.

- Dans la section Recherche de données sensibles d'une vignette du tableau de bord de surveillance de conformité, repérez une icône et cliquez sur le lien Données d'identification de source de données associé. La vue des bases de données configurées pour la surveillance de conformité s'ouvre sur une liste filtrée de bases de données pour lesquelles il est nécessaire de fournir des données d'identification.
- Cliquez sur le lien Voir les bases de données pour ouvrir la vue des bases de données configurées pour la surveillance de conformité et repérez les bases de données pour lesquelles la colonne Source de données ne contient pas d'icône .

2. Dans la vue des bases de données configurées pour la surveillance de conformité, sélectionnez les bases de données nécessitant des données d'identification et cliquez sur Actions de source de données > Fournir des données d'identification.
   Bon à savoir :
   - Si vous sélectionnez plusieurs bases de données et que vous cliquez sur Actions de source de données > Fournir des données d'identification, les données d'identification fournies seront sauvegardées pour toutes les bases de données sélectionnées. Vous devez, dans ce cas, veiller à ce que les bases de données sélectionnées soient bien toutes accessibles au moyen des mêmes données d'identification. Si certaines utilisent des données d'identification différentes, elles échoueront au test de connexion.
   - Le stockage des données d'identification permet la découverte et la classification des données sensibles pour certains types de conformité. Si la configuration automatisée n'est pas prise en charge, les sources de données créées lorsque vous stockez les données d'identification pourront servir dans vos propres scénarios de découverte des données sensibles.
3. Dans la boîte de dialogue Fournir des données d'identification, utilisez les champs Nom d'utilisateur et Mot de passe pour Fournir des données d'identification permettant l'accès aux bases de données sélectionnées. Cliquez sur OK pour retourner à la vue des bases de données configurées pour la surveillance de conformité.
4. Dans la vue des bases de données configurées pour la surveillance de conformité, sélectionnez les bases de données pour lesquelles des données d'identification sont stockées et cliquez sur Actions de source de données > Tester la connexion. Utilisez Tester la connexion pour vérifier que les données d'identification stockées permettent bien d'accéder à la base de données. Si le test de connexion échoue, la découverte et la classification des données sensibles ne fonctionneront pas.
   Important :
   - Le test des connexions peut prendre du temps. Il est déconseillé de tester un grand nombre de connexions à la fois.
   - Si un test de connexion échoue, allez à Configurer > Outils et vues > Définitions de source de données, sélectionnez la source de données et contrôlez la validité de sa définition. Par exemple, il peut être nécessaire de spécifier le port approprié pour les bases de données Db2 for z/OS, de corriger le nom d'une base de données PostgreSQL à casse mixte, ou encore de définir d'autres propriétés de connexion requises pour votre environnement.
   - En cas d'échec du test de connexion à une instance Microsoft SQL Server, vérifiez que le service Windows SQL Server Browser est démarré.

Résultats

Une fois que la recherche de données sensibles est activée, les résultats de ces recherches, ainsi que les éventuels changements apportés à la politique (notamment les changements dans les groupes et leurs membres) deviennent disponible après l'installation de la politique selon son planning d'installation. Par défaut, l'outil de surveillance de conformité pour déploiement rapide prévoit une installation des politiques quotidienne, exécutée à 10:30.

Rubrique parent : Configuration rapide de la surveillance de conformité

Comprendre les vues de surveillance de conformité

Apprenez à interpréter les vues de surveillance de conformité et à y répondre.

Interface utilisateur

L'outil Surveillance de conformité se compose des vues suivantes :

Vue Tableau de bord

Il s'agit de la vue par défaut. Elle fournit un aperçu de l'état actuel du déploiement de conformité, organisé par type de conformité. Ses vignettes individuelles reflètent l'état de configuration des différents composants de la surveillance de conformité et vous permettent d'identifier rapidement quels types de conformité nécessitent une configuration supplémentaire.

Vue des bases de données

Cette vue comprend un tableau indiquant quelles bases de données sont configurées avec les modèles de surveillance de conformité pris en charge.

Configurer la surveillance de conformité

L'outil Configurer la surveillance de conformité offre une interface guidée qui permet d'associer rapidement les bases de données aux modèles de conformité et d'exécuter la configuration initiale. Accédez à cet outil en cliquant sur l'icône dans la vignette Configurer la surveillance de conformité du tableau de bord ou en sélectionnant des bases de données et en cliquant sur le bouton Configurer la surveillance de conformité dans la vue des bases de données.

Dans les différentes vues de l'outil Surveillance de conformité, les tâches en rapport avec l'établissement de la surveillance de conformité peuvent être réalisées de différentes manières liées entre elles. Le tableau suivant indique dans quelles vues chaque tâche peut être réalisée.

Tableau 1. Synthèse des tâches prises en charge par les vues de surveillance de conformité

Tâche	Configurer la surveillance de conformité	Vue Tableau de bord	Vue des bases de données
Associer un type de conformité à une ou plusieurs bases de données	Dans la section Bases de données, sélectionnez les bases de données voulues dans la table Bases de données disponibles et cliquez sur l'icône pour les déplacer dans la table Bases de données sélectionnées.		

Tâche	Configurer la surveillance de conformité	Vue Tableau de bord	Vue des bases de données
Remplir des groupes		Dans la vignette d'un type de conformité, cliquez sur le lien Remplir un groupe ou sélectionnez Afficher les détails > Récapitulatif et cliquez sur l'icône  en regard d'un groupe.	
Définir des sources de données pour découvrir les données sensibles	Dans la section Bases de données, sélectionnez les bases de données voulues dans la table Bases de données sélectionnées et cliquez sur le bouton Fournir des données d'identification.	Dans la vignette d'un type de conformité, cliquez sur le lien Données d'identification de source de données, sélectionnez les bases de données voulues et cliquez sur Actions de source de données > Fournir des données d'identification.	Sélectionnez les bases de données et cliquez sur Actions de source de données > Fournir des données d'identification.

Important : Une fois configurées avec un modèle de surveillance de conformité, les bases de données qui ont été mises hors ligne continuent à apparaître dans l'outil Surveillance de conformité.

Politiques

Les modèles de surveillance de conformité pour déploiement rapide fournissent des politiques de sécurité conçues pour fonctionner efficacement sans nécessiter de modifications. Utilisez-les pour mettre en place rapidement un environnement de surveillance de conformité pleinement fonctionnel. Dans la vue du tableau de bord de surveillance de conformité, cliquez sur Afficher les détails > Politiques pour voir quelles politiques sont associées à un type spécifique de conformité.

Lorsque la surveillance de conformité est configurée à partir d'un gestionnaire central, les politiques de sécurité pour déploiement rapide sont automatiquement poussées vers tous les collecteurs. Elles sont installées en dernier si l'installation comprend également des politiques spécifiques, autres que les politiques de sécurité pour déploiement rapide par défaut.

Si vous souhaitez passer en revue les détails des politiques de surveillance de conformité, vous pouvez y accéder par l'intermédiaire du Localiseur de politique. Les politiques pour déploiement rapide se reconnaissent à leur nom, qui est de la forme : *type de conformité* pour déploiement rapide. Par exemple, la politique GDPR par défaut se nomme GDPR pour déploiement rapide. Vous pouvez aussi éditer les politiques de surveillance de conformité à l'aide du Générateur de politique pour les données.
Restriction : Dans les versions antérieures à Guardium version 10.1.4, le fait de modifier les règles et les groupes utilisés avec les politiques de sécurité pour déploiement rapide peut conduire à un statut de configuration inexact dans l'outil Surveillance de conformité.
Si vous avez modifié les politiques de surveillance de conformité, rétablissez leurs valeurs par défaut dans la vue du tableau de bord Surveillance de conformité en cliquant sur Afficher les détails dans la vignette du type de conformité souhaité, puis en sélectionnant l'onglet Politiques et en cliquant sur Restaurer les valeurs par défaut. Avant de rétablir les valeurs par défaut, le programme sauvegarde les valeurs personnalisées dans une politique dont le nom obéit à la convention suivante : *type de conformité* pour déploiement rapide *horodatage* (où *horodatage* indique la date et l'heure auxquelles les valeurs par défaut ont été rétablies). Par exemple, GDPR pour déploiement rapide 2017-05-01 19:17:59.
Important : Dans les versions antérieures à Guardium version 10.1.4, il peut être nécessaire de réinstaller la politique de sécurité pour déploiement rapide après l'utilisation de l'option Restaurer les valeurs par défaut. Pour plus d'informations, consultez Installation des politiques de sécurité.

Planning d'installation des politiques

Par défaut, l'outil de surveillance de conformité pour déploiement rapide prévoit une installation des politiques quotidienne, exécutée à 10:30.

Lorsque la surveillance de conformité est configurée à partir d'une machine autonome, un planning d'installation des politiques est défini s'il n'y a pas d'autre planning préexistant (qu'il soit actif ou en pause). Lorsque la surveillance de conformité est configurée à partir d'un gestionnaire central, le planning d'installation des politiques est configuré pour tous les collecteurs (qu'il y ait ou non un autre planning préexistant).

Groupes

L'outil de surveillance de conformité associe plusieurs groupes à chaque type de conformité. L'établissement d'une surveillance de conformité efficace nécessite que ces groupes soient tous peuplés. Dans la vue du tableau de bord de surveillance de conformité, cliquez sur Afficher les détails > Récapitulatif pour voir quels groupes sont associés à un type spécifique de conformité.

Restriction :

- Les groupes hiérarchisés ou imbriqués ne sont pas pris en charge.
- Un groupe vide n'est pas considéré comme une valeur générique et ne permet pas la capture du trafic.
- Dans les versions antérieures à Guardium version 10.1.4, le fait de modifier les règles et les groupes utilisés avec les politiques de sécurité pour déploiement rapide peut conduire à un statut de configuration inexact dans l'outil Surveillance de conformité.

Il est possible que vous constatiez une différence entre le nombre de bases de données et le nombre de membres indiqué pour le groupe IP de serveur dans l'onglet Afficher les détails > Récapitulatif, pour un type de conformité. Cette différence peut s'expliquer par la présence de plusieurs bases de données sur un même serveur de bases de données (une seule IP étant alors comptée pour ces bases de données). Il se peut aussi que le groupe IP de serveur ait été mis à jour en dehors de l'outil de surveillance de conformité.

Rapports

Les modèles de surveillance de conformité pour déploiement rapide fournissent plusieurs rapports prédéfinis pour chaque type de conformité. Dans la vue du tableau de bord de surveillance de conformité, cliquez sur Afficher les détails > Rapports pour voir quels rapports sont associés à un type spécifique de conformité. Ces rapports sont également disponibles sous la section Accélérateurs de la navigation Guardium principale. Cette liste de rapports est prédéfinie pour chaque type de conformité et ne reflète aucunement les rapports personnalisés que vous avez pu définir.

Restriction : Le modèle de surveillance de conformité HIPAA ne fournit aucun rapport prédéfini.

Utilisateurs et rôles

L'utilisateur en cours se voit attribuer le rôle correspondant au type de conformité sélectionné. Il a ainsi accès aux rapports et accélérateurs associés à partir de la navigation Guardium principale. Si différents utilisateurs Guardium configurent différents types de conformité, chacun n'a accès qu'aux rapports et accélérateurs associés au type de conformité qu'il configure.

Par exemple, si *utilisateur1* configure le type de conformité *GDPR* et si *utilisateur2* configure le type de conformité *PCI*, *utilisateur1* n'aura pas accès aux rapports et accélérateurs PCI, car le rôle PCI ne lui a pas été attribué. Pour des informations sur l'attribution manuelle de rôles spécifiques aux utilisateurs, consultez Vue d'ensemble de la gestion des accès.

Données sensibles

Il est possible que vous constatiez une différence entre le nombre de Correspondances trouvées pour un type particulier de conformité et le nombre de membres des groupes d'objets associés dans l'onglet Afficher les détails > Récapitulatif. La valeur indiquée pour Correspondances trouvées est le nombre de paires nom de table/nom de colonne uniques qui ont satisfait les critères du scénario de découverte de données sensibles. Le nombre de membres du groupe OBJETS est le nombre de noms de table uniques. Sa valeur est un cumul des résultats de toutes les recherches de données sensibles.

Important : Dans la section Recherche de données sensibles d'une vignette du tableau de bord de surveillance de conformité, les icônes indiquent qu'une ou plusieurs sources de données ont été configurées pour le scénario de découverte de données sensibles. Cliquez sur Voir les bases de données pour identifier quelles bases de données ont des sources de données définies pour la découverte de données sensibles.
Rubrique parent : Configuration rapide de la surveillance de conformité

Utilisation de l'accélérateur PCI/DSS pour implémenter la conformité à la norme PCI

Configurez l'accélérateur PCI/DSS d'IBM Security Guardium et créez une série de politiques et de rapports afin de satisfaire les exigences de la norme PCI/DSS.

La norme PCI/DSS (Payment Card Industry/Data Security Standard) est un ensemble d'exigences techniques et d'exploitation conçu pour protéger les données sur les titulaires de cartes.

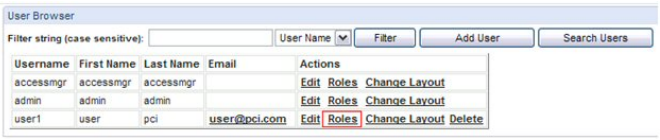
Avantage : offrez à vos clients une vue d'ensemble de la norme PCI/DSS et mettez à leur disposition des politiques et des rapports prédéfinis pour leur faire gagner du temps.

Procédez comme suit :

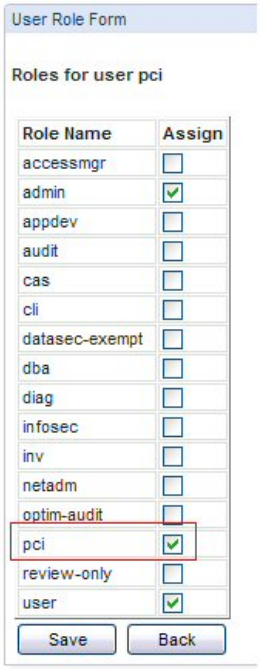
1. Configurez un rôle PCI.
2. Configurez des rapports et des politiques respectant les exigences.

Configuration d'un rôle PCI

1. Connectez-vous sur la page de l'interface utilisateur Guardium avec le compte utilisateur “accessmgr”. Sélectionnez un utilisateur (dans ce cas, user1) et cliquez sur Rôles.

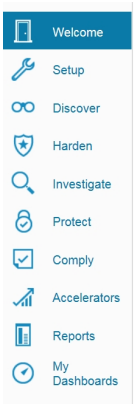


2. Dans le formulaire de rôles d'utilisateur, sélectionnez PCI, puis sauvegardez l'affectation.



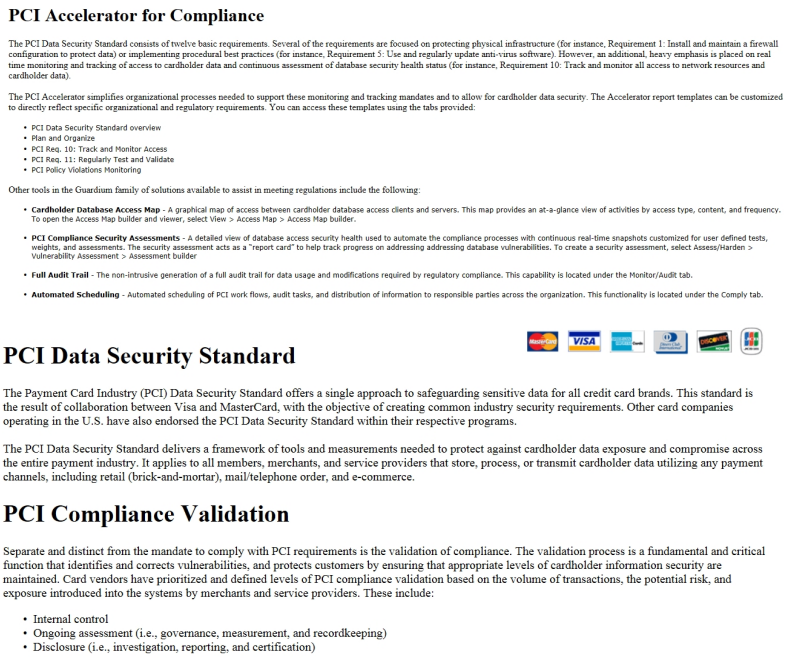
Implémentation de l'accélérateur PCI

Connectez-vous avec “user1” et cliquez sur Accélérateurs.



Présentation

1. Cliquez sur Accélérateur PCI pour mise en conformité.
2. Cliquez sur Norme de sécurité de données PCI.



PCI Accelerator for Compliance

The PCI Data Security Standard consists of twelve basic requirements. Several of the requirements are focused on protecting physical infrastructure (for instance, Requirement 1: Install and maintain a firewall configuration to protect data) or implementing procedural best practices (for instance, Requirement 5: Use and regularly update anti-virus software). However, an additional, heavy emphasis is placed on real time monitoring and tracking of access to cardholder data and continuous assessment of database security health status (for instance, Requirement 10: Track and monitor all access to network resources and cardholder data).

The PCI Accelerator simplifies organizational processes needed to support these monitoring and tracking mandates and to allow for cardholder data security. The Accelerator report templates can be customized to directly reflect specific organizational and regulatory requirements. You can access these templates using the tabs provided:

- PCI Data Security Standard overview
- Plan and Organize
- PCI Req. 10: Track and Monitor Access
- PCI Req. 11: Regularly Test and Validate
- PCI Policy Violations Monitoring

Other tools in the Guardium family of solutions available to assist in meeting regulations include the following:

- **Cardholder Database Access Map** - A graphical map of access between cardholder database access clients and servers. This map provides an at-a-glance view of activities by access type, content, and frequency. To open the Access Map builder and viewer, select View > Access Map > Access Map builder.
- **PCI Compliance Security Assessments** - A detailed view of database access security health used to automate the compliance processes with continuous real-time snapshots customized for user defined tests, weights, and assessments. The security assessment acts as a "report card" to help track progress on addressing addressing database vulnerabilities. To create a security assessment, select Assess/Harden > Vulnerability Assessment > Assessment builder
- **Full Audit Trail** - The non-intrusive generation of a full audit trail for data usage and modifications required by regulatory compliance. This capability is located under the Monitor/Audit tab.
- **Automated Scheduling** - Automated scheduling of PCI work flows, audit tasks, and distribution of information to responsible parties across the organization. This functionality is located under the Comply tab.

PCI Data Security Standard

The Payment Card Industry (PCI) Data Security Standard offers a single approach to safeguarding sensitive data for all credit card brands. This standard is the result of collaboration between Visa and MasterCard, with the objective of creating common industry security requirements. Other card companies operating in the U.S. have also endorsed the PCI Data Security Standard within their respective programs.

The PCI Data Security Standard delivers a framework of tools and measurements needed to protect against cardholder data exposure and compromise across the entire payment industry. It applies to all members, merchants, and service providers that store, process, or transmit cardholder data utilizing any payment channels, including retail (brick-and-mortar), mail/telephone order, and e-commerce.

PCI Compliance Validation

Separate and distinct from the mandate to comply with PCI requirements is the validation of compliance. The validation process is a fundamental and critical function that identifies and corrects vulnerabilities, and protects customers by ensuring that appropriate levels of cardholder information security are maintained. Card vendors have prioritized and defined levels of PCI compliance validation based on the volume of transactions, the potential risk, and exposure introduced into the systems by merchants and service providers. These include:

- Internal control
- Ongoing assessment (i.e., governance, measurement, and recordkeeping)
- Disclosure (i.e., investigation, reporting, and certification)

Planification et organisation

Planification et organisation

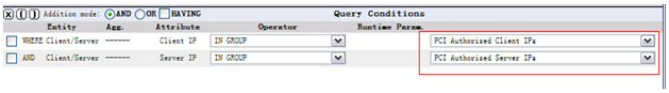
Cliquez sur Présentation pour en savoir plus sur la conformité des rapports prédéfinis.

1. Adresses IP du serveur des titulaires de cartes : liste de serveurs de base de données comportant des informations sur les titulaires de cartes. Selon la situation réelle de la société, définissez les informations sur le groupe d'adresses IP de serveur autorisées pour PCI, qui spécifient le serveur de base de données sur lequel sont stockées les informations sur les titulaires de cartes.
2. Bases de données de titulaires de cartes : base de données contenant des informations sur les titulaires de cartes. Définissez les informations sur le groupe désigné PCI - Bases de données de titulaires de cartes, qui sont stockées dans les informations sur les titulaires de cartes dans la base de données.
3. Objets de titulaire de carte : objet d'informations sur un titulaire de carte. La zone PCI - Objets sensibles du titulaire de carte doit être définie.
4. Carte des accès entre les clients et les serveurs de la BD : le mappage client/serveur et les adresses IP des serveurs autorisés PCI définissent les informations sur le groupe, qui spécifient les serveurs de bases de données sur lesquels sont stockées les informations sur les titulaires de cartes. Vous pouvez utiliser une requête pour identifier les accès effectués par les clients à la base de données des titulaires de cartes.
5. Utilisateurs de base de données actif : l'administrateur, en plus de catégories d'utilisateurs, ayant consulté la base de données des titulaires de cartes. Définissez les “adresses IP de serveur autorisées pour PCI. et les .administrateurs PCI..
6. Administration de la base de données de titulaires de cartes : opérations de gestion de la base de données des titulaires de cartes. Définissez les adresses IP des serveurs autorisés PCI et les utilisateurs administrateurs.
7. Programmes source autorisés : accès au programme de crédit. Définissez les adresses IP des serveurs autorisés PCI et les programmes source autorisés PCI. Procédure d'enregistrement des accès à la base de données des titulaires de cartes de crédit.

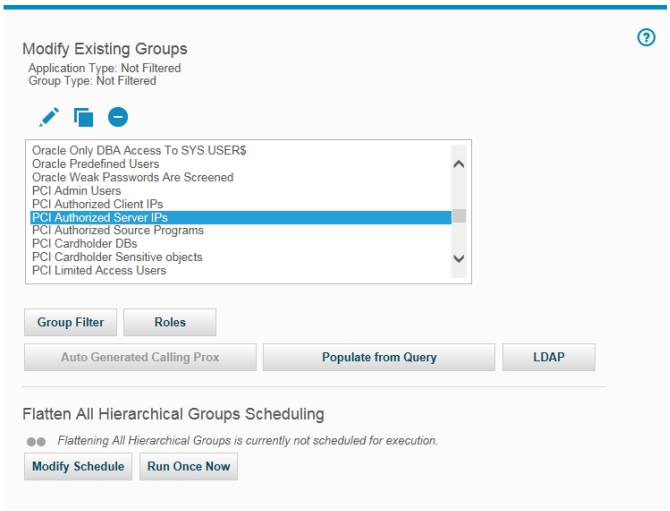
8. Accès non autorisé aux applications : pas d'accès au programme de crédit. Définissez les adresses IP des serveurs autorisés PCI et les programmes source autorisés PCI. Enregistrements du programme de crédit pour l'accès à la base de données des titulaires de cartes.
9. 8.5.8 Comptes partagés : huitième exigence de la norme PCI selon laquelle toute personne ayant un accès informatique doit être associée à un ID unique. Définissez les adresses IP des serveurs autorisés PCI afin de pouvoir compter le nombre de fois qu'un même nom d'utilisateur de base de données tente un accès depuis l'adresse IP de la base de données des titulaires de cartes.

Dans les instructions, cliquez pour afficher un formulaire de rapport, puis déterminez quel contenu de groupe spécifique doit être rempli.

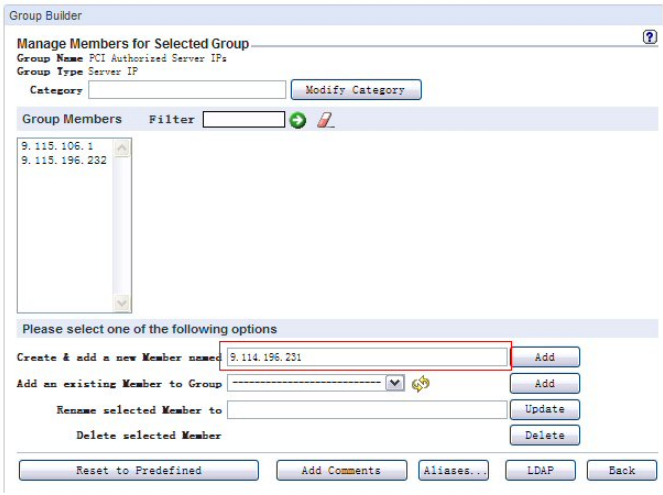
Nom réel du groupe :



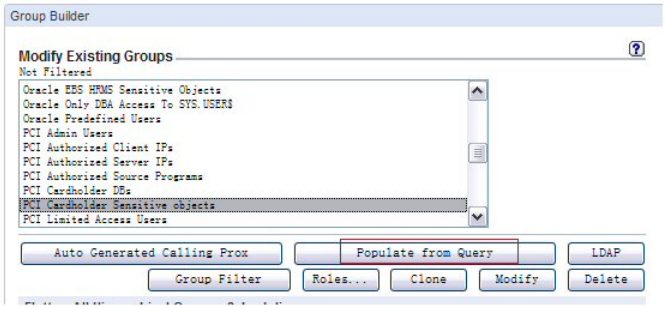
Sélectionnez Configuration > Outils et vues > Générateur de groupe, et dans la zone Modifier groupes existants, sélectionnez le nom du groupe.



Cliquez sur Modifier (icône représentant un crayon) et accédez à la page Gérer les membres du groupe sélectionné. Ajoutez de nouveaux membres.



Vous pouvez également remplir le groupe à l'aide d'une requête personnalisée.



Exigences PCI 10 - Suivi et surveillance

Cliquez sur Présentation pour en savoir plus sur la conformité des rapports prédéfinis et de la surveillance Guardium.

1. 10.2 et 10.3 - Automatisation : utilisez les manuels d'aide en ligne sur la protection et la conformité pour automatiser cette section.
2. 10.2.1 - Accès aux données : accès PCI aux données sur un titulaire de carte, définition des adresses IP de serveur autorisées pour PCI et des administrateurs PCI.
3. 10.2.2 - Activité d'administration : activité PCI par administrateur. Définition des adresses IP de serveur autorisées pour PCI et des administrateurs PCI.
4. 10.2.3 - Accès à la trace d'audit : pour que vous puissiez suivre cette section entièrement, vous devez définir au moins quatre types de rapport : Connexions vers le serveur SQL Guard, Traces d'audit des activités d'utilisateur sur le serveur Guardium, Exceptions de travail planifié et Listes des tâches des utilisateurs. Sélectionnez Configuration > Rapports > Générateur de rapport pour créer des rapports en fonction de vos besoins.
5. 10.2.4 Accès non valide : PCI - Tentatives de connexion non valides : enregistrement de l'échec de connexion dans la base de données. PCI - Accès non autorisé aux applications : enregistrement de l'accès à la base de données non défini dans les programmes source autorisés PCI.
6. Les trois sections suivantes peuvent également utiliser le manuel d'aide sur la surveillance et l'audit disponible dans l'aide en ligne imbriquée : 10.2.6 Journal d'initialisation, 10.5 Traces d'audit sécurisées et 10.6 Audit des accès.

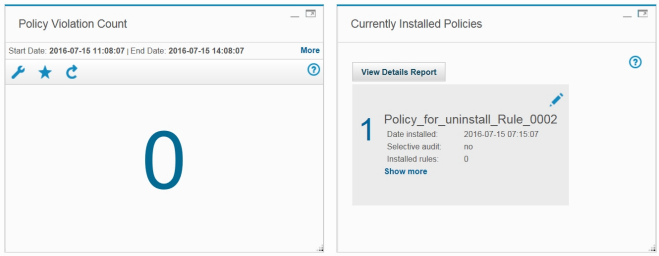
Exigences PCI 11 - Validation continue

Cliquez sur Présentation pour afficher une discussion sur l'importance de l'évaluation des vulnérabilités. Cliquez sur Renforcement > Générateur d'évaluation pour générer un processus d'évaluation.

Surveillance des politiques PCI

Cliquez sur Présentation pour découvrir la politique.

1. Pour afficher vos installations de politique en cours, sélectionnez Configuration > Outils et vues > Installation de politique et choisissez une politique adaptée à installer.



2. Violations de politique - Enregistrements des opérations de violation.

Rubrique parent : Surveillance et audit

Générateur de flux de travaux

Le générateur de flux de travaux est utilisé pour définir des flux de travaux personnalisés (étapes, transitions et actions) à utiliser dans le processus d'audit.

Pour plus d'informations, voir Construction de processus d'audit. Procédez comme suit :

- Définissez les étapes du flux de travaux (Statut d'événement)
- Définissez le flux de transit d'une étape à l'autre (Actions)
- Définissez quelles sont les actions qui requièrent une validation
- Affectez des rôles à chaque statut pour définir les utilisateurs autorisés à afficher chaque statut

Termes relatifs à cette fonction

Type d'événement - Flux de travaux personnalisé

Statut d'événement - Etat/statut du flux de travaux

Action liée à un événement - Action/Transition

Remarque : Le générateur de flux de travaux est un composant facultatif activé par la clé de produit.

Création d'un processus de flux de travaux

1. Avec un compte administrateur, ouvrez le générateur de flux de travaux en sélectionnant Conformité > Outils et vues > Générateur de flux de travaux. Avec un compte d'utilisateur ayant les privilèges DataPrivacy, ouvrez le générateur de flux de travaux en sélectionnant Accélérateurs > Confidentialité des données > Suivi et Surveillance > Trace d'audit et Automatisation de flux de travaux.
2. Dans le premier écran (Type d'événement), cliquez sur Statut d'événement pour accéder à la configuration du statut d'événement.
3. Cliquez sur Ajouter un statut d'événement pour définir un nouveau statut d'événement. Plusieurs statuts d'événement sont attendus. Entrez la description du statut et sélectionnez la case à cocher Tâche finale si la tâche est la dernière tâche du flux de travaux.
4. Cliquez sur Type d'événement, puis cliquez sur Ajouter dans Ajouter une définition de type d'événement pour définir un nouveau type d'événement.
5. Entrez la description et désignez la première tâche du flux de travaux.
6. Ensuite, choisissez tous les statuts autorisés pour le flux de travaux dans la liste Statut disponible en mettant en évidence l'élément de statut et en cliquant sur la flèche > entre la liste Statut disponible et la liste Statut autorisé.
7. Lorsque vous avez terminé, cliquez sur le bouton Sauvegarder. Remarque : le bouton Sauvegarder (ou Annuler) ne s'applique qu'aux modifications apportées au nom, à l'événement par défaut ou aux événements disponibles.
8. Accédez à la section Actions liées à un événement définies de l'écran du menu Type d'événement. Les actions liées à un événement définies impliquent la désignation des actions liées à un événement distinctes du flux de travaux.
9. Cliquez sur le bouton Nouveau.

10. Indiquez la description d'action liée à l'événement et désignez le statut précédent, le statut suivant, puis indiquez si la validation de cette action liée à l'événement est requise. Cliquez sur le bouton Appliquer.
11. Répétez les étapes 9 et 10 jusqu'à ce que toutes les actions liées à l'événement soient décrites et désignées.
12. Accédez à la section Rôles de l'écran du menu Type d'événement. Les rôles permettent de définir quels sont les utilisateurs qui peuvent afficher l'événement lorsque celui-ci se trouve dans une action liée à l'événement particulière. Par exemple, ils permettent de définir les utilisateurs qui peuvent voir les événements dont le statut est "En cours de révision" et les utilisateurs qui peuvent voir les événements dont le statut est "Approuvé".
13. Sélectionnez le statut de type d'événement et cliquez sur le bouton Rôles.
14. Dans le panneau Affecter des rôles de sécurité, sélectionnez tous les rôles à affecter (vous ne voyez que les rôles qui ont été affectés à votre compte). Cliquez sur Appliquer pour sauvegarder vos sélections. Cliquez sur le bouton Précédent.
15. Répétez les étapes 13 à 14 jusqu'à ce que des rôles soient définis pour tous les statuts de type d'événement.
16. La configuration depuis le générateur de flux de travaux est terminée.
17. Ouvrez le générateur de processus d'audit en sélectionnant Conformité > Outils et vues > Générateur de processus d'audit afin de planifier le flux de travaux et de générer et d'afficher des rapports de flux de travaux. Voir les étapes à effectuer dans le générateur de processus d'audit sous la section Définissez une tâche de rapport.

Les annexes contiennent un scénario d'utilisation, qui est un exemple de flux de travaux créé par le générateur de flux de travaux.

Remarque : Si le type de tâche dans le générateur de processus d'audit est un processus de classification, le générateur de flux de travaux ne peut pas créer de flux de travaux personnalisé.

Avertissement : lorsqu'un événement de flux de travaux est créé, un rôle peut être affecté à chaque statut utilisé par cet événement (en d'autres termes, les événements ne peuvent être vus que par ce rôle lorsqu'ils sont associés à ce statut).Lorsqu'un événement est associé à un processus d'audit, il est essentiel que chaque rôle affecté à un statut de cet événement possède un récepteur dans le processus d'audit.Si tel n'est pas le cas, il se peut qu'une ligne de résultat d'audit soit associée à un statut qui ne permet à aucun des récepteurs de l'afficher ou de changer son statut.

Si une ligne d'audit devient inaccessible, l'administrateur (qui peut afficher tous les événements, quels que soit leurs rôles) peut tout de même afficher la ligne et changer son statut. Toutefois, si la sécurité au niveau des données est activée, il se peut qu'il ne puisse pas afficher la ligne. L'administrateur doit alors désactiver la sécurité au niveau des données (depuis Profil global) ou posséder le rôle dataset_exempt. Il est important de configurer le processus d'audit pour que tous les rôles devant agir sur un événement associé à ce processus d'audit soient des récepteurs de ce processus d'audit.

Remarque : La suppression d'un statut d'événement n'est autorisée que si le statut n'est pas le statut de départ ou le statut de fin d'un événement, et s'il n'est utilisé par aucune action. La validation fournit la liste des événements/actions empêchant la suppression du statut.

Ajout d'événements par défaut uniquement à un nombre limité d'enregistrements

Lorsque vous exécutez une tâche de rapport de processus d'audit, les résultats sont sauvegardés dans la table REPORT_RESULT_DATA_ROW. Celle-ci contient une ligne pour chaque ligne du rapport. Si un événement par défaut est également affecté à cette tâche de rapport, une ligne est ajoutée à la table TASK_RESULT_ADDITIONAL_INFO, pour chaque ligne du rapport. Ceci peut entraîner un problème d'espace disque uniquement si des événements par défaut sont utilisés pour de nombreux résultats. Ne créez des événements que dans les résultats de tâche comportant un nombre limité d'enregistrements ; sinon, les utilisateurs ne pourront pas gérer les nombreux enregistrements. Si des événements par défaut sont utilisés de façon limitée comme prévu, vous ne rencontrerez pas de problème lié à l'espace disque ni à la facilité d'emploi, car il n'est pas facile de fermer des milliers d'événements.

- Création de flux de travaux personnalisés
  Définissez des flux de travaux personnalisés composés d'étapes, de transitions et d'actions propres à un client à utiliser ensuite dans un processus d'audit.
- Utilisation de flux de travaux personnalisés
  Définissez un processus d'audit qui respecte les pratiques recommandées pour les flux de travaux personnalisés du client. Ajoutez les pratiques et les processus d'audit spécifiques du client dans la solution Guardium.

Rubrique parent : Surveillance et audit

Création de flux de travaux personnalisés

Définissez des flux de travaux personnalisés composés d'étapes, de transitions et d'actions propres à un client à utiliser ensuite dans un processus d'audit.

Pourquoi et quand exécuter cette tâche

Définissez et gérez un flux de travaux en fonction des pratiques propres à un client.

Voir Générateur de flux de travaux pour une présentation de ce composant.

Configuration requise

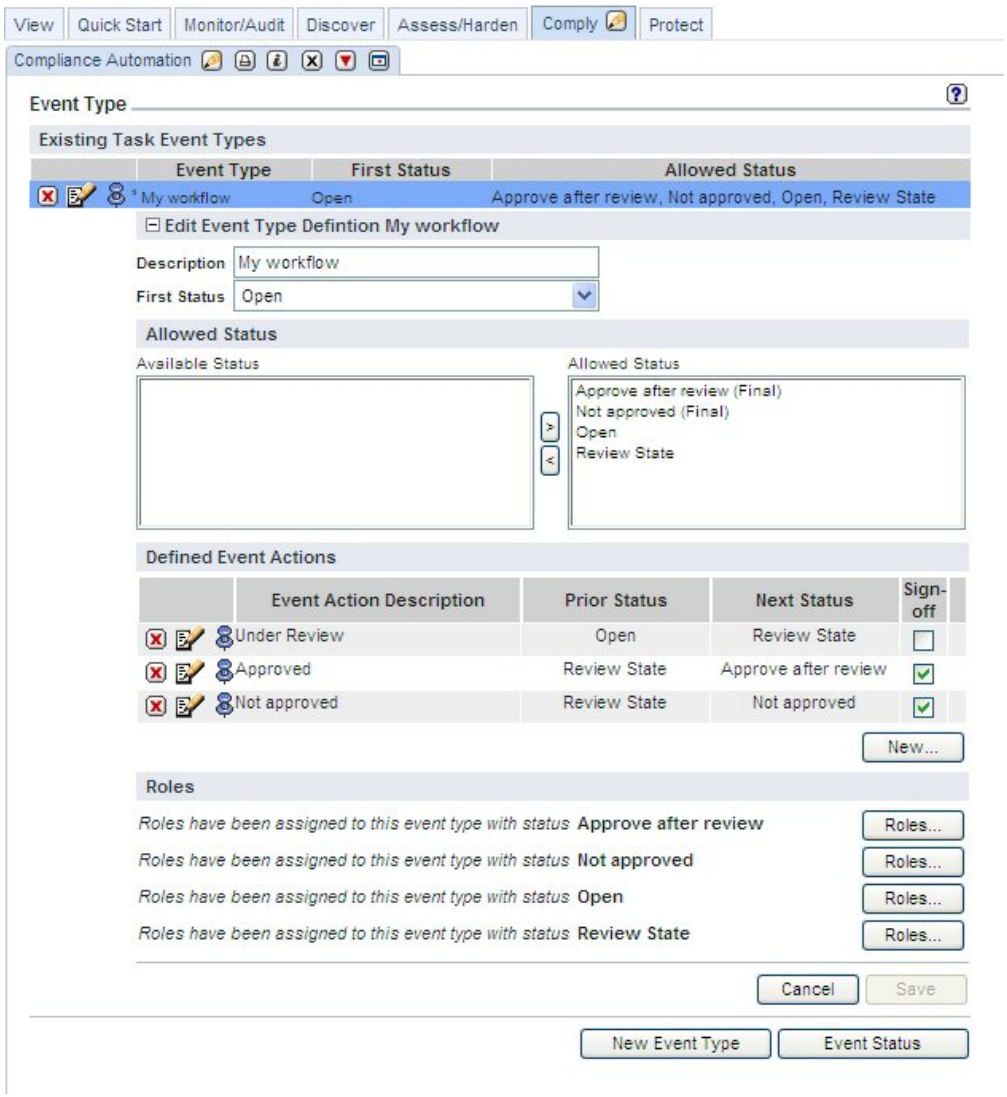
- Voir Création d'un flux de travaux d'audit. Pour plus d'informations, voir Automatisation du flux de travaux de conformité.
- Une fois que vous avez créé ce flux de travaux personnalisé, voir la section relative à la combinaison d'un flux de travaux personnalisé à un flux de travaux d'audit.

Procédure

1. Ouvrez le générateur de flux de travaux en sélectionnant Conformité > Outils et vues > Générateur de flux de travaux.
2. Dans le premier écran (Type d'événement), cliquez sur le bouton Statut d'événement pour accéder à la configuration du statut d'événement.
3. Cliquez sur Ajouter un statut d'événement pour définir un nouveau statut d'événement. Plusieurs statuts d'événement sont attendus. Entrez la description du statut et sélectionnez la case à cocher Tâche finale si la tâche est la dernière tâche du flux de travaux. Ensuite, passez à l'étape suivante.

   Exemple de flux de travaux simple comportant trois étapes : Ouvrir à Révision à Approuver ou Non approuvé. Chaque étape du flux de travaux constitue un statut d'événement de tâche défini distinct.

   Les tâches du flux de travaux de l'exemple sont : Ouvrir, Révision, Approuver après révision, ou Non approuvé. De plus, si la tâche constitue la dernière tâche d'un flux de travaux, sélectionnez la case à cocher dans la colonne Tâche finale. Par exemple, la dernière tâche dans l'exemple est Approuvé ou Non approuvé.



4. Cliquez sur le bouton Type d'événement, puis cliquez sur le bouton Ajouter dans Ajouter une définition de type d'événement pour définir un nouveau type d'événement.
5. Entrez la description et désignez la première tâche du flux de travaux.
6. Ensuite, choisissez tous les statuts autorisés pour le flux de travaux dans la liste Statut disponible en mettant en évidence l'élément de statut et en cliquant sur la flèche > entre la liste Statut disponible et la liste Statut autorisé.
7. Lorsque vous avez terminé, cliquez sur le bouton Sauvegarder.
8. Accédez à la section Actions liées à un événement définies de l'écran du menu Type d'événement. Les actions liées à un événement définies impliquent la désignation des actions liées à un événement distinctes du flux de travaux.
9. Cliquez sur le bouton Nouveau.

   Dans l'exemple de flux de travaux simple composé de trois étapes, l'action liée à l'événement En cours de révision possède le statut précédent Ouvrir et le statut suivant Révision. L'action liée à l'événement Approuvé suit En cours de révision avec le statut précédent Révision et le statut suivant Approuver après révision. Ou bien, l'action liée à l'événement Non approuvé possède le statut précédent Révision et le statut suivant Non approuvé. Les réviseurs désignés disposent également d'une capacité de validation par action liée à l'événement (en continu ou séquentielle). Voir la capture d'écran précédente.

10. Indiquez la description d'action liée à l'événement et désignez le statut précédent, le statut suivant, puis indiquez si la validation de cette action liée à l'événement est requise. Cliquez sur le bouton Appliquer.
11. Répétez les étapes 9 et 10 jusqu'à ce que toutes les actions liées à l'événement soient décrites et désignées.
12. Accédez à la section Rôles de l'écran du menu Type d'événement. Les rôles permettent de définir quels sont les utilisateurs qui peuvent afficher l'événement lorsque celui-ci se trouve dans une action liée à l'événement particulière. Par exemple, ils permettent de définir les utilisateurs qui peuvent voir les événements dont le statut est "En cours de révision" et les utilisateurs qui peuvent voir les événements dont le statut est "Approuvé".
13. Sélectionnez le statut de type d'événement et cliquez sur le bouton Rôles.
14. Dans le panneau Affecter des rôles de sécurité, sélectionnez tous les rôles à affecter (vous ne voyez que les rôles qui ont été affectés à votre compte). Cliquez sur Appliquer pour sauvegarder vos sélections. Cliquez sur le bouton Précédent.
15. Répétez les étapes 13 à 14 jusqu'à ce que des rôles soient définis pour tous les statuts de type d'événement.
16. La configuration depuis le générateur de flux de travaux est terminée.
17. Ouvrez le générateur de processus d'audit en sélectionnant Conformité > Outils et vues > Générateur de processus d'audit afin de planifier le flux de travaux et de générer et d'afficher des rapports de flux de travaux. Voir les étapes à effectuer dans le générateur de processus d'audit sous la section Définissez une tâche de rapport.

Rubrique parent : Générateur de flux de travaux

Utilisation de flux de travaux personnalisés

Définissez un processus d'audit qui respecte les pratiques recommandées pour les flux de travaux personnalisés du client. Ajoutez les pratiques et les processus d'audit spécifiques du client dans la solution Guardium.

Pourquoi et quand exécuter cette tâche

Flux de travaux personnalisés dans le processus Flux de travaux d'audit Guardium

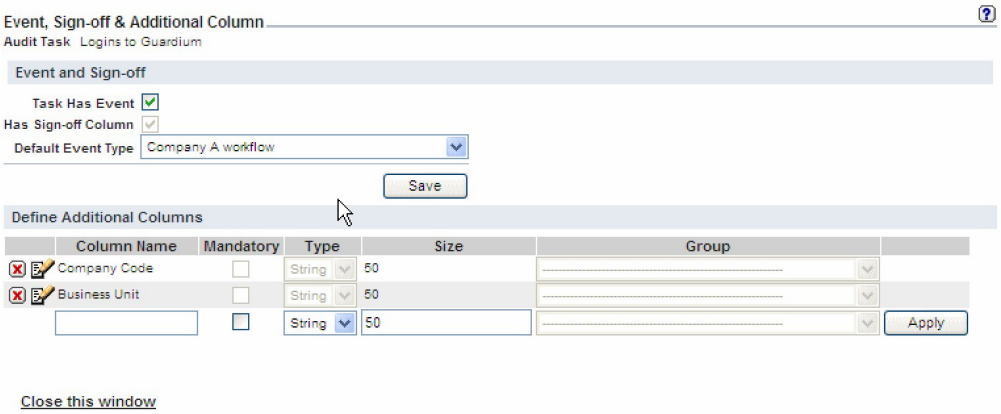
Vous pouvez gérer la séquence formelle des types d'événement créés dans le générateur de flux de travaux en cliquant sur le bouton Evénement et colonnes supplémentaires dans le fenêtre Tâches d'audit. Ce bouton apparaît une fois qu'une tâche d'audit a été créée et sauvegardée. Il n'apparaît pas tant que la tâche d'audit n'a pas été sauvegardée.

Configuration requise

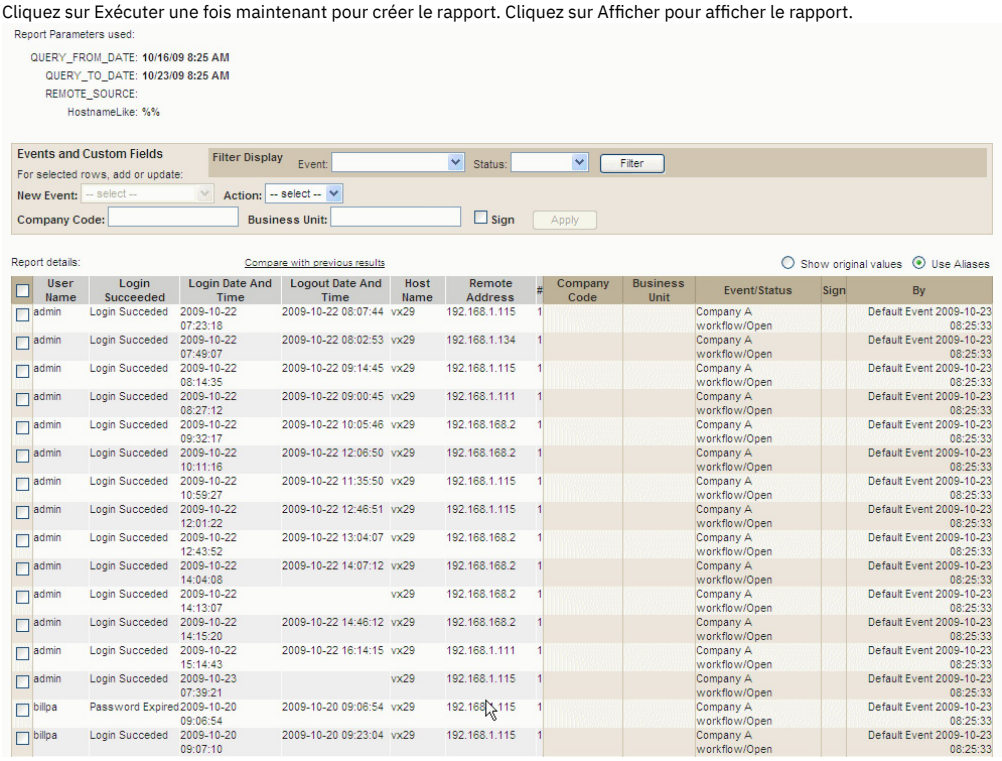
- Voir Création de flux de travaux personnalisés. Pour plus d'informations, voir Générateur de flux de travaux.
- Voir Création d'un flux de travaux d'audit. Pour plus d'informations, voir Automatisation du flux de travaux de conformité.
- Définissez un processus d'audit qui respecte les pratiques recommandées pour les flux de travaux personnalisés du client comme suit.

Procédure

1. Configurez les activités de flux de travaux ci-après lors de l'ajout d'une tâche d'audit.
2. Créez et sauvegardez une tâche d'audit. Une fois la tâche d'audit sauvegardée, un bouton supplémentaire, Evénement et colonnes supplémentaires, apparaît.
3. Cliquez sur ce nouveau bouton.



4. Dans l'écran suivant, sélectionnez la case à cocher Evénement et validation. Le flux de travaux créé dans le générateur de flux de travaux apparaît comme choix dans Evénement et validation.
5. Mettez ce choix en évidence. Sauvegardez votre sélection.
6. Si des informations supplémentaires (comme des codes de société, des intitulés d'unité commerciale etc.) sont requises dans le rapport de flux de travaux, ajoutez-les dans la section Définir des colonnes supplémentaires, puis cliquez sur Appliquer (pour sauvegarder). Lorsque vous avez terminé, fermez cette fenêtre.
7. Appliquez (sauvegardez) votre tâche d'audit. Appliquez (sauvegardez) l'intégralité de la définition de processus d'audit. Cliquez sur Exécuter une fois maintenant pour créer le rapport. Cliquez sur Afficher pour afficher le rapport.
8. Cliquez sur Exécuter une fois maintenant pour créer le rapport. Cliquez sur Afficher pour afficher le rapport.



Le bouton Evénement et colonnes supplémentaires apparaît dans toutes les tâches d'audit.

Remarque :

Si la sécurité au niveau des données, pour le niveau de données observé, a été activée (voir les paramètres Profil global), la sortie du processus d'audit est filtrée de sorte que les utilisateurs ne voient que les informations provenant de leurs bases de données.

Les choix de rapport lors de l'ajout d'une tâche d'audit répertorient deux rapports de procédure : Evénements en attente et Transition du statut de l'événement. Ajoutez-les à deux nouvelles tâches d'audit afin d'afficher les détails de tous les événements et de toutes les transitions de flux de travaux. Ces deux rapports ne sont pas filtrés (le filtrage de sécurité au niveau de données observé n'est pas appliqué). Ils sont disponibles par défaut dans la liste des rapports uniquement pour l'administrateur et pour les utilisateurs disposant du rôle d'administrateur.

Rubrique parent : Générateur de flux de travaux

Analytique de détection de menace

Guardium inclut l'analytique de détection de menace spécialisée, qui permet d'examiner et d'analyser des données auditées afin de détecter des symptômes pouvant indiquer divers types d'attaque de base de données.

L'analytique de détection de menace examine et analyse des données auditées afin de détecter des symptômes pouvant indiquer des attaques de base de données par injection SQL ou procédure mémorisée. Guardium ne s'appuie pas sur une comparaison à un dictionnaire de signatures d'attaque en constante évolution. A la place, il analyse l'activité des données d'audit, des exceptions et des données de valeur extrême (Détection des valeurs extrêmes) sur des périodes de temps étendues et recherche des modèles indiquant une attaque. En effectuant le suivi des événements suspects au fil du temps et en les mettant en corrélation, Guardium crée une vue d'ensemble des risques potentiels. Cette approche est plus souple et plus complète, et ne requiert pas de mise à jour régulière des signatures.

L'analyse de détection des menaces est prise en charge sur MySQL, Oracle et DB2.

- Caractéristiques d'une attaque par injection SQL
- Caractéristiques d'une attaque par procédure mémorisée
- Activation de l'analytique de détection de menace
  Cette rubrique décrit les exigences et les procédures relatives à l'activation de l'analytique de détection de menace.
- Utilisation de rapports de cas
  Cette rubrique explique comment utiliser des rapports de cas.
- Activation du flux de travaux du processus d'audit pour l'analytique de menace
  Cette procédure explique comment planifier et distribuer les processus d'audit requis pour l'utilisation des outils de diagnostic des menaces Guardium.
- Utilisation de tableaux de bord de diagnostic de menace
  Un tableau de bord de diagnostic de menace est un tableau de bord qui est appelé depuis un cas de menace spécifique dans le rapport Cas de STP malveillants suspectés ou Suspicion d'attaque par injection SQL.
- Fonctions d'analyse de la détection des menaces

Rubrique parent : Surveillance et audit

Caractéristiques d'une attaque par injection SQL

Les attaques par injection SQL tentent d'exploiter des vulnérabilités de l'application Web en concaténant une entrée utilisateur avec des requêtes SQL. Si elles aboutissent, ces attaques peuvent exécuter des commandes SQL malveillantes via la connexion d'application Web autorisée. Les attaques par injection SQL peuvent être difficiles à identifier car les étapes individuelles d'une attaque, analysées indépendamment les unes des autres, peuvent sembler normales. A l'aide de l'analytique de détection de menace, Guardium identifie les attaques par injection SQL potentielles en capturant les étapes individuelles et en les analysant dans le cadre d'une attaque complexe unique.

Les symptômes classiques d'une attaque par injection SQL que Guardium identifie sont les suivants :

- Un agresseur informatique tentant d'identifier la structure d'une requête SQL dynamique, par exemple le nombre de colonnes interrogées
- Un nombre anormalement élevé de nouvelles requêtes, notamment de requêtes structurées de façon unique ou inhabituelle
- Un accès à des tables contenant des informations sur la structure de la base de données

Rubrique parent : Analytique de détection de menace

Caractéristiques d'une attaque par procédure mémorisée

Une procédure mémorisée malveillante est un bloc de code conçu pour éviter toute détection et pour lancer des attaques complexes au cours d'une certaine période de temps. L'attaque peut se répéter exactement de la même façon ou bien ses caractéristiques peuvent changer au fil du temps. La procédure mémorisée peut être dormante pendant une période de temps étendue, ce qui la rend plus difficile à identifier comme étant suspecte. Même si une activité inhabituelle a été observée au cours d'un audit précédent, celle-ci est oubliée au moment de l'audit suivant. Une procédure mémorisée malveillante peut être utilisée pour déguiser la suppression d'une table importante, ou pour extraire le contenu d'une table.

Exemples d'activité suspecte : création d'une procédure mémorisée avec une instruction DROP pour des objets sensibles, verbe DROP, exceptions SQL générées par des objets manquants, procédure modifiée après avoir été dormante pendant une période de temps étendue.

Guardium effectue le suivi de l'activité relative à des procédures mémorisées individuelles et avec les données d'analyse des valeurs extrêmes, il met en corrélation les divers symptômes et utilisateurs. Il peut détecter les symptômes classiques suivants pour ce cas d'utilisation de procédure mémorisée malveillante (présentés dans l'ordre dans lequel ils apparaissent) :

1. Un administrateur de base de données crée une procédure malveillante A, qui supprime des données de la table client
2. Un mois plus tard, l'administrateur de base de données change une procédure B fréquemment utilisée afin d'appeler la procédure A
3. Un autre utilisateur appelle la procédure B modifiée, de sorte que les données de la table client sont supprimées par cet utilisateur innocent

Rubrique parent : Analytique de détection de menace

Activation de l'analytique de détection de menace

Cette rubrique décrit les exigences et les procédures relatives à l'activation de l'analytique de détection de menace.

Pour activer l'analytique de détection de menace :

- Assurez-vous de disposer de la quantité de mémoire requise minimale et de satisfaire les exigences de stockage pour la recherche (4 unités centrales et 24 Go de mémoire RAM).
- Vérifiez que votre système a consigné des données d'application. Spécifiquement, SQLI requiert des données d'application car l'injection est initiée à partir de l'application. Si le système "fait confiance" à l'application et ne la surveille pas dans Guardium, l'injection ne peut pas être identifiée.
- La détection de valeurs extrêmes n'est pas requise pour la détection de menace d'injection SQL, mais elle l'est pour la prise en charge complète de la détection des procédures mémorisées suspectes. Pour plus d'informations, voir Activation et désactivation de la détection de valeurs extrêmes localement sur un collecteur.
- Lors de la mise à niveau vers Guardium version 10.1 via le processus de mise à niveau, vous devez activer l'analyse pour la détection de menace sur chaque collecteur à l'aide de la commande d'API Guardium suivante : `grdapi enable_advanced_threat_scanning`. Pour plus d'informations sur les paramètres disponibles pour la commande enable_advanced_threat_scanning, consultez GrdAPI Threat Detection Analytics Functions.
- Configurez le processus d'audit pour envoyer des rapports de cas aux enquêteurs pertinents. Cette opération est facultative mais recommandée. Voir Activation du flux de travaux du processus d'audit pour l'analytique de menace pour plus d'informations.

Important : La détection de menace repose sur l'analyse et la corrélation des données consignées. Par conséquent, toute règle filtrant le trafic avant la consignation n'est pas prise en compte pour la détection de menace. Examinez soigneusement votre utilisation des règles IGNORER LA SESSION S-TAP afin de déterminer le risque que constitue la non-consignation de ces sessions par rapport à l'optimisation de la capacité du collecteur.

Exigences pour l'analyse des procédures mémorisées malveillantes

- L'algorithme d'analyse dépend en partie de groupes d'objets sensibles. Par défaut, il utilise des membres dans le groupe d'objets sensibles défini par le système (ID de groupe 5). Si vous avez déjà spécifié des groupes d'objets sensibles supplémentaires pour la détection de valeurs extrêmes, la détection de menace utilisera les mêmes groupes. Même si la détection de valeurs extrêmes n'est pas activée, vous pouvez définir vos propres groupes d'objets sensibles avec la même commande GuardAPI : `set_outliers_detection_parameter parameter_name="sensitiveObjectGroupIds" parameter_value=<ID de groupe>,<ID de groupe>,...`
- Des règles de politique doivent être installées pour que vous puissiez collecter le trafic nécessaire à l'analyse des procédures mémorisées malveillantes. Recommandation : Créez les règles ci-après dans votre politique dans l'ordre suggéré. Il est important de sélectionner la case à cocher Passer à la règle suivante pour toutes ces règles.
    1. Règle d'accès : Consigner l'ensemble des détails où le filtre de groupe de commandes est PROCEDURE DDL.
    2. Règle d'accès : Consigner l'ensemble des détails où le filtre de groupe de commandes est Commandes EXECUTE. Si votre base de données est Oracle, incluez la commande BEGIN dans la règle.
    3. Règle d'exception : Consigner uniquement lorsque le filtre des types d'erreur est SQL_ERROR.

Rubrique parent : Analytique de détection de menace

Utilisation de rapports de cas

Cette rubrique explique comment utiliser des rapports de cas.

Guardium analyse les symptômes au fil du temps, les met en corrélation et affecte un score par attaque possible identifiée. Si le score indique une attaque potentielle, l'ensemble d'événements devient un cas dont l'ID est unique sur chaque collecteur. Les cas sont externalisés dans des rapports de cas (un par attaque suspectée). Vous pouvez accéder aux rapports de cas comme suit :

- Configurez un processus d'audit afin de recevoir des notifications dans votre liste des tâches dans Central Manager, et ouvrez le rapport directement sur le collecteur associé pertinent. Notez que la liste des tâches est mise à jour une fois toutes les heures.
- Sélectionnez Examen > Exceptions.

La fenêtre des rapports de cas s'ouvre. Un rapport présente, par défaut, jusqu'à trois incidents (un par ligne). Chaque cas inclut un score de risque compris entre 1 et 3, 3 correspondant au risque le plus élevé. Vous pouvez :

- Survoler l'ID de cas pour afficher un récapitulatif de l'attaque (dossiers de procédure mémorisée seulement).
- Survoler l'ID de cas et cliquer sur Lier aux symptômes pour accéder au rapport détaillé sur les symptômes.
- Cliquez sur l'ID pour ouvrir le tableau de bord de diagnostic de menace propre au cas. Voir Utilisation de tableaux de bord de diagnostic de menace.

Restriction : Les rapports de cas présentent les restrictions suivantes :

- Il n'y a pas de sécurité au niveau des données.
- Ces rapports ne peuvent pas être clonés.
- Vous pouvez créer un rapport réparti pour ces rapports de cas ; toutefois, depuis Central Manager, il n'existe pas de lien direct depuis le rapport de cas vers le tableau de diagnostic de menace, ni d'infobulle supplémentaire ou de lien vers les symptômes.

Rubrique parent : Analytique de détection de menace

Activation du flux de travaux du processus d'audit pour l'analytique de menace

Cette procédure explique comment planifier et distribuer les processus d'audit requis pour l'utilisation des outils de diagnostic des menaces Guardium.

Pourquoi et quand exécuter cette tâche

Il existe deux processus d'audit préconfigurés qui contrôlent la distribution des rapports d'analytique de menace aux réviseurs appropriés :

- Cas de STP malveillants suspectés
- Cas d'injection SQL suspectés

Chaque processus extrait les cas suspectés pour un type d'attaque. Vous pouvez personnaliser ces processus ou copier et créer vos propres processus.

Procédure

1. Sélectionnez Conformité > Outils et vues > Générateur de processus d'audit. Si vous le souhaitez, filtrez les processus d'audit disponibles en cliquant sur le bouton d'option Inactif uniquement ou en entrant `Suspecté` dans la zone Filtrer.

   La tâche par défaut pour ce processus est le rapport correspondant (Cas de STP malveillants suspectés ou Cas d'injection SQL suspectés). Ne modifiez pas les paramètres d'exécution de ces rapports. Toutefois, vous pouvez ajouter des tâches supplémentaires à ce même processus d'audit. Par exemple, vous pouvez ajouter les deux rapports sur les menaces dans un seul processus d'audit.

   Si vous définissez ces processus d'audit depuis un gestionnaire central, définissez une tâche pour chaque collecteur pour lequel vous voulez afficher les données relatives aux menaces et utilisez l'option Source de données distante.

2. Cliquez sur Envoyer les résultats pour définir les récepteurs du processus d'audit devant recevoir les rapports sur les procédures mémorisées malveillantes suspectées.
3. Sélectionnez le récepteur par défaut (utilisateur), puis cliquez sur l'icône  afin de définir le ou les récepteurs appropriés pour votre organisation. Lorsque vous avez terminé, cliquez sur OK.
4. Cliquez sur Planifier un processus d'audit et révisez la planification pour le processus d'audit.

   Il est recommandé d'exécuter le processus tous les jours, toutes les heures à partir de 12h30 (généralement après l'exécution de la détection de valeurs extrêmes et des menaces). Notez que la case à cocher Exécution automatique des travaux dépendants n'a pas d'effet pour cette tâche.

   Important : Assurez-vous que la case à cocher Activer la planification est sélectionnée.
5. Cliquez sur Suivant, puis sur Sauvegarder, pour terminer la définition du processus d'audit.

Rubrique parent : Analytique de détection de menace

Utilisation de tableaux de bord de diagnostic de menace

Un tableau de bord de diagnostic de menace est un tableau de bord qui est appelé depuis un cas de menace spécifique dans le rapport Cas de STP malveillants suspectés ou Suspicion d'attaque par injection SQL.

un tableau de bord de diagnostic de menace effectue sensiblement les mêmes opérations que les autres tableaux de bord d'investigation, mais il est rempli avec des données provenant d'événements suspects (utilisateur de base de données, serveur, objets, etc.) et il utilise divers graphiques pour fournir différentes vues de l'événement et des événements connexes, qui peuvent être utiles lors de l'examen de l'attaque potentielle. Les données de valeur extrême et de recherche pertinentes sont également disponibles dans la page des graphiques du tableau de bord.

Dans la plupart des cas, il n'est pas nécessaire de changer les filtres existants pour les tableaux de bord de diagnostic de menace prédéfinis. Toutefois, si vous voulez procéder à votre propre analyse comparative, vous pouvez les modifier.

Voir Tableau de bord d'investigation pour plus d'informations sur l'utilisation de filtres de tableau de bord et de graphique.

Conseil : Vous ne pouvez ouvrir le tableau de bord de diagnostic de menace qu'en cliquant sur le numéro de cas dans le rapport sur les menaces approprié. Vous ne pouvez pas sauvegarder les modifications dans ce tableau de bord ou tout autre tableau de bord prédéfini. Si vous apportez des modifications et voulez garder le tableau de bord pour un examen ultérieur, vous devez le copier et le sauvegarder sous un nouveau nom. Vous devez aussi sauvegarder les filtres en cliquant sur le menu Filtres et en sélectionnant Sauvegarder.

Les données de référence constituent un ensemble de filtres prédéfinis propres à un graphique, pour l'analytique de détection de menace seulement, qui affichent des données similaires au cas que vous examinez, mais qui ne sont pas incluses dans le filtre de tableau de bord général. Les données de référence ne peuvent pas être changées par les utilisateurs. Survolez l'icône de filtre dans chaque graphique pour afficher les données de référence.

Dans un scénario standard d'attaque par injection SQL suspectée, le tableau de bord de diagnostic de menace est filtré pour cette attaque et inclut les filtres de tableau de bord généraux suivants :

- Serveur : 8.34.223.145
- Utilisateur de base de données : USER1
- Base de données : 8.4.134.213:31.5.12
- Type de base de données : MYSQL
- Objet : stp1_name

Le graphique pour l'utilisateur de base de données peut inclure des données de référence pour des utilisateurs de base de données similaires, comme USER2, USER3 et USER4. Ainsi, vous pouvez comparer les activités de l'utilisateur suspecté avec celles d'utilisateurs similaires, même si ces utilisateurs supplémentaires ne sont pas inclus dans les filtres de tableau de bord généraux.

Les champs n'incluent pas tous des données de référence associées. Tout champ pour lequel il n'existe pas de filtre de référence prédéfini est filtré comme dans le tableau de bord.

Dans certains graphiques, vous pouvez désactiver les filtres afin de comparer les données quels que soient les filtres choisis pour l'intégralité du tableau de bord. Vous obtenez ainsi une vue plus large de l'activité.

Cliquez sur l'icône de filtre pour ouvrir la fenêtre Paramètres de filtre de graphique et y apporter vos modifications.

- Examen des menaces d'injection SQL
- Examen des menaces de procédure mémorisée

Rubrique parent : Analytique de détection de menace

Examen des menaces d'injection SQL

Pourquoi et quand exécuter cette tâche

Cette procédure décrit l'examen d'une attaque par injection SQL suspectée dans le tableau de bord de diagnostic de menace.

Procédure

1. Depuis la liste des tâches ou depuis Examen > Exceptions, ouvrez le tableau de bord Cas d'injection SQL suspectés. Chaque ligne présente un cas, avec une évaluation de la probabilité d'une attaque et le niveau de risque de l'attaque.
2. Cliquez sur Afficher pour évaluer des faux positifs. Survolez l'ID de cas sélectionné et cliquez sur Symptômes pour ouvrir la page Symptômes de cas d'injection SQL. Chaque action suspecte est décrite et la chaîne SQL est affichée. Vous pouvez voir les modifications exactes que l'utilisateur a apporté aux chaînes. En progressant de chaîne en chaîne, vous pouvez déterminer la façon dont l'agresseur informatique a pu obtenir des données méthodiquement en se servant d'erreurs renvoyées par des requêtes précédentes.
3. Cliquez sur le numéro représentant l'ID afin d'ouvrir le tableau de bord de diagnostic par défaut pour les attaques par injection SQL, qui est filtré par date d'incident et détails de connexion d'application Web suspectée. Ainsi, vous pouvez restreindre l'examen au trafic de base de données qui a eu lieu au cours de l'attaque. Vous pouvez changer ou supprimer le filtre afin d'élargir la portée de l'examen. Utilisez la grille du bas pour obtenir plus de détails sur les données du graphique. Notez que si vous passez à un tableau de bord standard, tous les filtres définis pour l'attaque par injection SQL suspectée sont annulés.
4. Suivez les instructions ci-dessous lorsque vous examinez les graphiques :
   - Changez l'échelle de temps pour rechercher des pics au moment de l'attaque
   - Recherchez toute violation de politique de sécurité et déterminez si des violations sont associées à une autre activité au moment de l'attaque
5. Procédez à une exploration en aval en changeant les filtres, la période, etc., pour déterminer s'il existe des différences sur le système.
6. Evaluez les graphiques dans le tableau de bord :

   Nombre d'activités par heure et objet
   : Ce graphique présente les objets de base de données les plus utilisés au moment de l'attaque. En étendant la période du tableau de bord, vous pouvez comparer les différences d'activité avant et après l'attaque. Cliquez sur une cellule si vous voulez filtrer sur un objet particulier. La couleur indique des noms d'objet différents.

   Nombre d'erreurs par heure et erreur
   : Ce graphique présente le nombre d'erreurs SQL qui ont été générées par l'application Web. Un nombre élevé d'erreurs SQL peut indiquer qu'un certain type d'attaque par injection SQL a lieu. La couleur indique des types d'erreur différents.

   Nombre de valeurs extrêmes par heure et motif de valeur extrême
   : Une attaque par injection SQL implique un grand nombre de nouvelles requêtes possédant une structure différente des requêtes habituelles. Ces requêtes génèrent des valeurs extrêmes. Utilisez ce graphique pour observer le volume et le score des valeurs extrêmes générées par l'application Web attaquée.

   Nombre de violations par heure et violation
   : Au cours d'une attaque par injection SQL, l'agresseur informatique est susceptible d'enfreindre des politiques de sécurité consignant l'accès à des objets non autorisés. Comparez le nombre de violations et les types de violation afin de comprendre le risque de l'attaque.

   Types d'erreur suspecte
   : Utilisez ce graphique pour explorer des erreurs SQL spécifiques qui sont utilisées dans les attaques par injection SQL afin d'exploiter la vulnérabilité. Cliquez sur une cellule pour filtrer la recherche et examinez l'instruction SQL qui a généré cette erreur. Vous remarquerez peut-être un code SQL injecté.

   Noms d'objet suspect
   : Utilisez ce graphique pour afficher les objets suspects qui sont utilisés au cours des attaques par injection SQL. Etendez la période de recherche pour déterminer si ces objets ont été utilisés avant le début de l'attaque. Comparez le nombre d'utilisations de ces objets.

Rubrique parent : Utilisation de tableaux de bord de diagnostic de menace

Examen des menaces de procédure mémorisée

Pourquoi et quand exécuter cette tâche

Cette procédure décrit l'examen d'une attaque par procédure mémorisée suspectée dans le tableau de bord de diagnostic de menace.

Procédure

1. Depuis la liste des tâches ou depuis Examen > Exceptions, ouvrez le tableau de bord Cas de STP malveillants suspectés. Chaque ligne présente un cas, avec une évaluation de la probabilité d'une attaque et le niveau de risque de l'attaque.
2. Cliquez sur Afficher pour évaluer des faux positifs.
3. Survolez l'ID de cas sélectionné pour afficher les détails du cas.
4. Cliquez sur un symptôme pour ouvrir la page Symptômes de cas STP malveillants.
5. 5. Cliquez sur le numéro représentant l'ID afin d'ouvrir le tableau de bord de diagnostic par défaut pour les attaques par injection SQL, qui est filtré par date d'incident et détails de connexion d'application Web suspectée. Ainsi, vous pouvez restreindre l'examen au trafic de base de données qui a eu lieu au cours de l'attaque. Vous pouvez changer ou supprimer le filtre afin d'élargir la portée de l'examen. Utilisez la grille du bas pour obtenir plus de détails sur les données du graphique.
6. Suivez les instructions ci-dessous lorsque vous examinez les graphiques :
   - Changez l'échelle de temps pour rechercher des pics au moment de l'attaque
   - Recherchez toute violation de politique de sécurité et déterminez si des violations sont associées à une autre activité au moment de l'attaque
7. Procédez à une exploration en aval en changeant les filtres, la période, etc., pour déterminer s'il existe des différences sur le système.
8. Evaluez les graphiques dans le tableau de bord :

   Comparaison des erreurs sur différents serveurs
   : Utilisez ce graphique pour déterminer si ce serveur et cet utilisateur de base de données présentent exceptionnellement plus d'erreurs que d'autres serveurs et utilisateurs de base de données.

   Comparaison des erreurs pour différents utilisateurs de base de données dont le comportement est similaire
   : Utilisez ce graphique pour comparer les types d'erreur et le nombre d'erreurs pour cet utilisateur de base de données par rapport à ceux d'utilisateurs de base de données similaires. Un utilisateur de base de données similaire peut être tout utilisateur ayant créé des procédures mémorisées.

   Activités similaires sur des procédures mémorisées pour cet utilisateur de base de données
   : Utilisez ce graphique pour voir les procédures mémorisées que l'utilisateur a créées/modifiées au cours de la période spécifiée. Le graphique est filtré en fonction d'un verbe. Utilisez-le également pour procéder à une exploration en aval et voir les actions que l'utilisateur a effectuées sur les différentes procédures mémorisées.

   Comparaison des violations pour des utilisateurs de base de données dont le comportement est similaire
   : Comparez le nombre de violations et les types de violation (politique) pour les utilisateurs de base de données qui créent des procédures mémorisées.

Comparaison des valeurs extrêmes pour des utilisateurs de base de données dont le comportement est similaire
: Utilisez ce graphique pour comparer le nombre et le type de valeurs extrêmes pour cet utilisateur de base de données avec ceux d'autres utilisateurs de base de données qui créent des procédures mémorisées.

Valeurs extrêmes par données pour cet utilisateur de base de données
: Utilisez ce graphique pour observer le volume et le score des valeurs extrêmes pour l'utilisateur de base de données spécifié.

Rubrique parent : Utilisation de tableaux de bord de diagnostic de menace

GuardAPI Threat Detection Analytics Functions

enable_advanced_threat_scanning

Enables the scanner processes to check for specific database attacks such as SQL injection and malicious stored procedures.

Parameter	Value	Description
all		Optional. In a central management configuration only, enables all threat detection scanners on all managed units. Allowable values: `true`, `false`.
schedule_start		Optional. Specifies the date and time to start running the processes. The accepted format is yyyy-mm-dd hh:mm:ss (24-hour clock).
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

```
grdapi enable_advanced_threat_scanning all=true schedule_start="2016-03-24 12:00:05”
```

You will see the following message if threat analytics is enabled when outlier detection is not:

```
Warning - Enabling advance threat scanning (AKA Eagle Eye) when Analytic anomaly detection is disabled.
Advance threat scanning (AKA Eagle Eye) enabled.
ok
```

disable_advanced_threat_scanning

Disables threat detection scanners on the collector.

Parameter	Value	Description
all		In a central management configuration only, disables all threat detection scanners on all managed units.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

get_eagle_eye_info

Displays the current settings for threat detection parameters.

Parameter	Value	Description

Parameter	Value	Description
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

```
grdapi get_eagle_eye_info
Eagle Eye Parameters Values:
EI_CASES_DISPLAY_LIMIT = 3
EI_CONFIDENCE_PCT_CHANGE_TO_REDISPLAY_CASE = 30
EI_EAGLE_EYE_ENABLED = 1
EI_PROCESSOR_TIMEOUT_SEC = 420
EI_SCANNER_PATCH_DEF = 10
EI_SCANNER_TIMEOUT_SEC = 300ok
```

set_eagle_eye_parameter

Use under the direction of IBM personnel. Changes configuration parameters for threat detection. These parameters must be set explicitly using `parameter_name` and `parameter_value` as follows:

```
set_eagle_eye_scanner_parameter parameter_name=[parameter] parameter_value=[value]
```

Parameter	Value	Description
EI_CASES_DISPLAY LIMIT		The number of cases to be displayed in the to-do list report. Default is 3.
EI_CONFIDENCE_PCT_CHANGE_TO_REDISPLAY CASE		The percent of “confidence” change that will cause this case to be redisplayed in the to-do list report, even if it has already appeared before. This can happen if Guardium detects another symptom or symptoms that raise the confidence by this percentage value. Default is 30.
EI_PROCESSOR_TIMEOUT_SEC		Processors that run longer time than this threshold are turned off. Default is 420 seconds.
EI_SCANNER_PATCH_DEF		To avoid false positives as a result of patch installation, if in a single process run the number of stored procedures created exceeds this parameter then the process assumes a patch is installed and it stops analyzing symptoms. Default is 10 stored procedure creations detected in one run.
EI_SCANNER_TIMEOUT_SEC		Scanners that run longer time than this threshold are turned off. Default is 300 seconds.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

get_eagle_eye_scanners_info

Return scanner settings information.

Parameter	Value	Description

Parameter	Value	Description
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

The data returned will contain the following information:

Field	Description
ID	The scanner ID.
Name	The scanner name.
Status	The status of the scanner from the last run: I: in progress D: done K: killed E: done with errors
Enabled	Indicates if the scanner is enabled. True: enabled False: disabled
Permanent disabled	If the scanner was disabled 3 times in 24 hours, then it is permanently disabled. True: disabled False: enabled

Example:

```
grdapi get_eagle_eye_scanners_info
ID=0
ID:1, Name:SQLInjectionExceptionsScanner, Status:D, Enabled:true, Permanent disabled:false
ID:2, Name:NumNewConstructScanner, Status:D, Enabled:true, Permanent disabled:false
ID:3, Name:SQLInjectionSuspiciousObjectScanner, Status:D, Enabled:true, Permanent disabled:false
ID:4, Name:SqliQueryScanner, Status:Unknown, Enabled:false, Permanent disabled:true
ID:5, Name:EagleEyeSTPCreateProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:6, Name:EagleEyeSTPCallProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:7, Name:EagleEyeSTPExceptionProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:8, Name:EagleEyePreviousStpUsageProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:9, Name:EagleEyeSTPViolationProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:10, Name:EagleEyeSTPUserOutlierScanner, Status:D, Enabled:true, Permanent disabled:false
ok
```

set_eagle_eye_scanner_parameter

Use under the direction of IBM personnel. Activate or deactivate a scanner. These parameters must be set explicitly using `parameter_name` and `parameter_value` as follows:

```
set_eagle_eye_scanner_parameter parameter_name=[parameter] parameter_value=[value]
```

Parameter	Value	Description
scanner_id		Required. The unique ID of the scanner, which you can get from get_eagle_eye_scanners_info GuardAPI command.
is_active		Defines if the scanner should run. Used to start a scanner that was stopped automatically because it timed out. 0 : the scanner is stopped 1: the scanner is activated

Parameter	Value	Description
is_permanent_inactive		If the scanner was permanently disabled after it was disabled 3 times in 24 hours then it can only be enabled again using this GuardAPI. 1: the scanner is stopped permanently 0: the scanner is enabled
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

The following example reactivates a permanently deactivated scanner.

```
set_eagle_eye_scanner_parameter scanner_id=2 parameter_name=is_permanent_inactive parameter_value=0
```

get_eagle_eye_symptom_period_hours

Show the value of the symptom period parameter in hours. The symptom period determines how long back the process is looking and analyzing the collected symptoms for one case.

Parameter	Value	Description
case_name		Required. The case type. The following values are allowed: STP: malicious stored procedure case SQL_INJECTION: SQL Injection case
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

```
grdapi get_eagle_eye_symptom_period_hours case_name=STP
The symptoms period for case type: STP is: 168 in hours
ok
```

set_eagle_eye_symptom_period_hours

Set a value for the symptom period parameter in hours. The symptom period determine how long back the process is looking and analyzing the collected symptoms for a case.

Parameter	Value	Description

Parameter	Value	Description
case_name		Required. The case type. The following values are allowed: STP: malicious stored procedure case SQL_INJECTION: SQL Injection case
symptom_period_hours		Required. Integer. The number of hours in the past to analyze symptoms for a case.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

```
grdapi set_eagle_eye_symptom_period_hours case_name=STP symptom_period_hours=170
The symptoms period for case type: STP was changed. The old value was: 168. The new value is: 170
ok
```

get_eagle_eye_debug_level

For use by IBM Service personnel. Displays current debug level:

- 1: on
- 0: off

Parameter	Value	Description
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

```
grdapi get_eagle_eye_debug_level
ID=0
component=EAGLE_EYE level=1
ok
```

set_eagle_eye_debug_level

For use by IBM Service personnel. Displays current debug level.

Parameter	Value	Description
level		Integer. Required. Allowable values: 1: on 0: off

Parameter	Value	Description
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

```
grdapi set_eagle_eye_debug_level level=0
ID=0
ok
```

Parent topic: GuardAPI Reference

Tableau de bord d'investigation

Le tableau de bord d'investigation fournit des outils puissants permettant d'identifier et d'évaluer les problèmes pouvant exister dans votre environnement Guardium. Il utilise des données non filtrées locales ou système et fournit de nombreuses options de filtrage pour interroger les données dans un environnement Guardium entier, potentiellement depuis tout collecteur Guardium dans cet environnement.

Le tableau de bord d'investigation fournit des graphiques apparentés qui permettent de révéler des patterns, des anomalies et des relations dans vos données. Il ne requiert pas une connaissance approfondie des schémas de topologie, d'agrégation ou d'équilibrage de charge. Il contient les fonctions originales de recherche rapide pour les entreprises, ainsi que d'autres outils de visualisation et d'analyse des données.

Remarque : Il est recommandé d'afficher le tableau de bord d'investigation en mode plein écran.
Restriction : Le tableau de bord d'investigation et la sécurité au niveau des données ne peuvent pas être activés simultanément.

Modes d'exploitation

Le tableau de bord d'investigation prend en charge trois modes d'exploitation :

Central Manager only

Les requêtes qui sont soumises dans une instance de Central Manager renvoient des résultats au niveau de l'entreprise depuis tous les collecteurs Guardium pour lesquels la fonction de recherche est activée. Les requêtes qui sont soumises sur des unités gérées renvoient des résultats locaux.

Central Manager only est le mode d'exploitation par défaut.

All machines

Les requêtes de recherche au niveau de l'entreprise sont soumises depuis n'importe quelle machine de l'environnement Guardium pour laquelle la fonction de recherche est activée. Avec ce mode, l'obtention des résultats de recherche est plus lente et une connectivité entre toutes les unités gérées dans l'environnement est requise.

Local only

Ce mode limite les requêtes de recherche au collecteur local sur lequel la recherche est soumise : aucune donnée n'est extraite d'autres collecteurs se trouvant dans l'environnement Guardium. Sur un gestionnaire central en mode Local only, aucune donnée n'est affichée.

Voir GuardAPI Quick Search for Enterprise Functions pour des informations sur la définition du mode de recherche.

Composants de tableau de bord

Un tableau de bord est une collection d'un ou de plusieurs éléments :

- Des graphiques de données à trois axes, aussi appelés graphiques trimétriques. Ils peuvent être affichés sous forme de table des couleurs, diagramme à barres, graphique à bulles, diagramme linéaire, graphique circulaire, graphique en escalier et graphiques à zones.
- Un graphique à bulles animé - visualisation animée des modifications de données effectuées au cours des dernières 48 heures.
- Un graphique d'activité - graphique à courbes affichant le volume des activités et les valeurs extrêmes. Il se trouve au-dessus de la table des résultats.
- Une table des résultats - fournit les résultats de recherche et les fonctions d'investigation de la recherche rapide originale. La table des résultats se trouve toujours au bas du tableau de bord. Elle peut être ajoutée à n'importe quel tableau de bord.
- Une liste de facettes pouvant contenir l'une ou plusieurs des facettes suivantes : Où, Qui, Quoi, Exception, Quand. Elle apparaît dans la partie gauche de chaque tableau de bord et ne peut pas être supprimée.

Il existe quatre vues de surveillance de l'activité des données (DAM) par défaut et deux vues de surveillance de l'activité des fichiers (FAM) par défaut, comportant chacune des graphiques et des tables différents. Sélectionnez la vue dans le menu du tableau de bord  . Les vues par défaut ne peuvent pas être modifiées.

- Activation et désactivation du tableau de bord d'investigation
  Cette rubrique explique comment activer et désactiver le tableau de bord d'investigation.
- Activation de l'activité des fichiers dans le tableau de bord d'investigation
- Accès au tableau de bord d'investigation
- Tableau de bord d'investigation pour les données
  Le tableau de bord d'investigation comporte un groupe prédéfini de graphiques ainsi qu'une table qui vous permettent de comprendre ce qui se passe sur votre système à tout moment, et que vous pouvez utiliser comme point de départ pour créer vos propres tableaux de bord personnalisés.
- Tableau de bord d'investigation pour les fichiers
  Le tableau de bord d'investigation comporte un groupe prédéfini de graphiques ainsi qu'une table qui vous permettent de comprendre ce qui se passe sur votre système à tout moment, et que vous pouvez utiliser comme point de départ pour créer vos propres tableaux de bord personnalisés.
- Filtrage des données et sauvegarde des filtres dans le tableau de bord d'investigation
- Filtrage d'un graphique individuel
- Création, sauvegarde et exportation des tableaux de bord d'investigation
- Utilisation de la vue de topologie
  La vue de topologie est une visualisation des dispositifs Guardium dans les résultats de recherche.
- Recherche locale et recherche distribuée
- Utilisation de l'analyse approfondie des données
  La visualisation de l'analyse approfondie des données permet à l'utilisateur d'examiner en détail une séquence d'événements capturés par le système Guardium. Elle fournit une image complète de l'activité dans une fenêtre de temps spécifique et permet de détecter tout comportement inhabituel.

Rubrique parent : Surveillance et audit
Information associée:
GuardAPI Investigation Dashboard Functions
Investigation Dashboard CLI Commands

Activation et désactivation du tableau de bord d'investigation

Cette rubrique explique comment activer et désactiver le tableau de bord d'investigation.

Avant de commencer

La configuration matérielle minimale requise pour le tableau de bord d'investigation est la suivante :

- Une architecture 64 bits
- 24 Go de mémoire RAM
- Une unité centrale à 4 coeurs

Restriction : Le tableau de bord d'investigation et la sécurité au niveau des données ne peuvent pas être activés simultanément.

Pourquoi et quand exécuter cette tâche

Les étapes ci-dessous permettent d'activer ou de désactiver la recherche.

Procédure

1. Connectez-vous à la machine en tant qu'utilisateur ou administrateur possédant le rôle CLI.
2. Utilisez la commande GuardAPI suivante pour activer le tableau de bord d'investigation :

   ```
   grdapi enable_quick_search schedule_interval=2 schedule_units=MINUTE
   ```

   Par défaut, les violations ne sont pas incluses dans les résultats de recherche. Pour les inclure, associez le paramètre includeViolations à la valeur `true` :

   ```
   grdapi enable_quick_search schedule_interval=2 schedule_units=MINUTE includeViolations=true
   ```

   Pour activer la détection des valeurs extrêmes, voir Détection des valeurs extrêmes.

   Vous pouvez spécifier des paramètres supplémentaires, comme l'intervalle de mise à jour de l'index de recherche. Pour la liste complète des paramètres et leur description, voir la documentation de référence GuardAPI Investigation Dashboard Functions.

3. Utilisez la commande GuardAPI suivante pour désactiver la fonction de tableau de bord d'investigation à tout moment :

   ```
   grdapi disable_quick_search
   ```

Résultats

Une fois le tableau de bord d'investigation activé, voir Accès au tableau de bord d'investigation pour en savoir plus sur l'utilisation du tableau de bord d'investigation.

Avertissement :

- La fonctionnalité Tableau de bord d'investigation ouvre les ports 8983 et 9983 sur les gestionnaires centraux et les collecteurs. Les ports sont ouverts lorsque le tableau de bord d'investigation est activé, et fermés lorsqu'il est désactivé. Avant d'utiliser le tableau de bord d'investigation, assurez-vous que la communication bidirectionnelle entre les gestionnaires centraux et les collecteurs sur les ports 8983 et 9983 n'est pas bloquée par un pare-feu.
- Les données de recherche indexées sont conservées pendant trois jours. Utilisez la commande de l'interface de ligne de commande Guardium purge object pour changer la durée de conservation. Par exemple, la commande suivante définit une durée de conservation de cinq jours : store purge object age 39 5. Notez que `39` est le numéro d'identification d'objet par défaut associé à l'index de recherche. Pour plus d'informations, voir la documentation de référence Configuration and Control CLI Commands.

Rubrique parent : Tableau de bord d'investigation

Information associée:
GuardAPI Investigation Dashboard Functions
Investigation Dashboard CLI Commands

Activation de l'activité des fichiers dans le tableau de bord d'investigation

Avant de commencer

- L'offre groupée de surveillance de l'activité des fichiers (FAM) doit être installée et configurée. Voir Paramètres GIM pour la reconnaissance et la classification de fichiers.
- Le tableau de bord d'investigation doit être activé. Voir Activation et désactivation du tableau de bord d'investigation.
- N'utilisez pas le moteur d'exploration FAM V10.1 avec le système Guardium V10.0. N'utilisez pas le moteur d'exploration FAM V10.0 avec le système Guardium V10.1.

Pourquoi et quand exécuter cette tâche

Remarque : La fonction de surveillance de l'activité des fichiers (FAM) demande au serveur les adresses IP de serveur et utilise la première qu'elle trouve. Il n'est pas possible de sélectionner l'adresse IP "appropriée" depuis un nom d'hôte possédant plusieurs adresses IP. Les clients doivent spécifier l'adresse IP explicitement pour s'assurer que cette adresse IP apparaîtra dans les rapports.

Procédure

1. Sur le collecteur, à l'invite de l'interface de ligne de commande, exécutez la commande GuardAPI :
   `grdapi enable_fam_crawler [extraction_start] [schedule_start] [activity_schedule_interval] [activity_schedule_units] [entitlement_schedule_interval] [entitlement_schedule_units]` Exemple : la commande suivante envoie des résultats de reconnaissance et de classification mis à jour à la recherche d'entreprise, toutes les deux minutes pour les données de classification et tous les jours pour les informations d'autorisation.
   `grdapi enable_fam_crawler activity_schedule_interval=2 activity_schedule_units=MINUTE entitlement_schedule_interval=1 entitlement_schedule_units=DAY`
   Par défaut, l'extraction commence lorsque vous entrez la commande et le processus extrait les données à partir du moment où vous avez entré la commande.
2. Répétez cette opération sur chaque collecteur.

Rubrique parent : Tableau de bord d'investigation
Concepts associés:
Tableau de bord d'investigation pour les fichiers
Information associée:
GuardAPI Investigation Dashboard Functions

Accès au tableau de bord d'investigation

Procédure

1. Cliquez sur Examen > Recherche d'activité de données ou Examen > Recherche d'activité de fichiers.
2. Vous pouvez aussi activer la recherche dans l'interface utilisateur et rechercher le tableau de bord d'investigation. Ensuite, sélectionnez Recherche d'activité de données ou Recherche d'activité de fichiers.

Résultats

Le tableau de bord d'investigation par défaut pour les données ou les fichiers s'ouvre. Par défaut, le seul filtre qui est appliqué à l'intégralité du tableau de bord permet d'afficher l'heure la plus récente des données.
Rubrique parent : Tableau de bord d'investigation

Tableau de bord d'investigation pour les données

Le tableau de bord d'investigation comporte un groupe prédéfini de graphiques ainsi qu'une table qui vous permettent de comprendre ce qui se passe sur votre système à tout moment, et que vous pouvez utiliser comme point de départ pour créer vos propres tableaux de bord personnalisés.

Il existe quatre vues par défaut pour la surveillance de l'activité des données (DAM), comportant chacune des graphiques et des tables différents. Sélectionnez la vue dans le menu du tableau de bord  . Les vues par défaut ne peuvent pas être modifiées.

Les tableaux de bord par défaut contiennent des données pour la dernière heure écoulée, présentées sous l'une ou plusieurs des formes suivantes :

- Dans des graphiques trimétriques (graphiques de données à trois axes). La vue par défaut est une table des couleurs. Vous pouvez aussi choisir les vues suivantes : diagramme à barres, graphique à bulles, diagramme linéaire, graphique circulaire, graphique en escalier et graphique à zones.
- Dans une table des résultats : celle-ci contient les résultats de recherche et les fonctions d'investigation de la recherche rapide originale. La table des résultats se trouve toujours au bas du tableau de bord. Elle peut être ajoutée à n'importe quel tableau de bord. Les onglets sont les suivants :
  - Activité : onglets Récapitulatif et Détails. Chaque ligne dans l'onglet Récapitulatif indique le nombre d'instances des activités enregistrées par paire serveur-base de données ainsi que le nombre de types de base de données. Le récapitulatif détaillé indique le nombre de programmes source, d'utilisateurs de base de données et d'utilisateurs du système d'exploitation, le nom d'hôte du client, l'adresse IP du client et la date. Chaque ligne dans l'onglet Détails comporte des détails complets sur une activité.
  - Valeurs extrêmes : voir Interprétation des valeurs extrêmes dans le tableau de bord d'investigation.
  - Erreurs : onglets Récapitulatif et Détails. Chaque ligne dans l'onglet Récapitulatif indique le nombre d'instances des erreurs signalées et le nombre de types de base de données et d'utilisateurs de base de données. Le récapitulatif détaillé indique également le nombre d'adresses IP client, les types d'erreur et les dates. Chaque ligne dans l'onglet Détails comporte des détails complets sur une erreur.
  - Violations : onglets Récapitulatif et Détails. Chaque ligne dans l'onglet Récapitulatif indique le nombre d'instances des violations enregistrées par paire serveur-base de données ainsi que le nombre de types de base de données. Le récapitulatif détaillé indique le nombre de programmes source, d'utilisateurs

de base de données et d'utilisateurs du système d'exploitation, le nom d'hôte du client, l'adresse IP du client, la gravité, la violation et la date. Chaque ligne dans l'onglet Détails comporte des détails complets sur une violation.

Les vues supplémentaires que vous pouvez ajouter ou ouvrir sont les suivantes :

- Une vue de topologie Vue des statuts de serveur de recherche : voir Utilisation de la vue de topologie
- Un graphique à bulles animé : visualisation animée des modifications de données effectuées au cours des dernières 48 heures. Le graphique décrit le comportement des objets sur une période de 24 heures. Chaque objet est représenté par un cercle, et sa surface ainsi que sa position (axe des X et axe des Y) représentent trois variables sélectionnées par l'utilisateur. L'animation présente le comportement de l'objet sur 24 heures. Le graphique est accessible depuis la liste déroulante Ajouter un graphique.
- Un graphique d'activité : graphique à courbes affichant le volume des activités et les valeurs extrêmes, qui se trouve au-dessus de la table de résultats. Il est accessible depuis la liste déroulante Ajouter un graphique.
- Une analyse approfondie des données : visualisation 3D des activités de données. Voir Utilisation de l'analyse approfondie des données. Elle est accessible depuis la liste déroulante Ajouter un graphique.

Contrôles et options figurant dans cette page :

- Une liste de facettes catégorisées pouvant contenir les facettes Où, Qui, Quoi, Exception et Quand depuis les résultats de recherche apparaît dans la partie gauche de chaque tableau de bord et ne peut pas être retirée. Filtrez l'intégralité du tableau de bord à l'aide de facettes spécifiques en développant la liste et en cliquant sur des facettes individuelles.
- La ligne Filtres actifs dans la partie supérieure de la fenêtre affiche les filtres appliqués. Supprimez des filtres en cliquant sur  .
- Une zone de recherche : recherche de texte libre qui filtre les résultats dans toutes les zones simultanément, quelle que soit la facette.
-  La recherche distribuée : voir Recherche locale et recherche distribuée.
- La plage de temps pour laquelle les données sont présentées : modifiez-la en cliquant sur la liste déroulante dans le coin supérieur droit. Les options sont les suivantes : dernière heure, 3 dernières heures, dernier jour, 3 derniers jours, toute plage de temps que vous spécifiez. L'option par défaut est une heure.
- Une liste déroulante des filtres : voir Filtrage des données et sauvegarde des filtres dans le tableau de bord d'investigation.
-  Ajout d'un nouveau tableau de bord  Sauvegarde des modifications dans le tableau de bord  Sauvegarde du tableau de bord en tant que : voir Création, sauvegarde et exportation des tableaux de bord d'investigation.

Rubrique parent : Tableau de bord d'investigation
Concepts associés:
Interprétation des valeurs extrêmes dans le tableau de bord d'investigation
Tâches associées:
Utilisation de la vue de topologie
Utilisation de l'analyse approfondie des données

Tableau de bord d'investigation pour les fichiers

Le tableau de bord d'investigation comporte un groupe prédéfini de graphiques ainsi qu'une table qui vous permettent de comprendre ce qui se passe sur votre système à tout moment, et que vous pouvez utiliser comme point de départ pour créer vos propres tableaux de bord personnalisés.

Il existe deux vues de surveillance de l'activité des fichiers (FAM) par défaut, comportant chacune des graphiques et des tables différents. Sélectionnez la vue dans le menu du tableau de bord  . Les vues par défaut ne peuvent pas être modifiées.
Remarque : L'adresse IP du serveur et l'adresse IP du client sont toujours identiques dans le tableau de bord, sauf en cas de connexion via le bureau à distance sous Windows. L'adresse IP du client n'est prise en charge qu'en cas de connexion via une session de bureau à distance.
Remarque : La fonction de surveillance de l'activité des fichiers (FAM) demande au serveur les adresses IP de serveur et utilise la première qu'elle trouve. Il n'est pas possible de sélectionner l'adresse IP "appropriée" depuis un nom d'hôte possédant plusieurs adresses IP. Spécifiez l'adresse IP explicitement pour vous assurer que cette adresse IP apparaîtra dans les rapports.
Les tableaux de bord par défaut contiennent des données pour la dernière heure écoulée, présentées sous l'une ou plusieurs des formes suivantes :

- Dans des graphiques trimétriques (graphiques de données à trois axes). La vue par défaut est une table des couleurs. Vous pouvez aussi choisir les vues suivantes : diagramme à barres, graphique à bulles, diagramme linéaire, graphique circulaire, graphique en escalier et graphique à zones.

- Dans une table des résultats : celle-ci contient les résultats de recherche et les fonctions d'investigation de la recherche rapide originale. La table des résultats se trouve toujours au bas du tableau de bord. Elle peut être ajoutée à n'importe quel tableau de bord. Les onglets sont les suivants :

    - Activité : onglets Récapitulatif et Détails affichant les données surveillées en fonction des règles de politique du serveur de fichiers. Chaque ligne dans l'onglet Récapitulatif indique le nombre d'instances des activités d'accès enregistrées par serveur et utilisateur du système d'exploitation. L'onglet Détails indique le nom d'hôte du serveur, le serveur, le nom d'hôte du client, l'adresse IP du client, l'utilisateur du système d'exploitation, le nom complet du fichier, la commande, la date et l'heure. Chaque ligne dans l'onglet Détails comporte des détails complets sur une activité. Les données affichées dans l'onglet Activité sont cohérentes avec la date et l'heure du collecteur.
    - Valeurs extrêmes : voir Interprétation des valeurs extrêmes pour l'activité de fichier.
    - Erreurs : onglets Récapitulatif et Détails. Chaque ligne dans l'onglet Récapitulatif indique le nombre d'instances des erreurs signalées par serveur et adresse IP client, ainsi que la date. Le récapitulatif détaillé indique le détail des erreurs ainsi que l'heure. Chaque ligne dans l'onglet Détails comporte des détails complets sur une erreur.
    - Violations : onglets Récapitulatif et Détails. Chaque ligne dans l'onglet Récapitulatif indique le nombre d'instances des violations enregistrées par combinaison de serveur, programme source et utilisateur du système d'exploitation. Le récapitulatif détaillé indique l'adresse IP du client, la gravité, la violation et ses détails, la date et l'heure. Chaque ligne dans l'onglet Détails comporte des détails complets sur une violation. Les données affichées dans l'onglet Violations sont cohérentes avec la date et l'heure du serveur de fichiers.
    - Autorisation : onglets Récapitulatif et Détails. Pour les serveurs de fichiers, cet onglet présente les données sensibles en fonction des plans de décision de surveillance de l'activité des fichiers (FAM) en cours. Chaque ligne dans l'onglet Récapitulatif indique le nombre d'instances des activités d'accès enregistrées par serveur et propriétaire. L'onglet Détails indique le nom d'hôte du serveur, le chemin d'accès complet, le type, , la taille, les entités de classification (le plan de décision selon lequel ce fichier est identifié comme sensible), le propriétaire, le nom d'hôte du client, l'adresse IP du client, l'utilisateur du système d'exploitation, le nom complet du fichier, les utilisateurs et les groupes disposant des droits en écriture, lecture, exécution et suppression, la dernière modification, la version (Sharepoint seulement), l'heure de création, la date et l'heure. Chaque ligne dans l'onglet Détails comporte des détails complets sur une activité. Vous pouvez utiliser les données de cette table pour créer des règles de politique et des groupes pour des serveurs de fichiers ; voir Création d'une règle de politique FAM à partir de l'onglet Autorisations du tableau de bord d'investigation.

Les vues supplémentaires que vous pouvez ajouter ou ouvrir sont les suivantes :

- Une vue de topologie Vue des statuts de serveur de recherche : voir Utilisation de la vue de topologie
- Un graphique à bulles animé : visualisation animée des modifications de données effectuées au cours des dernières 48 heures. Le graphique décrit le comportement des objets sur une période de 24 heures. Chaque objet est représenté par un cercle, et sa surface ainsi que sa position (axe des X et axe des Y) représentent trois variables sélectionnées par l'utilisateur. L'animation présente le comportement de l'objet sur 24 heures. Le graphique est accessible depuis la liste déroulante Ajouter un graphique.
- Un graphique d'activité : graphique à courbes affichant le volume des activités et les valeurs extrêmes, qui se trouve au-dessus de la table de résultats. Le graphique est accessible depuis la liste déroulante Ajouter un graphique.

Contrôles et options figurant dans cette page :

- Une liste de facettes catégorisées pouvant contenir les facettes Où, Qui, Quoi, Exception et Quand depuis les résultats de recherche apparaît dans la partie gauche de chaque tableau de bord et ne peut pas être retirée. Filtrez l'intégralité du tableau de bord à l'aide de facettes spécifiques en développant la liste et en cliquant sur des facettes individuelles.
- La ligne Filtres actifs dans la partie supérieure de la fenêtre affiche les filtres appliqués. Supprimez des filtres en cliquant sur .
- Une zone de recherche : recherche de texte libre qui filtre les résultats dans toutes les zones simultanément, quelle que soit la facette.
- La recherche distribuée : voir Recherche locale et recherche distribuée.
- La plage de temps pour laquelle les données sont présentées : modifiez-la en cliquant sur la liste déroulante dans le coin supérieur droit. Les options sont les suivantes : dernière heure, 3 dernières heures, dernier jour, 3 derniers jours, toute plage de temps que vous spécifiez. L'option par défaut est une heure.
- Une liste déroulante des filtres : voir Filtrage des données et sauvegarde des filtres dans le tableau de bord d'investigation.
- Ajout d'un nouveau tableau de bord Sauvegarde des modifications dans le tableau de bord Sauvegarde du tableau de bord en tant que : voir Création, sauvegarde et exportation des tableaux de bord d'investigation.

Rubrique parent : Tableau de bord d'investigation
Concepts associés:
Interprétation des valeurs extrêmes pour l'activité de fichier
Tâches associées:
Utilisation de la vue de topologie

Filtrage des données et sauvegarde des filtres dans le tableau de bord d'investigation

Pourquoi et quand exécuter cette tâche

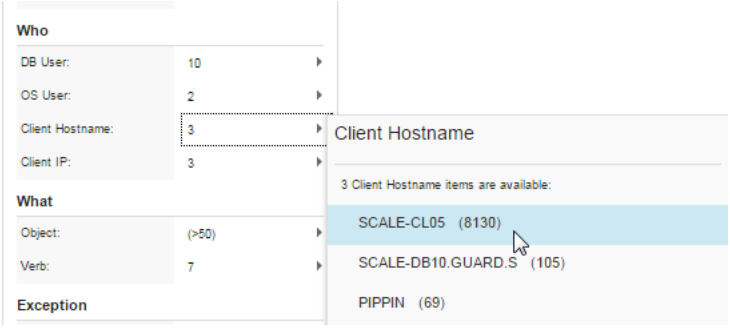
Vous pouvez filtrer les données dans l'intégralité du tableau de bord d'investigation ainsi que dans un graphique individuel. Vous pouvez explorer en aval la table des résultats dans les informations connexes.

Vous pouvez sauvegarder des filtres pour les utiliser ultérieurement. Lorsque vous sauvegardez un ensemble de filtres, vous choisissez de le partager ou non, et vous sélectionnez les rôles avec lesquels vous allez le partager.

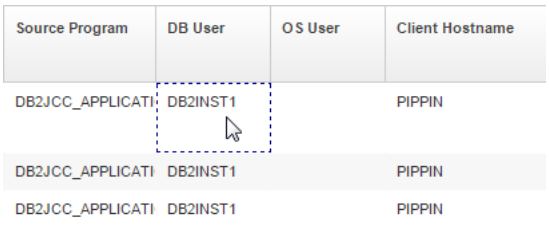
Procédure

1. Utilisez les règles et la syntaxe suivantes pour filtrer les données :
   - Pour rechercher une phrase exacte, placez les termes de recherche entre guillemets. Par exemple, “Liste des alertes de profilage. renvoie les entrées pour Liste des alertes de profilage de connexion, mais pas pour Alerte de liste de profil.
   - Pour rechercher tous les termes de recherche spécifiés, séparez les termes par un espace. Par exemple, Hadoop getlisting renvoie les entrées contenant le terme Hadoop et le terme getlisting dans tout emplacement ou toute séquence.
   - Pour rechercher l'un des termes de recherche spécifiés, séparez les termes par OR ou une barre verticale (|). Par exemple, Hadoop OR getlisting renvoie toutes les entrées contenant Hadoop ou getlisting dans tout emplacement.
   - Pour exclure un terme de recherche spécifié, utilisez NOT ou un point (.). Par exemple, NOT Hadoop ne renvoie aucune entrée contenant Hadoop dans tout emplacement.
   - Les caractères génériques sont pris en charge : utilisez des astérisques (*) au début ou à la fin d'une chaîne. Par exemple, 10.10.70.* renvoie toutes les entrées contenant la chaîne 10.10.70. suivie d'autres caractères.
   - Vous pouvez combiner plusieurs règles de recherche. Par exemple, 2016–5-08 (19.*|20.*) renvoie les résultats pour le 8 mai entre 19:00:00 et 20:59:59.

   L'ajout de filtres change chaque vue en fonction du *filtre de référence* spécifié pour la vue. Les filtres appliqués apparaissent dans la barre de menu. Vous pouvez les effacer un par un en cliquant sur X.
2. Affinez les résultats de recherche en appliquant l'une des méthodes suivantes :
   - Sélectionnez des filtres spécifiques reposant sur la liste de facettes :

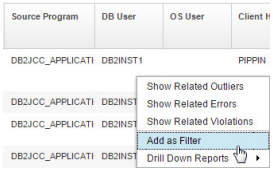


   - Cliquez sur les en-têtes de l'axe des X ou de l'axe des Y d'un graphique.
   - Cliquez sur un résultat de recherche individuel dans la table des résultats :



Remarque : Vous pouvez sélectionner une ou plusieurs lignes et cliquer avec le bouton droit de la souris sur l'une des cellules serveur/utilisateur de base de données/adresse IP client pour les ajouter à un groupe existant ou créer un nouveau groupe.

3. Examinez plus en détail et individuellement chaque résultat en cliquant avec le bouton droit sur des résultats de recherche spécifiques et en explorant les valeurs extrêmes, les erreurs ou les violations associées, ou en affichant l'un des rapports détaillés disponibles.



4. Pour sauvegarder un ensemble de filtres, cliquez sur Filtres > Sauvegarder. Entrez un nom pour le filtre et marquez-le comme Privé ou cliquez sur Partager avec pour le partager avec des rôles spécifiques. Pour sauvegarder l'ensemble de filtres comme ensemble de filtres par défaut (le tableau de bord s'ouvre systématiquement avec ces filtres), sélectionnez Définir comme filtre par défaut. Lorsque vous avez terminé, cliquez sur OK pour sauvegarder le filtre.

Rubrique parent : Tableau de bord d'investigation

Filtrage d'un graphique individuel

Pourquoi et quand exécuter cette tâche

Vous pouvez filtrer un graphique individuel. L'icône devient rouge lorsque des filtres spécifiques différents des filtres de tableau de bord généraux sont définis pour un graphique. Survolez l'icône pour voir les filtres utilisés dans ce graphique.

Un ensemble de filtres peut être inactif dans un graphique, ce qui signifie que les données du graphique ne sont pas filtrées en fonction du champ en question. Ainsi, Guardium peut afficher d'autres éléments, en plus de ceux liés au cas, qui peuvent être similaires ou fournir des informations supplémentaires pour l'examen.
Exemple : Lorsque vous examinez l'activité sur un serveur, il peut être judicieux de comparer l'un des graphiques à des données provenant d'autres serveurs. Pour cela, désactivez le filtre Serveur uniquement pour ce graphique. Cliquez sur l'icône et sélectionnez le bouton d'action Inactif pour la ligne Serveur.

Procédure

1. Cliquez sur l'icône . La fenêtre des paramètres de filtre de graphique s'ouvre.
2. Sélectionnez ou désélectionnez les boutons d'option en fonction de vos besoins, puis cliquez sur Appliquer.

Rubrique parent : Tableau de bord d'investigation

Création, sauvegarde et exportation des tableaux de bord d'investigation

Pourquoi et quand exécuter cette tâche

Vous pouvez filtrer les données dans le tableau de bord de nombreuses façons. Les ensembles de filtres peuvent être privés ou partagés. Par exemple, un utilisateur qui connaît l'environnement peut configurer des filtres pertinents. Il peut créer un filtre pour un enquêteur spécifique, puis le partager avec ce rôle. Vous ne pouvez pas changer et sauvegarder les tableaux de bord prédéfinis du système sous leurs noms originaux.
Important : Tous les tableaux de bord d'investigation sont publics. Lorsqu'un tableau de bord est sauvegardé, tous les utilisateurs ayant accès à des tableaux de bord ont également accès au tableau de bord sauvegardé via le menu des tableaux de bord. De plus, si vous sauvegardez un tableau de bord comme tableau de bord par défaut, tous les utilisateurs pourront le voir.
Vous pouvez utiliser les mêmes tableaux de bord avec des ensembles de filtres différents, selon les données que vous voulez afficher.
Exemple : Votre tableau de bord inclut un graphique d'activité qui représente les activités des utilisateurs de base de données, avec une répartition par adresse IP client. Vous souhaitez afficher les mêmes données filtrées en fonction de différentes bases de données, par exemple la base de données Ressources humaines et la base de données Finances. Vous pouvez également décider d'ajouter différents types de commande pour chaque base de données.

- Filtre 1 : en fonction de la base de données Ressources humaines, avec le verbe SELECT
- Filtre 2 : en fonction de la base de données FINANCES, avec le verbe UPDATE

Vous pouvez ouvrir le même tableau de bord et passer d'un ensemble de filtres associé à ce graphique à d'autres en utilisant les icônes et situées au-dessus de la liste Filtres actifs.

Tous les tableaux de bord d'investigation, y compris les diagnostics relatifs aux menaces, peuvent être chiffrés et exportés en vue de leur partage. Seules les définitions de tableau de bord sont exportées, et non les filtres.

Si un tableau de bord est configuré avec un ensemble de graphiques idéal pour l'analyse de types d'incident particuliers, vous pouvez le partager avec d'autres utilisateurs Guardium sans inclure de données réelles sur les attaques ni révéler les filtres.

Procédure

1. Pour sauvegarder l'affichage en cours, cliquez sur l'icône .

2. Pour sauvegarder un tableau de bord sous un autre nom en vue de sa modification et de son utilisation ultérieure, cliquez sur l'icône et sauvegardez-le avec un nom descriptif et éventuellement une catégorie. Vous pouvez également définir une catégorie lorsque vous sauvegardez le tableau de bord. Le nom et la catégorie peuvent comporter des espaces. Par la suite, pour extraire le tableau de bord, cliquez sur l'icône pour ouvrir le menu des tableaux de bord.
3. Pour exporter des tableaux de bord d'investigation, accédez à Manage > Gestion des données > Exportation de définitions. Dans le menu Type, sélectionnez Tableau de bord d'investigation, puis sélectionnez les définitions de tableau de bord à exporter. Ensuite, cliquez sur Exporter.

Rubrique parent : Tableau de bord d'investigation

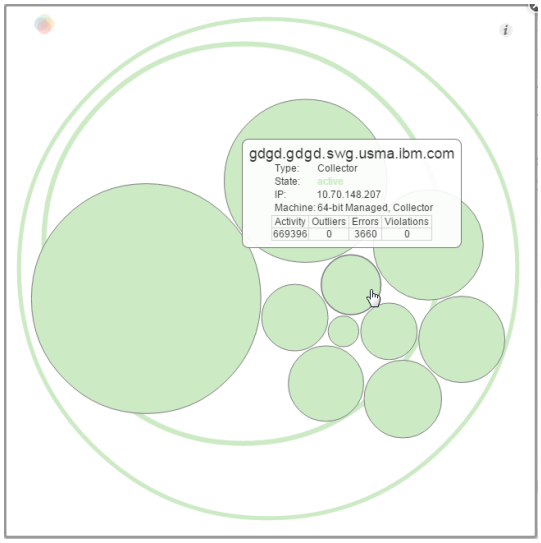
Utilisation de la vue de topologie

La vue de topologie est une visualisation des dispositifs Guardium dans les résultats de recherche.

Pourquoi et quand exécuter cette tâche

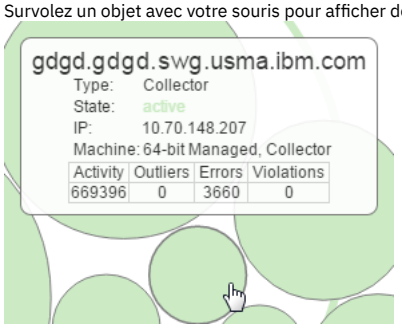
Vous pouvez afficher les détails de chaque serveur, sélectionner des critères de filtrage et restreindre les résultats de recherche à des segments spécifiques de l'environnement Guardium. Les cercles pleins représentent les collecteurs et les agrégateurs. Les cercles vides représentent les instances de Central Manager. La couleur du cercle indique le statut du serveur. La couleur du contour de l'instance de Central Manager indique son statut. La taille du cercle indique le volume relatif de données collectées.

La vue de topologie n'est pas prise en charge sur les machines autonomes.



Procédure

1. Pour ouvrir la vue de topologie, cliquez sur l'icône Vue des statuts de serveur de recherche Vue des statuts de serveur de recherche dans la barre d'outils du tableau de bord d'investigation.
2. Survolez un objet avec votre souris pour afficher des informations détaillées sur cet objet.



3. Sélectionnez un objet pour restreindre les résultats de recherche uniquement à cet objet et à ses enfants, le cas échéant. Utilisez Ctrl + clic pour sélectionner ou désélectionner plusieurs objets dans la vue de topologie.
4. Fermez la vue de topologie en cliquant sur l'icône de fermeture ou hors du navigateur de topologie. Les résultats de recherche sont mis à jour automatiquement afin de refléter les données disponibles en fonction de la portée sélectionnée dans la vue de topologie.

Rubrique parent : Tableau de bord d'investigation

Recherche locale et recherche distribuée

Pourquoi et quand exécuter cette tâche

Les tableaux de bord d'investigation peuvent s'exécuter en mode local ou distribué. En mode local, les recherches se limitent aux données disponibles sur la machine locale (la machine depuis laquelle la recherche est effectuée). Par exemple, une recherche locale qui est effectuée depuis un collecteur individuel renvoie des résultats à partir de sources de données se trouvant sur ce collecteur, mais pas à partir de sources de données se trouvant sur d'autres collecteurs dans l'environnement. En mode distribué, les recherches renvoient des données depuis l'environnement Guardium entier et les résultats ne sont pas limités à la machine sur laquelle est effectuée la

recherche. Un outil de topologie est mis à disposition pour que vous puissiez aisément restreindre les résultats de recherche à des segments spécifiques de l'environnement Guardium.

Par défaut, les tableaux de bord d'investigation fonctionnent en mode de recherche locale.

Procédure

1. Pour passer de la recherche locale à la recherche distribuée et inversement, cliquez sur l'icône Activer/Désactiver la recherche sur tous les dispositifs dans la barre d'outils de la fenêtre de recherche. Les résultats de recherche sont mis à jour automatiquement afin de refléter les données disponibles en fonction du mode de recherche sélectionné, locale ou distribuée.
2. Voir Utilisation de la vue de topologie pour des informations sur le filtrage des résultats de recherche globaux en fonction d'un segment spécifique de l'environnement Guardium.

Rubrique parent : Tableau de bord d'investigation

Utilisation de l'analyse approfondie des données

La visualisation de l'analyse approfondie des données permet à l'utilisateur d'examiner en détail une séquence d'événements capturés par le système Guardium. Elle fournit une image complète de l'activité dans une fenêtre de temps spécifique et permet de détecter tout comportement inhabituel.

Pourquoi et quand exécuter cette tâche

L'analyse approfondie des données introduit un paradigme révolutionnaire qui utilise les capacités visuelles de l'utilisateur pour offrir une vue générale des transactions de données et identifier les comportements inattendus. Guardium propose également des fonctions d'apprentissage automatique et d'analyse de données robustes contribuant aux audits et permettant de détecter les attaques. Des algorithmes, l'analyse de données et des graphiques ont été conçus en fonction de l'expérience et des connaissances acquises au fil du temps. L'analyse approfondie des données utilise la souplesse de la perception visuelle de l'utilisateur pour identifier dans les données brutes les associations et les flux qui ne correspondent pas à des modèles d'attaques connues et qui, sinon, passeraient inaperçus. L'outil présente divers aspects des données dans un scénario visuel complexe et fournit à l'observateur des outils permettant d'explorer directement de grandes quantités de données complexes.

L'analyse approfondie des données convertit les données auditées en une visualisation chronologique 3D du flux de données, des sources vers les destinations, en affichant les transactions de données dépliées, exactement comme elles ont eu lieu.

L'espace de visualisation contient deux niveaux, chacun représentant des entités du domaine d'audit d'un type spécifique. Chaque entrée dans les données d'audit est représentée sous forme de 'ligne clignotante' depuis un objet du niveau supérieur (par exemple une adresse IP client) vers un objet du niveau inférieur (par exemple une base de données). La ligne clignotante entre la source et la destination laisse une trace (un trait pointillé) indiquant la présence d'une interaction entre la source et la destination spécifiques, qui s'estompe progressivement en arrière-plan. Les traces représentent l'interaction entre les sources et les destinations dans la plage de temps sélectionnée. La taille de chaque source et de chaque destination est relative à leur niveau d'activité. Les sources se trouvent près de leurs destinations et d'autres sources similaires. Vous pouvez modifier l'affichage de diverses façons, pour ajouter des informations aux données ou afficher d'autres aspects des données. Vous pouvez consulter l'analyse approfondie des données à l'aide d'un casque de réalité virtuelle.

L'analyse approfondie des données répond à ce paradigme en constante évolution. Il ajoute la souplesse de la perception visuelle de l'utilisateur afin d'identifier des associations et des flux dans les données brutes, quels que soient les types d'attaque connus, qui autrement passeraient inaperçus.

L'analyse approfondie des données convertit les données auditées en une visualisation chronologique 3D des sources de données et des destinations, en affichant les transactions de données dépliées, exactement comme elles ont eu lieu. L'espace de visualisation contient deux niveaux, chacun représentant des entités du domaine d'audit d'un type. Chaque entrée dans les données d'audit est représentée sous forme de 'ligne clignotante' depuis un objet du niveau supérieur (par exemple une adresse IP client) vers un objet du niveau inférieur (par exemple une base de données). La ligne clignotante entre la source et la destination laisse une trace (un trait pointillé) indiquant la présence d'une interaction entre la source et la destination spécifiques, qui s'estompe progressivement en arrière-plan. La ligne clignotante est de la même couleur que la base de données de destination. Les traces représentent l'interaction entre les sources et les destinations dans la plage de temps sélectionnée. Les sources se trouvent près de leurs destinations et d'autres sources similaires. La taille de l'entité de destination est proportionnelle au volume des transactions relatives aux autres entités de destination. Vous pouvez modifier l'affichage de nombreuses façons : vous pouvez notamment appliquer un code couleurs à l'entité supérieure (la couleur change lorsque les détails de la source de données changent), effectuer un filtrage depuis le graphique d'analyse approfondie des données, et changer les facettes du tableau de bord d'investigation. Vous pouvez également consulter l'analyse approfondie des données à l'aide d'un casque de réalité virtuelle.

Procédure

1. Dans la fenêtre Tableau de bord d'investigation, cliquez sur Ajouter un graphique > Graphique d'analyse approfondie des données. La fenêtre Paramètres du graphique s'ouvre.
2. Dans la sous-fenêtre Paramètres du graphique, modifiez les types d'objet qui sont représentés dans les deux niveaux, et le type de flux de données. Si vous le souhaitez, vous pouvez trier les entités par couleur dans le niveau supérieur à l'aide d'un deuxième critère afin d'obtenir un autre niveau d'analyse. Par exemple, si les objets du niveau supérieur représentent des adresses IP client et que vous sélectionnez le tri par couleur pour le programme source, vous pouvez visualiser l'utilisation des différents programmes source par une adresse IP client spécifique, et l'utilisation d'un programme source commun par différentes adresses IP client. Un objet dont la couleur change à maintes reprises indique que l'utilisation du programme source change fréquemment pour une adresse IP client unique. Cliquez sur Appliquer.

Tableau 1. Paramètres du graphique d'analyse approfondie des données

Champ	Description et valeurs
Domaine de flux de données	Type de flux de données affiché : activités, erreurs, violations ou valeurs extrêmes.
Entités du plan supérieur	Entité représentée dans le niveau supérieur : adresse IP client, utilisateur de base de données, utilisateur du système d'exploitation ou programme source.
Entités du plan inférieur	Entité représentée dans le niveau inférieur : base de données, objet ou serveur.
Trier les couleurs des entités de niveau supérieur par	Classification par couleur supplémentaire (facultatif) des entités supérieures : aucune, par adresse IP client, par utilisateur de base de données, par utilisateur du système d'exploitation, par programme source.
Afficher les libellés du plan supérieur	Oui ou non
Afficher les libellés du plan inférieur	Oui ou non
Nbre max. d'entités dans le plan supérieur	Nombre maximal d'entités affichées dans le niveau supérieur.

Champ	Description et valeurs
Nbre max. d'entités dans le plan inférieur	Nombre maximal d'entités affichées dans le niveau inférieur.
Couleur des entités de niveau supérieur	Ouvre la palette de couleurs permettant de sélectionner une couleur pour les entités du niveau supérieur. Option désactivée si les entités supérieures sont triées par couleur.
Couleur de l'arrière-plan	Ouvre une palette de couleurs permettant de sélectionner la couleur de l'arrière-plan.
Couleur des plans	Ouvre une palette de couleurs permettant de sélectionner une couleur pour les niveaux (une couleur pour les deux niveaux).

3. Modifiez l'affichage comme suit :
   - Cliquez sur l'icône représentant une loupe afin de passer en mode plein écran pour plus de détails.
   - Faites pivoter la vue en maintenant le bouton gauche de la souris enfoncé et en faisant glisser le curseur.
   - Faites un panoramique en maintenant le bouton droit de la souris enfoncé et en faisant glisser le curseur.
   - Effectuez un zoom avant ou arrière avec la molette de la souris.
4. Affichez les entités comme suit :
   - Survolez une entité pour afficher ses détails dans la légende.
   - Cliquez sur une entité pour afficher uniquement ses flux de données (les autres entités s'estompent). Cliquez sur l'arrière-plan pour quitter.
   - Cliquez deux fois sur une entité pour l'utiliser comme filtre actif (dans le tableau de bord entier).
5. La sous-fenêtre d'informations, qui se trouve dans le coin supérieur droit, affiche l'horodatage des actions affichées, le nombre d'actions affichées jusque là, et le taux d'événements par seconde. Vous pouvez modifier l'affichage comme suit :

	Mettez en pause/redémarrez le flux de données
	Redémarrez le flux de données au début de la plage de temps
	Augmentez la vitesse du flux de données
	Réduisez la vitesse du flux de données
	Vue de dessus (vue d'ensemble)
	Vue de côté (par défaut)

6. Utilisez les boutons suivants, situés au-dessus du panneau de configuration, en fonction de vos besoins :

	Active le mode plein écran pour le graphique d'analyse approfondie des données
	Ouvre les paramètres du graphique
	Ferme le graphique d'analyse approfondie des données
	Ouvre une aide en incrustation

Rubrique parent : Tableau de bord d'investigation

Détection des valeurs extrêmes

Activez et démarrez la détection des valeurs extrêmes en deux étapes simples, en laissant Guardium faire le travail d'identification de tout comportement anormal d'un serveur ou d'un utilisateur, permettant ainsi de détecter au plus vite les attaques possibles.

Une valeur extrême est un comportement particulier d'une source spécifique (dans la surveillance de l'activité des données (DAM)), une base de données ou un utilisateur particulier dans une base de données, et dans Guardium version 10.1.2, dans la surveillance de l'activité des fichiers (FAM), un serveur ou un utilisateur du système d'exploitation), au cours d'une plage de temps ou dans une portée spécifique hors de la période de temps ou de la portée “normale” de la base de données ou de l'activité de l'utilisateur spécifique. Les valeurs extrêmes peuvent indiquer qu'une violation de sécurité a lieu, même si les activités elles-mêmes n'enfreignent pas directement une politique de sécurité existante.

Les activités d'un utilisateur identifiées comme atypiques et donc suspectes incluent les cas de figure suivants :

- L'utilisateur accède à une table pour la première fois
- L'utilisateur sélectionne dans une table des données qu'il n'a jamais sélectionnées auparavant
- Un volume exceptionnel d'erreurs. Par exemple, une application génère davantage d'erreurs SQL que dans le passé. Cela peut indiquer qu'une attaque par injection de SQL est en cours.
- Une activité qui, elle-même, n'est pas inhabituelle, mais dont le volume est inhabituel
- Une activité qui, elle-même, n'est pas inhabituelle, mais dont les circonstances ou le moment auquel elle se produit sont inhabituels. Par exemple, un administrateur de base de données accède à une table particulière plus fréquemment qu'à l'accoutumée. Cela pourrait indiquer que l'administrateur récupère des données par petites quantités au fil du temps.

Les activités d'un base de données identifiées comme atypiques et donc suspectes incluent les cas de figure suivants :

- Un volume exceptionnel d'erreurs
- Une activité qui, elle-même, n'est pas inhabituelle, mais dont le volume est inhabituel
- Une activité qui, elle-même, n'est pas inhabituelle, mais dont les circonstances ou le moment auquel elle se produit sont inhabituels

Les résultats de l'analyse des valeurs extrêmes sont disponibles depuis le tableau de bord d'investigation (Recherche rapide) ainsi que dans les rapports.

L'analyse des valeurs extrêmes fonctionne sur les données qui ont déjà été auditées par une politique de sécurité. Assurez-vous que les données dans lesquelles vous voulez rechercher d'éventuelles valeurs extrêmes ont déjà été auditées par une politique de sécurité.

La détection des valeurs extrêmes peut être effectuée sur :

- Un agrégateur, avec des données provenant de tous ses collecteurs (sauf les collecteurs exécutant la détection des valeurs extrêmes localement).
- Un collecteur, avec des données ne provenant que de ce collecteur.

- Démarrage rapide de la détection des valeurs extrêmes
  Cette rubrique explique comment activer des valeurs extrêmes et commencer à recevoir des alertes en quelques étapes simples.
- Activation et désactivation de la détection de valeurs extrêmes sur un agrégateur
  Activez, désactivez et configurez la détection de valeurs extrêmes sur un agrégateur afin de configurer la détection de valeurs extrêmes sur tous les collecteurs de l'agrégateur.
- Activation et désactivation de la détection de valeurs extrêmes localement sur un collecteur
  Lancez la détection de valeurs extrêmes sur un collecteur unique afin de n'évaluer que les données de ce collecteur.
- Interprétation des valeurs extrêmes dans le tableau de bord d'investigation
  Dans Guardium, vous disposez d'une interface graphique pratique pour identifier et répondre aux valeurs extrêmes détectées par l'algorithme.
- Interprétation des valeurs extrêmes pour l'activité de fichier
  Affichez les valeurs extrêmes de la surveillance de l'activité des fichiers dans le graphique d'activité du tableau de bord d'investigation et la table des résultats (le tableau de bord d'investigation doit être activé), ou révisez le rapport Liste des valeurs extrêmes d'analyse.
- Surveillance du statut de l'analyse des valeurs extrêmes
  Utilisez la page de statut de l'analyse des valeurs extrêmes pour surveiller le processus d'analyse des valeurs extrêmes sur une unité spécifique sur laquelle s'exécute le processus ainsi que sur un gestionnaire central ou un agrégateur.
- Regroupement d'utilisateurs et d'objets pour la détection de valeurs extrêmes
  Apprenez à ajouter des groupes, par exemple d'utilisateurs et d'objets, à l'algorithme de détection de valeurs extrêmes par défaut.
- Exclusion d'événements de la détection de valeurs extrêmes
  Il est possible d'exclure des événements de la détection de valeurs extrêmes. Par exemple, vous pouvez exclure une activité des données de test.

Rubrique parent : Surveillance et audit

Démarrage rapide de la détection des valeurs extrêmes

Cette rubrique explique comment activer des valeurs extrêmes et commencer à recevoir des alertes en quelques étapes simples.

Avant de commencer

- La détection des anomalies est activée (Configuration > Outils et vues > Détection des anomalies).

Pourquoi et quand exécuter cette tâche

La détection des valeurs extrêmes peut être lancée sur un nombre quelconque d'agrégateurs. Il est cependant conseillé de commencer avec un seul agrégateur, d'affiner la configuration et de l'étendre à d'autres agrégateurs une fois qu'elle est au point. Avant de commencer, décidez des ressources disponibles sur lesquelles investiguer les valeurs extrêmes. Limitez ensuite le nombre de valeurs extrêmes rapportées quotidiennement à une quantité qui puisse être investiguée. L'algorithme guardium fournit les événements les plus importants, et non seulement ceux du "top 10".

Etant donné que la détection des valeurs extrêmes est un processus distinct des règles de politique de sécurité et de leur application, vous ne pouvez pas configurer d'alertes en temps réel pour les valeurs extrêmes. Cependant, comme les données de valeur extrême sont incluses dans les rapports, vous pouvez créer une alerte de corrélation. Une alerte de corrélation est déclenchée par une requête qui effectue une recherche en arrière sur une période spécifiée afin de déterminer si le seuil d'alerte a été atteint.

Procédure

1. Activez des valeurs extrêmes. Voir Activation et désactivation de la détection de valeurs extrêmes sur un agrégateur ou Activation et désactivation de la détection de valeurs extrêmes localement sur un collecteur.
2.
3. Fixez le nombre maximum de valeurs extrêmes rapportées par jour. Voir .
4. Au besoin, affinez la définition des valeurs extrêmes. Consultez Regroupement d'utilisateurs et d'objets pour la détection de valeurs extrêmes et Exclusion d'événements de la détection de valeurs extrêmes.
5. Créez une requête.
   a. Accédez à Rapports > Outils de configuration de rapport > Générateur de requête.
   b. Définissez Domaine=Analyse, Nom de requête=Liste des valeurs extrêmes d'analyse ou Récapitulatif des valeurs extrêmes d'analyse par date. Les valeurs par défaut de tous les autres paramètres peuvent être conservées.
   c. Cliquez sur Créer un rapport.
6. Créez un processus d'audit.
   a. Sélectionnez Conformité > Outils et vues > Générateur de processus d'audit.
   b. Donnez un nom au processus et ajoutez la tâche (le rapport que vous venez de créer).
   c. Définissez des récepteurs. Déterminez le type de notifications souhaité. Vous pouvez configurer les alertes, effectuer des ajouts à la liste des tâches et affecter des utilisateurs pour la révision et la justification des résultats.
   d. Planifiez l'exécution quotidienne du processus et cliquez sur Sauvegarder.
7. Pour faciliter l'affichage, ajoutez les rapports de valeurs extrêmes à Mon tableau de bord.

Résultats

Après une semaine, la période d'apprentissage étant terminée, des données doivent figurer dans les rapports et des alertes doivent être émises.

Rubrique parent : Détection des valeurs extrêmes

Activation et désactivation de la détection de valeurs extrêmes sur un agrégateur

Activez, désactivez et configurez la détection de valeurs extrêmes sur un agrégateur afin de configurer la détection de valeurs extrêmes sur tous les collecteurs de l'agrégateur.

Avant de commencer

- Il est fortement recommandé d'activer les valeurs extrêmes uniquement sur les agrégateurs 64 bits qui présentent 24 gigaoctets de mémoire au moins.

Cette fonction est prise en charge depuis Guardium version 10.1.2.

Pourquoi et quand exécuter cette tâche

Restriction : La détection de valeurs extrêmes et la sécurité au niveau des données ne peuvent pas être activées simultanément.

Lorsque cette fonction est exécutée sur l'agrégateur, les données de détection de valeurs extrêmes sont extraites depuis les unités gérées et les phases d'apprentissage et d'analyse ont lieu sur l'agrégateur.

La détection de valeurs extrêmes est désactivée par défaut. La procédure ci-après est exécutée sur un gestionnaire central pour activer ou désactiver la détection de valeurs extrêmes sur tous les collecteurs qui envoient leurs données à l'agrégateur spécifié, sauf les collecteurs qui exécutent la détection de valeurs extrêmes localement. (Pour plus de détails sur la collection locale, voir Activation et désactivation de la détection de valeurs extrêmes localement sur un collecteur).

Si un collecteur a été déplacé d'un agrégateur à un autre ou si vous voulez activer la détection de valeurs extrêmes localement sur un collecteur, désactivez la détection de valeurs extrêmes sur l'agrégateur, activez la détection de valeurs extrêmes localement si pertinent, puis activez la détection de valeurs extrêmes sur l'agrégateur. A chaque fois que vous activez la détection de valeurs extrêmes sur l'agrégateur, vous actualisez la liste des collecteurs.

Procédure

1. Connectez-vous au gestionnaire central en tant qu'utilisateur ou administrateur possédant le rôle CLI.
2. Pour activer la fonction de détection de valeurs extrêmes, entrez :

   ```
   grdapi enable_outliers_detection_agg schedule_interval=1 schedule_units=HOUR
   aggregator_host_name=<aggregator host name> DAM_FAM=DAM
   ```

   où :

   - Le paramètre aggregator_host_name est le nom d'hôte de l'agrégateur.
   - FAM_DAM est un paramètre facultatif spécifiant le type des valeurs extrêmes. La valeur par défaut est DAM (surveillance de l'activité des données).

3. Pour désactiver la fonction de détection de valeurs extrêmes, entrez :

   ```
   grdapi disable_outliers_detection_agg aggregator_host_name=<aggregator host name>
   ```

   où :

   - Le paramètre aggregator_host_name est le nom de domaine qualifié complet de l'agrégateur.

Résultats

Le système lance la collecte des données de valeur extrême. Une fois l'apprentissage terminé (14 jours), les valeurs extrêmes sont disponibles dans le tableau de bord d'investigation (Interprétation des valeurs extrêmes dans le tableau de bord d'investigation et Interprétation des valeurs extrêmes pour l'activité de fichier) et le rapport Liste des valeurs extrêmes d'analyse.

Rubrique parent : Détection des valeurs extrêmes
Concepts associés:
Tableau de bord d'investigation
Information associée:
GuardAPI Outliers Detection Functions

Activation et désactivation de la détection de valeurs extrêmes localement sur un collecteur

Lancez la détection de valeurs extrêmes sur un collecteur unique afin de n'évaluer que les données de ce collecteur.

Avant de commencer

- Il est fortement recommandé d'activer les valeurs extrêmes uniquement sur les collecteurs 64 bits qui présentent 24 gigaoctets de mémoire au moins.

Pourquoi et quand exécuter cette tâche

Restriction : La détection de valeurs extrêmes et la sécurité au niveau des données ne peuvent pas être activées simultanément.

La détection de valeurs extrêmes est désactivée par défaut. Procédez comme suit pour activer ou désactiver la détection de valeurs extrêmes localement sur un collecteur. Lorsque la détection de valeurs extrêmes est activée localement sur un collecteur, les données de ce dernier ne sont pas combinées avec les données de son agrégateur.

Pour identifier un collecteur exécutant le processus d'analyse des valeurs extrêmes localement, accédez à la fenêtre de statut du processus d'analyse des valeurs extrêmes et reportez-vous à la ligne du collecteur individuel (pas sous l'agrégateur). La colonne Analyse des valeurs extrêmes activée apparaît en vert.

Pour remplacer une détection de valeurs extrêmes effectuée localement par une détection de valeurs extrêmes effectuée sur l'agrégateur, désactivez la détection de valeurs extrêmes localement, désactivez la collecte des valeurs extrêmes sur l'agrégateur, puis actualisez la liste des collecteurs en réactivant la détection de valeurs extrêmes sur l'agrégateur.

Procédure

1. Connectez-vous au collecteur en tant qu'utilisateur ou administrateur possédant du rôle CLI.
2. Pour activer la fonction de détection de valeurs extrêmes, entrez :

   ```
   grdapi enable_outliers_detection schedule_interval=1 schedule_units=HOUR DAM_FAM=DAM
   ```

   où :

   - FAM_DAM est un paramètre facultatif spécifiant le type des valeurs extrêmes. La valeur par défaut est DAM (surveillance de l'activité des données).

3. Pour désactiver la fonction de détection de valeurs extrêmes, entrez :

```
grdapi disable_outliers_detection
```

Résultats

Le système lance la collecte des données de valeur extrême. Une fois l'apprentissage terminé (7 jours), les valeurs extrêmes sont disponibles dans le tableau de bord d'investigation (voir Interprétation des valeurs extrêmes dans le tableau de bord d'investigation et Interprétation des valeurs extrêmes pour l'activité de fichier) et le rapport Liste des valeurs extrêmes d'analyse.

Rubrique parent : Détection des valeurs extrêmes
Information associée:
GuardAPI Outliers Detection Functions

Interprétation des valeurs extrêmes dans le tableau de bord d'investigation

Dans Guardium, vous disposez d'une interface graphique pratique pour identifier et répondre aux valeurs extrêmes détectées par l'algorithme.

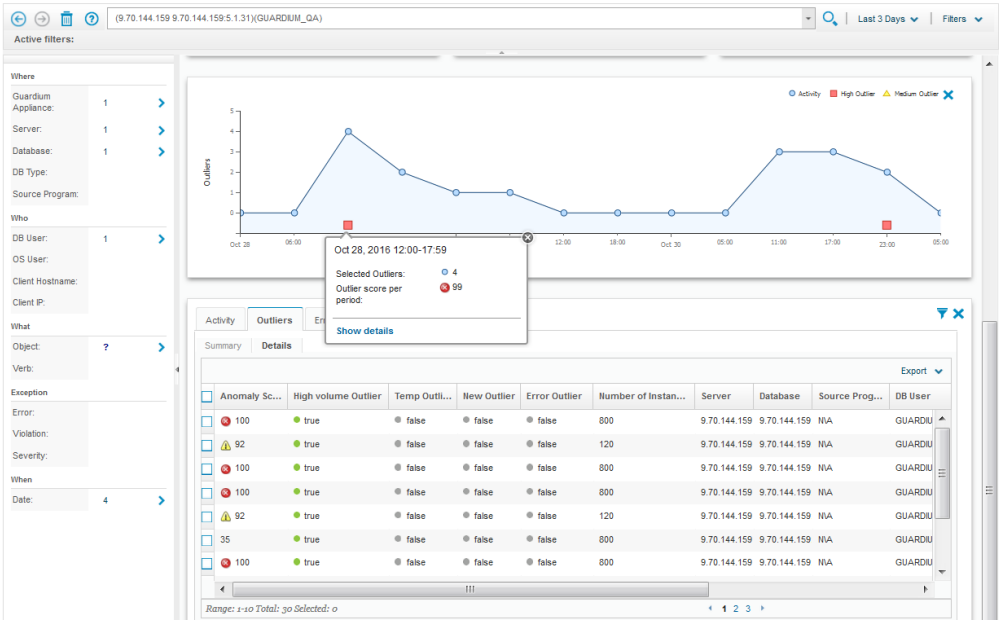
Pour que les données de détection de valeur extrême soient visibles dans le tableau de bord d'investigation, la recherche rapide doit être activée (grdapi enable_quick_search).

Le Graphique d'activité inclut des indicateurs rouges (haut) et jaune (moyen) reflétant la gravité ou le score total des valeurs extrêmes pour l'intervalle de temps sélectionné. Des indicateurs rouges signalent les événements anormaux qui requièrent une attention immédiate. Des indicateurs jaunes signalent les anomalies moins graves méritant votre attention dans le cadre d'autres investigations ou d'investigations liées.

Survolez un icône de valeur extrême pour afficher les détails des valeurs extrêmes détectées au cours de cette plage de temps. Pour filtrer la table de résultats afin d'afficher les activités ou les valeurs extrêmes qui ont eu lieu au cours de la même période, cliquez sur Afficher les détails.

Depuis Guardium version 10.1.2, l'onglet Valeurs extrêmes de la table de résultats comporte deux vues :

- Le récapitulatif comporte une ligne par source et par heure où une valeur extrême a été trouvée, avec un score d'anomalie et un ou plusieurs motifs. Notez que les valeurs extrêmes présentées dans l'onglet Récapitulatif ne sont pas toutes associées à des détails dans l'onglet Détails.
- Les détails présentent un échantillon d'événements qui sont survenus. Chaque événement se trouve sur une ligne distincte et est associé à un motif (sauf pour Diverses valeurs extrêmes, voir le tableau) et à d'autres détails (programme source, objet, verbe, etc.). Par exemple, pour un volume élevé, l'échantillon présente les événements associés au score le plus élevé. Vous pouvez configurer le nombre d'échantillons (lignes) qui apparaît dans l'onglet Détails pour chaque valeur extrême dans l'onglet Récapitulatif.



Le tableau suivant décrit les colonnes qui figurent dans les vues Récapitulatif et Détails :

Tableau 1. Colonnes dans les onglets Valeurs extrêmes de la table de résultats

Nom de colonne	Description	Autre action
Score d'anomalie	Onglet Récapitulatif : valeur d'agrégat calculée en fonction du volume de valeurs extrêmes, de la gravité d'événements individuels, du volume prévu de valeurs extrêmes pour un moment de la journée précis, et d'autres facteurs. Par exemple, sur un système qui identifie généralement 0 valeur extrême à 1h00 et 5 à 10 valeurs extrêmes à 13h00 les jours de semaine, la présence de deux valeurs extrêmes supplémentaires (2 valeurs extrêmes à 1h00 ou 12 valeurs extrêmes à 13h00) est plus significative et pondérée plus lourdement que le total horaire lui-même. Onglet Détails : le score d'anomalie est pertinent uniquement pour un événement de volume élevé.	Cliquez avec le bouton droit de la souris sur le score pour ouvrir un menu d'actions supplémentaires. Dans l'onglet Détails, le score peut être 0, ce qui indique que les événements individuels eux-mêmes ne sont pas suspects, mais que les événements accumulés au cours de cette heure le sont.
Valeur extrême de volume élevé	True ou False. Volume élevé d'activités d'un certain type, par exemple sur un objet, d'un utilisateur de base de données.	

Nom de colonne	Description	Autre action
Nouvelle valeur extrême	True ou False. Volume élevé d'activités sur de nouveaux objets. Par exemple, un administrateur crée curieusement un nombre élevé de nouvelles tables.	
Diverses valeurs extrêmes	Vue Récapitulatif seulement. True ou False. Volume élevé de différents types d'activité. Par exemple, un utilisateur de base de données effectue beaucoup plus d'activités que d'habitude ou effectue des activités à un moment inhabituel. Un échantillon des divers événements apparaît dans l'onglet Détails pour qu'un utilisateur de base de données puisse les identifier. Bien que les diverses valeurs extrêmes ne constituent pas une colonne dans l'onglet Détails, d'autres motifs peuvent leur être affectés. Si tel n'est pas le cas, elles apparaissent sans motif.	Voir la table Activité pour plus de détails.
Valeur extrême d'erreur	True ou False. Volume élevé d'erreurs.	
Valeur extrême en cours	Vue Récapitulatif seulement. True ou False. Evénement survenu au cours des dernières heures, qui n'est pas assez élevé pour créer une valeur extrême, mais qui est tout de même suspect.	Pas d'événement spécifique à afficher. Reportez-vous à la table Activité et procédez au filtrage en fonction de la base de données dans la liste des facettes, puis modifiez l'intervalle de temps par l'heure du comportement suspect.
Nombre d'instances	Vue Détails seulement. Nombre d'occurrences de cet événement particulier dans l'heure.	
Enregistrements affectés	Nombre d'enregistrements affectés par l'événement particulier. Nombre négatif si l'événement n'est pas, par définition, affecté à des enregistrements.	
Serveur	Serveur sur lequel l'événement est survenu.	
Base de données	Base de données dans laquelle l'événement est survenu.	
Programme source	Vue Détails seulement. Programme source dans lequel l'événement est survenu.	
Utilisateur de base de données	Vue Détails seulement. Utilisateur de base de données qui a exécuté l'événement de valeur extrême.	
Objet	Objet sur lequel l'utilisateur a exécuté l'événement.	
Utilisateur privilégié	Vue Récapitulatif seulement. True ou False. Indique si l'utilisateur est privilégié ou non.	
Verbe	Vue Détails seulement. Verbe avec lequel l'utilisateur a exécuté l'événement.	
Date	Date à laquelle l'événement est survenu, au format aaaa-mm-jj.	
Heure	Heure à laquelle l'événement est survenu, au format hh:mm:ss.	

Versions de Guardium antérieures à la 10.1.2 : il n'y a qu'une seule colonne Motif de valeur extrême contenant une ou plusieurs des valeurs suivantes :

rare
: condition très peu vue

volume élevé
: incidence inhabituellement élevée d'une condition

nouveau
: condition vue pour la première fois

erreur
: incidence inhabituellement élevée de conditions d'erreur

Les motifs de valeur extrême peuvent être combinés, si nécessaire. Par exemple, les motifs "rare" et "volume élevé" peuvent tous les deux être affectés à une valeur extrême si une condition très peu vue survient soudainement plusieurs fois.
Remarque :

Si un résultat négatif ("-") apparaît dans le rapport de résultats Enregistrements affectés, pour l'effacer, l'utilisateur doit réactiver la détection des valeurs extrêmes.

Rubrique parent : Détection des valeurs extrêmes
Information associée:
Détection des anomalies

Interprétation des valeurs extrêmes pour l'activité de fichier

Affichez les valeurs extrêmes de la surveillance de l'activité des fichiers dans le graphique d'activité du tableau de bord d'investigation et la table des résultats (le tableau de bord d'investigation doit être activé), ou révisez le rapport Liste des valeurs extrêmes d'analyse.

Les valeurs extrêmes prennent en charge la surveillance de l'activité de fichier depuis Guardium version 10.1.2

Pour que les données de détection de valeur extrême soient visibles dans le tableau de bord d'investigation, la recherche rapide doit être activée (grdapi enable_quick_search).

Identifiez les valeurs extrêmes en étudiant le graphique d'activité du tableau de bord d'investigation et la table des résultats (le tableau de bord d'investigation doit être activé), ou passez en revue le rapport Liste des valeurs extrêmes d'analyse.

Accédez au graphique récapitulatif en sélectionnant Données ou à partir du menu déroulant Interface utilisateur et en cliquant sur Entrée ; ou en entrant recherche rapide dans le champ de recherche et en cliquant sur Entrée.

Le Graphique d'activité inclut des indicateurs rouges (haut) et jaune (moyen) reflétant la gravité ou le score total des valeurs extrêmes pour l'intervalle de temps sélectionné. Des indicateurs rouges signalent les événements anormaux qui requièrent une attention immédiate. Des indicateurs jaunes signalent les anomalies moins graves méritant votre attention dans le cadre d'autres investigations ou d'investigations liées.

Le fait de passer le pointeur de la souris sur l'icône d'une valeur extrême permet d'obtenir les détails des valeurs extrêmes détectées au cours de cette période. Pour filtrer la table de résultats afin d'afficher les activités ou les valeurs extrêmes qui ont eu lieu au cours de la même période, cliquez sur Afficher les détails.

L'onglet Valeurs extrêmes de la table de résultats comporte deux vues :

- Le récapitulatif comporte une ligne par source et par heure où une valeur extrême a été trouvée, avec un score d'anomalie et un ou plusieurs motifs. Notez que les valeurs extrêmes présentées dans l'onglet Récapitulatif ne sont pas toutes associées à des détails dans l'onglet Détails.
- Les détails présentent un échantillon d'événements qui sont survenus. Chaque événement se trouve sur une ligne distincte et est associé à un motif et à d'autres détails. Par exemple, pour un volume élevé, l'échantillon présente les événements associés au score le plus élevé. Vous pouvez configurer le nombre d'échantillons (lignes) qui apparaît dans l'onglet Détails pour chaque valeur extrême dans l'onglet Récapitulatif.

Le tableau suivant décrit les colonnes qui figurent dans les vues Récapitulatif et Détails :

Tableau 1. Colonnes définies à la fois pour Récapitulatif et Détails

Nom de colonne	Description	Autre action
Score d'anomalie	Onglet Récapitulatif : valeur d'agrégat calculée en fonction du volume de valeurs extrêmes, de la gravité d'événements individuels, du volume prévu de valeurs extrêmes pour un moment de la journée précis, et d'autres facteurs. Par exemple, sur un système qui identifie généralement 0 valeur extrême à 1h00 et 5 à 10 valeurs extrêmes à 13h00 les jours de semaine, la présence de deux valeurs extrêmes supplémentaires (2 valeurs extrêmes à 1h00 ou 12 valeurs extrêmes à 13h00) est plus significative et pondérée plus lourdement que le total horaire lui-même. Onglet Détails : le score d'anomalie est pertinent uniquement pour un événement de volume élevé.	Cliquez avec le bouton droit de la souris sur le score pour ouvrir un menu d'actions supplémentaires. Dans l'onglet Détails, le score peut être 0, ce qui indique que les événements individuels eux-mêmes ne sont pas suspects, mais que les événements accumulés au cours de cette heure le sont.
Valeur extrême de volume élevé	True ou False. Volume élevé d'activités d'un certain type, par exemple sur un objet, d'un utilisateur de base de données.	
Nouvelle valeur extrême	True ou False. Volume élevé d'activités sur de nouveaux objets. Par exemple, un administrateur crée curieusement un nombre élevé de nouvelles tables.	
Valeur extrême d'erreur	True ou False. Volume élevé d'erreurs.	
Valeur extrême en cours	Vue Récapitulatif seulement. True ou False. Evénement survenu au cours des dernières heures, qui n'est pas assez élevé pour créer une valeur extrême, mais qui est tout de même suspect.	Pas d'événement spécifique à afficher. Reportez-vous à la table Activité et procédez au filtrage en fonction de la base de données dans la liste des facettes, à l'heure du comportement suspect.
Nombre d'instances	Vue Détails seulement. Nombre d'occurrences de cet événement particulier dans l'heure.	
Serveur	Serveur sur lequel l'événement est survenu.	
Utilisateur de système d'exploitation	Utilisateur de système d'exploitation qui a exécuté l'événement.	
Utilisateur privilégié	True ou False. Indique si l'utilisateur est privilégié ou non.	
Nom de fichier complet	Nom du fichier sur lequel l'utilisateur a exécuté l'événement.	
Commande	Commande avec laquelle l'utilisateur a exécuté l'événement.	
Date	Date à laquelle l'événement est survenu, au format aaaa-mm-jj.	
Heure	Heure à laquelle l'événement est survenu, au format hh:mm:ss.	

Rubrique parent : Détection des valeurs extrêmes
Concepts associés:
Tableau de bord d'investigation
Information associée:
GuardAPI Outliers Detection Functions
Détection des anomalies

Surveillance du statut de l'analyse des valeurs extrêmes

Utilisez la page de statut de l'analyse des valeurs extrêmes pour surveiller le processus d'analyse des valeurs extrêmes sur une unité spécifique sur laquelle s'exécute le processus ainsi que sur un gestionnaire central ou un agrégateur.

La page de statut de l'analyse des valeurs extrêmes qui est affichée dans le gestionnaire central présente les détails de tous les agrégateurs gérés et de leurs collecteurs. Tous les collecteurs dans le gestionnaire central apparaissent sur des lignes individuelles sous leur agrégateur. Lorsqu'elle est affichée depuis un agrégateur, cette fenêtre présente les détails des collecteurs de l'agrégateur spécifique. Lorsqu'elle est affichée depuis un collecteur, seul le collecteur est présenté.

La page est accessible depuis le menu Guardium Gestion > Maintenance > Statut d'analyse des valeurs extrêmes.

Les tableaux ci-dessous décrivent la page et les actions utilisateur recommandées.

Tableau 1. Colonnes de la page de statut de l'analyse des valeurs extrêmes

Colonne	Description	Actions
Unité	Nom de l'unité	Non disponible

Colonne	Description	Actions
	Ouvre la liste des unités qui envoient des données à cet agrégateur.	Cliquez pour afficher la liste des unités.
Unité en/hors fonction	Indique si l'unité est en fonction ou non.	Non disponible
Analyse des valeurs extrêmes activée	• Agrégateur : indique si l'analyse des valeurs extrêmes sur l'agrégateur est activée. Si elle est désactivée, le reste de la ligne après cette colonne est vide. • Ligne individuelle représentant un collecteur ou une unité autonome : la couleur verte indique que l'analyse des valeurs extrêmes est activée localement.	Non disponible
Send data for outlier mining (Envoyer des données pour l'analyse des valeurs extrêmes)	Collecteurs uniquement. Le collecteur envoie des données d'analyse des valeurs extrêmes à l'agrégateur. Les données pour l'analyse des valeurs extrêmes sont envoyées du collecteur à l'agrégateur si l'analyse des valeurs extrêmes est activée pour l'agrégateur et le collecteur n'exécute pas l'analyse des valeurs extrêmes localement.	Non disponible
Dernière anomalie trouvée	Date et heure locales sur le gestionnaire central de la dernière analyse des valeurs extrêmes exécutée qui a révélé une ou plusieurs anomalies (valeurs extrêmes). Affiche les données uniquement pour les unités exécutant la version 10.1.2 et les versions ultérieures.	Non disponible
Dernière analyse	Date et heure locales sur le gestionnaire central de la dernière analyse des valeurs extrêmes exécutée (date/heure de fin du processus). Affiche les données uniquement pour les unités exécutant la version 10.1.2 et les versions ultérieures.	Non disponible
Statut d'analyse des valeurs extrêmes	Statut de la dernière analyse des valeurs extrêmes exécutée. Vert : le processus a abouti. Jaune : le processus s'est terminé avec des avertissements. Rouge : le processus s'est terminé avec des erreurs. Affiche les données uniquement pour les unités exécutant la version 10.1.2 et les versions ultérieures.	Si une erreur/un avertissement ne s'est produit qu'une fois, réexécutez le processus (l'heure suivante) et vérifiez le résultat. Si une erreur se répète, prenez contact avec le support.
Détails	Le statut peut être rouge (erreur), jaune (avertissement) ou vert.	Pour les processus qui se sont terminés avec des avertissements (jaune), cliquez afin d'ouvrir un menu contextuel pour l'avertissement. Pour les processus qui se sont terminés avec des erreurs (rouge), cliquez afin d'ouvrir un menu contextuel pour l'erreur.
Apprentissage depuis	Date et heure auxquelles le processus d'analyse des valeurs extrêmes a été activé. Le processus apprend le comportement de la ressource depuis ce moment.	Non disponible
Recherche rapide activée/désactivée	Indique si la recherche rapide et Solr sont activés sur l'unité gérée. Lorsque la recherche rapide est désactivée, les données de cette machine ne sont pas incluses dans le tableau de bord d'investigation.	Voir Activation et désactivation du tableau de bord d'investigation.
Dernière info mise à jour	Date et heure de la dernière mise à jour des informations de cette ligne. En général, les données sont mises à jour toutes les cinq minutes environ.	Non disponible

Tableau 2. Boutons de la page de statut de l'analyse des valeurs extrêmes

Bouton	Description	Actions
Actualiser 	Actualise l'affichage.	Cliquez pour actualiser l'affichage.
Signe plus	Ce bouton apparaît uniquement lorsque l'unité détaillée sur la ligne est un agrégateur..	Cliquez pour ouvrir la liste des unités qui envoient des données à cet agrégateur.

Rubrique parent : Détection des valeurs extrêmes

Regroupement d'utilisateurs et d'objets pour la détection de valeurs extrêmes

Apprenez à ajouter des groupes, par exemple d'utilisateurs et d'objets, à l'algorithme de détection de valeurs extrêmes par défaut.

Pourquoi et quand exécuter cette tâche

Par défaut, il existe deux groupes d'utilisateurs et d'objets pondérés ou évalués plus lourdement par l'algorithme d'apprentissage automatique de Guardium : les administrateurs et les objets sensibles. Cependant, il se peut que vous ayez déjà créé des groupes supplémentaires également utiles pour la détection de valeurs extrêmes. Par exemple, vous pouvez avoir créé un groupe Utilisateurs suspects ou plusieurs groupes d'objets sensibles correspondant à différentes applications.

Procédure

1. Pour cette tâche, vous devez connaître l'ID de groupe interne à utiliser avec la commande grdapi. Pour obtenir l'ID de groupe, vous pouvez utiliser la commande suivante : `grdapi list_group_by_desc desc=[nom du groupe]`. Par exemple, si un groupe s'appelle BadGuys, vous pouvez entrer la commande suivante pour obtenir son ID de groupe interne :

   ```
   grdapi list_group_by_desc desc="BadGuys"
   ```

2. Une fois que vous connaissez l'ID, ajoutez-le en tant que groupe d'utilisateurs privilégiés pour un score amélioré comme suit (notez que vous devez aussi inclure le groupe par défaut 1 si vous voulez également améliorer les scores pour ce groupe). Pour ajouter un groupe dont l'ID est 1234, entrez : grdapi set_outliers_detection_parameter parameter_name="privUsersGroupIds" parameter_value=1,1234
3. Pour ajouter des données sensibles dont les ID sont 333 et 156, entrez : set_outliers_detection_parameter parameter_name="sensitiveObjectGroupIds" parameter_value=5,333,156

Résultats

Les groupes ou les objets sensibles spécifiés sont ajoutés à la détection de valeurs extrêmes et se voient attribuer un poids supplémentaire par l'algorithme.

Rubrique parent : Détection des valeurs extrêmes

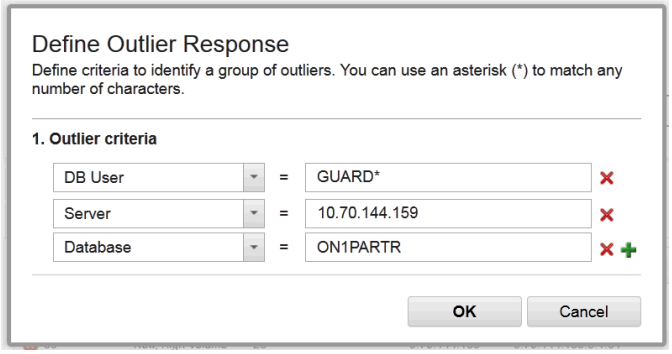
Exclusion d'événements de la détection de valeurs extrêmes

Il est possible d'exclure des événements de la détection de valeurs extrêmes. Par exemple, vous pouvez exclure une activité des données de test.

Exclusion d'événements correspondant à des critères spécifiques, avec la réponse à une valeur extrême

1. Faites un clic droit sur un indicateur de valeur extrême et sélectionnez Ignorer pour exclure les réponses à ce type de valeur extrême.
2. Entrez des valeurs spécifiques ou utilisez des entrées génériques (avec le caractère *) pour définir les éléments à ignorer.
3. Retirez tout champ inutile en cliquant sur les icônes ✕ appropriées.
4. Cliquez sur OK pour valider les modifications.
5. Pour inclure des événements précédemment ignorés, affichez le rapport Commentaires analytiques des utilisateurs, cliquez deux fois sur l'événement précédemment ignoré, puis sélectionnez Appeler > delete_analytic_user_feedback.

Par exemple, pour que toutes les activités du serveur 10.70.144.159, de la base de données ON1PARTR, et de tout utilisateur de base de données dont le nom commence par GUARD, soient ignorées, votre boîte de dialogue doit comporter les critères suivants :

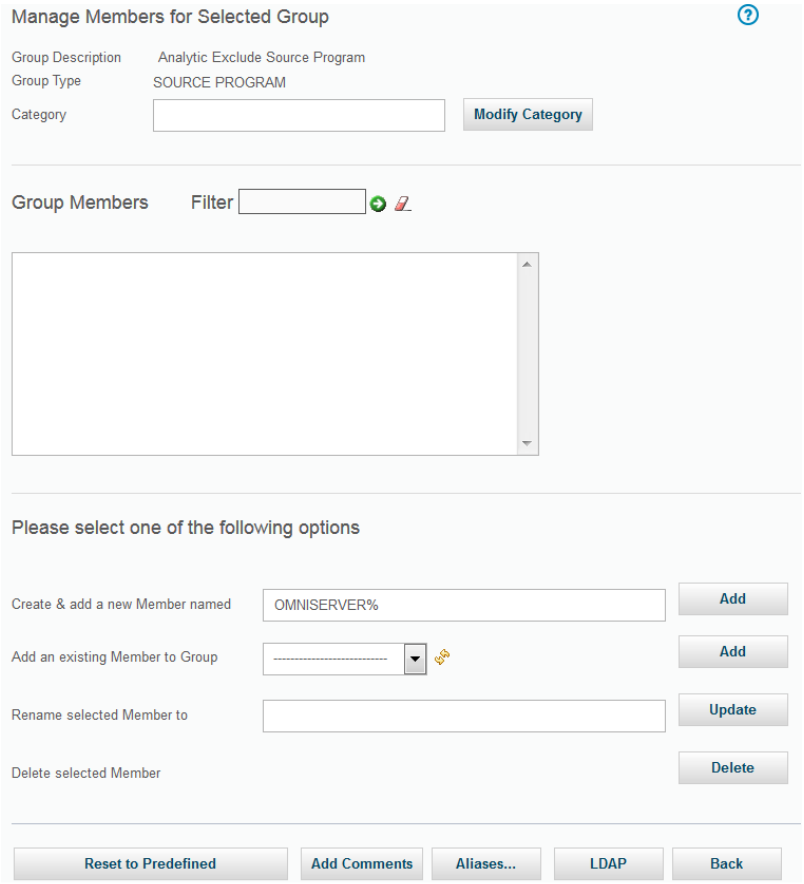


Exclusion d'événements à l'aide du générateur de groupe

Si de nombreux éléments doivent être exclus, utilisez le générateur de groupe Guardium et remplissez l'un des groupes suivants ou tous les groupes suivants, selon vos besoins :

- Analytic Exclude DB User
- Analytic Exclude OS User
- Analytic Exclude Server IP
- Analytic Exclude Service Name
- Analytic Exclude Source Program

Le générateur de groupe permet le téléchargement en bloc et autorise notamment le remplissage depuis une requête sur une table personnalisée.



Vous pouvez aussi utiliser des commandes GuardAPI pour remplir les groupes Analytic Exclude. Par exemple, pour ajouter OMNISERVER au groupe Analytic Exclude Source Program, utilisez la commande suivante :

```
grdapi create create_member_to_group_by_desc  desc="Analytic Exclude Source Program" member="OMNISERVER%"
```

Rubrique parent : Détection des valeurs extrêmes

Tableau de bord de protection des données

Le tableau de bord de protection des données Guardium fournit une vue récapitulative des données relatives au risque et à la conformité destinées aux responsables de la sécurité seniors.

Le tableau de bord de protection des données contient plusieurs graphiques et diagrammes, en plus des statistiques de conformité et de risque affichées en permanence sur un grand moniteur. Pour ouvrir le tableau de bord, accédez à Examen > Tableau de bord de protection des données Guardium.

ATTENTION :
La session n'expire pas et vous ne serez pas déconnecté automatiquement alors que vous consultez le tableau de bord de protection des données. Faites attention lorsque vous laissez le tableau de bord ouvert pour de longues périodes.
Informations :

- Le tableau de bord est actualisé automatiquement toutes les 20 minutes.
- Les paramètres de recherche par défaut sont définis pour la recherche distribuée avec des données collectées au cours du jour précédent.

Graphiques et diagrammes

Plusieurs graphiques à courbes vous permettent de comparer rapidement différents types de données. Par exemple, un graphique peut afficher le volume d'activités, d'erreurs et de violations au fil du temps.

Un graphique nommé Activités anormales affiche un récapitulatif des valeurs extrêmes liées à une activité générale. Dans ce graphique, un point récapitulatif pour les valeurs extrêmes représente un volume inattendu de valeurs extrêmes.

Informations : L'axe des Y dans ces graphiques est un axe logarithmique qui peut fausser les proportions du graphique, et les valeurs ou comptages ne sont pas consignés.

Statistiques de risque et de conformité

La statistique Risque affiche le nombre de tests ayant échoué avec une gravité critique ainsi que le nombre de sources de données dans lesquelles ces échecs sont survenus. Chaque source de données peut présenter plusieurs tests ayant échoué.

Sources de données surveillées affiche le nombre de sources de données pour lesquelles le système consigne des activités. Cette statistique est calculée à l'aide des données de domaine d'accès disponibles.

Tâches de la liste des tâches de conformité affiche le récapitulatif suivant pour les processus d'audit : le nombre de processus fermés aujourd'hui, le nombre de processus ouverts depuis moins de trois jours, et le nombre de processus ouverts depuis plus de trois jours.

Informations :

- Les statistiques ne sont pas affectées par les filtres de recherche de texte et de facette, mais elles le sont pas le mode de recherche. Pour changer le mode de recherche, utilisez l'icône afin de développer la sous-fenêtre supérieure, puis cliquez sur l'icône pour passer de la recherche distribuée à la recherche locale et inversement.
- Les composants des statistiques sont recalculés toutes les heures.

Rubrique parent : Surveillance et audit

Rapports

Un rapport définit de quelle manière sont présentées les données recueillies par une requête.

Le rapport par défaut est un tableau (rapport tabulaire) reflétant la structure de la requête, chaque attribut étant affiché dans une colonne à part. Tous les composants de présentation d'un rapport tabulaire (les titres des colonnes, par exemple) peuvent être personnalisés. Tous les rapports graphiques sont définis à l'aide du Générateur de rapport. En plus des paramètres de date de début et de fin (début et fin de la requête), les valeurs peuvent maintenant être affichées entre le début de la page et le début du tableau dans tous les rapports.

Avant d'utiliser le Générateur de rapport, créez une requête à l'aide du Générateur de requête. Voir Utilisation du Générateur de requête.

Le moyen le plus rapide de créer et d'afficher un rapport consiste à utiliser les étapes pour créer un rapport, puis à sélectionner le rapport dans Mon tableau de bord.

Déplacez-vous d'avant en arrière entre les écrans de menu à l'aide des boutons Retour et Suivant. La flèche arrière dans le navigateur Web ne fonctionne pas pour la navigation entre les écrans Guardium.

Icônes utilisées dans les rapports

Utilisez les icônes pour sélectionner les fonctions dans le Générateur de rapport.

Tableau 1. Icônes de rapport

Icônes graphiques	Fonction
	Processus ad hoc pour exécution unique
	Actualiser
	Ouvrir dans une nouvelle fenêtre
	Ajouter un rapport
	Ajouter aux favoris
	Modifier ou éditer la requête pour ce rapport ou personnaliser le graphique
	Supprimer
	Générateur de magasin de données
	Cloner
	Configurer les paramètres d'exécution
	Configurer les colonnes de rapport
<-- --> <--	Personnaliser le rapport

Rechercher un rapport pour édition

Pour accéder à une définition de rapport, sélectionnez l'icône du cycle de vie des rapports  , puis cliquez sur Générateur de rapport.

Recherchez un rapport en choisissant Domaine, Requête ou Titre de rapport. Les résultats s'affichent dans le panneau Résultats de la recherche de rapport.

- Pour localiser un rapport spécifique, sélectionnez ce rapport dans la liste Titre de rapport. Le rapport sélectionné s'affiche immédiatement dans le panneau Résultats de la recherche de rapport.

  Pour les autres types de recherche, cliquez sur le bouton Rechercher après avoir effectué des entrées dans un ou plusieurs champs, ou cliquez simplement sur le bouton Rechercher pour répertorier tous les rapports disponibles pour votre compte Guardium.

- Pour répertorier tous les rapports qui utilisent une requête spécifique, sélectionnez cette requête dans la liste de requêtes.
- Pour répertorier tous les rapports pour un type de graphique spécifique, sélectionnez-le dans la liste Type de graphique.

Pour localiser un rapport spécifique, sélectionnez ce rapport dans la liste Titre de rapport. Le rapport sélectionné s'affiche immédiatement dans le panneau Résultats de la recherche de rapport.

Si la recherche localise des rapports, ils s'affichent dans le panneau Résultats de la recherche de rapport. Cliquez sur l'un des boutons suivants :

- Nouveau - Voir Créer un rapport.
- Cloner - Voir Cloner un rapport.
- Modifier - Voir Modifier un rapport.
- Rôles - Voir Rôles de sécurité. Affectez des rôles aux rapports dans Générateur de rapport. Si vous affectez des rôles à des rapports alors que vous vous trouvez dans le Générateur de requête (Suivi), vous attribuez uniquement le rôle à la requête et non au rapport.
- Supprimer- Voir Retirer un rapport
- Commentaire - Voir Commentaires.
- Affectation d'API- Voir Affectation d'API
- Contrôle d'exploration en aval - Voir Modifier le menu Rapports d'exploration pour un rapport.

Créer un rapport

1. Pour accéder à une définition de rapport, sélectionnez l'icône du cycle de vie des rapports  , puis cliquez sur Générateur de rapport.
2. Cliquez sur Nouveau pour ouvrir le panneau Créer un rapport.
3. Dans la liste de requêtes, sélectionnez une valeur de requête à utiliser dans le rapport (par exemple, Connexions à Guardium)
4. Entrez un nom unique pour le rapport dans le champ Titre de rapport.

Personnaliser la présentation de rapport

Suivez les procédures des étapes pour personnaliser la présentation du rapport.

1. Dans le panneau Description des colonnes du rapport,
   - Eventuellement, remplacez le titre du rapport. La valeur par défaut provient de la définition du rapport. Vous pouvez modifier le titre sur la plupart des panneaux ultérieurs.
   - Optionnellement, vous pouvez remplacer les descriptions de colonne (en-têtes des colonnes).
2. Cliquez sur Suivant pour ouvrir le panneau Attributs de rapport.
   - Sélectionnez le bouton Tabulaire ou Graphique.
   - Cliquez sur Suivant pour ouvrir le panneau Envoyer le rapport.
3. Cliquez sur Sauvegarder pour soumettre le rapport pour création.

Créer un rapport graphique

Suivez les procédures des étapes pour créer un rapport graphique.

1. Effectuez les étapes précédentes dans Personnaliser la présentation du rapport pour les descriptions des colonnes du rapport, les descriptions des paramètres du rapport et les attributs du rapport.
2. Dans le panneau Type de graphique de rapport, sélectionnez le type Graphique et cliquez sur Suivant. Les options sont les suivantes : En aires, A barres, Zone de barre, Ligne de barre, Colonne, Zone de date, Colonne de date, Ligne de date, Ligne des libellés répartis, Barre individuelle, Colonne individuelle, Ligne, Pictogramme, Graphique circulaire, Polaire, Speedo et Barres empilées. Les options Graphique circulaire, Polaire, Speedo et Barres empilées sont recommandées. Choisissez-en un et cliquez sur Suivant.
3. Si le panneau Type de graphique de rapport n'est pas affiché, ignorez cette étape (toutes les données nécessaires ont été saisies). Sélectionnez le type de graphique pour le rapport dans la liste Type de graphique.
4. Cliquez sur Suivant pour ouvrir le panneau Paramètres de présentation de rapport.
   - Examinez les paramètres, qui varient pour chaque type de graphique.
   - Vous pouvez éventuellement remplacer tous les paramètres par défaut pour le type de graphique sélectionné.
5. Cliquez sur Suivant pour continuer vers le panneau Envoyer le rapport et effectuez la procédure Envoyer la définition du rapport.
6. Pour afficher votre rapport graphique, accédez à Mes tableaux de bord et ajoutez votre rapport graphique.

Remarque :

Une icône d'actualisation apparaît dans tous les rapports graphiques en regard de l'icône d'aide.

Envoyer la définition du rapport

1. Ajoutez éventuellement des commentaires (voir Commentaires).
2. Attribuez éventuellement des rôles (voir Rôles de sécurité).
3. Cliquez sur Sauvegarder.

Modifier un rapport

1. Recherchez le rapport à modifier. Accédez au menu d'outil de recherche du Générateur de rapport.
2. Cliquez sur Modifier pour ouvrir le panneau Colonnes de rapport.
3. Accédez à Personnaliser la présentation du rapport.

Cloner un rapport

1. Recherchez le rapport à cloner. Accédez au menu d'outil de recherche du Générateur de rapport.
2. Cliquez sur Cloner pour ouvrir le panneau Colonnes de rapport.
3. Entrez un nouveau nom pour le rapport cloné, dans la zone Titre du rapport. Vous pouvez entrer le nouveau nom dans l'un des écrans suivants : la seule exigence est que le nouveau nom doit être entré avant que le rapport cloné ne soit enregistré.
4. Accédez à Personnaliser la présentation du rapport.

Retirer un rapport

Notez que vous ne pouvez pas retirer de rapports prédéfinis et que vous ne pouvez pas retirer de rapports utilisés dans les processus d'audit.

1. Recherchez le rapport à retirer.
2. Cliquez sur Supprimer pour retirer le rapport.

Limitation de la taille du rapport

Les rapports tabulaires sont limités à 5 000 lignes de sortie, mais lorsqu'ils sont inclus dans un processus de flux de travail, n'importe quel nombre de lignes peut être exporté de la tâche de rapport vers un fichier CSV ou CEF. Voir Construction de processus d'audit.

Limites

La limite des boutons lors de l'affichage d'un rapport (générer PDF, générer CSV et imprimer) est de 30 000 lignes. Ceci n'est pas personnalisable.

La limite pour Remplir à partir d'une requête dans le Générateur de groupe et le Générateur d'alias lors d'une exécution via Exécuter une fois maintenant est 5 000 lignes. Ceci n'est pas personnalisable.

La limite pour Remplir à partir d'une requête dans le Générateur de groupe et le Générateur d'alias lors d'une exécution via Planification est 20 000 lignes. Cette limite est personnalisable, via la commande CLI, show/store populate_from_query_maxrecs.

Modifier le menu Rapports d'exploration pour un rapport

Par défaut, le menu déroulant d'un rapport comprend tous les rapports dont les paramètres d'exécution peuvent être fournis par les attributs du rapport, lequel reçoit les restrictions de rôle de sécurité habituelles. Pour désactiver ou activer des rapports sur le menu déroulant d'un rapport :

1. Localisez le rapport. Accédez au menu d'outil de recherche du Générateur de rapport.
2. Cliquez sur Contrôle d'exploration en aval pour ouvrir le panneau Contrôle d'exploration en aval du rapport.
3. Cochez la case pour désactiver un rapport ou désélectionnez la case pour activer un rapport.
4. Cliquez sur Appliquer. Le système affiche un message indiquant que vos modifications ont été appliquées avec succès.
5. Cliquez sur Terminé lorsque vous avez fini.

Affectation d'API

Par défaut, l'application Guardium contient des données de configuration qui relient plusieurs des fonctions de l'API aux rapports, fournissant aux utilisateurs, via l'interface graphique, des appels préparés aux API à partir des données de rapport. Utilisez l'Affectation d'API pour lier des fonctions d'API supplémentaires à des rapports Guardium prédéfinis ou des rapports personnalisés.

Pour plus d'informations sur l'utilisation de fonctions d'API associées, consultez la documentation sur GuardAPI Input Generation.

1. Localisez le rapport. Accédez au menu d'outil de recherche du Générateur de rapport.
2. Cliquez sur Affectation d'API pour ouvrir le panneau Affectation d'API montrant les fonctions d'API actuelles qui sont mappées au rapport sélectionné.
3. Cliquez sur une fonction d'API pour afficher une fenêtre contextuelle de l'API - Mappage de paramètre de rapport en cours, qui affiche les paramètres de l'API, si les paramètres de l'API sont requis, toutes les valeurs par défaut et si des champs de rapport sont actuellement mappés à ces paramètres.

   Si aucun champ du rapport n'est lié aux paramètres de l'API, il pourrait être inutile de lier une fonction d'API à un rapport. Le mappage des paramètres de l'API sur les champs de rapport peut être effectué à la fois à travers l'interface graphique et la CLI Guardium. Pour plus d'informations sur le mappage des paramètres de l'API sur les champs du rapport, consultez les sections Mappage des paramètres GuardAPI sur les entités de domaine et Attributs de la génération d'entrée GuardAPI.

4. Cliquez sur le signe plus grand que '>' pour ajouter la fonction d'API sélectionnée à la liste actuelle des fonctions qui sont affectées à ce rapport.
5. Cliquez sur Appliquer pour sauvegarder les changements.

Ouvrir la requête pour l'édition à partir du portlet de rapport

1. Ouvrez un portlet de rapport pour tout rapport basé sur la requête à éditer.
2. Cliquez sur Modifier la requête de ce rapport dans la barre d'outils. Vous devez être autorisé à modifier la requête sur laquelle le rapport est basé.

- Paramètres des rapports
  Vous pouvez utiliser des paramètres pour contrôler le contenu et la présentation d'un rapport.
- Création de tableaux de bord
  Vous pouvez créer un ou plusieurs tableaux de bord, y ajouter des rapports et configurer leur apparence.
- Affichage d'un rapport
  Il existe plusieurs façons d'afficher un rapport, y compris votre tableau de bord et votre recherche d'interface utilisateur.
- Création d'un rapport
  Si les rapports prédéfinis ne répondent pas à vos besoins, vous pouvez créer le vôtre.
- Création de rapports pour z/OS
  Cette rubrique explique comment créer des rapports Guardium pour des sources de données z/OS en personnalisant des rapports intégrés et des exemples de requête.
- Magasin de données
  Un magasin de données est un sous-ensemble d'un entrepôt de données. Un entrepôt de données agrège et organise les données de manière générique en vue de leur utilisation ultérieure pour l'analyse et les rapports. Un magasin de données commence par une analyse des données définies par l'utilisateur et met l'accent sur la satisfaction des exigences spécifiques de l'utilisateur en termes de contenu, présentation et facilité d'utilisation.
- Audit et rapport
  Guardium organise les données qu'il collecte en un ensemble de domaines. Chaque domaine contient un type différent d'informations relatives à un aspect spécifique : accès aux données, exceptions, violations de politique, etc.
- Requêtes
  Utilisez l'une des nombreuses requêtes prédéfinies fournies avec Guardium pour obtenir des informations sur vos données. Utilisez le Générateur de requête pour gérer des requêtes.

- Domaines, entités et attributs
  Un domaine fournit une vue des données que contient Guardium.
- Exploitation des rapports prédéfinis
  Au lieu de créer des rapports personnalisés ex nihilo, bénéficiez des contenus prédéfinis dans l'application Guardium.
- Interrogation des données
  Utilisez le Générateur de requête pour définir et modifier des questions sur les données collectées.
- Génération de rapports sur les tables et les colonnes dormantes
  Guardium propose des fonctionnalités qui peuvent aider les architectes de données et les administrateurs de base de données (DBA) à détecter quelles tables et quels champs ne sont pas utilisés.
- Génération d'appels d'API à partir de rapports
  Générez des appels de l'API Guard à partir d'un rapport, soit à partir d'une seule ligne dans un rapport, soit basés sur l'ensemble du rapport
- Utilisation de constantes dans les appels d'API
  Créez un attribut d'entité à utiliser pendant un appel de fonction d'API.
- Utilisation d'appels d'API à partir de rapports personnalisés
  Associez des fonctions d'API à des rapports et mappez des champs de rapport aux paramètres fonctionnels de l'API.
- Flux externe facultatif
  Les flux externes vous permettent d'envoyer des données de rapport Guardium directement sur une base de données externe.
- Mappage d'un flux externe
  Apprenez comment mapper un flux externe pour envoyer des données de rapport Guardium directement vers une base de données externe.
- Générateur de rapport réparti
  Cette fonctionnalité Central Manager permet de collecter automatiquement des données dans la totalité ou un sous-ensemble des unités gérées Guardium qui sont associées à cette instance de Central Manager donnée. Les rapports répartis sont conçus pour fournir une vue générale, pour corréler des données provenant des sources de données et pour résumer les vues des données. Vous pouvez continuer à utiliser des agrégateurs pour la collecte des données au niveau des lignes dans les collecteurs.
- Création d'un rapport réparti
  Guardium offre une fonction qui permet de collecter automatiquement des données de la totalité ou d'un sous-ensemble des unités gérées de Guardium qui sont associées à une instance donnée de Central Manager Guardium.

Paramètres des rapports

Vous pouvez utiliser des paramètres pour contrôler le contenu et la présentation d'un rapport.

Il existe deux types de paramètres de rapport :

- Un *paramètre d'exécution* fournit une valeur à utiliser dans une condition de requête. Il existe un ensemble par défaut de paramètres d'exécution pour toutes les requêtes, et n'importe quel nombre de paramètres d'exécution peut être défini dans la requête utilisée par le rapport.
- Un *paramètre de présentation* décrit une caractéristique physique du rapport, par exemple, si un rapport graphique comprend une légende ou des libellés, ou les couleurs à utiliser pour un élément. Tous les paramètres de présentation sont fournis avec les paramètres initiaux lorsque vous définissez un rapport.

Pour définir des paramètres de rapport :

1. Cliquez sur Configurer les paramètres du rapport pour afficher les options du rapport. Voir l'icône  .
2. Dans le panneau, entrez les paramètres d'exécution et de présentation dans les cases fournies, selon les besoins, pour que la tâche soit exécutée.
3. Cliquez sur Sauvegarder.
4. Pour afficher le rapport, accédez à Mes tableaux de bord.

Paramètres d'exécution standard

Les paramètres d'exécution suivants sont présents pour tous les rapports.

Paramètre d'exécution	Valeur par défaut et description
QUERY_FROM_DATE	Aucun pour un nouveau rapport, varie pour les rapports par défaut. La date de début du rapport est toujours requise.
QUERY_TO_DATE	Aucun pour un nouveau rapport, varie pour les rapports par défaut, bien que la valeur par défaut soit presque toujours MAINTENANT. Cette date est la date de fin du rapport et est toujours requise.
REMOTE_SOURCE	Néant. Dans un environnement Central Manager, vous pouvez exécuter un rapport sur une unité gérée en sélectionnant ce système Guardium dans la liste des Sources de données distantes.
SHOW_ALIASES	Néant (c'est-à-dire que la valeur par défaut du système est utilisée). Sélectionnez le bouton Activé pour toujours afficher les alias, ou Désactivé pour ne jamais afficher d'alias. Sélectionnez le bouton par défaut pour revenir à la valeur par défaut du système (contrôlée par l'administrateur) après que le bouton Activé ou Désactivé a été utilisé.

Commande de rapport GuardAPI pour renvoyer une liste de noms de paramètres d'exécution

Utilisez la commande GuardAPI, list_parameter_names_by_report_name. Cette fonction accepte un nom de rapport en tant que paramètre d'entrée et renvoie une liste de noms de paramètres d'exécution pour ce rapport.

Rubrique parent : Rapports

Création de tableaux de bord

Vous pouvez créer un ou plusieurs tableaux de bord, y ajouter des rapports et configurer leur apparence.

Avant de commencer

Pensez à la façon dont vous souhaitez organiser les rapports que vous consultez régulièrement. Voulez-vous les visualiser dans un tableau de bord, ou dans plusieurs tableaux de bord ?Voulez-vous les regrouper et les classer en fonction de leur objectif, de leur importance ou d'une autre approche ? Vous pouvez toujours réorganiser vos tableaux de bord ou en créer de nouveaux.

Pourquoi et quand exécuter cette tâche

Procédure

1. Cliquez sur Mes tableaux de bord > Création d'un tableau de bord pour ouvrir un nouveau tableau de bord.
2. Entrez un nom descriptif dans le champ Nom. Ce nom est utilisé dans la liste des tableaux de bord dans le menu.
3. Cliquez sur Ajouter un rapport pour afficher une liste des rapports disponibles. Si vous avez désigné certains rapports comme favoris, vous pouvez cocher la case Mes Favoris pour voir uniquement la liste de ces rapports. Si vous souhaitez visualiser uniquement les rapports graphiques, cochez la case Graphique uniquement.
4. La boîte de dialogue Ajouter un rapport affiche une liste de tous les rapports répondant à vos critères. Vous pouvez parcourir la liste des rapports ou saisir une chaîne dans le champ Filtre. La liste des rapports est mise à jour au fur et à mesure que vous tapez.
5. Cliquez sur le titre d'un rapport pour l'ajouter à votre tableau de bord. Continuez à ajouter autant de rapports que vous le souhaitez. Lorsque vous avez terminé d'ajouter des rapports, cliquez sur Fermer.

Résultats

Un tableau de bord vous permet d'accéder facilement à certains rapports sélectionnés.

Que faire ensuite

Examinez l'apparence de votre tableau de bord. Est-il facile à utiliser et trouvez-vous les informations dont vous avez besoin ? Sinon, vous pouvez le configurer davantage.
Rubrique parent : Rapports

Configuration de votre tableau de bord

Vous pouvez configurer plusieurs aspects de l'apparence de votre tableau de bord pour le rendre aussi utile que possible.

Pourquoi et quand exécuter cette tâche

Pensez à la façon dont vous utilisez vos rapports. Quelle disposition vous permet de réaliser facilement vos objectifs ?Expérimentez ces changements.

Procédure

1. Réorganisez les rapports. Pour déplacer un rapport, placez votre curseur sur la barre de titre du rapport et faites-le glisser vers un nouvel emplacement.
2. Choisissez un nouveau nombre de colonnes en cliquant sur 1, 2 ou 3 dans la zone Nombre de colonnes. Par défaut, vos rapports sont affichés sur deux colonnes. Si vous avez besoin de plus d'espace pour chaque rapport, cliquez sur 1 pour afficher son apparence lorsqu'il a la largeur totale du tableau de bord. Si vous préférez voir plusieurs rapports à la fois, essayez trois colonnes.
3. Redimensionnez les rapports. Faites glisser l'icône de redimensionnement pour que le un rapport soit plus long, plus court, plus étroit ou plus large. Si vous ajustez la largeur d'un rapport, tous les rapports de cette colonne utilisent la nouvelle largeur. Si vous modifiez le nombre de colonnes, toutes les colonnes reviennent à leur largeur par défaut.

Utilisation de votre tableau de bord

Utilisez les étapes pour ajouter un rapport au tableau de bord, puis pour personnaliser son apparence.

Pourquoi et quand exécuter cette tâche

Le tableau de bord remplace Ajouter à sous-fenêtre et Ajouter à Mes rapports personnalisés.

Procédure

1. Cliquez sur l'icône du tableau de bord à partir de la navigation.
2. Puis cliquez sur Création d'un tableau de bord.
3. Cliquez sur Ajouter un rapport pour sélectionner un rapport à partir de tous les rapports auxquels vous avez accès, y compris les nouveaux rapports que vous avez créés.
4. Utilisez le filtrage pour trouver rapidement le rapport qui vous intéresse.
5. Cliquez sur le nom du rapport pour l'ajouter à votre tableau de bord. Ajoutez autant de rapports à votre tableau de bord que vous le souhaitez, en sélectionnant chaque rapport.
6. Personnalisez votre tableau de bord en sélectionnant une présentation. La valeur par défaut est deux colonnes. Une colonne - les rapports sont égaux à la largeur du tableau de bord. Deux colonnes : les rapports sont égaux à la moitié de la largeur du tableau de bord. Trois colonnes : les rapports sont égaux à un tiers de la largeur du tableau de bord.
7. Personnalisez votre tableau de bord en déplaçant les rapports dans l'écran. Utilisez l'icône pour personnaliser le graphique.
8. Désignez des rapports spécifiques en tant que favoris en sélectionnant l'icône . Lors de l'ajout de rapports à un tableau de bord, filtrez en fonction des favoris ou filtrez en fonction des graphiques.
9. Nommez votre tableau de bord en cliquant sur l'icône d'édition.
10. Supprimez un tableau de bord, en cliquant sur l'icône de suppression .

Affichage d'un rapport

Il existe plusieurs façons d'afficher un rapport, y compris votre tableau de bord et votre recherche d'interface utilisateur.

Vous pouvez afficher un rapport de plusieurs façons :

- Si vous avez sauvegardé le rapport dans un tableau de bord, ouvrez le tableau de bord pour afficher le rapport.
- Vous pouvez ajouter le rapport à un tableau de bord. Ouvrez le tableau de bord et cliquez sur Ajouter un rapport, puis choisissez le rapport dans la liste.
- Certains rapports sont répertoriés dans les catégories du cycle de vie des Rapports.
- Certains rapports sont répertoriés dans le cycle de vie pour lequel ils sont les plus pertinents.
- Vous pouvez utiliser la fonction de recherche de l'interface utilisateur (UI) pour localiser le rapport. Sur la bannière, choisissez Interface utilisateur dans la liste déroulante en regard de la zone de recherche. Entrez le nom du rapport dans la zone de recherche. Les résultats commencent à apparaître une fois que vous avez saisi quelques caractères. Choisissez le rapport dans la liste des résultats.

Les choix suivants (avec des icônes) permettent d'éditer et de configurer le rapport :

- Editer la requête pour ce rapport 
- Processus ad hoc pour Exécuter une fois maintenant - Permet d'appeler les commandes GuardAPI. 
- Ouvrir dans une nouvelle fenêtre 
- Configurer les colonnes de rapport 
- Configurer les paramètres d'exécution - Un paramètre d'exécution fournit une valeur à utiliser dans une condition de requête. Il existe un ensemble par défaut de paramètres d'exécution pour toutes les requêtes, et n'importe quel nombre de paramètres d'exécution peut être défini dans la requête utilisée par le rapport. 
- Ajouter aux favoris 
- Actualiser 

Vous pouvez masquer les colonnes de la vue. Cliquez sur l'icône des colonnes et désactivez les cases à cocher pour les colonnes que vous souhaitez masquer.

Vous pouvez trier les données de rapport selon le contenu de n'importe quelle colonne. Cliquez sur le titre de la colonne selon lequel vous souhaitez effectuer le tri. Pour inverser l'ordre, cliquez à nouveau sur le titre. Le tri est toujours effectué sur les valeurs de données réelles, en ignorant tous les alias définis.

Vous pouvez imprimer un rapport pendant que vous le visualisez. Cliquez sur Exporter > Rapport entièrement imprimable pour ouvrir une copie imprimable du rapport dans un nouvel onglet. Cliquez sur l'icône de l'imprimante sur le nouvel onglet pour imprimer le rapport. Vous pouvez également imprimer un rapport en l'exportant vers un fichier PDF et en imprimant le fichier PDF.
Remarque : Pour une instance où le texte PDF est trop petit pour être lu, le rapport PDF comporte une limite physique sur la mesure dans laquelle il peut se développer horizontalement compte tenu de la largeur de la page. Etant donné que chaque ligne du rapport PDF doit correspondre à une seule ligne, la taille de la police de caractères change pour correspondre aux données et peut être très réduite afin d'afficher toutes les données.

Vous pouvez personnaliser les rapports graphiques en cliquant sur l'icône Personnalisation de graphique. Les options comprennent la conversion des données en un graphique à courbes, la modification de l'orientation des axes X et des axes Y, la conversion du rapport en un graphique circulaire ou un graphique à colonnes empilées.

Lors de l'affichage des rapports qui affichent des informations Oracle, parfois, le caractère de point d'interrogation (?) sert à informer l'utilisateur que les informations de connexion ne sont pas disponibles. A nouveau, lors de l'affichage des rapports qui affichent des informations Oracle, l'affichage du nombre -1 signifie qu'un nombre inconnu d'enregistrements sont affectés. Toutes les sessions Oracle sont enregistrées, y compris avec des connexions manquées.

Problème : le champ Utilisateur de système d'exploitation est vide dans les rapports IBM Security Guardium

Remarque pour les plateformes UNIX/Linux

Connexions à distance : l'utilisateur du système d'exploitation n'est pas un champ obligatoire pour se connecter à la base de données. Par conséquent, il appartient au client de la base de données de l'envoyer avec le paquet de connexion. Si les informations sur OS USER ne sont pas envoyées, ce champ est vide. Si la chaîne de connexion du client inclut des informations sur le propriétaire du processus, elle est utilisée pour remplir le champ OS USER.

Connexions locales : la même limitation s'applique aux connexions exécutées localement. Cependant, lorsque les connexions à la base de données sont effectuées localement, Guardium fournit un moyen d'identifier les informations OS USER en activant la chaîne d'ID utilisateur. Notez que la chaîne d'ID utilisateur peut être associée à une surcharge S-TAP supplémentaire et doit être considérée au cas par cas, au besoin.

La chaîne d'ID utilisateur est prise en charge avec les protocoles EXIT (remarque : pour la sortie DB2, niveau de correctif spécifique nécessaire).

La chaîne d'ID utilisateur est prise en charge avec ATAP pour MongoDB, Teradata et Sybase ASE (avec des IP réelles).

Plateforme Windows

Connexions à distance : l'utilisateur du système d'exploitation n'est pas un champ obligatoire pour se connecter à la base de données. Par conséquent, il appartient au client de la base de données de l'envoyer avec le paquet de connexion. Si les informations sur OS USER ne sont pas envoyées, ce champ est vide.

Connexions locales : la plateforme Windows choisit toujours l'utilisateur du système d'exploitation qui exécute le processus connecté au propriétaire du processus de la base de données (aucune chaîne d'ID utilisateur n'est requise dans Windows).

- Actualisation de rapports
  Certains rapports sont configurés pour actualiser leurs données automatiquement. Sur d'autres rapports, vous pouvez actualiser les données manuellement via l'interface utilisateur.
- Exportation d'un rapport
  Vous pouvez exporter un rapport vers un fichier PDF ou un fichier de valeurs séparées par des virgules.
- Affichage de rapports d'exploration en aval
  De nombreux rapports fournissent un accès aux rapports d'exploration qui contiennent des données plus granulaires.

Rubrique parent : Rapports

Actualisation de rapports

Certains rapports sont configurés pour actualiser leurs données automatiquement. Sur d'autres rapports, vous pouvez actualiser les données manuellement via l'interface utilisateur.

Lorsque vous affichez un rapport configuré pour s'actualiser automatiquement, la couleur de l'icône Flèches circulaires d'actualisation pour ce rapport est verte, ce qui indique que le rapport s'actualise automatiquement.

A un moment donné, le rapport cesse de s'actualiser si aucune modification supplémentaire n'est apportée et la couleur de l'icône d'actualisation passe du vert au rouge. Le moment où la couleur change est égal à la moitié du délai d'expiration de la session d'interface graphique (accessible à l'aide de la commande CLI show session timeout).

Par exemple, si le délai d'attente de la session est de 900 secondes par défaut, l'icône Flèches circulaires d'actualisation  sur le rapport Taux des demandes est verte pendant 450 secondes, puis devient rouge.

Il existe plusieurs façons d'actualiser les données du rapport manuellement :

- Cliquez sur Actualiser  dans la barre d'outils.
- Utilisez un bouton de la barre d'outils pour imprimer un rapport, télécharger les données du rapport ou écrire le rapport dans un fichier PDF. Les données du rapport sont actualisées avant l'une de ces actions.
- Définissez un intervalle de temps pour l'actualisation régulière, en définissant la valeur du paramètre refreshRate. Pour effectuer cette tâche :
  - Cliquez sur Personnaliser  dans la barre d'outils du rapport.
  - Dans la boîte de dialogue Configuration, définissez le paramètre refreshRate sur le nombre de secondes après lequel les données du rapport doivent être mises à jour. La valeur par défaut zéro indique que les données du rapport ne sont pas actualisées régulièrement.
  - Cliquez sur OK.

Personnaliser des rapports

Lorsque l'utilisateur édite un rapport ou le modifie via l'écran Personnalisation de rapport, l'utilisateur doit cliquer manuellement sur Actualiser. Il n'existe pas d'actualisation automatique.

Personnalisation de l'interface utilisateur - Dans la boîte de dialogue "Nouveau cycle de vie" et la boîte de dialogue "Nouveau groupe", les groupes sont limités à un maximum de 5 niveaux de profondeur. Par conséquent, même avec des noms de groupe plus longs, tous les niveaux de noms de groupe et de texte d'élément de noeud sont visibles dans la sous-fenêtre de navigation.

Personnalisation de l'interface utilisateur - Lorsque l'utilisateur entre "<" ou ">" dans la zone de texte de la boîte de dialogue "Nouveau cycle de vie" ou "Nouveau groupe", un message contextuel indique que "Le nom ne peut pas contenir les caractères spéciaux < ou >" et le bouton "OK" est désactivé.

Personnalisation de l'interface utilisateur - Dans la boîte de dialogue "Nouveau cycle de vie" et la boîte de dialogue "Nouveau groupe", l'utilisateur peut entrer un maximum de 50 caractères dans la zone de texte.

Rubrique parent : Affichage d'un rapport

Exportation d'un rapport

Vous pouvez exporter un rapport vers un fichier PDF ou un fichier de valeurs séparées par des virgules.

Vous pouvez exporter le contenu d'un rapport vers un fichier PDF (Portable Document Format) et enregistrer le fichier ou le visualiser. Dans la barre d'outils du rapport, cliquez sur Exporter > Télécharger au format PDF pour créer une copie PDF. Suivez l'invite pour enregistrer ou afficher le fichier.

Lorsque vous générez un grand fichier PDF, le processus peut entraîner l'interruption de l'interface utilisateur. Si vous prévoyez de générer de gros fichiers PDF, envisagez de le faire dans le cadre d'un processus d'audit ou augmentez la valeur de délai de l'interface utilisateur afin d'éviter ce problème.

Vous pouvez également exporter le contenu d'un rapport vers un fichier de valeurs séparées par des virgules (csv). Vous pouvez exporter tous les enregistrements (l'intégralité du rapport) dans le rapport, ou seulement les enregistrements d'affichage (les données affichées).

Dans la barre d'outils du rapport, cliquez sur Exporter > Télécharger tous les enregistrements ou Exporter > Télécharger les enregistrements d'affichage. Vous pouvez sauvegarder les résultats ou sélectionner une application dans laquelle les afficher.

Remarque : Si vous éditez un rapport et supprimez une colonne (par exemple, éditer un rapport avec sept colonnes et supprimer une colonne, en conservant six colonnes), lorsque le rapport est exporté en tant que fichier PDF, le rapport affiche les sept colonnes d'origine.

Rubrique parent : Affichage d'un rapport

Affichage de rapports d'exploration en aval

De nombreux rapports fournissent un accès aux rapports d'exploration qui contiennent des données plus granulaires.

Si des actions d'exploration en aval sont disponibles sur un rapport tabulaire, l'utilisateur peut le savoir en cliquant avec le bouton droit de la souris sur une ligne de la grille ; un menu contextuel apparaît alors avec toutes les actions d'exploration en aval disponibles.

Pour une disponibilité en tant que rapport d'exploration en aval :

- Tous les paramètres d'exécution du rapport d'exploration doivent être disponibles à partir du rapport affiché.
- Si des rôles de sécurité ont été affectés, vous devez avoir accès au rapport d'exploration.

Modifier le menu Rapports d'exploration pour un rapport

Par défaut, le menu déroulant d'un rapport comprend tous les rapports dont les paramètres d'exécution peuvent être fournis par les attributs du rapport, lequel reçoit les restrictions de rôle de sécurité habituelles. Pour désactiver ou activer des rapports sur le menu déroulant d'un rapport :

1. Localisez le rapport. Accédez au menu d'outil de recherche du Générateur de rapport.
2. Cliquez sur Contrôle d'exploration en aval pour ouvrir le panneau Contrôle d'exploration en aval du rapport.
3. Cochez la case pour désactiver un rapport ou désélectionnez la case pour activer un rapport.
4. Cliquez sur Appliquer. Le système affiche un message indiquant que vos modifications ont été appliquées avec succès.

5. Cliquez sur Terminé lorsque vous avez fini.

Rubrique parent : Affichage d'un rapport

Création d'un rapport

Si les rapports prédéfinis ne répondent pas à vos besoins, vous pouvez créer le vôtre.

Avant de commencer

Vous choisissez une requête sur laquelle ce rapport est basé, et le domaine de la requête. Si vous devez créer une requête, faites-le avant de créer un rapport basée sur celle-ci. Rappelez-vous qu'il existe une distinction entre les requêtes et les rapports. Une requête décrit un ensemble d'informations à obtenir à partir des données collectées. Un rapport décrit comment les données renvoyées par la requête sont présentées. Reportez-vous à Utilisation du Générateur de requête pour plus d'informations sur la création d'une requête. Reportez-vous à Domaines, entités et attributs pour plus d'informations sur l'utilisation des domaines.

Pourquoi et quand exécuter cette tâche

Vous pouvez trouver plus facile de cloner un rapport et de le modifier plutôt que de créer un rapport ex nihilo.

Procédure

1. Cliquez sur Rapports > Outils de configuration de rapport > Générateur de rapport pour ouvrir l'outil de recherche Générateur de rapport ou le menu de filtre. Si vous sélectionnez Rechercher à ce stade sans choisir de domaine ou de requête, un menu apparaît avec toutes les requêtes répertoriées. Sélectionnez une requête et utilisez les icônes (Ajouter un nouveau rapport  , Modifier  , Cloner  ou Supprimer  pour utiliser les requêtes.
2. Dans le menu de l'outil de recherche du Générateur de rapport, cliquez sur Nouveau  .
3. Le menu Créer un rapport apparaît. Sélectionnez une requête et attribuez un nom au rapport. Cliquez ensuite sur Suivant.
4. L'écran suivant renvoie les colonnes de table de la requête sélectionnée. Personnalisez-les ou utilisez-les comme telles. Cliquez ensuite sur Suivant.
5. Le menu Attributs de rapport apparaît. Choisissez un type de rapport, au format tabulaire ou graphique. Cliquez ensuite sur Suivant.
6. Ensuite, envoyez le rapport pour création en cliquant sur Sauvegarder. Un écran d'accusé de réception apparaît indiquant que les données ont été enregistrées avec succès.

Que faire ensuite

Si vous souhaitez inclure ce rapport dans un tableau de bord, ouvrez le tableau de bord, cliquez sur Ajouter des rapports et sélectionnez ce rapport dans la liste.
Rubrique parent : Rapports

Création de rapports pour z/OS

Cette rubrique explique comment créer des rapports Guardium pour des sources de données z/OS en personnalisant des rapports intégrés et des exemples de requête.

Si le processus de création de rapports pour des sources de données z/OS data est le même que pour d'autres bases de données, il n'existe pas toujours de mappage direct entre les concepts de grand système et les entités et attributs de génération de rapport de Guardium. Pour faciliter la communication entre des auditeurs et le personnel de grand système, cette section met en évidence le mappage entre les données d'événement de grand système et les entités et attributs Guardium. Il existe certains rapports intégrés personnalisables, et ces informations décrivent les requêtes supplémentaires qui sont utiles pour des scénarios d'audit classiques.

Rubrique parent : Rapports
Concepts associés:
Domaines, entités et attributs
Utilisation du Générateur de requête
Entités et attributs

Magasin de données

Un magasin de données est un sous-ensemble d'un entrepôt de données. Un entrepôt de données agrège et organise les données de manière générique en vue de leur utilisation ultérieure pour l'analyse et les rapports. Un magasin de données commence par une analyse des données définies par l'utilisateur et met l'accent sur la satisfaction des exigences spécifiques de l'utilisateur en termes de contenu, présentation et facilité d'utilisation.

Utilisez cette fonction pour :

- Définir et générer un magasin de données.
- Agréger les données récapitulées et analysées de toutes les unités pour permettre une vue générale/d'entreprise dans un temps de réponse raisonnable.
- Améliorer les performances des rapports en ligne sur les agrégateurs Guardium.
- Fournir des capacités d'analyse interactives pour trouver des modèles, des tendances et des valeurs extrêmes.
- Activer la réduction et le développement des niveaux de données

Un magasin de données est pratique et efficace pour tous les rapports prédéfinis Guardium. Il prépare les données à l'avance pour éviter une surcharge, des analyses complètes et de mauvaises performances.

L'icône Configuration de magasin de données est disponible dans n'importe quel rapport prédéfini.

Avantages :

- Fonctionnalité d'analyse Guardium qui prend en charge le cycle de vie complet de l'analyse des données.

- Le processus d'analyse débute à partir du Générateur de requête et du Générateur de table pivot où les utilisateurs définissent leurs besoins d'analyse de données, puis utilisent l'option "Définir en tant que magasin de données".
- Le programme d'extraction du magasin de données s'exécute dans un lot selon le calendrier spécifié. Il récapitule les données en heures, jours, semaines ou mois selon la granularité demandée, puis enregistre les résultats dans une nouvelle table de la base de données Guardium Analytic.
- Les données sont ensuite accessibles aux utilisateurs via les utilitaires standard Rapports et Processus d'audit, ainsi que tout autre domaine/entité traditionnel. Les données d'extraction du magasin de données sont disponibles sous le domaine DM et le nom de l'entité est défini selon le nouveau nom de table spécifié pour les données du magasin de données. A l'aide du Générateur de requête et du Générateur de rapport standard, les utilisateurs peuvent cloner la requête par défaut et éditer la requête et le rapport, générer un portlet et l'ajouter à une sous-fenêtre.
- Le regroupement des données réduit considérablement le volume de données. Il élimine les jointures de plusieurs tables en stockant l'analyse de données dans une table non normalisée et pré-calculée.
- La vue d'entreprise est prise en charge à l'aide de l'utilitaire d'agrégation standard pour les nouvelles tables d'analyse Guardium. S'il existe une grande quantité de données de ligne détaillées aux niveaux supérieurs de la hiérarchie d'agrégation, la fonctionnalité d'agrégation sélective, qui permet l'agrégation de module(s) spécifique(s), peut être configurée pour agréger uniquement les données d'analyse.

Le générateur de magasin de données est accessible via le générateur de requête, les résultats du rapport et la vue de table pivot.

Sélectionnez l'icône Définir en tant que magasin de données. Le bouton est disponible uniquement après la sauvegarde.

L'accès à l'écran est activé pour les utilisateurs avec l'autorisation Génération de magasin de données (Autorisations associées aux rôles utilisateur). Affichez le nouveau bouton Définir en tant que magasin de données uniquement pour les utilisateurs disposant de l'autorisation appropriée.

Persistance du magasin de données - les modifications apportées à la requête, au rapport ou à la table pivot d'origine n'affectent pas le magasin de données. Un instantané de la définition d'analyse créée est sauvegardé avec le magasin de données lors de la création.

Si le magasin de données est basé sur la table pivot, le processus d'extraction ne calcule pas la ligne de total (somme des colonnes) et le pourcentage de colonne n'est pas pris en charge.

En plus de la définition du magasin de données, les éléments suivants sont créés par le processus de définition du magasin de données :

- Nouveau domaine et entité
- Requête par défaut
- Rapport par défaut et portlet
- Nouvelle table de magasin de données dans la nouvelle base de données "DATAMART" pour stocker les données extraites

Magasin de données - Générateur de requête et de rapport

Le processus de définition de magasin de données crée un domaine, une entité, une requête et un rapport par défaut. La requête et le rapport par défaut sont accessibles via le menu Générateur de rapport.

Cliquez sur le magasin de données pour ouvrir l'interface graphique du Localiseur de requête. Les champs Requête, Rapport et Entité filtrent uniquement les domaines de magasin de données (le nom de domaine commence par DatamartDefinition.DOMAIN_PREFIX).

Interface graphique du Générateur de rapport : les rapports sur les magasins de données par défaut et tous les autres rapports liés aux domaines de magasin de données sont disponibles dans l'interface graphique du Générateur de rapport.

Procédez comme suit :

1. En tant qu'administrateur, sélectionnez l'icône Magasin de données  .
2. Sélectionnez Nouveau pour créer un magasin de données ou faites un choix dans la liste des magasins de données précédemment créés.
3. Complétez les champs demandant le nom du magasin de données et le nom de la table (la valeur par défaut est DM). Spécifiez une granularité temporelle et sélectionnez une heure de début initiale à partir de l'icône du calendrier. La description est facultative.
4. Utilisez le planificateur pour planifier l'exécution de cette fonction (Exécuter une fois maintenant).
5. Utilisez la section Rôles pour restreindre le magasin de données uniquement aux utilisateurs disposant de l'autorisation appropriée.
6. Sauvegardez la configuration.

   Remarque : Les changements apportés à la requête/au rapport d'origine n'ont pas d'incidence sur le magasin de données existant.
   Remarque : Lorsqu'une extraction du magasin de données s'exécute (Planifié ou Exécuter une fois maintenant) pour la première fois, elle extrait les données à partir de la date de début initiale jusqu'à l'heure courante en fonction de la granularité temporelle. Elle sauvegarde le début de période suivant dans la table DM_EXTRACTION_STATE. Lors de l'exécution suivante, elle extrait les données à partir du début de période suivant. Si une extraction de magasin de données est recherchée avant le début de période suivant, l'extraction de magasin de données apparaît vide, car elle a déjà traité cette période. Pour extraire les données avant le début de période suivant, rétablissez les anciennes données, puis réexécutez le magasin de données.

Gestion centrale et magasin de données

Dans un environnement de gestion centralisée, la configuration est distribuée automatiquement aux unités gérées.

La planification d'extraction peut être annulée sur une unité gérée.

Dans le cas de plusieurs instances de Central Manager, la définition de magasin de données peut être clonée à l'aide de la fonction d'exportation/importation.

Ajoutez la planification d'extraction du magasin de données à l'écran de distribution de Central Manager.

Extraction du magasin de données

Données extraites :

1. Exportation de : Journal des exceptions - Détaille les exceptions/erreurs capturées par Guardium. Le journal comprend la description de l'exception/erreur, le nom d'utilisateur, l'adresse source, le protocole de base de données et plus encore.
2. Exportation de : Journal de session - Comprend des détails sur les sessions de sources de données (de la connexion à la déconnexion). Le journal comprend les horodatages de début et de fin de session, le système d'exploitation et l'utilisateur de la base de données de la session, le programme source et plus encore.
3. Exportation de : Journal de session terminée - La session peut durer longtemps. L'extraction s'exécute toutes les heures. Ce journal envoie les sessions qui se sont terminées après l'heure commencée.
4. Exportation de : Journal d'accès - Comprend les détails des informations de connexion et le récapitulatif des activités par heure. Le journal comprend le système d'exploitation et l'utilisateur de la base de données, les instructions SQL réussies et échouées, l'IP du client, l'IP du serveur et plus encore.
5. Exportation de : SQL complet - Ce journal comprend les détails des instructions SQL exécutées. Le journal comprend le SQL complet, les enregistrements affectés, l'ID de la session et plus encore.
6. Exportation de : Liste des valeurs extrêmes - Ce journal comprend les valeurs extrêmes. Le journal comprend l'IP du serveur, l'utilisateur de la base de données, le type de valeur extrême, la base de données et plus encore.
7. Exportation de : Récapitulatif des valeurs extrêmes - Ce journal comprend un récapitulatif horaire des valeurs extrêmes. Le journal comprend l'IP du serveur, l'utilisateur de la base de données, la base de données et plus encore.
8. Exportation de : Membres de groupe - Comprend un journal de tous les membres du groupe. Le journal comprend le type de groupe, la description de groupe, le membre de groupe et l'indicateur Tuple.
9. Exportation de : Journal d'extraction d'exportation - Comprend le journal des données liées à tous les fichiers d'exportation ou de copie ayant un nom commençant par "Exportation :".
10. Exportation de : Violations de politique - Une violation de politique est consignée chaque fois qu'une règle de politique est déclenchée. Ce journal comprend les détails des violations consignées, telles que l'utilisateur de la base de données, le programme source, la description de la règle d'accès, la chaîne SQL complète et plus encore.
11. Exportation de : Moniteur d'utilisation de la mémoire tampon - Fournit un ensemble étendu de statistiques d'utilisation de la mémoire tampon du sniffer.
12. Exportation de : Résultats VA - Fournit les résultats d'évaluation de vulnérabilité
13. Exportation de : Violations de politique - Détaillé – identique à journal d'extraction d'exportation, mais contient des tuples Objet/Verbe. Il est recommandé de n'utiliser que l'un ou l'autre des journaux.
14. Exportation de : Journal des accès - Détaillé – identique à Journal des accès, mais contient en plus les champs suivants de l'entité Evénement d'application : Nom d'utilisateur de l'événement, Type d'événement, Chaîne de valeur de l'événement, Numéro de valeur de l'événement, Date d'événement. Il est recommandé d'utiliser l'un ou l'autre des journaux (version normale ou détaillée), mais pas les deux.
15. Exportation de : Instances reconnues - Fournit le résultat de l'application S-TAP Discovery, qui découvre les instances de base de données
16. Exportation de : Bases de données reconnues (découvertes)
17. Exportation de : Résultats du classificateur
18. Exportation de : Sources de données
19. Exportation de : Statut S-TAP
20. Exportation de : Correctifs installés
21. Exportation de : Informations système
22. Exportation de : Utilisateur – Rôle
23. Exportation : Journal du processus de classification
24. Exportation : Liste des valeurs extrêmes - étendu
25. Exportation : récapitulatif des valeurs extrêmes par heure - étendu

Nom du magasin de données	Titre du rapport	Type d'unité	ID mag. données
Exportation : journal d'accès	Exportation : journal d'accès	Collecteur	22
Exportation : journal de session	Exportation : journal de session	Collecteur	23
Exportation : journal de session terminée	Exportation : journal de session	Collecteur	24
Exportation : journal des exceptions	Exportation : journal des exceptions	Tous	25
Exportation : SQL complet	Exportation : SQL complet	Collecteur	26
Exportation : liste des valeurs extrêmes	Liste des valeurs extrêmes d'analyse	Tous	27
Exportation : récapitulatif des valeurs extrêmes par heure	Récapitulatif des valeurs extrêmes d'analyse		
Par date	Tous	28	
Exportation : journal d'extraction d'exportation	Journal d'extraction défini par l'utilisateur	Tous	31
Exportation : membres de groupe	Exportation : membres de groupe	Tous	29
Exportation : violations de politique	Exportation : violations de politique	Collecteur	32
Exportation : moniteur d'utilisation de la mémoire tampon	Moniteur d'utilisation de la mémoire tampon	Tous	33
Exportation : Résultats VA	Exportation de l'évaluation de la sécurité	Tous	34
Exportation : violations de politique - Détaillé	Exportation : violations de politique	Collecteur	38
Exportation : journal des accès - Détaillé	Exportation : journal d'accès	Collecteur	39
Exportation : Instances reconnues	Instances reconnues	Tous	40
Exportation : Bases de données reconnues	Bases de données reconnues	Tous	41
Exportation : Résultats du classificateur	Résultats du classificateur	Tous	42
Exportation : Sources de données	Sources de données	Central Manager,	
Autonome	43		
Exportation : Statut S-TAP	Moniteur d'état S-TAP	Collecteur	44
Exportation : Correctifs installés	Correctifs installés	Tous	45
Exportation : Informations système	Correctifs installés	Tous	46
Exportation : Utilisateur - Rôle	Utilisateur - Rôle	Central Manager,	
Autonome	47		

Nom du magasin de données	Titre du rapport	Type d'unité	ID mag. données
Exportation : Journal du processus de classification	Journal du processus de classification	Tous	48
Exportation : Liste des valeurs extrêmes - étendu	Liste des valeurs extrêmes d'analyse - étendu	Tous	49
Exportation : récapitulatif des valeurs extrêmes par heure - étendu	Récapitulatif des valeurs extrêmes d'analyse par date - étendu	Tous	50

Récapitulatif du problème

Le mécanisme du magasin de données (DataMart) exporte régulièrement les données du sniffer Guardium en fonction de la requête définie.

Les fichiers de sortie peuvent être écrits à la demande sur une machine externe (configurable).

Les fichiers extraits sont compressés.

L'extraction peut être programmée (par défaut, elle a lieu toutes les heures).

Le préfixe des fichiers extraits est Global_ID et le nom d'hôte court de la machine source.

Les fichiers extraits peuvent inclure des en-têtes de colonnes (descriptions des attributs).

Utilisation

Tous les exemples figurant ci-dessous s'appuient sur le magasin de données “Exportation : journal des exceptions”. Pour les autres extractions, remplacez ce nom par l'un des suivants :

"Exportation : journal d'accès"

"Exportation : journal de session"

"Exportation : journal de session terminée"

"Exportation : journal des exceptions"

"Exportation : SQL complet"

"Exportation : liste des valeurs extrêmes"

"Exportation : récapitulatif des valeurs extrêmes par heure"

"Exportation : membres de groupe"

"Exportation : journal d'extraction d'exportation"

"Exportation : Violations de politique"

"Exportation : moniteur d'utilisation de la mémoire tampon"

"Exportation : Résultats VA"

"Exportation : Résultats du classificateur"

"Exportation : Bases de données reconnues"

"Exportation : journal des accès - Détaillé"

"Exportation : Instances reconnues"

"Exportation : Sources de données"

"Exportation : Statut S-TAP"

"Exportation : Correctifs installés"

"Exportation : Informations système"

"Exportation : Utilisateur - Rôle"

"Exportation : Journal du processus de classification"

"Exportation : Liste des valeurs extrêmes - étendu"

"Exportation : récapitulatif des valeurs extrêmes par heure - étendu"

Les extractions d'exportation sont prédéfinies dans le système (via le mécanisme de magasins de données) et désactivées par défaut. Pour activer les extractions d'exportation (toutes ou spécifiques), vous devez programmer les magasins de données via l'appel grdapi ci-après. Vous pouvez aussi utiliser l'interface graphique à cet effet.

Programmation d'un travail pour l'extraction d'un magasin de données :

grdapi schedule_job jobType=dataMartExtraction cronString=”0 1 0/1 ? * 1,2,3,4,5,6,7” objectName=”Exportation : journal des exceptions” startTime=”AAAA-MM-JJ HH:MM:SS”

Notez que le paramètre startTime sert à spécifier la date et l'heure du futur démarrage, si celui-ci doit être différé. Pour un démarrage immédiat, vous pouvez omettre ce paramètre.

Pour supprimer des extractions d'exportation spécifiques, vous pouvez exécuter l'appel suivant :

Suppression d'un travail programmé :

grdapi delete_schedule deleteJob="true" jobGroup="DataMartExtractionJobGroup” jobname="DataMartExtractionJob_25”

jobname	description de travail/ objectName
DataMartExtractionJob_22	Exportation : journal d'accès
DataMartExtractionJob_23	Exportation : journal de session
DataMartExtractionJob_24	Exportation : journal de session terminée
DataMartExtractionJob_25	Exportation : journal des exceptions
DataMartExtractionJob_26	Exportation : SQL complet
DataMartExtractionJob_27	Exportation : liste des valeurs extrêmes
DataMartExtractionJob_28	Exportation : récapitulatif des valeurs extrêmes par heure
DataMartExtractionJob_29	Exportation : membres de groupe
DataMartExtractionJob_31	Exportation : journal d'extraction d'exportation
DataMartExtractionJob_32	Exportation : violations de politique
DataMartExtractionJob_33	Exportation : moniteur d'utilisation de la mémoire tampon
DataMartExtractionJob_34	Exportation : Résultats VA
DataMartExtractionJob_38	Exportation : violations de politique - Détaillé
DataMartExtractionJob_39	Exportation : journal des accès - Détaillé
DataMartExtractionJob_40	Exportation : Instances reconnues
DataMartExtractionJob_41	Exportation : Bases de données reconnues
DataMartExtractionJob_42	Exportation : Résultats du classificateur
DataMartExtractionJob_43	Exportation : Sources de données
DataMartExtractionJob_44	Exportation : Statut S-TAP
DataMartExtractionJob_45	Exportation : Correctifs installés
DataMartExtractionJob_46	Exportation : Informations système
DataMartExtractionJob_47	Exportation : Utilisateur - Rôle
DataMartExtractionJob_48	Exportation : Journal du processus de classification
DataMartExtractionJob_49	Exportation : Liste des valeurs extrêmes - étendu
DataMartExtractionJob_50	Exportation : récapitulatif des valeurs extrêmes par heure - étendu

Vous pouvez activer ou désactiver l'extraction à l'aide de la commande suivante :

Activer le magasin de données :

grdapi datamart_set_active Name=”Exportation : journal des exceptions”

Désactiver le magasin de données :

grdapi datamart_set_inactive Name=”Exportation : journal des exceptions”

Inclure l'en-tête dans l'extraction du magasin de données :

Vous pouvez déterminer s'il faut inclure la ligne d'en-tête (noms de colonne) dans le fichier CSV de sortie via l'appel grdapi suivant :

grdapi datamart_include_file_header Name=” Exportation : journal des exceptions” includeFileHeader=”Yes”

Définir les détails de l'hôte cible :

Pour spécifier l'hôte cible de l'extraction d'exportation, vous devez fournir l'hôte, le chemin et les données d'identification via l'appel grdapi suivant :

grdapi datamart_update_copy_file_info destinationHost=”Machine_Hôte” destinationPassword=”********” destinationPath=”/emplacement/de/stockage/” destinationUser=”utilisateur” Name=”Exportation : journal des exceptions” transferMethod=”SCP” withCOMPLETEfile=false

Le paramètre withCOMPLETEfile est optionnel. Sa valeur par défaut est true. La valeur true signifie qu'un fichier COMPLETE est envoyé après le transfert réussi d'un fichier de données. Pour plus de détails, consultez la section “Fichier COMPLETE”.

Lors de l'exécution de cette commande, un fichier factice est envoyé à la machine cible pour contrôler la validité des détails de connexion. Vous pouvez aussi utiliser l'appel grdapi datamart_validate_copy_file_info à cet effet.

Contrôler la validité d'une connexion à l'hôte cible :

Pour contrôler la validité d'une connexion à un hôte cible, utilisez l'appel grdapi suivant :

grdapi datamart_validate_copy_file_info destinationHost=”Machine_hôte” destinationPassword=”********” destinationPath=”/emplacement/de/stockage/” destinationUser=”utilisateur” transferMethod=”SCP”

Vous pouvez suivre le journal d'extraction via le rapport prédéfini "Journal d'extraction du magasin de données". Ce rapport est disponible via l'écran Générateur de rapport ; vous pouvez l'ajouter à un panneau.

Entrez l'option de personnalisation dans le rapport “Journal d'extraction du magasin de données” et définissez ce qui suit :

- Entrez une valeur pour Nom : %
- Entrez le début de la période >= : AAAA-MM-JJ HH:MM:SS (entrée une date passée)

- Entrez une valeur pour Statut : %

Cliquez sur Mettre à jour pour activer le rapport Journal d'extraction du magasin de données qui montre les dernières extractions.

Heure de début recommandée pour le planificateur

Les magasins de données de valeurs extrêmes doivent être programmés 10 minutes après l'heure, car avant cela, les données ne sont pas encore prêtes. Leur préparation commence à l'heure pile.

Il est bon de programmer les extractions du journal des accès, du journal des exceptions, du journal SQL complet et du journal des sessions terminées avec un certain laps de temps entre chacune. Pour obtenir les données cohérentes pour chaque exécution, le journal des sessions terminées doit être programmé en dernier.

Nos recommandations

Description du travail	**cronString recommandé**	**Toutes les heures à :**
Exportation : journal d'accès	0 40 0/1 ? * 1,2,3,4,5,6,7	00:40
Exportation : journal de session	0 45 0/1 ? * 1,2,3,4,5,6,7	00:45
Exportation : journal de session terminée	0 46 0/1 ? * 1,2,3,4,5,6,7	00:46
Exportation : journal des exceptions	0 25 0/1 ? * 1,2,3,4,5,6,7	00:25
Exportation : SQL complet	0 30 0/1 ? * 1,2,3,4,5,6,7	00:30
Exportation : liste des valeurs extrêmes	0 10 0/1 ? * 1,2,3,4,5,6,7	00:10
Exportation : récapitulatif des valeurs extrêmes par heure	0 10 0/1 ? * 1,2,3,4,5,6,7	00:10
Exportation : journal d'extraction d'exportation	0 50 0/1 ? * 1,2,3,4,5,6,7	00:50
Exportation : membres de groupe	0 15 0/1 ? * 1,2,3,4,5,6,7	00:15
Exportation : violations de politique	0 5 0/1 ? * 1,2,3,4,5,6,7	00:05
Exportation : moniteur d'utilisation de la mémoire tampon	0 12 0/1 ? * 1,2,3,4,5,6,7	00:12
Exportation : Résultats VA	0 0 2 ? * 1,2,3,4,5,6,7	Tous les jours à 2h
Exportation : violations de politique - Détaillé	0 5 0/1 ? * 1,2,3,4,5,6,7	00:05
Exportation : journal des accès - Détaillé	0 40 0/1 ? * 1,2,3,4,5,6,7	00:40
Exportation : Instances reconnues	0 20 0/1 ? * 1,2,3,4,5,6,7	00:20
Exportation : Bases de données reconnues	0 20 0/1 ? * 1,2,3,4,5,6,7	00:20
Exportation : Résultats du classificateur	0 20 0/1 ? * 1,2,3,4,5,6,7	00:20
Exportation : Sources de données	0 0 7 ? * 1,2,3,4,5,6,7	Tous les jours à 7h
Exportation : Statut S-TAP	0 0/5 0/1 ? * 1,2,3,4,5,6,7	Toutes les 5 minutes
Exportation : Correctifs installés	0 0 5 ? * 1,2,3,4,5,6,7	Tous les jours à 5h
Exportation : Informations système	0 0 5 ? * 1,2,3,4,5,6,7	Tous les jours à 5h
Exportation : Utilisateur - Rôle	0 5 0/1 ? * 1,2,3,4,5,6,7	00:05
Exportation : Journal du processus de classification	0 25 0/1 ? * 1,2,3,4,5,6,7	00:25
Exportation : Liste des valeurs extrêmes - étendu	0 10 0/1 ? * 1,2,3,4,5,6,7	00:10
Exportation : récapitulatif des valeurs extrêmes par heure - étendu	0 10 0/1 ? * 1,2,3,4,5,6,7	00:10

Purgez le répertoire /var/exportdir

Si un transfert de fichier a échoué pour quelque raison que ce soit, par exemple, la machine cible est en panne, un autre transfert est tenté à l'exécution suivante. Le journal des éléments en attente se trouve dans le répertoire /var/exportdir. Le processus de purge élimine les arriérés de plus d'un jour.

Fichier COMPLETE

Le fichier COMPLETE vide est envoyé pour avertir un système externe qu'un fichier est prêt.

- Pour chaque fichier, en plus du fichier, un fichier COMPLETE est également envoyé. Le nom de fichier COMPLETE est [nom_fichier]_COMPLETE.gz

1762144738_gibm32_EXP_SESSION_LOG_20151028230000_COMPLETE.gz

- Le processus est synchrone - par exemple, le fichier (fichier SESSION LOG) est d'abord généré, puis il est copié, et c'est seulement lorsque sa copie est terminée que le fichier COMPLETE est généré et copié.

- Un fichier COMPLETE est envoyé même s'il n'y a pas de données à envoyer.

Changer la date et l'heure du démarrage initial du magasin de données :

Pour changer la date et l'heure du démarrage initial du magasin de données, utilisez l'appel grdapi update_datamart.

grdapi update_datamart Name="Exportation : journal de session" initial_start=[valeur démarrage initial]

Exemple :

Régler le démarrage initial sur la date et l'heure courantes :

grdapi update_datamart Name="Exportation : journal de session" initial_start=< >

Régler le démarrage initial au 1er octobre 2016

grdapi update_datamart Name="Exportation : journal de session" initial_start="2016-10-01 00:00:00"

Copier un bundle de fichiers

Il est possible de regrouper plusieurs exports CSV de magasins de données dans un bundle. Le bundle contient le magasin de données principal. Chaque magasin de données inclus dans un bundle extrait des données en fonction de son propre planning. Une fois que le magasin de données principal a extrait les données, il place les fichiers de données de tous les magasins de données inclus dans le bundle dans le même fichier tar et envoie celui-ci à un serveur de destination. Le magasin de données principal doit être le dernier du planning.

Par exemple, le bundle inclut “Exportation : SQL complet”, “Exportation : journal des exceptions”, “Exportation : journal de session” et “Exportation : journal de session terminée” comme magasin de données principal.

L'ordonnancement recommandé pour ce bundle est le suivant :

Description du travail cronString recommandé Toutes les heures à :

Exportation : journal de session 0 45 0/1 ? * 1,2,3,4,5,6,7 00:45

Exportation : journal de session terminée 0 46 0/1 ? * 1,2,3,4,5,6,7 00:46

Exportation : journal des exceptions 0 25 0/1 ? * 1,2,3,4,5,6,7 00:25

Exportation : SQL complet 0 30 0/1 ? * 1,2,3,4,5,6,7 00:30

Créer un bundle :

grdapi datamart_copy_file_bundle action="create" bundle_name=[nom du bundle] main_datamart_name=[nom du magasin de données principal]

Inclure un magasin de données dans un bundle :

grdapi datamart_copy_file_bundle action="include" bundle_name=[nom du bundle] datamart_name=[nom du magasin de données]

Exclure un magasin de données d'un bundle :

grdapi datamart_copy_file_bundle action="exclude" bundle_name=[nom du bundle] datamart_name=[nom du magasin de données]

Supprimer un bundle :

grdapi datamart_copy_file_bundle action="delete" bundle_name=[nom du bundle]

Obtenir les informations d'un bundle :

grdapi datamart_copy_file_bundle action="info" bundle_name=[nom du bundle]

Exemple :

grdapi datamart_copy_file_bundle action="create" bundle_name="SFE_BUNDLE" main_datamart_name="Exportation : journal de session terminée"

grdapi datamart_copy_file_bundle action="include" bundle_name="SFE_BUNDLE" datamart_name="Exportation : journal des exceptions"

grdapi datamart_copy_file_bundle action="include" bundle_name="SFE_BUNDLE" datamart_name="Exportation : SQL complet"

grdapi datamart_copy_file_bundle action="include" bundle_name="SFE_BUNDLE" datamart_name="Exportation : journal de session"

> grdapi datamart_copy_file_bundle action="info" bundle_name="SFE_BUNDLE" main_datamart_name="Exportation : journal de session" datamart_name=""

ID=0

==========

Nom du bundle : SFE_BUNDLE

==========

Magasin de données principal : Exportation : journal de session terminée

Magasins de données :

Exportation : SQL complet

Exportation : journal des exceptions

Exportation : journal de session

Get_Datamart Info grdapi

L'appel grdapi get_datamart_info obtient les informations détaillées d'un magasin de données.

get_datamart_info datamart_name=[nom du magasin de données]

Exemple,

grdapi get_datamart_info datamart_name="Exportation : journal d'extraction d'exportation"

==========

Nom de magasin de données : Exportation : journal d'extraction d'exportation

==========

Description :

Rapport de base : Journal d'extraction défini par l'utilisateur

Requête de base : Journal d'extraction défini par l'utilisateur

Extraire le résultat vers : Fichier

Début initial : 2016-04-18 09:00:00

Date de création : 2016-12-28 18:01:24

Granularité temporelle : 1 HEURE

Actif : vrai

Nom de fichier : EXP_DM_EXTRACTION_LOG

Lignes par fichier : 500000

En-tête du fichier : "Décalage UTC","Nom","Début de période","Fin de période","ID exécution","Heure de début","Heure de fin","Statut","Statut de fichier","Enregistrements extraits","Détails","Horodatage"

Inclure l'en-tête du fichier : vrai

Informations sur la copie de fichier

Nom d'hôte : host.com

Nom d'utilisateur : admin

Répertoire : /local/incoming/

Méthode de transfert : SCP

Nom du bundle :

Magasin de données principal du bundle : faux

Envoi d'un fichier COMPLETE : faux

Informations sur la dernière extraction

Etat : 1

Horodatage : 2017-01-18 14:50:00

Prochaine période : 2017-01-18 14:00:00

Dernier ID extrait : 0

Journal d'extraction

Horodatage : 2017-01-18 14:50:02

Statut de l'extraction : OK

Heure de début : 2017-01-18 14:50:00

Heure de fin : 2017-01-18 14:50:00

Début de période : 2017-01-18 13:00:00

Fin de période : 2017-01-18 14:00:00

Enregistrements extraits : 26

Détails : SCP à : host.com, Utilisateur : admin, Chemin : /local/incoming/, Fichier : DMv2_gibm32_EXP_DM_EXTRACTION_LOG_20170118180000.gz

Dernier de la période : vrai

Nom de fichier : /var/dump/DATAMART/EXP_DM_EXTRACTION_LOG_20170118180000.csv

Nom du bundle :

Statut du transfert de fichier : Terminé

Commentaires

==========

Le magasin de données Full_SQL ne fonctionne que si la politique Consigner l'ensemble des détails ou Consigner les détails masqués est définie et installée.

Les magasins de données de valeurs extrêmes ne fonctionnent que si la détection des valeurs extrêmes est activée.

Si le planificateur du magasin de données a été arrêté pendant un certain temps et que vous ne souhaitez pas que les données soient extraites de manière rétroactive, avant de replanifier l'exécution des extractions, définissez le Début initial correct dans l'écran Configuration de magasin de données.

Magasins de données définis par l'utilisateur

Le transfert de données à un hôte de destination peut aussi se faire au moyen d'un magasin de données personnalisé. Le magasin de données doit être du type Fichier, son nom doit commencer par “Exportation :” et le nom du fichier doit commencer par “EXP_”.

Dépendances

==========

Comment appliquer un correctif :

==========

http://www-01.ibm.com/support/knowledgecenter/SSMPHH_8.2.0/com.ibm.guardium.using.doc/topics/how_to_install_patches.html?lang=en

Commandes GuardAPI pour magasins de données

grdapi datamart_copy_file_bundle

Paramètres de fonction :

action - Chaîne - requis - Liste de valeurs constantes

bundle_name - Chaîne - requis

datamart_name - Chaîne

main_datamart_name - Chaîne

grdapi datamart_include_file_header

Paramètres de fonction :

includeFileHeader - Chaîne - requis - Liste de valeurs constantes

Name - Chaîne - requis

grdapi datamart_set_active

Paramètres de fonction :

Name - Chaîne - requis

grdapi datamart_set_inactive

Paramètres de fonction :

Name - Chaîne - requis

grdapi datamart_update_copy_file_info

Paramètres de fonction :

destinationHost - Chaîne

destinationPassword - Chaîne

destinationPath - Chaîne

destinationUser - Chaîne

Name - Chaîne - requis

transferMethod - Chaîne - Liste de valeurs constantes

withCOMPLETEfile - Booléen

grdapi datamart_validate_copy_file_info

Paramètres de fonction :

destinationHost - Chaîne - requis

destinationPassword - Chaîne - requis

destinationPath - Chaîne - requis

destinationUser - Chaîne - requis

transferMethod - Chaîne - Liste de valeurs constantes

grdapi update_datamart

Paramètres de fonction :

Comment - Chaîne

initial_start - Date

Name - Chaîne - requis

grdapi get_datamart_info

Paramètres de fonction :

datamart_name - Chaîne - requis

isExtended - Booléen

Rubrique parent : Rapports

Audit et rapport

Guardium organise les données qu'il collecte en un ensemble de domaines. Chaque domaine contient un type différent d'informations relatives à un aspect spécifique : accès aux données, exceptions, violations de politique, etc.

Tous les domaines et leurs contenus sont décrits dans l'annexe Domaines, entités et attributs.

Il existe un générateur de requête distinct pour chaque domaine et l'accès à chaque générateur de requête est contrôlé par des rôles de sécurité. Quel que soit le domaine, le même outil de génération de requêtes à usage général est utilisé pour créer toutes les requêtes. Pour obtenir des instructions détaillées sur la façon de créer des requêtes, consultez la rubriqueRequêtes.

En plus de l'ensemble standard de domaines, les utilisateurs peuvent définir des domaines personnalisés pour contenir des informations pouvant être téléchargées sur le dispositif Guardium. Par exemple, votre entreprise peut utiliser une table qui relie des noms d'utilisateurs de base de données génériques (hr23455 ou qa4872, par exemple) à des personnes réelles (Paula Smith, John Doe). Une fois que cette table a été téléchargée, les noms réels peuvent être affichés dans les rapports Guardium à partir du domaine personnalisé. Pour plus d'informations détaillées sur la façon de définir et d'utiliser des domaines personnalisés, consultez la rubrique Corrélation des données externes.

Rubrique parent : Rapports

Requêtes

Utilisez l'une des nombreuses requêtes prédéfinies fournies avec Guardium pour obtenir des informations sur vos données. Utilisez le Générateur de requête pour gérer des requêtes.

Utilisez des requêtes pour poser des questions sur vos données, par exemple, quels sont les clients qui mettent à jour une base de données spécifique pendant les heures de week-end ?

Les requêtes sont différentes des rapports. Une requête décrit un jeu de données, tandis qu'un rapport présente les données renvoyées par une requête.

Une fois la requête terminée, présentez les résultats de la requête à l'aide des rapports. Les rapports sont généralement affichés sous forme de tableaux, mais vous pouvez personnaliser la présentation d'un rapport comme vous le souhaitez.

Pour utiliser des requêtes, ouvrez le Générateur de requête en cliquant sur Conformité > Génération de rapports personnalisés > Générateur de requête personnalisée. Choisissez un domaine à rechercher, sélectionnez une entité principale, puis utilisez la requête au besoin.

Vous ne pouvez pas modifier les requêtes prédéfinies, mais vous pouvez créer un clone d'une requête et le modifier.

Entité principale

L'entité principale que vous sélectionnez pour une requête détermine ce qui suit :

- Niveau de détail du rapport. Il existe une ligne de données pour chaque occurrence de l'entité principale incluse dans le rapport. L'emplacement de l'entité principale dans la hiérarchie des entités est important en termes de valeurs pouvant être affichées. Les attributs de toutes les entités sous l'entité principale peuvent être comptabilisés, mais pas affichés (car il peut y avoir de nombreuses occurrences pour chaque ligne). Pour choisir ce niveau de détail, cochez la case Trier par nombre.
- Le nombre total est un nombre d'instances de l'entité principale incluses dans cette ligne du rapport, ajoutée en tant que dernière colonne du rapport. Pour ajouter ou supprimer la colonne de nombre du rapport, cliquez sur la case à cocher Ajouter un nombre. Cela peut entraîner dans certains cas une amélioration des performances de la requête/du rapport.
- Pour ajouter ou supprimer la possibilité d'afficher une ligne par valeur dans le rapport, (ce qui peut entraîner une augmentation des performances de la requête/du rapport dans certains cas), cliquez sur la case à cocher Ajouter une ligne distincte. Cette sélection produit des rapports condensés.
- L'optimisation de partition est activée par défaut et améliore les performances de requête avec des tables de base de données partitionnées. Sur Guardium V10.1.2 et versions ultérieures, cette fonctionnalité peut être désactivée en désélectionnant la case à cocher Optimisation de partition. L'optimisation de partition ne doit pas être désactivée sans instructions du support IBM.
- Champs de temps par rapport auxquels les paramètres d'exécution Début de la période et Fin de la période sont comparés pour sélectionner les lignes du rapport. Le Générateur de requête utilise l'entité principale (entre autres paramètres) pour déterminer les champs de temps utilisés lors de la définition des valeurs Début de la période et Fin de la période. Cela peut être important pour les sessions à exécution longue, par exemple lorsque des sessions groupées sont ouvertes par un serveur d'applications. Le cas échéant, le Début de la période/la Fin de la période issus de l'entité Période d'accès sont utilisés, dans d'autres cas, les valeurs de période selon l'entité principale sont sélectionnées :
  - Session - l'horodatage utilisé concerne la dernière mise à jour apportée à l'entité de la session
  - Début de session - l'heure de début de l'entité de session est utilisée
  - Fin de session - l'heure de fin de l'entité de session est utilisée
  - SQL complet - horodatage du domaine SQL complet ; la requête comprend des lignes issues du domaine SQL complet, même si elles ne sont pas liées à des valeurs (par exemple, lorsque l'élément Consigner l'ensemble des détails est défini, il n'y a pas de valeurs)

- Valeurs du SQL complet - horodatage issu du domaine SQL complet. La requête comprend des lignes uniquement si elles contiennent des valeurs émanant du domaine SQL complet, même si elles ne sont pas liées au domaine Champ
- Valeurs du SQL de champ - horodatage issu du domaine SQL complet. La requête comprend des lignes uniquement si elles contiennent des valeurs émanant du domaine SQL complet, et si elles sont liées au domaine Champ

- L'écran Entité principale contient la sélection Exécutez en deux étapes.

  Utilisez cette sélection pour une exécution en deux étapes des tâches d'audit du rapport de type.

  Applicable uniquement aux rapports sur les requêtes sur des tables spécifiques. Ce mécanisme en deux étapes s'applique à l'exécution de requêtes en tant que processus d'audit avec des colonnes et des conditions uniquement sur les entités suivantes : Accès (client-serveur), Session, Période d'accès, Enregistrement (SQL), Objet et Phrase (Commande).

  Ce mécanisme en deux étapes n'est pas utilisé si la requête contient une condition avec l'opérateur `Like Group` ou tout opérateur associé à l'alias (tel que `In Aliases Group`) ou la condition HAVING.

  En plus d'utiliser le générateur de requête, chaque requête peut être définie en deux étapes. Par défaut, les requêtes s'exécutent à l'aide de l'ancienne méthode. Pour qu'une requête s'exécute en deux étapes, un indicateur doit être défini dans le générateur de requête. En outre, cette méthode d'exécution des requêtes peut être désactivée (dans l'ensemble du système) pour que toutes les tâches d'audit utilisent l'ancienne méthode en créant le fichier : /var/log/guard/DontRunInTwoStages. L'existence de ce fichier indique que la nouvelle méthode en deux étapes NE DOIT PAS être utilisée.
  Remarque : Les champs contenant des tuples (champs combinés) dans l'exécution en deux étapes ne sont pas pris en charge dans cette version.

Remarque : Remarque : la liste déroulante de l'Entité principale comprend uniquement les entités principales. Cependant, l'accès à des entités secondaires (par exemple Début de session et Fin de session) peut se faire via son entité principale correspondante (par exemple, Session pour Début de session et Fin de session).

Tri

Par défaut, les données de la requête sont triées en ordre croissant par valeur d'attribut, les clés de tri sont classées à mesure que les attributs apparaissent dans la requête. Les alias sont ignorés à des fins de tri. Les valeurs de données réelles sont toujours utilisées pour le tri. Les attributs pour lesquels des valeurs sont calculées par la requête (Nombre, Min, Max ou Moy) ne peuvent pas être triés.

Pour modifier l'ordre de tri par défaut :

1. Cochez la case Trier par.
2. Entrez un nombre pour Niveau de tri (1 est la clé de tri la plus importante).
3. En option, cochez la case Ordre décroissant pour trier les valeurs de cet attribut par ordre décroissant.

La dernière colonne d'un rapport tabulaire est un comptage des occurrences d'entité principale. Pour effectuer un tri à partir de ce nombre par ordre décroissant (en d'autres termes, répertorier le plus grand nombre d'occurrences en premier), cochez la case Trié par occurrences.

Horodatages

Un horodatage (t minuscule) est un type de données contenant une valeur combinée de date et heure, qui, lorsqu'il est affiché, apparaît au format aaaa-mm-jj hh:mm:ss (par exemple, 2012-07-17 15:40:25). Lors de la création ou de l'édition d'une requête, la plupart des attributs dotés d'un type de données d'horodatage s'affichent avec une icône d'horloge dans le panneau Liste d'entités.

Un horodatage (T majuscule) est un attribut défini dans de nombreux types d'entités, contenant l'heure à laquelle l'entité a été mise à jour pour la dernière fois. Pour de nombreux attributs d'horodatage, vous pouvez imprimer séparément les composants de date, d'heure, de semaine ou d'année en faisant référence aux attributs d'horodatage supplémentaires (date, heure, jour de semaine ou année).

- Utilisation du Générateur de requête
  Utilisez le Générateur de requête pour créer ou modifier des requêtes. Spécifiez le domaine que vous souhaitez interroger, choisissez une entité principale, puis utilisez le Générateur de requête pour définir ou modifier une requête.
- Conditions de requête
  Utilisez les opérateurs AND, OR et HAVING avec des parenthèses pour créer des conditions de requête.

Rubrique parent : Rapports

Utilisation du Générateur de requête

Utilisez le Générateur de requête pour créer ou modifier des requêtes. Spécifiez le domaine que vous souhaitez interroger, choisissez une entité principale, puis utilisez le Générateur de requête pour définir ou modifier une requête.

1. Ouvrez le Générateur de requête en cliquant sur Conformité > Génération de rapports personnalisés > Générateur de requête personnalisée.
2. Déterminez le domaine que vous souhaitez interroger. Sélectionnez un élément dans le menu Localiseur de domaine et cliquez sur Recherche, ou sur Nouveau  pour créer un domaine personnalisé.
3. Choisissez une requête existante à l'aide des menus de filtrage dans le Localiseur de requête ou cliquez sur Nouveau pour créer une nouvelle requête.
4. Il existe trois composants principaux dans l'écran du Générateur de requête :
   - La sous-fenêtre Liste d'entités identifie toutes les entités et les attributs contenus dans le domaine. Les entités sont représentées sous forme de dossiers et les attributs sont les éléments des dossiers. Cliquez sur un dossier d'entité pour afficher ses attributs, ou cliquez de nouveau pour les masquer. Pour une description de l'ensemble des entités et des attributs, voir Entités et Attributs dans les informations Domaines, entités et attributs.
   - La sous-fenêtre Champs de requête répertorie tous les champs accessibles, les informations à afficher pour ce champ (valeur, nombre, minimum, maximum ou moyenne) et l'ordre de tri. Pour plus d'informations sur l'utilisation de cette sous-fenêtre, voir *Présentation des champs de requête*.
   - La sous-fenêtre Conditions de requête spécifie les conditions de sélection de ces champs (par exemple, `where VERB = UPDATE`). Pour plus d'informations sur l'utilisation de cette sous-fenêtre, voir *Présentation des conditions de requête*.

Création d'une requête

1. Ouvrez le Générateur de requête pour le domaine approprié.
2. Cliquez sur Nouveau pour ouvrir le panneau Nouvelle requête - Détails globaux.
3. Entrez un nom de requête unique dans la zone Nom de requête. N'incluez pas les caractères apostrophe dans le nom de la requête.

4. Sélectionnez l'entité principale pour la requête dans la liste des entités principales. N'oubliez pas que l'entité principale contrôle le niveau de détail disponible pour la requête et qu'elle ne peut pas être modifiée. Fondamentalement, chaque ligne de données renvoyée par la requête représente une instance unique de l'entité principale et un nombre d'occurrences pour cette instance.
5. Cliquez sur Suivant. La nouvelle requête s'ouvre dans le panneau Générateur de requête. Pour compléter la définition, voir l'une des rubriques suivantes :
    - Présentation du Générateur de requête
    - Modification d'une requête

Modification d'une requête

Vous ne pouvez pas modifier les requêtes prédéfinies de Guardium, mais vous pouvez cloner une requête et modifier le clone au besoin.

1. Sélectionnez un domaine et une entité principale pour ouvrir le Générateur de requête pour la requête que vous souhaitez modifier.
2. Cliquez sur Cloner, entrez un nouveau nom pour la requête (les apostrophes ne sont pas autorisées) et cliquez sur Sauvegarder.
3. Reportez-vous à la rubrique Présentation du Générateur de requête pour modifier tout composant de la définition de la requête.

Suppression d'une requête

Vous ne pouvez pas supprimer une requête utilisée par un autre composant. Pour supprimer cette requête, vous devez d'abord supprimer tous les composants qui l'utilisent (rapports ou alertes de corrélation, par exemple). Lors de la tentative de suppression d'une requête, les rapports et les alertes de corrélation dépendants de la requête sont répertoriés.

1. Sélectionnez un domaine et une requête pour ouvrir le Générateur de requête pour la requête que vous souhaitez supprimer.
2. Cliquez sur Supprimer.

Présentation des champs de requête

La sous-fenêtre champs de requête répertorie les colonnes de données devant être renvoyées par la requête.

Les menus Mode champ indiquent ce qu'il convient afficher dans le champ : Valeur, Nombre (nombre de valeurs distinctes), Min, Max, Moyenne ou Somme pour la ligne. La sélection Valeur n'est pas disponible pour les attributs issus d'entités supérieures à l'entité principale dans la hiérarchie d'entités pour le domaine.

Il existe deux façons d'ajouter un champ à la sous-fenêtre Champs de requête :

- Méthode du menu contextuel :
    1. Dans la Liste d'entités, cliquez sur le champ à ajouter.
    2. Sélectionnez Ajouter un champ dans le menu contextuel.
- Méthode glisser-déposer :
    1. Dans la Liste d'entités, cliquez sur l'icône du nom du champ (et non sur le nom du champ lui-même), faites glisser l'icône dans la sous-fenêtre Champs de requête et relâchez-la.

Lorsqu'un champ est ajouté, il est placé à la fin de la liste.

Pour déplacer un champ vers le haut ou vers le bas dans la sous-fenêtre Champs de requête, cochez la case du champ et cliquez sur les icônes Haut ou Bas pour déplacer le champ d'une ligne vers le haut ou le bas.

Précaution concernant les attributs SQL complet dans les requêtes

Utilisez avec précaution l'attribut SQL complet dans une requête. Il peut produire des rapports très volumineux, car chaque valeur distincte de l'attribut (chaîne de requête SQL complet dans ce cas) est renvoyée dans une ligne distincte.

D'autre part, le rapport peut ne contenir aucune information ou plusieurs colonnes vides alors que vous attendez des chaînes SQL complet. Guardium capture uniquement le SQL complet lorsque cela lui est demandé dans les règles de politique - et les règles peuvent ne pas avoir été déclenchées pendant la période de génération de rapports.

Ne confondez pas l'attribut SQL complet avec la possibilité d'explorer le SQL pour la plupart des requêtes dans le domaine Accès aux données ayant des éléments en commun avec les requêtes SQL.

Groupes de types autres que les types définis dans l'attribut

La validation sur le type de groupe est souvent restrictive. Pour des exemples de types de groupes, consultez Aperçu des groupes. A l'aide des Conditions de requête, le Générateur de requête, un groupe de types autres que le type défini pour l'attribut dans la condition du groupe est autorisé. Ces choix supplémentaires ne concernent que les opérateurs IN GROUP et IN DYNAMIC GROUP. La sélection de types autres que le type défini pour la condition est effectuée dans le paramètre d'exécution du rapport tabulaire.

1. Créez un groupe dans le Générateur de groupe en cliquant sur Configuration > Outils & Vues > Générateur de groupe. Spécifiez un nom de groupe et choisissez OBJETS pour Type de groupe.
2. Créez un rapport d'accès dans le Générateur de rapport en cliquant sur Configuration > Rapports > Générateur de rapport.
3. Spécifiez un nom de requête et cliquez sur le dossier OBJETS dans la liste d'entités afin d'afficher plus d'options.
4. Sélectionnez Nom d'objet et cliquez une fois pour obtenir le choix ADD CONDITION. Cliquez sur Ajouter une condition pour ajouter une ligne à la section Conditions de requête dans le corps principal de l'écran de menu.
5. Accédez à la liste déroulante en regard de l'attribut Nom de l'objet et sélectionnez, dans la colonne Opérateur, IN GROUP ou GROUPE IN DYNAMIC. Dans la deuxième sélection déroulante (colonne Paramètre d'exécution), sélectionnez le groupe que vous avez créé à l'étape 1.
6. Sauvegardez votre travail. Cliquez sur Générer un rapport tabulaire, puis cliquez sur Ajouter à mes nouveaux rapports.
7. Accédez à l'onglet Mes nouveaux rapports et mettez en surbrillance le rapport que vous avez créé.
8. Cliquez sur Personnaliser en regard du nom du rapport. Vous ouvrez un onglet appelé Personnalisation de portlet (paramètres d'exécution).
9. Ouvrez la sélection déroulante et les groupes du type correspondant à l'entité testée apparaissent au début de la liste, suivis d'une double ligne en pointillés, et des groupes restants. Différents groupes peuvent alors être sélectionnés.
10. Sauvegardez votre travail en cliquant sur Mettre à jour.

Tableau 1. Boutons

Boutons	Etapes

Boutons	Etapes
Supprimer	1. Sélectionnez la requête à supprimer. 2. Cliquez sur Supprimer.
Cloner	1. Sélectionnez la requête à cloner. 2. Cliquez sur le Clone. 3. Entrez un nouveau nom pour la requête clonée.
Rôles	Si vous affectez des rôles à des rapports alors que vous vous trouvez dans le Générateur de requête, vous attribuez uniquement le rôle à la requête et non au rapport. Affectez des rôles aux rapports dans Générateur de rapport. Voir Rapports.
Sauvegarder	Cliquez sur Sauvegarder lorsque vous avez terminé toutes les tâches requises sur l'écran du menu.
Retour	Déplacez-vous entre les écrans de menu d'une tâche ou d'une fonction Guardium multi-écran à l'aide du bouton Retour. La flèche arrière dans le navigateur Web ne fonctionne pas pour la navigation entre les écrans de menu.
Définir comme magasin de données	Un magasin de données est un sous-ensemble d'un entrepôt de données. Un entrepôt de données agrège et organise les données de manière générique en vue de leur utilisation ultérieure pour l'analyse et les rapports.

Rubrique parent : Requêtes
Concepts associés:
Domaines, entités et attributs

Conditions de requête

Utilisez les opérateurs AND, OR et HAVING avec des parenthèses pour créer des conditions de requête.

Les opérateurs AND, OR et HAVING sont situés dans la barre de titre Conditions de requête du Générateur de requête.

Faites un choix dans la Liste d'entités et utilisez les opérateurs pour créer des conditions de requête dans le cadre de votre requête.

Utilisation des opérateurs AND et OR :

- Les opérateurs AND ont la priorité sur les opérateurs OR.
- Ajoutez un opérateur AND ou un opérateur OR à la fin ou au milieu de la liste de conditions à l'aide du menu d'ajout de condition ou faites glisser et déposez l'icône de l'attribut. Sélectionnez et supprimez les conditions en cliquant sur Supprimer. Sauvegardez la requête. Si la requête SQL générée n'est pas valide, la requête n'est pas enregistrée et un message d'erreur apparaît.

Utilisation de parenthèses :

- Toutes les conditions sont indépendantes. Regroupez les conditions en les entourant des parenthèses gauche et droite. Utilisez des parenthèses dans des conditions de requête complexes.
- Lorsqu'une condition est sélectionnée, appuyer sur le bouton de parenthèse gauche ajoute une condition de parenthèse gauche avant la première condition sélectionnée. En appuyant sur le bouton de parenthèse droite, vous ajoutez une condition de parenthèse droite après la première condition sélectionnée. Si aucune condition n'est sélectionnée, appuyer sur les boutons des parenthèses n'a aucun effet.
- Lors de la création d'une condition de requête qui utilise des parenthèses, les parenthèses apparaissent dans l'INTERFACE UTILISATEUR AVANT l'opérateur, mais sont appliquées APRÈS l'opérateur. Par exemple, une condition de requête est affichée comme suit, *ceci (AND cela OR autre)*. Cependant, la logique réelle est *ceci AND (cela OR autre)*.

Echappement des caractères de barre oblique inversée (\) : Pour mettre en échappement correctement un caractère de barre oblique inversée pour une utilisation dans une condition de requête, utilisez quatre caractères de barre oblique inversée. Par exemple, pour spécifier `domain\user`, entrez `domain\\\\user`.

Le panneau d'affichage des conditions comprend deux parties : l'une commence par la condition WHERE et l'autre commence par la condition HAVING.

Dans la partie HAVING, le champ agrégé comporte les options : Nombre, Min, Max et MOY. L'option SUM s'applique également à certaines entités dont le nom comporte l'ID (ID session, ID global, ID SQL complet, ID instance). Si l'option HAVING n'est pas cochée, la condition est insérée dans la partie WHERE avec le champ agrégé en tant que chaîne vide. Si l'option HAVING est cochée, la condition est insérée dans la partie HAVING et le champ agrégé contient des options. Après l'ajout ou la suppression d'une condition, l'option de condition est mise à jour. Appuyez sur Sauvegarder pour générer un SQL. Le SQL est validé avant la sauvegarde. Si la validation a échoué (par exemple, erreur de syntaxe), elle génère un message d'erreur d'alerte et place une description d'erreur plus détaillée dans le journal. Si vous ajoutez une condition à la partie incorrecte, (par exemple, l'option HAVING est définie et l'icône d'attribut est supprimée sur la partie WHERE, ou vice versa), un message d'alerte non concordant est généré. Si la condition sélectionnée se trouve dans la partie WHERE, mais l'option HAVING est définie, la condition d'ajout échoue car le paramètre n'est pas concordant.

Les attributs Accès total, SQL échoués et SQL réussis ne peuvent être ajoutés que dans une clause HAVING (pas dans la clause WHERE).

Les requêtes autorisées doivent comporter une colonne d'horodatage, et au moins une colonne avec Mode=Count OU l'indicateur de comptage défini (ou les deux). La colonne de requête à évaluer par la requête doit être l'une des colonnes avec Mode=Count OU la colonne du Total des accès (si l'indicateur de comptage est défini).

Ajouter ou supprimer une condition de requête

1. Pour supprimer une condition de requête, cochez la case dans la ligne pour cette condition et cliquez sur le bouton X (Supprimer l'élément marqué) dans la barre de titre des Conditions de requête.
2. Pour ajouter une condition, créez une ligne dans la liste Conditions de requête pour le champ approprié dans la sous-fenêtre Liste d'entités.

   Pour ajouter une condition AND, sélectionnez le bouton d'option AND dans la barre de titre des Conditions de requête et effectuez l'une des opérations suivantes :

   - Sélectionnez une entité dans la sous-fenêtre Liste d'entités et sélectionnez Ajouter une condition dans le menu contextuel.
   - Faites glisser l'icône de champ de la sous-fenêtre Liste d'entités et déposez-la dans la sous-fenêtre Conditions de requête.

   Pour ajouter une condition OR, sélectionnez le bouton d'option OR dans la barre de titre des Conditions de requête et effectuez l'une des opérations suivantes :

- Faites glisser l'icône de champ de la sous-fenêtre Liste d'entités et relâchez-la au début d'une condition OR.
- Cochez la case correspondant à la condition à laquelle vous souhaitez ajouter la condition OR, cliquez sur le champ dans la sous-fenêtre Liste d'entités, puis sélectionnez Ajouter une condition dans le menu contextuel.

3. *Facultatif* : utilisez le menu déroulant Agrégat pour sélectionner un agrégat de l'attribut à utiliser pour la condition de requête : Nombre, Min (valeur minimale), Max (valeur maximale) ou MOY (valeur moyenne). Des restrictions s'appliquent, comme suit :
   - Vous ne pouvez pas utiliser un agrégat dans une condition OR.
   - Vous ne pouvez pas ajouter de condition OR à une condition qui contient un agrégat.
4. Sélectionnez l'opérateur pour la nouvelle condition dans la liste. Certains types d'attributs ne possèdent pas le même ensemble d'opérateurs disponibles. Par exemple, les attributs qui ne peuvent être associés à des groupes ne disposent d'aucune option de groupe (IN GROUP, LIKE GROUP). Cependant, lors de l'ajout de tuples (plusieurs attributs combinés pour former un seul groupe) en tant que condition d'une requête, tous les opérateurs pour une nouvelle condition sont disponibles pour la sélection.

Tableau 1. Opérateur pour une nouvelle condition

Opérateur	**Description**
<	Inférieur à
< =	Inférieur ou égal à
< >	Non égal à
=	Egal à
>	Supérieur à
> =	Supérieur ou égal à
CATEGORIZED AS	Membre d'un groupe appartenant à la catégorie sélectionnée dans la liste déroulante, qui s'affiche lorsqu'un opérateur de groupe est sélectionné.
CLASSIFIED AS	Membre d'un groupe appartenant à la classification sélectionnée dans la liste déroulante, qui s'affiche lorsqu'un opérateur de groupe est sélectionné.
IN DYNAMIC GROUP	Membre d'un groupe sélectionné dans la liste déroulante dans la colonne des paramètres d'exécution, qui apparaît lorsqu'un opérateur de groupe est sélectionné.
IN GROUP	Membre du groupe sélectionné dans la liste déroulante dans la colonne des paramètres d'exécution, qui apparaît lorsqu'un opérateur de groupe est sélectionné. IN GROUP et IN ALIASES GROUP ne peuvent pas être utilisés en même temps.
IN DYNAMIC ALIASES GROUP	L'opérateur fonctionne sur un groupe du même type que IN DYNAMIC GROUP, mais suppose que les membres de ce groupe sont des alias.
IN ALIASES GROUP	L'opérateur fonctionne sur un groupe du même type que IN GROUP, mais suppose que les membres de ce groupe sont des alias. Notez que les opérateurs IN GROUP/IN ALIASES GROUP s'attendent à ce que le groupe contienne des valeurs ou des alias réels respectivement. Un alias fournit un synonyme qui remplace une valeur mémorisée d'un type d'attribut spécifique. Il est couramment utilisé pour afficher un nom explicite ou convivial pour une valeur de données. Par exemple, Financial Server peut être défini comme un alias pour l'adresse IP 192.168.2.18.
IS NOT NULL	La valeur d'attribut existe, mais peut être vide ou non imprimable
IS NULL	Attribut vide
IN PERIOD	Pour un horodatage uniquement, se situe dans la période de temps sélectionnée
LIKE	
LIKE GROUP	Correspond à une valeur like qui est spécifiée dans les cases. Une valeur like utilise le signe pourcentage en tant que caractère générique et correspond à tout ou partie de la valeur. Les caractères alphabétiques ne sont pas sensibles à la casse. Par exemple, %tea% correspond à tea, TeA, tEam, steam. Si aucun signe de pourcentage n'est inclus, l'opération de comparaison est une opération d'égalité (=).
NOT IN DYNAMIC GROUP	Non égal à un membre d'un groupe sélectionné dans la liste déroulante dans la colonne des paramètres d'exécution, qui apparaît lorsqu'un opérateur de groupe est sélectionné.
NOT IN DYNAMIC ALIASES GROUP	L'opérateur fonctionne sur un groupe du même type que NOT IN DYNAMIC GROUP, mais suppose que les membres de ce groupe sont des alias.
NOT IN GROUP	Non égal à un membre du groupe sélectionné dans la liste déroulante dans la colonne des paramètres d'exécution, qui apparaît lorsqu'un opérateur de groupe est sélectionné.
NOT IN ALIASES GROUP	L'opérateur fonctionne sur un groupe du même type que NOT IN GROUP, mais suppose que les membres de ce groupe sont des alias.
NOT IN PERIOD	Pour un horodatage uniquement, ne se situe pas dans la période de temps sélectionnée
NOT LIKE	Non similaire à la valeur spécifiée (voir la description de LIKE)
NOT LIKE GROUP	Non similaire à la valeur spécifiée dans LIKE GROUP
NOT REGEXP	Ne correspond pas à l'expression régulière spécifiée
REGEXP	Correspond à l'expression régulière spécifiée. Pour des informations détaillées sur l'utilisation d'expressions régulières, voir Expressions régulières.

Remarque : Quatre mots spéciaux ne sont pas autorisés comme nom d'un paramètre : user, group, role, page.

Une erreur se produit en cas de tentative de sauvegarde d'une requête avec l'un de ces mots dans le paramètre. Cela s'applique à deux types de conditions :

- Lors de la création d'une condition de requête avec un opérateur tel que =, <, LIKE, etc., et de la sélection du Paramètre. Ce champ n'autorise pas les mots spéciaux.
- Lors de la création d'une condition de requête avec un opérateur de type DYNAMIC GROUP (IN, NOT IN, IN ALIAS, etc.), ce champ n'autorise pas les mots spéciaux.

5. Pour un opérateur de groupe, sélectionnez un groupe dans la liste.

   Pour la plupart des autres opérateurs, vous devez fournir une valeur pour la condition ou indiquer qu'une valeur de paramètre d'exécution (ne contenant pas de points d'exclamation) est fournie ultérieurement (lorsque la requête est exécutée). Dans ce cas, une liste déroulante avec trois options apparaît. Effectuez l'une des opérations suivantes :

   - Sélectionnez Valeur et entrez une valeur exacte dans la zone.
   - Sélectionnez Paramètre et entrez un nom pour le paramètre d'exécution (le nom ne doit pas contenir d'espaces).
   - Sélectionnez Attribut et sélectionnez un autre attribut correspondant à celui sélectionné (par exemple, cette opération peut être utilisée pour tester le trafic local en faisant correspondre les adresses IP du client et du serveur).

   Utilisez l'icône Ajouter une expression associée aux sélections Valeur, Paramètre et Attribut pour entrer des conditions de requête incluant des chaînes définies par l'utilisateur et des expressions mathématiques.

   Utilisez cette fonction pour ajouter une condition basée non pas sur l'intégralité du contenu de l'attribut tel quel, mais sur une partie de l'attribut, sur une fonction de l'attribut ou sur une fonction combinant plusieurs attributs.

   Exemple : `INSTR(:attribute, '150.1') = 5`, qui renvoie toutes les instances de l'attribut IP client contenant les 5 caractères répertoriés. Entrez le caractère 5 dans la zone de saisie en regard de l'icône Ajouter une expression. Entrez l'expression `INSTR(:attribute, '150.1')` dans la fenêtre distincte Générer une expression. Testez la validité de l'expression dans cette même fenêtre Générer une expression. Autre exemple : `LENGTH(:attribute) >= 40` renvoie la longueur de toute instruction SQL supérieure à 40 caractères. L'expression peut ou non contenir des références à l'attribut même, ainsi que des références à d'autres attributs.

6. Lorsque vous avez terminé d'ajouter toutes les conditions, n'oubliez pas de sauvegarder la définition.

Générer une expression dans une condition de requête

Utilisez l'icône Ajouter une expression associée aux sélections Valeur, Paramètre et Attribut pour entrer des conditions de requête incluant des chaînes définies par l'utilisateur et des expressions mathématiques.

Utilisez cette fonction pour ajouter une condition basée non pas sur l'intégralité du contenu de l'attribut tel quel, mais sur une partie de l'attribut, sur une fonction de l'attribut ou sur une fonction combinant plusieurs attributs.

Par exemple :

Renvoyer l'emplacement de la chaîne `150.1`, de la valeur 192.150.1.x., où la chaîne `150.1` se trouve en position de cinquième caractère dans la valeur. La chaîne `150.1` représente toutes les instances de l'IP du client correspondant aux 5 caractères répertoriés.

Lorsque la fonction est exécutée dans le champ Expression, elle renvoie une valeur, et cette valeur doit figurer dans la zone de saisie.

Utilisez la fonction `INSTR(:attribute, '150.1')` avec la valeur "5" dans la zone de saisie en regard de l'icône Ajouter une expression pour renvoyer les enregistrements contenant `150.1` dans le cinquième emplacement.

Si la fonction est `INSTR(:attribute, '150.1') = 5`, elle devient une phrase booléenne, et les seules valeurs dans la zone de saisie sont 0 ou 1.

Entrez l'expression `INSTR(:attribute, '150.1')` dans la fenêtre distincte Générer une expression.

Testez la validité de l'expression dans cette même fenêtre Générer une expression.

Autre exemple : `LENGTH(:attribute) >= 40` renvoie la longueur de toute instruction SQL supérieure à 40 caractères. L'expression peut ou non contenir des références à l'attribut même, ainsi que des références à d'autres attributs.

Rubrique parent : Requêtes

Domaines, entités et attributs

Un domaine fournit une vue des données que contient Guardium.

Chaque domaine contient un ensemble de données liées à un objectif ou une fonction spécifique (accès aux données, exceptions, violations de politique, etc.). Pour une description de tous les domaines, voir la section Domaines.

Chaque domaine contient une ou plusieurs entités. Une entité est un ensemble d'attributs liés, et un attribut est fondamentalement une valeur de champ. Pour une description de l'ensemble des entités et des attributs, voir Entités et Attributs.

Une requête Guardium renvoie les données d'un seul domaine. Lorsque la requête est définie, une entité dans ce domaine est désignée comme l'entité principale de la requête. Chaque ligne de données renvoyée par une requête contient un nombre d'occurrences de l'entité principale correspondant aux valeurs renvoyées pour les attributs sélectionnés, pour la période demandée. Cela permet de créer des rapports bidimensionnels à partir d'entités qui n'ont pas de relation un à un.

Il existe un générateur de requête distinct pour chaque domaine et l'accès à chaque générateur de requête est contrôlé par des rôles de sécurité. Ainsi, chaque rôle Guardium a généralement accès à un sous-ensemble de domaines, selon la fonction de ce rôle au sein de l'entreprise. Les utilisateurs du rôle d'administrateur Guardium ont généralement accès à tous les domaines de rapport.

Certains domaines ne sont disponibles que lorsque des composants facultatifs (CAS ou Classification, par exemple) sont installés. D'autres domaines rapportent des informations relatives au dispositif Guardium (activité d'archivage, par exemple) et sont disponibles par défaut pour les utilisateurs du rôle administrateur Guardium.

Certains des attributs décrits dans cette annexe sont disponibles pour les utilisateurs disposant du rôle d'administrateur uniquement. Ces attributs sont libellés : Réservé uniquement au rôle d'administrateur.

Pour les utilisateurs qui ne disposent pas du rôle d'administrateur, ces attributs ne sont pas disponibles auprès du générateur de requête.

De même, certains attributs ne sont pas disponibles pour certains protocoles de base de données. Lors de l'utilisation d'un générateur de requête, si vous remarquez qu'une entité ou un attribut décrit dans la documentation n'est pas répertorié dans la sous-fenêtre Entités, cette entité ou cet attribut n'est pas disponible pour le type de base de données sélectionné.

Voir les sujets suivants :

- Domaines
- Entités et attributs
- Génération de requête

- Domaines
  Le tableau suivant décrit les générateurs de requêtes et les domaines associés qui sont fournis avec votre système Guardium. Votre entreprise peut avoir défini des domaines personnalisés supplémentaires.
- Domaines personnalisés
  Les domaines personnalisés permettent l'utilisation de domaines définis par l'utilisateur et peuvent définir toutes les tables de données téléchargées sur le dispositif.
- Entités et attributs
  Cette rubrique contient une description des attributs contenus dans chaque entité.
- Rapports sur les autorisations de base de données
  Vous pouvez utiliser les rapports sur les autorisations de base de données pour vérifier que les utilisateurs ont accès uniquement aux données appropriées. Votre système Guardium comprend des rapports sur les autorisations de base de données prédéfinis pour plusieurs types de bases de données.

Rubrique parent : Rapports

Domaines

Le tableau suivant décrit les générateurs de requêtes et les domaines associés qui sont fournis avec votre système Guardium. Votre entreprise peut avoir défini des domaines personnalisés supplémentaires.

Chaque domaine contient un ensemble de données liées à un objectif ou une fonction spécifique (accès aux données, exceptions, violations de politique, etc.). Pour une description de tous les domaines, voir la section Domaines.

Chaque domaine contient une ou plusieurs entités. Une entité est un ensemble d'attributs liés, et un attribut est fondamentalement une valeur de champ. Pour une description de l'ensemble des entités et des attributs, voir Entités et Attributs.

Une requête Guardium renvoie les données d'un seul domaine. Lorsque la requête est définie, une entité dans ce domaine est désignée comme l'entité principale de la requête. Chaque ligne de données renvoyée par une requête contient un nombre d'occurrences de l'entité principale correspondant aux valeurs renvoyées pour les attributs sélectionnés, pour la période demandée. Cela permet de créer des rapports bidimensionnels à partir d'entités qui n'ont pas de relation un à un.

Il existe un générateur de requête distinct pour chaque domaine et l'accès à chaque générateur de requête est contrôlé par des rôles de sécurité. Ainsi, chaque rôle Guardium a généralement accès à un sous-ensemble de domaines, selon la fonction de ce rôle au sein de l'entreprise. Les utilisateurs du rôle d'administrateur Guardium ont généralement accès à tous les domaines de rapport.

Certains domaines ne sont disponibles que lorsque des composants facultatifs (CAS ou Classification, par exemple) sont installés. D'autres domaines rapportent des informations relatives au dispositif Guardium (activité d'archivage, par exemple) et sont disponibles par défaut pour les utilisateurs du rôle administrateur Guardium.

Certains des attributs décrits dans cette annexe sont disponibles pour les utilisateurs disposant du rôle d'administrateur uniquement. Ces attributs sont libellés : Réservé uniquement au rôle d'administrateur.

Pour les utilisateurs qui ne disposent pas du rôle d'administrateur, ces attributs ne sont pas disponibles auprès du générateur de requête.

De même, certains attributs ne sont pas disponibles pour certains protocoles de base de données. Lors de l'utilisation d'un générateur de requête, si vous remarquez qu'une entité ou un attribut décrit dans la documentation n'est pas répertorié dans la sous-fenêtre Entités, cette entité ou cet attribut n'est pas disponible pour le type de base de données sélectionné.

Voir les sujets suivants :

- Domaines
- Entités et attributs
- Génération de requête

L'accès au générateur de requête pour chaque domaine est contrôlé par des rôles de sécurité, de sorte que chaque rôle d'utilisateur a généralement accès à un ensemble distinct de domaines. Certains domaines ne sont disponibles que lorsque des composants facultatifs (CAS par exemple) sont installés.

Dans le portail d'administration par défaut, tous les générateurs de requête peuvent être ouverts à partir du menu de l'onglet Outils > Génération de rapport. Dans le portail utilisateur par défaut, de nombreux générateurs de requêtes peuvent être ouverts à partir de l'application Génération de rapport personnalisé : Surveillance/Audit > Générer des rapports.

Après une brève description du domaine, la colonne Description répertorie le rôle de sécurité par défaut attribué à chaque domaine et indique comment accéder au domaine à partir du portail d'utilisateur par défaut (si disponible).

Tableau 1. Domaines

Générateur de requête (Domaine)	**Description**
Politique d'accès (Politique d'accès)	Utilisez ce domaine pour suivre toutes les politiques disponibles sur le système. Semblable au domaine Politiques installées utilisé pour suivre toutes les politiques installées sur le système. Rôles : tous. Portail utilisateur : non disponible
Accès (LOGGER INFO)	Toutes les données liées au client/serveur, à la session, au SQL et aux périodes d'accès. Il s'agit des données collectées par les moteurs d'inspection chaque fois qu'une demande est envoyée à un serveur surveillé. Rôles : tous Portail utilisateur : Surveillance/Audit > Générer des rapports > Suivre l'accès aux données
Agrégation/Archive (AGGREGATION/EXPORT/IMPORT)	Activité d'agrégation et d'archivage, y compris la date, l'heure et le statut de chaque opération (archive, envoi, purge, etc.). Rôles : admin Portail utilisateur : non disponible
Alerte (ALERT)	Toutes les alertes générées et envoyées par Guardium. Rôles : tous Portail utilisateur : Surveillance/Audit > Générer des rapports > Suivre les alertes envoyées

Générateur de requête (Domaine)	Description
Application (Données d'application)	Données de connexion, de session et d'application enregistrées pour une application spéciale non Guardium (Siebel et SAP, par exemple). Rôles : admin Portail utilisateur : non disponible
Processus d'audit (AUDIT TRAIL)	Exécution des processus d'audit et répartition des résultats. Rôles : tous Portail utilisateur : Surveillance/Audit > Générer des rapports > Générateur de processus d'audit
Reconnaissance automatique (AUTODETECT DB DISCOVERY)	Activité de reconnaissance automatique de la base de données, y compris tous les processus qui ont été exécutés, ainsi que les hôtes et les ports détectés. Rôles : tous Portail utilisateur : Reconnaître > Reconnaissance de base de données > Générateur de requête de reconnaissance automatique
Changements de CAS (Changements de CAS)	Tous les changements détectés par CAS, y compris toutes les données modifiées enregistrées. Rôles : cas Portail utilisateur : non disponible
Configuration CAS (Configuration CAS)	Configuration d'une instance CAS, décrivant l'utilisation de modèles sur des hôtes spécifiques. Rôles : cas Portail utilisateur : non disponible
CAS Historique de l'hôte (CAS Historique de l'hôte)	Historique des changements CAS appliqués aux hôtes de l'agent CAS. Rôles : cas Portail utilisateur : non disponible
Modèles CAS (Modèles CAS)	Rapports sur le contenu des modèles CAS (qui définissent les éléments à surveiller). Rôles : cas Portail utilisateur : non disponible
Résultats du classificateur (Processus de classification)	Rapports sur les exécutions et les résultats de processus de classement. Rôles : admin Portail utilisateur : non disponible
Commentaires (COMMENT)	Commentaires définis par l'utilisateur pour différents composants Guardium. Rôles : tous Portail utilisateur : Surveillance/Audit > Générer des rapports > Générateur de commentaires
Générateur de domaine personnalisé	Des domaines personnalisés ont été définis pour télécharger des tables et des produits couramment utilisés. Voir Table personnalisée car un domaine personnalisé contient une ou plusieurs tables personnalisées. Si le domaine contient plusieurs tables, vous définissez les relations entre les tables lors de la définition du domaine personnalisé.
Générateur de requête personnalisée	Les domaines définis par l'utilisateur peuvent définir toutes les tables de données téléchargées sur le dispositif Guardium. Rôles : tous Portail utilisateur : Surveillance/Audit > Générer des rapports > Générateur de requête personnalisée
Générateur de table personnalisée	Une table personnalisée contient un ou plusieurs attributs dont vous souhaitez disposer sur le dispositif Guardium. Par exemple, vous pouvez avoir une table de base de données existante reliant les noms d'utilisateurs codés à des noms réels. Dans le trafic réseau, seuls les noms codés sont visibles. En définissant une table personnalisée sur le dispositif Guardium et en téléchargeant des données pour cette table à partir de la table existante, vous pouvez relier les noms codés et les noms réels.
Utilisateurs par défaut de la base de données activés	Analyse sans données d'identification - Processus permettant d'analyser une liste de bases de données et de vérifier si les utilisateurs par défaut sont activés. Les utilisateurs par défaut ainsi que la liste des serveurs à analyser sont fournis en tant que paramètres de l'API. Un groupe par défaut est fourni pour chaque type de base de données avec les utilisateurs et les mots de passe par défaut créés par la base de données sur chaque installation que les clients peuvent ajouter/supprimer dans cette liste. Les groupes sont de type Utilisateur DB/Mot de passe DB et les noms des groupes par défaut sont : Utilisateurs par défaut ORACLE ; Utilisateurs par défaut DB2 ; Utilisateurs par défaut SYBASE ; Utilisateurs par défaut MS SQL SERVER ; Utilisateurs par défaut INFORMIX ; Utilisateurs par défaut MYSQL ; Utilisateurs par défaut TERADATA ; Utilisateurs par défaut IBM® ISERIES ; Utilisateurs par défaut POSTGRESQL ; Utilisateurs par défaut NETEZZA
Instance reconnue (Instances reconnues)	Instances reconnues par GIM Rôles : tous Portail utilisateur : Surveillance/Audit > Générer des rapports > Instance reconnue
Utilisation de la mémoire tampon d'entreprise	Affiche l'agrégat d'utilisation de la mémoire tampon du Sniffer par toutes les unités gérées. Rôles : aucun Portail utilisateur : non disponible
Exceptions (voir la note à la fin du tableau) (LOGGER EXCEPTIONS)	Toutes les exceptions et les données liées aux exceptions. Il s'agit des exceptions SQL envoyées à partir d'un serveur de base de données et collectées par les moteurs d'inspection, ainsi que des exceptions générées par Guardium même. Rôles : tous Portail utilisateur : Surveillance/Audit > Générer des rapports > Suivre les exceptions
Flat Log (Flat Log)	Activité de traitement de Flat Log. Rôles : aucun Portail utilisateur : Surveillance/Audit > Générer des rapports > Générateur Flat Log
Evénements GIM (Evénements GIM)	Guardium Installation Manager Rôles : tous Portail utilisateur : Surveillance/Audit > Générer des rapports > Evénements GIM

Générateur de requête (Domaine)	Description
Groupe (Groupe)	Membres dans les groupes Guardium. Rôles : tous Portail utilisateur : Surveillance/Audit > Générer des rapports > Générateur de groupe
Activité Guardium (USER ACTIVITY AUDIT)	Toutes les modifications effectuées par les utilisateurs Guardium sur une entité Guardium, telles qu'une définition ou une modification de rapport ou de requête. Rôles : admin Portail utilisateur : non disponible
Connexion à Guardium (USER LOGIN)	Tous les informations de connexion et de déconnexion d'utilisateur Guardium. Rôles : admin Portail utilisateur : non disponible
Politique installée (Politique installée)	Fournit la description des paramètres et des règles de la politique installée. Le domaine Politique installée prend en charge plusieurs politiques et plusieurs actions par règle. Rôles : all Portail utilisateur : non disponible
Violations de politique (ACCESS RULES VIOLATIONS)	Toutes les données de violation de politique, pour toutes les violations de la politique détectées par les moteurs d'inspection ou les agents STAP Guardium. Rôles : tous Portail utilisateur : Surveillance/Audit > Générer des rapports > Générateur de violations de politique
Récapitulatif des violations de politique (Violations de règles d'accès)	Toutes les données de violation de politique, pour un récapitulatif de toutes les violations de la politique détectées par les moteurs d'inspection ou les agents STAP Guardium. Rôles : tous Portail utilisateur : Surveillance/Audit > Générer des rapports > Générateur de récapitulatifs de violations de politique
Résultats de relecture	Réexécution du flux de données à partir d'une source de données par une autre source de données différente. Rôles : aucun Portail utilisateur : non disponible
Connexions corrompues (HUNTER)	Processus de serveur de base de données locaux qui ont contourné S-TAP pour se connecter à la base de données via une mémoire partagée, des tubes nommés ou d'autres moyens non standard. S'applique uniquement à l'agent S-TAP Unix, lorsque la méthode de surveillance TEE a été utilisée. Rôles : tous Portail utilisateur : Surveillance/Audit > Générer des rapports > Générateur de connections corrompues
Résultat d'évaluation de la sécurité (Moniteur de Résultats de test d'évaluation)	Enregistre les résultats des processus d'évaluation de la vulnérabilité. Rôles : aucun Portail utilisateur : non disponible
Utilisation de la mémoire tampon du sniffer (Moniteur d'Utilisation de la mémoire tampon du sniffer)	Statistiques du moteur d'inspection. Rôles : aucun Portail utilisateur : non disponible
Utilisateur/Rôle/Application (Application utilisateur de rôle)	Se rapporte aux utilisateurs, aux rôles et aux applications Guardium (pour indiquer qui a accès aux applications Guardium). Rôles : admin Portail utilisateur : non disponible
Tests VA (Tests d'évaluation)	Se rapporte aux tests disponibles pour les évaluations de sécurité. Rôles : admin Portail utilisateur : non disponible
Changement de valeur (Changement de valeur)	Tous les changements suivis par l'application de changement de valeur basée sur le déclencheur. Rôles : admin Portail utilisateur : non disponible

Rubrique parent : Domaines, entités et attributs

Domaines personnalisés

Les domaines personnalisés permettent l'utilisation de domaines définis par l'utilisateur et peuvent définir toutes les tables de données téléchargées sur le dispositif.

L'utilisation de ces domaines d'autorisation personnalisés (privilèges) concerne les rapports d'autorisation détectés si vous êtes connecté en tant qu'utilisateur. Pour voir ces rapports, accédez à l'onglet utilisateur Autorisations sur la base de données.

Un certain nombre de domaines personnalisés ont été prédéfinis.

Accès [personnalisé]

Ce domaine contient les mêmes entités que le domaine d'accès aux données standard. Il est fourni en tant que domaine personnalisé pour permettre la création de domaines supplémentaires définis par l'utilisateur, y compris des informations provenant de ce domaine et des tables personnalisées qui ont été téléchargées par l'utilisateur. [Personnalisé] Le domaine d'accès est destiné à être cloné. Ce domaine est mis à jour sur chaque version, donc il n'est pas conseillé de créer des rapports sur ce domaine. Pour une description des entités incluses dans le domaine Accès, consultez la description du domaine Accès dans la rubrique Domaines.

Informations S-TAP (Central Manager)

Rapport : voir Rapports S-TAP. Sur Central Manager, un rapport supplémentaire, Informations S-TAP, est disponible. Ce rapport surveille les S-TAP de l'ensemble de l'environnement. Téléchargez ces données à l'aide du Générateur de table personnalisée.

Les Informations S-TAP constituent un domaine personnalisé prédéfini qui contient l'entité Informations S-TAP et ne sont pas modifiables.

Lors de la définition d'une requête personnalisée, accédez à la page de chargement et cliquez sur Vérifier/Réparer pour créer la table personnalisée dans la base de données CUSTOM, faute de quoi la requête de sauvegarde ne la valide pas. Cette table se charge automatiquement à partir de toutes les sources distantes. Un utilisateur ne peut sélectionner quelles sources éloignées sont utilisées - il extrait les données de toutes les sources.

Sur la base de cette table personnalisée et du domaine personnalisé, il existe deux rapports :

La vue S-TAP d'entreprise affiche, à partir de Central Manager, des informations sur un agent S-TAP actif sur un collecteur et/ou une unité gérée. S'il existe des doublons pour le même moteur S-TAP, l'un étant actif et l'un inactif, le rapport utilise uniquement le moteur actif.

La vue détaillée S-TAP d'entreprise affiche, à partir de Central Manager, des informations sur tous les agents S-TAP actifs et passifs sur tous les collecteurs et/ou les unités gérées.

Si la vue S-TAP d'entreprise et la vue détaillée S-TAP d'entreprise semblent identiques, c'est parce qu'un seul agent S-TAP sur une unité gérée est affiché. La vue détaillée S-TAP d'entreprise semblerait différente si davantage d'agents S-TAP et d'unités gérées étaient impliqués.

Ces deux rapports peuvent être choisis dans l'onglet Moniteur TAP d'un système autonome, mais ils ne contiennent aucune information.

Domaines d'autorisation de base de données

En plus d'authentifier des utilisateurs et de restreindre des privilèges d'accès aux données basés sur des rôles, y compris pour les utilisateurs de la base de données les plus privilégiés, il est nécessaire d'effectuer périodiquement des examens d'autorisation, le processus de validation et de veiller à ce que les utilisateurs disposent uniquement des privilèges requis pour s'acquitter de leurs tâches. Ce rapport est également connu sous le nom de rapport d'attestation de droits d'utilisateur de base de données.

Utilisez les rapports Guardium prédéfinis d'autorisation (privilège) sur la base de données (par exemple) pour voir qui dispose des privilèges système et qui a accordé ces privilèges à d'autres utilisateurs et à d'autres rôles. Les rapports d'autorisation sur la base de données sont importants pour les auditeurs qui suivent les modifications apportées à l'accès à la base de données et pour garantir l'absence de faille de sécurité liée à des comptes persistants ou des privilèges illégaux.

Les rapports d'autorisation sur la base de données utilisent la fonctionnalité Domaine personnalisé pour créer des liens entre les données externes sur la base de données sélectionnée avec les données internes des rapports d'autorisation prédéfinis. Consultez les Rapports d'autorisation sur la base de données pour plus d'informations sur l'utilisation des rapports prédéfinis d'autorisation sur la base de données. Pour visualiser les rapports d'autorisation, connectez-vous au portail utilisateur et accédez à l'onglet Autorisations de base de données.

Remarque : Les rapports d'autorisation de base de données sont des composants facultatifs activés par la clé de produit. Si ces composants n'ont pas été activés, les choix n'apparaissent pas dans les sélections Générateur de domaine personnalisé/Requête de domaine personnalisé/Générateur de table personnalisée.

Les rapports d'autorisation prédéfinis sont répertoriés comme suit. Ils apparaissent en tant que noms de domaine dans les sélections Générateur de domaine personnalisé/Requête de domaine personnalisé/Générateur de table personnalisée.

- Autorisation sur la base de données Oracle
- Autorisation sur la base de données MYSQL
- Autorisation sur la base de données DB2
- Autorisation sur la base de données SYBASE
- Autorisation sur la base de données Informix
- Autorisation sur la base de données MSSQL 2000
- Autorisation sur la base de données MSSQL 20005/2008
- Autorisation sur la base de données Netezza
- Autorisation sur la base de données Teradata
- Autorisation sur la base de données PostgreSQL

Autorisation sur la base de données Oracle

Les domaines suivants sont fournis pour faciliter le téléchargement et la génération de rapports sur les Autorisations sur la base de données Oracle. Chacun des domaines suivants possède une entité unique (avec le même nom), et il existe un rapport prédéfini pour chaque domaine. Ces domaines sont disponibles dans les sélections Générateur de domaine personnalisé/Requête de domaine personnalisé/Générateur de table personnalisée. Comme pour d'autres entités et rapports prédéfinis, ceux-ci ne peuvent pas être modifiés, mais vous pouvez cloner et personnaliser vos propres versions de ces domaines ou rapports. Pour visualiser les rapports d'autorisation, connectez-vous au portail utilisateur et accédez à l'onglet Autorisations de base de données.

Oracle

- Cptes ORA ALTER SYSTEM - Comptes avec les privilèges ALTER SYSTEM et ALTER SESSION
- Cptes ORA avec BECOME USER - Comptes avec les privilèges BECOME USER
- Tous les privilèges système ORA et option d'administration - Rapport affichant tous les privilèges système et l'option d'administration pour les utilisateurs et les rôles
- Privilège d'accès aux objets et aux colonnes ORA - Privilèges octroyés sur les objets et les colonnes (avec ou sans option d'octroi)
- Accès aux objets ORA par un utilisateur public - Accès aux objets par PUBLIC
- Privilèges sur les objets ORA - Privilèges d'objet par compte de base de données ne figurant pas dans le SYS ni dans un rôle DBA
- Privilège d'exécution ORA par un utilisateur public sur une procédure système - Exécuter un privilège sur les procédures SYS PL/SQL affectées à PUBL
- Rôles ORA octroyés - Rôles octroyés aux utilisateurs et aux rôles
- Privilège système ORA octroyé - Rapport hiérarchique montrant le privilège système octroyé aux utilisateurs, y compris les définitions récursives (c'est-à-dire les privilèges affectés aux rôles, puis ces rôles affectés aux utilisateurs)
- Cptes SYSDBA et SYSOPER ORA - Comptes avec privilèges SYSDBA et SYSOPER

Pour que les autorisations puissent télécharger des données à partir de différentes sources de données, l'exigence générale est que l'ID de connexion utilisé pour accéder à la base de données puisse lire les tables utilisées dans la requête (masquée pour toutes les autorisations).

La liste suivante (contenant l'en-tête de la ligne de commentaire) détaille les privilèges minimaux requis, dans la table de la base de données (ou la vue de la table de la base de données) pour que l'autorisation soit opérationnelle.

/* Le privilège Select sur ces tables/vues est requis */

grant select on sys.dba_tab_privs to sqlguard;

grant select on sys.dba_roles to sqlguard;

grant select on sys.dba_users to sqlguard;

grant select on sys.dba_role_privs to sqlguard;

grant select on sys.dba_sys_privs to sqlguard;

grant select on sys.obj$ to sqlguard;

grant select on sys.user$ to sqlguard;

grant select on sys.objauth$ to sqlguard;

grant select on sys.table_privilege_map to sqlguard;

grant select on sys.dba_objects to sqlguard;

grant select on sys.v_$pwfile_users to sqlguard;

grant select on sys.dba_col_privs to sqlguard;

Autorisation sur la base de données MYSQL

Les domaines suivants sont fournis pour faciliter le téléchargement et la génération de rapports sur les Autorisations sur la base de données MYSQL. Chacun des domaines suivants possède une entité unique (avec le même nom), et il existe un rapport prédéfini pour chaque domaine. Ces domaines sont disponibles dans les sélections Générateur de domaine personnalisé/Requête de domaine personnalisé/Générateur de table personnalisée. Comme pour d'autres entités et rapports prédéfinis, ceux-ci ne peuvent pas être modifiés, mais vous pouvez cloner et personnaliser vos propres versions de ces domaines ou rapports. Pour visualiser les rapports d'autorisation, connectez-vous au portail utilisateur et accédez à l'onglet Autorisations de base de données.

MYSQL : les requêtes se terminant par _40 utilisent la version la plus basique du schéma mysql (pour MySQL 4.0 et au-delà). L'information_schema n'a pas changé depuis qu'il a été introduit dans MySQL 5.0, donc il existe un ensemble de requêtes _50, mais aucune requête _51. Les requêtes _50 sont compatibles avec MySQL 5.0 et 5.1 et pour la version 6.0 lorsqu'elle sera commercialisée, car l'information_schema ne devrait pas changer en version 6.0. Les requêtes se terminant par _502 (MYSQL502) utilisent la nouvelle information_schema, qui contient beaucoup plus d'informations et ressemble à un véritable dictionnaire de données.

- Privilèges sur la base de données MYSQL 40
- Privilèges d'utilisateur MYSQL 40
- Privilèges d'hôte MYSQL 40
- Privilèges sur la table MYSQL 40
- Privilèges sur la base de données MYSQL 500
- Privilèges d'utilisateur MYSQL 500
- Privilèges d'hôte MYSQL 500
- Privilèges sur la table MYSQL 500
- Privilèges sur la base de données MYSQL 502
- Privilèges d'utilisateur MYSQL 502
- Privilèges d'hôte MYSQL 502
- Privilèges sur la table MYSQL 502

Pour que les autorisations puissent télécharger des données à partir de différentes sources de données, l'exigence générale est que l'ID de connexion utilisé pour accéder à la base de données puisse lire les tables utilisées dans la requête (masquée pour toutes les autorisations).

La liste suivante détaille les privilèges minimaux requis, dans la table de la base de données (ou la vue de la table de la base de données) pour que l'autorisation soit opérationnelle.

Remarque : en plus des privilèges requis, l'utilisateur doit se connecter à la base de données MYSQL pour télécharger les données.

Les requêtes d'autorisation pour toutes les versions MySQL via MySQL 5.0.1 utilisent cet ensemble de tables : mysql.db mysql.host mysql.tables_priv mysql.user

A partir de MySQL 5.0.2, et pour toutes les versions ultérieures, les requêtes d'autorisation utilisent ce jeu de tables : information_schema.SCHEMA_PRIVILEGES mysql.host information_schema.TABLE_PRIVILEGES information_schema.USER_PRIVILEGES

Si une source de données possède un type de base de données MYSQL, mais n'a pas de nom de base de données (voir Définitions de source de données, le nom de la base de données sous Emplacement est vide), les données de téléchargement bouclent à travers toutes les bases de données MYSQL auxquelles l'utilisateur a accès.

Autorisation sur la base de données DB2

Les domaines suivants sont fournis pour faciliter le téléchargement et la génération de rapports sur les Autorisations sur la base de données DB2. Chacun des domaines suivants possède une entité unique (avec le même nom), et il existe un rapport prédéfini pour chaque domaine. Ces domaines sont disponibles dans les sélections Générateur de domaine personnalisé/Requête de domaine personnalisé/Générateur de table personnalisée. Comme pour d'autres entités et rapports prédéfinis, ceux-ci ne peuvent pas être modifiés, mais vous pouvez cloner et personnaliser vos propres versions de ces domaines ou rapports. Pour visualiser les rapports d'autorisation, connectez-vous au portail utilisateur et accédez à l'onglet Autorisations de base de données.

- Privilèges de niveau colonne DB2 (SELECT, UPDATE, ETC.)
- Privilèges de niveau base de données DB2 (CONNECT, CREATE, ETC.)
- Privilèges de niveau index DB2 (CONTROL)
- Privilèges de niveau package DB2 (sur les packages de code – BIND, EXECUTE, ETC.)
- Privilèges de niveau table DB2 (SELECT, UPDATE, ETC.) Récapitulatif des privilèges DB2

Pour que les autorisations puissent télécharger des données à partir de différentes sources de données, l'exigence générale est que l'ID de connexion utilisé pour accéder à la base de données puisse lire les tables utilisées dans la requête (masquée pour toutes les autorisations).

La liste suivante (contenant l'en-tête de la ligne de commentaire) détaille les privilèges minimaux requis, dans la table de la base de données (ou la vue de la table de la base de données) pour que l'autorisation soit opérationnelle.

/* Le privilège Select sur ces tables/vues est requis */

GRANT SELECT ON SYSCAT.COLAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.DBAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.INDEXAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.PACKAGEAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.DBAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.TABAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.SCHEMAAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.PASSTHRUAUTH TO SQLGUARD;

Autorisation sur la base de données SYBASE

Les domaines suivants sont fournis pour faciliter le téléchargement et la génération de rapports sur les Autorisations sur la base de données SYBASE. Chacun des domaines suivants possède une entité unique (avec le même nom), et il existe un rapport prédéfini pour chaque domaine. Ces domaines sont disponibles dans les sélections Générateur de domaine personnalisé/Requête de domaine personnalisé/Générateur de table personnalisée. Comme pour d'autres entités et rapports prédéfinis, ceux-ci ne peuvent pas être modifiés, mais vous pouvez cloner et personnaliser vos propres versions de ces domaines ou rapports. Pour visualiser les rapports d'autorisation, connectez-vous au portail utilisateur et accédez à l'onglet Autorisations de base de données.

- Privilège système SYBASE et rôles octroyés à l'utilisateur, y compris l'option d'octroi
- Rôle SYBASE octroyé à l'utilisateur et privilèges système octroyés à l'utilisateur et rôle incluant l'option d'octroi
- Accès aux objets SYBASE par le public
- Privilège d'exécution SYBASE sur les fonctions de procédure, octroyé à un utilisateur public
- Comptes SYBASE disposant de rôles d'administrateur système ou de la sécurité
- Privilège sur les objets et les colonnes SYBASE octroyé avec l'option d'octroi
- Rôle SYBASE octroyé à l'utilisateur

Pour que les autorisations puissent télécharger des données à partir de différentes sources de données, l'exigence générale est que l'ID de connexion utilisé pour accéder à la base de données puisse lire les tables utilisées dans la requête (masquée pour toutes les autorisations).

La liste suivante (contenant l'en-tête de la ligne de commentaire) détaille les privilèges minimaux requis, dans la table de la base de données (ou la vue de la table de la base de données) pour que l'autorisation soit opérationnelle.

/* Le privilège Select sur ces tables/vues est requis */

/* Requis sur la base de données MASTER */

grant select on master.dbo.sysloginroles to sqlguard

grant select on master.dbo.syslogins to sqlguard

grant select on master.dbo.syssrvroles to sqlguard

/*Requis sur toutes les bases de données, y compris MASTER */

grant select on sysprotects to sqlguard

grant select on sysusers to sqlguard

grant select on sysobjects to sqlguard

grant select on sysroles to sqlguard

Si une source de données possède un type de base de données SYBASE, mais n'a pas de nom de base de données (voir Définitions de source de données, le nom de la base de données sous Emplacement est vide), les données de téléchargement bouclent à travers toutes les bases de données SYBASE auxquelles l'utilisateur a accès.

Autorisation sur la base de données Informix

Les domaines suivants sont fournis pour faciliter le téléchargement et la génération de rapports sur les Autorisations sur la base de données Informix. Chacun des domaines suivants possède une entité unique (avec le même nom), et il existe un rapport prédéfini pour chaque domaine. Ces domaines sont disponibles dans les sélections Générateur de domaine personnalisé/Requête de domaine personnalisé/Générateur de table personnalisée. Comme pour d'autres entités et rapports prédéfinis, ceux-ci ne peuvent pas être modifiés, mais vous pouvez cloner et personnaliser vos propres versions de ces domaines ou rapports. Pour visualiser les rapports d'autorisation, connectez-vous au portail utilisateur et accédez à l'onglet Autorisations de base de données.

- Privilèges Informix sur les objets par compte de base de données, à l'exclusion du compte et des rôles système
- Privilèges de niveau de base de données Informix, rôles et langue octroyés à l'utilisateur, y compris l'option d'octroi
- Privilèges de niveau base de données Informix, rôles et langue octroyés à l'utilisateur et au rôle, y compris l'option d'octroi
- Octroi sur les objets Informix accordé à un utilisateur public
- Privilège d'exécution Informix sur procédure et fonction Informix, octroyé au public
- Compte Informix disposant de privilèges d'administrateur de base de données Privilèges Informix sur les objets et les colonnes octroyés avec l'option d'octroi
- Rôle Informix octroyé à un utilisateur et un rôle

Pour que les autorisations puissent télécharger des données à partir de différentes sources de données, l'exigence générale est que l'ID de connexion utilisé pour accéder à la base de données puisse lire les tables utilisées dans la requête (masquée pour toutes les autorisations). La liste suivante (contenant l'en-tête de la ligne de

commentaire) détaille les privilèges minimaux requis, dans la table de la base de données (ou la vue de la table de la base de données) pour que l'autorisation soit opérationnelle.

/* Le privilège Select sur ces tables/vues est requis */

Étant donné que tous les utilisateurs disposent de privilèges suffisants pour les privilèges SELECT du catalogue système, il n'est pas nécessaire d'octroyer un privilège à un utilisateur. Informix ne préconise pas l'octroi de privilèges sur le catalogue système aux utilisateurs. L'octroi devrait être utilisé.Mais dans ce cas, ils ne sont pas obligatoires.

grant select on systables to sqlguard;

grant select on systabauth to sqlguard;

grant select on sysusers to sqlguard;

grant select on sysroleauth to sqlguard;

grant select on syslangauth to sqlguard;

grant select on sysroutinelangs to sqlguard;

grant select on sysprocauth to sqlguard;

grant select on sysprocedures to sqlguard;

grant select on syscolauth to sqlguard;

Si une source de données possède un type de base de données Informix, mais n'a pas de nom de base de données (voir Définitions de source de données, le nom de la base de données sous Emplacement est vide), les données de téléchargement bouclent à travers toutes les bases de données Informix auxquelles l'utilisateur a accès.

Autorisation sur la base de données MSSQL 2000

Les domaines suivants sont fournis pour faciliter le téléchargement et la génération de rapports sur les Autorisations sur la base de données MSSQL 2000. Chacun des domaines suivants possède une entité unique (avec le même nom), et il existe un rapport prédéfini pour chaque domaine. Ces domaines sont disponibles dans les sélections Générateur de domaine personnalisé/Requête de domaine personnalisé/Générateur de table personnalisée. Comme pour d'autres entités et rapports prédéfinis, ceux-ci ne peuvent pas être modifiés, mais vous pouvez cloner et personnaliser vos propres versions de ces domaines ou rapports. Pour visualiser les rapports d'autorisation, connectez-vous au portail utilisateur et accédez à l'onglet **Autorisations de base de données**.

- Privilèges sur les objets MSSQL2000 par compte de base de données, n'incluant pas l'utilisateur système par défaut
- Privilèges de rôle/système MSSQL2000 octroyés à un utilisateur y compris l'option d'octroi
- Rôle MSSQL2000 octroyé à un utilisateur et un rôle Privilèges système octroyés à un utilisateur et un rôle y compris l'option d'octroi
- Accès aux objets MSSQL2000 par un utilisateur public
- Privilèges d'exécution MSSQL2000 sur les procédures et fonctions système, octroyés à PUBLIC
- Comptes de base de données MSSQL2000 avec les rôles db_owner et db_securityadmin
- Compte de serveur MSSQL2000 avec les rôles sysadmin, serveradmin et security admin /* exécution de cette autorisation sur la base de données MASTER uniquement */
- Privilèges sur les objets et les colonnes MSSQL2000 octroyés avec l'option d'octroi
- Rôle MSSQL2000 octroyé à un utilisateur et un rôle

Pour que les autorisations puissent télécharger des données à partir de différentes sources de données, l'exigence générale est que l'ID de connexion utilisé pour accéder à la base de données puisse lire les tables utilisées dans la requête (masquée pour toutes les autorisations).

La liste suivante (contenant l'en-tête de la ligne de commentaire) détaille les privilèges minimaux requis, dans la table de la base de données (ou la vue de la table de la base de données) pour que l'autorisation soit opérationnelle.

/* Le privilège Select sur ces tables/vues est requis */

/* Requis sur la base de données MASTER */

grant select on dbo.syslogins to sqlguard

/*Requis sur toutes les bases de données, y compris MASTER */

grant select on dbo.sysprotects to sqlguard

grant select on dbo.sysusers to sqlguard

grant select on dbo.sysobjects to sqlguard

grant select on dbo.sysmembers to sqlguard

Si une source de données possède un type de base de données MSSQL, mais n'a pas de nom de base de données (voir Définitions de source de données, le nom de la base de données sous Emplacement est vide), les données de téléchargement bouclent à travers toutes les bases de données MSSQL auxquelles l'utilisateur a accès.

Autorisation sur la base de données MSSQL 20005/2008

Les domaines suivants sont fournis pour faciliter le téléchargement et la génération de rapports sur les Autorisations sur la base de données MSSQL 2005 ou MSSQL 2008. Chacun des domaines suivants possède une entité unique (avec le même nom), et il existe un rapport prédéfini pour chaque domaine. Ces domaines sont disponibles dans les sélections Générateur de domaine personnalisé/Requête de domaine personnalisé/Générateur de table personnalisée. Comme pour d'autres entités et rapports prédéfinis, ceux-ci ne peuvent pas être modifiés, mais vous pouvez cloner et personnaliser vos propres versions de ces domaines ou rapports. Pour visualiser les rapports d'autorisation, connectez-vous au portail utilisateur et accédez à l'onglet **Autorisations de base de données**.

Remarque : les domaines d'autorisation pour MSSQL2005 répertoriés couvrent également MSSQL2008.

- Privilèges sur les objets MSSQL2005/8 par compte de base de données, n'incluant pas l'utilisateur système par défaut
- Privilèges de rôle/système MSSQL2005/8 octroyés à un utilisateur
- Privilège de rôle/système MSSQL2005/8 octroyés à un utilisateur et un rôle y compris l'option d'octroi
- Accès aux objets MSSQL2005/8 par PUBLIC
- Privilèges d'exécution MSSQL2005/8 sur les procédures et fonctions système, octroyés à PUBLIC
- Comptes de base de données MSSQL2005/8 avec les rôles db_owner et db_securityadmin
- Compte de serveur MSSQL2005/8 avec les rôles sysadmin, serveradmin et security admin /* exécution uniquement sur la base de données MASTER */
- Privilèges sur les objets et les colonnes MSSQL2005/8 octroyés avec l'option d'octroi
- Rôle MSSQL2005/8 octroyé à un utilisateur et un rôle

Pour que les autorisations puissent télécharger des données à partir de différentes sources de données, l'exigence générale est que l'ID de connexion utilisé pour accéder à la base de données puisse lire les tables utilisées dans la requête (masquée pour toutes les autorisations).

La liste suivante (contenant l'en-tête de la ligne de commentaire) détaille les privilèges minimaux requis, dans la table de la base de données (ou la vue de la table de la base de données) pour que l'autorisation soit opérationnelle.

/* Le privilège Select sur ces tables/vues est requis */

/* Requis sur la base de données MASTER */

grant select on sys.server_principals to sqlguard

/*Requis sur toutes les bases de données, y compris MASTER */

grant select on sys.database_permissions to sqlguard

grant select on sys.database_principals to sqlguard

grant select on sys.all_objects to sqlguard

grant select on sys.database_role_members to sqlguard

grant select on sys.columns to sqlguard

Si une source de données possède un type de base de données MSSQL, mais n'a pas de nom de base de données (voir Définitions de source de données, le nom de la base de données sous Emplacement est vide), les données de téléchargement bouclent à travers toutes les bases de données MSSQL auxquelles l'utilisateur a accès.

Autorisation sur la base de données Netezza

Les domaines suivants sont fournis pour faciliter le téléchargement et la génération de rapports sur les Autorisations sur la base de données Netezza. Chacun des domaines suivants possède une entité unique (avec le même nom), et il existe un rapport prédéfini pour chaque domaine. Ces domaines sont disponibles dans les sélections Générateur de domaine personnalisé/Requête de domaine personnalisé/Générateur de table personnalisée. Comme pour d'autres entités et rapports prédéfinis, ceux-ci ne peuvent pas être modifiés, mais vous pouvez cloner et personnaliser vos propres versions de ces domaines ou rapports. Pour visualiser les rapports d'autorisation, connectez-vous au portail utilisateur et accédez à l'onglet **Autorisations de base de données**.

Remarque : il n'existe pas de traduction de texte d'erreur de base de données pour Netezza. L'erreur apparaît dans la description d'exception. Les utilisateurs peuvent cloner/ajouter un rapport avec la description d'exception pour Netezza au besoin.

- Privilèges sur les objets Netezza par nom d'utilisateur de base de données - Privilèges sur les objets avec ou sans option d'octroi par nom d'utilisateur de base de données à l'exclusion du compte ADMIN.
- Privilèges d'administrateur Netezza par nom d'utilisateur de base de données - Privilèges d'administration avec ou sans option d'octroi par nom d'utilisateur de base de données à l'exclusion du compte ADMIN.
- Groupe/Rôle Netezza octroyé à un utilisateur - Groupe (Rôle) octroyé à l'utilisateur
- Privilèges sur les objets Netezza par groupe - Privilèges sur les objets avec ou sans option d'octroi par GROUP, à l'exclusion du compte PUBLIC.
- Privilèges d'administrateur Netezza par groupe - Privilèges d'administrateur avec ou sans option d'octroi par GROUP, à l'exclusion du compte PUBLIC.
- Privilèges d'administrateur Netezza par nom d'utilisateur de base de données, groupe - Privilèges d'administration avec ou sans option d'octroi par nom d'utilisateur de base de données à l'exclusion du compte ADMIN et le groupe PUBLIC.
- Privilèges sur les objets Netezza octroyés - Les privilèges sur les objets octroyés avec ou sans option d'octroi à PUBLIC.
- Privilèges d'administrateur Netezza octroyés - Les privilèges d'administrateur octroyés avec ou sans option d'octroi à PUBLIC.

- Privilège d'administrateur global Netezza octroyé à des utilisateurs et des groupes - Privilège d'administrateur global octroyé à des utilisateurs et des groupes à l'exclusion du compte ADMIN.
- Privilège d'accès global aux objets Netezza octroyé à des utilisateurs et des groupes - Privilège d'accès global aux objets octroyé à des utilisateurs et des groupes à l'exclusion du compte ADMIN.

Pour que les autorisations puissent télécharger des données à partir de différentes sources de données, l'exigence générale est que l'ID de connexion utilisé pour accéder à la base de données puisse lire les tables utilisées dans la requête (masquée pour toutes les autorisations).

La liste suivante (contenant l'en-tête de la ligne de commentaire) détaille les privilèges minimaux requis, dans la table de la base de données (ou la vue de la table de la base de données) pour que l'autorisation soit opérationnelle.

```
/* Le privilège Select sur ces tables/vues est requis */

/* Ce script doit être exécuté à partir de la base de données système */

GRANT SELECT ON SYSTEM VIEW TO sqlguard;

GRANT LIST ON DATABASE TO sqlguard;

GRANT LIST ON USER TO sqlguard;

GRANT LIST ON GROUP TO sqlguard;

GRANT SELECT ON _V_CONNECTION TO sqlguard;
```

Pour les requêtes d'autorisation Netezza, il est recommandé de se connecter à la base de données SYSTEM, notamment en octroyant le privilège à l'utilisateur qui va exécuter ces rapports. Le privilège d'octroi DOIT être effectif dans la base de données SYSTEM ou le privilège octroyé sera effectif sur une seule base de données. Lorsque le privilège accordé est effectif à partir de la base de données SYSTEM, une fonctionnalité spéciale permet au privilège octroyé d'être transmis à toutes les bases de données.

Autorisations sur la base de données Teradata

Les domaines suivants sont fournis pour faciliter le téléchargement et la génération de rapports sur les Autorisations sur la base de données Teradata. Chacun des domaines suivants possède une entité unique (avec le même nom), et il existe un rapport prédéfini pour chaque domaine. Ces domaines sont disponibles dans les sélections Générateur de domaine personnalisé/Requête de domaine personnalisé/Générateur de table personnalisée. Comme pour d'autres entités et rapports prédéfinis, ceux-ci ne peuvent pas être modifiés, mais vous pouvez cloner et personnaliser vos propres versions de ces domaines ou rapports. Pour visualiser les rapports d'autorisation, connectez-vous au portail utilisateur et accédez à l'onglet **Autorisations de base de données**.

- Privilèges sur les objets Teradata par compte de base de données, n'incluant pas les utilisateurs système par défaut
- Privilèges et rôles système Teradata octroyés aux utilisateurs y compris l'option d'octroi.
- Rôles Teradata octroyés aux utilisateurs et aux rôles y compris l'option d'octroi.
- Rôle Teradata octroyé aux utilisateurs et aux rôles.Privilèges système octroyés aux utilisateurs et aux rôles y compris l'option d'octroi.
- Privilèges sur les objets et systèmes Teradata octroyés à public. Remarque : le rôle ne peut être octroyé au public dans Teradata.
- Privilèges d'exécution Teradata sur des objets de base de données système octroyés à un utilisateur public
- Privilèges d'administrateur système et de sécurité Teradata octroyés à un utilisateur et un rôle.
  Remarque : Le rôle d'administrateur système ou de sécurité n'existe pas dans Teradata. L'utilisateur doit créer ses propres rôles. Les privilèges système suivants ne sont normalement pas accordés à un utilisateur standard : ABORT SESSION, CREATE DATABASE, CREATE PROFILE, CREATE ROLE,CREATE USER, DROP DATABASE, DROP PROFILE, DROP ROLE, DROP USER, MONITOR RESOURCE, MONITOR SESSION, REPLICATION OVERRIDE, SET SESSION RATE, SET RESOURCE RATE.
- Privilèges sur les objets Teradata octroyés avec l'option d'octroi aux utilisateurs. A l'exclusion de DBC et du bénéficiaire = 'All'.

Pour que les autorisations puissent télécharger des données à partir de différentes sources de données, l'exigence générale est que l'ID de connexion utilisé pour accéder à la base de données puisse lire les tables utilisées dans la requête (masquée pour toutes les autorisations).

La liste suivante (contenant l'en-tête de la ligne de commentaire) détaille les privilèges minimaux requis, dans la table de la base de données (ou la vue de la table de la base de données) pour que l'autorisation soit opérationnelle.

```
/* Le privilège Select sur ces tables/vues est requis */

GRANT SELECT ON DBC.AllRights TO sqlguard;

GRANT SELECT ON DBC.Tables TO sqlguard;

GRANT SELECT ON DBC.AllRoleRights TO sqlguard;

GRANT SELECT ON DBC.RoleMembers TO sqlguard;
```

Autorisation sur la base de données PostgreSQL

Les domaines suivants sont fournis pour faciliter le téléchargement et la génération de rapports sur les Autorisations sur la base de données PostgreSQL. Chacun des domaines suivants possède une entité unique (avec le même nom), et il existe un rapport prédéfini pour chaque domaine. Ces domaines sont disponibles dans les sélections Générateur de domaine personnalisé/Requête de domaine personnalisé/Générateur de table personnalisée. Comme pour d'autres entités et rapports prédéfinis, ceux-ci ne peuvent pas être modifiés, mais vous pouvez cloner et personnaliser vos propres versions de ces domaines ou rapports. Pour visualiser les rapports d'autorisation, connectez-vous au portail utilisateur et accédez à l'onglet **Autorisations de base de données**.

Il existe sept domaines/requêtes/rapports personnalisés d'autorisation pour PostgreSQL. Il s'agit des éléments suivants (chacun est répertorié avec le nom du rapport, la description, la note) :

- Privilèges PostgreSQL sur les bases de données octroyés au rôle utilisateur public avec ou sans option GRANT Privilège sur les bases de données octroyé au public, à l'utilisateur et au rôle, avec ou sans option d'octroi. A exécuter sur n'importe quelle base de données, idéalement PostgreSQL.
- Privilège PostgreSQL sur la langue octroyé au rôle utilisateur public avec ou sans option GRANT. Privilège sur la langue octroyé au public, à l'utilisateur et au rôle, avec ou sans option d'octroi. A exécuter pour chaque base de données.
- Privilège PostgreSQL sur le schéma octroyé au rôle utilisateur public avec ou sans option GRANT. Privilège sur le schéma octroyé au public, à l'utilisateur et au rôle, avec ou sans option d'octroi. A exécuter pour chaque base de données.
- Privilège PostgreSQL sur l'espace de table octroyé au rôle utilisateur public avec ou sans option GRANT. Privilège sur l'espace de table octroyé au public, à l'utilisateur et au rôle, avec ou sans option d'octroi. A exécuter sur n'importe quelle base de données, idéalement PostgreSQL.
- Rôle ou utilisateur PostgreSQL octroyé à un utilisateur ou un rôle. Rôle ou utilisateur octroyé à un utilisateur ou un rôle, y compris l'option d'octroi. A exécuter une fois dans une base de données. De préférence PostgreSQL.
- Privilège de superutilisateur PostgreSQL octroyé à un utilisateur ou un rôle. Privilège de superutilisateur octroyé à un utilisateur ou un rôle. A exécuter une fois dans une base de données. De préférence PostgreSQL.
- Privilèges système PostgreSQL octroyés à un utilisateur et un rôle. Privilèges système octroyés à un utilisateur et un rôle. A exécuter une fois dans une base de données. De préférence PostgreSQL.
- Privilèges PostgreSQL sur les séquences et les fonctions de la vue de table octroyés à un utilisateur public. Privilèges sur les tables, vues, séquences et fonctions octroyés à un utilisateur public. A exécuter pour chaque base de données. A exécuter pour chaque base de données.
- Privilèges PostgreSQL sur les séquences et les fonctions de la vue de table octroyés avec l'option GRANT. Privilèges sur les tables, vues, séquences et fonctions octroyés à un utilisateur et un rôle avec l'option d'octroi uniquement. A l'exclusion du compte PostgreSQL.
- Privilèges PostgreSQL sur les séquences et les fonctions de la vue de table octroyés aux rôles. Privilèges sur les tables, vues, séquences et fonctions octroyés aux rôles.A l'exclusion du public. A exécuter pour chaque base de données.
- Privilèges PostgreSQL sur les séquences et les fonctions de la vue de table octroyés à un nom de connexion. Privilèges sur les tables, vues, séquences et fonctions octroyés aux noms de connexion. A l'exclusion de l'utilisateur système postgres. A exécuter pour chaque base de données.

Remarque : à partir de la version 8.3.6, PostgreSQL ne prend pas en charge l'option d'octroi administrateur au public. Uniquement sur les fonctions, à l'exclusion des procédures mémorisées. Aucun support pour l'octroi sur les colonnes, uniquement l'octroi sur la table. Public est un groupe, et non un utilisateur. Public n'apparaît dans pg_roles. Les seuls privilèges qui doivent exécuter toutes ces requêtes sont : GRANT CONNECT ON DATABASE PostgreSQL TO username;

Pour que les autorisations puissent télécharger des données à partir de différentes sources de données, l'exigence générale est que l'ID de connexion utilisé pour accéder à la base de données puisse lire les tables utilisées dans la requête (masquée pour toutes les autorisations).

La liste suivante (contenant l'en-tête de la ligne de commentaire) détaille les privilèges minimaux requis, dans la table de la base de données (ou la vue de la table de la base de données) pour que l'autorisation soit opérationnelle.

/* Le privilège Select sur ces tables/vues est requis */

/*Requis sur la base de données POSTGRES*/

grant connect on database postgres to sqlguard;

/*Requis sur toutes les bases de données, y compris POSTGRES (déjà octroyés par défaut à PUBLIC) * / */

grant select on pg_class to sqlguard;

grant select on pg_namespace to sqlguard;

grant select on pg_roles to sqlguard;

grant select on pg_proc to sqlguard;

grant select on pg_auth_members to sqlguard;

grant select on pg_language to sqlguard;

grant select on pg_tablespace to sqlguard;

grant select on pg_database to sqlguard;

Si une source de données possède un type de base de données PostgreSQL, mais n'a pas de nom de base de données (voir Définitions de source de données, le nom de la base de données sous Emplacement est vide), les données de téléchargement bouclent à travers toutes les bases de données PostgreSQL auxquelles l'utilisateur a accès.

Rubrique parent : Domaines, entités et attributs

Entités et attributs

Cette rubrique contient une description des attributs contenus dans chaque entité.

Pour une présentation des domaines, des entités et des attributs, voir Domaines, entités et attributs. Pour une description de tous les domaines, voir Domaines.

Pour les sources de données z/OS (Db2, jeux de données et IMS), certains attributs sont spécifiques. La signification des attributs existants peut aussi être différente de celle qui est décrite ici. Pour plus d'informations sur les entités et les attributs spécifiques des sources de données z/OS, consultez ce qui suit :

- Entités et attributs des rapports pour Data Sets
- Entités et attributs des rapports pour Db2 for z/OS
- Entités et attributs des rapports pour IMS

Entité Politique d'accès

Décrit toutes les politiques disponibles sur le système. Semblable à l'entité Politiques installées utilisée pour toutes les politiques installées sur le système.

Liste d'entités pour la politique d'accès - Entité Politique d'accès, Entité Politique de règle, Entité Action de règle et Notification d'alerte. Voir Entité Règle pour consulter une liste d'attributs. Voir Entité Action de règle pour consulter une liste d'attributs. Voir Entité Notification d'alerte pour consulter une liste d'attributs.

Tableau 1. Entité Période d'accès

Attribut	Description
ID politique	Identifie de manière unique une politique d'accès
Description de la politique	Décrit la politique d'accès
Trace d'audit sélectif	Indique s'il s'agit d'une politique de trace d'audit sélectif (T/F).
Modèle d'audit	Modèle de test utilisé pour une politique de trace d'audit sélectif.
Horodatage	Horodatage de la création de l'enregistrement.

Entité Période d'accès

Les périodes d'accès sont liées aux sessions. Par défaut, une période d'accès est d'une heure, mais cette durée peut être modifiée par l'administrateur Guardium dans la configuration du moteur d'inspection (correspond à la Granularité de consignation).

Les valeurs de délai d'attente dépendent du nombre de sessions ouvertes par l'unité d'exécution de l'analyseur. Chaque unité d'exécution de l'analyseur comporte les valeurs par défaut suivantes : si le nombre de sessions ouvertes est >0 et <250, le délai d'attente est de 60 minutes. Si le nombre de sessions ouvertes >=250 et <500, le délai d'attente est de 30 minutes. Si le nombre de sessions ouvertes est >=500 et <750, le délai d'attente est de 15 minutes, si le nombre de sessions ouvertes est >=750 et <1200, le délai d'attente est de 5 minutes. Si le nombre de sessions ouvertes est >=1200, le délai d'attente est de 2 minutes.

Tableau 2. Entité Période d'accès

Attribut	Description
ID session	Identifie une session de manière unique.
ID instance	Identifie de manière unique une instance de construction.
ID construction	Identifie de manière unique une construction de commande (par exemple, sélectionnez a à partir de b).
Accès total	Nombre total d'instances de construction pour cette période d'accès.
Date de début de période	Date uniquement à partir de l'attribut de début de période.
Jour de la semaine du début de période	Jour de la semaine uniquement à partir de l'attribut de début de période.
Heure de début de période	Heure uniquement à partir de l'attribut de début de période.
Horodatage	Initialement, la valeur Horodatage est définie la première fois qu'une demande est observée sur une connexion client-serveur pendant une période d'accès. Par défaut, une période d'accès est d'une heure, mais cette durée peut être modifiée par l'administrateur Guardium dans la configuration du moteur d'inspection - consultez le guide d'administration de Guardium. Par la suite, pour chaque demande ultérieure, elle est mise à jour lorsque le système met à jour le temps d'exécution moyen et le nombre de commandes pour cette période.
Fin de la période	Date et heure de la fin de la période d'accès.
Date de fin de période	Date uniquement à partir de l'attribut de fin de période.
Jour de la semaine de fin de période	Jour de la semaine uniquement à partir de l'attribut de fin de période.
Heure de fin de période	Heure uniquement à partir de l'attribut de fin de période.
Utilisateur de l'application	Nom d'utilisateur de l'application.
Temps moyen d'exécution	Temps moyen d'exécution de la commande pendant la période. Relatif uniquement aux instructions SQL. Non applicable à FTP ou au trafic de partage de fichiers Windows.
SQL échoués (2)	Nombre de requêtes SQL échouées. Voir la note à la fin du tableau.
SQL réussis (2)	Nombre de requêtes SQL réussies. Voir la note à la fin du tableau.
ID événement d'application	ID événement d'application si défini à partir de l'API.
Total d'enregistrements affectés (2)	Nombre total d'enregistrements affectés. Voir la note à la fin du tableau.
Moyenne d'enregistrements affectés (2)	Nombre moyen d'enregistrements affectés. Voir la note à la fin du tableau.

Attribut	Description
Total d'enregistrements affectés (Desc) (2)	Si l'attribut Total d'enregistrements affectés est une chaîne de caractères plutôt qu'un nombre, cette valeur apparaît ici (par exemple, Grand ensemble de résultats ou N/A.) Enregistrements affectés - Ensemble de résultats du nombre d'enregistrements qui sont affectés par chaque exécution d'instructions SQL. Remarque : L'option affectée aux enregistrements est une opération de sniffer qui requiert que le sniffer traite des paquets de réponse supplémentaires et reporte la consignation des données impactées, ce qui augmente la taille de la mémoire tampon et peut avoir un effet néfaste sur les performances globales des sniffers. Un impact significatif provient de réponses vraiment volumineuses. Pour éviter une surcharge importante du système associée à cette opération, Guardium utilise un ensemble de seuils par défaut qui permet au sniffer de décider de sauter l'opération de traitement lorsque les seuils sont dépassés. Vous pouvez utiliser les commandes CLI store max_results_set_size, store max_result_set_packet_size et store max_tds_response_packets pour définir les niveaux de granularité. Exemple de valeurs d'ensemble de résultats : • Cas 1, valeur affectée par l'enregistrement : nombre positif - Représente la taille correcte de l'ensemble de résultats. • Cas 2, valeur affectée par l'enregistrement : -2 - Le nombre d'enregistrements a dépassé la limite configurable (réglable via l'interface CLI). • Cas 3, valeur affectée par l'enregistrement : -1 - Affiche les cas non pris en charge de configurations de paquets par Guardium. • Cas 4, valeur affectée par l'enregistrement : -2 - Si l'ensemble de résultats est envoyé en mode de diffusion en continu (streaming). • Cas 5, valeur affectée par l'enregistrement : -2 - Le résultat intermédiaire pendant le comptage des enregistrements pour informer l'utilisateur de la valeur actuelle se termine par un entier positif pour le nombre total d'enregistrements.
Afficher les secondes	Si le nombre d'accès par seconde est suivi, il contient des comptages pour chaque seconde de la période d'accès (habituellement une heure).
Temps moyen d'exécution notifié	Temps moyen d'exécution notifié en millisecondes
Fuseau horaire d'origine	Décalage UTC. Il s'agit de souligner qu'un décalage UTC doit être défini de sorte que l'horodatage provenant de deux collecteurs différents qui se trouvent dans deux fuseaux horaires différents s'agrège correctement. Si ce décalage n'était pas été défini, il existerait une condition où les utilisateurs ne seraient pas vraiment en mesure de déterminer ou de voir une véritable représentation du moment où les événements sont survenus dans le temps. Par exemple, sur un agrégateur qui regroupe les données de différents fuseaux horaires, vous pouvez voir le début de session d'un enregistrement à 21h00 avec le fuseau horaire d'origine UTC-02:00, et un autre enregistrement où le début de session est 21h00 avec le fuseau horaire d'origine UTC-05:00. Cela signifie que ces événements se sont produits à 3 heures d'intervalle, mais à la même heure locale respective (21h00).

Les attributs ID session, ID instance, ID construction et Total des accès sont uniquement disponibles pour les utilisateurs ayant le rôle d'administrateur..

SQL échoués, SQL réussis, ID événement d'application, Total d'enregistrements affectés, Moyenne d'enregistrements affectés et Total d'enregistrements affectés (Desc) sont des attributs qui apparaissent uniquement lorsque l'entité principale de la requête permet ce niveau de détail. Ils ne sont pas disponibles si Client-Server ou Session est l'entité principale.

Entité Règle d'accès

Nom attribué à une règle d'accès lors de sa définition. Il est disponible pour les rapports uniquement à partir de l'entité Violation de règle de politique (décrite plus loin), lorsqu'une violation de règle d'accès est consignée.

Tableau 3. Entité Règle d'accès

Attribut	Description
Description de la règle d'accès	Description issue de la définition de règle de politique d'accès.

Entité Types d'activité

Disponible uniquement à partir du domaine Agrégation/Archive, qui par défaut est disponible pour les utilisateurs disposant uniquement du rôle d'administrateur. L'entité Types d'activité ne peut être consultée qu'à partir de l'entité Journaux d'agrégation/d'importation/d'exportation. Elle identifie un type d'action (Préparer pour l'agrégation, Chiffrer, Envoyer, etc.)..

Tableau 4. Entité Types d'activité

Attribut	Description
Type d'activité	Description d'une activité d'agrégation/importation/exportation.

Entité Journal d'agrégation/archive

Disponible uniquement à partir du domaine Agrégation/Archive, qui par défaut est disponible pour les utilisateurs disposant uniquement du rôle d'administrateur. Une ou plusieurs entités Journal d'agrégation/importation/exportation sont créées pour chaque activité. Par exemple, lorsqu'un système agrégateur importe des données, vous verrez généralement au moins quatre activités :

Préparer pour l'agrégation

Vérifier les importations en double (une par fichier exporté vers cet agrégateur)

Extraire (une par fichier à fusionner)

Fusionner (une par fichier fusionné)

Tableau 5. Entité Journal d'agrégation/archive

Attribut	Description
Horodatage	Mis à jour au début et à la fin de l'activité en cours de consignation (préparer pour archivage, chiffrer, envoyer, etc.).
Statut	Statut de l'activité du journal d'agrégation/importation/exportation.
Nom d'utilisateur	Nom d'utilisateur sous lequel l'activité a été démarré.
Heure de début	Heure de début de l'activité.
Heure de fin	Heure de fin de l'activité.
Début de période	Heure de début de traitement des données. Chaque activité d'archivage ou d'agrégation fonctionne sur une journée complète d'activité.
Fin de la période	Heure de fin pour l'activité en cours de traitement.
Nom de fichier	Nom du fichier utilisé pour l'activité. Les fichiers créés par l'archive et les opérations d'exportation sont nommés comme suit : <daysequence>-<scp_host>-w<run_datestamp>-d<data_date>.dbdump.enc Par exemple : 732423-g1.guardium.com-w20050425.040042-d2005-04-22.dbdump.enc La date des données contenues dans le fichier, au format aaaa-mm-jj est data_date, près de la fin du nom de fichier (juste avant .dbdump.enc). Veillez à ne pas confondre cette date avec la date d'exécution, qui apparaît plus avant dans le nom du fichier et est la date à laquelle les données ont été archivées ou exportées.
Commentaire	Commentaire supplémentaire sur l'activité.
Nom d'hôte Guardium	Nom d'hôte Guardium.
Enregistrements purgés	Si le type d'activité est Purger, nombre d'enregistrements purgés. Sinon, N/A.
Fuseau horaire d'origine	Décalage UTC. Cela concerne en particulier les agrégateurs dont les collecteurs se trouvent dans des fuseaux horaires différents. Les activités qui se sont produites à des heures d'intervalle ne semblent pas arriver au même moment lorsqu'elles sont importées dans l'agrégateur. Par exemple, sur un agrégateur qui regroupe les données de différents fuseaux horaires, vous pouvez voir le début de session d'un enregistrement à 21h00 avec le fuseau horaire d'origine UTC-02:00, et un autre enregistrement où le début de session est 21h00 avec le fuseau horaire d'origine UTC-05:00. Cela signifie que ces événements se sont produits à 3 heures d'intervalle, mais à la même heure locale respective (21h00).

Entité Notification d'alerte

Décrit une notification d'alerte de politique.

Tableau 6. Entité Notification d'alerte

Attribut	Description
ALERT_NOTIFICATION_ID	Identifie la notification d'alerte.
ALERT_ID	Identifie la définition d'alerte.
Type de notification d'alerte	Type d'alerte issu de la définition de règle de politique.
Utilisateur d'alerte	Récepteur de l'alerte.
Destination d'alerte	Type d'alerte (EMAIL, SNMP, SYSLOG, CUSTM).
Horodatage	Enregistrement d'alerte d'horodatage créé.

ALERT_NOTIFICATION_ID et ALERT_ID sont uniquement disponibles pour les utilisateurs disposant du rôle d'administrateur.

Entité Données d'application

Utilisée pour les rapports SAP et Siebel.

Tableau 7. Entité Données d'application

Attribut	Description
ID données d'application	Identificateur unique pour ces données.
Code d'application	Code de type d'application.
ID SQL complet	Identifies the full SQL data.
Type d'application	Type d'application.
Utilisateur	Nom d'utilisateur de l'application.
Type d'opération	Type d'opération.
Date de changement	Date du changement.
Horodatage	Horodatage de cet enregistrement.
Nom de l'élément	Nom de l'élément affecté.

Attribut	Description
Code de transaction	Code de transaction.
ID système	Identificateur unique du système.
Détails d'un enregistrement 1	Varie selon le type d'élément.
Détails d'un enregistrement 2	Varie selon le type d'élément.
Détails d'un enregistrement 3	Varie selon le type d'élément.
Détails d'un enregistrement 4	Varie selon le type d'élément.
VBKey	Valeur VBKey.
Fuseau horaire d'origine	Décalage UTC. Cela concerne en particulier les agrégateurs dont les collecteurs se trouvent dans des fuseaux horaires différents. Les activités qui se sont produites à des heures d'intervalle ne semblent pas arriver au même moment lorsqu'elles sont importées dans l'agrégateur. Par exemple, sur un agrégateur qui regroupe les données de différents fuseaux horaires, vous pouvez voir le début de session d'un enregistrement à 21h00 avec le fuseau horaire d'origine UTC-02:00, et un autre enregistrement où le début de session est 21h00 avec le fuseau horaire d'origine UTC-05:00. Cela signifie que ces événements se sont produits à 3 heures d'intervalle, mais à la même heure locale respective (21h00).

Entité Evénements d'application

Cette entité est créée chaque fois que le système observe un appel de l'API des événements d'application (qui définit ces valeurs d'attribut) ou un appel de procédure mémorisée qui a été identifiée comme une Procédure d'identification personnalisée (mappage des paramètres de la procédure mémorisée sur ces attributs).

Tableau 8. Entité Evénements d'application

Attribut	Description
ID événement d'application	Identificateur unique pour cette entité d'événements d'application.
Nom d'utilisateur de l'événement	Nom d'utilisateur, défini par GuardAppEvent:Start.
Type d'événement	Type d'événement, défini par GuardAppEvent:Start.
Chaîne de valeur d'événement	Valeur de chaîne, définie par GuardAppEvent:Start.
Numéro de valeur d'événement	Valeur numérique, définie par GuardAppEvent:Start.
Date d'événement	Valeur de date et heure, définie par GuardAppEvent:Start. Elle s'affiche au format aaaa-mm-jj hh:mm:ss. Remarque : Une tentative de définir la date d'événement à l'aide d'un format autre que aaaa-mm-jj ne renvoie que des zéros. La portion de temps (hh:mm:ss) est facultative et, si elle est omise, est 00:00:00.
Horodatage	Créé une seule fois, lorsque l'événement est consigné. Ne confondez pas cet attribut avec l'attribut Date d'événement, qui peut être défini à l'aide d'un appel d'API ou à partir d'un paramètre de procédure mémorisée. (Consultez le guide d'administration Guardium pour une description de l'API des événements d'application et des procédures d'identification personnalisées.)
Type de publication d'événement	Type d'événement, défini par GuardAppEvent: Released.
Nom d'utilisateur de publication d'événement	Nom d'utilisateur, défini par GuardAppEvent: Released.
Chaîne de valeur de publication d'événement	Valeur de chaîne, définie par GuardAppEvent: Released.
Numéro de valeur de publication d'événement	Valeur numérique, définie par GuardAppEvent: Released.
Date de publication d'événement	Valeur de date et heure, définie par GuardAppEvent:Released. Elle s'affiche au format aaaa-mm-jj hh:mm:ss.
Fuseau horaire d'origine	Décalage UTC. Cela concerne en particulier les agrégateurs dont les collecteurs se trouvent dans des fuseaux horaires différents. Les activités qui se sont produites à des heures d'intervalle ne semblent pas arriver au même moment lorsqu'elles sont importées dans l'agrégateur. Par exemple, sur un agrégateur qui regroupe les données de différents fuseaux horaires, vous pouvez voir le début de session d'un enregistrement à 21h00 avec le fuseau horaire d'origine UTC-02:00, et un autre enregistrement où le début de session est 21h00 avec le fuseau horaire d'origine UTC-05:00. Cela signifie que ces événements se sont produits à 3 heures d'intervalle, mais à la même heure locale respective (21h00).

ID événement d'application est uniquement disponible pour les utilisateurs disposant du rôle d'administrateur.

Entité Nom d'utilisateur de l'application

Cette entité affiche le nom d'utilisateur à partir de l'événement d'application si cet événement existe. Sinon, le nom d'utilisateur s'affiche à partir de l'instance de construction.

Tableau 9. Entité Nom d'utilisateur de l'application

Attribut	Description
Nom d'utilisateur de l'application	Identificateur unique pour l'entité Nom d'utilisateur de l'application.

Entité Journal d'évaluation

Cette entité est créée chaque fois qu'une évaluation est exécutée.

Tableau 10. Entité Journal d'évaluation

Attribut	Description
ID journal d'évaluation	Identifie une évaluation de manière unique.
Horodatage	Horodatage de l'évaluation.
Date d'horodatage	Partie date de l'horodatage.
Heure d'horodatage	Partie heure de l'horodatage.
Type du journal d'évaluation	Requête prédéfinie ou test personnalisé.
Gravité du journal d'évaluation	Gravité du test d'évaluation : Critique, Majeure, Mineure, Avertissement, Information. Liste ordonnée des niveaux de gravité. Gravité du test d'évaluation : Critique, Majeure, Mineure, Avertissement, Information. La gravité la plus importante est en tête de liste. La gravité la plus faible est en fin de liste.
ID1 résultat d'évaluation	Identifie l'ensemble des résultats d'évaluation.
Message	Message retourné par l'évaluation.
Détails	Détails de cette évaluation.

L'ID journal d'évaluation est uniquement disponible pour les utilisateurs disposant du rôle d'administrateur.

Entité Source de données de résultat d'évaluation

Cette entité identifie une source de données accessible par le test d'évaluation.

Tableau 11. Entité Source de données de résultat d'évaluation

Attribut	Description
ID source de données de résultat d'évaluation	Identifie un ensemble de résultats d'une source de données.
ID résultat d'évaluation	Identifie le résultat.
Type de base de données	Type de base de données : Oracle, MS-SQL, DB2, Sybase, Informix, etc.
Nom de base de données	Nom de base de données.
Niveau de version	Niveau de version de la base de données.
Niveau de correctif	Niveau de correctif de la base de données.
Info version complète	Informations sur la version complète de la source de données
Nom de la source de données	Nom de la source de données.
Description	Description de la source de données.
Hôte	Nom d'hôte de la source de données.
Port	Numéro de port sur l'hôte.
Nom de service	Nom de service de la source de données.
Nom d'utilisateur	Nom d'utilisateur utilisé pour accéder à la source de données.

ID source de données de résultat d'évaluation et ID résultat d'évaluation sont uniquement disponibles pour les utilisateurs disposant du rôle d'administrateur.

Entité En-tête de résultat d'évaluation

Cette entité est créée pour chaque tâche dans l'ensemble de résultats d'évaluation.

Tableau 12. Entité En-tête de résultat d'évaluation

Attribut	Description
ID résultat d'évaluation	Identifie l'ensemble des résultats d'évaluation.
ID évaluation	Identifie l'évaluation.
ID tâche	Identifie la tâche dans l'évaluation.
Indicateur de modification de paramètres	Indique si des paramètres ont été modifiés depuis la dernière exécution.
Date d'exécution	Date à laquelle l'évaluation a été exécutée.
Reçus par tous	Indique si ces résultats ont été reçus par tous les destinataires de la liste de distribution.
Score global	Score global de l'évaluation.
Du	Date de début de l'évaluation.
Au	Date de fin de l'évaluation.
Description de l'évaluation	Nom de l'évaluation issu de la définition.
Filtrer les adresses IP client	Clients sélectionnés : adresse IP exacte, adresse avec des caractères génériques (*) ou vide pour sélectionner tous.

Attribut	Description
Filtrer les adresses IP serveur	Serveurs sélectionnés : adresse IP exacte, adresse avec des caractères génériques (*) ou vide pour sélectionner tous.
Recommandation	Recommandation retournée pour la tâche.

ID résultat d'évaluation, ID évaluation et ID tâche sont uniquement disponibles pour les utilisateurs disposant du rôle d'administrateur.

Entité Tests d'évaluation

Cette entité contient des entrées pour les tests disponibles.

Tableau 13. Entité Tests d'évaluation

Attribut	Description
Description du test	Description textuelle du test
Type de test	Type de test d'évaluation (Observé, Prédéfini, Personnalisé, Basé sur une requête, CVE)
Type de source de données	Type de source de données (DB2, Informix, MYSQL, ORACLE, SYBASE, etc.)
Seuil	Seuil défini par l'utilisateur pour remplacer la valeur définie lors de la création du test
Valeur de seuil par défaut	Seuil par défaut qui définit les critères de réussite/échec
Gravité	Gravité de l'évaluation (Critique, Majeure, Mineure, Attention, Info)
Catégorie	Catégorie d'évaluation (Privilège, Authentification, Configuration, Version, Autre)
Horodatage	Le test d'horodatage a été créé

Entité Processus d'audit

Cette entité contient des paramètres de définition de base pour un processus d'audit.

Tableau 14. Entité Processus d'audit

Attribut	Description
Description du processus	Description issue de la définition du processus d'audit.
Actif	Indique si le processus est actif (pouvant être planifié).
Nombre de jours de conservation des résultats	Le nombre de jours durant lesquels les résultats sont conservés par le système.
Quantité de résultats conservés	Nombre d'ensembles de résultats qui doivent être conservés par le système.

Entité Commentaires de processus d'audit

Cette entité possède des commentaires liés à une définition de processus d'audit. Les commentaires liés aux résultats du processus d'audit sont contenus dans l'entité Commentaires des résultats du processus d'audit.

Tableau 15. Entité Commentaires de processus d'audit

Attribut	Description
Commentaire du processus d'audit	Texte du commentaire.
Auteur du commentaire du processus d'audit	Auteur du commentaire.
Horodatage du commentaire du processus d'audit	Horodatage du commentaire.

Entité Tâche d'audit

Cette entité décrit une tâche d'audit unique (dans le cadre d'un processus d'audit).

Tableau 16. Entité Tâche d'audit

Attribut	Description
Type de tâche	Une valeur numérique indique si la tâche est un rapport, une évaluation de sécurité, une trace d'audit d'entité, un jeu de confidentialité ou un processus de classification. Des alias sont définis pour ces types, de sorte que les rapports comportant des alias sont plus simples à lire.
Description de la tâche	Nom de la tâche issue de la définition de la tâche.

Entité Résultat de processus d'audit

Cette entité contient la date d'exécution d'un ensemble de résultats de processus d'audit.

Tableau 17. Entité Résultat de processus d'audit

Attribut	Description

Attribut	Description
Date d'exécution	Date à laquelle le processus d'audit a été exécuté.

Entité Commentaires de résultats de processus d'audit

Cette entité possède des commentaires liés aux résultats de processus d'audit. Les commentaires liés à une définition de processus d'audit sont contenus dans l'entité Commentaires du processus d'audit.

Tableau 18. Entité Commentaires de résultats de processus d'audit

Attribut	Description
Commentaire du processus d'audit	Texte du commentaire.
Auteur du commentaire du processus d'audit	Auteur du commentaire.
Horodatage du commentaire du processus d'audit	Horodatage du commentaire.

Entité Analyse de reconnaissance automatique

Cette entité identifie à quel moment une analyse est exécutée.

Tableau 19. Entité Analyse de reconnaissance automatique

Attribut	Description
Horodatage de l'analyse	Date/heure d'exécution de l'analyse.
Fuseau horaire d'origine	Décalage UTC. Cela concerne en particulier les agrégateurs dont les collecteurs se trouvent dans des fuseaux horaires différents. Les activités qui se sont produites à des heures d'intervalle ne semblent pas arriver au même moment lorsqu'elles sont importées dans l'agrégateur. Par exemple, sur un agrégateur qui regroupe les données de différents fuseaux horaires, vous pouvez voir le début de session d'un enregistrement à 21h00 avec le fuseau horaire d'origine UTC-02:00, et un autre enregistrement où le début de session est 21h00 avec le fuseau horaire d'origine UTC-05:00. Cela signifie que ces événements se sont produits à 3 heures d'intervalle, mais à la même heure locale respective (21h00).

Entité Colonnes modifiées

Cette entité décrit une colonne modifiée.

Tableau 20. Entité Colonnes modifiées

Attribut	Description
Nom de la colonne changée	Nom de la colonne modifiée dans la base de données.
Ancienne valeur	Valeur avant le changement.
Nouvelle valeur	Valeur après le changement.
Fuseau horaire d'origine	Décalage UTC. Cela concerne en particulier les agrégateurs dont les collecteurs se trouvent dans des fuseaux horaires différents. Les activités qui se sont produites à des heures d'intervalle ne semblent pas arriver au même moment lorsqu'elles sont importées dans l'agrégateur. Par exemple, sur un agrégateur qui regroupe les données de différents fuseaux horaires, vous pouvez voir le début de session d'un enregistrement à 21h00 avec le fuseau horaire d'origine UTC-02:00, et un autre enregistrement où le début de session est 21h00 avec le fuseau horaire d'origine UTC-05:00. Cela signifie que ces événements se sont produits à 3 heures d'intervalle, mais à la même heure locale respective (21h00).

Entité Valeurs de données modifiées

Cette entité est utilisée avec la solution de réplication IBM InfoSphere Change Data Capture (InfoSphere CDC) qui permet la réplication vers et à partir des bases de données prises en charge. La maintenance des bases de données répliquées peut être utilisée pour réduire la surcharge de traitement et le trafic réseau.

Les clients IBM Guardium avec surveillance des activités de base de données ont accès à InfoSphere CDC.

Cette fonctionnalité Guardium utilise l'exit utilisateur Java CDC pour envoyer des informations de changement de valeur au collecteur Guardium.

Les exits utilisateur pour InfoSphere CDC permettent à l'utilisateur de définir un ensemble d'actions qu'InfoSphere CDC peut exécuter avant ou après un événement de base de données sur une table spécifiée.

Tableau 21. Entité Valeurs de données modifiées

Attribut	Description
ID SQL complet	Identificateur unique du SQL complet.
Nom de la table	Nom de la table de base de données
Nom de la colonne	Nom de la colonne de base de données
Ancienne valeur	Valeur avant le changement.
Nouvelle valeur	Valeur après le changement.

Attribut	Description
Horodatage	Date/heure auxquelles l'enregistrement a été créé.

Deux fichiers qui doivent être installés sur le serveur de base de données sont destinés à l'agent Guardium qui s'interface avec l'application IBM InfoSphere Change Data Capture (InfoSphere CDC). Ils se trouvent dans le répertoire sources/apps/GuardCDC/lib/ de la génération. Ces fichiers sont : protobuf-java-2.4.1.jar; et GuardCdc.jar

Instructions d'installation

Prérequis - l'application InfoSphere Change Data Capture (InfoSphere CDC) doit déjà être installée sur le serveur de base de données.

Étapes d'installation de l'agent Guardium sur le serveur de base de données :

1. Copiez ces deux fichiers dans le répertoire RepEngine/lib/ du répertoire cdchome. Par exemple, le chemin complet serait /cdchome/cdc6.5.2/RepEngine/lib/
2. Décompressez chaque fichier
3. Editez le fichier guard_cdc_user_exit_config.mxl pour ajouter le nom Guardium_Host. Un exemple de l'emplacement de ce fichier est /cdchome/cdc6.5.2/RepEngine/lib/com/guardium/cdc/userexit/
4. Configurez InfoSphere CDC pour écrire sur GuardiumAgent. Il existe plusieurs étapes pour définir et configurer l'application CDC. Ces étapes peuvent être obtenues auprès de l'équipe de développement/support d'InfoSphere CDC chez IBM.

Entité Résultats du processus de classification

Cette entité est créée pour chaque règle de processus de classification déclenchée.

Tableau 22. Entité Résultats du processus de classification

Attribut	Description
Catalogue	Emplacement du catalogue de l'ensemble de résultats.
Schéma	Nom du schéma, le cas échéant.
Nom de la table	Nom de la table issu de la définition de règle.
Nom de la colonne	Nom de la colonne issu de la définition de règle.
Description de la règle	Description de la règle de politique du classificateur.
Commentaires	Tous les commentaires ajoutés à cette définition de règle.
Nom de la classification	Classification de la règle.
Catégorie	Catégorie de la règle.
Description de la source de données	Source de données de la règle.

Entité Exécution du processus de classification

Cette entité décrit l'exécution du travail d'un processus de classification.

Tableau 23. Entité Exécution du processus de classification

Attribut	Description
Description du processus	Issue de la définition de processus.
Statut	Statut du travail.
Date/heure de la file d'attente	Horodatage de l'envoi du travail à la file d'attente du classificateur/d'évaluation.
Date/heure de début	Horodatage au début du travail.
Date/heure de fin	Horodatage à la fin du travail.
Sources de données	Identifie la liste des sources de données du travail.

Entité Client-serveur

Cette entité décrit une connexion client-serveur spécifique. Une instance est créée chaque fois qu'un ensemble unique d'attributs (à l'exclusion de l'horodatage) est détecté.

Tableau 24. Entité Client-serveur

Attribut	Description
ID accès	Identificateur unique pour cette connexion client/serveur.
Horodatage	Étant donné que tous les attributs de cette entité contiennent des informations statiques, cet horodatage est créé une seule fois, lorsque Guardium observe une demande sur la connexion client-serveur définie pour la première fois.
Date d'horodatage	Date uniquement issue de l'horodatage.
Heure d'horodatage	Heure uniquement issue de l'horodatage.
Jour de la semaine de l'horodatage	Jour de la semaine uniquement issu de l'horodatage.
Année de l'horodatage	Année uniquement issue de l'horodatage.
Type de serveur	DB2, Oracle, Sybase, etc.
Adresse IP client	Adresse IP client.

Attribut	Description
Adresse IP du serveur	Adresse IP du serveur.
Protocole réseau	Protocole réseau utilisé (par ex., TCP, UDP, etc. Notez que pour K-TAP sur Oracle, il peut s'afficher en tant qu'IPC ou BEQ)
Protocole de base de données	Protocole spécifique du serveur de base de données.
Version du protocole de la base de données	Version de protocole pour le protocole de base de données.
Nom d'utilisateur de la base de données	Nom d'utilisateur de la base de données. Le nom d'utilisateur de la base de données est celui de la personne qui s'est connectée à la base de données, localement ou à distance.
Programme source	Programme source de l'interaction.
Adresse MAC du client	Adresse matérielle du client.
Nom d'hôte du client	Nom d'hôte du client.
Nom de service	Nom du service de l'interaction. Dans certains cas (les connexions à la mémoire partagée AIX, par exemple), le nom du service est un alias qui est utilisé jusqu'à ce que le service réel soit connecté. Dans ce cas, une fois que le service réel est connecté, une nouvelle session est démarrée - de sorte que ce qui apparaît à l'utilisateur comme une session unique est consigné sous la forme de deux sessions. Pour Teradata, le nom du service contient la valeur de l'ID hôte logique de la session.
Système d'exploitation du serveur	Système d'exploitation du serveur. Pour Informix, le système d'exploitation peut apparaître comme suit : IEEEM indiquant Unix ou JDBCIEEEI indiquant WindowsDEC indiquant DEC Alpha Pour Teradata, dans la mesure où il n'existe pas d'informations directes sur le système d'exploitation du client/serveur, le type de format de données est utilisé, indiquant comment les données entières sont stockées pendant la session de base de données. Ceci est étroitement lié à la plateforme utilisée et peut apparaître comme suit : IBM® MAINFRAME // format de données mainframe IBM HONEYWELL MAINFRAME // format de données mainframe Honeywell AT&T 3B2 // format de données AT&T 3B2. INTEL 8086 // format de données Intel 8086 (IBM PC ou compatible) VAX // format de données VAX AMDAHL // format de données Amdahl
Système d'exploitation du client	Système d'exploitation du client. Pour Teradata, dans la mesure où il n'existe pas d'informations directes sur le système d'exploitation du client/serveur, le type de format de données est utilisé, indiquant comment les données entières sont stockées pendant la session de base de données. Ceci est étroitement lié à la plateforme utilisée et peut apparaître comme suit : IBM MAINFRAME // format de données mainframe IBM HONEYWELL MAINFRAME // format de données mainframe Honeywell AT&T 3B2 // format de données AT&T 3B2. INTEL 8086 // format de données Intel 8086 (IBM PC ou compatible) VAX // format de données VAX AMDAHL // format de données Amdahl
Utilisateur système d'exploitation	Compte utilisateur du système d'exploitation pour l'interaction.
Nom d'hôte de serveur	Nom d'hôte du serveur.
Description du serveur	Description du serveur (le cas échéant).
IP client/Utilisateur BD	Valeur d'attribut couplée comprenant l'adresse IP du client et le nom d'utilisateur de la base de données.
Adresse IP client analysée	S'applique uniquement au trafic chiffré. Lorsque cette valeur est définie, l'adresse IP du client est définie sur des zéros. L'adresse IP client analysée possède une mappe pour la source CEF. Si la requête utilisée pour le CEF NE contient PAS l'adresse IP client mais contient l'adresse IP client analysée, l'adresse IP client analysée sera utilisée pour la source. Si les deux sont incluses dans la requête, l'adresse IP client est prioritaire.
IP serveur/Utilisateur BD	Valeur d'attribut couplée comprenant l'adresse IP du serveur et le nom d'utilisateur de la base de données.
Client-serveur par session	Client-serveur par session est également une entité principale. Accédez à cette entité secondaire en cliquant sur l'entité client-serveur principale.

ID accès est uniquement disponible pour les utilisateurs disposant du rôle d'administrateur.

Remarque : Pour le Suivi des accès uniquement, le nom de l'entité Client-serveur apparaît dans le menu déroulant en tant que deux entités possibles : Client-serveur et Client-serveur par session.

L'attribut Client-serveur par session reçoit un comptage de l'attribut Client-serveur et les conditions de date de l'attribut Session.

L'attribut Client-serveur reçoit un comptage de l'attribut Client-serveur et les conditions de date également de l'attribut Client/Server.

Si l'utilisateur choisit Client-serveur, la requête est remplie avec ATTRIBUTE_ID = 1. Si l'utilisateur choisit Client-serveur par session, la requête est remplie avec MAIN_ATTRIBUTE_ID = 0.

Entité Surveillance de l'utilisation de la mémoire tampon CM

Dans Central Manager, affiche l'agrégat de l'entité Utilisation de la mémoire tampon du sniffer qui a été téléchargée.

Tableau 25. Entité Surveillance de l'utilisation de la mémoire tampon CM

Attribut	Description
ID utilisation de la mémoire tampon de sniffer	
Horodatage	Date/heure auxquelles l'enregistrement a été créé.
% d'UC utilisé par le sniffer	Pourcentage de l'unité centrale utilisé par le sniffer.
% de mémoire utilisé par le sniffer	Pourcentage de mémoire utilisé par le sniffer.
% d'UC utilisé par MySQL	Pourcentage de l'unité centrale utilisé par MySQL.
% de mémoire utilisé par MySQL	Pourcentage de mémoire utilisé par MySQL.
ID processus	Identificateur de processus du sniffer.
Mémoire	Quantité de mémoire utilisés par le sniffer.
Temps	Temps d'utilisation par le sniffer.
Mémoire tampon disponible	Quantité de mémoire tampon disponible.
Débit de l'analyseur	Débit d'analyse des messages.
File d'attente de l'analyseur	Taille de la file d'attente d'analyse.
Total de l'analyseur	Nombre total de messages analysés.
File d'attente du consignateur	Taille de la file d'attente du consignateur.
Total du consignateur	Nombre total de message consignés.
File d'attente de session	Taille de la file d'attente de la session.
Total de sessions	Nombre total de sessions.
Données du gestionnaire	Données internes du moteur du sniffer.
STR supplémentaire	Données internes du moteur du sniffer.
Connexions du sniffer utilisées	Nombre total de connexions en cours de surveillance depuis le redémarrage du moteur d'inspection.
Paquets supprimés par le sniffer	Paquets supprimés par le sniffer.
Paquets ignorés par le sniffer	Paquets ignorés par le sniffer.
Paquets régulés par le sniffer	Nombre total de connexions qui ont été ignorées en raison de la régulation depuis le redémarrage du moteur d'inspection.
Connexions du sniffer terminées	Nombre total de connexions surveillées et terminées depuis le redémarrage du moteur d'inspection.
Nombre de sessions du consignateur	Nombre de sessions consignées.
Paquets du consignateur ignorés par la règle	Paquets ignorés par une action associée à une règle de politique.
Paquets perdus de l'analyseur	Paquets perdus de l'analyseur.
Bases de données surveillées du consignateur	Liste des types de base de données en cours de surveillance.
Mysql est démarré	Indicateur booléen pour le redémarrage interne de la base de données (1=a été redémarré, 0=non redémarré).
Charge de l'UC système	Utilisation de l'unité centrale système.
Temps d'activité du système	Temps depuis le dernier démarrage.
Utilisation du disque Mysql	Utilisation du disque MySQL.
Utilisation de la mémoire système	Utilisation de la mémoire système.
Utilisation du disque var système	Utilisation du disque var système.
Utilisation du disque racine système	Utilisation du disque racine système.
Reçus sur Eth0	Messages reçus sur ETH 0.
Envoyés sur Eth0	Messages envoyés sur ETH 0.
Indiscriminés reçus	Débit de réception de paquets sur les cartes réseau du sniffer (ports non interface).

Attribut	Description
Descripteurs de fichier ouverts	Descripteurs de fichier ouverts.
Descripteurs de fichier ouverts MySQL	Descripteurs de fichier ouverts de la base de données
Sessions normales	Nombre de sessions normales.
Sessions non ouvertes	Nombre de sessions non ouvertes par le sniffer.
Expiration de sessions	Nombre de sessions arrivées à expiration.
Sessions ignorées	Nombre de sessions ignorées par le sniffer.
Session directement fermée	Nombre de sessions directement fermées.
Session devinée	Nombre de sessions devinées.
Horodatage SqlGuard	Date/heure auxquelles l'enregistrement est inséré dans la table personnalisée
Nom de la source de données	Nom de la source de données utilisée pour télécharger l'enregistrement

Entité Commande

Pour chaque commande, une entité est créée pour chaque nœud et position de parent dans lesquels la commande apparaît dans une construction de commande.

Tableau 26. Entité Commande

Attribut	Description
ID commande	Identifie la commande de manière unique.
ID construction	Identifie de manière unique la construction (par exemple, sélectionnez a à partir de b).
Verbe SQL	Verbe principal de la commande SQL (par exemple, select, insert, delete, etc.).
Profondeur	Profondeur de la commande dans l'arbre d'analyse SQL.
Parent	Identificateur du noeud parent dans l'arbre d'analyse.

ID commande et ID construction sont uniquement disponibles pour les utilisateurs disposant du rôle d'administrateur.

Entité Commentaires

Cette entité décrit un commentaire utilisateur. Elle est disponible uniquement dans le domaine Commentaires, qui est réservé aux administrateurs. Ce domaine inclut uniquement les commentaires partageables, c'est-à-dire tous les commentaires à l'exception de ceux qui s'exécutent localement (voir l'entité Commentaires locaux).

Tableau 27. Entité Commentaires

Attribut	Description
Auteur du commentaire	Utilisateur Guardium qui a créé le commentaire.
Référence du commentaire	Indique l'élément auquel le commentaire est associé - une requête, un résultat de processus d'audit ou un autre commentaire, par exemple.
Contenu du commentaire	Texte complet du commentaire.
Horodatage	Date/heure auxquelles le commentaire a été créé.
Année de l'horodatage	Année uniquement issue de l'horodatage.
Jour de la semaine de l'horodatage	Jour de la semaine uniquement issu de l'horodatage.
Heure d'horodatage	Heure uniquement issue de l'horodatage.
Date d'horodatage	Date uniquement issue de l'horodatage.
Description d'objet	Nom de l'objet à partir duquel le commentaire a été défini. Par exemple, un commentaire défini sur une politique possède la description d'objet ACCESS_RULE_SET.
Associations d'enregistrements	Liste des enregistrements avec lesquels ce commentaire est associé.

Entité Texte d'erreur renvoyé par la base de données

Le texte de chaque message d'erreur de la base de données commune est stocké dans une table dans la base de données interne Guardium. Ce texte est disponible à des fins de génération de rapports uniquement à partir de l'entité d'exception propriétaire pour chaque exception qui est une erreur de base de données. Certains types d'exceptions - déconnexions ou reconnexions S-TAP, par exemple - n'auront aucun texte d'erreur de base de données.

Tableau 28. Entité Texte d'erreur renvoyé par la base de données

Attribut	Description
Texte d'erreur renvoyé par la base de données	Code d'erreur de la base de données suivi d'une brève description textuelle de l'erreur. Le code d'erreur est issu de l'attribut Description d'exception de l'entité Exception. En utilisant le code d'erreur en tant que clé, le texte d'erreur est obtenu à partir d'une table interne sur le dispositif Guardium qui contient les messages d'erreur les plus courants (environ 54 000 d'entre eux). Par exemple : ORA-00942: table or view does not exist
Code d'erreur	Affiche le code d'erreur de la base de données.

Entité Source de données

Cette entité (sous l'entité Suivi de la configuration CAS/Détails d'élément surveillé) identifie une source de données.

Tableau 29. Entité Source de données

Attribut	Description
ID source de données	Identifie un ensemble de résultats d'une source de données.
Type de source de données	Type de source de données - Oracle, MS-SQL, DB2, Sybase, Informix, etc.
Nom de source de données	Nom de la source de données
Description de la source de données	Description de la source de données
Hôte	Nom d'hôte de la source de données
Port	Numéro de port sur l'hôte
Nom de service	Nom de service de la source de données
Nom d'utilisateur	Nom d'utilisateur pour accéder à la source de données.
Nom de base de données	Nom de base de données
Dernier commentaire	Dernier commentaire
Partagé	Oui ou Non
Propriétés de connexion	La zone de la Propriété de connexion ne contient d'informations que si des propriétés de connexion supplémentaires doivent être incluses dans l'URL JDBC pour établir une connexion JDBC avec cette source de données.

Entité Hôte détecté

Cette entité identifie un hôte reconnu.

Tableau 30. Entité Hôte détecté

Attribut	Description
Adresse IP du serveur	Adresse IP de l'hôte reconnu.
Nom d'hôte de serveur	Nom d'hôte de l'hôte reconnu.
Fuseau horaire d'origine	Décalage UTC. Cela concerne en particulier les agrégateurs dont les collecteurs se trouvent dans des fuseaux horaires différents. Les activités qui se sont produites à des heures d'intervalle ne semblent pas arriver au même moment lorsqu'elles sont importées dans l'agrégateur. Par exemple, sur un agrégateur qui regroupe les données de différents fuseaux horaires, vous pouvez voir le début de session d'un enregistrement à 21h00 avec le fuseau horaire d'origine UTC-02:00, et un autre enregistrement où le début de session est 21h00 avec le fuseau horaire d'origine UTC-05:00. Cela signifie que ces événements se sont produits à 3 heures d'intervalle, mais à la même heure locale respective (21h00).

Entité Instances détectées

Cette entité identifie des instances reconnues.

Tableau 31. Entité Instances détectées

Attribut	Description
Horodatage	Valeur d'horodatage créée lorsque Guardium enregistre cette instance de l'entité (chaque instance a un horodatage unique).
Hôte	Nom d'hôte de cette instance
Protocole	Protocole spécifique à cette instance
Port min	Plage de ports, numéro de port minimum pour les moteurs d'inspection
Port max.	Plage de ports, numéro de port maximum pour les moteurs d'inspection
Adresse IP client	Adresse IP/masque du client
Exclure l'adresse IP client	Adresse IP/masque de clients à exclure
Noms de processus	Nom de l'exécutable de la base de données
Tube nommé	Tube nommé utilisé par la base de données
Port de la base de données K-TAP	Port de la base de données pour K-TAP
Rép. installation de la base de données	Répertoire d'installation de la base de données
Nom de processus	Nom du processus
Ajustement de la mémoire partagée DB2	Taille d'en-tête de paquet
Position du client de la mémoire partagée DB2	Décalage de zone d'E-S client

Attribut	Description
Taille de la mémoire partagée DB2	Taille du segment de mémoire partagée DB2
Nom d'instance	Nom de l'instance reconnue
Version Informix	Version Informix

Entité Port détecté

Cette entité identifie un port reconnu.

Tableau 32. Entité Port détecté

Attribut	Description
Port	Numéro du port reconnu.
Analyse tentée	Indique si une analyse pour un service de base de données pris en charge a été tentée sur ce port. T=oui, F=non.
Type de port	Indique le type de port (généralement TCP).
Type de base de données	Si une analyse du port a trouvé un type de base de données pris en charge, indique le type (DB2, Informix, MS SQL Server, etc.)
Horodatage de l'analyse	La date et l'heure auxquelles ce port spécifique a été analysé.
Fuseau horaire d'origine	Décalage UTC. Cela concerne en particulier les agrégateurs dont les collecteurs se trouvent dans des fuseaux horaires différents. Les activités qui se sont produites à des heures d'intervalle ne semblent pas arriver au même moment lorsqu'elles sont importées dans l'agrégateur. Par exemple, sur un agrégateur qui regroupe les données de différents fuseaux horaires, vous pouvez voir le début de session d'un enregistrement à 21h00 avec le fuseau horaire d'origine UTC-02:00, et un autre enregistrement où le début de session est 21h00 avec le fuseau horaire d'origine UTC-05:00. Cela signifie que ces événements se sont produits à 3 heures d'intervalle, mais à la même heure locale respective (21h00).

Entité Exception

Cette entité est créée pour chaque exception rencontrée.

Tableau 33. Entité Exception

Attribut	Description
ID exception	Identifie l'exception de manière unique.
ID type d'exception	Identifie le type d'exception de manière unique.
Horodatage de l'exception	Date et heure de consignation de l'entité Exception.
Date de l'exception	Date uniquement issue de l'horodatage.
Heure de l'exception	Heure uniquement issue de l'horodatage.
Jour de semaine d'exception	Jour de la semaine uniquement issu de l'horodatage.
Année d'exception	Année uniquement issue de l'horodatage.
Adresse source	Adresse IP source de l'exception.
Port source	Numéro de port source.
Adresse de destination	Adresse IP de destination.
Port de destination	Numéro de port de destination.
Protocole de base de données	Protocole de base de données pour l'exception.
Nouvelle valeur TTL	Réservé uniquement au rôle d'administrateur.
Description de l'exception	Description de l'exception. Pour une reconnexion S-TAP ou une exception de délai, cet attribut contient l'adresse IP ou le nom DNS du serveur de base de données. Pour une exception de base de données, il s'agit d'un code d'erreur issu du système de gestion de base de données. Pour la plupart des messages communs (environ 54 000 d'entre eux), une description de texte plus longue est disponible dans l'attribut Texte d'erreur renvoyé par la base de données. Ce texte provient de la table de la base de données interne Guardium de messages d'erreur, et non de l'exception elle-même.
Chaîne SQL à l'origine de l'exception	Chaîne SQL à l'origine de l'exception.
Nom d'utilisateur	Nom d'utilisateur de la base de données. Sur le trafic chiffré, où la corrélation est requise, cette valeur peut ne pas être disponible, mais elle est toujours disponible à partir de l'attribut Nom d'utilisateur de la base de données dans l'entité Client-serveur.
Nom d'utilisateur de l'application	Nom d'utilisateur de l'application.
Lien vers plus d'informations sur l'exception	Lien facultatif parfois disponible, selon la source d'exception.
ID1 global	Identificateur global de l'exception.

Attribut	Description
Fuseau horaire d'origine	Décalage UTC. Cela concerne en particulier les agrégateurs dont les collecteurs se trouvent dans des fuseaux horaires différents. Les activités qui se sont produites à des heures d'intervalle ne semblent pas arriver au même moment lorsqu'elles sont importées dans l'agrégateur. Par exemple, sur un agrégateur qui regroupe les données de différents fuseaux horaires, vous pouvez voir le début de session d'un enregistrement à 21h00 avec le fuseau horaire d'origine UTC-02:00, et un autre enregistrement où le début de session est 21h00 avec le fuseau horaire d'origine UTC-05:00. Cela signifie que ces événements se sont produits à 3 heures d'intervalle, mais à la même heure locale respective (21h00).

ID exception et ID type d'exception sont uniquement disponibles pour les utilisateurs disposant du rôle d'administrateur.

Entité Type d'exception

Il existe un ensemble fixe de types d'exceptions, dont l'un est associé à chaque exception consignée. Ils sont disponibles pour la génération de rapports uniquement à partir de l'entité d'exception propriétaire.

Tableau 34. Entité Type d'exception

Attribut	Description
Description de l'exception	Description de texte du type d'exception, dans la liste suivante. La plupart de ces textes ne devraient jamais être visualisés. Voir les remarques en italique pour les exceptions et les remarques les plus courantes. Une nouvelle construction a été utilisée Le processus d'alerte a généré une exception Exception du traitement des alertes personnalisées Le serveur de base de données a renvoyé une erreur Pour ce message, un code d'erreur de base de données est stocké dans l'attribut Description de l'exception de l'entité Exception, et une version texte du message d'erreur de la base de données sera disponible dans l'attribut Texte d'erreur renvoyé par la base de données de l'entité Texte d'erreur renvoyé par la base de données. Exception du protocole de BD Déboguer les impressions via le mécanisme des EXCEPTIONs Requêtes de base de données abandonnées Les informations sur la session ont été supprimées en raison du trafic excessif. Erreur lors du processus système d'audit de configuration Erreur lors du processus de classification Appel de requête non valide Echec de connexion Exception du protocole de BD de niveau inférieur Le travail planifié a généré une exception Exception de l'évaluation de sécurité Exception de sécurité Pour ce message, une exception de classe personnalisée a été émise lorsque l'exécution du code de violation est bloquée, par exemple lorsque des utilisateurs utilisent l'API Java™ pour définir leurs propres alertes ou évaluations. Session fermée de manière prématurée Exception de l'analyseur SQL Reconnexion de la connectivité de l'agent S-TAP Pour ce message, l'adresse IP ou le nom DNS du serveur de base de données sont disponibles dans l'attribut Description de l'exception de l'entité Exception Dépassement du délai de connectivité de l'agent S-TAP Pour ce message, l'adresse IP ou le nom DNS du serveur de base de données sont disponibles dans l'attribut Description de l'exception de l'entité Exception TCP ERROR Pour ce message, des informations supplémentaires sur l'erreur sont incluses dans l'attribut Description de l'exception de l'entité Exception La classe a généré une exception Impossible de purger le rapport

Entité Champ

Chaque fois que Guardium rencontre un nouveau champ, il crée une entité de champ.

Tableau 35. Entité Champ

Attribut	Description
ID champ	Identifie le champ de manière unique.
ID construction	Identifie de manière unique la construction dans laquelle il a été référencé.
ID commande	Identifie de manière unique la commande principale à partir de la construction dans laquelle il a été référencé.
ID objet	Identifie de manière unique l'objet à partir de la construction dans laquelle il a été référencé.
Nom du champ	Nom du champ.
Clause List Clause Where Clause Order by Clause Having Clause Group By Clause On	Utilisez ces attributs pour ordonner des requêtes SQL complexes. Exemple de requêtes SQL : Order by SELECT * FROM dept_costs WHERE dept_total > (SELECT avg FROM avg_cost) ORDER BY department Having SELECT column_name1, SUM(column_name2) FROM table_name GROUP BY column_name1 HAVING (numerical function condition) Group By SELECT column_name1, SUM(column_name2) FROM table_name GROUP BY column_name1 Où SELECT FirstName, LastName, City FROM Users WHERE City = Los Angeles

ID champ, ID construction, ID commande et ID objet sont uniquement disponibles pour les utilisateurs disposant du rôle d'administrateur.

Entité Valeur SQL de champ

Ces entités ne sont créées que par des actions de règle de politique consignées avec des valeurs. Par exemple : CONSIGNER L'ENSEMBLE DES DETAILS AVEC LES VALEURS et CONSIGNER L'ENSEMBLE DES DETAILS PAR SESSION AVEC LES VALEURS. La valeur de champ consignée peut ou non être associée à un nom de champ. Par exemple, les noms de champ sont disponibles (dans l'entité Champ) si l'instruction suivante est consignée :

insert into t1 (foo, bar) (10, 20)

Mais ils ne sont pas disponibles lorsque l'instruction suivante est consignée :

insert into t2 (10, 20)

Tableau 36. Entité Valeur SQL de champ

Attribut	Description
Valeur	Valeur de champ issue de la construction consignée.

Entité Flat Log

Cette entité décrit l'activité de traitement de Flat Log.

Tableau 37. Entité Flat Log

Attribut	Description
SQL complet	SQL complet consigné.
Horodatage	Date/heure de la consignation.
Date d'horodatage	Partie date de l'horodatage.
Heure d'horodatage	Partie heure de l'horodatage.

Attribut	Description
Temps de réponse	Temps de réponse à la requête en millisecondes.
Enregistrements affectés	Nombre d'enregistrements affectés par la demande.
Réussite	Indique si la requête a abouti (True/False).
Type d'instruction	Type d'instruction SQL SQL : commande SQL simple et directe, par exemple, saisie directement dans l'interface CLI RAW : PREPARE d'une instruction SQL pour une exécution ultérieure, par exemple, conn.prepareStatement (sélectionnez a de b où c=:valeur) BIND : exécution d'une instruction préparée incluant des valeurs de paramètre liées Le type d'instruction fait partie de l'entité FULL SQL et n'est audité que si vous avez configuré CONSIGNER L'ENSEMBLE DES DETAILS pour cette instruction dans la politique. Vous ne pouvez pas filtrer les types d'instructions spécifiques dans la politique, par exemple, les instructions SQL et BIND d'audit uniquement. Vous pouvez, cependant, les filtrer dans les rapports.
Données renvoyées	Données renvoyées (le cas échéant)
Info de liaison	Informations de liaison pour la demande
Valeurs des variables de liaison	Pour DB2 / zOS, contient une liste de variables de liaison séparées par des virgules
Fuseau horaire d'origine	Décalage UTC. Cela concerne en particulier les agrégateurs dont les collecteurs se trouvent dans des fuseaux horaires différents. Les activités qui se sont produites à des heures d'intervalle ne semblent pas arriver au même moment lorsqu'elles sont importées dans l'agrégateur. Par exemple, sur un agrégateur qui regroupe les données de différents fuseaux horaires, vous pouvez voir le début de session d'un enregistrement à 21h00 avec le fuseau horaire d'origine UTC-02:00, et un autre enregistrement où le début de session est 21h00 avec le fuseau horaire d'origine UTC-05:00. Cela signifie que ces événements se sont produits à 3 heures d'intervalle, mais à la même heure locale respective (21h00).

Entité SQL complet

Les entités SQL complet ne sont créées que par les actions de règle de politique suivantes : CONSIGNER L'ENSEMBLE DES DETAILS, CONSIGNER L'ENSEMBLE DES DETAILS AVEC LES VALEURS, CONSIGNER L'ENSEMBLE DES DETAILS PAR SESSION ou CONSIGNER L'ENSEMBLE DES DETAILS PAR SESSION AVEC LES VALEURS.

Tableau 38. Entité SQL complet

Attribut	Description
SQL complet	Instruction SQL complet, y compris les valeurs.
Horodatage	L'horodatage enregistre l'heure à laquelle le SQL est exécuté dans le serveur de base de données.
Temps de réponse	Temps de réponse à la demande en millisecondes. Lorsque les demandes sont surveillées sur le trafic réseau, les temps de réponse reflètent fidèlement le temps nécessaire pour répondre à la demande (Guardium horodate à la fois la demande du client et la réponse du serveur).
Enregistrements affectés	Nombre d'enregistrements affectés pour chaque session. Sur les rapports utilisant cet attribut, nous vous suggérons d'activer des alias pour afficher correctement des cas spéciaux tels qu'Ensemble de résultats de grande taille ou N/A.
Données renvoyées	Données renvoyées pour cette demande (le cas échéant, et si disponible).
ID SQL complet	Identificateur unique du SQL complet.
ID instance	Identificateur unique de l'instance du SQL complet.
Réussite	Indique si l'appel a abouti.
Enregistrements affectés (Desc)	Lorsque l'attribut Enregistrements affectés est une valeur de chaîne plutôt qu'un nombre, cette chaîne est stockée ici. Par exemple : Ensemble de résultats de grande taille ou N/A.
Description de la règle d'accès	Description de la règle de politique utilisée
Nombre de données renvoyées	Nombre de lignes renvoyées par l'instruction SQL utilisée dans la règle de politique.
Validation automatique	Les entrées sont automatiquement numérotées.
Temps de réponse de prise en compte	Temps de réponse de prise en compte en millisecondes.
Nombre de kilooctets dans les demandes	Enregistre le nombre d'octets dans les requêtes.
Nombre de kilooctets dans les réponses	Enregistre le nombre d'octets dans les réponses.

Attribut	Description
Type d'instruction	Type d'instruction SQL SQL : commande SQL simple et directe, par exemple, saisie directement dans l'interface CLI RAW : PREPARE d'une instruction SQL pour une exécution ultérieure, par exemple, conn.prepareStatement (sélectionnez a de b où c=:valeur) BIND : exécution d'une instruction préparée incluant des valeurs de paramètre liées Le type d'instruction fait partie de l'entité FULL SQL et n'est audité que si vous avez configuré CONSIGNER L'ENSEMBLE DES DETAILS pour cette instruction dans la politique. Vous ne pouvez pas filtrer les types d'instructions spécifiques dans la politique, par exemple, les instructions SQL et BIND d'audit uniquement. Vous pouvez, cependant, les filtrer dans les rapports.
Valeurs des variables de liaison	Pour DB2 / zOS, contient une liste de variables de liaison séparées par des virgules
Fuseau horaire d'origine	Décalage UTC. Cela concerne en particulier les agrégateurs dont les collecteurs se trouvent dans des fuseaux horaires différents. Les activités qui se sont produites à des heures d'intervalle ne semblent pas arriver au même moment lorsqu'elles sont importées dans l'agrégateur. Par exemple, sur un agrégateur qui regroupe les données de différents fuseaux horaires, vous pouvez voir le début de session d'un enregistrement à 21h00 avec le fuseau horaire d'origine UTC-02:00, et un autre enregistrement où le début de session est 21h00 avec le fuseau horaire d'origine UTC-05:00. Cela signifie que ces événements se sont produits à 3 heures d'intervalle, mais à la même heure locale respective (21h00).

ID SQL complet, ID instance et Réussite sont uniquement disponibles pour les utilisateurs disposant du rôle d'administrateur.

Entité Valeurs de SQL complet

Ces entités ne sont créées que par des actions de règle de politique suivantes : CONSIGNER L'ENSEMBLE DES DETAILS AVEC LES VALEURS et CONSIGNER L'ENSEMBLE DES DETAILS PAR SESSION AVEC LES VALEURS.

Tableau 39. Entité Valeurs de SQL complet

Attribut	Description
Valeurs	Une ou plusieurs valeurs issues de la construction consignée.
Horodatage	Date et heure auxquelles l'entité de valeurs de SQL complet a été créée.

Entité Evénements GIM

Cette entité décrit les événements survenus lors de l'utilisation de Guardium Installation Manager (GIM).

Tableau 40. Entité Evénements GIM

Attribut	Description
Générateur d'événements	Adresse IP du client (c'est-à-dire DB-Server) qui a généré l'événement.
Description de l'événement	Description de l'événement.
Heure de l'événement	Le moment où l'événement a eu lieu.

Entité Groupe

Cette entité décrit un groupe qui a été défini pour Guardium.

Tableau 41. Entité Groupe

Attribut	Description
Description du groupe	Nom du groupe.
Sous-type du groupe	Sous-type, le cas échéant, défini pour le groupe.
Horodatage	Date et heure de création de l'entité de groupe.

Entité Membre de groupe

Cette entité décrit un membre de groupe qui a été défini pour Guardium.

Tableau 42. Entité Membre de groupe

Attribut	Description
Membre de groupe	Nom du membre de groupe.
Horodatage	Date et heure auxquelles le membre du groupe a été créé ou mis à jour.
Date d'horodatage	Date uniquement issue de l'horodatage.
Heure d'horodatage	Heure uniquement issue de l'horodatage.
Année de l'horodatage	Année uniquement issue de l'horodatage.

Attribut	Description
Jour de la semaine de l'horodatage	Jour de la semaine uniquement issu de l'horodatage.

Entité Type de groupe

Cette entité décrit un type de groupe Guardium (utilisateur, adresse IP client, commande, etc.)..

Tableau 43. Entité Type de groupe

Attribut	Description
Type du groupe	Identifie le type de groupe.
Horodatage	Date et heure de création du type de groupe.

Types d'activité Guardium

Cette entité décrit les différentes activités d'utilisateur

Tableau 44. Types d'activité Guardium

Attribut	Description
Description du type d'activité	Description de l'activité
ID type d'activité	Identifie le type d'activité de manière unique.

Entité Rôle Guardium

Cette entité (sous Entité Utilisateur) identifie un rôle Guardium.

Tableau 45. Entité Rôle Guardium

Attribut	Description
Identificateur de rôle	ID du rôle identifié.
Rôle	Rôle Guardium répertorié.

Entité Applications Guardium

Cette entité (sous Entité Utilisateur) identifie une application Guardium.

Tableau 46. Entité Applications Guardium

Attribut	Description
Identificateur d'application	ID de l'application identifiée.
Application	Application Guardium répertoriée (par exemple, Générateur de requête, Générateur de politique, etc.).

Entité Types d'activité Guardium

Une instance est définie dans la base de données Guardium interne pour chaque type d'activité.

Tableau 47. Entité Types d'activité Guardium

Attribut	Description
Description du type d'activité	Description d'une activité.

Entité Audit d'activité utilisateur Guardium

Cette entité est créée pour chaque activité utilisateur Guardium.

Tableau 48. Entité Audit d'activité utilisateur Guardium

Attribut	Description
ID connexion	ID utilisé pour la connexion.
Nom d'utilisateur	Nom d'utilisateur Guardium pour l'activité.
Horodatage	Créé lorsque l'activité a été consignée.
Entité modifiée	L'entité Guardium modifiée (une définition de groupe, par exemple).
Clé d'entité utilisée	Clé utilisée pour accéder à l'entité.
Valeur de clé	Nouvelle valeur de l'entité.
Toutes les valeurs	Toutes les valeurs modifiées.
Description d'objet	Nom de l'objet spécifique modifié.
ID global	ID global unique pour la session.
Nom d'hôte	Nom d'hôte de l'utilisateur.

Entité Connexion des utilisateurs Guardium

Cette entité est créée chaque fois qu'un utilisateur se connecte au dispositif Guardium.

Tableau 49. Entité Connexion des utilisateurs Guardium

Attribut	Description
ID connexion	ID utilisé pour la connexion.
Nom d'utilisateur	Créé lorsque l'utilisateur Guardium se connecte ou se déconnecte (il existe une entité par session Guardium).
Date et heure de connexion	Date et heure de connexion de l'utilisateur.
Date et heure de déconnexion	Date et heure de déconnexion de l'utilisateur.
Connexion réussie	Indique si la connexion a abouti.
ID global	ID global unique pour la session.
Nom d'hôte	Nom d'hôte de l'utilisateur.
Adresse distante	Adresse distante de l'utilisateur.

Entité Hôte

Une entité Hôte CAS est créée la première fois que CAS est visualisé sur un hôte de serveur de base de données. Elle est mise à jour chaque fois que le statut en ligne/hors ligne change. L'entité Hôte est également disponible dans le domaine CAS Historique de l'hôte.

Tableau 50. Entité Hôte

Attribut	Description
Nom d'hôte	Nom d'hôte du serveur de base de données (peut s'afficher en tant qu'adresse IP)
Type de système d'exploitation	Système d'exploitation : UNIX ou WIN
Est en ligne	Statut en ligne (Oui/Non) lorsque l'enregistrement a été écrit
ID hôte	Identifie l'enregistrement de l'hôte

Entité Configuration hôte

Une entité Configuration hôte est créée pour chaque élément dans une instance CAS.

Tableau 51. Entité Configuration hôte

Attribut	Description
ID libellé d'état d'audit	Identificateur numérique unique pour l'élément de configuration
Horodatage	Horodatage de la création de l'entité
Nom d'hôte	Nom d'hôte ou adresse IP du serveur de base de données
Type de système d'exploitation	Système d'exploitation : Unix ou Windows.
Type de base de données	Type de base de données : Oracle, MS-SQL, DB2, Sybase, Informix ou N/A si le changement concerne une instance du système d'exploitation.
Nom d'instance	Nom de l'instance du jeu de modèles
Type	Type de l'élément surveillé qui a changé. Script OS ou script SQL : changement déclenché par le script OS contenu dans la définition du modèle d'élément surveillé. Variable d'environnement : variable d'environnement (Unix uniquement) Variable de registre : variable de registre (Windows uniquement) Fichier : un fichier spécifique. Il n'existe pas d'entité de configuration hôte pour un modèle de fichier défini dans le jeu de modèles utilisé par l'instance. Au lieu de cela, il existe une entité de configuration hôte distincte pour chaque fichier qui correspond au modèle.
Elément surveillé	Nom de l'élément modifié, issu de la Description (si entré), sinon nom par défaut selon le type (nom de fichier, par exemple).

Entité Evénement hôte

Une entité Evénement hôte est créée chaque fois qu'un événement est détecté ou signalé (voir les types d'événement) par CAS.

Tableau 52. Entité Evénement hôte

Attribut	Description
ID événement d'hôte d'audit	Identifie l'entité Evénement hôte
Heure de l'événement	Date et heure auxquelles l'événement a été enregistré

Attribut	Description
Type d'événement	Identifie l'événement en cours d'enregistrement : Client actif - CAS a démarré sur l'hôte du serveur de base de données Client inactif - CAS s'est arrêté sur l'hôte du serveur de base de données Reprise en ligne désactivée - Un serveur est disponible (après une interruption), donc les données CAS sont écrites sur le serveur Reprise en ligne activée - Le serveur n'est pas disponible, donc les données CAS sont écrites dans le fichier de reprise en ligne Serveur inactif - Le serveur de base de données s'est arrêté Serveur actif - Le serveur de base de données a démarré
Horodatage	Horodatage de la création de l'entité
ID hôte d'audit	Identifie l'hôte
Fuseau horaire d'origine	Décalage UTC. Cela concerne en particulier les agrégateurs dont les collecteurs se trouvent dans des fuseaux horaires différents. Les activités qui se sont produites à des heures d'intervalle ne semblent pas arriver au même moment lorsqu'elles sont importées dans l'agrégateur. Par exemple, sur un agrégateur qui regroupe les données de différents fuseaux horaires, vous pouvez voir le début de session d'un enregistrement à 21h00 avec le fuseau horaire d'origine UTC-02:00, et un autre enregistrement où le début de session est 21h00 avec le fuseau horaire d'origine UTC-05:00. Cela signifie que ces événements se sont produits à 3 heures d'intervalle, mais à la même heure locale respective (21h00).

Entité Incident

Les entités Incident sont créées par des processus de génération d'incidents, ou manuellement en attribuant une violation de politique à un incident.

Tableau 53. Entité Incident

Attribut	Description
Horodatage	Date/heure auxquelles l'incident a été créé.
Nom de catégorie	Catégorie attribuée à l'incident.
Numéro d'incident	Numéro d'incident (affecté séquentiellement).

Entité Gravité d'incident

La description de la gravité d'un incident.

Tableau 54. Entité Gravité d'incident

Attribut	Description
Description de la gravité d'un incident	Le code de gravité est l'un des suivants : INFO, FAIBLE, MOYEN, ELEVE

Entité Statut d'incident

Décrit le statut d'une entité Incident.

Tableau 55. Entité Statut d'incident

Attribut	Description
Description du statut	Les valeurs possibles sont les suivantes : OPEN - L'incident n'a pas encore été affecté à un utilisateur. ASSIGNED - L'incident a été affecté. CLOSED - L'incident est fermé.

Entité Politique installée

Décrit la politique installée.

Tableau 56. Entité Politique installée

Attribut	Description
ID	Identifie l'enregistrement d'installation de la politique.
ID jeu de règles	Identifie le jeu de règles.
Description de la politique	Description issue de la définition de politique.
Trace d'audit sélectif	Indique s'il s'agit d'une politique de trace d'audit sélectif (T/F).
Modèle d'audit	Modèle de test utilisé pour une politique de trace d'audit sélectif.
Horodatage	Horodatage de la création de l'enregistrement.

Attribut	Description
Séquence	Définit l'ordre de séquence lorsqu'il existe plusieurs politiques installées.

Entité Config d'instance

Une entité Config d'instance est créée chaque fois qu'une configuration d'instance est définie. Cette entité définit comment l'instance CAS se connecte à la base de données (si nécessaire) et identifie le jeu de modèles utilisé par l'instance. Elle fournit le statut actuel de l'instance (en cours d'utilisation, activé ou désactivé) et la date de la dernière révision.

Attributs de l'entité Config d'instance

Tableau 57. Entité Config d'instance

Attribut	Description
ID Config	Identifie cet enregistrement de configuration.
Horodatage	Enregistrement d'horodatage créé.
Type de base de données	Type de base de données : Oracle, MS-SQL, DB2, Sybase, Informix ou N/A pour une instance du système d'exploitation
Instance	Nom de l'instance
Utilisateur	Nom d'utilisateur que CAS utilise pour se connecter à la base de données, ou N/A pour une instance du système d'exploitation.
Port	Numéro de port CAS utilisé pour se connecter à la base de données ou vide pour une instance du système d'exploitation
Répertoire principal de base de données	Répertoire principal de la base de données, ou vide pour une instance du système d'exploitation
ID jeu de modèles	Identifie le jeu de modèles utilisé par cette instance
Type de système d'exploitation	Système d'exploitation de l'hôte : UNIX ou Windows

Entité Jointure

Une table de jointure est une façon de mettre en œuvre de nombreuses relations à plusieurs. Utilisez l'entité Jointure pour joindre des tables dans une instruction SELECT SQL.

Tableau 58. Entité Jointure

Attribut	Description
ID jointure	Identificateur unique
ID construction	Identifie la construction dans laquelle la jointure est référencée.
SQL de jointure	Tables de jointure
SQL Where	Clause Where (conditions de jointure)
Horodatage	Date et heure de création de l'entité Jointure.

Entité Commentaires locaux

Cette entité décrit un commentaire local. Elle est disponible uniquement dans le domaine Commentaires, qui est réservé aux administrateurs. Cette entité comprend uniquement des commentaires locaux pour les processus et les ensembles de résultats qui s'exécutent localement. Les commentaires partageables sont définis dans l'entité Commentaires.

Tableau 59. Entité Commentaires locaux

Attribut	Description
Auteur du commentaire	Utilisateur Guardium qui a créé le commentaire.
Référence du commentaire	Indique l'élément auquel le commentaire est associé - une requête, un résultat de processus d'audit ou un autre commentaire, par exemple.
Contenu du commentaire	Texte complet du commentaire.
Horodatage	Date/heure auxquelles le commentaire a été créé.
Année de l'horodatage	Année uniquement issue de l'horodatage.
Jour de la semaine de l'horodatage	Jour de la semaine uniquement issu de l'horodatage.
Heure d'horodatage	Heure uniquement issue de l'horodatage.
Date d'horodatage	Date uniquement issue de l'horodatage.
Description d'objet	Nom de l'objet à partir duquel le commentaire a été défini. Par exemple, un commentaire défini sur un incident possède la description d'objet INCIDENT.
Associations d'enregistrements	Liste des enregistrements avec lesquels ce commentaire local est associé.

Vue emplacement

Détermination des jours non archivés

Utilisez une requête (onglet Outils > Génération de rapports > Générateur de rapports > requête Vue emplacement) qui peut être modifiée pour créer un rapport montrant les fichiers archivés. Ce rapport répertorie tous les fichiers comportant des dates d'archivage. Les dates ne figurant pas sur ce rapport indiquent que les fichiers n'ont pas été archivés. Exécutez l'archivage pour les dates qui ne figurent pas dans la liste, si nécessaire.

Tableau 60. Entité Vue emplacement

Attribut	Description
Du	Date de début
Au	Date de fin
Agrégateur	Système Guardium sur lequel le fichier a été généré. Cependant, il peut s'agir d'un collecteur, pas seulement d'un agrégateur
Hôte	Nom d'hôte
Nom d'utilisateur	Nom d'utilisateur
Chemin d'accès	Nom du chemin vers les fichiers
Type de système	Quel protocole a été utilisé lors de l'archivage - s'il s'agissait de SCP ou FTP ou Centera ou TSM
Nombre de destinations	Destinations d'archives

Entité Corrélation de connexion

Obsolète à partir de la version 4.0 de Guardium. Il s'agissait de la seule entité du domaine Suivi de trace d'accès, qui est obsolète à partir de la version 4.0 de S-TAP. Si vous possédez d'anciennes requêtes ou des rapports utilisant ce domaine, ils ne fonctionnent pas dans cette version et toutes les informations de connexion à la base de données enregistrées dans ce domaine datent d'avant l'installation de la version 4.0 de S-TAP.

Entité Texte du message

Pour une alerte de seuil, texte du message.

Tableau 61. Entité Texte du message

Attribut	Description
ID texte du message	Identifie le texte du message de manière unique.
Objet du message	Objet du message (pour un e-mail, par exemple).
Texte du message	Texte du message.
Fuseau horaire d'origine	Décalage UTC. Cela concerne en particulier les agrégateurs dont les collecteurs se trouvent dans des fuseaux horaires différents. Les activités qui se sont produites à des heures d'intervalle ne semblent pas arriver au même moment lorsqu'elles sont importées dans l'agrégateur. Par exemple, sur un agrégateur qui regroupe les données de différents fuseaux horaires, vous pouvez voir le début de session d'un enregistrement à 21h00 avec le fuseau horaire d'origine UTC-02:00, et un autre enregistrement où le début de session est 21h00 avec le fuseau horaire d'origine UTC-05:00. Cela signifie que ces événements se sont produits à 3 heures d'intervalle, mais à la même heure locale respective (21h00).

Entité Messages envoyés

Pour chaque message d'alerte de seuil envoyé, type de message, destinataires, statut et date de ce message.

Tableau 62. Entité Messages envoyés

Attribut	Description
ID message	Identifie le message de manière unique.
Type de message	Type de message.
Envoyé à	Un ou plusieurs destinataires du message.
Statut du message	Statut du message : ECHEC L'opération d'envoi a échoué. EN ATTENTE Le message n'a pas encore été envoyé. ENVOYE Le message a été envoyé.
Date du message	Date d'envoi du message.
Contexte de message	Type de message : INFO Message d'information. AVERTISSEMENT Condition d'erreur possible. ALERTE Alerte en temps réel ou de seuil. ERREUR Condition d'erreur logicielle ou matérielle. DEBOGAGE Message de débogage.
Emetteur du message	Module créant le message, par exemple moniteur ou GuardiumJetspeedUser.

Attribut	Description
Fuseau horaire d'origine	Décalage UTC. Cela concerne en particulier les agrégateurs dont les collecteurs se trouvent dans des fuseaux horaires différents. Les activités qui se sont produites à des heures d'intervalle ne semblent pas arriver au même moment lorsqu'elles sont importées dans l'agrégateur. Par exemple, sur un agrégateur qui regroupe les données de différents fuseaux horaires, vous pouvez voir le début de session d'un enregistrement à 21h00 avec le fuseau horaire d'origine UTC-02:00, et un autre enregistrement où le début de session est 21h00 avec le fuseau horaire d'origine UTC-05:00. Cela signifie que ces événements se sont produits à 3 heures d'intervalle, mais à la même heure locale respective (21h00).

Entité Surveiller les valeurs

Une entité Surveiller les valeurs est créée pour chaque insertion, mise à jour ou suppression enregistrée, contient les détails du changement (nom de table, action, texte SQL, etc.).

Tableau 63. Entité Surveiller les valeurs

Attribut	Description
Horodatage	Date et heure où le changement a été enregistré sur le dispositif Guardium. Cet horodatage est créé lors de l'opération de téléchargement de données. Il ne s'agit pas du moment où le changement a été enregistré sur la base de données d'audit. Pour obtenir ce temps, utilisez l'entité Horodatage de l'audit.
Date d'horodatage	Date uniquement issue de l'horodatage.
Heure d'horodatage	Heure uniquement issue de l'horodatage.
Année de l'horodatage	Année uniquement issue de l'horodatage.
Jour de la semaine de l'horodatage	Jour de la semaine uniquement issu de l'horodatage.
Adresse IP du serveur	Adresse IP du serveur de base de données.
Type de base de données	Type de base de données.
Nom de service	Oracle uniquement. Nom de service de la base de données.
Nom de base de données	DB2, Informix, Sybase, MS SQL Server uniquement. Nom de base de données.
Clé primaire d'audit	Pour Sybase et MS SQL Server uniquement. Une clé primaire utilisée pour relier les anciennes et les nouvelles valeurs (qui doivent être consignées séparément pour ces types de base de données).
Nom de la connexion d'audit	Nom d'utilisateur de base de données défini dans la source de données.
Nom de la table d'audit	Nom de la table changé.
Propriétaire de l'audit	Propriétaire de la table changée.
Action d'audit	Insérer, mettre à jour ou supprimer.
Ancienne valeur d'audit	Liste séparée par des virgules des anciennes valeurs, au format : column-name=column_value,
Nouvelle valeur d'audit	Liste séparée par des virgules des nouvelles valeurs, au format : column-name=column_value,
Texte SQL	Disponible uniquement avec Oracle 9. L'instruction SQL complète qui provoque le changement de valeur.
ID déclenché	ID unique (sur cette base de données d'audit) générée pour le changement.
Horodatage de l'audit	Date et heure auxquelles le déclencheur a été exécuté.
Date d'horodatage d'audit	Partie date de l'horodatage d'audit.
Heure d'horodatage d'audit	Partie heure de l'horodatage d'audit.
Jour de la semaine d'horodatage d'audit	Jour de la semaine de l'horodatage d'audit.
Année de l'horodatage d'audit	Année de l'horodatage d'audit.
Fuseau horaire d'origine	Décalage UTC. Cela concerne en particulier les agrégateurs dont les collecteurs se trouvent dans des fuseaux horaires différents. Les activités qui se sont produites à des heures d'intervalle ne semblent pas arriver au même moment lorsqu'elles sont importées dans l'agrégateur. Par exemple, sur un agrégateur qui regroupe les données de différents fuseaux horaires, vous pouvez voir le début de session d'un enregistrement à 21h00 avec le fuseau horaire d'origine UTC-02:00, et un autre enregistrement où le début de session est 21h00 avec le fuseau horaire d'origine UTC-05:00. Cela signifie que ces événements se sont produits à 3 heures d'intervalle, mais à la même heure locale respective (21h00).

Entité Changements surveillés

Cette entité est créée chaque fois qu'un élément surveillé change. Elle identifie l'élément surveillé dans l'instance CAS et pointe vers les données sauvegardées pour le changement.

Tableau 64. Entité Changements surveillés

Attribut	Description
Identificateur du changement	Identificateur unique du changement.
Temps d'échantillonnage	Horodatage (date et heure sur l'hôte) auquel cet échantillon a été réalisé
ID configuration d'audit	Identifie la configuration hôte

Attribut	Description
ID données sauvegardées	Identifie l'entité Données sauvegardées pour ce changement
ID libellé d'état d'audit	Identifie l'entité Configuration hôte pour ce changement
Horodatage	Date et heure auxquelles cet enregistrement de changement a été créé sur le serveur (horloge du serveur du dispositif Guardium)
MD5	Indique si la comparaison se fait ou non en calculant une somme de contrôle à l'aide de l'algorithme MD5 et en comparant cette valeur avec la valeur calculée la dernière fois que l'élément a été vérifié. Par défaut, MD5 n'est pas utilisé. Si MD5 est utilisé, mais la taille des données brutes est supérieure à la limite de taille MD5 configurée pour l'hôte CAS, le calcul et la comparaison MD5 sont ignorés. Indépendamment du fait que MD5 soit ou non utilisé, la valeur actuelle du dernier horodatage modifié pour l'élément et la taille de l'élément sont comparées aux valeurs sauvegardées la dernière fois que l'élément a été vérifié.
Propriétaire	Unix uniquement. Si le type d'élément est un fichier, propriétaire du fichier
Autorisations	Unix uniquement. Si le type d'élément est un fichier, autorisations sur le fichier
Taille	Taille du fichier, mais il existe des valeurs spéciales comme suit : -1 = Le fichier existe, mais contient zéro octet 0 (zéro) = Le fichier n'existe pas, or ce nom de fichier est surveillé (il n'a jamais existé ou n'a pas été supprimé)
Dernière modification	Horodatage de la dernière modification, extrait du système de fichiers au moment de l'échantillonnage
Date de la dernière modification	Date de la dernière modification
Heure de la dernière modification	Heure de la dernière modification
Jour de la semaine de la dernière modification	Jour de la semaine de la dernière modification
Année de la dernière modification	Année de la dernière modification
Groupe	Unix uniquement. Si le type d'élément est un fichier, propriétaire du groupe

Entité Monitored Item Details

Une entité Détails d'élément surveillé est créée pour chaque élément surveillé dans une instance CAS.

Tableau 65. Entité Détails d'élément surveillé

Attribut	Description
ID configuration d'audit	Identifie la configuration hôte
Horodatage	Horodatage de la création de l'entité
ID modèle	Identifie le modèle d'élément pour cet élément surveillé
Elément surveillé	Selon le type d'audit, il s'agit du script de système d'exploitation ou SQL, de la variable d'environnement ou de registre ou du nom de fichier. En ce qui concerne un modèle de fichier défini dans un modèle d'élément, il existe une entité Détails d'élément surveillé pour chaque fichier qui correspond au modèle, mais il n'existe aucune entité Détails d'élément surveillé pour le modèle de fichier même. Si un modèle de fichier est utilisé, il est toujours disponible dans l'attribut Contenu du modèle.
ID jeu de configurations d'audit	Identifie le jeu de modèles dans la configuration hôte
Type d'audit	Type d'élément surveillé : Script OS ou Script SQL : texte réel ou chemin d'accès vers un système d'exploitation ou un script SQL, dont la sortie est comparée à la sortie produite la prochaine fois qu'il est exécuté Variable d'environnement ou variable de registre : variable d'environnement ou variable de registre (Windows) Fichier : fichier spécifique ou motif pour identifier un ensemble de fichiers
Activé	Indique si le modèle est activé
En synchronisation	Indique si la définition d'élément de modèle sur le serveur correspond à la définition d'élément de modèle sur l'hôte CAS
Fréquence d'audit	Intervalle maximum auquel l'objet doit être testé
Utiliser MD5	Indique si la comparaison se fait ou non en calculant une somme de contrôle à l'aide de l'algorithme MD5 et en comparant cette valeur avec la valeur calculée la dernière fois que l'élément a été vérifié. Par défaut, MD5 n'est pas utilisé. Si MD5 est utilisé, mais la taille des données brutes est supérieure à la limite de taille MD5 configurée pour l'hôte CAS, le calcul et la comparaison MD5 sont ignorés. Indépendamment du fait que MD5 soit ou non utilisé, la valeur actuelle du dernier horodatage modifié pour l'élément et la taille de l'élément sont comparées aux valeurs sauvegardées la dernière fois que l'élément a été vérifié.
Sauvegarder des données	Si cet attribut est sélectionné, la version précédente de l'élément peut être comparée à la version actuelle
Description	Description facultative de l'instance
Contenu du modèle	Entrée de modèle qui constitue la base de cet élément surveillé, définie à partir de l'attribut Nom d'accès de l'entité Modèle lors de la création de l'instance. En règle générale, elle est identique à l'élément surveillé, mais dans le cas où un modèle de fichier a été utilisé dans le modèle, il s'agit du modèle de fichier

Entité Objet

Une instance de cette entité est créée pour chaque objet dans un schéma unique.

Tableau 66. Entité Objet

Attribut	Description
ID objet	Identifie l'objet de manière unique.
ID construction	Identifie de manière unique la construction dans laquelle l'objet est référencé.
Schéma	Schéma de base de données pour l'objet. Remarque : Cet attribut est obsolète car il n'est jamais rempli
Nom d'objet	Nom de l'objet.
Module1 d'objet d'application	Identifie de manière unique le module d'objet d'application.

ID objet et ID construction sont uniquement disponibles pour les utilisateurs disposant du rôle d'administrateur.

Entité Commande d'objet

Décrit une entité Commande d'objet.

Tableau 67. Entité Commande d'objet

Attribut	Description
Objet/Commande	Valeur d'objet combinée à une valeur de commande.

Entité Champ d'objet

Décrit une entité Champ d'objet. Les champs Remarque sans objet ne s'affichent pas dans les rapports incluant l'objet.

Tableau 68. Entité Champ d'objet

Attribut	Description
Objet/Champ	Valeur d'objet combinée à une valeur de champ.

Entité Violation de règle de politique

Cette entité est créée chaque fois qu'une violation de règle de politique est consignée. Toutes les violations de règle de politique ne sont pas consignées - voir la description des actions de règle au chapitre 11 : Création de politiques. La règle d'accès qui cause la violation est disponible dans l'Entité Règle d'accès dépendante (décrite précédemment).

Tableau 69. Entité Violation de règle de politique

Attribut	Description
ID journal de violation	Identifie l'entité Violation de manière unique.
Nom d'utilisateur d'application	Nom de l'utilisateur créant la violation de règle de politique.
Chaîne SQL complète	Chaîne SQL provoquant la violation de règle de politique.
Horodatage	Créé lorsque la violation de règle de politique est enregistrée. Toutes les violations de règle de politique ne sont pas consignées - voir la description des actions de règle au chapitre 11 : Création de politiques.
Date d'horodatage	Date uniquement issue de l'horodatage.
Heure d'horodatage	Heure uniquement issue de l'horodatage.
Jour de la semaine de l'horodatage	Jour de la semaine uniquement issu de l'horodatage.
Année de l'horodatage	Année uniquement issue de l'horodatage.
Message envoyé	Texte du message de violation de règle de politique qui a été envoyé.
Nombre total d'occurrences	Nombre d'occurrences ayant déclenché la violation.
ID événement d'application	ID événement d'application (le cas échéant - définis à l'aide de l'API d'événements d'application)
Description de la règle d'accès	Description de la règle à partir de sa définition.
Nom de catégorie	Catégorie définie pour la règle.
Gravité	Gravité définie pour la règle (la gravité d'un incident auquel cet attribut est affecté peut être différente).
Numéro d'incident	Si affecté à un incident, il s'agit du numéro d'incident.
Nom de la classification	Nom du processus de classification.
ID construction	Identifie de manière unique la construction dans laquelle il a été référencé.
ID exécution du processus CLS	ID de l'exécution du travail du processus de classification.
Fuseau horaire d'origine	Décalage UTC. Cela concerne en particulier les agrégateurs dont les collecteurs se trouvent dans des fuseaux horaires différents. Les activités qui se sont produites à des heures d'intervalle ne semblent pas arriver au même moment lorsqu'elles sont importées dans l'agrégateur. Par exemple, sur un agrégateur qui regroupe les données de différents fuseaux horaires, vous pouvez voir le début de session d'un enregistrement à 21h00 avec le fuseau horaire d'origine UTC-02:00, et un autre enregistrement où le début de session est 21h00 avec le fuseau horaire d'origine UTC-05:00. Cela signifie que ces événements se sont produits à 3 heures d'intervalle, mais à la même heure locale respective (21h00).

ID journal de violation est uniquement disponible pour les utilisateurs disposant du rôle d'administrateur.

Entité Objet qualifié

Un *tuple* permet de combiner plusieurs attributs pour former un seul membre de groupe. Dans ce cas, les champs IP serveur, Nom de service, Nom de base de données, Utilisateur de base de données et Objet sont combinés.

Tableau 70. Entité Objet qualifié

Attribut	Description
Objet qualifié	Tuple - IP serveur, Nom de service, Nom de base de données, Utilisateur de base de données, Objet.

Entité Connexions corrompues

Une instance est créée pour chaque connexion à la base de données détectée par le processus Hunter S-TAP mais pas par S-TAP même, indiquant que la connexion a contourné les chemins d'accès surveillés par S-TAP.

Tableau 71. Entité Connexions corrompues

Attribut	Description
Horodatage	Valeur d'horodatage créée lorsque le dispositif Guardium enregistre la connexion corrompue signalée par Hunter.
Nom d'hôte de serveur	Nom d'hôte du serveur de base de données.
Programme source	Nom du programme source pour la connexion.
Port source	Port source pour la connexion.
ID processus source	ID du processus source.
Programme cible	Nom du programme cible pour la connexion.
Port cible	Port cible pour la connexion.
ID processus cible	ID du processus cible.
Utilisateur système d'exploitation	Nom du compte d'utilisateur du système d'exploitation.
Type d'IPC	Type de communication interprocessus utilisée pour la connexion, qui peut provenir de la liste suivante : Mémoire partagée SHM Protocole internet IPv4 version 4 Protocole internet IPv5 version 6 Tube nommé FIFO Tube simple PIPE Protocole internet INET (HPUX)
Type du serveur de la base de données	Type de serveur de base de données : Oracle, DB2, Informix ou Sybase.
Fuseau horaire d'origine	Décalage UTC. Cela concerne en particulier les agrégateurs dont les collecteurs se trouvent dans des fuseaux horaires différents. Les activités qui se sont produites à des heures d'intervalle ne semblent pas arriver au même moment lorsqu'elles sont importées dans l'agrégateur. Par exemple, sur un agrégateur qui regroupe les données de différents fuseaux horaires, vous pouvez voir le début de session d'un enregistrement à 21h00 avec le fuseau horaire d'origine UTC-02:00, et un autre enregistrement où le début de session est 21h00 avec le fuseau horaire d'origine UTC-05:00. Cela signifie que ces événements se sont produits à 3 heures d'intervalle, mais à la même heure locale respective (21h00).

Entité Règle

Peut être utilisé pour une entité Règle de politique installée ou une entité Règle de politique d'accès. Il existe une entité pour chaque règle de politique(s) installée(s) ou de politique(s) d'accès. Outre les champs d'identification (qui identifient uniquement les composants sur la base de données interne), tous ces champs sont décrits dans le rubrique d'aide sur les Politiques.

- GDM_INSTALLED_POLICY_RULES_ID - Identifie une règle de politique installée.
- ACCESS_RULE_ID - Identifie une règle d'accès.
- Description de règle - Issue de la définition de politique.
- Position de règle - Position dans la politique.
- Type de règle - Accès, Exception ou Extrusion.
- LAST_ACCESSED - Dernier
- IP client - Issu de la définition de règle.
- Masque de réseau client - Issu de la définition de règle.
- Groupe d'IP client - Issu de la définition de règle.
- IP serveur - Issu de la définition de règle.
- Masque d'IP serveur - Issu de la définition de règle.
- MAC client - Issu de la définition de règle.
- Protocole réseau - Issu de la définition de règle.
- Groupe de protocoles réseau - Issu de la définition de règle.
- Champ - Issu de la définition de règle.
- Groupe de champs - Issu de la définition de règle.
- Objet - Issu de la définition de règle.

- Groupe d'objets - Issu de la définition de règle.
- Commande - Issu de la définition de règle.
- Groupe de commandes - Issu de la définition de règle.
- Groupe objet-champ - Issu de la définition de règle.
- Type de base de données - Issu de la définition de règle.
- Nom de service - Issu de la définition de règle.
- Groupe de noms de service - Issu de la définition de règle.
- Nom de base de données - Issu de la définition de règle.
- Groupe de noms de base de données - Issu de la définition de règle.
- Utilisateur de base de données - Issu de la définition de règle.
- Groupe d'utilisateurs de base de données - Issu de la définition de règle.
- Utilisateur Utilisateur - Issu de la définition de règle.
- Groupe d'utilisateurs d'application - Issu de la définition de règle.
- Utilisateur de système d'exploitation - Issu de la définition de règle.
- Groupe d'utilisateurs de système d'exploitation - Issu de la définition de règle.
- Application source - Issu de la définition de règle.
- Groupe de programmes source - Issu de la définition de règle.
- Modèle/Modèle XML - Issu de la définition de règle.
- Période - Issu de la définition de règle.
- Nb min. - Issu de la définition de règle.
- Intervalle de réinitialisation - Issu de la définition de règle.
- Continuer vers la règle/révocation suivante - Issu de la définition de règle.
- Val. enreg. - Issu de la définition de règle.
- L'événement d'application existe - Issu de la définition de règle.
- Type d'événement - Issu de la définition de règle.
- Valeur texte de l'événement d'application - Issu de la définition de règle.
- Valeur date de l'événement d'application - Issu de la définition de règle.
- Nom d'utilisateur de l'événement - Issu de la définition de règle.
- Code d'erreur - Issu de la définition de règle.
- Type d'exception - Issu de la définition de règle.
- Nom de catégorie - Issu de la définition de règle.
- Nom de classification - Issu de la définition de règle.
- Gravité - Issu de la définition de règle.
- Modèle de données - Issu de la définition de règle.
- Modèle SQL - Issu de la définition de règle.
- Modèle de masquage - Issu de la définition de règle.
- Adresse IP client / Groupe - Fournit la possibilité d'afficher un attribut unique et sa valeur (le cas échéant) dans une seule colonne du rapport.
- Adresse IP serveur / Groupe - Fournit la possibilité d'afficher un attribut unique et sa valeur (le cas échéant) dans une seule colonne du rapport.
- Protocole réseau / Groupe - Fournit la possibilité d'afficher un attribut unique et sa valeur (le cas échéant) dans une seule colonne du rapport.
- Nom du champ / Groupe - Fournit la possibilité d'afficher un attribut unique et sa valeur (le cas échéant) dans une seule colonne du rapport.
- Nom d'objet / Groupe - Fournit la possibilité d'afficher un attribut unique et sa valeur (le cas échéant) dans une seule colonne du rapport.
- Commande / Groupe - Fournit la possibilité d'afficher un attribut unique et sa valeur (le cas échéant) dans une seule colonne du rapport.
- Nom de service / Groupe - Fournit la possibilité d'afficher un attribut unique et sa valeur (le cas échéant) dans une seule colonne du rapport.
- Nom de base de données / Groupe - Fournit la possibilité d'afficher un attribut unique et sa valeur (le cas échéant) dans une seule colonne du rapport.
- Utilisateur Utilisateur / Groupe - Fournit la possibilité d'afficher un attribut unique et sa valeur (le cas échéant) dans une seule colonne du rapport.
- Utilisateur du système d'exploitation / Groupe - Fournit la possibilité d'afficher un attribut unique et sa valeur (le cas échéant) dans une seule colonne du rapport.
- Programme source / Groupe - Fournit la possibilité d'afficher un attribut unique et sa valeur (le cas échéant) dans une seule colonne du rapport.
- Code d'erreur / Groupe - Fournit la possibilité d'afficher un attribut unique et sa valeur (le cas échéant) dans une seule colonne du rapport.
- Utilisateur Texte d'événement / Numérique / Date - Texte des événements d'application et attributs numériques et date.
- Catégorie / Classification - Catégorie et classification combinées de la règle.
- GDM_Installed_Policy_Header_ID - Identifie un en-tête de politique installée.

Remarque : GDM_INSTALLED_POLICY_RULES_ID et ACCESS_RULE_ID sont uniquement disponibles pour les utilisateurs disposant du rôle d'administrateur.

Entité Action de règle

Peut être utilisé pour une entité Action de règle de politique installée ou une entité Action de règle de politique d'accès. Il existe une entité pour chaque règle de politique(s) installée(s) ou de politique(s) d'accès.

- Séquence - Séquence de l'action dans la règle.
- Action
  - Bloquer la demande - Voir Actions de blocage dans les politiques.
  - Consigner ou ignorer la violation ou le trafic - Voir Consigner ou ignorer les actions dans les politiques.
  - Alerte - Voir Actions d'alerte dans les politiques.

Entité Saved Data

Une entité Données sauvegardées est créée chaque fois qu'un changement est détecté pour un élément surveillé, si la case Conserver les données est sélectionnée pour cet élément dans la définition du modèle d'élément.

Tableau 72. Entité Données sauvegardées

Attribut	Description
ID données sauvegardées	Identifie de manière unique l'élément de données sauvegardées
Données sauvegardées	Données réelles sauvegardées
Horodatage	Horodatage de l'enregistrement de l'entité Données sauvegardées dans la base de données du serveur
Identificateur du changement	Identifie l'entité Changements surveillés pour cette entité Données sauvegardées

ID données sauvegardées est uniquement disponible pour les utilisateurs disposant du rôle d'administrateur.

Entité IP serveur - Port de serveur

Décrit une entité IP serveur - Port de serveur.

Tableau 73. Entité IP serveur - Port de serveur

Attribut	Description
IP serveur/Port serveur	Valeur IP du serveur combinée à une valeur de port du serveur.

Entité Session

Cette entité est créée pour chaque session de base de données Client-serveur.

Tableau 74. Entité Session

Attribut	Description
ID global	Identifie de manière unique l'accès à la session.
ID session	Identifie la session de manière unique.
ID accès	Identifie de manière unique la période d'accès.
Horodatage	Initialement, un horodatage créé pour la première demande sur une connexion client-serveur où il n'y a pas de session active en cours. Ultérieurement, il est mis à jour lorsque la session est fermée ou lorsqu'elle est marquée inactive après une longue période sans activité observée. Lors du suivi des informations sur la session, vous serez probablement plus intéressé par les attributs Début de session et Fin de session que par l'attribut Horodatage.
Date d'horodatage	Date uniquement issue de l'horodatage.
Heure d'horodatage	Heure uniquement issue de l'horodatage.
Jour de la semaine de l'horodatage	Jour de la semaine uniquement issu de l'horodatage.
Année de l'horodatage	Année uniquement issue de l'horodatage.
Début de session	Date et heure du début de session. Début de session est également une Entité principale. Accédez à cette entité secondaire en cliquant sur l'entité primaire de session.
Date de début de la session	Date uniquement du début de la session.
Heure de début de la session	Heure uniquement du début de la session.
Jour de la semaine du début de la session	Jour de la semaine uniquement du début de la session.
Année du début de la session	Année uniquement du début de la session.
Port du client	Numéro du port du client.
Port du serveur	Numéro du port du serveur.
Indicateur inactif	Par défaut 0 - Ouvert pour les sessions générées par le package SQL. 1 - Fermé (déconnexion reçue). 2 - Probablement fermé, non fermé sans paquets pendant une longue durée. 3 - Pour les sessions générées à partir de paquets non SQL.
TTL	Réservé uniquement au rôle d'administrateur.
Fin de session	Date et heure de la fin de session. Fin de session est également une Entité principale. Accédez à cette entité secondaire en cliquant sur l'entité primaire de session.
Date de fin de la session	Date uniquement de la fin de la session.
Heure de fin de la session	Heure uniquement de la fin de la session.
Jour de la semaine de la fin de la session	Jour de la semaine uniquement de la fin de la session.
Année de la fin de la session	Année uniquement de la fin de la session.
Nom de base de données	Nom de la base de données pour la session (MSSQL ou Sybase uniquement). Remarque : pour Oracle, le Nom de la base de données peut contenir des informations supplémentaires et spécifiques à l'application telles que le module en cours d'exécution pour une session qui a été définie dans la colonne MODULE de la vue V$SESSION
Session ignorée	Indique si une partie de la session a été ignorée (à partir d'un moment donné).
Ignoré depuis	Horodatage créé au début de la non prise en compte de cette session.
Chaîne d'identifiant d'utilisateur	Pour une session rapportée par l'agent S-TAP (mode K-Tap uniquement), chaîne d'utilisateurs du système d'exploitation lorsque les utilisateurs emploient un nom différent. Les valeurs qui apparaissent ici varient selon la plateforme du système d'exploitation, par exemple sous AIX la chaîne IBM IBM IBM peut apparaître en tant que préfixe. Remarque : pour les zones Solaris, les identifiants d'utilisateur peuvent être rapportés au lieu des noms d'utilisateur dans la chaîne d'identifiant d'utilisateur.
Ancien ID session	Indique la session à partir de laquelle cette session a été créée. Zéro s'il s'agit de la première session de la connexion.
ID terminal	ID du terminal de la connexion, utilisé en interne pour résoudre les informations de session.
ID processus	ID de processus du client qui a établi la connexion (pas toujours disponible).

Attribut	Description
Chaîne d'identifiant d'utilisateur compressée	Valeurs compressées. Voir Chaîne d'identifiant d'utilisateur.
Délai (s.)	Indique la durée entre le début de la session et la fin de la session (en secondes).
Fuseau horaire d'origine	Décalage UTC. Cela concerne en particulier les agrégateurs dont les collecteurs se trouvent dans des fuseaux horaires différents. Les activités qui se sont produites à des heures d'intervalle ne semblent pas arriver au même moment lorsqu'elles sont importées dans l'agrégateur. Par exemple, sur un agrégateur qui regroupe les données de différents fuseaux horaires, vous pouvez voir le début de session d'un enregistrement à 21h00 avec le fuseau horaire d'origine UTC-02:00, et un autre enregistrement où le début de session est 21h00 avec le fuseau horaire d'origine UTC-05:00. Cela signifie que ces événements se sont produits à 3 heures d'intervalle, mais à la même heure locale respective (21h00).

ID global, ID session et ID accès sont uniquement disponibles pour les utilisateurs disposant du rôle d'administrateur.

Entité Gravité

Gravité de l'incident pour un incident ou une violation de politique

Tableau 75. Entité Gravité

Attribut	Description
Description de la gravité	Le code de gravité est l'un des suivants : INFO, FAIBLE, MOYEN, ELEVE

Entité Utilisation de la mémoire tampon du sniffer

Le système crée cette entité à l'intervalle défini par la commande CLI store system netfilter-buffer-size (toutes les 60 secondes par défaut).

Tableau 76. Entité Utilisation de la mémoire tampon du sniffer

Attribut	Description
Horodatage	Date/heure auxquelles l'enregistrement a été créé.
% d'utilisation de l'UC par le sniffer	Pourcentage de l'unité centrale utilisé par le sniffer.
% d'utilisation de la mémoire par le sniffer	Pourcentage de mémoire utilisé par le sniffer.
% d'utilisation de l'UC par Mysql	Pourcentage de l'unité centrale utilisé par MySQL.
% d'utilisation de la mémoire par Mysql	Pourcentage de mémoire utilisé par MySQL.
ID processus du sniffer	Identificateur de processus du sniffer.
Mémoire utilisée par le sniffer	Quantité de mémoire utilisés par le sniffer.
Durée du sniffer	Temps d'utilisation par le sniffer.
Mémoire tampon disponible	Quantité de mémoire tampon disponible.
Débit de l'analyseur	Débit d'analyse des messages.
Débit du consignateur	Débit de consignation des messages.
Longueur de la file d'attente de l'analyseur	Taille de la file d'attente d'analyse.
Total de l'analyseur	Nombre total de messages analysés.
Longueur de la file d'attente du consignateur	Taille de la file d'attente du consignateur.
Total du consignateur	Nombre total de message consignés.
Longueur de la file d'attente de la session	Taille de la file d'attente de la session.
Total de sessions	Nombre total de sessions.
Données du gestionnaire	Données internes du moteur du sniffer.
Informations supplémentaires	Données internes du moteur du sniffer.
Paquets perdus de l'analyseur	Paquets perdus de l'analyseur.
Reçus sur Eth0	Messages reçus sur ETH 0.
Envoyés sur Eth0	Messages envoyés sur ETH 0.
Bases de données surveillées du consignateur	Liste des types de base de données en cours de surveillance.
Paquets du consignateur ignorés par la règle	Paquets ignorés par une action associée à une règle de politique.

Attribut	Description
Nombre de sessions du consignateur	Nombre de sessions consignées.
Utilisation du disque Mysql	Utilisation du disque MySQL.
Mysql est démarré	Indicateur booléen pour le redémarrage interne de la base de données (1=a été redémarré, 0=non redémarré).
Indiscriminés reçus	Débit de réception de paquets sur les cartes réseau du sniffer (ports non interface).
Connexions du sniffer terminées	Nombre total de connexions surveillées et terminées depuis le redémarrage du moteur d'inspection.
Connexions du sniffer utilisées	Nombre total de connexions en cours de surveillance depuis le redémarrage du moteur d'inspection.
Paquets supprimés par le sniffer	Paquets supprimés par le sniffer.
Paquets ignorés par le sniffer	Paquets ignorés par le sniffer.
Paquets régulés par le sniffer	Nombre total de connexions qui ont été ignorées en raison de la régulation depuis le redémarrage du moteur d'inspection.
Charge de l'UC système	Utilisation de l'unité centrale système.
Utilisation de la mémoire système	Utilisation de la mémoire système.
Utilisation du disque racine système	Utilisation du disque racine système.
Temps d'activité du système	Temps depuis le dernier démarrage.
Utilisation du disque var système	Utilisation du disque var système.
Sessions normales	Nombre de sessions normales.
Sessions non ouvertes	Nombre de sessions non ouvertes par le sniffer.
Expiration de sessions	Nombre de sessions arrivées à expiration.
Sessions ignorées	Nombre de sessions ignorées par le sniffer.
Session directement fermée	Nombre de sessions directement fermées.
Session devinée	Nombre de sessions devinées.
Descripteurs de fichier ouverts	Descripteurs de fichier ouverts.
Descripteurs de fichier de base de données ouverts	Descripteurs de fichier ouverts de la base de données
Débit DI	
Longueur de la file d'attente DI	
Total DI	
Paquets perdus DI	
Demandes Flat Log	Demandes Flat Log.

Définition de l'évaluation basée sur SQL

Cette entité décrit une définition d'évaluation basée sur SQL

Tableau 77. Définition de l'évaluation basée sur SQL

Attribut	Description
Associer variable de sortie	Facultatif. Détermine si le texte saisi dans l'instruction SQL est un bloc de procédure de code qui renvoie une valeur devant être liée à une variable Guardium interne, utilisée dans la comparaison à la Valeur cible de comparaison.
Valeur cible de comparaison	Valeur utilisée comme référence pour comparer la valeur de retour émise par l'instruction SQL à l'aide de l'opérateur de comparaison.
Référence externe	Référence à Center for Internet Security (CIS) ou Common Vulnerabilities and Exposures (CVE).
Opérateur	Opérateur utilisé pour la condition.
Texte de recommandation pour échec	Texte recommandé pour l'échec du test.
Texte de recommandation pour réussite	Texte recommandé pour la réussite du test.
Texte de résultat pour échec	Le texte du résultat pour l'échec s'affiche lorsque le test échoue.
Texte de résultat pour réussite	Le texte du résultat pour la réussite s'affiche lorsque le test aboutit.
Type de retour	Type de retour renvoyé par l'instruction SQL.
Brève description	Brève description du test d'évaluation.
Instruction SQL For Details	Instruction SQL pour Détail. Instruction SQL qui récupère une liste de chaînes pour générer une chaîne de détails avec préfixe Détail + liste de chaînes.
SQL	Instruction SQL exécutée pour le test.

Entité SQL

Entité SQL

Cette entité est créée pour chaque chaîne SQL unique. Les valeurs sont remplacées par des points d'interrogation : seul le format de la chaîne est mémorisé.

Tableau 78. Entité SQL

Attribut	Description
Sql	Chaîne SQL.
ID construction	Identifie de manière unique la construction dans laquelle le code SQL est apparu
Info de liaison	Informations de liaison pour cette chaîne SQL.
SQL tronqué	Indique si le SQL a été tronqué ou non où : 0 - faux / non, non tronqué 1 - vrai / oui, tronqué

Entité Récepteur de tâche

Indique l'action requise par le récepteur des résultats.

Tableau 79. Entité Récepteur de tâche

Attribut	Description
Action requise	Indique si l'action de signature est requise.

Entité Liste de tâches des résultats de tâche

Indique le statut actuel des résultats.

Tableau 80. Entité Liste de tâches des résultats de tâche

Attribut	Description
Statut	Indique le statut actuel des résultats.
(Transférer à un niveau supérieur) Action requise	Indique si une action de liste des tâches est requise.
Action requise	Indique si l'action de signature est requise.

Entité Modèle

Une entité de modèle CAS est créée pour chaque modèle d'élément dans un ensemble de modèles. Un élément est un fichier spécifique ou un modèle de fichier, une variable d'environnement ou de registre, la sortie d'un script de système d'exploitation ou d'un script SQL ou la liste des utilisateurs connectés.

Tableau 81. Entité Modèle

Attribut	Description
ID modèle	Identificateur unique pour le modèle d'élément dans l'ensemble de tous les modèles d'élément
ID jeu de modèles	Identificateur unique du jeu de modèles.
Nom d'accès	Selon le type d'audit, il s'agit du script de système d'exploitation ou SQL, de la valeur d'environnement ou de registre, d'un nom de fichier ou d'un modèle de nom de fichier
Type d'audit	Type d'élément surveillé
Fréquence d'audit (min.)	Intervalle maximum (en minutes) entre les tests
Utiliser MD5	Indique si la comparaison se fait ou non en calculant une somme de contrôle à l'aide de l'algorithme MD5 et en comparant cette valeur avec la valeur calculée la dernière fois que l'élément a été vérifié. Par défaut, MD5 n'est pas utilisé. Si MD5 est utilisé, mais la taille des données brutes est supérieure à la limite de taille MD5 configurée pour l'hôte CAS, le calcul et la comparaison MD5 sont ignorés. Indépendamment du fait que MD5 soit ou non utilisé, la valeur actuelle du dernier horodatage modifié pour l'élément et la taille de l'élément sont comparées aux valeurs sauvegardées la dernière fois que l'élément a été vérifié.
Sauvegarder des données	Indique si la case Conserver les données a été cochée. Dans l'affirmative, les versions précédentes de l'élément peuvent être comparées à la version actuelle
Modifiable	Indique si ce modèle peut ou non être modifié. Les modèles Guardium par défaut ne peuvent pas être modifiés. En outre, une fois qu'un ensemble de modèles a été utilisé dans une instance CAS, il ne peut pas être modifié. Dans tous les cas, un ensemble de modèles peut toujours être cloné et l'ensemble cloné peut être modifié
Description	Description facultative du modèle
Horodatage	Date et heure de la dernière mise à jour du modèle

ID modèle et ID jeu de modèles sont uniquement disponibles pour les utilisateurs disposant du rôle d'administrateur.

Entité Jeu de modèles

L'entité Jeu de modèles CAS est créée pour chaque jeu de modèles, soit un ensemble d'éléments de modèle pour un système d'exploitation ou une base de données particuliers.

Tableau 82. Entité Jeu de modèles

Attribut	Description
ID jeu de modèles	Identificateur unique pour le jeu de modèles, numéroté séquentiellement
Type de système d'exploitation	Système d'exploitation : Unix ou Windows
Type de base de données	Type de base de données : Oracle, MS-SQL, DB2, Sybase, Informix ou N/A pour un modèle du système d'exploitation
Nom de jeu de modèles	Nom de modèle
IsDefault	Indique si ce modèle est le modèle par défaut pour la combinaison spécifiée du type du système d'exploitation et du type de base de données
Modifiable	Indique si ce modèle peut ou non être modifié. Les modèles Guardium par défaut ne peuvent pas être modifiés. En outre, une fois qu'un ensemble de modèles a été utilisé dans une instance CAS, il ne peut pas être modifié. Dans tous les cas, un ensemble de modèles peut toujours être cloné et l'ensemble cloné peut être modifié
Horodatage	Date et heure de la dernière mise à jour du modèle

ID jeu de modèles est uniquement disponible pour les utilisateurs disposant du rôle d'administrateur.

Entité Résultats de test

Cette entité est créée pour chaque ensemble de résultats de test.

Tableau 83. Entité Résultats de test

Attribut	Description
ID résultat de test	Identifie le résultat de test.
ID résultat d'évaluation	Identifie l'ensemble des résultats d'évaluation.
ID1 test	Identifie le test.
ID test d'évaluation	Identifie le test d'évaluation (tâche).
Résultat du test	Résultat du test renvoyé.
ID résultat de rapport	Identifie le résultat du rapport.
Indicateur de modification de paramètres	Indique si les paramètres ont été modifiés depuis le dernier test.
Texte des résultats	Texte renvoyé par le test.
Description du test	Description issue de la définition de test.
Recommandation	Recommandation renvoyée par le test.
Description du score	Description du résultat.
Chaîne de seuil	Invite de seuil pour le test (par exemple, Nombre maximal d'adresses IP différentes autorisé par utilisateur)
Gravité	Gravité attribuée au résultat du test.
Catégorie	Catégorie attribuée au résultat du test.
ID1 source de données de résultat d'évaluation	Identifie la source de données du résultat de test.
Détails des résultats	Détails du test.
Description de groupe d'exceptions	Description de groupe d'exceptions. Remplie lorsque le test est exécuté.

ID résultat du test, ID résultat d'évaluation et ID test d'évaluation sont uniquement disponibles pour les utilisateurs disposant du rôle d'administrateur.

Entité Détails d'alerte de seuil

Cette entité est créée chaque fois qu'une alerte de corrélation est déclenchée.

Tableau 84. Entité Détails d'alerte de seuil

Attribut	Description
ID Journal des alertes	Identifie de manière unique l'entité des détails d'alerte.
Valeur de requête	Valeur renvoyée par la requête.
Valeur de base	Valeur affectée à l'alerte statistique.
Date de début vérifiée	Date et heure de début vérifiées par la condition d'alerte.
Date de fin vérifiée	Date et heure de fin vérifiées par la condition d'alerte.
Seuil d'alerte	Seuil d'alerte défini pour l'alerte.
Notification envoyée	Texte de la notification envoyée.
Horodatage	Créé une seule fois, lorsque l'alerte statistique est consignée.
Description d'alerte	Description contenue dans la définition d'alerte.

L'ID journal des alertes est uniquement disponible pour les utilisateurs disposant du rôle d'administrateur.

Niveau d'utilisation d'unités

Plusieurs rapports d'utilisation d'unités sont fournis par défaut via Gérer > Rapports > Utilisation d'unités, y compris :

- Utilisation d'unités : affiche le niveau d'utilisation maximum de chaque unité dans la période donnée. Une exploration affiche les détails d'une unité dans toutes les périodes du rapport.
- Distribution de l'utilisation d'unités : pour chaque unité, ce rapport affiche le pourcentage de périodes dans le calendrier du rapport dont les niveaux d'utilisation sont bas, moyens et élevés.
- Seuils d'utilisation : ce rapport prédéfini affiche toutes les valeurs de seuil bas et haut pour tous les paramètres d'utilisation d'unité.
- Récapitulatif quotidien de l'utilisation d'unités - Fournit un résumé quotidien des données d'utilisation d'unité.

En outre, le suivi des Niveaux d'utilisation d'unités permet aux utilisateurs de créer des requêtes et des rapports personnalisés.
Conseil : Activez les alias pour tous les rapports personnalisés et prédéfinis à l'aide des données d'utilisation des unités pour garantir que les niveaux d'utilisation des unités s'affichent en tant que chaînes explicites et non en tant que nombres. Par exemple, faible, moyen et élevé au lieu de 1, 2 ou 3.
La liste d'attributs contient les éléments suivants :

- Nom d'hôte
- Début de la période
- Nombre de redémarrages
- Niveau de nombre de redémarrages
- Mémoire du sniffer
- Niveau de mémoire du sniffer
- Pourcentage de mémoire MySQL
- Niveau de pourcentage de mémoire MySQL
- Espace mémoire tampon disponible
- Niveau d'espace mémoire tampon disponible
- File d'attente de l'analyseur
- Niveau de file d'attente de l'analyseur
- File d'attente du consignateur
- Niveau de file d'attente du consignateur
- Utilisation du disque MySQL
- Niveau d'utilisation du disque MySQL
- Charge de l'UC système
- Niveau de charge de l'UC système
- Utilisation du disque var système
- Niveau d'utilisation du disque var système
- Niveau global d'utilisation des unités
- Nombre de demandes
- Niveau de nombre de demandes
- Nombre de SQL complets
- Niveau de nombre de SQL complets
- Nombre d'exceptions
- Niveau de nombre d'exceptions
- Nombre de violations de politique
- Niveau de nombre de violations de politique
- Nombre de demandes Flat Log
- Niveau de nombre de demandes Flat Log

Remarque : Chaque paramètre possède une valeur et un niveau calculés en fonction de la valeur et des seuils.

Entité Utilisateur

Identifie l'utilisateur Guardium défini comme un récepteur de résultats de processus d'audit.

Tableau 85. Entité Utilisateur

Attribut	Description
Nom de la connexion	Nom d'utilisateur Guardium.
Prénom	Prénom de l'utilisateur Guardium.
Nom	Nom de l'utilisateur Guardium.
Adresse électronique	Adresse électronique définie pour l'utilisateur Guardium.
Dernier actif	Horodatage de la dernière activité de cet utilisateur.

Rubrique parent : Domaines, entités et attributs

Rapports sur les autorisations de base de données

Vous pouvez utiliser les rapports sur les autorisations de base de données pour vérifier que les utilisateurs ont accès uniquement aux données appropriées. Votre système Guardium comprend des rapports sur les autorisations de base de données prédéfinis pour plusieurs types de bases de données.

Remarque : Les rapports d'autorisation de base de données sont des composants facultatifs activés par la clé de produit. Si ces composants n'ont pas été activés, les choix n'apparaissent pas dans les sélections Générateur de domaine personnalisé/Requête de domaine personnalisé/Générateur de table personnalisée.

Les rapports d'autorisation prédéfinis sont répertoriés comme suit. Ils apparaissent en tant que noms de domaine dans les sélections Générateur de domaine personnalisé/Requête de domaine personnalisé/Générateur de table personnalisée :

- Domaines des autorisations de la base de données Oracle
- Domaines des autorisations de la base de données MYSQL

- Domaines des autorisations de la base de données DB2
- Domaines des autorisations de la base de données DB2 for i 6.1 et 7.1
- Domaines des autorisations de la base de données SYBASE
- Domaines des autorisations de la base de données Informix
- Domaines des autorisations de la base de données MSSQL 2000
- Domaines des autorisations de la base de données MSSQL 2005
- Domaines des autorisations de la base de données Netezza
- Domaines des autorisations de la base de données Teradata
- Domaines des autorisations de la base de données PostgreSQL

Voir aussi Optimisation des autorisations.

Autorisation sur la base de données Oracle

Les domaines suivants sont fournis pour faciliter le téléchargement et la génération de rapports sur les Autorisations de la base de données Oracle. Chacun des domaines suivants possède une entité unique (avec le même nom), et il existe un rapport prédéfini pour chaque domaine. Ces domaines sont disponibles dans les sélections Générateur de domaine personnalisé/Requête de domaine personnalisé/Générateur de table personnalisée. Comme pour d'autres entités et rapports prédéfinis, ceux-ci ne peuvent pas être modifiés, mais vous pouvez cloner et personnaliser vos propres versions de ces domaines ou rapports. Pour visualiser les rapports d'autorisation, connectez-vous au portail utilisateur et accédez à l'onglet Autorisations de base de données.

Oracle

- Cptes ORA ALTER SYSTEM - Comptes avec les privilèges ALTER SYSTEM et ALTER SESSION
- Cptes ORA avec BECOME USER - Comptes avec les privilèges BECOME USER
- Tous les privilèges système ORA et option d'administration - Rapport affichant tous les privilèges système et l'option d'administration pour les utilisateurs et les rôles
- Privilège d'accès aux objets et aux colonnes ORA - Privilèges octroyés sur les objets et les colonnes (avec ou sans option d'octroi)
- Accès aux objets ORA par un utilisateur public - Accès aux objets par PUBLIC
- Privilèges sur les objets ORA - Privilèges d'objet par compte de base de données ne figurant pas dans le SYS ni dans un rôle DBA
- Privilège d'exécution ORA par un utilisateur public sur une procédure système - Exécuter un privilège sur les procédures SYS PL/SQL affectées à PUBL
- Rôles ORA octroyés - Rôles octroyés aux utilisateurs et aux rôles
- Privilège système ORA octroyé - Rapport hiérarchique montrant le privilège système octroyé aux utilisateurs, y compris les définitions récursives (c'est-à-dire les privilèges affectés aux rôles, puis ces rôles affectés aux utilisateurs)
- Cptes SYSDBA et SYSOPER ORA - Comptes avec privilèges SYSDBA et SYSOPER

Pour que les autorisations puissent télécharger des données à partir de différentes sources de données, l'exigence générale est que l'ID de connexion utilisé pour accéder à la base de données puisse lire les tables utilisées dans la requête (masquée pour toutes les autorisations).

La liste suivante (contenant l'en-tête de la ligne de commentaire) détaille les privilèges minimaux requis, dans la table de la base de données (ou la vue de la table de la base de données) pour que l'autorisation soit opérationnelle.

/* Le privilège Select sur ces tables/vues est requis */

grant select on sys.dba_tab_privs to sqlguard;

grant select on sys.dba_roles to sqlguard;

grant select on sys.dba_users to sqlguard;

grant select on sys.dba_role_privs to sqlguard;

grant select on sys.dba_sys_privs to sqlguard;

grant select on sys.obj$ to sqlguard;

grant select on sys.user$ to sqlguard;

grant select on sys.objauth$ to sqlguard;

grant select on sys.table_privilege_map to sqlguard;

grant select on sys.dba_objects to sqlguard;

grant select on sys.v_$pwfile_users to sqlguard;

grant select on sys.dba_col_privs to sqlguard;

Autorisation sur la base de données MYSQL

Les domaines suivants sont fournis pour faciliter le téléchargement et la génération de rapports sur les Autorisations de la base de données MYSQL. Chacun des domaines suivants possède une entité unique (avec le même nom), et il existe un rapport prédéfini pour chaque domaine. Ces domaines sont disponibles dans les sélections Générateur de domaine personnalisé/Requête de domaine personnalisé/Générateur de table personnalisée. Comme pour d'autres entités et rapports prédéfinis, ceux-ci ne peuvent pas être modifiés, mais vous pouvez cloner et personnaliser vos propres versions de ces domaines ou rapports. Pour visualiser les rapports d'autorisation, connectez-vous au portail utilisateur et accédez à l'onglet Autorisations de base de données.

MYSQL : les requêtes se terminant par "_40" utilisent la version la plus basique du schéma mysql (pour MySQL 4.0 et au-delà). L'information_schema n'a pas changé depuis qu'il a été introduit dans MySQL 5.0, donc il existe un ensemble de requêtes _50, mais aucune requête _51. Les requêtes _50 sont compatibles avec MySQL 5.0 et 5.1 et pour la version 6.0 lorsqu'elle sera commercialisée, car l'information_schema ne devrait pas changer en version 6.0. Les requêtes se terminant par "_502" (MYSQL502) utilisent la nouvelle information_schema, qui contient beaucoup plus d'informations et ressemble à un véritable dictionnaire de données.

- Privilèges sur la base de données MYSQL 40
- Privilèges d'utilisateur MYSQL 40
- Privilèges d'hôte MYSQL 40
- Privilèges sur la table MYSQL 40

- Privilèges sur la base de données MYSQL 500
- Privilèges d'utilisateur MYSQL 500
- Privilèges d'hôte MYSQL 500
- Privilèges sur la table MYSQL 500
- Privilèges sur la base de données MYSQL 502
- Privilèges d'utilisateur MYSQL 502
- Privilèges d'hôte MYSQL 502
- Privilèges sur la table MYSQL 502

Pour que les autorisations puissent télécharger des données à partir de différentes sources de données, l'exigence générale est que l'ID de connexion utilisé pour accéder à la base de données puisse lire les tables utilisées dans la requête (masquée pour toutes les autorisations).

La liste suivante détaille les privilèges minimaux requis, dans la table de la base de données (ou la vue de la table de la base de données) pour que l'autorisation soit opérationnelle.

Remarque : en plus des privilèges requis, l'utilisateur doit se connecter à la base de données MYSQL pour télécharger les données.

Les requêtes d'autorisation pour toutes les versions MySQL via MySQL 5.0.1 utilisent cet ensemble de tables : mysql.db mysql.host mysql.tables_priv mysql.user

A partir de MySQL 5.0.2, et pour toutes les versions ultérieures, les requêtes d'autorisation utilisent ce jeu de tables : information_schema.SCHEMA_PRIVILEGES mysql.host information_schema.TABLE_PRIVILEGES information_schema.USER_PRIVILEGES

Si une source de données possède un type de base de données MYSQL, mais n'a pas de nom de base de données (voir Définitions de source de données, le nom de la base de données sous Emplacement est vide), les données de téléchargement bouclent à travers toutes les bases de données MYSQL auxquelles l'utilisateur a accès.

Autorisation sur la base de données DB2

Les domaines suivants sont fournis pour faciliter le téléchargement et la génération de rapports sur les Autorisations de la base de données DB2. Chacun des domaines suivants possède une entité unique (avec le même nom), et il existe un rapport prédéfini pour chaque domaine. Ces domaines sont disponibles dans les sélections Générateur de domaine personnalisé/Requête de domaine personnalisé/Générateur de table personnalisée. Comme pour d'autres entités et rapports prédéfinis, ceux-ci ne peuvent pas être modifiés, mais vous pouvez cloner et personnaliser vos propres versions de ces domaines ou rapports. Pour visualiser les rapports d'autorisation, connectez-vous au portail utilisateur et accédez à l'onglet Autorisations de base de données.

- Privilèges de niveau colonne DB2 (SELECT, UPDATE, ETC.)
- Privilèges de niveau base de données DB2 (CONNECT, CREATE, ETC.)
- Privilèges de niveau index DB2 (CONTROL)
- Privilèges de niveau package DB2 (sur les packages de code – BIND, EXECUTE, ETC.)
- Privilèges de niveau table DB2 (SELECT, UPDATE, ETC.) Récapitulatif des privilèges DB2

Pour que les autorisations puissent télécharger des données à partir de différentes sources de données, l'exigence générale est que l'ID de connexion utilisé pour accéder à la base de données puisse lire les tables utilisées dans la requête (masquée pour toutes les autorisations).

La liste suivante (contenant l'en-tête de la ligne de commentaire) détaille les privilèges minimaux requis, dans la table de la base de données (ou la vue de la table de la base de données) pour que l'autorisation soit opérationnelle.

/* Le privilège Select sur ces tables/vues est requis */

GRANT SELECT ON SYSCAT.COLAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.DBAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.INDEXAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.PACKAGEAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.DBAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.TABAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.SCHEMAAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.PASSTHRUAUTH TO SQLGUARD;

Autorisations DB2 z/OS
: Les domaines suivants sont fournis pour faciliter le téléchargement et la génération de rapports sur les Autorisations de la base de données DB2 for z/OS.

Privilèges sur les objets exécutables DB2 zOS octroyés à un utilisateur public

Privilèges sur les objets DB2 zOS octroyés à un utilisateur public

Privilèges système Db2 zOS octroyés au bénéficiaire - V8

Privilèges système Db2 zOS octroyés au bénéficiaire - V9

Privilèges système Db2 zOS octroyés au bénéficiaire - V10 et version ultérieure

Privilèges sur les bases de données Db2 zOS octroyés au bénéficiaire

Privilèges sur les schémas Db2 zOS octroyés au bénéficiaire - V9 et version ultérieure

Privilèges sur les schémas Db2 zOS octroyés au bénéficiaire - V8 uniquement

Ressources de base de données Db2 zOS octroyées à un bénéficiaire

Privilèges sur les objets Db2 zOS octroyés à un bénéficiaire

Privilèges système Db2 zOS octroyés avec l'option GRANT - V8

Privilèges système Db2 zOS octroyés avec l'option GRANT - V9

Privilèges système Db2 zOS octroyés avec l'option GRANT - V10 et version ultérieure

Ressources de base de données Db2 zOS octroyées à un utilisateur public

Privilèges sur les schémas Db2 zOS octroyés à un utilisateur public

Privilèges sur les bases de données Db2 zOS octroyés à un utilisateur public

Privilèges système Db2 zOS octroyés à un utilisateur public - V10 et version ultérieure

Privilèges système Db2 zOS octroyés à un utilisateur public - V9

Privilèges système Db2 zOS octroyés à un utilisateur public - V8

Privilèges sur les objets Db2 zOS octroyés avec l'option GRANT

Ressources de base de données Db2 zOS octroyées avec l'option GRANT

Privilèges sur les schémas Db2 zOS octroyés avec l'option GRANT - V8 uniquement

Privilèges sur les schémas Db2 zOS octroyés avec l'option GRANT - V9 et version ultérieure

Privilèges sur les bases de données Db2 zOS octroyés avec l'option GRANT

Autorisations de la base de données DB2 for i 6.1 et 7.1

Les domaines suivants sont fournis pour faciliter le téléchargement et la génération de rapports sur les Autorisations de la base de données DB2 for i. Chacun des domaines suivants possède une entité unique (avec le même nom), et il existe un rapport prédéfini pour chaque domaine. Ces domaines sont disponibles dans les sélections Générateur de domaine personnalisé/Requête de domaine personnalisé/Générateur de table personnalisée. Comme pour d'autres entités et rapports prédéfinis, ceux-ci ne peuvent pas être modifiés, mais vous pouvez cloner et personnaliser vos propres versions de ces domaines ou rapports. Pour visualiser les rapports d'autorisation, connectez-vous au portail utilisateur et accédez à l'onglet Autorisations de base de données.

Utilisez le script, gdmmonitor-db2-IBMi.sql, pour détailler les privilèges minimaux requis, dans la table de la base de données (ou la vue de la table de la base de données) pour que l'autorisation soit opérationnelle.

Privilèges sur les objets attribués au bénéficiaire (Type d'objet : Schéma, Table, Vue, Package, Routine, séquence, colonne, variable globale et schéma XML)

Privilèges sur les objets attribués à PUBLIC (Type d'objet : Schéma, Table, Vue, Package, Routine, séquence, colonne, variable globale et schéma XML)

Privilèges sur les objets exécutables octroyés à PUBLIC (Type d'objet : package et Routine)

Privilèges sur les objets attribués au bénéficiaire avec GRANT OPTION (Type d'objet : Schéma, Table, Vue, Package, Routine, séquence, colonne, variable globale et schéma XML)

Tous les privilèges d'objet excluent les schémas système par défaut d'un groupe Guardium prédéfini appelé "DB2 for i exclude system schemas - entitlement report". Ajoutez à ce groupe les schémas à exclure.

Autorisations de la base de données SYBASE

Les domaines suivants sont fournis pour faciliter le téléchargement et la génération de rapports sur les Autorisations de la base de données SYBASE. Chacun des domaines suivants possède une entité unique (avec le même nom), et il existe un rapport prédéfini pour chaque domaine. Ces domaines sont disponibles dans les sélections Générateur de domaine personnalisé/Requête de domaine personnalisé/Générateur de table personnalisée. Comme pour d'autres entités et rapports prédéfinis, ceux-ci ne peuvent pas être modifiés, mais vous pouvez cloner et personnaliser vos propres versions de ces domaines ou rapports. Pour visualiser les rapports d'autorisation, connectez-vous au portail utilisateur et accédez à l'onglet Autorisations de base de données.

- Privilège système SYBASE et rôles octroyés à l'utilisateur, y compris l'option d'octroi
- Rôle SYBASE octroyé à l'utilisateur et privilèges système octroyés à l'utilisateur et rôle incluant l'option d'octroi
- Accès aux objets SYBASE par le public
- Privilège d'exécution SYBASE sur les fonctions de procédure, octroyé à un utilisateur public
- Comptes SYBASE disposant de rôles d'administrateur système ou de la sécurité
- Privilège sur les objets et les colonnes SYBASE octroyé avec l'option d'octroi
- Rôle SYBASE octroyé à l'utilisateur

Pour que les autorisations puissent télécharger des données à partir de différentes sources de données, l'exigence générale est que l'ID de connexion utilisé pour accéder à la base de données puisse lire les tables utilisées dans la requête (masquée pour toutes les autorisations).

La liste suivante (contenant l'en-tête de la ligne de commentaire) détaille les privilèges minimaux requis, dans la table de la base de données (ou la vue de la table de la base de données) pour que l'autorisation soit opérationnelle.

/* Le privilège Select sur ces tables/vues est requis */

/* Requis sur la base de données MASTER */

grant select on master.dbo.sysloginroles to sqlguard

grant select on master.dbo.syslogins to sqlguard

grant select on master.dbo.syssrvroles to sqlguard

/*Requis sur toutes les bases de données, y compris MASTER */

grant select on sysprotects to sqlguard

grant select on sysusers to sqlguard

grant select on sysobjects to sqlguard

grant select on sysroles to sqlguard

Si une source de données possède un type de base de données SYBASE, mais n'a pas de nom de base de données (voir Définitions de source de données, le nom de la base de données sous Emplacement est vide), les données de téléchargement bouclent à travers toutes les bases de données SYBASE auxquelles l'utilisateur a accès.

Autorisations de la base de données SYBASE

Version prise en charge : sybase IQ 15 et version supérieure.

La définition de table personnalisée suivante est créée pour télécharger des données : (vous pouvez ignorer l'identifiant).

139 | Privilèges sur les objets SybaseIQ15 par utilisateur de base de données

140 | Privilèges sur les objets SybaseIQ15 par groupe

141 | Droit système et groupe octroyé à un utilisateur

142 | Droit système SybaseIQ15 et groupe octroyé à un utilisateur ou un groupe

143 | Accès aux objets SybaseIQ15 par un utilisateur public

144 | Privilège d'exécution SybaseIQ15 sur les fonctions de procédure à un utilisateur public

145 | Groupe d'utilisateurs SybaseIQ15 disposant d'autorisations d'administrateur de base de données, etc.

146 | Privilège d'accès aux vues de table SybaseIQ15 octroyé avec l'option Octroyer

147 | Groupe SybaseIQ15 octroyé à un utilisateur et un groupe

148 | Politique de connexion SybaseIQ15 pour un groupe d'utilisateurs avec un nom de connexion

Les requêtes/rapports correspondants sont les suivants : (vous pouvez ignorer l'identifiant.)

597 | Privilèges sur les objets SybaseIQ15 par utilisateur de base de données

598 | Privilèges sur les objets SybaseIQ15 par groupe

599 | Droit système et groupe octroyé à un utilisateur

600 | Droit système SybaseIQ15 et groupe octroyé à des utilisateurs et des groupes

601 | Accès aux objets SybaseIQ15 par un utilisateur public

602 | Privilèges d'exécution SybaseIQ15 sur les procédures et les fonctions octroyés à un utilisateur public

603 | Groupe d'utilisateurs SybaseIQ15 disposant d'autorisations d'administrateur de base de données/d'administrateur/de droits d'accès sur une base de données distante

604 | Privilège d'accès aux vues de table SybaseIQ15 octroyé avec l'option GRANT

605 | Groupe SybaseIQ15 octroyé à un utilisateur et un groupe

606 | Politique de connexion SybaseIQ15 pour un utilisateur et un groupe avec le paramètre d'option de connexion

Ils se trouvent sous les autorisations de base de données avec les autres.

==========

Description de chaque privilège - certains sont explicites, certains peuvent nécessiter quelques explications supplémentaires :

1 /*

Privilèges sur les objets par utilisateur de base de données.

Les objets sont la table, les vues, la procédure et les fonctions.

Il s'agit des privilèges accordés aux utilisateurs uniquement, à l'exclusion du groupe ou de l'appartenance à un groupe.

*/

2. /*

Privilèges sur les objets par groupe.

Les objets sont la table, les vues, la procédure et les fonctions.

Il s'agit de privilèges octroyés au groupe uniquement.

*/

3 /* Droit système et groupe octroyé aux utilisateurs.

*/

4 /* Droit système et groupe octroyé à des utilisateurs et des groupes

*/

5 /* accès aux objets par un utilisateur public.

Y compris les tables, les vues, les fonctions et les procédures

*/

6 /* Privilège d'exécution sur les procédures et les fonctions octroyé à PUBLIC :

*/

7 /* Utilisateurs et groupes avec droits d'accès à une base de données Administrateur de base de données, Administrateur d'autorisations, Administrateur ou Administrateur de base de données distant.

*/

8 /* Les privilèges sur les tables et les vues sont accordés avec une option d'octroi aux utilisateurs et aux groupes.

Notez qu'il s'agit du seul type d'option d'octroi autorisé dans Sybase IQ. Les routines ne peuvent pas être octroyées avec une option d'octroi.

*/

9 /* Groupe octroyé aux utilisateurs et au groupe.

*/

10 /* Politique de connexion affectée à l'utilisateur et au groupe avec le paramètre d'option de connexion */

Utilisation de GuardAPI pour ajouter une source de données aux rapports Sybase IQ

Utilisation de GuardAPI pour ajouter une source de données à chacun des rapports Sybase IQ et exécuter le rapport.

Consultez les exemples ci-dessous sur la façon d'ajouter une source de données à chacun des nouveaux rapports, puis d'exécuter chaque rapport.

Ajouter une source de données à TOUS les rapports d'autorisation SybaseIQ

grdapi create_datasource type="Sybase IQ" user=ent password=Guardium123 host=9.70.144.152 name="SybaseIQ15 entitlement6" shared=true owner=admin application=CustomDomain port=2638 dbName=sn5qpuff

Ajouter une source de données à TOUS les rapports d'autorisation SybaseIQ

grdapi create_datasourceRef_by_name application=CustomTables objName="Privilège d'exécution SybaseIQ15 sur les fonctions de procédure à un utilisateur public"datasourceName="SybaseIQ15 entitlement 6"

grdapi create_datasourceRef_by_name application=CustomTablesobjName="Groupe SybaseIQ15 octroyé à un utilisateur et un groupe" datasourceName="SybaseIQ15 entitlement 6"

grdapi create_datasourceRef_by_name application=CustomTablesobjName="Politique de connexion SybaseIQ15 pour un groupe d'utilisateurs avec un nom de connexion"datasourceName="SybaseIQ15 entitlement 6"

grdapi create_datasourceRef_by_name application=CustomTablesobjName="Accès aux objets SybaseIQ15 par un utilisateur public" datasourceName="SybaseIQ15 entitlement 6"

grdapi create_datasourceRef_by_name application=CustomTablesobjName="Privilèges sur les objets SybaseIQ15 par utilisateur de base de données" datasourceName="SybaseIQ15 entitlement 6"

grdapi create_datasourceRef_by_name application=CustomTablesobjName="Privilèges sur les objets SybaseIQ15 par groupe" datasourceName="SybaseIQ15 entitlement 6"

grdapi create_datasourceRef_by_name application=CustomTablesobjName="Droit système et groupe octroyé à un utilisateur"datasourceName="SybaseIQ15 entitlement 6"

grdapi create_datasourceRef_by_name application=CustomTablesobjName="Droit système SybaseIQ15 et groupe octroyé à un utilisateur ou un groupe"datasourceName="SybaseIQ15 entitlement 6"

grdapi create_datasourceRef_by_name application=CustomTablesobjName="Privilège d'accès aux vues de table SybaseIQ15 octroyé avec l'option Octroyer"datasourceName="SybaseIQ15 entitlement 6"

grdapi create_datasourceRef_by_name application=CustomTablesobjName="Groupe d'utilisateurs SybaseIQ15 disposant d'autorisations d'administrateur de base de données, etc."datasourceName="SybaseIQ15 entitlement 6"

Exécuter TOUS les rapports d'autorisation SybaseIQ

grdapi upload_custom_data tableName=SYBASEIQ15_EXEC_PRIV_ON_PROC_FUNC_TO_PUBLIC

grdapi upload_custom_data tableName=SYBASEIQ15_GROUP_GRANTED_TO_USER_AND_GROUP

grdapi upload_custom_data tableName=SYBASE_OBJ_COL_PRIVS_GRANTED_WITH_GRAN

grdapi upload_custom_data tableName=SYBASEIQ15_OBJECT_ACCESS_BY_PUBLIC

grdapi upload_custom_data tableName=SYBASEIQ15_OBJECT_PRIVS_BY_DB_USER

grdapi upload_custom_data tableName=SYBASEIQ15_OBJECT_PRIVILEGES_BY_GROUP

grdapi upload_custom_data

tableName=SYBASEIQ15_SYSTEM_AUTHORITY_AND_GROUP_GRANTED_TO_USER grdapi upload_custom_data

tableName=SYBASEIQ15_SYSTEM_AUTHORITY_AND_GROUP_GRANTED_TO_USER_AND_GROUP grdapi upload_custom_data

tableName=SYBASEIQ15_TABLE_VIEWS_PRIV_GRANTED_WITH_GRANT grdapi upload_custom_data

tableName=SYBASEIQ15_USER_GROUP_WITH_DBA_PERMS_ADMIN_ETC

Autorisation sur la base de données Informix

Les domaines suivants sont fournis pour faciliter le téléchargement et la génération de rapports sur les Autorisations sur la base de données Informix. Chacun des domaines suivants possède une entité unique (avec le même nom), et il existe un rapport prédéfini pour chaque domaine. Ces domaines sont disponibles dans les sélections Générateur de domaine personnalisé/Requête de domaine personnalisé/Générateur de table personnalisée. Comme pour d'autres entités et rapports prédéfinis, ceux-ci ne peuvent pas être modifiés, mais vous pouvez cloner et personnaliser vos propres versions de ces domaines ou rapports. Pour visualiser les rapports d'autorisation, connectez-vous au portail utilisateur et accédez à l'onglet Autorisations de base de données.

- Privilèges Informix sur les objets par compte de base de données, à l'exclusion du compte et des rôles système
- Privilèges de niveau de base de données Informix, rôles et langue octroyés à l'utilisateur, y compris l'option d'octroi
- Privilèges de niveau base de données Informix, rôles et langue octroyés à l'utilisateur et au rôle, y compris l'option d'octroi
- Octroi sur les objets Informix accordé à un utilisateur public
- Privilège d'exécution Informix sur procédure et fonction Informix, octroyé au public
- Compte Informix disposant de privilèges d'administrateur de base de données Privilèges Informix sur les objets et les colonnes octroyés avec l'option d'octroi
- Rôle Informix octroyé à un utilisateur et un rôle

Pour que les autorisations puissent télécharger des données à partir de différentes sources de données, l'exigence générale est que l'ID de connexion utilisé pour accéder à la base de données puisse lire les tables utilisées dans la requête (masquée pour toutes les autorisations). La liste suivante (contenant l'en-tête de la ligne de commentaire) détaille les privilèges minimaux requis, dans la table de la base de données (ou la vue de la table de la base de données) pour que l'autorisation soit opérationnelle.

/* Le privilège Select sur ces tables/vues est requis */

Étant donné que tous les utilisateurs disposent de privilèges suffisants pour les privilèges SELECT du catalogue système, il n'est pas nécessaire d'octroyer un privilège à un utilisateur. Informix ne préconise pas l'octroi de privilèges sur le catalogue système aux utilisateurs. L'octroi ci-dessous devrait être utilisé.Mais dans ce cas, ils ne sont pas obligatoires.

grant select on systables to sqlguard;

grant select on systabauth to sqlguard;

grant select on sysusers to sqlguard;

grant select on sysroleauth to sqlguard;

grant select on syslangauth to sqlguard;

grant select on sysroutinelangs to sqlguard;

grant select on sysprocauth to sqlguard;

grant select on sysprocedures to sqlguard;

grant select on syscolauth to sqlguard;

Si une source de données possède un type de base de données Informix, mais n'a pas de nom de base de données (voir Définitions de source de données, le nom de la base de données sous Emplacement est vide), les données de téléchargement bouclent à travers toutes les bases de données Informix auxquelles l'utilisateur a accès.

Autorisation sur la base de données MSSQL 2000

Les domaines suivants sont fournis pour faciliter le téléchargement et la génération de rapports sur les Autorisations sur la base de données MSSQL 2000. Chacun des domaines suivants possède une entité unique (avec le même nom), et il existe un rapport prédéfini pour chaque domaine. Ces domaines sont disponibles dans les sélections Générateur de domaine personnalisé/Requête de domaine personnalisé/Générateur de table personnalisée. Comme pour d'autres entités et rapports prédéfinis, ceux-ci ne peuvent pas être modifiés, mais vous pouvez cloner et personnaliser vos propres versions de ces domaines ou rapports. Pour visualiser les rapports d'autorisation, connectez-vous au portail utilisateur et accédez à l'onglet **Autorisations de base de données**.

- Privilèges sur les objets MSSQL2000 par compte de base de données, n'incluant pas l'utilisateur système par défaut
- Privilèges de rôle/système MSSQL2000 octroyés à un utilisateur y compris l'option d'octroi
- Rôle MSSQL2000 octroyé à un utilisateur et un rôle Privilèges système octroyés à un utilisateur et un rôle y compris l'option d'octroi
- Accès aux objets MSSQL2000 par un utilisateur public
- Privilèges d'exécution MSSQL2000 sur les procédures et fonctions système, octroyés à PUBLIC
- Comptes de base de données MSSQL2000 avec les rôles db_owner et db_securityadmin
- Compte de serveur MSSQL2000 avec les rôles sysadmin, serveradmin et security admin /* exécution de cette autorisation sur la base de données MASTER uniquement */
- Privilèges sur les objets et les colonnes MSSQL2000 octroyés avec l'option d'octroi
- Rôle MSSQL2000 octroyé à un utilisateur et un rôle

Pour que les autorisations puissent télécharger des données à partir de différentes sources de données, l'exigence générale est que l'ID de connexion utilisé pour accéder à la base de données puisse lire les tables utilisées dans la requête (masquée pour toutes les autorisations).

La liste suivante (contenant l'en-tête de la ligne de commentaire) détaille les privilèges minimaux requis, dans la table de la base de données (ou la vue de la table de la base de données) pour que l'autorisation soit opérationnelle.

/* Le privilège Select sur ces tables/vues est requis */

/* Requis sur la base de données MASTER */

grant select on dbo.syslogins to sqlguard

/*Requis sur toutes les bases de données, y compris MASTER */

grant select on dbo.sysprotects to sqlguard

grant select on dbo.sysusers to sqlguard

grant select on dbo.sysobjects to sqlguard

grant select on dbo.sysmembers to sqlguard

Si une source de données possède un type de base de données MSSQL, mais n'a pas de nom de base de données (voir Définitions de source de données, le nom de la base de données sous Emplacement est vide), les données de téléchargement bouclent à travers toutes les bases de données MSSQL auxquelles l'utilisateur a accès.

Autorisation sur la base de données MSSQL 20005/2008

Les domaines suivants sont fournis pour faciliter le téléchargement et la génération de rapports sur les Autorisations sur la base de données MSSQL 2005 ou MSSQL 2008. Chacun des domaines suivants possède une entité unique (avec le même nom), et il existe un rapport prédéfini pour chaque domaine. Ces domaines sont disponibles dans les sélections Générateur de domaine personnalisé/Requête de domaine personnalisé/Générateur de table personnalisée. Comme pour d'autres entités et rapports prédéfinis, ceux-ci ne peuvent pas être modifiés, mais vous pouvez cloner et personnaliser vos propres versions de ces domaines ou rapports. Pour visualiser les rapports d'autorisation, connectez-vous au portail utilisateur et accédez à l'onglet **Autorisations de base de données**.

Remarque : Les domaines d'autorisation pour MSSQL2005 répertoriés ci-dessous couvrent également MSSQL2008.
Remarque : Les objets dans les chaînes de requête dynamique NE sont PAS affichées dans xxx_DEPENDENCIES. Un objet dans une chaîne SQL EXECUTE IMMEDIATE appelée par une unité de programme stockée ne montre pas de dépendance. Cette requête exclut le propriétaire du schéma défini dans le groupe ID 202 "Dependencies_exclude_schema-MSSQL". L'utilisateur a la possibilité d'ajouter ou de soustraire le nom du schéma dans ce groupe pour la requête des dépendances.

- Privilèges sur les objets MSSQL2005/8 par compte de base de données, n'incluant pas l'utilisateur système par défaut
- Privilèges de rôle/système MSSQL2005/8 octroyés à un utilisateur
- Privilège de rôle/système MSSQL2005/8 octroyé à un utilisateur et un rôle y compris l'option d'octroi
- Accès aux objets MSSQL2005/8 par PUBLIC
- Privilèges d'exécution MSSQL2005/8 sur les procédures et fonctions système, octroyés à PUBLIC
- Comptes de base de données MSSQL2005/8 avec les rôles db_owner et db_securityadmin
- Compte de serveur MSSQL2005/8 avec les rôles sysadmin, serveradmin et security admin /* exécution uniquement sur la base de données MASTER */
- Privilèges sur les objets et les colonnes MSSQL2005/8 octroyés avec l'option d'octroi
- Rôle MSSQL2005/8 octroyé à un utilisateur et un rôle

Pour que les autorisations puissent télécharger des données à partir de différentes sources de données, l'exigence générale est que l'ID de connexion utilisé pour accéder à la base de données puisse lire les tables utilisées dans la requête (masquée pour toutes les autorisations).

La liste suivante (contenant l'en-tête de la ligne de commentaire) détaille les privilèges minimaux requis, dans la table de la base de données (ou la vue de la table de la base de données) pour que l'autorisation soit opérationnelle.

/* Le privilège Select sur ces tables/vues est requis */

/* Requis sur la base de données MASTER */

grant select on sys.server_principals to sqlguard

/*Requis sur toutes les bases de données, y compris MASTER */

grant select on sys.database_permissions to sqlguard

grant select on sys.database_principals to sqlguard

grant select on sys.all_objects to sqlguard

grant select on sys.database_role_members to sqlguard

grant select on sys.columns to sqlguard

Si une source de données possède un type de base de données MSSQL, mais n'a pas de nom de base de données (voir Définitions de source de données, le nom de la base de données sous Emplacement est vide), les données de téléchargement bouclent à travers toutes les bases de données MSSQL auxquelles l'utilisateur a accès.

Autorisation sur la base de données Netezza

Les domaines suivants sont fournis pour faciliter le téléchargement et la génération de rapports sur les Autorisations sur la base de données Netezza. Chacun des domaines suivants possède une entité unique (avec le même nom), et il existe un rapport prédéfini pour chaque domaine. Ces domaines sont disponibles dans les sélections Générateur de domaine personnalisé/Requête de domaine personnalisé/Générateur de table personnalisée. Comme pour d'autres entités et rapports prédéfinis, ceux-ci ne peuvent pas être modifiés, mais vous pouvez cloner et personnaliser vos propres versions de ces domaines ou rapports. Pour visualiser les rapports d'autorisation, connectez-vous au portail utilisateur et accédez à l'onglet **Autorisations de base de données**.

Remarque : il n'existe pas de traduction de texte d'erreur de base de données pour Netezza. L'erreur apparaît dans la description d'exception. Les utilisateurs peuvent cloner/ajouter un rapport avec la description d'exception pour Netezza au besoin.

- Privilèges sur les objets Netezza par nom d'utilisateur de base de données - Privilèges sur les objets avec ou sans option d'octroi par nom d'utilisateur de base de données à l'exclusion du compte ADMIN.
- Privilèges d'administrateur Netezza par nom d'utilisateur de base de données - Privilèges d'administration avec ou sans option d'octroi par nom d'utilisateur de base de données à l'exclusion du compte ADMIN.
- Groupe/Rôle Netezza octroyé à un utilisateur - Groupe (Rôle) octroyé à l'utilisateur
- Privilèges sur les objets Netezza par groupe - Privilèges sur les objets avec ou sans option d'octroi par GROUP, à l'exclusion du compte PUBLIC.
- Privilèges d'administrateur Netezza par groupe - Privilèges d'administrateur avec ou sans option d'octroi par GROUP, à l'exclusion du compte PUBLIC.
- Privilèges d'administrateur Netezza par nom d'utilisateur de base de données, groupe - Privilèges d'administration avec ou sans option d'octroi par nom d'utilisateur de base de données à l'exclusion du compte ADMIN et le groupe PUBLIC.
- Privilèges sur les objets Netezza octroyés - Les privilèges sur les objets octroyés avec ou sans option d'octroi à PUBLIC.
- Privilèges d'administrateur Netezza octroyés - Les privilèges d'administrateur octroyés avec ou sans option d'octroi à PUBLIC.
- Privilège d'administrateur global Netezza octroyé à des utilisateurs et des groupes - Privilège d'administrateur global octroyé à des utilisateurs et des groupes à l'exclusion du compte ADMIN.
- Privilège d'accès global aux objets Netezza octroyé à des utilisateurs et des groupes - Privilège d'accès global aux objets octroyé à des utilisateurs et des groupes à l'exclusion du compte ADMIN.

Pour que les autorisations puissent télécharger des données à partir de différentes sources de données, l'exigence générale est que l'ID de connexion utilisé pour accéder à la base de données puisse lire les tables utilisées dans la requête (masquée pour toutes les autorisations).

La liste suivante (contenant l'en-tête de la ligne de commentaire) détaille les privilèges minimaux requis, dans la table de la base de données (ou la vue de la table de la base de données) pour que l'autorisation soit opérationnelle.

/* Le privilège Select sur ces tables/vues est requis */

/* Ce script doit être exécuté à partir de la base de données système */

GRANT SELECT ON SYSTEM VIEW TO sqlguard;

GRANT LIST ON DATABASE TO sqlguard;

GRANT LIST ON USER TO sqlguard;

GRANT LIST ON GROUP TO sqlguard;

GRANT SELECT ON _V_CONNECTION TO sqlguard;

Pour les requêtes d'autorisation Netezza, il est recommandé de se connecter à la base de données SYSTEM, notamment en octroyant le privilège à l'utilisateur qui va exécuter ces rapports. Le privilège d'octroi DOIT être effectif dans la base de données SYSTEM ou le privilège octroyé sera effectif sur une seule base de données. Lorsque le privilège accordé est effectif à partir de la base de données SYSTEM, une fonctionnalité spéciale permet au privilège octroyé d'être transmis à toutes les bases de données.

Autorisations sur la base de données Teradata

Les domaines suivants sont fournis pour faciliter le téléchargement et la génération de rapports sur les Autorisations sur la base de données Teradata. Chacun des domaines suivants possède une entité unique (avec le même nom), et il existe un rapport prédéfini pour chaque domaine. Ces domaines sont disponibles dans les sélections Générateur de domaine personnalisé/Requête de domaine personnalisé/Générateur de table personnalisée. Comme pour d'autres entités et rapports prédéfinis, ceux-ci ne peuvent pas être modifiés, mais vous pouvez cloner et personnaliser vos propres versions de ces domaines ou rapports. Pour visualiser les rapports d'autorisation, connectez-vous au portail utilisateur et accédez à l'onglet **Autorisations de base de données**.

- Privilèges sur les objets Teradata par compte de base de données, n'incluant pas les utilisateurs système par défaut
- Privilèges et rôles système Teradata octroyés aux utilisateurs y compris l'option d'octroi.
- Rôles Teradata octroyés aux utilisateurs et aux rôles y compris l'option d'octroi.
- Rôle Teradata octroyé aux utilisateurs et aux rôles.Privilèges système octroyés aux utilisateurs et aux rôles y compris l'option d'octroi.
- Privilèges sur les objets et systèmes Teradata octroyés à public. Remarque : le rôle ne peut être octroyé au public dans Teradata.
- Privilèges d'exécution Teradata sur des objets de base de données système octroyés à un utilisateur public
- Privilèges d'administrateur système et de sécurité Teradata octroyés à un utilisateur et un rôle.
  Remarque : Le rôle d'administrateur système ou de sécurité n'existe pas dans Teradata. L'utilisateur doit créer ses propres rôles. Les privilèges système suivants ne sont normalement pas accordés à un utilisateur standard : ABORT SESSION, CREATE DATABASE, CREATE PROFILE, CREATE ROLE,CREATE USER, DROP DATABASE, DROP PROFILE, DROP ROLE, DROP USER, MONITOR RESOURCE, MONITOR SESSION, REPLICATION OVERRIDE, SET SESSION RATE, SET RESOURCE RATE.
- Privilèges sur les objets Teradata octroyés avec l'option d'octroi aux utilisateurs. A l'exclusion de DBC et du bénéficiaire = 'All'.

Pour que les autorisations puissent télécharger des données à partir de différentes sources de données, l'exigence générale est que l'ID de connexion utilisé pour accéder à la base de données puisse lire les tables utilisées dans la requête (masquée pour toutes les autorisations).

La liste suivante (contenant l'en-tête de la ligne de commentaire) détaille les privilèges minimaux requis, dans la table de la base de données (ou la vue de la table de la base de données) pour que l'autorisation soit opérationnelle.

/* Le privilège Select sur ces tables/vues est requis */

GRANT SELECT ON DBC.AllRights TO sqlguard;

GRANT SELECT ON DBC.Tables TO sqlguard;

GRANT SELECT ON DBC.AllRoleRights TO sqlguard;

GRANT SELECT ON DBC.RoleMembers TO sqlguard;

Autorisation sur la base de données PostgreSQL

Les domaines suivants sont fournis pour faciliter le téléchargement et la génération de rapports sur les Autorisations sur la base de données PostgreSQL. Chacun des domaines suivants possède une entité unique (avec le même nom), et il existe un rapport prédéfini pour chaque domaine. Ces domaines sont disponibles dans les sélections Générateur de domaine personnalisé/Requête de domaine personnalisé/Générateur de table personnalisée. Comme pour d'autres entités et rapports prédéfinis, ceux-ci ne peuvent pas être modifiés, mais vous pouvez cloner et personnaliser vos propres versions de ces domaines ou rapports. Pour visualiser les rapports d'autorisation, connectez-vous au portail utilisateur et accédez à l'onglet **Autorisations de base de données**.

Il existe sept domaines/requêtes/rapports personnalisés d'autorisation pour PostgreSQL. Il s'agit des éléments suivants (chacun est répertorié avec le nom du rapport, la description, la note) :

- Privilèges PostgreSQL sur les bases de données octroyés au rôle utilisateur public avec ou sans option GRANT Privilège sur les bases de données octroyé au public, à l'utilisateur et au rôle, avec ou sans option d'octroi. A exécuter sur n'importe quelle base de données, idéalement PostgreSQL.
- Privilège PostgreSQL sur la langue octroyé au rôle utilisateur public avec ou sans option GRANT. Privilège sur la langue octroyé au public, à l'utilisateur et au rôle, avec ou sans option d'octroi. A exécuter pour chaque base de données.
- Privilège PostgreSQL sur le schéma octroyé au rôle utilisateur public avec ou sans option GRANT. Privilège sur le schéma octroyé au public, à l'utilisateur et au rôle, avec ou sans option d'octroi. A exécuter pour chaque base de données.
- Privilège PostgreSQL sur l'espace de table octroyé au rôle utilisateur public avec ou sans option GRANT. Privilège sur l'espace de table octroyé au public, à l'utilisateur et au rôle, avec ou sans option d'octroi. A exécuter sur n'importe quelle base de données, idéalement PostgreSQL.
- Rôle ou utilisateur PostgreSQL octroyé à un utilisateur ou un rôle. Rôle ou utilisateur octroyé à un utilisateur ou un rôle, y compris l'option d'octroi. A exécuter une fois dans une base de données. De préférence PostgreSQL.
- Privilège de superutilisateur PostgreSQL octroyé à un utilisateur ou un rôle. Privilège de superutilisateur octroyé à un utilisateur ou un rôle. A exécuter une fois dans une base de données. De préférence PostgreSQL.
- Privilèges système PostgreSQL octroyés à un utilisateur et un rôle. Privilèges système octroyés à un utilisateur et un rôle. A exécuter une fois dans une base de données. De préférence PostgreSQL.
- Privilèges PostgreSQL sur les séquences et les fonctions de la vue de table octroyés à un utilisateur public. Privilèges sur les tables, vues, séquences et fonctions octroyés à un utilisateur public. A exécuter pour chaque base de données. A exécuter pour chaque base de données.
- Privilèges PostgreSQL sur les séquences et les fonctions de la vue de table octroyés avec l'option GRANT. Privilèges sur les tables, vues, séquences et fonctions octroyés à un utilisateur et un rôle avec l'option d'octroi uniquement. A l'exclusion du compte PostgreSQL.
- Privilèges PostgreSQL sur les séquences et les fonctions de la vue de table octroyés aux rôles. Privilèges sur les tables, vues, séquences et fonctions octroyés aux rôles.A l'exclusion du public. A exécuter pour chaque base de données.
- Privilèges PostgreSQL sur les séquences et les fonctions de la vue de table octroyés à un nom de connexion. Privilèges sur les tables, vues, séquences et fonctions octroyés aux noms de connexion. A l'exclusion de l'utilisateur système postgres. A exécuter pour chaque base de données.

Remarque : à partir de la version 8.3.6, PostgreSQL ne prend pas en charge l'option d'octroi administrateur au public. Uniquement sur les fonctions, à l'exclusion des procédures mémorisées. Aucun support pour l'octroi sur les colonnes, uniquement l'octroi sur la table. Public est un groupe, et non un utilisateur. Public n'apparaît dans pg_roles. Les seuls privilèges qui doivent exécuter toutes ces requêtes sont : GRANT CONNECT ON DATABASE PostgreSQL TO username;

Pour que les autorisations puissent télécharger des données à partir de différentes sources de données, l'exigence générale est que l'ID de connexion utilisé pour accéder à la base de données puisse lire les tables utilisées dans la requête (masquée pour toutes les autorisations).

La liste suivante (contenant l'en-tête de la ligne de commentaire) détaille les privilèges minimaux requis, dans la table de la base de données (ou la vue de la table de la base de données) pour que l'autorisation soit opérationnelle.

/* Le privilège Select sur ces tables/vues est requis */

/*Requis sur la base de données POSTGRES*/

grant connect on database postgres to sqlguard;

/*Requis sur toutes les bases de données, y compris POSTGRES (déjà octroyés par défaut à PUBLIC) * / */

grant select on pg_class to sqlguard;

grant select on pg_namespace to sqlguard;

grant select on pg_roles to sqlguard;

grant select on pg_proc to sqlguard;

grant select on pg_auth_members to sqlguard;

grant select on pg_language to sqlguard;

grant select on pg_tablespace to sqlguard;

grant select on pg_database to sqlguard;

Si une source de données possède un type de base de données PostgreSQL, mais n'a pas de nom de base de données (voir Définitions de source de données, le nom de la base de données sous Emplacement est vide), les données de téléchargement bouclent à travers toutes les bases de données PostgreSQL auxquelles l'utilisateur a accès.

Rubrique parent : Domaines, entités et attributs

Exploitation des rapports prédéfinis

Au lieu de créer des rapports personnalisés ex nihilo, bénéficiez des contenus prédéfinis dans l'application Guardium.

Obtenez les informations que vous recherchez plus rapidement en accédant à des rapports prédéfinis disponibles dans l'application Guardium. Ces rapports prédéfinis peuvent être clonés et personnalisés selon les besoins de l'utilisateur.

L'utilisation des rapports prédéfinis de Guardium est une pratique recommandée qui permet aux organisations d'identifier rapidement et facilement les risques de sécurité, tels que les objets exposés de manière inappropriée, les utilisateurs disposant de droits excessifs et des actions administratives non autorisées. Voici quelques exemples des nombreux rapports prédéfinis : comptes avec privilèges système, tous les privilèges système et administrateur, répertoriés par utilisateur et rôle, privilèges sur les objets par utilisateur et tous les objets avec accès public.

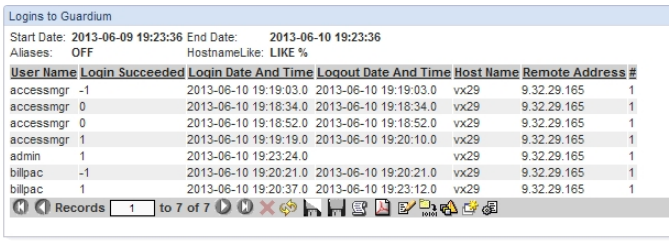
Tous les paramètres et toutes les valeurs sont affichés sur tous les rapports. Les paramètres et les valeurs peuvent être édités à l'aide du bouton Personnaliser dans n'importe quel écran de rapport.

Plusieurs exemples de rapport sont décrits ci-dessous.

Connexions à Guardium

Toutes les valeurs de ce rapport proviennent de l'entité Connexions à Guardium. Pour la période de rapport, chaque ligne du rapport répertorie les informations suivantes : Nom d'utilisateur, Connexion réussie (1= Réussite, 0= Echec, -1= mot de passe expiré, -2= connexion à partir d'une adresse IP différente), Date et heure de connexion, Date et heure de déconnexion (vide si l'utilisateur ne s'est pas encore déconnecté), Nom d'hôte, Adresse distante (de l'utilisateur) et nombre de connexions pour la ligne.

Emplacement du rapport : Rapports > Surveillance du système Guardium > Connexions à Guardium


Logins to Guardium

Start Date: 2013-06-09 19:23:36 End Date: 2013-06-10 19:23:36
Aliases: OFF HostnameLike: LIKE %

User Name	Login Succeeded	Login Date And Time	Logout Date And Time	Host Name	Remote Address	#
accessmgr	-1	2013-06-10 19:19:03.0	2013-06-10 19:19:03.0	vx29	9.32.29.165	1
accessmgr	0	2013-06-10 19:18:34.0	2013-06-10 19:18:34.0	vx29	9.32.29.165	1
accessmgr	0	2013-06-10 19:18:52.0	2013-06-10 19:18:52.0	vx29	9.32.29.165	1
accessmgr	1	2013-06-10 19:19:19.0	2013-06-10 19:20:10.0	vx29	9.32.29.165	1
admin	1	2013-06-10 19:23:24.0		vx29	9.32.29.165	1
billpac	-1	2013-06-10 19:20:21.0	2013-06-10 19:20:21.0	vx29	9.32.29.165	1
billpac	1	2013-06-10 19:20:37.0	2013-06-10 19:23:12.0	vx29	9.32.29.165	1

Records 1 to 7 of 7

Tableau 1. Connexions à Guardium

Domaine	Requête de base	Entité principale
Connexions à Guardium	Connexions à Guardium	Connexion des utilisateurs Guardium
Paramètre d'exécution	Opérateur	Valeur par défaut
Nom d'hôte	LIKE	%
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Moniteur d'utilisation de la mémoire tampon

Fournit un ensemble étendu de statistiques d'utilisation des mémoires tampon.

Emplacement du rapport : Rapports > Rapports opérationnels Guardium > Utilisation de la mémoire tampon d'entreprise

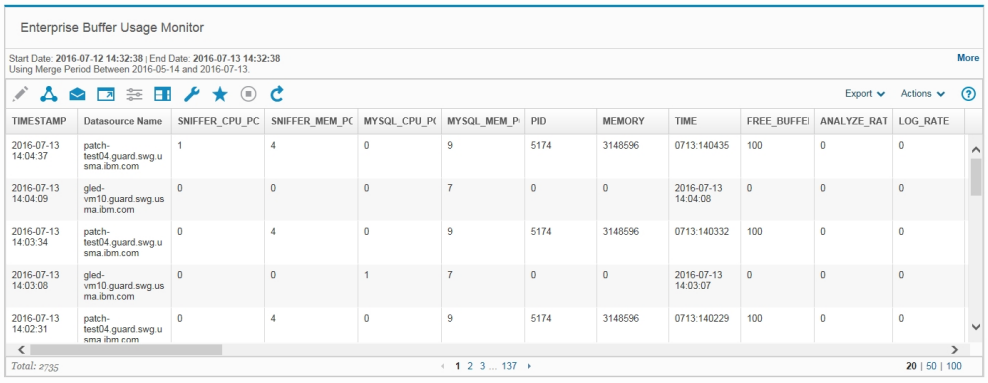


Tableau 2. Moniteur d'utilisation de la mémoire tampon

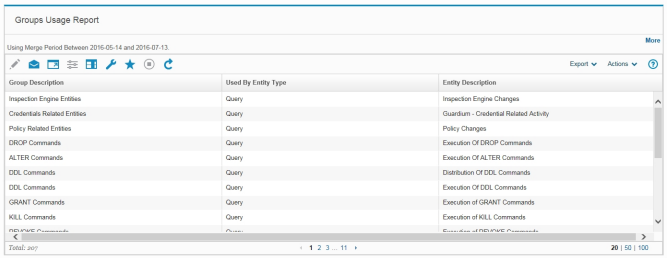
Domaine	Requête de base	Entité principale
Utilisation de la mémoire tampon	Moniteur d'utilisation de la mémoire tampon	Moniteur d'utilisation de la mémoire tampon du sniffer
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Rapport d'utilisation des groupes

Ce rapport affiche la liste de tous les groupes définis et de toutes les entités qui dépendent de chaque groupe.

Remarque : 328 enregistrements sont disponibles dans ce rapport.

Emplacement du rapport : Rapports > Surveillance du système Guardium > Rapport d'utilisation des groupes



Applications Guardium

Pour chaque application Guardium, chaque ligne répertorie un rôle de sécurité affecté, ou le mot Tous, indiquant que tous les rôles sont affectés.

Emplacement du rapport : Rapports > Rapports opérationnels Guardium en temps réel > Toutes les applications Guardium - Rôle

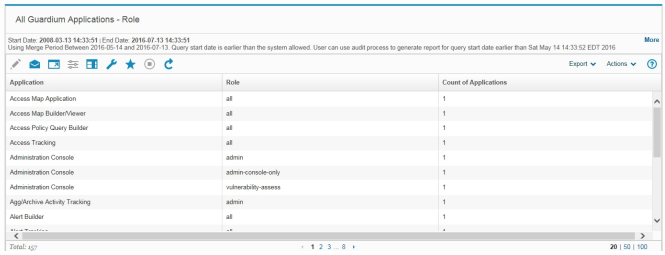


Tableau 3. Applications Guardium

Domaine	Requête de base	Entité principale
interne - non disponible	Toutes les applications Guardium	non disponible
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 100 JOURS
Fin de la période	<=	MAINTENANT

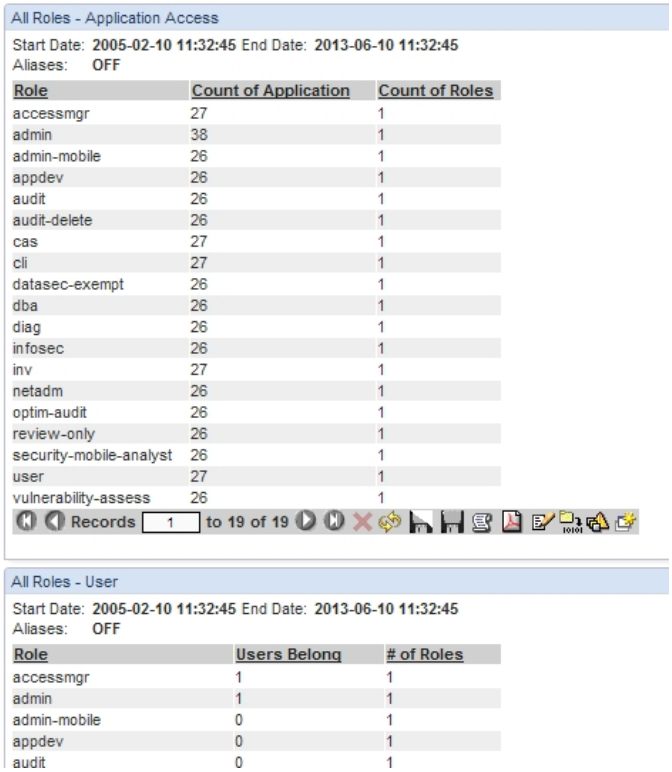
Rôles Guardium

Cette sous-fenêtre de menu affiche deux rapports : Tous les rôles - Accès aux applications et Tous les rôles - Utilisateur.

Tous les rôles - Accès aux applications - Pour chaque rôle, ce rapport répertorie le nombre d'applications auxquelles il est affecté.

Pour répertorier les applications auxquelles un rôle est affecté, cliquez sur le rôle et accédez au rapport Détails de l'enregistrement.

Emplacement du rapport : Rapports > Surveillance du système Guardium > Tous les rôles - Accès aux applications



All Roles - Application Access

Start Date: **2005-02-10 11:32:45** End Date: **2013-06-10 11:32:45**
Aliases: **OFF**

Role	Count of Application	Count of Roles
accessmgr	27	1
admin	38	1
admin-mobile	26	1
appdev	26	1
audit	26	1
audit-delete	26	1
cas	27	1
cli	27	1
datasec-exempt	26	1
dba	26	1
diag	26	1
infosec	26	1
inv	27	1
netadm	26	1
optim-audit	26	1
review-only	26	1
security-mobile-analyst	26	1
user	27	1
vulnerability-assess	26	1

Records 1 to 19 of 19

All Roles - User

Start Date: **2005-02-10 11:32:45** End Date: **2013-06-10 11:32:45**
Aliases: **OFF**

Role	Users Belong	# of Roles
accessmgr	1	1
admin	1	1
admin-mobile	0	1
appdev	0	1
audit	0	1

Tableau 4. Tous les rôles - Accès aux applications

Domaine	Requête de base	Entité principale
interne - non disponible	Tous les rôles - Accès aux applications	non disponible
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 100 MOIS
Fin de la période	<=	MAINTENANT

Tous les rôles - Utilisateur

Pour chaque rôle, ce rapport répertorie le nombre d'utilisateurs auxquels il est affecté. Pour répertorier les utilisateurs auxquels un rôle est affecté, cliquez sur le rôle et accédez au rapport Détails de l'enregistrement.

Tableau 5. Tous les rôles - Utilisateur

Domaine	Requête de base	Entité principale
interne - non disponible	Rôles - Utilisateur	non disponible
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 100 MOIS
Fin de la période	<=	MAINTENANT

Utilisateurs Guardium

Répertorie chaque utilisateur, la date de la dernière activité et le nombre de rôles affectés. Pour chaque utilisateur, vous pouvez explorer le rapport Détails de l'enregistrement pour voir les rôles affectés à cet utilisateur.

Tableau 6. Utilisateurs Guardium

Domaine	Requête de base	Entité principale
interne - non disponible	Rôle utilisateur	non disponible
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 100 MOIS
Fin de la période	<=	MAINTENANT

Niveaux d'utilisation d'unités

Les rapports par défaut suivants fournissent des données d'utilisation des unités :

- Utilisation d'unités : affiche le niveau d'utilisation maximum de chaque unité dans la période donnée. Une exploration affiche les détails d'une unité dans toutes les périodes du rapport.

- Distribution de l'utilisation d'unités : pour chaque unité, ce rapport affiche le pourcentage de périodes dans le calendrier du rapport dont les niveaux d'utilisation sont bas, moyens et élevés.
- Seuils d'utilisation : ce rapport prédéfini affiche toutes les valeurs de seuil bas et haut pour tous les paramètres d'utilisation d'unité.
- Récapitulatif quotidien de l'utilisation d'unités - Fournit un résumé quotidien des données d'utilisation d'unité.

Tableau 7. Niveaux d'utilisation d'unités

Domaine	Requête de base	Entité principale
Interne - non disponible	Distribution de l'utilisation d'unités	Niveaux d'utilisation d'unités
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 24 HEURES
Fin de la période	<=	MAINTENANT

- Rapports prédéfinis
  Au moment de l'installation, le dispositif Guardium est configuré avec un certain nombre de rapports prédéfinis.
- Rapports d'administration prédéfinis
  La présente section fournit une brève description de tous les rapports prédéfinis sur la présentation de l'administrateur par défaut.
- Rapports d'utilisateur prédéfinis
  La présente section fournit une brève description de tous les rapports prédéfinis sur la présentation d'utilisateur par défaut.
- Rapports prédéfinis communs
  La présente section fournit une brève description de tous les rapports prédéfinis sur les présentations d'utilisateur par défaut et d'administrateur par défaut.

Rubrique parent : Rapports

Rapports prédéfinis

Au moment de l'installation, le dispositif Guardium est configuré avec un certain nombre de rapports prédéfinis.

Tous les paramètres et toutes les valeurs sont affichés sur tous les rapports. Les paramètres et les valeurs peuvent être édités à partir du bouton Personnaliser dans n'importe quel écran de rapport.

Utilisez la fonction de recherche de l'aide pour accéder directement au rapport spécifique. Utilisez des guillemets autour des mots ou des expressions pour définir précisément les termes de recherche.

Les rapports prédéfinis sont décrits dans les pages suivantes :

- Rapports d'administrateur prédéfinis Rapports d'administration prédéfinis - Il s'agit des rapports prédéfinis disponibles pour l'administrateur.
- Rapports prédéfinis issus d'Accessmgr (voir la rubrique Vue d'ensemble de la gestion des accès) : Rapports sur les utilisateurs et les rôles ; Sources de données autorisées ; Serveurs autorisés ; Bases de données non associées ; Sources de données non associées.

API pour exécuter un processus d'audit à partir de rapports tabulaires et graphiques

Dans l'interface graphique Guardium, il existe une icône (Processus ad hoc pour exécution unique) permettant d'effectuer un appel GuardAPI, create_ad_hoc_audit_and_run_once.

Cette action ouvre une fenêtre avec les champs suivants :

- Adresses e-mail - Liste d'adresses e-mail séparées par des virgules.
- Type de contenu pour le destinataire d'e-mail : PDF/CSV (bouton d'option 0 - PDF / 1 -CSV)
- Ajouter un utilisateur comme récepteur (case à cocher)

Le comportement de ce processus est le suivant :

1 S'il s'agit d'un nouveau processus, un ou plusieurs récepteurs d'e-mail peuvent être créés dans la liste (le cas échéant) avec un type de contenu tel qu'indiqué dans le paramètre emailContentType. Est également créé un récepteur pour l'utilisateur connecté (appelant l'API) si le paramètre includeUserReceiver est vérifié (true).

2 - S'il s'agit d'un processus existant, tous les récepteurs d'e-mail sont supprimés et remplacés par les e-mails de la nouvelle liste (le cas échéant) avec le type de contenu tel que défini dans le paramètre emailContentType. Si la liste est vide, tous les récepteurs d'e-mail sont supprimés. S'il existe déjà un récepteur pour l'utilisateur, il N'est PAS supprimé même si le paramètre includeUserreceiver est faux, cependant, si le paramètre est vrai et qu'il n'y a pas de récepteur de ce type, il est ajouté.

Une fois que la procédure d'audit est générée, elle est automatiquement exécutée (similaire à la procédure Exécuter une fois maintenant) et les utilisateurs devraient recevoir un élément dans leur liste de tâches pour ce processus d'audit.

GuardAPI qui crée un processus d'audit ad hoc conserve les résultats jusqu'à 7 jours (et non 1 jour). Les résultats sont supprimés au bout de 7 jours.

Pour plus d'informations sur les paramètres, consultez la commande GuardAPI, create_ad_hoc_audit_and_run_once, dans la rubrique d'aide GuardAPI Input Generation.

Cas d'utilisation pour les rapports prédéfinis

Administrateur de base de données

- Erreurs SQL - Une augmentation des erreurs SQL peut indiquer une attaque par injection SQL.
- DDL (vérifier les changements de schéma) - Ce rapport affiche l'adresse IP client à partir de laquelle la DDL a été demandée, le verbe SQL principal (une commande DDL spécifique) et le total des objets accessibles pour cet enregistrement.
- Connexions ayant échoué - Ce rapport indique les tentatives d'accès à la base de données avec des données d'identification de connexion ayant expiré.

Agent de sécurité de l'information

- Connexions ayant échoué - Personnes possédant des données d'identification appropriées et tentant d'accéder à la base de données.
- Connexions d'utilisateurs arrêtés - Utilisateurs arrêtés tentant d'accéder à la base de données.
- Violations de politiques - Utilisateurs et problèmes qui enfreignent les politiques de sécurité.

Auditeurs

- Rapports de conformité - PCI, SOX, Confidentialité des données
- Flux de travail de conformité - Affiche les preuves des acceptations et des procédures.

Rubrique parent : Exploitation des rapports prédéfinis

Rapports d'administration prédéfinis

La présente section fournit une brève description de tous les rapports prédéfinis sur la présentation de l'administrateur par défaut.

La sélection de rapport de l'interface graphique Guardium comporte cinq sections :

- Outils de configuration de rapport,
- Rapports opérationnels Guardium,
- Rapports opérationnels Guardium en temps réel,
- Eléments de configuration Guardium et
- Surveillance du système Guardium.

Remarque : Si la sécurité au niveau des données pour les données observées a été activée (voir les paramètres du Profil global), la sortie du processus d'audit est filtrée afin que les utilisateurs ne puissent visualiser que les informations de leur base de données.

Les rapports d'administration prédéfinis sont répertoriés par ordre alphabétique.

Agents S-TAP actifs changés

Cette alerte s'exécute uniquement sur les systèmes de Central Manager. L'hôte S-TAP, la version S-TAP, l'agent S-TAP modifié, l'horodatage et le nombre sont affichés.

Tableau 1. Agents S-TAP actifs changés

Domaine	Requête de base	Entité principale
interne - non disponible	Agents S-TAP actifs changés	non disponible
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	néant	néant

Connexions des administrateurs

Récapitulatif des connexions à la base de données à l'aide d'un nom d'utilisateur de base de données défini dans le groupe Administrateurs. Le rapport affiche l'adresse IP du client à partir de laquelle l'utilisateur possédant des privilèges d'administration s'est connecté à la base de données, le nom d'utilisateur de la base de données, le programme source, la date et l'heure de début de la session et le total de sessions pour cet enregistrement.

Tableau 2. Connexions des administrateurs

Domaine	Requête de base	Entité principale
Accès	Connexion des administrateurs	Session
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Journal d'agrégation/archivage

Ce rapport répertorie l'activité d'agrégation Guardium par type d'activité. Chaque ligne du rapport contient les attributs suivants : Type d'activité, Heure de début, Nom de fichier, Statut, Commentaire, Nom d'hôte Guardium, Enregistrements purgés, Début de période, Fin de période et nombre d'enregistrements de journal pour la ligne. Vous pouvez limiter la sortie en définissant le paramètre d'exécution du nom d'hôte Guardium défini sur % par défaut (pour sélectionner tous les serveurs). La colonne Enregistrements purgés contient un nombre d'enregistrements purgés uniquement lorsque le type d'activité est Purger.

Tableau 3. Journal d'agrégation/archivage

Domaine	Requête de base	Entité principale
Agrégation/Exportation/Importation	Journal d'agrégation/archivage	Journal d'agrégation/archivage
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 SEMAINE
Fin de la période	<=	MAINTENANT
Nom d'hôte Guardium	LIKE	%

Toutes les applications Guardium - Rôle

Cette sous-fenêtre de menu affiche deux rapports : Tous les rôles - Accès aux applications et Tous les rôles - Utilisateur.

Tous les rôles - Accès aux applications

Pour chaque rôle, ce rapport répertorie le nombre d'applications auxquelles il est affecté. Pour répertorier les applications auxquelles un rôle est affecté, cliquez sur le rôle et accédez au rapport Détails de l'enregistrement.

Tableau 4. Tous les rôles - Accès aux applications

Domaine	Requête de base	Entité principale
interne - non disponible	Tous les rôles - Accès aux applications	non disponible
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 100 MOIS
Fin de la période	<=	MAINTENANT

Tous les rôles - Utilisateur

Pour chaque rôle, ce rapport répertorie le nombre d'utilisateurs auxquels il est affecté. Pour répertorier les utilisateurs auxquels un rôle est affecté, cliquez sur le rôle et accédez au rapport Détails de l'enregistrement.

Tableau 5. Tous les rôles - Utilisateur

Domaine	Requête de base	Entité principale
interne - non disponible	Rôle - Utilisateur	non disponible
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 100 MOIS
Fin de la période	<=	MAINTENANT

Paramètres de dispositif

Ce rapport affiche les paramètres de configuration issus d'un système Guardium. Utilisez le rapport *Paramètres de dispositif* pour réviser et valider rapidement les paramètres Guardium.

Tableau 6. Paramètres de dispositif

Domaine	Requête de base	Entité principale
interne - non disponible	Agents S-TAP actifs changés	non disponible
Paramètre d'exécution	Opérateur	Valeur par défaut
Afficher les alias		Boutons d'option (Activé, Désactivé, Valeur par défaut)
Source de données distante		Menu déroulant

Récapitulatif des objets d'application

Ce rapport est un récapitulatif de chaque définition dans l'application Guardium. Par exemple, entrez Oracle dans l'espace ObjectNameLike dans la page Paramètres d'exécution des Objets d'application et recherchez tous les types d'objet et les descriptions d'objets où Oracle est utilisé.

Remarque : Ce rapport présente des métadonnées et, en tant que tel, n'est pas filtré dans le mécanisme de sécurité de niveau de données. Ces métadonnées peuvent inclure des informations liées à la base de données telles que les SID Oracle.

Tableau 7. Récapitulatif des objets d'application

Domaine	Requête de base	Entité principale
Objets d'application	Récapitulatif des objets d'application	Objets d'application
Paramètre d'exécution	Opérateur	Valeur par défaut
ObjectNameLike	%	%
ObjectTypeNameLike	%	%

Clients TAP approuvés

Seuls des agents S-TAP spécifiques sont autorisés à se connecter à l'application Guardium. Ce rapport montre quel agent S-TAP est approuvé et le statut de celui-ci.

Tableau 8. Clients TAP approuvés

Domaine	Requête de base	Entité principale
interne - non disponible	Clients TAP approuvés	non disponible
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Journal du processus d'audit

Journal du processus d'audit

Ce rapport montre un journal d'activité détaillé pour toutes les tâches, y compris les heures de début et de fin. Ce rapport est disponible pour les administrateurs via l'onglet Moniteur de Guardium. Les tâches d'audit montrent les heures de début et de fin, toutefois le début et la fin des évaluations de sécurité et des classifications (qui se trouvent dans une file d'attente) sont identiques.

Le processus d'audit a été étendu à la validation de lignes spécifiques au-delà de l'utilisateur qui valide tout le processus d'audit. Affiche une liste des éléments validés et du statut de lignes spécifiques.

Utilisez ce journal de processus d'audit pour arrêter les processus d'audit. Les tâches peuvent être arrêtées uniquement si elles n'ont pas été exécutées ou sont en cours d'exécution. Toutes les autres tâches qui n'ont pas démarré ne s'exécutent pas. Les résultats partiels ne sont pas fournis. Si les tâches sont terminées, arrêter le processus d'audit n'arrête pas l'envoi des résultats. L'arrêt du processus d'audit se fait via une commande GrdAPI, invoke api, à partir du rapport Journal du processus d'audit. Pour tout utilisateur, il affiche uniquement la ligne appartenant à l'utilisateur (mais sans les détails, simplement avec les tâches). Les administrateurs visualisent tous les détails et peuvent arrêter l'exécution de tous les utilisateurs. Les utilisateurs peuvent arrêter uniquement leurs propres exécutions.

Remarque :

L'arrêt du processus d'audit n'annule pas les requêtes exécutées à l'aide d'une source distante. De même, aucun de ces rapports en ligne n'utilise une source distante.

Non pris en charge pour les jeux de confidentialité et les flux externes. Autrement dit, si la tâche Jeu de confidentialité a été démarrée ou le Flux externe a démarré - ils se terminent même si le processus est arrêté (par opposition à une requête qui est interrompue).

ID journal du processus d'audit

Nom de la connexion

ID exécution

Horodatage

ID processus d'audit

Description du processus d'audit

ID tâche d'audit

Description de la tâche d'audit

Type d'événement

Détails

Nombre de journaux de processus d'audit

Correctifs disponibles

Affiche une liste des correctifs disponibles. Il n'existe pas de paramètres d'exécution, et ce domaine de rapport concerne uniquement le système.

Moniteur d'utilisation de la mémoire tampon

Fournit un ensemble étendu de statistiques d'utilisation des mémoires tampon. Voir la description de l'entité Utilisation de la mémoire tampon du sniffer pour une description des champs répertoriés dans ce rapport.

Tableau 9. Moniteur d'utilisation de la mémoire tampon

Domaine	Requête de base	Entité principale
Utilisation de la mémoire tampon	Moniteur d'utilisation de la mémoire tampon	Moniteur d'utilisation de la mémoire tampon du sniffer
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Déploiement CAS

Ce rapport CAS indique le Type de base de données, le Nom du système d'exploitation, le Nom d'hôte et le Type de système d'exploitation.

Tableau 10. Déploiement CAS

Domaine	Requête de base	Entité principale
CAS	Déploiement CAS	N/A
Paramètre d'exécution	Opérateur	Valeur par défaut
Type de base de données	Like	%
OS_Name	Like	%
Nom d'hôte	Like	%
OS_Type	Like	%

Changements (CAS)

Détails des changements CAS

Pour chaque élément surveillé, les modifications sont classées par ordre de propriétaire.

Tableau 11. Détails des changements CAS

Domaine	Requête de base	Entité principale
Changements de CAS	Détails des changements CAS	Configuration hôte
Paramètre d'exécution	Opérateur	Valeur par défaut

Domaine	Requête de base	Entité principale
DB_Type	Like	%
Host_Name	Like	%
Instance_Name	Like	%
Monitored_Item	Like	%
OS_Type	Like	%
Type	Like	%

Données sauvegardées CAS

Ce rapport répertorie les données sauvegardées pour chaque changement détecté. Ce rapport est trié par nom d'hôte, puis par l'heure de modification la plus récente.

Tableau 12. Données sauvegardées CAS

Domaine	Requête de base	Entité principale
Changements de CAS	Données sauvegardées CAS	Données sauvegardées
Paramètre d'exécution	Opérateur	Valeur par défaut
Host_Name	Like	%
Monitored_Item	Like	%
Saved_Data_Id	Like	%

Configuration (CAS)

Instances CAS

Ce rapport répertorie les définitions d'instance CAS (une instance CAS applique un modèle défini à un hôte CAS spécifique). L'ordre de tri par défaut pour ce rapport n'est pas standard. Les clés de tri sont, de majeure à mineure : Nom d'hôte (croissant), Instance (croissant) et Dernier changement de statut (décroissant).

Tableau 13. Instances CAS

Domaine	Requête de base	Entité principale
Configuration CAS	Instances CAS	Détails d'élément surveillé
Paramètre d'exécution	Opérateur	Valeur par défaut
Host_Name	Like	%
OS_Type	Like	%
DB_Type	Like	%
Instance	Like	%

Configuration d'instance CAS

Ce rapport répertorie les modifications de la configuration de l'instance CAS. L'ordre de tri par défaut pour ce rapport n'est pas standard. Les clés de tri sont, de majeure à mineure : Nom d'hôte (croissant), Instance (croissant) et Dernier changement de statut (décroissant). Vous pouvez limiter la sortie à l'aide de l'un des paramètres d'exécution suivants, ce qui sélectionne toutes les valeurs par défaut.

Tableau 14. Configuration d'instance CAS

Domaine	Requête de base	Entité principale
Configuration CAS	Configuration d'instance CAS	Détails d'élément surveillé
Paramètre d'exécution	Opérateur	Valeur par défaut
Host_Name	Like	%
OS_Type	Like	%
Template_Id	Like	%

Liste des profils de connexion

La Liste des profils de connexion est un groupe de toutes les connexions autorisées (la Liste des profils de connexion affiche tous les détails de connexion).

Tableau 15. Liste des profils de connexion

Domaine	Requête de base	Entité principale
interne - non disponible	Liste des profils de connexion	Serveur client
Paramètre d'exécution	Opérateur	Valeur par défaut
Date de début de la requête	>=	MAINTENANT A 1 JOUR
Date de fin de la requête	<=	MAINTENANT

Connexions mises en quarantaine

Les politiques Guardium peuvent être utilisées pour mettre fin ou mettre en quarantaine les connexions en temps réel. Utilisez les alertes de seuil, en fonction des requêtes. Voir Quarantaine dans la rubrique Politiques pour les instructions de configuration.

Tableau 16. Connexions mises en quarantaine

Domaine	Requête de base	Entité principale
Quarantaine de connexion	Connexions mises en quarantaine	Quarantaine de connexion
Paramètre d'exécution	Opérateur	Valeur par défaut
Adresse IP du serveur	LIKE	%
Utilisateur base de données	LIKE	%
Nom du serveur	LIKE	%
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Pisteur de l'UC

Répertorie l'Hôte Software TAP et le nombre d'UC sur les machines exécutant des agents S-TAP.

Tableau 17. Pisteur de l'UC

Domaine	Requête de base	Entité principale
interne - non disponible	non disponible	non disponible
Paramètre d'exécution	Opérateur	Valeur par défaut
néant	N/A	N/A

Utilisation de l'UC

Par défaut, affiche l'utilisation de l'UC pendant les deux dernières heures. Ce rapport graphique est destiné à afficher uniquement l'activité récente. Si vous modifiez les paramètres d'exécution De et A pour inclure un délai plus long, vous pouvez recevoir un message indiquant qu'il y a trop de données. Utilisez un rapport tabulaire pour afficher une période plus longue.

Tableau 18. Utilisation de l'UC

Domaine	Requête de base	Entité principale
Mémoire tampon du sniffer	Utilisation de l'UC	Moniteur d'utilisation de la mémoire tampon du sniffer
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 2 HEURES
Fin de la période	<=	MAINTENANT

Bases de données par type / Nombre de bases de données par type

Type de serveur et sources de clients pour chaque type de base de données surveillé.

Tableau 19. Bases de données par type

Domaine	Requête de base	Entité principale
Accès	Nombre de bases de données par type	Client-serveur
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Bases de données reconnues

Pour la période de génération de rapports, pour chaque entité de Port reconnu où la valeur d'attribut Type de base de données est NOT LIKE Inconnu, ce rapport énumère l'Horodatage de l'analyse, l'IP serveur, le Nom d'hôte de serveur, le Type de base de données, le Port, le Type de port et le nombre de Ports reconnus pour la ligne.

Tableau 20. Bases de données reconnues

Domaine	Requête de base	Entité principale
Reconnaissance automatique	Bases de données reconnues	Port reconnu
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT
PortNotLike	NOT LIKE	Aucune valeur par défaut.

Liste de mappage des utilisateurs de la base de données

Mappage entre les utilisateurs de la base de données (appelants de SQL ayant provoqué une violation) et les adresses de messagerie pour les alertes en temps réel.

Tableau 21. Liste de mappage des utilisateurs de la base de données

Domaine	Requête de base	Entité principale

Domaine	Requête de base	Entité principale
Reconnaissance automatique	Liste de mappage des utilisateurs de la base de données	Connexion des utilisateurs Guardium
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Utilisateurs de la base de données par défaut activés

Ce rapport détaille les utilisateurs par défaut trouvés activés après une analyse de base de données dans le groupe d'utilisateurs par défaut et la liste des serveurs fournis à l'API d'analyse sans données d'identification. Lorsqu'un utilisateur activé est détecté dans une base de données, cette occurrence de base de données/utilisateur n'est rapportée qu'une seule fois. Les analyses ultérieures mettent à jour l'horodatage et la version de la base de données. Si une analyse ultérieure ne trouve pas un utilisateur précédemment détecté, l'horodatage reste inchangé afin de conserver un historique avec la dernière détection d'un utilisateur activé sur une base de données. Les analyses sont exécutées sous le programme d'écoute du classificateur et les travaux soumis (avec l'API non_credential_scan) peuvent être suivis à l'aide du rapport File d'attente de travaux Guardium.

Tableau 22. Utilisateurs de la base de données par défaut activés

Domaine	Requête de base	Entité principale
Utilisateurs de la base de données par défaut activés	Utilisateurs de la base de données par défaut activés	Utilisateurs de la base de données par défaut activés
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Sources de données

Répertorie toutes les sources de données définies : Type de source de données, Nom de source de données, Description de source de données, Hôte, Port, Nom de service, Nom d'utilisateur, Nom de base de données, Dernière connexion, Partagé et Propriétés de connexion.

Vous pouvez restreindre la sortie de ce rapport à l'aide du paramètre d'exécution Nom de source de données, qui par défaut est défini sur "%" pour sélectionner toutes les sources de données.

Tableau 23. Sources de données

Domaine	Requête de base	Entité principale
interne - non disponible	Sources de données	non disponible
Paramètre d'exécution	Opérateur	Valeur par défaut
Nom de source de données	LIKE	%
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Instances reconnues

Ce rapport S-TAP détaille les informations suivantes :

Horodatage, Hôte, Protocole, Port min., Port max., Port de la base de données K-TAP, Nom d'instance, Client, Client à exclure, Nom de processus, Tube nommé, Répertoire d'instance de base de données, Ajustement de la mémoire partagée DB2, Position du client de la mémoire partagée DB2, Taille de la mémoire partagée DB2.

Tableau 24. Instances reconnues

Domaine	Requête de base	Entité principale
Exception	Instances reconnues	Exception
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Journal d'extraction du magasin de données

Un magasin de données est un sous-ensemble d'un entrepôt de données. Un entrepôt de données agrège et organise les données de manière générique en vue de leur utilisation ultérieure pour l'analyse et les rapports. Un magasin de données commence par une analyse des données définies par l'utilisateur et met l'accent sur la satisfaction des exigences spécifiques de l'utilisateur en termes de contenu, présentation et facilité d'utilisation.

Le programme d'extraction du magasin de données s'exécute dans un lot selon le calendrier spécifié. Il récapitule les données en heures, jours, semaines ou mois selon la granularité demandée, puis enregistre les résultats dans une nouvelle table de la base de données Guardium Analytic.

Les données sont ensuite accessibles aux utilisateurs via les utilitaires standard Rapports et Processus d'audit, ainsi que tout autre domaine/entité traditionnel. Les données d'extraction du magasin de données sont disponibles sous le domaine DM et le nom de l'entité est défini selon le nouveau nom de table spécifié pour les données du magasin de données. A l'aide du Générateur de requête et du Générateur de rapport standard, les utilisateurs peuvent cloner la requête par défaut et éditer la requête et le rapport, générer un portlet et l'ajouter à une sous-fenêtre.

Le journal d'extraction se compose des éléments suivants : Nom de magasin de données, IP collecteur, IP serveur, Heure de début, Heure de fin, ID, Début d'exécution, Fin d'exécution, Nombre d'enregistrements, Statut, Code d'erreur.

Journal d'exportation/importation des définitions

Ce rapport répertorie l'activité d'exportation/importation Guardium par type d'activité. Chaque ligne du rapport contient les attributs suivants : Type d'activité, Heure de début, Nom de fichier, Statut, Commentaire et nombre d'enregistrements de journal pour la ligne.

Tableau 25. Journal d'exportation/importation des définitions

Domaine	Requête de base	Entité principale
Agrégation/Archive	Journal des définitions d'exportation/importation	Journal d'agrégation/archivage
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Demandes supprimées

Demandes de suivi supprimées par un moteur d'inspection (Description d'exception = Requête de base de données abandonnée). Dans des situations extrêmement rares de fort volume, certaines demandes peuvent être perdues. Lorsque cela se produit, les sessions à partir desquelles les requêtes ont été perdues sont répertoriées dans le rapport Demandes supprimées.

Tableau 26. Demandes supprimées

Domaine	Requête de base	Entité principale
Exceptions	Demandes supprimées	Exception
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Nombre d'exceptions

Pour la période de rapport, nombre total d'exceptions enregistrées.

Tableau 27. Nombre d'exceptions

Domaine	Requête de base	Entité principale
Exceptions	Nombre d'exceptions	Exception
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Vue S-TAP d'entreprise (détaillée)

Voir Informations S-TAP (Central Manager) pour plus d'informations sur ce rapport.

Historique de l'association S-TAP d'entreprise

L'Historique de l'association S-TAP d'entreprise indique combien de temps l'agent S-TAP a rapporté au système Guardium spécifique dans l'environnement d'Equilibrage de charge.

Vue S-TAP d'entreprise

Voir Informations S-TAP (Central Manager) pour plus d'informations sur ce rapport.

Exporter les données sensibles vers Discovery

Guardium et InfoSphere Discovery comportent des mécanismes pour la classification des données sensibles.

Une interface bidirectionnelle est fournie pour transférer les données sensibles identifiées de Guardium vers InfoSphere Discovery et d'InfoSphere Discovery vers Guardium.

Ces données sont transférées via des fichiers CSV. Voir Corrélation avec des données externes (interface bidirectionnelle) pour plus d'informations.

Tableau 28. Exporter les données sensibles vers Discovery

Domaine	Requête de base	Entité principale
Interne - non disponible	Exporter les données sensibles vers Discovery	Résultats du processus de classification
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 3 HEURES
Fin de la période	<=	MAINTENANT
Description de règle	LIKE	
Schéma	LIKE	

Moniteur d'utilisation de la mémoire tampon d'entreprise

Ce rapport montre l'agrégat d'utilisation de la mémoire tampon du sniffer par toutes les unités gérées. Il est nécessaire de définir le calendrier de téléchargement. Voir la description de l'entité Utilisation de la mémoire tampon du sniffer pour une description des champs répertoriés dans ce rapport.

Tableau 29. Moniteur d'utilisation de la mémoire tampon d'entreprise

Domaine	Requête de base	Entité principale
Utilisation de la mémoire tampon d'entreprise	Utilisation de la mémoire tampon d'entreprise	Utilisation de la mémoire tampon du sniffer
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

File d'attente de travaux Guardium

Affiche la file d'attente de travaux Guardium. Connue précédemment sous le nom File d'attente de travaux du classificateur/d'évaluation. Pour chaque travail, elle répertorie les attributs suivants : ID exécution de processus, Type de processus, Statut, ID processus du travail Guardium, ID résultat de rapport, Description du travail Guardium, Description de la tâche d'audit, Durée en file d'attente, Heure de début, Heure de fin et Sources de données.

Tableau 30. File d'attente de travaux Guardium

Domaine	Requête de base	Entité principale
Interne - non disponible	File d'attente de travaux Guardium	non disponible
Paramètre d'exécution	Opérateur	Valeur par défaut
Description du travail	LIKE	%
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

File d'attente de travaux

Les évaluations et les classifications s'exécutent dans leur propre processus appelé la file d'attente de travaux. Les travaux sont mis en file d'attente et leur statut est maintenu, tandis qu'un programme d'écoute examine périodiquement la file d'attente à la recherche de travaux en attente.

Arrêt

Lorsque vous exécutez des travaux, lorsque vous cliquez avec le bouton droit de la souris pour une exploration, une option permet d'arrêter le travail en cours d'exécution et de l'annuler. Le travail ne peut pas être redémarré à ce stade.

Arrêt

Les travaux en cours d'exécution sont surveillés afin de réduire le nombre de travaux en suspens qui pourraient provoquer une surcharge de la file d'attente des travaux. Si un travail est inactif pendant 30 minutes, le programme d'écoute est interrompu et redémarré, ce qui arrête l'exécution d'un travail. Avant que le programme d'écoute ne soit redémarré, un processus appelé nettoyeur s'exécute, le statut passe de EXECUTION EN COURS à ARRETE, puis le programme d'écoute est redémarré. Le statut ARRETE signifie que le travail n'a pas pu être terminé.

Resoumission

Parfois, le programme d'écoute est redémarré pour des raisons autres qu'un travail suspendu, par exemple le redémarrage de la machine. Lorsque le nettoyeur arrête les travaux en cours, il observe si le travail a répondu au cours des 8 dernières minutes. Dans l'affirmative, le travail est copié et cette copie est renvoyée sur la file d'attente. Le travail initial arrêté s'affiche dans la file d'attente et contient toujours les résultats qu'il a pu traiter.

Surveillance

Le mécanisme par lequel les travaux maintiennent leur statut actif est en modifiant l'horodatage sur l'enregistrement de la file d'attente de travaux. Il est important de noter que l'enregistrement de la file d'attente de travaux est utilisé pour l'ensemble du travail. Chaque règle de classificateur ou test d'évaluation interagit avec l'horodatage pour son processus parent, et elle/il ne comporte pas d'horodatages individuels surveillés.

Le classificateur met à jour son horodatage avant que chaque règle soit testée et après chaque opération SQL. Par exemple, si le classificateur analyse les données dans une base de données prenant en charge la pagination, il modifie l'horodatage après que chaque lot de données est renvoyé de la base de données. La raison en est que, en fonction de l'état de la base de données cible, le classificateur peut appeler certaines requêtes longues qui sont limitées à 30 minutes d'exécution.

Les évaluations modifient l'horodatage après l'estimation de chaque test de l'évaluation. La plupart des tests d'évaluation s'exécutent en quelques secondes ou moins.

Tests observés

L'exception aux tests d'évaluation relativement rapides est la catégorie des tests d'évaluation observés. Ces tests sont basés sur des requêtes et des rapports qui utilisent les données de sniffing internes sur le dispositif Guardium. Ils peuvent être exécutés pendant des périodes plus longues et ne peuvent pas mettre à jour l'horodatage pendant leur exécution. Par conséquent, l'horodatage des tests d'évaluation observés est fixé à deux heures dans le futur quand ils sont démarrés, ce qui leur laisse deux heures et trente minutes pour s'exécuter. Cela peut être source de confusion lorsque l'horodatage de la file d'attente des travaux est défini à un point dans le futur. Comme pour tout autre test d'évaluation, lorsque le test observé se termine, l'horodatage est modifié. Si le test suivant est un test observé, l'horodatage est de nouveau réglé deux heures dans l'avenir. Sinon, l'horodatage est réglé sur l'heure courante.

Statut des clients GIM

Affiche une liste de clients GIM.

Tableau 31. Statut des clients GIM

Domaine	Requête de base	Entité principale

Domaine	Requête de base	Entité principale
Statut des clients GIM	Statut des clients GIM	Clients GIM
Paramètre d'exécution	Opérateur	Valeur par défaut
Nom du client	%	N/A
Système d'exploitation du client	%	N/A

Liste des événements GIM

Affiche une liste d'événements GIM.

Tableau 32. Liste des événements GIM

Domaine	Requête de base	Entité principale
Evénements GIM	Evénements GIM	Evénements GIM
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Modules installés GIM

Affiche une liste des modules GIM installés.
Remarque : Ce rapport montre les modules qui ont été associés à l'hôte. Si un module a été affecté à un hôte, la version affectée apparaît dans ce rapport, même si le module n'a pas encore été planifié ou installé. Pour vérifier le module installé, examinez le rapport Statut des clients GIM.

Tableau 33. Modules installés GIM

Domaine	Requête de base	Entité principale
Base installée GIM	Base installée GIM	GIM installé
Paramètre d'exécution	Opérateur	Valeur par défaut
néant	non applicable	non applicable

Rapport d'utilisation des groupes

Affiche la liste de tous les groupes définis et de toutes les entités qui dépendent de chaque groupe.

Exceptions de l'API Guardium

Affiche un horodatage et une description de toutes les exceptions GuardAPI. Il s'agit de travaux où l'ID type d'exception est GUARD_API_EXCEPTION.

Tableau 34. Exceptions de l'API Guardium

Domaine	Requête de base	Entité principale
Exception	Exceptions de l'API Guardium	Exception
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Applications Guardium

Pour chaque application Guardium, chaque ligne répertorie un rôle de sécurité affecté, ou le mot Tous, indiquant que tous les rôles sont affectés.

Tableau 35. Applications Guardium

Domaine	Requête de base	Entité principale
interne - non disponible	Toutes les applications Guardium	non disponible
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 100 JOURS
Fin de la période	<=	MAINTENANT

Détails du groupe Guardium

Pour la période de rapport, chaque ligne du rapport répertorie un membre du groupe. Les colonnes contiennent les informations suivantes : Description de groupe, Type de groupe, Sous-type du groupe, Horodatage (issu de l'entité Membre de groupe), Membre de groupe et nombre d'entités de Membre de groupe pour la ligne. La valeur de l'horodatage est définie à l'heure courante chaque fois que l'enregistrement est mis à jour.

Vous pouvez restreindre la sortie de ce rapport à l'aide des paramètres d'exécution, tous deux utilisés avec l'opérateur LIKE et la valeur par défaut %, qui sélectionne toutes les valeurs.

Tableau 36. Détails du groupe Guardium

Domaine	Requête de base	Entité principale
Groupe	Détails du groupe Guardium	Membre de groupe

Domaine	Requête de base	Entité principale
Paramètre d'exécution	Opérateur	Valeur par défaut
Description du groupe	LIKE	%
Type du groupe	LIKE	%
Début de la période	>=	MAINTENANT A 100 MOIS
Fin de la période	<=	MAINTENANT

Utilisateurs Guardium

Répertorie chaque utilisateur, la date de la dernière activité et le nombre de rôles affectés. Pour chaque utilisateur, vous pouvez explorer le rapport Détails de l'enregistrement pour voir les rôles affectés à cet utilisateur.

Tableau 37. Utilisateurs Guardium

Domaine	Requête de base	Entité principale
interne - non disponible	Rôle utilisateur	non disponible
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 100 MOIS
Fin de la période	<=	MAINTENANT

Historique de l'hôte (CAS)

CAS Historique de l'hôte

Ce rapport répertorie les événements de l'hôte CAS. L'ordre de tri par défaut pour ce rapport n'est pas standard. Les clés de tri sont, de majeure à mineure : Nom d'hôte (croissant), Instance et Heure de l'événement (décroissant).

Tableau 38. CAS Historique de l'hôte

Domaine	Requête de base	Entité principale
CAS Historique de l'hôte	CAS Historique de l'hôte	Evénement hôte
Paramètre d'exécution	Opérateur	Valeur par défaut
Host_Name	Like	%
OS_Type	Like	%
Event_Type	Like	%

Moteurs d'inspection inactifs

Répertorie tous les moteurs d'inspection inactifs

Tableau 39. Moteurs d'inspection inactifs

Domaine	Requête de base	Entité principale
interne - non disponible	Moteurs d'inspection inactifs	En-tête de vérification d'agent S-TAP
Paramètre d'exécution	Opérateur	Valeur par défaut
Date de début de la requête	>=	MAINTENANT A 3 HEURES
Date de fin de la requête	>=	MAINTENANT

S-TAP inactifs depuis

Récapitule tous les S-TAP inactifs définis sur le système. Possède un seul paramètre d'exécution : Début de la période, qui est défini sur Maintenant -1 heure par défaut. Utilisez ce paramètre pour contrôler la façon dont vous souhaitez définir des S-TAP inactifs. Ce rapport contient les mêmes colonnes de données pour le rapport de statut S-TAP avec l'ajout d'un comptage pour chaque ligne du rapport.

Tableau 40. S-TAP inactifs depuis

Domaine	Requête de base	Entité principale
interne - non disponible	S-TAP inactifs depuis	non disponible
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 HEURE

Correctifs installés

Affiche une liste des correctifs installés. Il n'existe pas de paramètres d'exécution, et ce domaine de rapport concerne uniquement le système.

Tableau 41. Correctifs installés

Domaine	Requête de base	Entité principale
interne - non disponible	Correctifs installés	non disponible
Paramètre d'exécution	Opérateur	Valeur par défaut

Domaine	Requête de base	Entité principale
néant	non applicable	non applicable

Connexions à Guardium

Toutes les valeurs de ce rapport proviennent de l'entité Connexions à Guardium. Pour la période de rapport, chaque ligne du rapport répertorie les informations suivantes : Nom d'utilisateur, Connexion réussie (1= Réussite, 0= Echec), Date et heure de connexion, Date et heure de déconnexion (vide si l'utilisateur ne s'est pas encore déconnecté), Nom d'hôte, Adresse distante (de l'utilisateur) et nombre de connexions pour la ligne.

Tableau 42. Connexions à Guardium

Domaine	Requête de base	Entité principale
Connexions à Guardium	Connexions à Guardium	Connexion des utilisateurs Guardium
Paramètre d'exécution	Opérateur	Valeur par défaut
Nom d'hôte	LIKE	%
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Alertes T/R consignées

Pour la période de rapport, nombre total d'alertes en temps réel consignées, répertoriées par la description de règle.

Tableau 43. Alertes T/R consignées

Domaine	Requête de base	Entité principale
Violations de politique	Alertes T/R consignées	Violation de règle de politique
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Alertes de seuil consignées

Pour la période de rapport, nombre total d'alertes de seuil enregistrées.

Tableau 44. Alertes de seuil consignées

Domaine	Requête de base	Entité principale
Alerte	Alertes consignées	Détails d'alerte de seuil
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Collecteurs de consignation (valable uniquement à partir de l'unité d'agrégation)

Le rapport Collecteurs de consignation apparaît sous l'onglet Moniteur quotidien et il est valable uniquement sur une unité agrégation. Ce rapport indique le nombre de sessions par IP serveur, par collecteur et par jour. Par exemple : le 19 mai, l'agrégateur n° 1 a collecté 100 sessions pour le serveur 192.168.x.x1, 50 sessions pour le serveur 192.168.x.x2 ; l'agrégateur n° 2 a collecté 30 sessions pour le serveur 192.168.x.x3, 90 sessions pour le serveur 192.168.x.x4; etc.

Tableau 45. Collecteurs de consignation

Domaine	Requête de base	Entité principale
Exceptions	Collecteurs de consignation	Collecteurs de consignation
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Unités gérées (Central Manager)

Rapport d'entreprise sur une instance Central Manager qui montre les unités gérées en cours d'exécution. Utilisez ce rapport dans une alerte statistique pour envoyer un e-mail à un administrateur chaque fois qu'une unité gérée est en panne.

Tableau 46. Unités gérées (Central Manager)

Domaine	Requête de base	Entité principale
interne - non disponible	Unités gérées	Unités gérées
Paramètre d'exécution	Opérateur	Valeur par défaut
Nom d'hôte	LIKE	%
Source de données distante		Menu déroulant
Afficher les alias		Boutons d'option (Activé, Désactivé, Valeur par défaut)

Nombre de processus d'audit actifs

Nombre de processus d'audit Guardium actifs. Lorsque la gestion centrale est utilisée, ce rapport contient des données uniquement sur Central Manager et est vide sur toutes les unités gérées (le message standard s'affiche : Aucune donnée trouvée pour la requête demandée). Ce rapport ne comporte pas de paramètres d'exécution.

Tableau 47. Nombre de processus d'audit actifs

Domaine	Requête de base	Entité principale
Processus d'audit	Nombre de processus actifs	Processus d'audit
Paramètre d'exécution	Opérateur	Valeur par défaut
néant	non applicable	non applicable

Examens des processus d'audit en attente

Nombre de processus d'audit Guardium en attente, répertoriés par les utilisateurs Guardium.

Tableau 48. Examens des processus d'audit en attente

Domaine	Requête de base	Entité principale
Processus d'audit	Examens des processus d'audit en attente	Liste de tâches des résultats de tâche
Paramètre d'exécution	Opérateur	Valeur par défaut
néant	non applicable	non applicable

Journal des changements de l'hôte Guardium principal

Journal des changements principaux de l'hôte pour les agents S-TAP. L'hôte principal est l'unité Guardium vers laquelle l'agent S-TAP envoie des données. Chaque ligne du rapport répertorie les informations suivantes : Hôte S-TAP, Nom d'hôte Guardium, Début de période et Fin de période.

Tableau 49. Journal des changements de l'hôte Guardium principal

Domaine	Requête de base	Entité principale
interne - non disponible	Journal des changements de l'hôte SGuard principal	non disponible
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Entités et attributs de requête

Ce rapport répertorie toutes les entités et les attributs dans les rapports Guardium et a été créé pour simplifier la liaison entre les attributs Guardium et les appels GuardAPI.

Utilisez ce rapport pour appeler également create_constant_attribute, create_api_parameter_mapping, delete_api_parameter_mapping, ou list_param_mapping_for_function.

Tableau 50. Entités et attributs de requête

Domaine	Requête de base	Entité principale
Tous les domaines de rapport Guardium	Toutes les entités pour le domaine de rapport	Tous les attributs de l'entité
Paramètre d'exécution	Opérateur	Valeur par défaut
Nom du rapport comme suit Si <> '%', affiche uniquement le domaine/l'entité et les attributs utilisés par les rapports qui correspondent au nouveau paramètre. Si '%', tous les domaines, requêtes et attributs sont affichés (y compris ceux qui ne sont utilisés par aucun rapport).	non applicable	non applicable

Statistiques de réexécution

Ce rapport affiche les informations suivantes : Statistiques de réexécution pour la date de début/fin d'exécution ; Nom de la configuration ; Nom de la configuration de planification ; Statut du travail ; Description des statistiques ; ID session ; Requêtes réussies ; Requêtes échouées ; Nombre total de requêtes ; Type ; Tâches actives/en attente/terminées.

Tableau 51. Statistiques de réexécution

Domaine	Requête de base	Entité principale
Suivi des résultats de réexécution	Statistiques de réexécution	Statistiques de résultat de réexécution
Paramètre d'exécution	Opérateur	Valeur par défaut
Date de début de la requête	>=	MAINTENANT A 1 JOUR
Date de fin de la requête	<=	MAINTENANT

Domaine	Requête de base	Entité principale
Session	>=	N/A
Session	<=	N/A

Récapitulatif de réexécution

Pour la période de rapport, mesure des requêtes ayant échoué ou réussi. Marque de contrôle requise dans Configuration de réexécution pour Requête échouée ou Requête réussie.

Tableau 52. Récapitulatif de réexécution

Domaine	Requête de base	Entité principale
Résultats de relecture	Récapitulatif de réexécution	Résultats de relecture
Paramètre d'exécution	Opérateur	Valeur par défaut
Date de début de la requête	>=	MAINTENANT A 1 JOUR
Date de fin de la requête	<=	MAINTENANT
Statut des résultats	%	N/A
Nom de la configuration de planification	%	N/A

Données restaurées

Ce rapport comporte deux colonnes : RESTORED_DAY et EXPIRATION_DATE. Lorsque l'utilisateur restaure des données de l'archive, cette table est remplie en fonction des données restaurées et de la durée spécifiée de conservation de ces données. Le processus de purge examine cette table pour déterminer quelles données peuvent être purgées et nettoie les enregistrements qui sont arrivés à expiration. RESTORED_DAY est la date des données qui ont été restaurées et sont dans le passé. EXPIRATION_DATE est la date à laquelle ces données seront purgées et une date

dans le futur.

Tableau 53. Données restaurées

Domaine	Requête de base	Entité principale
Données restaurées	Données restaurées	Données restaurées
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 10 JOURS
Fin de la période	<=	MAINTENANT A +10 JOURS

Taux des demandes

Par défaut, affiche le taux des demandes au cours des deux dernières heures. Ce rapport graphique est destiné à afficher uniquement l'activité récente. Si vous modifiez les paramètres d'exécution pour inclure un délai plus long, vous pouvez recevoir un message indiquant qu'il y a trop de données. Utilisez un rapport tabulaire pour afficher une période plus longue.

Tableau 54. Taux des demandes

Domaine	Requête de base	Entité principale
Mémoire tampon du sniffer	Taux des demandes	Moniteur d'utilisation de la mémoire tampon du sniffer
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 2 HEURES
Fin de la période	<=	MAINTENANT

Connexions Rogue

Ce rapport n'est disponible que lorsque l'option Hunter est activée sur les serveurs Unix. L'option Hunter n'est utilisée que lorsque la méthode de surveillance Tee est utilisée. Ce rapport répertorie tous les processus locaux qui ont contourné S-TAP pour se connecter à la base de données.

Tableau 55. Connexions Rogue

Domaine	Requête de base	Entité principale
Connexions Rogue	Connexions Rogue	Connexions Rogue
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Exceptions des travaux planifiés

Affiche un horodatage et la description pour chaque exception de travail programmé (y compris les erreurs d'évaluation). . Il s'agit de travaux où l'ID type d'exception est l'un des suivants : SCHED_JOB_EXCEPTION, ASSESSMENT_EXCEPTION ou ASMT_ERROR.

Tableau 56. Exceptions des travaux planifiés

Domaine	Requête de base	Entité principale

Domaine	Requête de base	Entité principale
Mémoire tampon du sniffer	Utilisation de l'UC	Utilisation de la mémoire tampon du sniffer
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 2 HEURES
Fin de la période	<=	MAINTENANT

Travaux planifiés

Affiche la liste des travaux actuellement programmés.

Tableau 57. Travaux planifiés

Domaine	Requête de base	Entité principale
interne - non disponible	Travaux planifiés	non disponible
Paramètre d'exécution	Opérateur	Valeur par défaut
néant	non applicable	non applicable

Nombre de sessions

Pour la période de rapport, le nombre total de sessions différentes s'ouvrent.

Tableau 58. Nombre de sessions

Domaine	Requête de base	Entité principale
Accès	Nombre de sessions	Session
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Nombre de verbes SQL

Pour la période de rapport, nombre total de commandes SQL différentes émises.

Tableau 59. Nombre de verbes SQL

Domaine	Requête de base	Entité principale
Accès	Nombre de verbes SQL	SQL
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Historique des changements de configuration S-TAP

Ce rapport n'est affiché que lorsqu'un moteur d'inspection est ajouté ou modifié. Répertorie les changements de configuration S-TAP - chaque changement de moteur d'inspection s'affiche sur une ligne distincte. Chaque ligne contient les informations suivantes : Hôte S-TAP, Type du serveur de la base de données, Port de base de données source, Port de base de données cible, Adresse IP client de la base de données, Masque du client de la base de données et Horodatage pour le changement.

Tableau 60. Historique des changements de configuration S-TAP

Domaine	Requête de base	Entité principale
interne - non disponible	Historique des changements de configuration	non disponible
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Statut S-TAP

Affiche les informations de statut sur chaque moteur d'inspection défini sur chaque hôte S-TAP. Ce rapport ne comporte pas de paramètres de date de début et de fin car il rapporte le statut en cours. Chaque ligne du rapport répertorie les informations suivantes : Hôte S-TAP, Type du serveur de la base de données, Statut, Dernière réponse, Nom d'hôte principal. Indicateurs Oui/Non pour les attributs suivants : K-TAP installé, TEE installé, Pilote de mémoire partagée installé, Pilote de mémoire partagée installé DB2, Pilote de tubes nommés installé et Serveur d'applications installé. De plus, il répertorie les bases de données Hunter.

Remarque : Le pilote de mémoire partagé DB2 a été remplacé par la fonction DB2 Tap.

Tableau 61. Statut S-TAP

Domaine	Requête de base	Entité principale
interne - non disponible	Statut S-TAP	non disponible
Paramètre d'exécution	Opérateur	Valeur par défaut
néant	N/A	N/A

Vérification S-TAP

Répertoriez tous les résultats des vérifications S-TAP.

Tableau 62. Vérification S-TAP

Domaine	Requête de base	Entité principale
interne - non disponible	Vérification S-TAP	En-tête de vérification d'agent S-TAP
Paramètre d'exécution	Opérateur	Valeur par défaut
Date de début de la requête	>=	MAINTENANT A 3 HEURES
Date de fin de la requête	>=	MAINTENANT

Evénements S-TAP

Utilisez ce rapport pour plus d'informations sur l'agent S-TAP (à partir de la table SOFTWARE_TAP_EVENT dans une base de données interne).

Tableau 63. Evénements S-TAP

Domaine	Requête de base	Entité principale
interne - non disponible	Evénements S-TAP	non disponible
Paramètre d'exécution	Opérateur	Valeur par défaut
type d'événement	LIKE	%
type d'hôte	LIKE	%
Début de la période	>=	MAINTENANT A 3 JOURS
Fin de la période	<=	MAINTENANT

Informations S-TAP (Central Manager)

Rapport : voir Rapports S-TAP. Sur Central Manager, un rapport supplémentaire, Informations S-TAP, est disponible. Ce rapport surveille les S-TAP de l'ensemble de l'environnement. Téléchargez ces données à l'aide du Générateur de table personnalisée.

Les Informations S-TAP constituent un domaine personnalisé prédéfini qui contient l'entité Informations S-TAP et ne sont pas modifiables comme le domaine d'autorisation.

Lors de la définition d'une requête personnalisée, accédez à la page de chargement et cliquez sur Vérifier/Réparer pour créer la table personnalisée dans la base de données CUSTOM, faute de quoi la requête de sauvegarde ne la valide pas. Cette table se charge automatiquement à partir de toutes les sources distantes. Un utilisateur ne peut sélectionner quelles sources éloignées sont utilisées - il extrait les données de toutes les sources.

Sur la base de cette table personnalisée et du domaine personnalisé, il existe deux rapports :

La vue S-TAP d'entreprise affiche, à partir de Central Manager, des informations sur un agent S-TAP actif sur un collecteur et/ou une unité gérée. S'il existe des doublons pour le même moteur S-TAP, l'un étant actif et l'un inactif, le rapport utilise uniquement le moteur actif.

La vue détaillée S-TAP d'entreprise affiche, à partir de Central Manager, des informations sur tous les agents S-TAP actifs et inactifs sur tous les collecteurs et/ou les unités gérées.

Si la vue S-TAP d'entreprise et la vue détaillée S-TAP d'entreprise semblent identiques, c'est parce qu'un seul agent S-TAP sur une unité gérée est affiché. La vue détaillée S-TAP d'entreprise semblerait différente si davantage d'agents S-TAP et d'unités gérées étaient impliqués.

Ces deux rapports peuvent être choisis dans l'onglet Moniteur TAP d'un système autonome, mais ils ne contiennent aucune information.

Alerte : voir Affichage d'une définition de processus d'audit pour l'alerte : Moteurs d'inspection et S-TAP - alerte sur toutes les activités liées au moteur d'inspection et à la configuration S-TAP

Dernière réponse de S-TAP

La requête et le rapport prédéfinis sont disponibles, mais ne sont ajoutés à aucune sous-fenêtre.

La requête/le rapport affiche Tous les hôtes S-TAP et la dernière réponse (signal de présence) envoyée par chaque hôte.

Le but de cette requête est de pouvoir définir une alerte qui se déclenche lorsque S-TAP sur un hôte n'a pas répondu pendant une période donnée.

Les paramètres d'entrée sont : Date de début de la dernière réponse et Date de fin de la dernière réponse.

Par exemple, lorsqu'elle est exécutée avec Date de début de la dernière réponse = MAINTENANT A 5 JOURS et Date de fin de la dernière réponse = MAINTENANT A 3 HEURES, elle affiche le nom d'hôte et le dernier temps de réponse pour les hôtes qui ont envoyé la dernière réponse au cours des 5 derniers jours, mais n'avaient aucune réponse au cours des 3 dernières heures.

Moniteur d'état S-TAP

Pour chaque génération de rapport S-TAP rapportant à ce dispositif Guardium, ce rapport identifie les éléments suivants : Hôte S-TAP, Version S-TAP, Type du serveur de la base de données, Statut (actif ou inactif), Dernière réponse reçue (date et heure), Nom d'hôte principal. Indicateurs true/false pour : KTAP, TEE, Mémoire partagée de serveur MS SQL, Mémoire partagée DB2, surveillance de TCP local, Utilisation des Tubes nommés et Chiffrement.

Ce rapport ne comporte pas de paramètres d'exécution, et est basé sur une requête du système uniquement qui ne peut pas être modifiée.

Fichiers STAP/Z

STAP/Z fournit des fichiers contenant des données brutes collectées sur DB2 (surz/OS) contenant des événements DB2, des instructions SQL, etc. Ce rapport répertorie les éléments suivants : ID interface, Nom de fichier UA (Événement d'audit non normalisé), Nom de fichier UT (texte d'événement d'audit non normalisé), Nom de fichier UH (variables d'hôte d'événement d'audit non normalisé), Statut de fichier, Nombre total d'événements traités, Nombre d'événements ayant échoué et Horodatage. Les paramètres d'exécution sont FileName Like % et FileStatus Like %.

Ce rapport comporte deux paramètres d'exécution,, FileName Like % et FileStatus Like %. Il est basé sur une requête du système uniquement qui ne peut pas être modifiée.

Exceptions TCP

Pour la période de rapport, pour chaque exception où la Description d'exception de l'entité Type d'exception est une Exception de protocole TCP/IP, une ligne de ce rapport répertorie les valeurs d'attribut suivantes issues de l'entité Exception : Horodatage de l'exception, Description d'exception, Adresse source, Adresse de destination, Port source, Port de destination et nombre d'Exceptions pour cette ligne.

Tableau 64. Exceptions TCP

Domaine	Requête de base	Entité principale
Exceptions	Exceptions TCP	Exception
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Modèles (CAS)

Modèles CAS

Ce rapport répertorie les modèles CAS. Par défaut, tous les éléments de modèle sont répertoriés.

Tableau 65. Modèles CAS

Domaine	Requête de base	Entité principale
Modèles CAS	Modèles CAS	Modèle
Paramètre d'exécution	Opérateur	Valeur par défaut
Access_Name	Like	%
Template_Set_Name	Like	%
Audit_Type	Like	%

Exceptions de tests

Indiquez les paires de test/source de données qui sont exemptées temporairement. Voir create_test_exception pour plus d'informations sur l'utilisation des Exceptions de test.

Tableau 66. Exceptions de tests

Domaine	Requête de base	Entité principale
interne - non disponible	Exceptions de tests	non disponible
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 12 MOIS
Fin de la période	<=	MAINTENANT

Débit

Pour chaque Période d'accès dans la période de rapport, chaque ligne répertorie l'heure de Début de période, le nombre d'Adresses IP serveur et le nombre total d'accès (entités Période d'accès).

Vous pouvez restreindre la sortie de ce rapport à l'aide du paramètre d'exécution Adresses IP serveur qui, par défaut, est défini sur % pour sélectionner toutes les adresses IP.

Tableau 67. Débit

Domaine	Requête de base	Entité principale
interne - non disponible	Débit du serveur de la base de données	non disponible
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT
Adresse IP du serveur	LIKE	%

Débit (graphique)

Ce rapport est une version au format de graphique à courbes des libellés répartis du rapport tabulaire Débit. Il répertorie le nombre total d'accès au cours de la période de rapport, un point de données par Heure de début de période.

Vous pouvez restreindre la sortie de ce rapport à l'aide du paramètre d'exécution Adresses IP serveur qui, par défaut, est défini sur % pour sélectionner toutes les adresses IP.

Tableau 68. Débit (graphique)

Domaine	Requête de base	Entité principale
Accès	Débit du serveur de la base de données - Graphique	Période d'accès
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT
Adresse IP du serveur	LIKE	%

Rapports Trace d'audit d'activité d'utilisateur

La sélection du menu Trace d'audit d'activité d'utilisateur affiche deux rapports. En outre, de chacun de ces rapports, un troisième rapport peut être produit. Voir :

- Trace d'audit de l'activité d'utilisateur
- Activités système/sécurité
- Activité détaillée des utilisateurs Guardium (Exploration)

Trace d'audit de l'activité d'utilisateur

Pour la période de rapport, pour chaque nom d'utilisateur vu sur une entité Audit d'activité d'utilisateur Guardium, chaque ligne affiche les éléments suivants : Nom d'utilisateur Guardium, Description du type d'activité (issue de l'entité Types d'activité Guardium), Nombre d'entités modifiées, Nom d'hôte et nombre total d'entités Audits d'activité Guardium pour cette ligne.

À partir de n'importe quelle ligne de ce rapport, le rapport d'Activité détaillée des utilisateurs Guardium est disponible en tant que rapport d'analyse.

Tableau 69. Trace d'audit de l'activité d'utilisateur

Domaine	Requête de base	Entité principale
Activité Guardium	Trace d'audit de l'activité d'utilisateur	Audit d'activité utilisateur Guardium
Paramètre d'exécution	Opérateur	Valeur par défaut
Nom d'hôte	LIKE	%
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Activités système/sécurité

Pour la période de rapport, pour chaque nom d'utilisateur vu sur une entité Audit d'activité d'utilisateur Guardium, chaque ligne affiche les éléments suivants : Nom d'utilisateur Guardium, Description du type d'activité (issue de l'entité Types d'activité Guardium), Nombre d'entités modifiées, Nom d'hôte et nombre total d'entités Audits d'activité Guardium pour cette ligne.

À partir de n'importe quelle ligne de ce rapport, le rapport d'Activité détaillée des utilisateurs Guardium est disponible en tant que rapport d'analyse.

Tableau 70. Activités système/sécurité

Domaine	Requête de base	Entité principale
Activité Guardium	Trace d'audit de l'activité d'utilisateur	Audit d'activité utilisateur Guardium
Paramètre d'exécution	Opérateur	Valeur par défaut
Nom d'hôte	LIKE	%
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Activité détaillée des utilisateurs Guardium (Exploration)

Ce rapport n'est pas disponible dans le menu, mais peut être ouvert pour n'importe quelle ligne du rapport Trace d'audit d'activité d'utilisateur ou du rapport Activités système/sécurité. Pour la ligne sélectionnée du rapport, en fonction du Nom d'utilisateur et de la Description du type d'activité, ce rapport énumère les valeurs d'attribut suivantes, toutes issues de l'entité Audit d'activité d'utilisateur Guardium, à l'exception de la Description du type d'activité, qui provient de l'entité Types d'activité Guardium : Nom d'utilisateur, Horodatage, Entité modifiée, Description d'objet, Toutes les valeurs et un nombre d'entités Audits d'activité d'utilisateur Guardium pour la ligne.

Tableau 71. Activité détaillée des utilisateurs Guardium (Exploration)

Domaine	Requête de base	Entité principale
Activité Guardium	Activité détaillée des utilisateurs Guardium	Audit d'activité utilisateur Guardium
Paramètre d'exécution	Opérateur	Valeur par défaut
Description du type d'activité		valeur du rapport appelant
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT
Nom d'utilisateur		valeur du rapport appelant

Avertissement : les utilisateurs doivent savoir que les activités de l'utilisateur racine et d'autres comptes système sensibles sont enregistrées. L'exploration dans l'activité de ces utilisateurs peut afficher des commandes sensibles et des mots de passe saisis sur la ligne de commande. Par conséquent, dans la mesure du possible, les utilisateurs ne doivent pas entrer d'informations de ligne de commande sensibles qu'ils ne voudraient pas afficher sur ce rapport d'exploration.

Listes des tâches des utilisateurs

Affiche pour chaque processus d'audit Guardium : une description, un nom de connexion, une action requise (examiner ou approuver), le statut, l'utilisateur qui a signé ou révisé et la date d'exécution de la tâche spécifiée.

Tableau 72. Listes des tâches des utilisateurs

Domaine	Requête de base	Entité principale
interne - non disponible	Liste des tâches des utilisateurs	non disponible
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Commentaires utilisateur partageables

Les commentaires utilisateur partageables sont tous des commentaires, à l'exception des commentaires définis pour le moteur d'inspection, la politique installée et les résultats des processus d'audit. Pour chaque commentaire utilisateur partageable, ce rapport énumère la date de création, le type d'élément auquel il s'applique (une alerte, par exemple), l'utilisateur qui a créé le commentaire et le contenu du commentaire.

Remarque : les commentaires définis pour les moteurs d'inspection, les politiques installées ou les résultats des processus d'audit peuvent être visualisés à partir des définitions individuelles, mais ils ne peuvent pas être affichés dans un rapport.

Tableau 73. Commentaires utilisateur partageables

Domaine	Requête de base	Entité principale
Commentaires	Commentaires définis	Commentaires
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 2 MOIS
Fin de la période	<=	MAINTENANT

Niveaux d'utilisation d'unités

Les rapports par défaut suivants fournissent des données d'utilisation des unités :

- Utilisation d'unités : affiche le niveau d'utilisation maximum de chaque unité dans la période donnée. Une exploration affiche les détails d'une unité dans toutes les périodes du rapport.
- Distribution de l'utilisation d'unités : pour chaque unité, ce rapport affiche le pourcentage de périodes dans le calendrier du rapport dont les niveaux d'utilisation sont bas, moyens et élevés.
- Seuils d'utilisation : ce rapport prédéfini affiche toutes les valeurs de seuil bas et haut pour tous les paramètres d'utilisation d'unité.
- Récapitulatif quotidien de l'utilisation d'unités - Fournit un résumé quotidien des données d'utilisation d'unité.

Tableau 74. Niveaux d'utilisation d'unités

Domaine	Requête de base	Entité principale
Interne - non disponible	Distribution de l'utilisation d'unités	Niveaux d'utilisation d'unités
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 24 HEURES
Fin de la période	<=	MAINTENANT

Valeurs changées

Pour la période considérée, ce rapport fournit des informations détaillées sur les changements de valeurs surveillées. Toutes les valeurs d'attribut affichées proviennent de l'entité Surveiller les valeurs. La requête sur laquelle ce rapport est basé contient une séquence de tri non standard, comme suit :

- Adresse IP serveur
- Type de base de données
- Horodatage de l'audit
- Nom de la table d'audit
- Propriétaire de l'audit

La requête sur laquelle ce rapport est basé comporte un certain nombre de paramètres d'exécution, tous utilisant l'opérateur LIKE et par défaut la valeur %, ce qui signifie que toutes les valeurs seront sélectionnées.

Pour chaque valeur surveillée sélectionnée, une ligne de rapport contient les éléments suivants : Horodatage, Adresse IP serveur, Type de base de données, Nom de service, Nom de base de données, Nom de la connexion d'audit, Horodatage de l'audit, Nom de la table d'audit, Propriétaire de l'audit, Action d'audit, Ancienne valeur d'audit, Nouvelle valeur d'audit, Texte SQL, ID déclenché et un nombre d'entités Colonnes changées pour cette ligne.

Tableau 75. Valeurs changées

Domaine	Requête de base	Entité principale
Valeur changée	Valeurs changées	Colonnes changées

Domaine	Requête de base	Entité principale
Paramètre d'exécution	Opérateur	Valeur par défaut
Action d'audit	LIKE	%
Nom de la connexion d'audit	LIKE	%
Propriétaire de l'audit	LIKE	%
Nom de la table d'audit	LIKE	%
Type de base de données	LIKE	%
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT
Adresse IP du serveur	LIKE	%

Rubrique parent : Exploitation des rapports prédéfinis

Rapports d'utilisateur prédéfinis

La présente section fournit une brève description de tous les rapports prédéfinis sur la présentation d'utilisateur par défaut.

Pour une description des rapports sur la configuration d'administrateur par défaut, voir Rapports d'administration prédéfinis.

Remarque : Si la sécurité au niveau des données pour les données observées a été activée (voir les paramètres du Profil global), la sortie du processus d'audit est filtrée afin que les utilisateurs ne puissent visualiser que les informations de leur base de données.

Afficher la politique installée

Le rapport Politique installée affiche des informations sur la politique installée. Cliquez sur le lien Politique installée pour afficher les règles de politique dans une fenêtre distincte.

Nombre de bases de données par type

Affiche le nombre de serveurs et de clients pour chaque type de base de données surveillée (la période par défaut est le jour courant).

Taux des demandes

Par défaut, affiche le taux des demandes au cours des deux dernières heures. Ce rapport graphique est destiné à afficher uniquement l'activité récente. Si vous modifiez les paramètres d'exécution De et A pour inclure un délai plus long, vous pouvez recevoir un message indiquant qu'il y a trop de données. (Utilisez un rapport tabulaire pour afficher une période plus longue.)

Sessions par type de serveur

Pour chaque type de serveur (DB2, Informix, etc.), une ligne de ce rapport affiche le nombre total de sessions ouvertes pendant la période de rapport (par défaut, les trois dernières heures).

Exécution DML sur objets sensibles

Pour chaque verbe SQL issu du groupe Commandes DML qui fait référence à un Nom d'objet dans le groupe Objets sensibles, ce rapport affiche une ligne pour chaque Période d'accès, Adresse IP du client et Programme source, avec un nombre total d'objets référencés dans cette ligne. Bien que le titre du rapport contienne le mot Exécutions, il n'y a aucune garantie que toutes les commandes rapportées ont été effectivement exécutées.

Utilisation d'objets sensibles

Pour chaque objet dans le groupe Objets sensibles, affiche une ligne pour chaque Adresse IP du client et Programme source ayant fait référence à l'objet pendant la période de rapport et un nombre de références d'objet.

Le groupe Objets sensibles est vide au moment de l'installation. Une personne de votre entreprise doit remplir le groupe avec l'ensemble approprié de membres.

Activité par adresse IP client

Pour chaque adresse IP du client visualisée pendant la période de rapport, une ligne comptabilise le nombre de Verbes SQL, les noms d'objets et le nombre total de sessions.

Serveurs de base de données

Pour chaque adresse IP du serveur accessible pendant la période de rapport, une ligne du rapport affiche les éléments suivants : Type de serveur, Nom de la base de données, Nom de service, nombre de programmes source qui accèdent à ce serveur et nombre total de sessions pour cette ligne.

Accès IMS (z/OS)

Utilisez cette option pour rapporter l'accès à IMS (z/OS).

Tableau 1. Accès IMS (z/OS)

Domaine	Requête de base	Entité principale
Accès	Accès IMS	Serveur client

Domaine	Requête de base	Entité principale
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 2 HEURES
Fin de la période	<=	MAINTENANT

Objet IMS (z/OS)

Utilisez cette option pour rapporter l'objet à IMS (z/OS).

Tableau 2. Objet IMS (z/OS)

Domaine	Requête de base	Entité principale
Accès	Objet IMS	Objet
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 2 HEURES
Fin de la période	<=	MAINTENANT

Evénement IMS (z/OS)

Utilisez cette option pour rapporter l'événement à IMS (z/OS).

Tableau 3. Evénement IMS (z/OS)

Domaine	Requête de base	Entité principale
Accès	Evénement IMS	SQL
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 2 HEURES
Fin de la période	<=	MAINTENANT

Détails d'accès aux données IMS (z/OS)

Utilisez cette option pour rapporter les détails d'accès aux données à IMS (z/OS).

Tableau 4. Détails d'accès aux données IMS (z/OS)

Domaine	Requête de base	Entité principale
Accès	Détails d'accès aux données IMS	SQL complet
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 2 HEURES
Fin de la période	<=	MAINTENANT
Adresse IP client	LIKE	
DBUserName	LIKE	
Nom IMS	LIKE	
IP du serveur	LIKE	

Violations de politique

Pour chaque violation de règle de politique consignée pendant la période de rapport, ce rapport fournit les éléments suivants : Horodatage issu de l'entité Violation de règle de politique, Description de règle d'accès, Adresse IP client, Adresse IP serveur, Nom d'utilisateur de la base de données, Chaîne SQL complète issue de l'entité Violation de règle de politique, Description de gravité, et nombre de violations pour cette ligne. Vous ne pouvez pas accéder à la requête sur laquelle ce rapport est basé (Liste des violations de politique avec sévérité), mais vous pouvez cloner le rapport.

Distribution des exceptions

Chaque secteur du graphique circulaire représente la proportion d'exceptions pour chaque valeur d'attribut Description de l'exception (issue de l'entité Type d'exception) qui a été consignée au cours de la période de rapport.

Comme pour n'importe quel graphique, vous pouvez explorer le graphique circulaire pour afficher la version tabulaire de la requête sur laquelle le graphique est basé. Il existe plusieurs rapports d'exceptions accessibles à partir de ce rapport tabulaire (ou des explorations en aval à partir de ce rapport) qui sont disponibles ici, mais ne sont pas inclus dans les menus.

Moniteur d'exceptions

Nombre d'exceptions consignées au cours de la période de rapport. Un point de données est créé chaque fois que vous actualisez le rapport sur votre portail.

Echecs des tentatives de connexion d'utilisateur

Pour chaque échec de tentative de connexion pendant la période de rapport, répertorie les éléments suivants : Nom d'utilisateur, Adresse source, Adresse de destination et Type de protocole de base de données pour le serveur auquel l'utilisateur a tenté de se connecter.

Erreurs SQL

Pour chaque erreur SQL pendant la période de rapport, affiche les éléments suivants : Adresse IP client, Adresse IP serveur, Type de serveur, Nom d'utilisateur de la base de données, Texte d'erreur renvoyé par la base de données et total des occurrences d'erreur pour cet enregistrement.

Nombre d'exceptions

Nombre total d'exceptions (entités d'exception) consignées au cours de la période de rapport.

Connexions d'utilisateurs arrêtés

Répertorie toutes les connexions établies par les utilisateurs de la base de données qui sont membres du groupe d'utilisateurs arrêtés de la base de données. Chaque ligne répertorie les éléments suivants : Nom d'utilisateur de la base de données, Adresse IP client, Adresse IP serveur, Type de serveur, Programme source, heure de dernière connexion (valeur maximale de l'attribut Début de session) et nombre de sessions pour la ligne.

Le groupe Utilisateurs arrêtés de la base de données est vide au moment de l'installation. Il doit être rempli par une personne sur votre site. La requête sur laquelle ce rapport est basé (Connexions d'utilisateurs arrêtés) ne peut pas être consultée à partir d'un générateur de requête.

Dernière connexion des utilisateurs actifs

Dernière connexion enregistrée pendant la période de rapport pour chaque membre du groupe Utilisateurs actifs. Tous les membres du groupe sont répertoriés, y compris en l'absence de connexion pendant la période de rapport. Ce rapport est différent de la plupart des autres rapports basés sur des membres d'un groupe. Dans le cas "normal", si aucune activité n'est trouvée pour un membre, ce membre n'est pas répertorié.

Chaque ligne répertorie les éléments suivants : Nom d'utilisateur de la base de données, Adresse IP client, Adresse IP serveur, Type de serveur, Programme source, heure de dernière connexion (valeur maximale de l'attribut Début de session) et nombre de sessions pour la ligne.

Le groupe Utilisateurs actifs est vide au moment de l'installation. Il doit être rempli par une personne sur votre site. La requête sur laquelle ce rapport est basé (Dernières connexions des utilisateurs actifs) ne peut pas être consultée à partir d'un générateur de requête.

Utilisateurs actifs sans activité

Liste des membres du groupe Utilisateurs actifs qui n'ont pas eu d'activité pendant la période de rapport. Ce rapport est vide si tous les utilisateurs ont eu une activité pendant la période concernée.

Le groupe Utilisateurs actifs est prédéfini mais il est vide au moment de l'installation. Il doit être rempli par une personne sur votre site. La requête sur laquelle ce rapport est basé (Utilisateurs actifs sans activité) ne peut pas être consultée à partir d'un générateur de requête.

Echecs des tentatives de connexion d'utilisateur arrêtés

Répertorie les échecs de tentatives de connexion par les utilisateurs de la base de données qui sont membres du groupe d'utilisateurs arrêtés de la base de données. Ce rapport est vide s'il n'y a eu aucune tentative de connexion ayant échouée effectuée par un membre de ce groupe pendant la période de rapport.

Le groupe Utilisateurs arrêtés de la base de données est prédéfini mais il est vide au moment de l'installation. Il doit être rempli par une personne sur votre site. La requête intégrée pour ce rapport n'est pas accessible. La requête sur laquelle ce rapport est basé (Echecs des tentatives de connexion par des utilisateurs arrêtés) ne peut pas être consultée à partir d'un générateur de requête.

Erreurs excessives par période

Affiche le nombre d'erreurs par période, par exemple plus de N erreurs en 60 minutes pour les mêmes adresse IP client, adresse IP serveur, type de serveur, nom d'utilisateur de la base de données.

Utilisateurs inactifs depuis

Affiche l'utilisateur et le dernier début de session pour tous les utilisateurs possédant des enregistrements d'accès et dont l'horodatage de début de session maximal est antérieur à 90 jours. (Un utilisateur inactif est ignoré s'il ne s'est jamais connecté, ou si toutes ses anciennes connexions ont été purgées)

Connexion des administrateurs

Pour chaque Nom d'utilisateur de la base de données inclus dans le groupe Administrateurs, qui a établi une ou plusieurs sessions pendant la période de rapport, chaque ligne répertorie les éléments suivants : Adresse IP client, Nom d'utilisateur de la base de données, Programme source, Heure de début de session et Nombre de sessions pour cette ligne.

Connexion des utilisateurs prédéfinis de la base de données

Pour chaque Nom d'utilisateur de la base de données inclus dans le groupe Utilisateurs prédéfinis de la base de données, qui a établi une ou plusieurs sessions pendant la période de rapport, chaque ligne répertorie les éléments suivants : Nom d'utilisateur de la base de données, Adresse IP client, Adresse IP serveur, Programme source, Nom de la base de données, Nom de service, et Nombre de sessions pour cette ligne.

Utilisation de commandes d'administration

Pour chaque Verbe SQL inclus dans le groupe Commandes d'administration qui a été visualisé pendant la période de rapport, ce rapport répertorie les éléments suivants : Verbe SQL, Profondeur, Nom d'objet et Adresse IP client, ainsi qu'un nombre d'objets référencés.

Utilisation d'objets d'administration

Pour chaque Nom d'objet inclus dans le groupe Objets d'administration qui a été visualisé pendant la période de rapport, chaque ligne répertorie les éléments suivants : Nom d'objet, Adresse IP client, Adresse IP serveur, Nom de service, Nom de base de données, Programme source, Nom d'utilisateur de la base de données et Nombre d'objets pour cette ligne.

Exécution DML sur objets d'administration

Pour chaque verbe SQL issu du groupe Commandes DML qui fait référence à un Nom d'objet dans le groupe Objets d'administration, ce rapport affiche une ligne pour les éléments suivants : Nom d'utilisateur de la base de données, Adresse IP client, Adresse IP serveur, Type de serveur, Nom de service, Nom de base de données, Verbe SQL, Nom d'objet et Nombre d'objets référencés dans cette ligne.

Exécution des commandes BACKUP

Pour chaque verbe SQL issu du groupe Commandes BACKUP qui a été visualisé pendant la période de rapport, ce rapport affiche les éléments suivants : Adresse IP client, Adresse IP serveur, Nom de service, Nom d'utilisateur de la base de données, Programme source, Nom de base de données, Nom d'objet, Verbe SQL et Nombre d'objets référencés dans cette ligne.

Exécution des commandes RESTORE

Pour chaque verbe SQL issu du groupe Commandes BACKUP qui a été visualisé pendant la période de rapport, ce rapport affiche les éléments suivants : Adresse IP client, Adresse IP serveur, Nom de service, Nom d'utilisateur de la base de données, Programme source, Nom de base de données, Nom d'objet, Verbe SQL et Nombre d'objets référencés dans cette ligne.

Exécution des commandes REVOKE

Pour chaque verbe SQL issu du groupe Commandes REVOKE qui a été visualisé pendant la période de rapport, ce rapport affiche les éléments suivants : Adresse IP client, Adresse IP serveur, Nom de service, Nom d'utilisateur de la base de données, Programme source, Nom de base de données, Nom d'objet, Verbe SQL et Nombre d'objets référencés dans cette ligne.

Exécution des commandes KILL

Pour chaque verbe SQL issu du groupe Commandes KILL qui a été visualisé pendant la période de rapport, ce rapport affiche les éléments suivants : Adresse IP client, Adresse IP serveur, Nom de service, Nom d'utilisateur de la base de données, Programme source, Nom de base de données, Nom d'objet, Verbe SQL et Nombre d'objets référencés dans cette ligne.

Exécution des commandes DBCC

Pour chaque verbe SQL issu du groupe Commandes DBCC qui a été visualisé pendant la période de rapport, ce rapport affiche les éléments suivants : Adresse IP client, Adresse IP serveur, Nom de service, Nom d'utilisateur de la base de données, Programme source, Nom de base de données, Nom d'objet, Instruction SQL et Nombre d'objets référencés dans cette ligne.

Exécution des commandes GRANT

Pour chaque verbe SQL issu du groupe Commandes GRANT qui a été visualisé pendant la période de rapport, ce rapport affiche les éléments suivants : Adresse IP client, Adresse IP serveur, Nom de service, Nom d'utilisateur de la base de données, Programme source, Nom de base de données, Nom d'objet, Verbe SQL et Nombre d'objets référencés dans cette ligne.

Utilisation du compte privilégié

Affiche l'utilisateur, le verbe SQL et le nombre de périodes pendant lesquelles le verbe SQL a été exécuté par un utilisateur dans le groupe Administrateurs

Accès de l'utilisateur privilégié aux objets métiers

Affiche l'utilisateur, le verbe SQL, l'objet et le verbe SQL exécuté par un objet qui se trouve dans un groupe sélectionné d'objets métier

Exécution des commandes CREATE

Pour chaque verbe SQL issu du groupe Commandes CREATE qui a été visualisé pendant la période de rapport, ce rapport affiche les éléments suivants : Adresse IP client, Adresse IP serveur, Nom de service, Nom d'utilisateur de la base de données, Programme source, Nom de base de données, Nom d'objet, Verbe SQL et Nombre d'objets référencés dans cette ligne.

Commandes DDL

Toutes les commandes DDL envoyées à la base de données. Ce rapport affiche l'adresse IP client à partir de laquelle la DDL a été demandée, le verbe SQL principal (une commande DDL spécifique) et le total des objets accessibles pour cet enregistrement.

Pour chaque verbe SQL issu du groupe Commandes DDL qui a été visualisé pendant la période de rapport, ce rapport affiche les éléments suivants : Adresse IP client, Adresse IP serveur, Type de serveur, Verbe SQL et Nombre de commandes référencées dans la ligne.

Exécution des commandes ALTER

Toutes les commandes ALTER émises. Le rapport affiche l'adresse IP du client à partir de laquelle la DDL a été demandée, l'adresse IP du serveur, le nom du service, le nom d'utilisateur de la base de données, le programme source, le nom de la base de données, le nom de l'objet et le verbe SQL principal (commande DDL spécifique) pour chaque combinaison d'adresse IP client/commande DDL répertoriée sur cette ligne spécifique.

Pour chaque verbe SQL issu du groupe Commandes ALTER qui a été visualisé pendant la période de rapport, ce rapport affiche les éléments suivants : Adresse IP client, Adresse IP serveur, Nom de service, Nom d'utilisateur de la base de données, Programme source, Nom de base de données, Nom d'objet, Verbe SQL et Nombre d'objets référencés dans cette ligne.

Distribution DDL

Ce graphique à barres affiche la répartition des commandes visualisées à partir du groupe Commandes DDL pendant la période de rapport. Pour chaque commande visualisée, une barre représente le nombre total d'objets affectés.

Exécution des commandes DROP

Pour chaque verbe SQL issu du groupe Commandes DROP qui a été visualisé pendant la période de rapport, ce rapport affiche les éléments suivants : Adresse IP client, Adresse IP serveur, Nom de service, Nom d'utilisateur de la base de données, Programme source, Nom de base de données, Nom d'objet, Verbe SQL et Nombre d'objets référencés dans cette ligne.

Un utilisateur Une adresse IP

Pour chaque nom d'utilisateur de base de données pour lequel les données de session ont été collectées au cours de la période de rapport, chaque ligne de ce rapport affiche le nombre d'adresses IP du client à partir desquelles l'utilisateur s'est connecté et le nombre total de sessions.

Récapitulatif d'activité d'adresse IP client

Ce rapport affiche l'activité de la période de rapport à partir d'une seule adresse IP du client spécifiée en tant que paramètre d'exécution. Chaque ligne du rapport affiche les éléments suivants : Adresse IP client, Programme source, Verbe SQL, Profondeur (de la phrase dans la commande SQL), Nom d'objet et nombre de fois où cet objet a été référencé pour cette ligne.

Liste de sessions

Ce rapport répertorie toutes les sessions de la base de données pour la période de rapport. Pour chaque session, le rapport affiche les éléments suivants : Horodatage de la session (entité), Début de session (horodatage), Type de serveur, Adresse IP client, Adresse IP serveur, Port du client, Port du serveur, Protocole réseau, Protocole de base de données, Version du protocole de la base de données, Nom d'utilisateur de la base de données, Programme source et Nombre de sessions pour cette ligne (qui doit toujours être égal à 1).

Comme pour la plupart des rapports, des rapports détaillés sont disponibles. Il existe un certain nombre de rapports de session accessibles à partir de ce rapport, mais ils ne sont inclus dans aucun menu. Il s'agit des rapports suivants comportant les paramètres d'exécution pour les rapports définis à l'aide des valeurs issues de la ligne sélectionnée du rapport :

Tableau 5. Liste de sessions

Rapport	Paramètres d'exécution
Sessions par adresse IP client	Adresse IP serveur, Type de serveur
Sessions par adresse IP serveur	Type de serveur
Sessions par programme source	Type de serveur, Adresse IP serveur
Sessions par utilisateur	Type de serveur, Adresse IP serveur
Détails des sessions par serveur	Type de serveur, Adresse IP serveur

Liste de commandes

Ce rapport répertorie tous les verbes SQL visualisés pendant la période de rapport. Au niveau le plus externe, les commandes sont regroupées par l'heure de Début de période issue de l'entité Période d'accès, qui est généralement une heure, à l'heure. Votre administrateur Guardium peut modifier la durée d'accès en modifiant la granularité de consignation, qui est d'une heure par défaut. Pour chaque période d'accès de la période de rapport, chaque ligne répertorie l'heure de début de la période d'accès, un verbe SQL, la profondeur du verbe dans l'instruction SQL, le parent (pointeur vers le verbe propriétaire) et un nombre d'occurrences pour la ligne .

Liste d'objets

Ce rapport répertorie tous les objets visualisés pendant la période de rapport. Au niveau le plus externe, les objets sont regroupés par l'heure de Début de période issue de l'entité Période d'accès, qui est généralement une heure, à l'heure. Votre administrateur SQL Guard peut modifier la durée d'accès en modifiant la granularité de consignation, qui est d'une heure par défaut. Pour chaque période d'accès dans la période de rapport, chaque ligne répertorie l'heure de début de la période d'accès, un nom d'objet et le nombre d'occurrences pour cette ligne.

Récapitulatif d'activité d'objet

Ce rapport affiche l'activité de la période de rapport pour un nom d'objet unique, spécifié en tant que paramètre d'exécution. Chaque ligne du rapport affiche les éléments suivants : Adresse IP client, Programme source, Verbe SQL, Profondeur (de la phrase dans la commande SQL), Nom d'objet et nombre de fois où cet objet a été référencé pour cette ligne.

Candidats à l'archivage

Ce rapport répertorie les objets (tables de base de données ou procédures mémorisées, par exemple) qui n'ont pas été consultés pendant une période prolongée. Vous ne pouvez pas accéder à la requête sur laquelle ce rapport est basé.

Activité du partage de fichiers Windows

Ce rapport répertorie toute l'activité SQL du partage de fichiers Windows visualisée pendant la période de rapport. Au niveau le plus externe, les commandes SQL sont regroupées par l'heure de Début de période issue de l'entité Période d'accès, qui est généralement une heure, à l'heure. Votre administrateur Guardium peut modifier la durée d'accès en modifiant la granularité de consignation, qui est d'une heure par défaut. Pour chaque période d'accès dans la période de rapport, chaque ligne répertorie l'heure de début de la période d'accès, le nom du service, l'adresse IP du client, l'adresse IP du serveur, le programme source, SQL (issu de l'entité SQL) et un nombre d'occurrences pour la ligne. Vous ne pouvez pas accéder à la requête sur laquelle ce rapport est basé, mais vous pouvez cloner le rapport.

Détails des accès par heure

Ce rapport produit une liste très détaillée pour chaque nom d'utilisateur de la base de données visualisé dans la période de rapport, à savoir une heure par défaut pour ce rapport. Chaque ligne du rapport répertorie les éléments suivants : Nom d'utilisateur de la base de données, Adresse IP client, Adresse IP serveur, Début de période, Programme source, SQL (issu de l'entité SQL) et nombre d'occurrences pendant la période d'accès.

SQL complet par nom d'utilisateur de base de données

Ce rapport affiche les valeurs d'attribut SQL complet de la période de rapport qui ont été consignées pour un Nom d'utilisateur de la base de données unique, spécifié en tant que paramètre d'exécution. Chaque ligne du rapport affiche les éléments suivants : ID SQL complet, Horodatage (issu de l'entité SQL complet), Adresse IP client, Nom d'utilisateur de la base de données, Début de session, Programme source, SQL complet et nombre d'occurrences pour la ligne.

SQL complet par adresse IP client

Ce rapport affiche les valeurs d'attribut SQL complet de la période de rapport qui ont été consignées pour une adresse IP client unique, spécifiée en tant que paramètre d'exécution. Chaque ligne du rapport affiche les éléments suivants : ID SQL complet, Horodatage (issu de l'entité SQL complet), Adresse IP client, Nom d'utilisateur de la base de données, Début de session, Programme source, SQL complet et nombre d'occurrences pour la ligne.

Liste Flat LOG

Répertorie les tâches de traitement Flat Log.

Résultats du processus de classification

Répertorie les tâches de processus de classification.

DW Objets dormants

Affiche tous les membres d'un groupe qui ne sont pas membres d'un deuxième groupe, en mettant l'accent sur les tables dormantes. Par exemple, ce rapport montre les objets qui se trouvent dans le groupe de tous les objets, mais qui n'ont pas été utilisés dans une instruction SELECT.

DW Objets-champs dormants

Affiche tous les membres d'un groupe qui ne sont pas membres d'un deuxième groupe, en mettant l'accent sur les tables et les colonnes dormantes. Dans ce cas, les groupes sont de type 2-tuple (membres composites d'une paire d'attributs de valeur). Par exemple, ce rapport montre les objets qui se trouvent dans le groupe de tous les objets et tous les champs, mais qui n'ont pas été utilisés dans une instruction SELECT.

DW Accès EXECUTE à l'objet

Utilisez ce rapport pour remplir le groupe appelé DW Objets EXECUTE avec un ensemble de noms de procédures mémorisées exécutées. Utilisez ensuite le mappage indirect dans Générateur de groupe/Proc. appelante générée automatiquement pour générer tous les objets utilisés dans ces procédures.

DW Accès SELECT à l'objet

Ce rapport affiche tous les noms d'objet accessibles via une instruction SELECT.

DW Accès SELECT à l'objet/au champ

Ce rapport affiche tous les noms d'objet et de champ accessibles via une instruction SELECT.

Requêtes à exécution longue

Pour la période de rapport, ce rapport répertorie les requêtes les plus longues, avec en tête de liste le temps d'exécution moyen le plus long. Pour chaque requête, répertorie l'Adresse IP client, l'Adresse IP serveur, SQL, le Début de période (issu de l'entité Période d'accès), le Temps moyen d'exécution et le nombre d'occurrences pour cette ligne. Vous ne pouvez pas accéder à la requête sur laquelle ce rapport est basé.

Débit

Ce rapport produit un comptage de toutes les adresses IP serveur visualisées et des accès totaux pendant la période de rapport. Au niveau le plus externe, les accès sont regroupés par l'heure de Début de période issue de l'entité Période d'accès, qui est généralement une heure, à l'heure. Votre administrateur Guardium peut modifier la durée d'accès en modifiant la granularité de consignation, qui est d'une heure par défaut. Chaque ligne répertorie l'heure de début de la période, le nombre d'adresses IP du serveur visualisées et le nombre total d'accès pour la ligne.

Vous pouvez restreindre la sortie de ce rapport à l'aide du paramètre d'exécution Adresse IP serveur qui, par défaut, est défini sur "%" pour sélectionner toutes les adresses IP.

Débit (graphique)

Ce rapport est une version de graphique à courbes des libellés distribués du rapport tabulaire Débit, qui répertorie le nombre total d'accès pendant la période de rapport, un point de données par heure de début de période.

Vous pouvez restreindre la sortie de ce rapport à l'aide du paramètre d'exécution Adresse IP serveur qui, par défaut, est défini sur "%" pour sélectionner toutes les adresses IP.

Nombre de tâches actives de jeux de confidentialité

Nombre de processus d'audit Guardium actifs contenant une ou plusieurs tâches de jeu de confidentialité. Lorsque la gestion centrale est utilisée, ce rapport contient des données uniquement sur Central Manager et est vide sur toutes les unités gérées (le message standard s'affiche : Aucune donnée trouvée pour la requête demandée). Ce rapport comporte des paramètres d'exécution non standard : il n'y a pas de paramètres de date de début et de fin, de sorte que tous les processus d'audit contenant une ou plusieurs tâches de jeu de confidentialité sont rapportés. Vous pouvez cloner la requête sur laquelle ce rapport est basé (Nombre de processus de jeu de confidentialité actifs), mais vous ne pouvez pas cloner ou régénérer le rapport par défaut. La requête clonée contient tous les paramètres d'exécution standard (y compris les dates de début et de fin).

File d'attente de travaux Guardium

Affiche la file d'attente de travaux Guardium. Pour chaque travail, elle répertorie les attributs suivants : ID exécution de processus, Type de processus, Statut, ID processus cls/éval, ID résultat de rapport, Description cls/éval, Description de la tâche d'audit, Durée en file d'attente, Heure de début, Heure de fin et Sources de données.

Tableau 6. File d'attente de travaux Guardium

Domaine	Requête de base	Entité principale
interne - non disponible	File d'attente de travaux Guardium	non disponible
Paramètre d'exécution	Opérateur	Valeur par défaut
Description du travail	LIKE	%
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Bases de données reconnues

Pour la période de génération de rapports, pour chaque entité de Port reconnu où la valeur d'attribut Type de base de données est NOT LIKE Inconnu, ce rapport énumère l'Horodatage de l'analyse, l'IP serveur, le Nom d'hôte de serveur, le Type de base de données, le Port, le Type de port et le nombre de Ports reconnus pour la ligne.

Tableau 7. Bases de données reconnues

Domaine	Requête de base	Entité principale
Reconnaissance automatique	Bases de données reconnues	Port reconnu
Paramètre d'exécution	Opérateur	Valeur par défaut
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Sources de données

Ce rapport apparaît sur la présentation par défaut pour les administrateurs et les utilisateurs. Voir la rubrique Sources de données sur la page Rapports prédéfinis - Communs.

Historique des versions de la source de données

Ce rapport apparaît sur la présentation par défaut pour les administrateurs et les utilisateurs. Voir la rubrique Historique des versions de source de données sur la page Rapports prédéfinis - Communs.

File d'attente de travaux Guardium

Affiche la file d'attente de travaux Guardium. Pour chaque travail, elle répertorie les attributs suivants : ID exécution de processus, Type de processus, Statut, ID processus cls/éval, ID résultat de rapport, Description cls/éval, Description de la tâche d'audit, Durée en file d'attente, Heure de début, Heure de fin et Sources de données.

Examens des processus d'audit en attente

Pour chaque nom de connexion d'utilisateur Guardium, ce rapport répertorie le nombre et le type des processus d'audit Guardium en attente. Un processus d'audit en attente a une valeur d'attribut Statut (dans l'entité Liste de tâches des résultats des tâches) autre que Signé/révisé. Ce rapport comporte des paramètres d'exécution non standard : il n'y a pas de dates de début et de fin, ce qui signifie que tous les résultats de tâches en attente sont rapportés. Vous pouvez cloner la requête sur laquelle ce rapport est basé (même nom), mais vous ne pouvez pas cloner ou régénérer le rapport par défaut. La requête clonée contient tous les paramètres d'exécution standard (y compris les dates de début et de fin).

Nombre de processus d'audit actifs

Nombre de processus d'audit Guardium actifs. Lorsque la gestion centrale est utilisée, ce rapport contient des données uniquement sur Central Manager et est vide sur toutes les unités gérées (le message standard s'affiche : Aucune donnée trouvée pour la requête demandée). Ce rapport comporte des paramètres d'exécution non standard : il n'y a pas de paramètres de date de début et de fin, de sorte que tous les processus d'audit actifs sont rapportés. Vous pouvez cloner la requête sur laquelle ce rapport est basé (Nombre de processus actifs), mais vous ne pouvez pas cloner ou régénérer le rapport par défaut. La requête clonée contient tous les paramètres d'exécution standard (y compris les dates de début et de fin).

Afficher la politique installée

Dans le panneau Politique installée, ce rapport spécial affiche les informations sur la politique installée, comme son nom, le nombre de règles qu'elle contient et ses paramètres de définition. Vous ne pouvez pas accéder à la requête sur laquelle ce rapport est basé.

Nombre de violations de politiques

Pour la période de rapport, ce rapport affiche le nombre de violations de politique consignées.

Alertes de seuil consignées

Ce rapport affiche une barre représentant le nombre total d'alertes consignées pendant la période de rapport, pour chaque type d'alerte de seuil consignée, en fonction de l'attribut Description d'alerte de l'entité Détails de l'alerte de seuil.

Alertes T/R consignées

Ce rapport affiche une barre représentant le nombre total d'alertes consignées pendant la période de rapport, pour chaque type d'alerte en temps réel consignée, en fonction de l'attribut Description de la règle d'accès de l'entité Violation de règle de politique.

Violations/Incidents

Consultez la rubrique Gestion des incidents.

Rubrique parent : Exploitation des rapports prédéfinis

Rapports prédéfinis communs

La présente section fournit une brève description de tous les rapports prédéfinis sur les présentations d'utilisateur par défaut et d'administrateur par défaut.

Les rapports communs sont les suivants :

- Historique des versions de la source de données
- Sources de données

Moniteur d'état

Le rapport graphique du Moniteur d'état affiche l'état actuel du dispositif Guardium : nombre de paquets par seconde et de requêtes par seconde traités, espace disque et mémoire utilisés, etc. Chaque champ est décrit dans le tableau suivant.

La case affiche la sortie de la commande Linux VMSTAT. Si vous connaissez cette commande, ces statistiques devraient vous être familières.

Tableau 1. Moniteur d'état

Champ	Description
procs	Nombre de processus : **r** : En attente d'exécution. **b** : En veille ininterrompu (bloqué, en attente d'un autre événement).
memory	Utilisation de la mémoire (ko) : **swpd** : Quantité de mémoire virtuelle utilisée. **free** : Quantité de mémoire inoccupée. **buff** : Quantité utilisée en tant que mémoires tampon. **cache** : Quantité réservée pour le cache.
swap	Quantité de mémoire (ko) : **si** : Permuté à partir du disque. **so** : Permuté vers le disque.
io	Blocs d'entrée/sortie (ko/s) : **bi** : Blocs reçus d'une unité par bloc **bo** : Blocs envoyés vers une unité par bloc
system	Système : **in** : Interruptions par seconde, y compris l'horloge **cs** : Interrupteurs contextuels par seconde
cpu	Pourcentage du temps d'UC total utilisé par : **us** : Temps passé à exécuter le code hors noyau **sy** : Temps passé à exécuter le code noyau **id** : Délai d'inactivité (à l'exclusion de l'attente des E-S) **wa** : Temps passé à attendre les E-S **st** : Temps volé d'une machine virtuelle
(n)pps / (m)rps	Dans la flèche en regard du moteur d'analyse, deux moyennes sont calculées pour les cinq dernières secondes : **n** est le nombre moyen de paquets réseau par seconde et **m** est le nombre moyen des demandes de base de données réseau par seconde.
Moteur d'analyse (q-d) ------ (p)	Pour le moteur d'analyse, la première ligne répertorie le nombre total de messages mis en file d'attente pour traitement (**q**), suivi du nombre de messages supprimés (**d**) pour éviter la saturation de la mémoire tampon. La deuxième ligne répertorie le nombre total de messages traités (**p**). Le numéro traité est réinitialisé à zéro lorsque le moteur d'inspection est redémarré.
Type de serveur (q) ---- (p)	Pour chaque type de serveur, le nombre de messages en attente de traitement (**q**) est répertorié et le nombre de messages traités (**p**) est répertorié.
Espace disque disponible	Nombre d'octets disponibles.
n% d'utilisation de la base de données	Pourcentage de l'allocation d'espace de base de données utilisée.

Champ	Description
Fichiers/Autre	La partie Fichiers/Autre du Moniteur d'état représente les données accumulées dans nondb-sql logger. Le consignateur Nondb-sql enregistre des événements de fermeture de session arrivant à l'Analyseur à partir de sessions "ignorées" qui ont été fermées en interne par l'Analyseur (INACTIVE_FLAG=-1). L'Analyseur a la possibilité de fermer les connexions par expiration du délai (si la session est inactive depuis longtemps). Si les données de fermeture de session arrivent à l'Analyseur à partir de la session "ignorée" qui a été fermée par expiration du délai, elle sont enregistrées dans la section nondb-sql logger. L'Analyseur n'enregistre jamais de données directement dans la base de données. Cette section représente également le nombre de requêtes de base de données (comme des insertions dans GDM_SECURE_PARAMS) envoyées par l'Analyseur au Consignateur, ainsi que d'autres protocoles pris en charge tels que FTP.

Historique des versions de la source de données

Emplacement de la présentation par défaut

- admin : disponible en tant qu'exploration en aval à partir du rapport Sources de données
- user : Reconnaître > Reconnaissance de base de données

Sources de données

Répertorie toutes les sources de données définies : Type de source de données, Nom de source de données, Description de source de données, Hôte, Port, Nom de service, Nom d'utilisateur, Nom de base de données, Dernière connexion, Partagé et Propriétés de connexion.

Vous pouvez restreindre la sortie de ce rapport à l'aide du paramètre d'exécution Nom de source de données, qui par défaut est défini sur "%" pour sélectionner toutes les sources de données.

Tableau 2. Sources de données

Domaine	Requête de base	Entité principale
interne - non disponible	Sources de données	non disponible
Paramètre d'exécution	Opérateur	Valeur par défaut
Nom de source de données	LIKE	%
Début de la période	>=	MAINTENANT A 1 JOUR
Fin de la période	<=	MAINTENANT

Processus d'audit prédéfinis

Il existe un processus d'audit prédéfini nommé Surveillance du dispositif, qui contient les rapports d'instance répertoriés. Ce processus d'audit est inactif par défaut. L'administrateur peut l'activer et le programmer selon ses besoins.

Remarque : Lors de la planification de ce processus d'audit, vérifiez que les dates DE / A pour chaque rapport sont logiques pour l'intervalle de processus défini (par exemple, il n'est pas logique d'avoir une période de rapport d'un jour si le processus d'audit ne s'exécute qu'une seule fois par semaine - vous manquez ainsi six jours d'activité).
Le processus d'audit Surveillance du dispositif contient les rapports suivants :

- Echecs de connexion à Guardium
- Utilisateurs actifs de Guardium
- Erreurs d'agrégation ou d'archivage
- Changements liés à la politique
- Moteurs d'inspection et changements d'agent S-TAP
- Changements de source de données
- Changements de configuration d'instance CAS
- Instances CAS
- Modèles CAS
- Excep des travaux planifiés

Rubrique parent : Exploitation des rapports prédéfinis

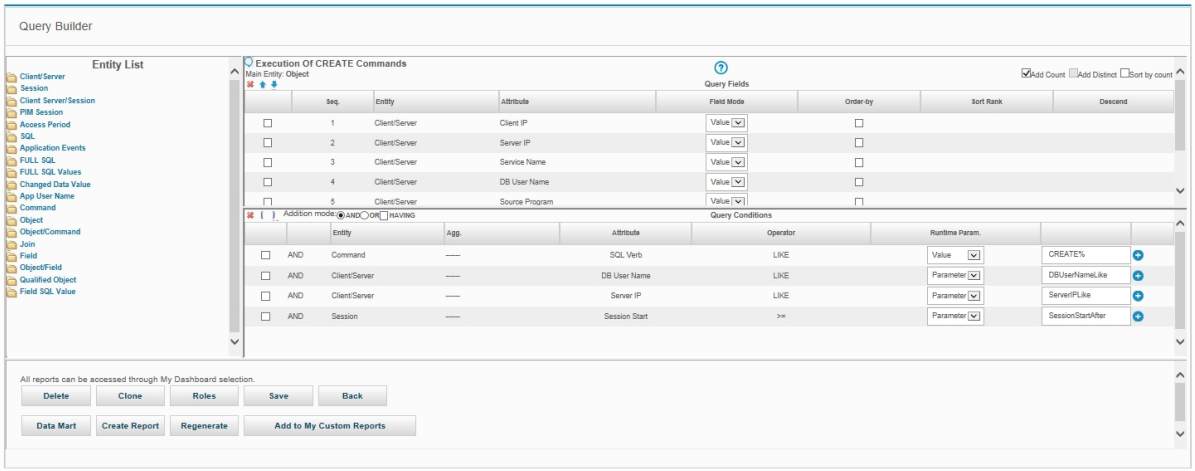
Interrogation des données

Utilisez le Générateur de requête pour définir et modifier des questions sur les données collectées.

Il existe une distinction entre les requêtes et les rapports :

- Une requête décrit un ensemble d'informations pouvant être obtenues à partir des données collectées. Par exemple, rechercher tous les clients qui mettent à jour une base de données spécifique pendant les heures de fin de semaine ou quels utilisateurs non autorisés ont tenté d'accéder à des données sensibles (numéros de sécurité sociale ou numéro de carte de crédit).
- Un rapport décrit comment sont présentées les données renvoyées par une requête.

Il existe un Générateur de requête distinct pour chaque domaine, qui s'ouvre à partir du Localiseur de requête pour ce domaine (voir la section Ouvrir le Localiseur de requête). Cliquez sur Rapports > Outils de configuration de rapport > Générateur de requête.



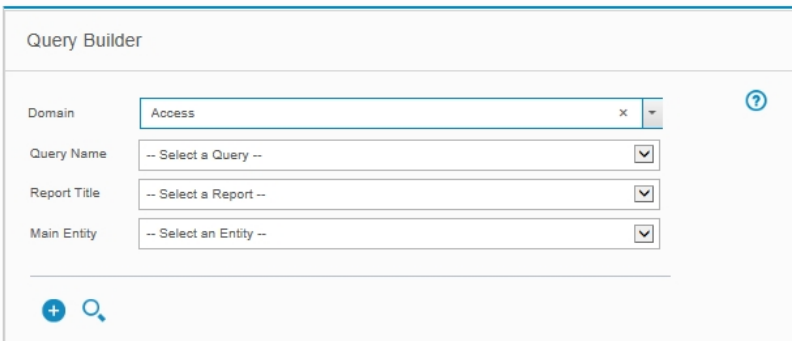
Le générateur de requêtes contient trois sous-fenêtres :

- La sous-fenêtre Liste d'entités identifie toutes les entités et les attributs contenus dans le domaine. Les entités sont représentées sous forme de dossiers et les attributs sont les éléments de ces dossiers. Cliquez sur un dossier d'entité pour afficher ses attributs, ou cliquez de nouveau pour les masquer. Pour une description de l'ensemble des entités et des attributs, voir Entités et Attributs dans la rubrique d'aide Domaines, entités et attributs.
- La sous-fenêtre Champs de requête répertorie tous les champs accessibles, les informations à afficher pour ce champ (valeur, nombre, minimum, maximum ou moyenne) et l'ordre de tri. Pour plus d'informations sur l'utilisation de cette sous-fenêtre, voir Présentation des champs de requête.
- La sous-fenêtre Conditions de requête spécifie les conditions de sélection des champs répertoriés (par exemple, "where VERB = UPDATE"). Pour plus d'informations sur l'utilisation de cette sous-fenêtre, voir Présentation des conditions de requête dans la rubrique d'aide Requêtes.

Pour obtenir des informations complètes, consultez la rubrique d'aide Requêtes.

Ouvrez le Localiseur de requête

Il existe un Générateur de requête distinct pour chaque domaine de génération de rapports, il est donc important d'ouvrir le Générateur de requête correct. Sinon, les informations que vous souhaitez visualiser ne s'affichent pas. Tous les domaines sont décrits dans la rubrique Domaines de l'Annexe Domaines, entités et attributs.



Après avoir déterminé le domaine à utiliser, cliquez sur Rapports > Outils de configuration de rapport > Générateur de requête.

Recherche d'une requête

Pour localiser et afficher une définition de requête dans le Générateur de requête, il existe plusieurs options :

1. Utilisez le Localiseur de requête - voir Utiliser le Localiseur de requête.
2. A partir d'un rapport basé sur la requête, cliquez sur Editer la requête de ce rapport dans la barre d'outils du rapport.

Utilisez le Localiseur de requête

1. Ouvrez le Localiseur de requête pour le domaine approprié (voir Ouvrir le Localiseur de requête).
2. Facultatif. Si vous connaissez l'Entité principale pour la requête, sélectionnez-la dans la liste.
3. Cliquez sur Rechercher.

   S'il n'existe qu'une seule requête définie pour l'entité principale sélectionnée, cette requête s'ouvre immédiatement dans le panneau de définition de requête.

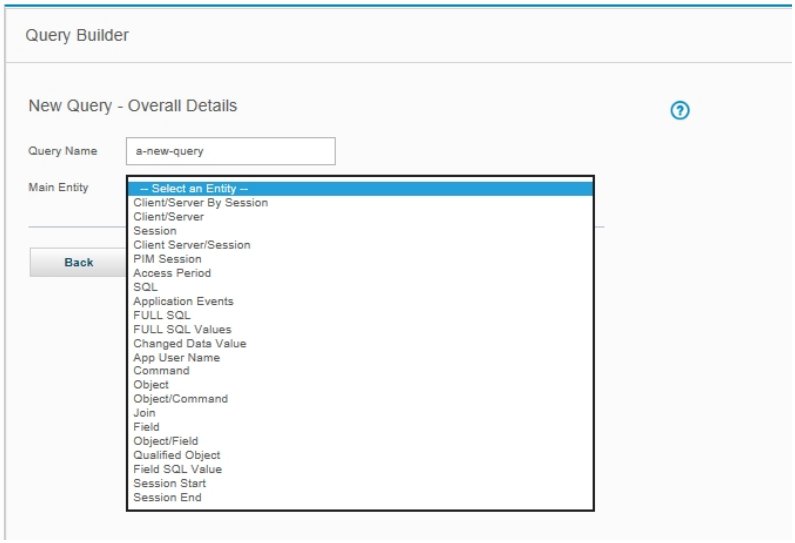
   S'il existe plusieurs requêtes définies pour l'Entité principale sélectionnée, ou si aucune entité principale n'a été sélectionnée, une liste de requêtes s'affiche dans le panneau Liste de requêtes.

   Si une entité principale a été sélectionnée pour laquelle aucune requête n'a été définie, vous êtes informé.
4. Effectuez l'une des opérations suivantes :

   Pour ouvrir le panneau Générateur de requête pour l'une des requêtes répertoriés, cliquez sur la requête. Pour définir une nouvelle requête, cliquez sur Nouveau.

Créer une requête

1. Ouvrez le Localiseur de requête pour le domaine approprié (voir Ouvrir le Localiseur de requête).
2. Cliquez sur Nouveau pour ouvrir le panneau Nouvelle requête - Détails globaux.
3. Entrez un nom de requête unique dans la zone Nom de requête. N'incluez pas les caractères apostrophe dans le nom de la requête.
4. Sélectionnez l'entité principale pour la requête dans la liste des entités principales. L'entité principale contrôle le niveau de détail disponible pour la requête et qu'elle ne peut pas être modifiée. Fondamentalement, chaque ligne de données renvoyée par la requête représente une instance unique de l'entité principale et un nombre d'occurrences pour cette instance.
5. Cliquez sur Suivant. La nouvelle requête s'ouvre dans le panneau Générateur de requête. Pour compléter la définition, voir la section suivante sur les Champs de requête.



Présentation des champs de requête

Présentation des champs de requête

La sous-fenêtre Champs de requête répertorie les colonnes de données devant être renvoyées par la requête.

Il existe deux façons d'ajouter un champ à la sous-fenêtre Champs de requête :

- Méthode du menu contextuel :

1. Cliquez sur le champ à ajouter.
2. Sélectionnez Ajouter un champ dans le menu contextuel.

- Méthode glisser-déposer :

1. Cliquez sur l'icône du champ (pas sur le nom du champ).
2. Faites glisser l'icône dans la liste Champs de requête et relâchez-la.

Indépendamment de la méthode utilisée, le champ est ajouté à la fin de la liste.

Déplacez ou supprimez des champs dans la sous-fenêtre Champs de requête

Pour déplacer un champ dans la sous-fenêtre Champs de requête :

1. Cochez la case pour le champ.
2. Utilisez les boutons suivants pour déplacer le champ vers l'emplacement désiré :

   Cliquez sur Haut pour remonter le champ d'une ligne.

   Cliquez sur Bas pour descendre le champ d'une ligne.

Modification d'une requête

1. Ouvrez le Localiseur de requête pour le domaine approprié (voir Ouvrir le Localiseur de requête).
2. Utilisez le Localiseur de requête pour ouvrir la requête à modifier.
3. Reportez-vous à la rubrique Présentation du Générateur de requête pour modifier tout composant de la définition de la requête.

Créer un rapport

Une fois qu'une requête a été définie, il existe plusieurs options pour ajouter rapidement un rapport tabulaire basé sur cette requête à une présentation de menu existante. Ces options s'appliquent uniquement aux rapports tabulaires.

1. Ouvrez le Localiseur de requête pour le domaine approprié (voir Ouvrir le Localiseur de requête).
2. Utilisez le Localiseur de requête pour ouvrir la requête à utiliser pour le rapport.
3. Effectuez l'une des opérations suivantes :

   Pour créer un rapport, cliquez sur Créer un rapport. Pour répéter un rapport tabulaire existant, cliquez sur Régénérer.

   Pour ajouter un rapport tabulaire à l'onglet Mes rapports personnalisés, cliquez sur Ajouter à Mes rapports personnalisés dans le panneau. (Si aucun rapport tabulaire n'a encore été généré pour la requête, vous devez d'abord cliquer sur Créer un rapport.)

   Pour visualiser des données significatives dans le rapport tabulaire, cliquez sur pour accéder aux paramètres d'exécution (modifiez l'heure de début et courante).

Rubrique parent : Rapports

Génération de rapports sur les tables et les colonnes dormantes

Guardium propose des fonctionnalités qui peuvent aider les architectes de données et les administrateurs de base de données (DBA) à détecter quelles tables et quels champs ne sont pas utilisés.

Pourquoi et quand exécuter cette tâche

Le concept de base est le suivant. Vous souhaitez savoir quelles tables ne sont pas en cours de consultation. Téléchargez tous les noms de table de votre base de données ou de la Base de données de gestion de la configuration (CMDB) à l'aide des fonctions personnalisées de requêtes et de domaines de Guardium. Utilisez ensuite le rapport (à partir de la requête personnalisée) pour remplir un groupe d'objets.

Puis, utilisez un rapport qui exploite des données surveillées pour afficher tous les noms d'objet qui ont participé à une instruction SELECT. Il existe des rapports prédéfinis pour cela dans Guardium 8, commençant tous par le préfixe DW (Data Warehouse). Ensuite, utilisez la sortie pour remplir l'un des groupes prédéfinis.

Enfin, utilisez un rapport prédéfini qui affiche tous les membres du premier groupe qui ne sont pas membres du deuxième groupe.

Il existe deux ensembles de ces rapports et groupes : l'un est axé sur les tables et l'autre sur les tables et les colonnes. La seule différence est que, dans le second cas, les groupes sont de type 2-tuple (membres composites d'une paire d'attributs de valeur, appelés tuple).

Examinons un exemple de bout en bout impliquant une base de données Oracle et l'utilisateur EMP.

Procédez comme suit.

1. Téléchargez tous les noms de table et/ou toutes les combinaisons de table/colonne à partir de l'ensemble des tables du catalogue système (définitions des objets de la base de données).
2. Utilisez les données surveillées pour déterminer quelles tables et/ou tables/colonnes ont été consultées pendant une période donnée.
3. Créez un rapport sur tous les éléments de l'étape 1 qui ne figurent pas à l'étape 2.

Les fonctions Guardium suivantes sont utilisées pour cette tâche.

- Corrélez les données externes pour le téléchargement des noms de tables et de colonnes
- Remplissez des groupes à partir des requêtes
- Générez des rapports

Procédure

1. Téléchargez toutes les tables à partir du catalogue système. Pour ce faire, créez une table personnalisée.

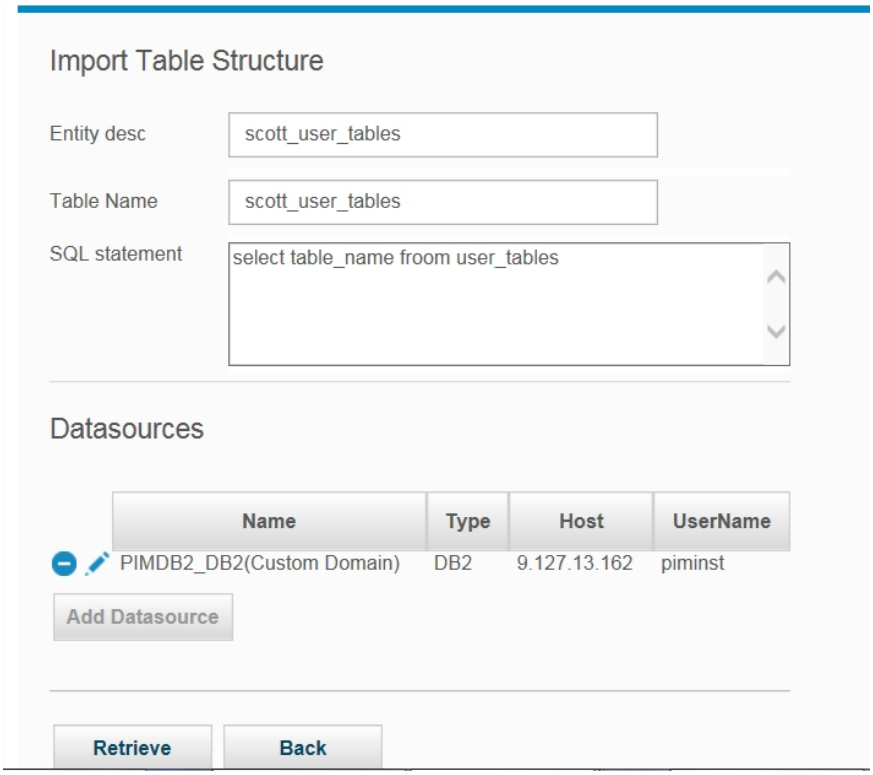
   Prérequis

   a. Définissez la connexion à la base de données de la source de données/test
   b. Téléchargez des données (créez une table personnalisée)
   c. Créez un domaine (fusionnez des tables personnalisées avec des rapports existants)

   Voir Corrélation avec des données externes pour plus d'informations.

   L'exemple suivant est disponible à partir de Conformité > Génération de rapport personnalisée > Générateur de table personnalisée > Télécharger la définition > Structure d'importation de table.

   Lorsque la configuration est terminée, cliquez sur le bouton Extraire.



Configuration - Télécharger la définition, Structure d'importation de table

Téléchargez les données afin qu'elles se trouvent dans le système Guardium (en tant que table personnalisée) et, si vous le souhaitez, planifiez ce téléchargement. Ces données permettent de déterminer le sur-ensemble de toutes les tables définies dans le système.

Mappage de tous les objets (et/ou objets-champs) dans le système

Dans cet exemple, les données dormantes basées sur les noms de table sont utilisées. Toutefois, l'analyse peut inclure des colonnes, à condition que les tâches de téléchargement soient définies pour renvoyer des paires `<objet,champ>` et utilisent des groupes de tuples à comparer à un tuple observé `objet+champ`.

Pour les instances Objet-Champ, remplacez le rapport DW Objets dormants par le rapport DW Champs d'objets dormants. Pour les instances Objet-Champ, remplacez le rapport DW Accès SELECT à l'objet par le rapport DW Accès Objet-Champ.

Une fois que vous avez terminé le téléchargement, définissez un domaine personnalisé basé uniquement sur cette table personnalisée et définissez un rapport qui extrait les noms de table.

Ensuite, remplissez le groupe DW Tous les objets à partir de ce rapport et planifiez l'action d'importation à partir de la requête si vous le souhaitez. Vous créez ainsi un groupe qui possède toutes les tables telles qu'elles sont définies par le catalogue système.

Remarque : Lorsque vous remplissez le groupe DW Tous les objets, vous devez inclure les informations pour cliquer sur Exécuter une fois maintenant -> Sélectionner tout -> Cliquez sur le bouton Importer. Faites de même pour le groupe "DW Objets consultés par SELECT". Vous devez importer toutes les définitions planifiées.

Lorsque vous avez terminé, cliquez sur le bouton Sauvegarder.

2. Mappage direct de l'objet

   Utilisez les données surveillées pour déterminer quelles tables et/ou tables/colonnes ont été consultées pendant une période donnée.

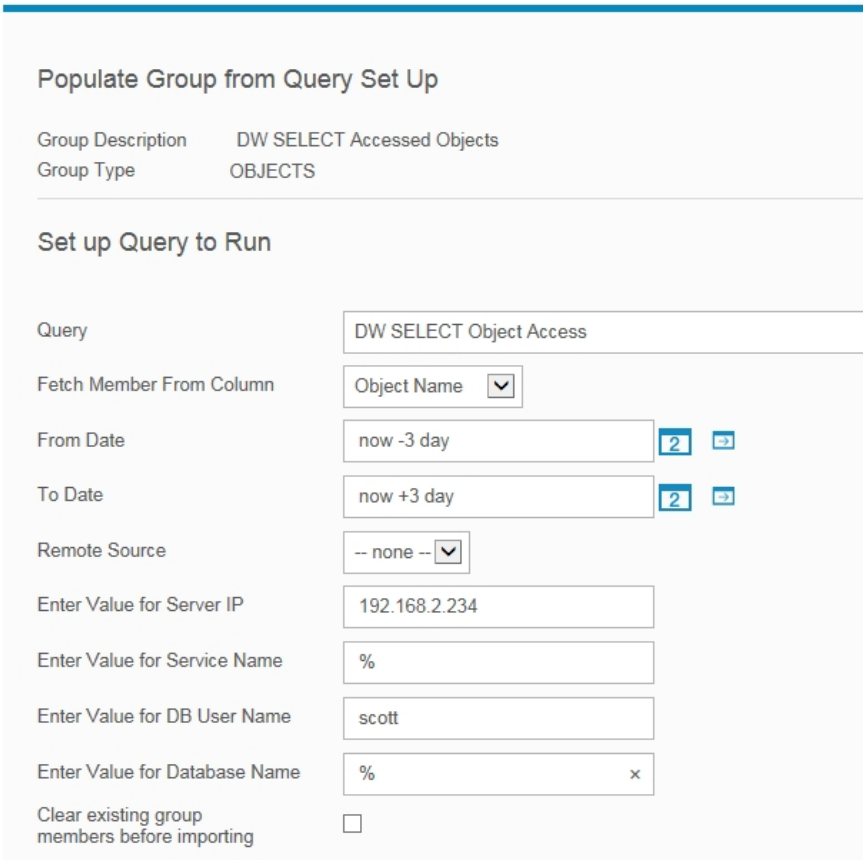
   Examinez d'autres rapports prédéfinis. Le rapport DW Accès SELECT à l'objet affiche tous les noms d'objet accessibles via une instruction SELECT.

   A présent, remplissez le groupe DW Objets consultés par SELECT à partir du rapport, en complétant les attributs de filtrage dont vous avez besoin.

   Remarque : Lorsque vous remplissez le groupe DW Tous les objets, vous devez inclure les informations pour cliquer sur "Exécuter une fois maintenant" -> Sélectionner tout -> Cliquez sur le bouton Importer. Faites de même pour le groupe "DW Objets consultés par SELECT". Vous devez importer toutes les définitions planifiées.

   L'exemple suivant est disponible à partir de Configurer > Outils et vues > Générateur de groupe > Sélectionnez DW Tous les objets > Remplir à partir d'une requête > DW Accès SELECT à l'objet.

   Lorsque vous avez terminé, cliquez sur le bouton Sauvegarder.



Configuration - Remplir un groupe à partir d'une requête, Nom d'objet

3. Créez un rapport sur tous les éléments de l'étape 1 qui ne figurent pas à l'étape 2.

   Utilisez le rapport DW Objets dormants pour afficher des objets qui se trouvent dans le groupe de tous les objets, mais qui n'ont pas été utilisés dans une instruction SELECT.

   Comparez ce rapport avec le rapport précédent Noms de table. Notez que EMP ne figure pas dans ce rapport car il a été utilisé dans une instruction SELECT.

   Remarque : Dans la mesure où les membres du groupe sont gérés et synchronisés de manière centralisée entre Central Manager et les unités gérées, le contenu de ce rapport peut être différé jusqu'à 30 minutes. Si vous devez accéder aux informations les plus récentes, exécutez ce rapport sur Central Manager ou demandez à votre administrateur Guardium de synchroniser l'unité gérée sur Central Manager.

   Autres façons d'accéder aux tables

   Mappage indirect des objets

   Outre l'accès SELECT direct, les tables peuvent être consultées à l'aide de procédures et de fonctions mémorisées. Dans ce cas, vous devez mapper des éléments supplémentaires pour permettre à Guardium de générer les instructions SELECT.

   Tout d'abord, utilisez le rapport DW Accès EXECUTE à l'objet pour remplir le groupe appelé DW Objets EXECUTE avec un ensemble de noms de procédures mémorisées exécutées. Utilisez ensuite le mappage indirect pour générer tous les objets utilisés dans ces procédures.

   Supposons que vous disposez d'une procédure définie :

```
create or replace procedure num_depts(deptnums out NUMBER) is
begin
    select count(*) into deptnums from dept;
end;
```

   Dans ce cas, chaque exécution de num_depts exécute également une instruction SELECT sur DEPT.

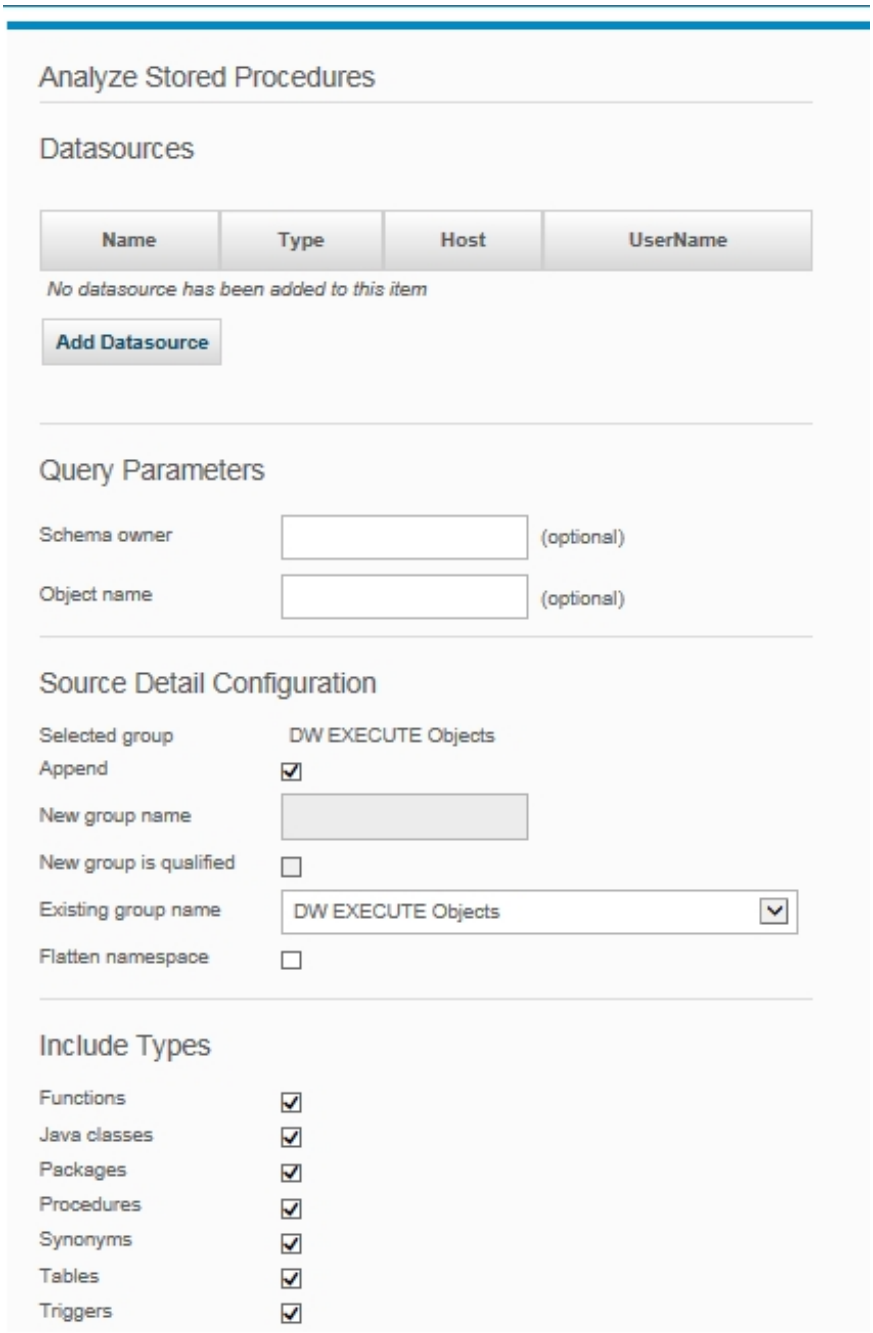
   A l'aide de la fonction "populate group from query", utilisez la colonne Nom d'objet dans le rapport DW Accès EXECUTE à l'objet pour remplir le groupe "Objets EXECUTE DW". Puis, utilisez ce groupe pour remplir le groupe DW Objets consultés par EXECUTE.

   Dans le Générateur de groupe, sélectionnez le groupe "Objets EXECUTE DW" dans la liste et cliquez sur Proc. appelante générée automatiquement. Sélectionnez l'option Utilisation de dépendances en amont, prise en charge uniquement pour Oracle dans Guardium 8, ou Générer des objets sélectionnés.

   Si vous choisissez d'utiliser des dépendances, vous devez sélectionner une base de données ayant accès à DBA_DEPENDENCIES et le type de dépendances à suivre.

   Sélectionnez d'ajouter des membres au groupe DW Objets consultés par EXECUTE.

   L'exemple suivant est disponible à partir de Configuration > Outils et vues > Générateur de groupe > Sélectionnez DW Objets consultés par EXECUTE > Proc. appelante générée automatiquement > Utilisation de dépendances en amont > Analyser les procédures mémorisées.



Configuration - Proc. appelante générée automatiquement, Utilisation de dépendances en amont

Cette opération ajoute les objets dépendants au groupe DW Objets consultés par EXECUTE.

Rubrique parent : Rapports

Génération d'appels d'API à partir de rapports

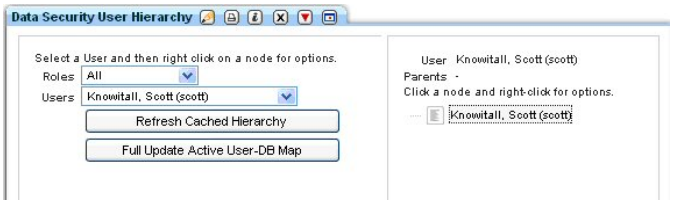
Générez des appels de l'API Guard à partir d'un rapport, soit à partir d'une seule ligne dans un rapport, soit basés sur l'ensemble du rapport

Valeur ajoutée : grâce à une interface graphique, à l'aide des données existantes sur le système, qui figurent dans les rapports en tant que paramètres d'appels d'API, vous pouvez rapidement et facilement générer et remplir des appels d'API sans avoir à exécuter de commandes au niveau du système. Vous pouvez également saisir de longs appels d'API pour effectuer rapidement des opérations telles que la création de sources de données, la définition de moteurs d'inspection, la gestion de hiérarchies utilisateur ou celle des fonctionnalités de Guardium, telles que S-TAP.

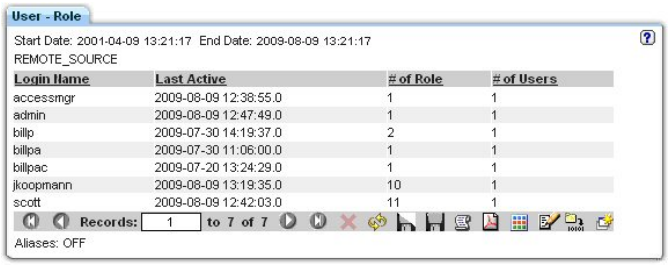
Appel d'API à une ligne

Pour ce scénario, vous générez des appels de fonction d'API pour remplir la Hiérarchie utilisateur pour la sécurité des données.

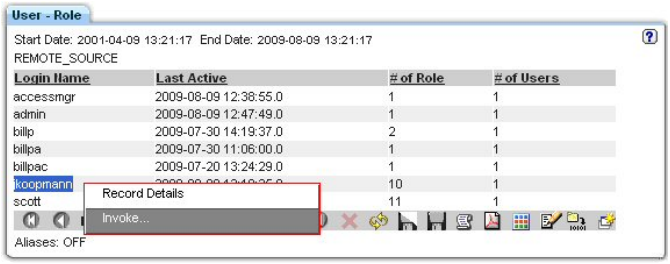
1. Pour commencer, affichez la **Hiérarchie utilisateur pour la sécurité des données** en cours de l'utilisateur **scott**



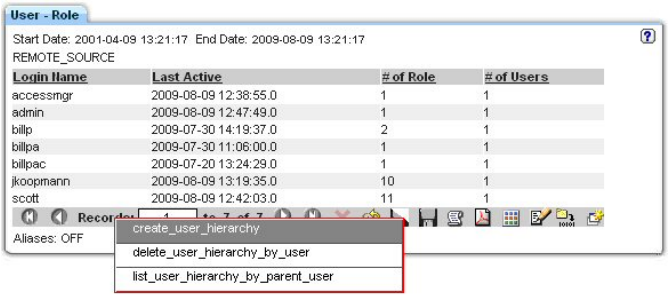
2. Pour appeler une fonction d'API, vous devez rechercher un rapport auquel sont associées les fonctions d'API souhaitées. Dans la mesure où la création d'une hiérarchie utilisateur est liée aux utilisateurs, la sélection d'un rapport d'utilisateur devrait donner de bons résultats. Pour ce scénario, sélectionnez le rapport **Utilisateur - Rôle**.



3. **Cliquez deux fois sur une ligne** correspondant à l'exploration en aval pour afficher l'option **Appeler...**

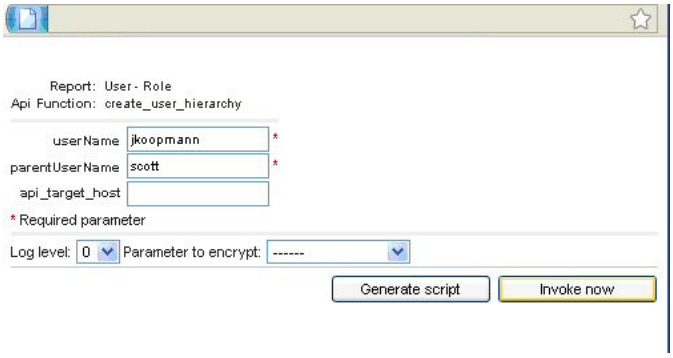


4. Cliquez sur l'option **Appeler...** pour afficher une liste de fonctions API mappées à ce rapport



5. Cliquez sur l'**API** que vous souhaitez appeler pour afficher le Formulaire d'appel d'API pour le rapport et la fonction d'appel d'API

6. Remplissez les paramètres obligatoires et les paramètres non obligatoires pour l'appel de l'API sélectionnée. De nombreux paramètres sont préremplis à partir du rapport, mais vous pouvez les modifier pour créer un appel d'API spécifique. Pour obtenir de l'aide spécifique pour compléter les paramètres obligatoires ou non requis, veuillez consulter les appels spécifiques de fonction d'API dans le guide de référence de GuardAPI.



7. Utilisez la liste déroulante pour sélectionner le **Niveau de consignation,** où le niveau de consignation représente les éléments suivants : (0 - renvoie ID=*identificateur* et ERR=*code_erreur* tel que défini dans Codes de retour, 1 - affiche des informations supplémentaires à l'écran, 2 - place les informations dans les journaux de débogage de l'application Guardium, 3 - réalise ces deux opérations)

8. Utilisez la liste déroulante pour sélectionner un **Paramètre à chiffrer**.

Remarque : Vous pouvez activer le chiffrement des paramètres en configurant le Secret partagé. Il est pertinent uniquement pour appeler la fonction d'API via la génération de script.

9. Sélectionnez **Appeler maintenant** ou **Générer un script.**

   a. Si vous sélectionnez l'option **Appeler maintenant**, l'appel d'API s'exécute immédiatement et affiche un écran de sortie d'appel d'API indiquant l'état de l'appel d'API.

   b. Si vous sélectionnez l'option **Générer un script** : ouvrez le script généré dans un éditeur ou, éventuellement, enregistrez-le sur le disque pour l'éditer et l'exécuter ultérieurement - en remplaçant toutes les valeurs des paramètres vides (marquées par "< >") si elles se trouvent dans le script.
   Remarque : Les paramètres vides restent dans le script car l'appel d'API les ignore

   Exemple de script

   # Modèle de script pour l'appel de la fonction guardAPI create_user_hierarchy :

   # Syntaxe : ssh cli@a1.corp.com<create_user_hierarchy_api_call.txt

   # remplacer toute valeur < > par la valeur obligatoire

   #

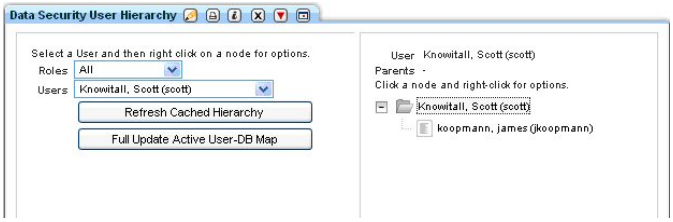
   grdapi create_user_hierarchy userName=jkoopmann parentUserName=scott

   c. Exécutez l'appel de la fonction CLI.

   Exemple d'appel

   $ ssh cli@a1.corp.com<create_user_hierarchy_api_call.txt

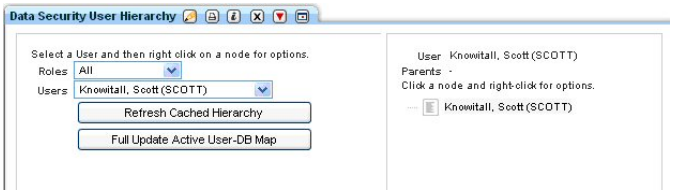
10. Validez. Pour ce scénario, il s'agit d'un réaffichage de la Hiérarchie utilisateur pour la sécurité des données.



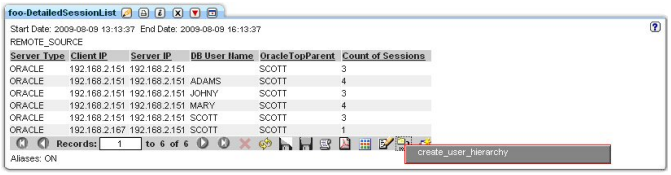
Appel d'API à plusieurs lignes

Ce scénario utilise un rapport personnalisé avec des paramètres mappés sur les champs de rapport. Pour plus d'informations, consultez les autres scénarios de cette section.

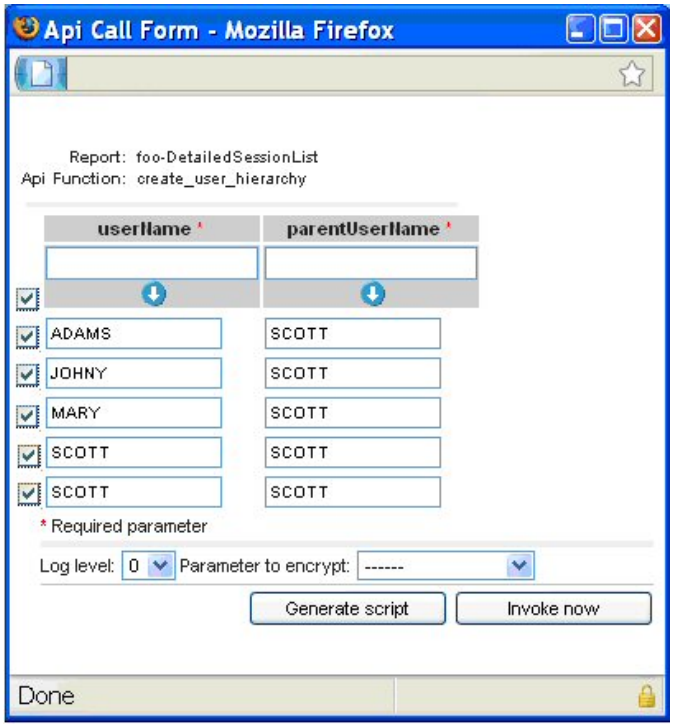
1. Pour commencer, affichez la **Hiérarchie utilisateur pour la sécurité des données** en cours de l'utilisateur **scott**



2. Cliquez sur l'icône **Appeler...** pour afficher une liste des API mappées à ce rapport



3. Cliquez sur l'**API** que vous souhaitez appeler pour afficher le Formulaire d'appel d'API pour le rapport et la fonction d'appel d'API. Demander un appel d'API à partir d'un rapport pour plusieurs lignes produit un formulaire d'appel d'API qui affiche et permet d'éditer tous les enregistrements à l'écran (en fonction de la taille de l'extraction) jusqu'à 20 enregistrements.



4. Utilisez les **cases à cocher** pour sélectionner/désélectionner les lignes ciblées pour l'appel d'API.

5. Remplissez les **Paramètres obligatoires** et les **paramètres non obligatoires** pour l'appel d'API sélectionné. De nombreux paramètres sont préremplis à partir du rapport, mais vous pouvez les modifier pour créer un appel d'API spécifique. Pour obtenir de l'aide spécifique pour compléter les paramètres obligatoires ou non obligatoires, veuillez consulter les appels spécifiques de fonction d'API dans le guide de référence de GuardAPI. En outre, utilisez l'ensemble de paramètres pour l'API pour saisir une valeur pour un paramètre et, en cliquant sur le bouton flèche vers le bas, remplissez ce paramètre pour tous les enregistrements.

6. Utilisez la liste déroulante pour sélectionner le **Niveau de consignation,** où le niveau de consignation représente les éléments suivants : (0 - renvoie ID=*identificateur* et ERR=*code_erreur* tel que défini dans Codes de retour, 1 - affiche des informations supplémentaires à l'écran, 2 - place les informations dans les journaux de débogage de l'application Guardium, 3 - réalise ces deux opérations)

7. Utilisez la liste déroulante pour sélectionner un **Paramètre à chiffrer**.
Remarque : Vous pouvez activer le chiffrement des paramètres en configurant le Secret partagé. Il est pertinent uniquement pour appeler la fonction d'API via la génération de script.

8. Sélectionnez **Appeler maintenant** ou **Générer un script.**

    a. Si vous sélectionnez l'option **Appeler maintenant**, l'appel d'API s'exécute immédiatement et affiche un écran de sortie d'appel d'API indiquant l'état de l'appel d'API. Dans ce scénario, les deux derniers appels d'API échouent car vous ne pouvez pas avoir une relation cyclique dans la hiérarchie.

    b. Si vous sélectionnez l'option **Générer un script** : ouvrez le script généré dans un éditeur ou, éventuellement, enregistrez-le sur le disque pour l'éditer et l'exécuter ultérieurement - en remplaçant toutes les valeurs des paramètres vides (marquées par "< >") si elles se trouvent dans le script. Dans ce scénario, vous pouvez facilement supprimer les deux dernières lignes du script, sachant qu'elles créent des erreurs cycliques.
    Remarque : Les paramètres vides restent dans le script car l'appel d'API les ignore.

    Exemple de script

    # Modèle de script pour l'appel de la fonction guardAPI create_user_hierarchy :

    # Syntaxe : ssh cli@a1.corp.com<create_user_hierarchy_api_call.txt

    # remplacer toute valeur < > par la valeur obligatoire

    #

    grdapi create_user_hierarchy userName=ADAMS parentUserName=SCOTT

    grdapi create_user_hierarchy userName=JOHNY parentUserName=SCOTT

    grdapi create_user_hierarchy userName=MARY parentUserName=SCOTT

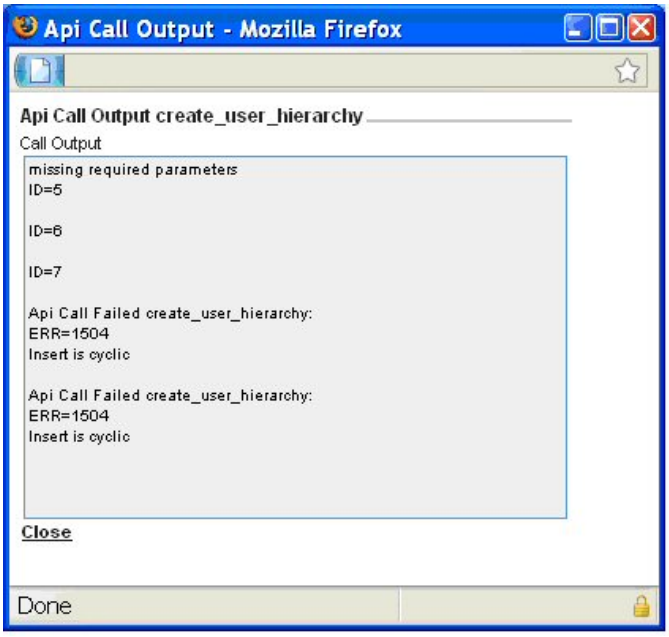
    grdapi create_user_hierarchy userName=SCOTT parentUserName=SCOTT

    grdapi create_user_hierarchy userName=SCOTT parentUserName=SCOTT

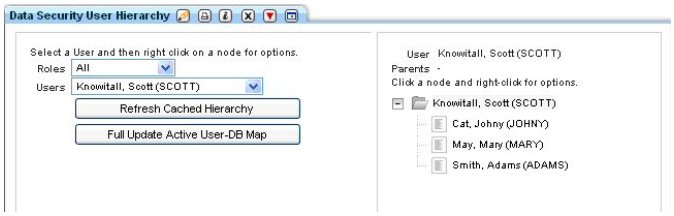
    c. Exécutez l'appel de la fonction CLI.

    Exemple d'appel

    $ ssh cli@a1.corp.com<create_user_hierarchy_api_call.txt



9. Validez. Pour ce scénario, il s'agit d'un réaffichage de la Hiérarchie utilisateur pour la sécurité des données.



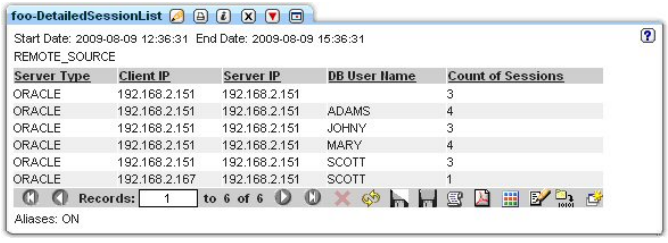
Rubrique parent : Rapports

Utilisation de constantes dans les appels d'API

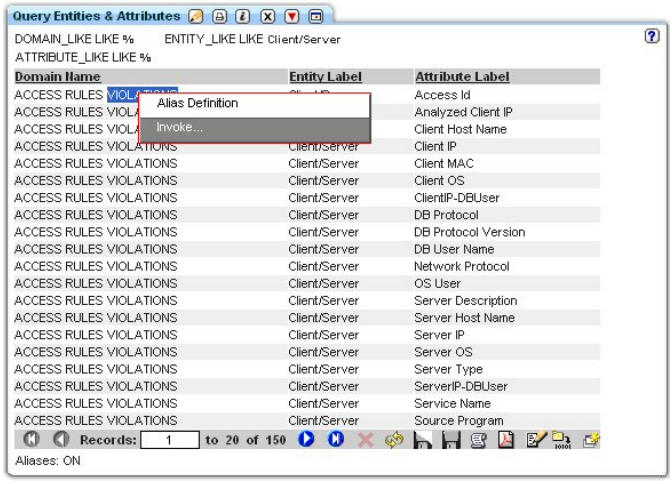
Créez un attribut d'entité à utiliser pendant un appel de fonction d'API.

Valeur ajoutée : via une interface graphique, créez une constante définie par l'utilisateur qui peut être utilisée pour remplir un paramètre dans un appel de fonction d'API.

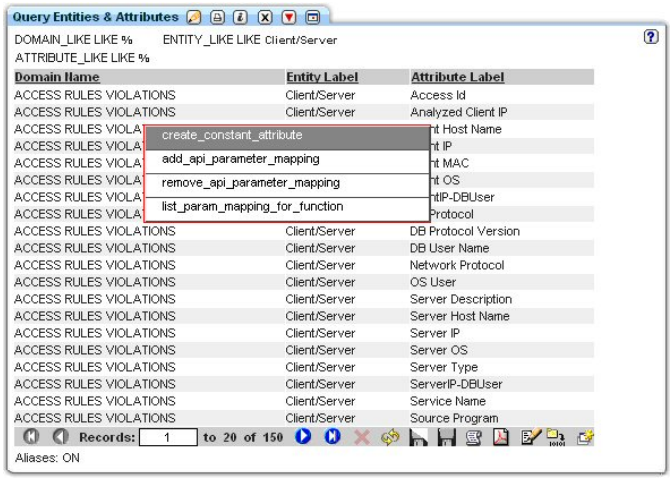
1. A partir de votre rapport, vous pouvez la modifier pour obtenir un champ que vous pouvez utiliser pour les mappages de paramètres.



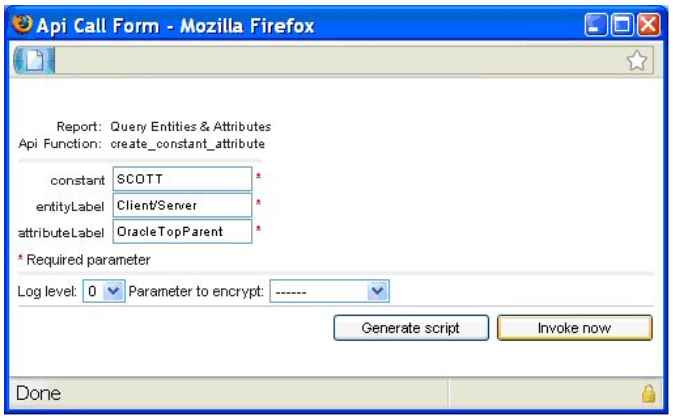
2. Accédez à l'entité Entités de requête & Rapport d'attributs pour le client-serveur dans le domaine ACCESS RULES VIOLATIONS. Cliquez deux fois sur une ligne et sélectionnez l'option Appeler...



3. Appelez la fonction d'API create_constant_attribute.

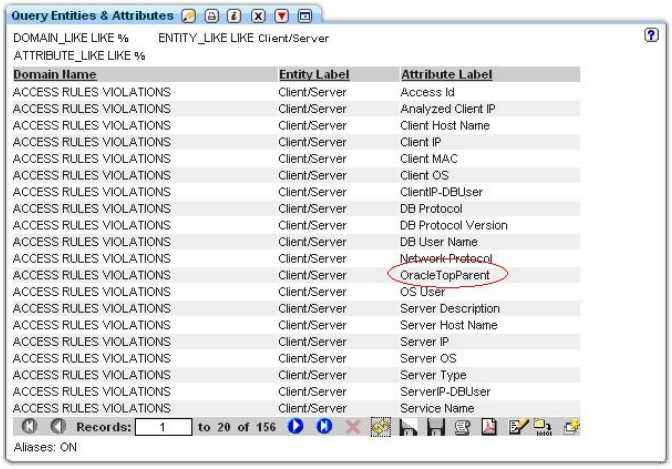


4. Remplissez la valeur constante à utiliser ('SCOTT'), remplissez le libellé attributLabel que vous souhaitez nommer ('OracleTopParent'), puis cliquez sur le bouton Appeler maintenant pour créer la constante.

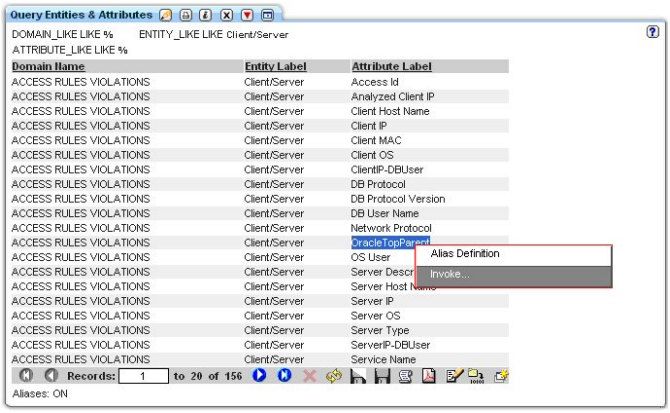


5. En cliquant sur le bouton Appeler maintenant, vous générez un état de Sortie d'appel d'API indiquant que la constante a été créée.

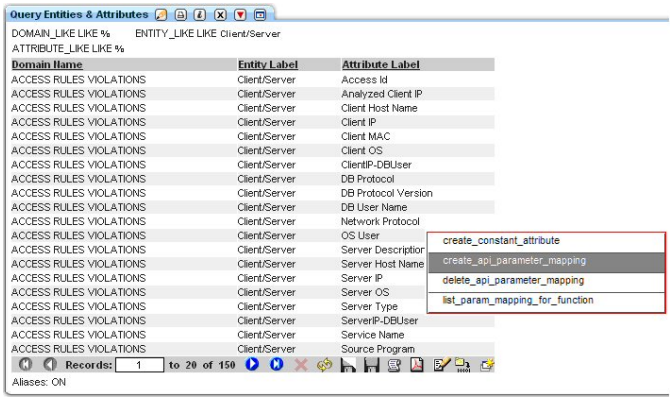
6. Un réaffichage du rapport Entités et attributs de requête montre l'attribut créé.



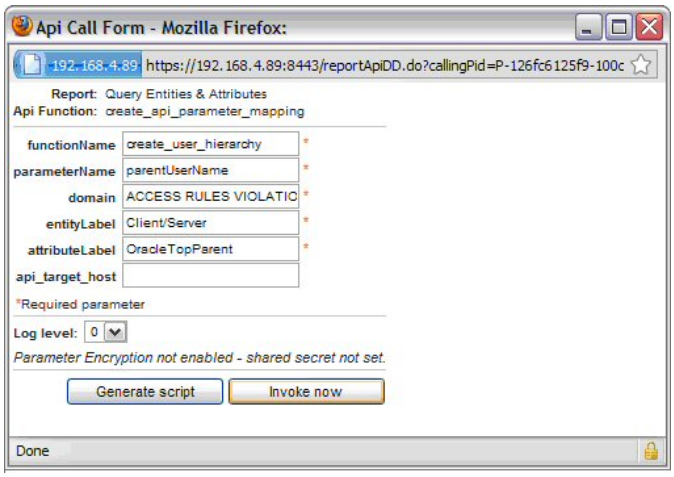
7. La nouvelle constante peut maintenant être mappée pour le rapport. Cliquez deux fois sur une ligne et sélectionnez l'option Appeler...



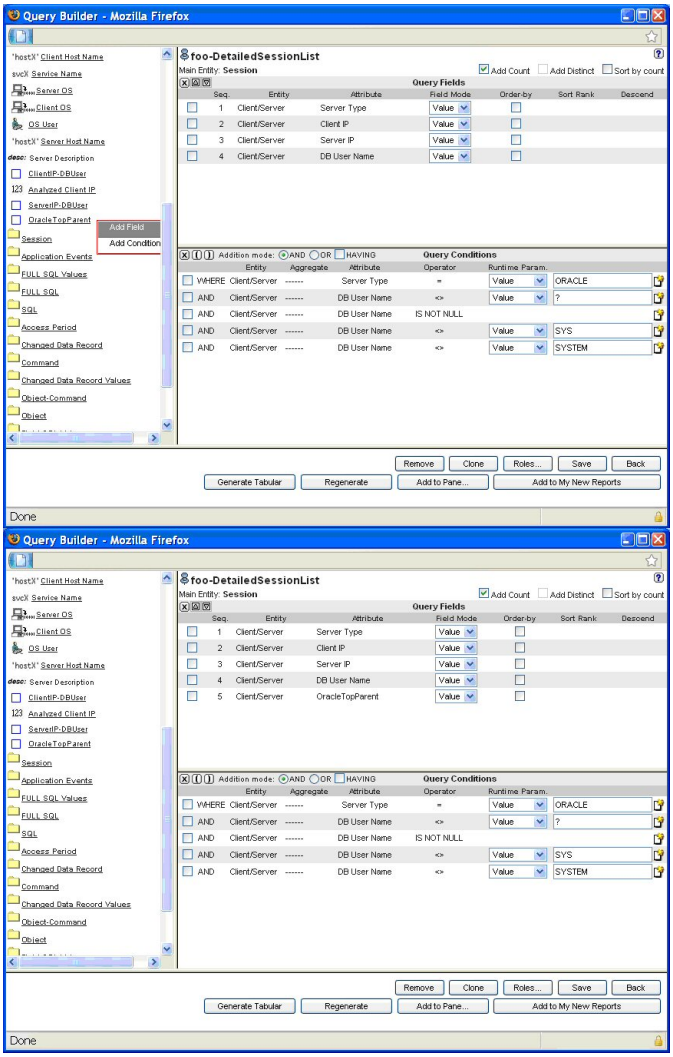
8. Sélectionnez l'option create_api_parameter_mapping.



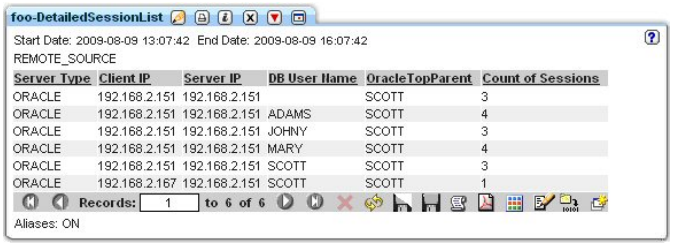
9. Renseignez les valeurs functionName et parameterName et cliquez sur le bouton Appeler maintenant.



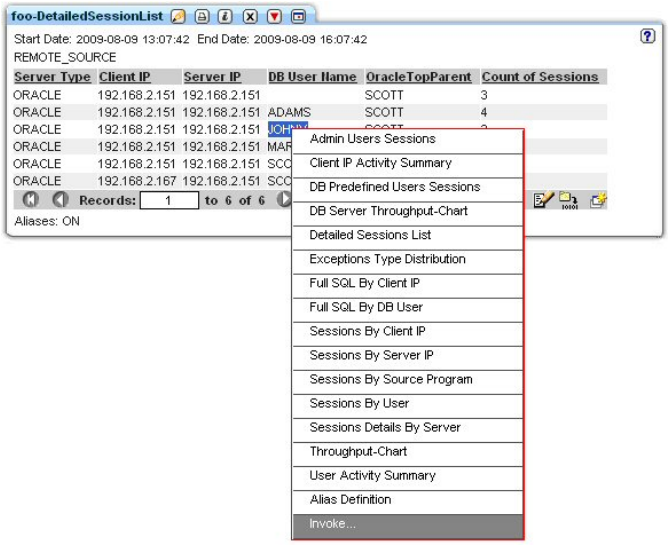
10. Le nouvel attribut doit être ajouté au rapport. Editez la requête via le Générateur de requête et ajoutez le champ.



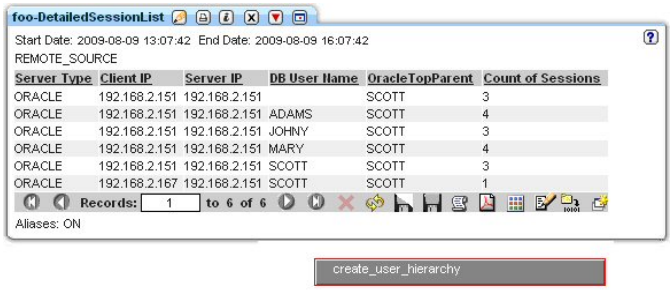
11. Lorsque le rapport est affiché, le nouvel attribut apparaît.



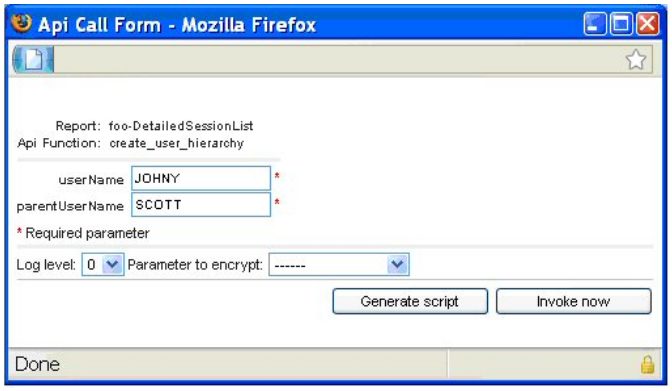
12. Pour valider l'utilisation de la nouvelle constante, cliquez deux fois sur une ligne et sélectionnez l'option Appeler...



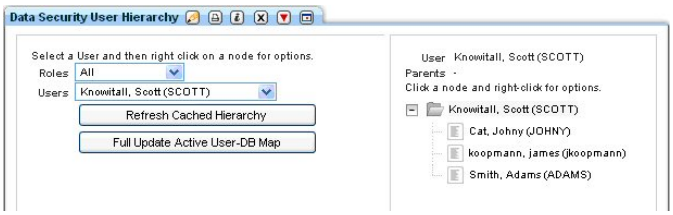
13. Sélectionnez la fonction d'API



14. parentNameName est alors renseigné à partir de la nouvelle constante ajoutée. Cliquez sur le bouton Appeler maintenant.



15. Validez la nouvelle hiérarchie utilisateur pour la sécurité des données.



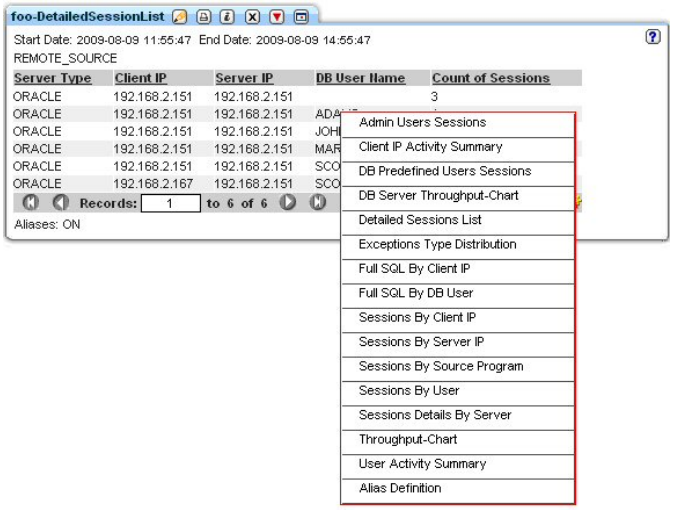
Rubrique parent : Rapports

Utilisation d'appels d'API à partir de rapports personnalisés

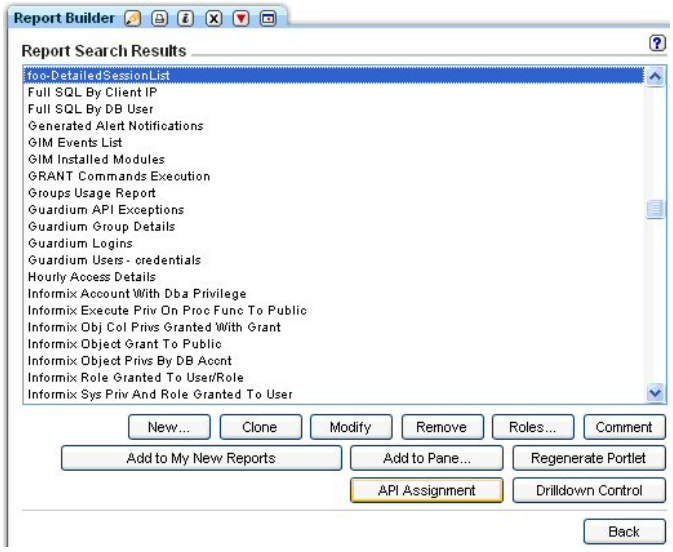
Associez des fonctions d'API à des rapports et mappez des champs de rapport aux paramètres fonctionnels de l'API.

Valeur ajoutée : via une interface graphique, mappez rapidement et facilement des paramètres d'API sur des champs de rapports personnalisés à utiliser dans des appels de fonction d'API.

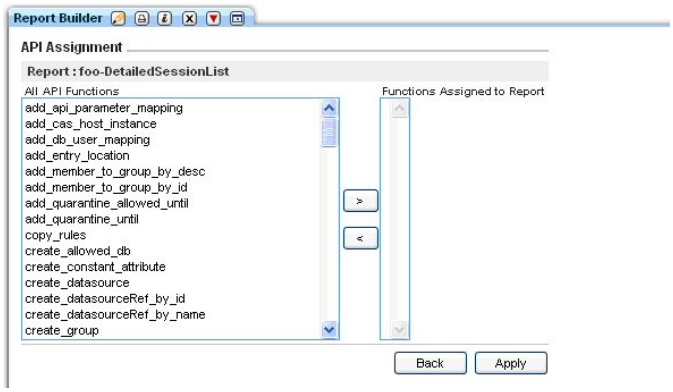
1. Par défaut, un nouveau rapport personnalisé ne possède aucune fonction d'API associée. Vous pouvez le constater dans le rapport personnalisé en cours où un double clic sur une ligne ne génère qu'une liste de rapports d'exploration supplémentaires à exécuter, mais ne contient pas l'option Appeler.



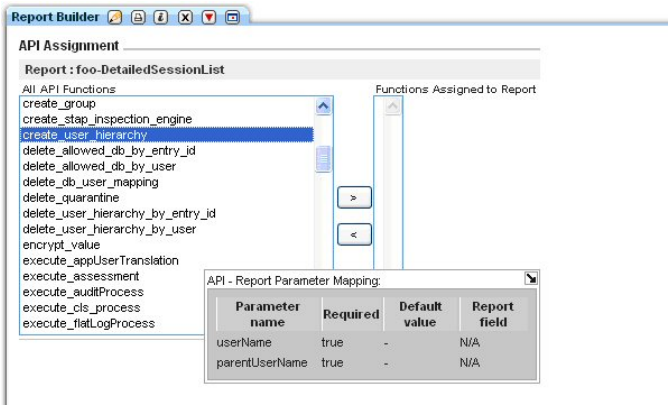
2. L'association des fonctions d'API aux rapports s'effectue via le Générateur de rapport de Guardium. Ouvrez le Générateur de rapport, localisez le rapport personnalisé, puis cliquez sur le bouton Affectation d'API.



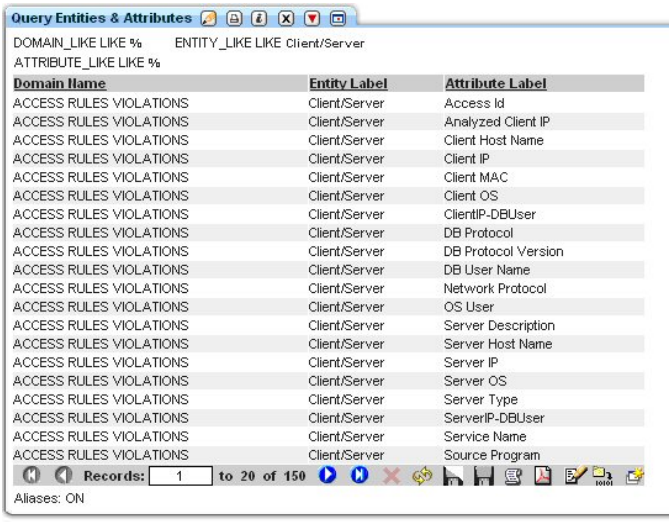
3. Le panneau Affectation d'API affiche toutes les fonctions d'API affectées au rapport sélectionné. Notez que pour notre scénario, le rapport sélectionné ne comporte pas de fonctions d'API.



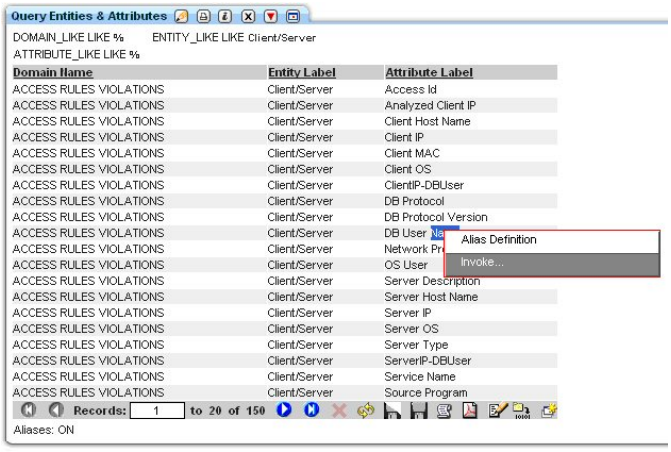
4. Pour attribuer une fonction d'API à un rapport, recherchez une API que vous souhaitez associer au rapport, cliquez sur la flèche Supérieur à, puis cliquez sur le bouton Appliquer. Pour notre scénario, nous avons sélectionné create_uer_hierarchy. Lors de la sélection, une fenêtre contextuelle apparaît qui affiche les mappages des paramètres du rapport (les champs du rapport utilisés lors de l'appel de la fonction d'API). Notez qu'aucun champ du rapport n'est mappé à un nom de paramètre.



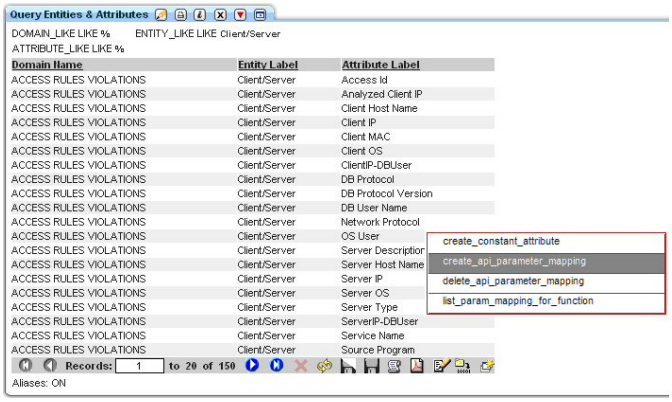
5. A ce stade, aucun des champs de rapport n'est mappé aux paramètres de l'API. Les utilisateurs peuvent accéder au rapport "Entités et attributs de requête" pour créer ces mappages, faute de quoi, lors de l'appel de l'API, aucun paramètre n'a de valeur. Ajoutez les mappages de paramètres d'API. Ouvrez le rapport "Entités et attributs de requête" et créez les mappages. Dans la mesure où le rapport de ce scénario utilise l'entité Client-Serveur dans le domaine ACCESS RULES VIOLATIONS, filtrez le rapport à l'aide du bouton de personnalisation, en modifiant le rapport pour afficher uniquement l'entité Client-Serveur.



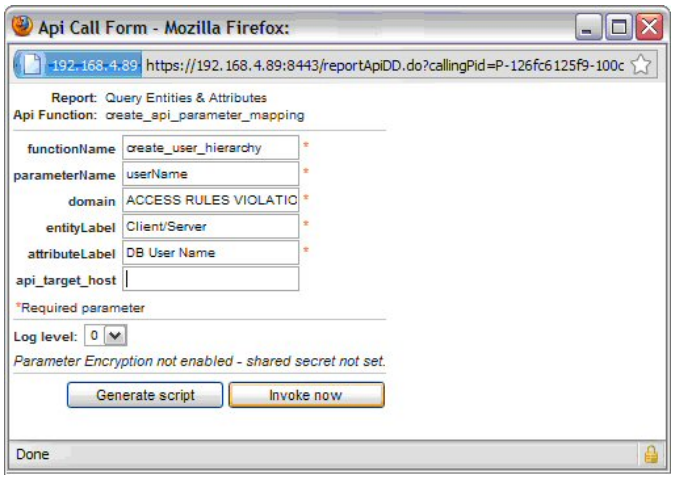
6. Cliquez deux fois sur l'attribut que vous souhaitez attribuer à un nom de paramètre et cliquez sur l'option Appeler...



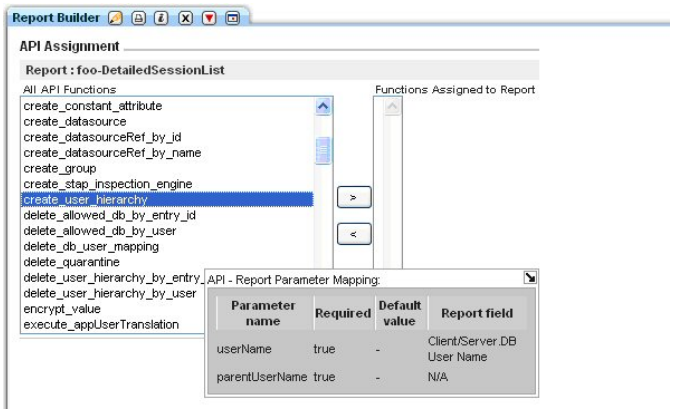
7. Sélectionnez la fonction d'API create_api_parameter_mapping.



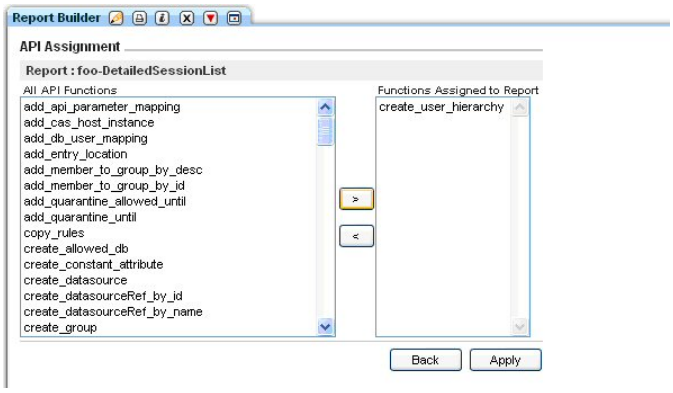
8. Renseignez les valeurs functionName et parameterName, dans le formulaire d'appel d'API, puis cliquez sur le bouton Appeler maintenant.



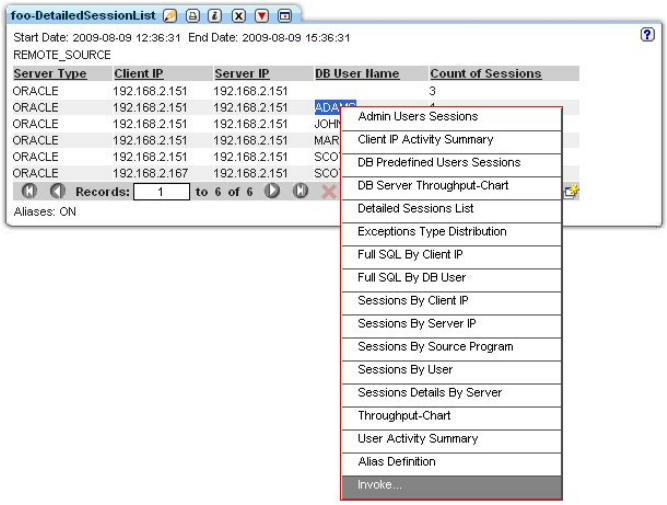
9. A présent, revenez au Générateur de rapport pour visualiser votre rapport et examinez l'affectation d'API. Cliquez sur la fonction d'API create_user_hierarchy pour afficher l'API - Mappage de paramètre de rapport contenant votre mappage de la valeur userName sur le champ du rapport Nom d'utilisateur de la base de données client-serveur.



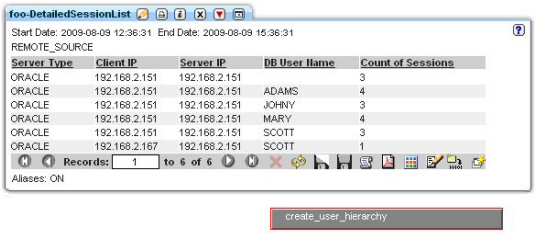
10. Cliquez sur la flèche Supérieur à ">", puis sur le bouton Appliquer



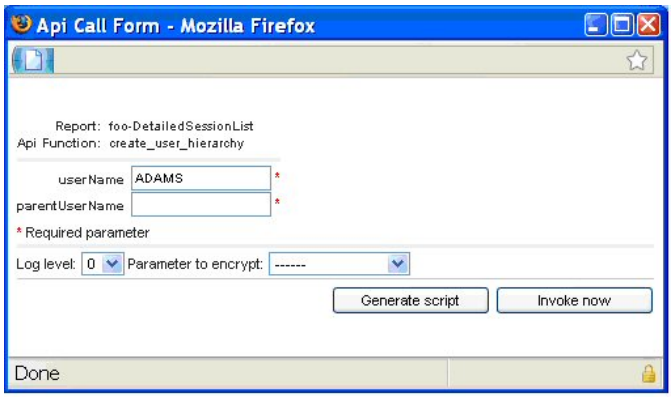
11. A présent, lorsque vous appelez la fonction d'API create_user_hierarchy via le rapport, le paramètre userName est renseigné à partir du rapport. Pour visualiser, revenez au rapport et cliquez deux fois sur une ligne, puis sur l'option Appeler...



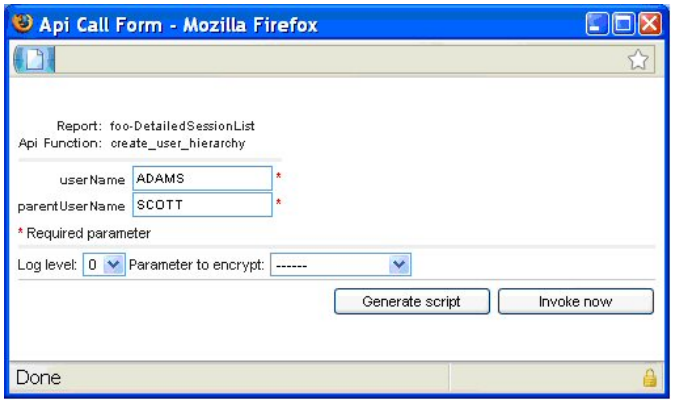
12. Cliquez sur la fonction d'API (en l'occurrence create_user_hierarchy).



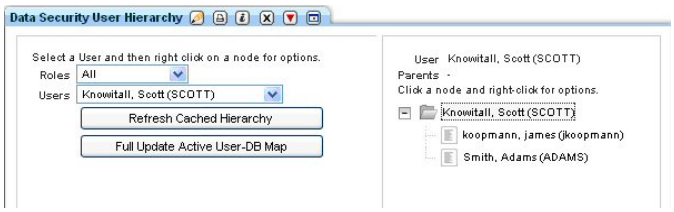
13. Notez que le nom d'utilisateur userName est maintenant rempli à partir du champ du rapport.



14. Complétez le paramètre parentUserName et cliquez sur le bouton Appeler maintenant



15. Vérifiez que la nouvelle hiérarchie utilisateur pour la sécurité des données a été ajoutée.



Rubrique parent : Rapports

Flux externe facultatif

Les flux externes vous permettent d'envoyer des données de rapport Guardium directement sur une base de données externe.

L'envoi de données de rapport à une base de données externe est utile dans plusieurs scénarios, par exemple lors de la combinaison ou de la corrélation des données de Guardium avec des données autres que Guardium, lors de l'utilisation des données Guardium avec des outils externes de génération de rapport ou lors de l'enregistrement d'analyses par machine dans des rapports particulièrement volumineux.

Avant d'utiliser les flux externes, vérifiez les conditions préalables suivantes :

- Mappez un flux entre Guardium et une base de données externe. Actuellement, les flux externes prennent en charge les bases de données relationnelles et peuvent ne pas fonctionner avec d'autres types de bases de données.
- Créez un rapport définissant les données à envoyer via le flux externe. Les rapports prédéfinis sont incompatibles avec les flux externes. Si vous souhaitez utiliser un rapport prédéfini, réalisez une copie de ce rapport et utilisez la copie pour le flux externe.
- Définissez un processus d'audit qui utilise le flux externe.

La première fois qu'une tâche de flux externe facultative s'exécute, la représentation interne nécessaire des sources d'audit est créée. Une limitation est que les données horodatées antérieurement à la date de création de la source d'audit ne peuvent pas être stockées. Cela signifie que la première fois que la tâche est exécutée, elle n'exporte que des données pour la date courante. Lors des exécutions ultérieures de la tâche après cette date, toutes les données à partir de cette date peuvent être exportées. (En d'autres termes, le lendemain, vous pouvez exporter les données du jour plus les données du jour précédent.)

Créer une tâche de flux externe facultative

Si vous n'avez pas encore commencé à définir un processus d'automatisation du flux de travail de conformité, consultez la rubrique Créer un processus de flux de travail avant d'effectuer cette procédure.

1. Si la sous-fenêtre Ajouter une nouvelle tâche ne s'ouvre pas, cliquez sur Ajouter une tâche d'audit.
2. Cliquez sur Flux externe.
3. Sélectionnez le type de flux dans la liste Type de flux. (Les contrôles qui apparaissent ensuite dépendent du type de flux sélectionné). Un type de flux prédéfini est Dernier objet référencé.
   Remarque : Vous devez mapper un flux externe avant de tenter d'utiliser cette fonctionnalité.
4. Sélectionnez un type d'événement dans la liste Type d'événement.
5. Sélectionnez un rapport dans la liste des rapports. Selon le rapport sélectionné, un nombre variable de paramètres apparaît dans la sous-fenêtre Paramètres de tâche.
6. Dans la zone Retard d'extraction, entrez le nombre d'heures pendant lesquelles le flux doit être retardé et sélectionnez la zone Continu pour inclure les données jusqu'à l'exécution de la tâche d'audit. Le journal d'extraction ne s'exécute que lorsque la boîte Continu est sélectionnée.
7. Dans la sous-fenêtre Sources de données, identifiez une ou plusieurs sources de données pour le flux externe. Pour obtenir des instructions sur la façon de définir ou de sélectionner des sources de données, consultez la rubrique Sources de données.
8. Entrez toutes les valeurs de paramètres dans la sous-fenêtre Paramètres de tâche. Les paramètres varient en fonction du rapport sélectionné. La colonne Nombre n'est pas prise en charge dans Flux externe.
9. Cliquez sur Appliquer.

Rubrique parent : Rapports
Concepts associés:
Construction de processus d'audit
Tâches associées:
Mappage d'un flux externe

Mappage d'un flux externe

Apprenez comment mapper un flux externe pour envoyer des données de rapport Guardium directement vers une base de données externe.

Avant de commencer

Vérifiez les conditions préalables suivantes avant de mapper un flux externe :

- Identifiez la base de données externe qui reçoit des données du flux et rassemblez les informations de connexion requises pour cette base de données (adresse IP, numéro de port, nom d'utilisateur, mot de passe, etc.). Actuellement, les flux externes prennent en charge les bases de données relationnelles et peuvent ne pas fonctionner avec d'autres types de bases de données.
- Identifiez le rapport Guardium qui fournit des données au flux externe.
-

Pourquoi et quand exécuter cette tâche

Les flux externes vous permettent d'envoyer des informations de rapport Guardium directement sur une base de données externe. Tout ce qui peut être défini dans un rapport peut être envoyé via un flux externe. Ces flux dépendent du mappage des attributs DOMAIN_ID et ATTRIBUTE_ID issus du mécanisme de génération de rapports Guardium vers les champs de table sur la base de données externe. Chaque mappage se compose des enregistrements de quatre tables (EF_MAP_TYPE_HDR, EF_MAP_TABLE, EF_MAP_COLUMN et EF_MAP_GDM_TYPE). Utilisez la fonction grdapi_create_ef_mapping pour créer ces tables et établir le mappage.

Procédure

1. Générez un rapport avec les données que vous souhaitez transférer à l'aide d'un flux externe. Vous pouvez le faire à partir d'un gestionnaire central, d'un agrégateur ou d'une instance autonome de Guardium, à condition que le système puisse accéder aux données de rapport dont vous avez besoin.
2. A partir de l'interface CLI, exécutez `grdapi create_ef_mapping reportName="Mon rapport"`. En plus d'établir le mappage, la fonction grdapi_create_ef_mapping génère également un exemple d'instruction create table à utiliser dans les étapes suivantes.
3. Sur le système Guardium où votre rapport est défini, recherchez dans /var/log/guard un nom de fichier similaire à ef_sample_[my_report].sql. Ce fichier contient l'exemple d'instruction create table. Vous devez modifier les instructions de ce fichier pour qu'elles correspondent aux exigences de votre base de données externe. Après avoir modifié le fichier, exécutez les instructions sur votre base de données externe pour créer les tables cible.
4. Le flux externe doit désormais être disponible dans les processus de flux de travaux définis dans le générateur de processus d'audit. Consultez la documentation Flux externe facultatif pour plus d'informations.

Rubrique parent : Rapports
Concepts associés:
Flux externe facultatif

Générateur de rapport réparti

Cette fonctionnalité Central Manager permet de collecter automatiquement des données dans la totalité ou un sous-ensemble des unités gérées Guardium qui sont associées à cette instance de Central Manager donnée. Les rapports répartis sont conçus pour fournir une vue générale, pour corréler des données provenant des sources de données et pour résumer les vues des données. Vous pouvez continuer à utiliser des agrégateurs pour la collecte des données au niveau des lignes dans les collecteurs.

Cette fonctionnalité atténue un problème qui peut survenir dans des environnements d'entreprise complexes lorsque les utilisateurs ne connaissent pas toujours l'unité gérée exacte qui comporte les données requises pour un rapport particulier. Cela peut se produire car le lien entre les collecteurs et les bases de données Guardium peut changer avec le temps en fonction d'options de configuration telles que l'équilibrage de charge. Ce problème est compliqué par des considérations telles que la période et la politique de conservation des données sur l'agrégateur et les collecteurs.

Il est facile de créer un rapport réparti. Il suffit de le définir via l'écran Rapports répartis, de l'ajouter à une sous-fenêtre, puis de l'utiliser.

En outre, cette fonctionnalité utilise facultativement les magasins de données sur Central Manager pour permettre la collecte planifiée des données agrégées dans le temps. En substance, les données de rapport réparti sont stockées sur Central Manager en tant que table plate, de sorte qu'aucune jointure complexe n'est nécessaire pour créer le rapport souhaité, ce qui peut considérablement améliorer le temps de réponse pour ces rapports d'entreprise.

Les données du rapport réparti peuvent être collectées auprès des collecteurs, des agrégateurs et même des instances Central Manager. Les versions réparties par défaut des rapports incluent le nom d'hôte de l'unité responsable de ces données.

Les rapports répartis prédéfinis sont les suivants :

- Vérification S-TAP d'entreprise
- Journal d'agrégation/archivage
- Echecs des tentatives de connexion d'utilisateur
- Exceptions des travaux planifiés

Exécution des rapports répartis : immédiate ou planifiée

Lorsque vous définissez un rapport réparti, exécutez-le immédiatement ou programmez-le pour l'exécuter en arrière-plan et collectez les résultats dans Central Manager :

- Immédiate : ce mode regroupe des données à la demande (lors de l'exécution via l'interface utilisateur graphique) et affiche les résultats en collectant les résultats issus des unités gérées concernées. Le rapport réparti comprend un indicateur de statut selon lequel les données sont toujours en transit ou toutes les données ont été reçues d'une unité gérée particulière. Dans ce mode, les données ne sont pas enregistrées sur Central Manager. Dès que le rapport est fermé, les données disparaissent.
- Planifié : ce mode rassemble les données à l'avance afin de permettre une réponse instantanée. Pendant l'intervalle de temps que vous spécifiez dans le planificateur, toutes les données agrégées pertinentes issues des unités gérées spécifiées sont envoyées vers une table du magasin de données désigné sur l'ordinateur de Central Manager et créent un rapport par défaut sur cette table. Cette table a également ses propres domaine et entité pour permettre la création de requêtes et de rapports supplémentaires à l'aide du générateur de requête. Ces rapports peuvent être ajoutés à un processus d'audit afin d'exécuter régulièrement le processus et d'attribuer les résultats du processus à un Rôle, un Utilisateur et/ou un Groupe d'utilisateurs pour examen ou validation.

Considérations relatives à la planification des rapports répartis

- Dans un environnement mixte où Central Manager est à 32 bits et les unités gérées sont à 64 bits, le rapport réparti n'affiche pas les informations issues des systèmes 64 bits. Pour afficher des informations dans ce cas, Central Manager doit être mis à niveau vers 64 bits.
- En raison de la coordination des données à envoyer à Central Manager, il est essentiel que le temps d'horloge sur toutes les unités gérées soit défini en temps réel sur le fuseau horaire où se trouvent les unités gérées. Même une différence de dix minutes entre Central Manager et les unités gérées affecte les performances et la fiabilité des rapports répartis.
- Les définitions de rapports répartis programmés peuvent être exportées et importées, mais les définitions de rapports répartis immédiats ne peuvent pas être exportées ou importées. La planification même n'est pas incluse dans la définition exportée et importée. Il est recommandé de conserver un enregistrement des définitions et de la planification si nécessaire pour les recréer sur un autre système, comme une sauvegarde ou un test de Central Manager. La sauvegarde système comprend des configurations de rapport réparti.
- Si vous spécifiez que les données du rapport sont collectées à partir des agrégateurs et des collecteurs, on peut penser que le rapport réparti par défaut inclue des données en double (bien que le nom d'hôte Guardium soit différent). Dans ce cas, il est préférable de spécifier uniquement des collecteurs ou des agrégateurs uniquement pour la configuration des rapports répartis.
- Les rapports répartis sont basés sur des rapports non répartis existants. Lors de la définition d'un rapport réparti en mode planifié, si la requête d'origine comprend des paramètres d'exécution, vous devez fournir ces valeurs (ou des caractères génériques, %).

- Prévoyez le fait que vous disposez à présent de données résidant sur Central Manager dans une base de données dont vous ne disposiez pas précédemment. Vous devrez donc planifier des changements opérationnels pour la purge, les mises à niveau et la sauvegarde.

Création d'un rapport réparti

La génération de rapport réparti est uniquement disponible à partir d'un dispositif configuré en tant que Central Manager. Pour accéder au générateur de rapport réparti lors de la connexion en tant qu'administrateur, accédez à Rapports > Outils de configuration de rapport > Générateur de rapport réparti.

Dans le Générateur de rapport réparti, vous pouvez effectuer une sélection dans une liste des rapports existants pour modifier la configuration ou l'ajouter à une sous-fenêtre, ou cliquez sur Nouveau pour créer un rapport réparti. En général, tout rapport existant sur Central Manager peut être réparti immédiatement ou exécuté selon une planification (ou les deux).

Création d'un rapport réparti

Dans le Générateur de rapport, sélectionnez Nouveau, ce qui efface toutes les données existantes dans le générateur de rapport, dans le menu déroulant Rapport de base, sélectionnez l'un des rapports existants disponibles pour la distribution. Chaque rapport de la liste peut être réparti une fois en tant qu'immédiat et une fois en tant que planifié. Ceux qui sont définis pour être répartis immédiatement ont le terme (Immédiat) ajouté au nom du rapport réparti.

Sélectionnez un rapport existant pour créer un rapport réparti.

Dans la section Collecter les données depuis du générateur, choisissez Toutes les unités gérées (que gère Central Manager) ou spécifiez certains Groupes et/ou des unités gérées spécifiques.

Remarque : vous pouvez définir des groupes d'unités gérées à partir de Central Manager. Exemples de groupes : groupe de collecteurs et d'agrégateurs ; groupes basés sur l'application, la responsabilité ou la géographie.

Dans la section Mode de fonctionnement du générateur, choisissez le mode de fonctionnement du rapport :

- Immédiat : exécution du rapport lorsque l'utilisateur le demande. Lorsque vous sélectionnez cette option, aucune option supplémentaire n'est à prendre en compte. Vous pouvez cliquer sur Appliquer pour sauvegarder les changements, puis cliquez éventuellement sur Ajouter à sous-fenêtre pour ajouter le rapport à l'interface graphique.
- Planifié : exécution dans un lot qui prépare et rassemble les données à l'avance.

Avec l'option Rapport planifié, vous spécifiez les valeurs supplémentaires suivantes :

- Granularité temporelle : spécifiez la période pendant laquelle le magasin de données est capturé. L'extraction du magasin de données est effectuée à la prochaine limite d'intervalle de Granularité temporelle et couvre l'intervalle de temps spécifié. L'extraction du magasin de données pour une granularité en JOURS commence à minuit et s'exécute tous les X jours. L'extraction du magasin de données pour une granularité en HEURES commence à la limite de l'heure suivante et s'exécute toutes les X heures. L'extraction du magasin de données pour une granularité en MINUTES commence à la limite de la minute suivante et s'exécute toutes les X minutes. Par exemple, si vous spécifiez une Granularité temporelle de 1 heure pour le rapport Nombre de connexions échouées, le compte est basé sur une agrégation horaire des connexions échouées.
- Purger après : indiquez combien de temps conserver les données de rapport dans le magasin de données avant de les purger automatiquement.
- Paramètres d'exécution : selon le rapport sur lequel vous basez le rapport réparti, vous devez spécifier les paramètres d'exécution. Pour visualiser les valeurs valides pour ces champs, examinez la requête pour le rapport d'origine ou spécifiez le caractère générique, %.

Cliquez sur Appliquer. Lorsque le système a terminé d'enregistrer la configuration du rapport réparti, les paramètres Modifier le planning et Rôles sont activés.

Pour créer la planification, cliquez sur Modifier le planning, ce qui vous permet d'accéder au planificateur général.

La définition de la planification est transmise aux unités gérées et indique à chaque unité gérée quand et à quelle fréquence envoyer les données agrégées à Central Manager.

Pour spécifier quels rôles peuvent visualiser ce rapport réparti, cliquez sur Rôles.

Modification d'un rapport réparti existant

Pour les rapports répartis existants, vous pouvez :

- Modifier la configuration, y compris les unités gérées, les détails de la planification ou les paramètres d'exécution
- Ajouter un rapport à un tableau de bord
- Supprimer un rapport réparti
- Créez un rapport planifié basé sur un rapport immédiat existant. Cette option remplace le rapport immédiat. Vous ne pouvez pas créer un rapport immédiat à partir d'un rapport planifié existant.

Pour sélectionner un rapport existant, utilisez la zone de recherche de texte ou faites défiler la liste des rapports existants et sélectionnez celui que vous souhaitez modifier.

Affichage des rapports répartis

Les colonnes supplémentaires suivantes sont incluses dans les rapports répartis :

- Source : le système Guardium dont les données ont été collectées.
- FU : Fuseau horaire - Le système Guardium peut être situé dans un fuseau horaire différent de Central Manager.
- Date : cette colonne indique l'heure du début de la période pour les rapports planifiés et permet de regrouper les résultats selon l'heure et le jour. Pour le mode Immédiat, cette colonne affiche l'heure de début et n'est pas significative.
  Remarque : Seul un maximum de trois champs de dates sont autorisés.

Modifier et mettre à jour

Pour les rapports répartis, modifiez et mettez à jour le rapport de base et mettez à jour le rapport réparti en fonction de la structure du rapport mis à jour.

Si un utilisateur modifie les colonnes dans un rapport de base, ou ajoute ou supprime la clause where dans le rapport de base, puis enregistre et régénère le rapport, pour mettre à jour le rapport réparti basé sur ce rapport mis à jour, l'utilisateur doit seulement cliquer sur "Sauvegarder les changements de rapport" sur le rapport réparti existant pour que les modifications prennent effet.

Si l'utilisateur choisit de mettre à jour le paramètre de rapport existant, l'utilisateur doit d'abord cliquer sur "Appliquer les changements de rapport", puis mettre à jour la valeur du paramètre, puis cliquer sur "Sauvegarder les changements de rapport" pour que les mises à jour prennent effet.

En savoir plus sur le temps

Lors de l'exécution d'un rapport, le personnaliseur de rapport vous permet de spécifier une fenêtre de temps absolu pour la requête (du 3-31-2014 de 8h00 au 3-31-2014 11h00) ou une fenêtre de temps relatif (MAINTENANT A 3 HEURES).

Pour le temps absolu, chaque système Guardium fonctionne à son heure locale. Par exemple, si un rapport réparti collecte les données des systèmes Guardium sur les fuseaux Eastern Standard Time (EST) et Pacific Standard Time (PST), chaque système exécute la requête en fonction de l'heure locale. Dans cet exemple (utile pour vérifier les heures de pointe du matin, minuit ou tout temps absolu spécifique), un système à New York recueille les résultats de 08h00 à 11h00 EST et un système en Californie collecte les résultats de 08h00 à 11h00 PST.

Pour une spécification de temps relatif, chaque système exécute MAINTENANT A N selon l'heure courante sur ce système. Cette fonction est importante pour les rapports en temps réel. Le temps absolu ne peut pas être utilisé pour des rapports en temps réel ou proches du temps réel. Utilisez le mode Immédiat pour la surveillance en temps réel.

Affichage du statut de rapport réparti

Chaque rapport réparti est accompagné d'un rapport de statut indiquant à l'utilisateur quelles machines ont réussi à produire des résultats et lesquelles n'y ont pas réussi. Le lien pour accéder au rapport de statut est mis en surbrillance lorsque vous accédez au rapport dans l'interface graphique.

Pour les rapports planifiés, cliquer sur une ligne dans le Rapport de statut permet l'exécution de l'API pour réexécuter le rapport sur la ou les unités spécifiques.

Si l'exécution spécifique du Rapport réparti en mode Planifié renvoie une erreur, vous pouvez réexécuter le rapport à partir du rapport de statut comme suit :

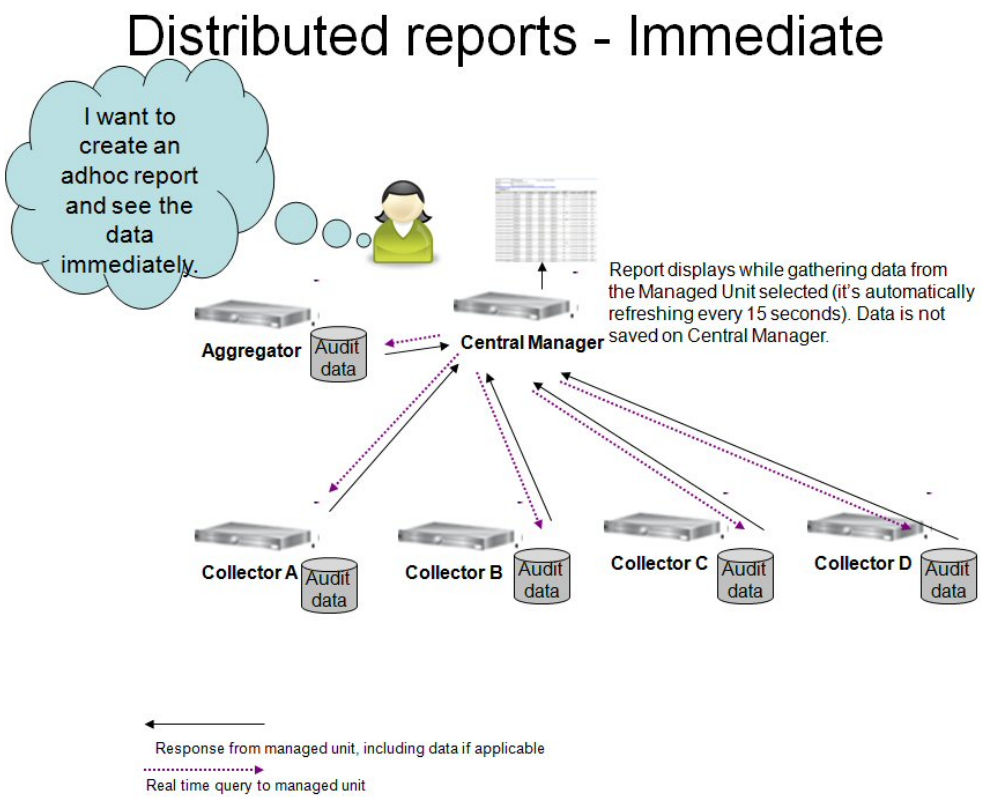
1. Cliquez deux fois sur l'une des lignes du rapport de statut pour afficher le menu Appeler. Cliquez sur Appeler.
2. Cliquez sur la sélection, rerun_distributed_report.
3. Un écran contextuel qui apparaît vous permet de choisir l'exécution spécifique à relancer. Toutes les lignes du rapport peuvent être ouvertes, mais seules les lignes avec l'état ERREUR peuvent être réexécutées.

GuardAPI pour la réexécution de rapport réparti

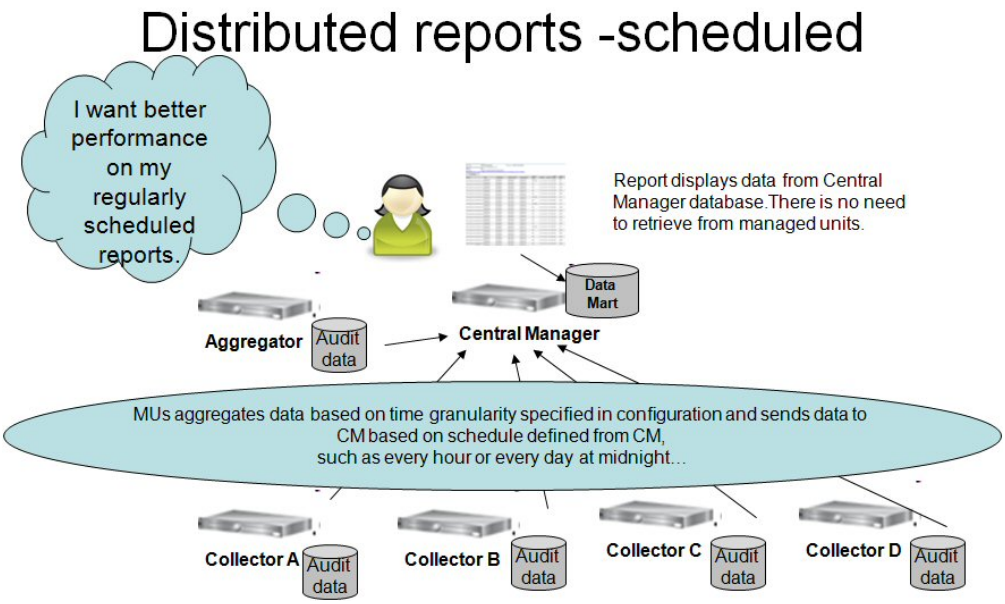
La commande de nouvelle tentative décrite dans l'interface graphique pour appeler le rapport d'état est également accessible via la commande GuardAPI.

Syntaxe

grdapi rerun_distributed_report



Ce diagramme illustre le processus d'exécution d'un rapport réparti immédiat.



Ce diagramme illustre le processus de planification d'un rapport réparti.

Amélioration de rapport réparti - définissez le système cible sur n'importe quel système Guardium

Le Rapport réparti répartit la demande de requête sur les systèmes Guardium spécifiés, il collecte les données dans le système cible, consolide les résultats et fournit des vues sur les résultats consolidés. Les résultats sont disponibles via le Générateur de requête pour la définition de requêtes supplémentaires.

La fonction Rapport réparti peut maintenant définir le système cible sur n'importe quel système Guardium. La version précédente ne permet pas de définir le système cible et elle se rapporte toujours à Central Manager (CM).

Justification des exigences

Dans de nombreux cas, CM est surchargé (quel que soit le rapport réparti) et CM est parfois utilisé en tant qu'agrégateur qui ajoute de la charge.

Dans ce cas, il est beaucoup plus efficace de permettre à l'utilisateur de déterminer le système cible.

Solution

- Un système cible peut être défini pour chaque rapport réparti. Une commande CLI est disponible pour définir les systèmes cible facultatifs. La liste définie via l'interface CLI est affichée dans l'interface graphique du générateur de rapport réparti.
- Remarque importante : cette modification affecte uniquement le mode Rapport réparti planifié. Le mode immédiat n'est pas inclus dans ce changement. Cela signifie que l'afficheur de résultat de rapport réparti ad-hoc est accessible uniquement via CM.
- La définition du rapport réparti est toujours modifiable via CM uniquement.

Changement d'interface graphique

- Un nouveau champ "Envoyer des données à" est ajouté à l'écran Générateur de rapport réparti pour permettre à l'utilisateur de définir le ou les systèmes cible (collecteur(s) ou agrégateur(s)) pour le rapport réparti.
- Ce champ n'est pertinent qu'en cas de mode planifié (sinon il est désactivé).
- La valeur par défaut est définie sur CM.
- La liste des Systèmes cible disponibles est limitée aux systèmes qui ont été définis via l'interface CLI (voir la liste des interfaces CLI ci-dessous).
- La définition du rapport réparti est modifiable via CM et affichable uniquement via la cible.
- L'option "Ajouter à sous-fenêtre" du rapport (ajout de l'afficheur du rapport au menu) est disponible à partir de l'écran de définition sur le Système cible et sur CM.
- Cette option est disponible sur CM même si CM n'est pas le système cible pour ce rapport. Elle permet de visualiser le Statut du rapport réparti sur CM, mais aucune donnée n'est affichée dans le rapport même.

Commandes CLI (disponibles uniquement via CM)

1. Définir le système en tant que système cible

grdapi set_distributed_report_target target_host_name=[unit host name]

2. Annuler le système en tant que système cible

grdapi cancel_distributed_report_target target_host_name=[unit host name]

S'il existe encore des rapports distribués avec cette unité en tant que cible, renvoie une erreur et la liste de ces rapports

3. Obtenir la liste du système cible

grdapi get_distributed_report_target_info

Commandes CLI supplémentaires

Pour les rapports répartis planifiés, stockez ou affichez la valeur d'un nombre maximum de lignes par unité.

show scheduled_distributed

store scheduled_distributed

La commande Store a un paramètre, maximum_rows_per_unit. Si la valeur de ce paramètre est supérieure à 15 000 ou égale à 0 (sans limite), l'utilisateur voit un message d'avertissement :

"Selon le nombre de collecteurs, définir le nombre maximal de lignes par unité sur une valeur élevée peut avoir un impact négatif sur les performances".

Rubrique parent : Rapports

Création d'un rapport réparti

Guardium offre une fonction qui permet de collecter automatiquement des données de la totalité ou d'un sous-ensemble des unités gérées de Guardium qui sont associées à une instance donnée de Central Manager Guardium.

A propos de cette tâche - Cet exemple décrit comment obtenir une vue plus large et un aperçu de la corrélation pour les exceptions (par exemple, les erreurs SQL) enregistrées sur des collecteurs spécifiques.

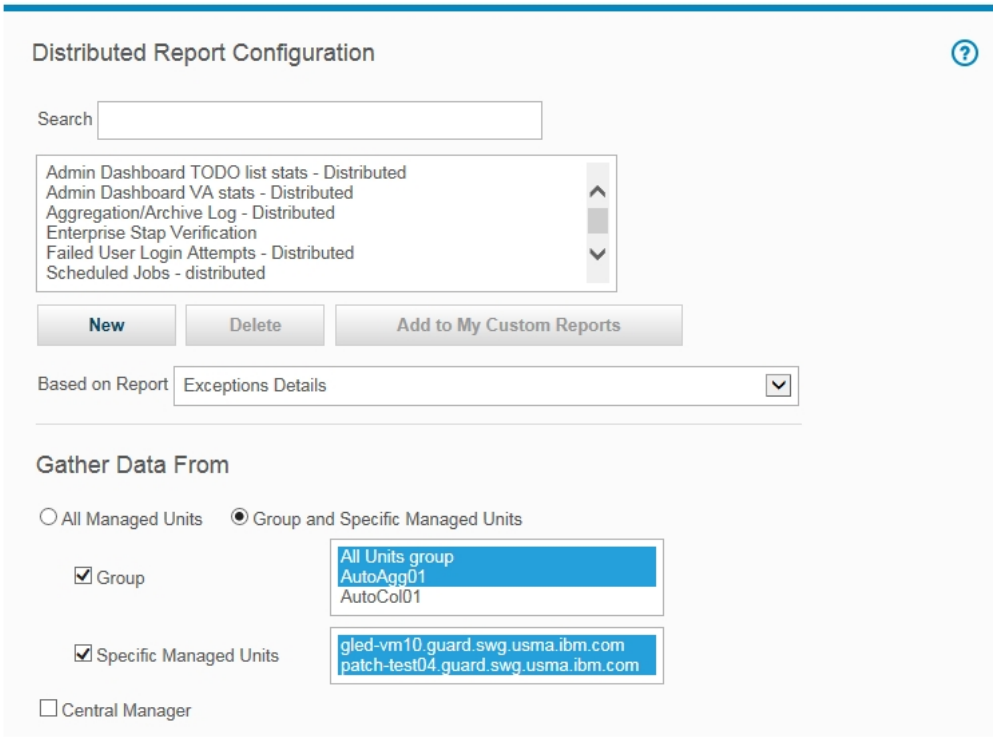
Récapitulatif des étapes

Prérequis - créez un groupe d'unités gérées via l'écran Central Management.

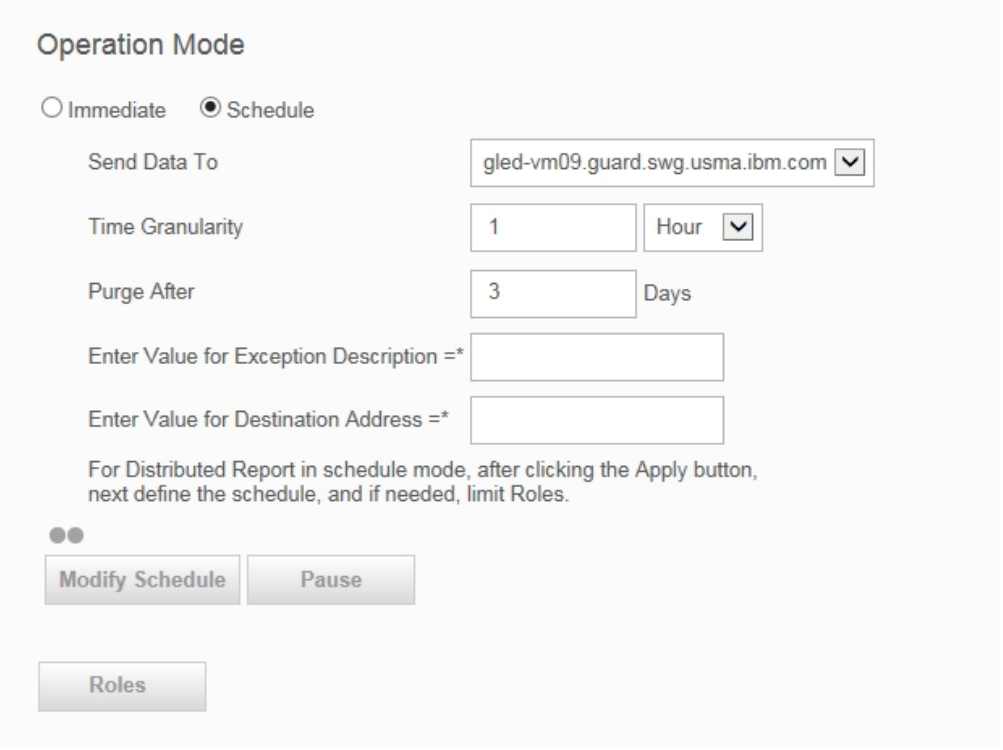
1. Créez un rapport réparti.
2. Examinez les données recueillies.
3. Créez des rapports récapitulatifs supplémentaires sur les données recueillies.

Procédure

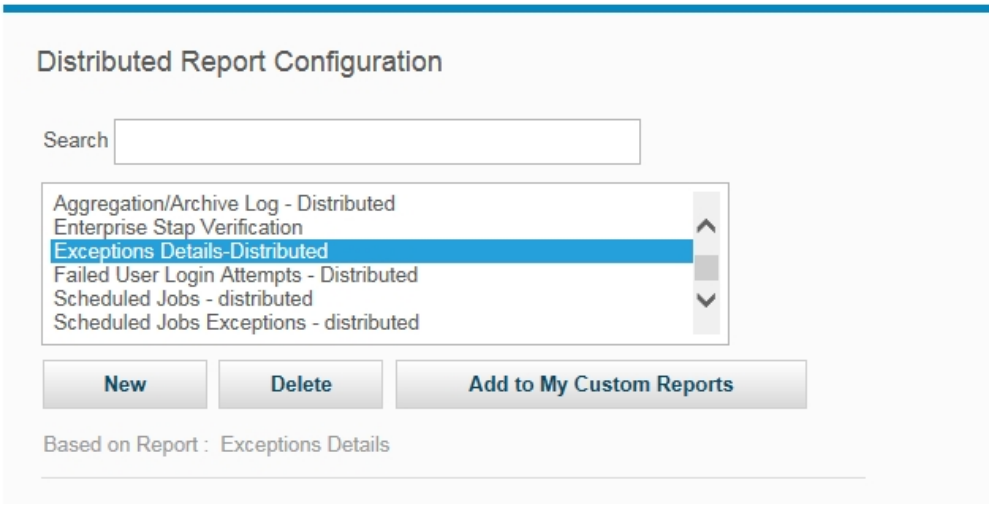
1. Cliquez sur Rapports > Outils de configuration de rapport > Générateur de rapport réparti.
2. Cliquez sur Nouveau.
3. Sélectionnez Rapport de base dans la liste (la liste affiche les rapports définis par l'utilisateur). Pour cet exemple, sélectionnez Détails des exceptions.



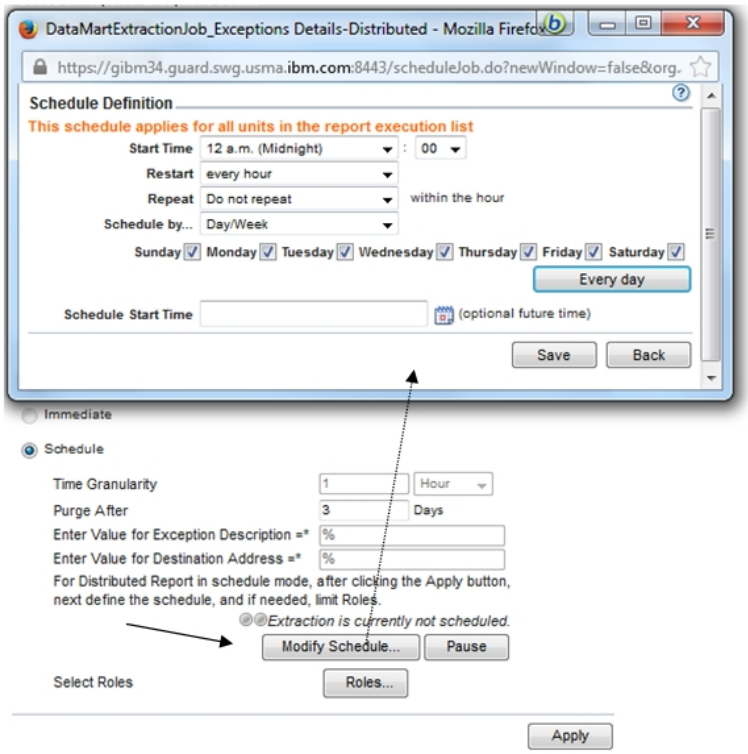
4. Faites défiler l'écran vers le bas pour spécifier les unités gérées à inclure dans ce rapport réparti. Pour cet exemple, sélectionnez deux groupes dans la liste de groupe et des unités gérées dans la liste Unités gérées. Dans cet exemple, désélectionnez "Central Manager" (dans le cas où Central Manager est également un agrégateur, il peut être nécessaire de l'inclure).
5. La capture d'écran suivante montre le paramétrage du Mode de fonctionnement. Le mode Immédiat est principalement destiné à la surveillance en ligne/en temps réel, tel que, l'affichage des tentatives de connexion échouées récentes, l'affichage des exceptions excessives récentes ou l'affichage des alertes en temps réel. Le mode Planifié est une collecte de données continue qui s'exécute régulièrement en fonction de la planification définie. Cet exemple récapitule les exceptions toutes les heures. Il est nécessaire d'indiquer des valeurs pour Description d'exception et Adresse de destination.



6. Cliquez sur Appliquer pour créer le rapport réparti.
7. Une fois appliqué, le nouveau rapport réparti est ajouté et mis en surbrillance dans la zone de liste.

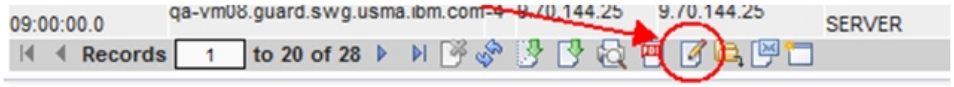


8. L'étape suivante consiste à le planifier en cliquant sur Modifier le planning (obligatoire pour activer le processus).



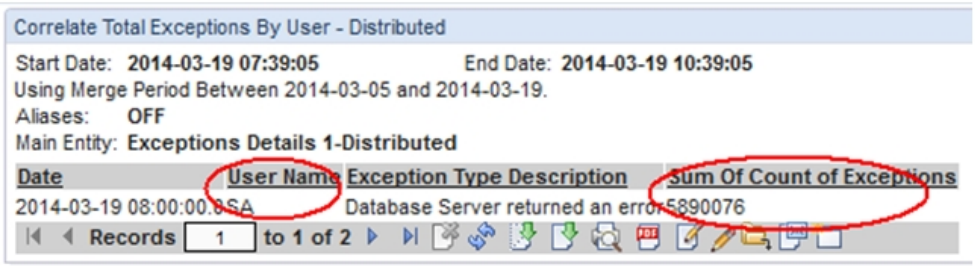
9. Vous pouvez limiter ce rapport à des rôles spécifiques en cliquant sur Rôles et en sélectionnant les rôles pertinents.
10. Dans cet exemple spécifique, le rapport est effectué toutes les heures - il n'est pas nécessaire d'attendre au moins une heure pour obtenir les résultats initiaux. Remarque : La ligne indiquant "Statut du rapport réparti - Cliquez ici pour obtenir plus de détails" affiche le statut de la collecte des données, si des données sont manquantes dans les unités gérées, la ligne est en rouge. Cliquez sur cette ligne pour accéder au rapport détaillé du statut par unité et par heure.

11. Les données sont recueillies auprès de toutes les unités gérées spécifiées et stockées dans la nouvelle entité désignée (table). Cette entité est maintenant disponible via le Générateur de requête et le Générateur de rapport pour créer des requêtes et des rapports supplémentaires à partir de cette nouvelle table. L'option de création de requêtes et de rapports supplémentaires est également disponible via l'écran de résultat du rapport réparti. Cliquez sur Editer la requête pour ce rapport.



Ce rapport par défaut ne peut pas être modifié, cliquez sur Cloner, nommez-le, supprimez tous les attributs et conservez la date, le nom d'utilisateur, la description du type d'exception et la somme du nombre d'exceptions.

La capture d'écran suivante montre un exemple du rapport de corrélation du nombre total d'exceptions par utilisateur (réparti). Cette vue récapitule le nombre total d'exceptions par utilisateur à partir de toutes les bases de données associées aux unités gérées Guardium, sélectionnées pour ce rapport réparti. De même, vous pouvez afficher le nombre total de tentatives de connexion échouées dans l'ensemble du système ou le nombre total des exceptions par programme source.



Rubrique parent : Rapports

Evaluation et renforcement

La solution Guardium Vulnerability Assessment constitue la première étape en matière de gestion du cycle de vie pour la conformité et la sécurité d'un environnement informatique. Vous pouvez utiliser un ensemble d'évaluations prédéfini ou personnalisé et réaliser des audits de flux de travaux afin d'identifier et de traiter les vulnérabilités de base de données automatiquement et de manière pro-active en améliorant les configurations et en renforçant les infrastructures.

- Introduction à Guardium Vulnerability Assessment
  Guardium Vulnerability Assessment vous permet d'identifier et de corriger les vulnérabilités en matière de sécurité dans votre infrastructure de base de données.
- Tests d'évaluation des vulnérabilités
  Guardium fournit plusieurs types de test pour vous permettre d'évaluer vos vulnérabilités.
- Evaluations
  Les évaluations constituent un groupe de tests qui analysent les infrastructures de base de données à la recherche des vulnérabilités et fournissent une évaluation de l'état de santé de la sécurité des données et des bases de données avec des mesures en temps réel et des historiques de mesures.
- Changement obligatoire de schéma
  Le schéma utilisé pour les tests d'évaluation des vulnérabilités sur IBM DB2 for z/OS a changé dans Guardium, version 9.1. Si vous effectuez une mise à niveau à partir d'une version antérieure à 9.1, vous devez mettre à jour la base de données pour pouvoir continuer à utiliser ces tests.
- Evaluation des vulnérabilités RACF
  Si vous utilisez IBM DB2 for z/OS, vous pouvez recourir à des test d'évaluation des vulnérabilités pour évaluer les vulnérabilités liées à votre fonction de contrôle d'accès RACF. Vous devez disposer au minimum de la version 9.1 de Guardium pour réaliser des évaluations RACF.
- Configuration Auditing System (CAS)
  CAS procède au suivi des changements de configuration et génère des rapports. Les données sont disponibles sur le système Guardium et peuvent être utilisées pour les rapports et les alertes.

Introduction à Guardium Vulnerability Assessment

Guardium Vulnerability Assessment vous permet d'identifier et de corriger les vulnérabilités en matière de sécurité dans votre infrastructure de base de données.

Database Vulnerability Assessment est utilisé pour analyser l'infrastructure de base de données afin d'identifier d'éventuelles vulnérabilités et pour fournir une évaluation de l'intégrité de la sécurité des données et des bases de données, en temps réel et avec des mesures historiques.

Vulnerability Assessment utilise trois types d'artefact :

Test
: Un test vérifie l'environnement de base de données à la recherche d'une menace ou d'un sujet de préoccupation particulier.

Evaluation
: Une évaluation est un travail qui inclut une série de tests exécutés ensemble.

Source de données
: Source de données même, par exemple, une base de données ou un fichier XML, et informations de connexion nécessaires pour accéder aux données.

L'application Guardium Vulnerability Assessment permet aux organisations d'identifier et de traiter les vulnérabilités de base de données de façon cohérente et automatisée. Le processus d'évaluation de Guardium évalue l'intégrité de votre environnement de base de données et recommande des améliorations via les opérations suivantes :

- Evaluation de la configuration système par rapport aux meilleures pratiques et recherche des vulnérabilités et des menaces potentielles relatives aux ressources de base de données, notamment les risques liés à la configuration et les comportements à risque. Par exemple, l'identification de tous les comptes par défaut qui n'ont pas été désactivés, la vérification des privilèges publics et des méthodes d'authentification choisies, etc.
- Recherche des vulnérabilités intrinsèques présentes dans l'environnement informatique, par exemple les correctifs de sécurité manquants,
- Recommandation et hiérarchisation d'un plan d'action basé sur les zones à risques et vulnérabilités les plus critiques détectées. La génération de rapports et de recommandations fournit les lignes directrices pour savoir comment répondre aux changements de conformité et renforcer la sécurité de l'environnement de base de données évalué.

L'évaluation des vulnérabilités de base de données de Guardium combine deux méthodes de test principales pour garantir une couverture totale. Elle tire parti de multiples sources d'informations pour obtenir une image complète de l'intégrité de la sécurité de la base de données et de l'environnement des données.

1. Logiciels utilisant un agent installé sur chaque point de terminaison (par exemple un serveur de base de données). Ils peuvent déterminer les aspects d'un point de terminaison qui ne peuvent pas l'être à distance, par exemple l'accès direct d'un administrateur aux données sensibles depuis la console de la base de données.
2. Analyse-interrogation d'un point de terminaison sur le réseau via un accès utilisant des données d'identification.

Dans la solution Guardium Vulnerability and Threat Management sont incluses les fonctionnalités suivantes :

- Database Auto-Discovery procède à la reconnaissance automatique de l'environnement de base de données et crée une représentation graphique des interactions entre les clients et les serveurs de base de données.
- Database Content Classifier procède automatiquement à la reconnaissance et à la classification des données sensibles, par exemple les numéros de carte de crédit à 16 chiffres et les numéros de sécurité sociale à 9 chiffres, pour aider les organisations à identifier rapidement les erreurs et défaillances informatiques liées au stockage de données confidentielles.
- Database Vulnerability Assessment analyse l'infrastructure de base de données à la recherche des vulnérabilités et fournit l'évaluation de l'intégrité de la sécurité des données et des bases de données, en temps réel et avec des mesures historiques.
- CAS (Configuration Auditing System) assure le suivi d'éléments, tels que les structures de base de données, les contrôles de sécurité et d'accès, les valeurs de données critiques et les fichiers de configuration de base de données.
- Compliance Workflow Automation automatise l'intégralité du processus de conformité en commençant par l'évaluation et le renforcement, via la surveillance des activités jusqu'à la production de rapports d'audit, la diffusion des rapports et la validation par des parties prenantes clés.

CAS (Configuration Auditing System) joue un rôle important en matière d'identification des vulnérabilités et des menaces. Les modèles CAS de Guardium préconfigurés et définis par l'utilisateur peuvent être utilisés dans le test d'évaluation et fournissent une vision globale de l'environnement de base de données. Avec CAS, Guardium peut identifier les vulnérabilités de la base de données au niveau du système d'exploitation, par exemple les droits d'accès aux fichiers, la propriété des fichiers et les variables d'environnement. Ces tests sont visibles dans le panneau Définition de jeu de modèles CAS et leur nom contient le mot *Assessment*.

Remarque : Vulnerability Assessment (VA) et Configuration Auditing System (CAS) ne sont pris en charge qu'en anglais.

Common Vulnerabilities and Exposures (CVE®) est un dictionnaire de noms communs (c'est-à-dire d'identifiants CVE) concernant les vulnérabilités de sécurité de notoriété publique. Les identifiants communs de CVE facilitent le partage de données sur des bases de données et des outils de sécurité des réseaux distincts et fournissent une base de référence pour l'évaluation de la couverture de sorte que, si un rapport incorpore des identificateurs CVE, les utilisateurs puissent rapidement et précisément accéder aux correctifs dans l'une des bases de données distinctes compatibles avec CVE afin de remédier au problème.

De nombreuses organisations ont rendu leurs produits et services de sécurité de données compatibles avec CVE en incorporant des identifiants CVE. Guardium surveille en permanence les données CVE (Common Vulnerabilities and Exposures) à partir de MITRE Corporation et ajoute ces tests pour rechercher les vulnérabilités associées aux bases de données pertinentes.

Pour faciliter la recherche de vulnérabilités individuelles tout en consultant les noms CVE concernant des bases de données spécifiques, l'utilisateur, lorsqu'il configure les tests via le Générateur d'évaluation de sécurité, peut sélectionner le bouton d'option CVE pour la base de données souhaitée, puis sélectionner et ajouter l'identifiant CVE approprié. D'autres informations peuvent toujours être trouvées sur la copie principale de la liste CVE gérée par MITRE Corporation.

Pour que CVE soit toujours actualisé dans la solution Guardium, Guardium téléchargera et utilisera la base de données CVE en cours pour remplir une table de base de données avec l'ensemble des entrées et candidats CVE. Guardium compare à l'aide d'un programme les données CVE téléchargées aux données CVE déjà présentes dans le référentiel de Guardium Vulnerability Assessment, ce qui produit une liste de nouvelles données CVE à réviser. L'équipe de sécurité Guardium des bases de données passe en revue manuellement ces candidats pour la base de connaissances de Guardium Vulnerability, les teste et ajoute les candidats pertinents à la base de connaissances GA de Guardium Vulnerability Assessment. Ces tests sont balisés avec le numéro CVE approprié et une fois dans le référentiel GA, ils sont exécutés automatiquement à l'aide de l'application Guardium Vulnerability Assessment.

Remarque :

- Pour la génération de rapports d'évaluation des vulnérabilités (VA) et des rapports sur les autorisations (Entitlement), lorsque vous recherchez des scripts pour octroyer des privilèges pour les rapports relatifs aux autorisations, utilisez les scripts du répertoire gdmmonitor_scripts. N'utilisez pas le dossier entitlement_monitor_role, qui n'est plus mis à jour.
- Lorsque vous utilisez une clé de licence d'utilisation de produit ayant expiré ou une licence avec un nombre limité de sources de données, le message suivant peut s'afficher : `Impossible d'ajouter la source de données. Le nombre maximal de sources de données autorisées par la licence a été atteint.` La date dans Licence valide jusqu'au et le nombre de sources de données sont visibles dans le panneau Configuration système de la console d'administration. Un processus de vulnérabilité ou de classification avec *N* sources de données est comptabilisé sous forme de *N* analyses à chaque exécution.
- Guardium Vulnerability Assessment nécessite l'accès aux bases de données dont il effectue l'évaluation. Pour cela, Guardium fournit un ensemble de scripts SQL (un script pour chaque type de base de données) qui crée les utilisateurs et les rôles dans la base de données que Guardium doit utiliser.

  Les scripts de modèle sont disponibles sur le système Guardium dès qu'il est généré et vous pouvez les rechercher et les télécharger via le serveur de fichiers dans le chemin suivant : /log/debug-logs/gdmmonitor_scripts/. Pour plus d'informations, consultez le fichier README.txt.

Exceptions de test de Guardium Vulnerability Assessment

Les groupes d'exceptions de test de Guardium Vulnerability Assessment sont préremplis avec les membres, le schéma, les objets ou les privilèges par défaut créés lors de l'installation d'une base de données. Utilisez-les pour éviter tout faux positif lors de l'exécution d'évaluations des vulnérabilités. Si une évaluation échoue, liez le groupe d'exceptions approprié au test afin d'exclure les membres par défaut, puis réexécutez le test : s'il s'exécute sans violation, cela signifie que les violations initiales étaient dues aux membres, au schéma, aux objets ou aux privilèges par défaut créés lors de l'installation de la base de données.

Tableau 1. Groupes VA pour tester le mappage

ID de groupe	Nom de groupe	Nom de test	ID test	Type de base de données
82	Octrois approuvés par Sybase au public	Pas de privilège public non exempt	61	SYBASE ASE
83	Octrois approuvés par MS-SQL au public	Pas de privilège public non exempt	270	MSSQL
115	Octrois approuvés par DB2 au public	Pas de privilège sur les objets public	105	DB2 LUW
144	Octrois approuvés par Db2 au public non restrictifs	Pas de privilège sur les objets public	105	DB2 LUW
116	Octrois approuvés par Teradata au public	Privilèges objet octroyés à PUBLIC	2029	TERADATA
117	Octrois approuvés par PostgreSQL au public	Privilèges sur les objets octroyés à PUBLIC	315	POSTGRESQL
118	Octrois approuvés par Netezza au public	Privilèges objet octroyés à PUBLIC (Netezza)	2053	NETEZZA
65	Administrateurs de base de données MS-SQL	Seuls les administrateurs de base de données dans les rôles de serveur fixes	159	MSSQL
165	Accès à SYS.USER$ uniquement pour l'administrateur de base de données Oracle	Accès à SYS.USER$ uniquement pour l'administrateur de base de données	222	ORACLE
166	Privilèges DDL MS-SQL octroyés à l'utilisateur	Privilèges DDL octroyés à l'utilisateur	321	MSSQL
167	Procédures MS-SQL octroyées à des utilisateurs	Procédures octroyées à des utilisateurs	322	MSSQL
168	Pas de privilège MS-SQL utilisateur individuel	Pas de privilège utilisateur individuel	154	MSSQL
170	Droits sur des procédures et des fonctions Sybase IQ octroyés à PUBLIC	Droits sur des procédures et des fonctions octroyés à PUBLIC.	2230	SYBASE IQ
171	Pas de privilèges sur des procédures ou des fonctions Sybase IQ spécifiques	Pas de privilèges sur des procédures ou des fonctions spécifiques.	2227	SYBASE IQ

ID de groupe	Nom de groupe	Nom de test	ID test	Type de base de données
172	Pas d'accès aux procédures étendues -SQL d'accès au registre	Pas d'accès aux procédures étendues d'accès au registre	215	MSSQL
173	Rôle MS-SQL octroyé à un rôle	Rôle octroyé à un rôle	323	MSSQL
185	Accès aux autorisations de niveau serveur MS-SQL octroyé à des utilisateurs sans rôle d'administrateur de base de données	Accès aux autorisations de niveau serveur octroyé à des utilisateurs sans rôle d'administrateur de base de données	2289	MSSQL
186	Privilèges MS-SQL octroyés aux membres des rôles de base de données MSDB	Privilèges octroyés aux membres des rôles de base de données MSDB	2296	MSSQL
48	Version + correctifs de la base de données DB2	Version : DB2	16	DB2 LUW
48	Version + correctifs de la base de données DB2	Niveau de correctif DB2	54	DB2 LUW
49	Version + correctifs de la base de données Informix	Version : Informix	17	INFORMIX
49	Version + correctifs de la base de données Informix	Niveau de correctif Informix	55	INFORMIX
50	Version + correctifs de la base de données MS Sql Server	Version : Microsoft SQL Server	18	MSSQL
50	Version + correctifs de la base de données MS Sql Server	Niveau de correctif Microsoft SQL Server	56	MSSQL
51	Version + correctifs de la base de données MySql	Version : MySql	19	MYSQL
51	Version + correctifs de la base de données MySql	Niveau de correctif MySql	57	MYSQL
52	Version + correctifs de la base de données Oracle	Niveau de correctif Oracle	58	ORACLE
52	Version + correctifs de la base de données Oracle	Version : Oracle	20	ORACLE
53	Version + correctifs de la base de données Sybase	Version : Sybase	21	SYBASE ASE
53	Version + correctifs de la base de données Sybase	Niveau de correctif Sybase	59	SYBASE ASE
109	Version + correctifs Teradata PDE	Version : Teradata PDE	284	TERADATA
109	Version + correctifs Teradata PDE	Niveau de correctif Teradata PDE	286	TERADATA
110	Version + correctifs Teradata TDBMS	Niveau de correctif Teradata TDBMS	287	TERADATA
110	Version + correctifs Teradata TDBMS	Version : Teradata TDBMS	285	TERADATA
111	Version + correctifs Teradata TDGSS	Version : Teradata TDGSS	290	TERADATA
111	Version + correctifs Teradata TDGSS	Niveau de correctif Teradata TDGSS	288	TERADATA
112	Version + correctifs Teradata TGTW	Version : Teradata TGTW	291	TERADATA
112	Version + correctifs Teradata TGTW	Niveau de correctif Teradata TGTW	289	TERADATA
113	Version + correctifs Netezza	Niveau de version Netezza	306	NETEZZA
113	Version + correctifs Netezza	Niveau de correctif Netezza	307	NETEZZA
114	Version + correctifs Postgress	Niveau de version PostGreSQL	308	POSTGRESQL
114	Version + correctifs Postgress	Niveau de correctif PostGreSQL	309	POSTGRESQL
169	Version + correctifs de la base de données SybaseIQ	Version : Sybase IQ	377	SYBASE IQ
169	Version + correctifs de la base de données SybaseIQ	Niveau de correctif Sybase IQ	378	SYBASE IQ

MongoDB

Développée en 2007, MongoDB est une base de données NoSQL orientée documents. MongoDB utilise des documents JSON avec des schémas dynamiques (format nommé BSON). Dans MongoDB, une collection est l'équivalent d'une table de SGBD relationnel et les documents sont l'équivalent des enregistrements dans une table de SGBD relationnel.

MongoDB est le système de base de données NoSQL le plus important avec la croissance la plus forte. Il a tendance à être utilisé comme un système opérationnel et comme back end pour les applications Web car il facilite la programmation des données non relationnelles, telles que les documents JSON souvent présents dans les applications Web.

- Première base de données NoSQL prise en charge pour Guardium Vulnerability Assessment (VA)
- Première connexion de base de données autre que JDBC. La connexion utilise un pilote Java.
- Les sources de données MongoDB prennent en charge les connexions de serveur SSL et les connexions client-serveur avec des certificats client SSL.
- La solution VA de Guardium pour les clusters MongoDB peut être exécutée sur mongos, un noeud principal et tous les noeuds secondaires pour les jeux de répliques.
- Les rapports d'autorisation (Entitlement) et de test basé sur une requête (Query Based Builder) ne sont pas pris en charge pour MongoDB.

Source de données MongoDB avec SSL

Vous pouvez importer un certificat serveur, ce qui se fait de façon officieuse pour les certificats autosignés. Le client peut également importer son certificat. Les certificats fonctionnent également sur le gestionnaire central et pour le transfert d'exécution de la base de données sur les collecteurs.

CAS pour MongoDB

Le modèle d'évaluation CAS MongoDB vous permet d'indiquer plusieurs chemins dans la source de données pour analyser différents composants du système de fichiers.

Teradata Aster

Aster Data

Acquis par Teradata en 2011, Aster Data est utilisé en principe pour les applications d'entrepôts de données et de traitement analytique (OLAP). Aster Data a créé une infrastructure nommée SQL-MapReduce qui permet au langage SQL d'être utilisé avec Map Reduce. Il est associé le plus souvent aux types d'applications à parcours de navigation.

Une évaluation de la sécurité doit être créée pour exécuter tous les tests sur le noeud Queen. Toutes les connexions de base de données pour Aster Data passent uniquement par le noeud Queen.

Les tests sur les noeuds Worker et Loader sont requis uniquement lors de l'exécution des tests CAS (Droits d'accès aux fichiers et Propriété des fichiers).

Les tests de privilèges sont effectués en boucle sur toutes les bases de données d'une instance d'Aster donnée.

SAP HANA

SAP HANA est un système de gestion de base de données relationnelle orienté colonnes sur une plateforme In-Memory, développé et commercialisé par SAP SE. L'architecture de HANA est conçue pour traiter les hauts débits de transaction et le traitement de requêtes complexes.

- Privilèges de base de données pour les évaluations de vulnérabilité et la classification
  Guardium fournit un ensemble de scripts pour simplifier la création de groupes ou de rôles avec le minimum de privilèges nécessaires à l'exécution d'évaluations de vulnérabilité.
- Déploiement de VA pour Db2 for i
  Activez un groupe d'utilisateurs pour exécuter des évaluations de vulnérabilités, et configurer et exécuter les tests.
- Utilisation de VA avec Cloudera
  Découvrez comment utiliser Guardium Vulnerability Assessment (VA) avec les distributions Cloudera d'Apache Hadoop.

Rubrique parent : Evaluation et renforcement

Privilèges de base de données pour les évaluations de vulnérabilité et la classification

Guardium fournit un ensemble de scripts pour simplifier la création de groupes ou de rôles avec le minimum de privilèges nécessaires à l'exécution d'évaluations de vulnérabilité.

Avant de commencer

Cette tâche implique de télécharger les scripts d'un système Guardium et de les exécuter sur un serveur de base de données. Vous devrez identifier l'adresse IP de la machine utilisée pour accéder au système Guardium. Il peut s'agir de l'adresse IP d'un poste de travail individuel, sur lequel vous téléchargerez les scripts avant de les transférer sur un serveur de base de données, ou de l'adresse IP du serveur de base de données lui-même.

Pourquoi et quand exécuter cette tâche

L'exécution des évaluations de vulnérabilité Guardium et l'utilisation du classificateur Guardium requièrent l'accès à la base de données et des privilèges de base de données spécifiques. Guardium fournit un ensemble de scripts pour simplifier la création de groupes ou de rôles avec le minimum de privilèges nécessaires à l'exécution d'évaluations de vulnérabilité. Une fois créés, ces groupes ou rôles peuvent être affectés à n'importe quel utilisateur de base de données ayant besoin d'exécuter une évaluation. Vous devrez créer une source de données Guardium avec cet utilisateur pour effectuer l'analyse d'évaluation de vulnérabilité (VA).

Les scripts fournis couvrent la plupart des types de base de données. Chacun est conçu pour être exécuté dans l'outil de base de données lui-même. Chaque script inclut des instructions détaillées dans son en-tête. Les privilèges octroyés pour chaque type de base de données peuvent être vus dans le script regardant chaque octroi. Important : Avant d'exécuter un script, l'administrateur de base de données doit lire les instructions dans l'en-tête et passer en revue les actions qui seront exécutées par le script sur la base de données.

Procédure

1. Sur un système Guardium, activez le serveur de fichiers en utilisant la commande CLI fileserver. Par exemple, pour activer le serveur de fichiers pour une heure et télécharger les scripts sur un système dont l'IP est `10.0.0.1`, utilisez la commande suivante :

   ```
   fileserver 10.0.0.1 3600
   ```

   Lorsque la commande réussit, le serveur de fichiers doit afficher une sortie similaire à la suivante :

```
Starting the file server...
The file server is ready at https://guardium.host.com:8445
The timeout has been set to 3600 seconds and it may timeout during the uploading.

The upload will only be accessible from the IP you are logged in from: 10.0.0.1

Press ENTER to stop the file server.
```

2. Sur la machine où vous avez téléchargé les scripts, utilisez un navigateur web pour accéder au serveur de fichiers. Par exemple, pour un système Guardium fonctionnant sur `https://guardium.host.com:8445`, accédez aux scripts d'évaluation de vulnérabilité et de classification aux URL suivantes :

   ```
   https://guardium.host.com:8445/log/debug-logs/gdmmonitor_scripts/
   https://guardium.host.com:8445/log/debug-logs/classification_role/
   ```

   Important : Les processus de reconnaissance du classificateur Guardium requièrent un plus haut niveau d'accès à la base de données que pour les tests d'évaluation de vulnérabilité. Il est conseillé d'utiliser les scripts dans `gdmmonitor_scripts` pour l'évaluation de vulnérabilité et les scripts dans `classification_role` pour le classificateur. Avant d'exécuter un script, l'administrateur de base de données doit lire les instructions dans l'en-tête et passer en revue les actions qui seront exécutées par le script sur la base de données. Avant d'exécuter un script, l'administrateur de base de données doit lire les instructions dans l'en-tête et passer en revue les actions qui seront exécutées par le script sur la base de données.
3. Téléchargez les scripts requis en utilisant l'action Clic droit > Enregistrer la cible du lien... du navigateur web ou une fonction similaire. Passez en revue les fichiers README.txt pour identifier les scripts à utiliser pour un type spécifique de base de données.
   Conseil : Il y a trois scripts pour Microsoft SQL Server :
   - gdmmonitor-mss2000-only.sql est pour Microsoft SQL Server 2000
   - gdmmonitor-mss.sql est pour Microsoft SQL Server 2005 et versions plus récentes
   - gdmmonitor-mss-SA.sql est utilisé pour fournir les privilèges d'administration requis pour six des tests d'évaluation de vulnérabilité de Microsoft SQL Server. Si vous n'autorisez pas ces privilèges, les tests retourneront des erreurs indiquant des privilèges inadéquats. Ces six tests ne représentent pas plus de 5 % des tests disponibles.

Que faire ensuite

Après avoir téléchargé les scripts requis pour vos serveurs de base de données, lisez attentivement et suivez les instructions figurant dans leur en-tête.

Rubrique parent : Introduction à Guardium Vulnerability Assessment

Déploiement de VA pour Db2 for i

Activez un groupe d'utilisateurs pour exécuter des évaluations de vulnérabilités, et configurer et exécuter les tests.

Pourquoi et quand exécuter cette tâche

Procédure de déploiement

1. Vulnerability Assessment est déployé à partir du système Guardium.
2. L'utilisateur exécute un script fourni par Guardium sur la base de données cible pour créer un rôle avec les privilèges appropriés. Il crée ensuite une connexion de source de données à la base de données.
3. Créez une évaluation de la sécurité, puis sélectionnez vos sources de données et les tests que vous souhaitez exécuter.
4. Une fois l'exécution terminée, un rapport est créé, indiquant que les tests ont réussi ou échoué ainsi que les détails de recommandation pour renforcer la sécurité.

Prise en charge des versions d'IBM for i :

Partitions IBM for i 6.1, 7.1 et 7.2

Couverture du test VA (115 tests au total) :

Profils avec des droits spéciaux

Profils avec accès à l'utilisation de la fonction de base de données

Politiques relatives aux mots de passe

Privilège sur les objets de base de données octroyé à PUBLIC

Privilège sur les objets de base de données octroyé à un utilisateur individuel

Privilège sur les objets de base de données octroyé avec l'option grant

APAR de sécurité

Rapports sur les autorisations :

Profils avec des droits spéciaux

Groupe octroyé à l'utilisateur

Privilège sur les objets de base de données octroyé à PUBLIC

Privilèges sur les objets exécutables de base de données octroyés à PUBLIC

Privilège sur les objets de base de données octroyé à un utilisateur individuel

Privilège sur les objets de base de données octroyé avec l'option grant

Procédure

1. Utilisez le Générateur de groupe pour créer un groupe d'utilisateurs qui, selon votre souhait, utilisera VA. Ouvrez le Générateur de groupe en cliquant sur Configurer > Outils et vues > Générateur de groupe. L'étape suivante utilise un script pour le groupe nommé gdmmonitor.
2. Exécutez le script suivant sur votre système Db2 for i pour octroyer au groupe les privilèges nécessaires à l'exécution de VA. Cette opération s'effectue en dehors du système Guardium à l'aide d'un client natif de base de données.

   ```
   grant select on SYSIBMADM.FUNCTION_INFO to gdmmonitor;
   grant select on SYSIBMADM.FUNCTION_USAGE to gdmmonitor;
   grant select on SYSIBMADM.GROUP_PROFILE_ENTRIES to gdmmonitor;
   grant select on SYSIBMADM.SYSTEM_VALUE_INFO to gdmmonitor;
   grant select on SYSIBMADM.USER_STORAGE to gdmmonitor;
   grant select on Qsys2.Authorizations to gdmmonitor;
   grant select on SYSIBMADM.USER_INFO to gdmmonitor;
   grant select on QSYS2.SYSSCHEMAAUTH to gdmmonitor;
   grant select on QSYS2.SYSTABAUTH to gdmmonitor;
   grant select on QSYS2.SYSPACKAGEAUTH to gdmmonitor;
   grant select on QSYS2.SYSROUTINEAUTH to gdmmonitor;
   grant select on QSYS2.SYSSEQUENCEAUTH to gdmmonitor;
   grant select on QSYS2.SYSCOLAUTH to gdmmonitor;
   ```

   A partir de la version IBM Db2 for i 7.1, incluez également les scripts :

   ```
   grant select on QSYS2.SYSVARIABLEAUTH to gdmmonitor;
   grant select on QSYS2.SYSXSROBJECTAUTH to gdmmonitor;
   ```

3. Créez une connexion JDBC à votre système Db2 for i. Ouvrez le Localiseur de source de données en cliquant sur Configurer > Outils et vues > Définitions de source de données, puis Evaluation de la sécurité dans le menu Sélection d'application.
   a. Cliquez sur Nouveau et entrez les informations appropriées. Pour Propriété de connexion, entrez "property1=com.ibm.as400.access.AS400JDBCDriver;translate binary=true".
4. Créez une évaluation à l'aide du Générateur d'évaluation. Ouvrez le Générateur d'évaluation en cliquant sur Renforcement > Vulnerability Assessment > Générateur d'évaluation.
   a. Entrez une description pour l'évaluation.
   b. Ajouter la source de données créée à l'étape précédente en cliquant sur Ajouter une source de données, en sélectionnant la source de données dans le Localiseur de source de données, puis en cliquant sur Ajouter.
   Remarque : Vous devez cliquer sur Appliquer pour sauvegarder l'évaluation avant de configurer les tests.
5. Ajoutez des tests à l'évaluation en cliquant sur Configurer tests. Cliquez sur l'onglet IBM for i, sélectionnez les tests que vous souhaitez ajouter et cliquez sur Ajouter des sélections.
6. Cliquez sur Revenir pour revenir au Localiseur d'évaluation de sécurité. Exécutez le test en cliquant sur Exécuter une fois maintenant ou planifiez le test à l'aide du Générateur de processus d'audit. Ouvrez le Générateur de processus d'audit en cliquant sur Reconnaissance > Classifications > Générateur de processus d'audit.
7. Cliquez sur Afficher les résultats pour afficher les détails de tous les tests exécutés, y compris les recommandations pour améliorer votre score.

Résultats

Que faire en cas d'échec d'un test ?

- Vous pouvez appliquer un correctif à votre base de données si l'échec est relatif aux correctifs.
- Vous pouvez reconfigurer les paramètres de base de données en fonction des recommandations concernant les meilleures pratiques à adopter
- Vous pouvez révoquer des privilèges système ou des privilèges sur les objets qui ne sont pas requis par vos applications.
- Vous pouvez révoquer des objets octroyés directement à un bénéficiaire et octroyer les privilèges sur les objets à un rôle ou à un groupe, puis affecter le bénéficiaire à ce rôle ou à ce groupe
- Vous pouvez changer le paramètre de stratégie de mot de passe ou changer le mot de passe par défaut de l'utilisateur.
- Si votre application nécessite l'octroi de privilèges spécifiques, vous pouvez créer un groupe d'exceptions et l'associer au test ayant échoué puis relancer l'exécution du test.

Rubrique parent : Introduction à Guardium Vulnerability Assessment

Utilisation de VA avec Cloudera

Découvrez comment utiliser Guardium Vulnerability Assessment (VA) avec les distributions Cloudera d'Apache Hadoop.

Cloudera Manager

Configuration de la source de données

La source de données Cloudera Manager utilise l'API Java de Cloudera Manager pour une connexion. Elle n'utilise pas JDBC.

Le nom du cluster doit être défini dans l'interface graphique de la source de données. Il s'agit du nom de cluster affiché dans l'interface Cloudera Manager, sur la côté gauche.

Pour exécuter des tests d'évaluation de vulnérabilité pour Cloudera Manager, vous devez définir un utilisateur de source de données avec le rôle Lecture seule. Cela s'applique à la plupart des tests. Quelques-un d'entre eux nécessitent, pour leur exécution, un utilisateur de source de données ayant le rôle d'administrateur du cluster.

Les tests d'évaluation de vulnérabilité suivants requièrent un utilisateur de source de données avec le rôle d'administrateur du cluster :

1. Ordre des back ends d'authentification
2. Port HTTP pour la console d'administration
3. Port HTTPS pour la console d'administration
4. Utiliser l'authentification TLS des agents vis-à-vis du serveur
5. Utiliser le chiffrement TLS pour la console d'administration
6. Utiliser le chiffrement TLS pour les agents

Cette information est également disponible dans le script gdmmonitor de Cloudera Manager (/log/var-log-guard/gdmmonitor_scripts/gdmmonitor-Cloudera-Manager.sql).

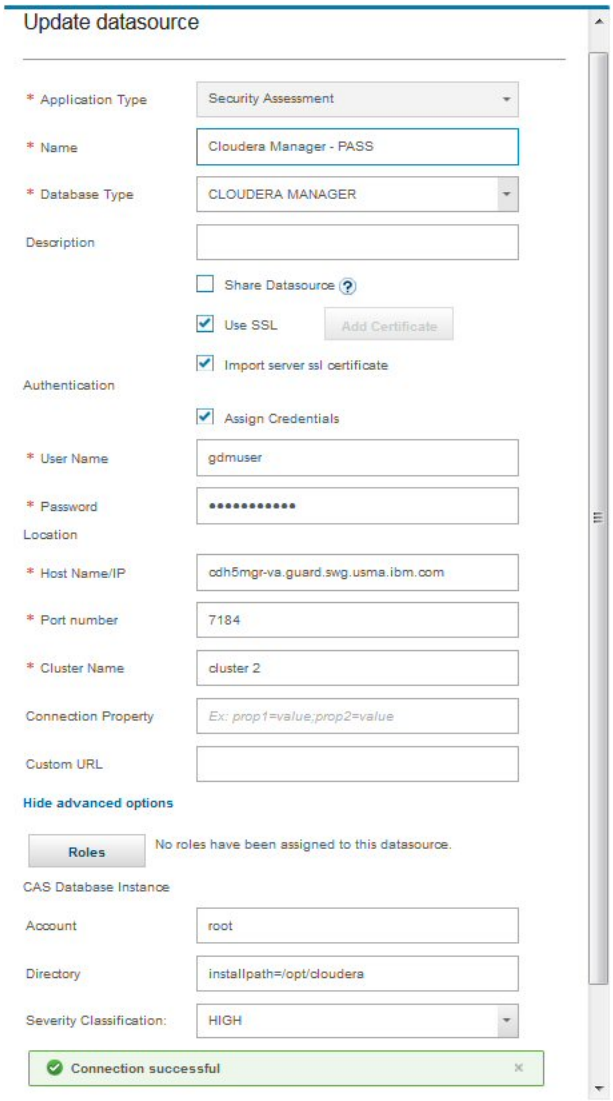
Si SSL est activé, cochez “Utiliser SSL” ainsi que “Importer le certificat SSL du serveur”

Valeurs à spécifier dans la section Instance de base de données CAS

Le compte doit être root.

Le répertoire doit être le chemin d'installation de Cloudera Manager. Par exemple : installpath=/opt/cloudera

Exemple de valeurs pour la source de données Cloudera Manager.



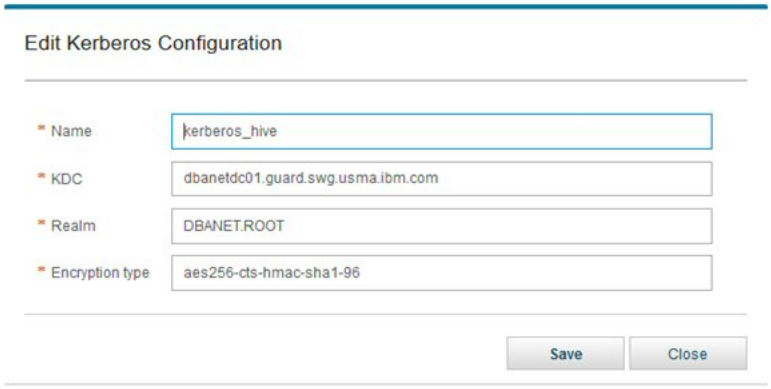
Hive

Configuration de la source de données

Utilisez le pilote Apache Hive JDBC driver 1.1.1.

Kerberos - Le nom d'utilisateur et le mot de passe doivent être ceux d'une combinaison Kerberos valide. Celle-ci est également utilisée pour CA. Faites des tests pour vous assurer que vos ID utilisateur et mot de passe Kerberos sont utilisables pour vous connecter à la ligne de commande beeline.

Assurez-vous qu'une configuration Kerberos est déjà créée, dans laquelle sont définis les centre de distribution de clés (KDC) et superdomaine (realm) pour votre dispositif (appliance). Dans l'interface Guardium, allez à Configurer > Outils et vues > Configuration Kerberos. Si aucune configuration Kerberos n'a été créée, cliquez sur l'icône + pour en créer une.



Après avoir créé une configuration Kerberos, vous pouvez la sélectionner pour configurer votre source de données.

Si SSL est activé, cochez la case “Utiliser SSL” ainsi que la case “Importer le certificat SSL du serveur”.

Remarque : Hive peut utiliser soit LDAP/SSL, soit Kerberos, mais pas les deux en même temps.

Valeurs à spécifier dans la section Instance de base de données CAS

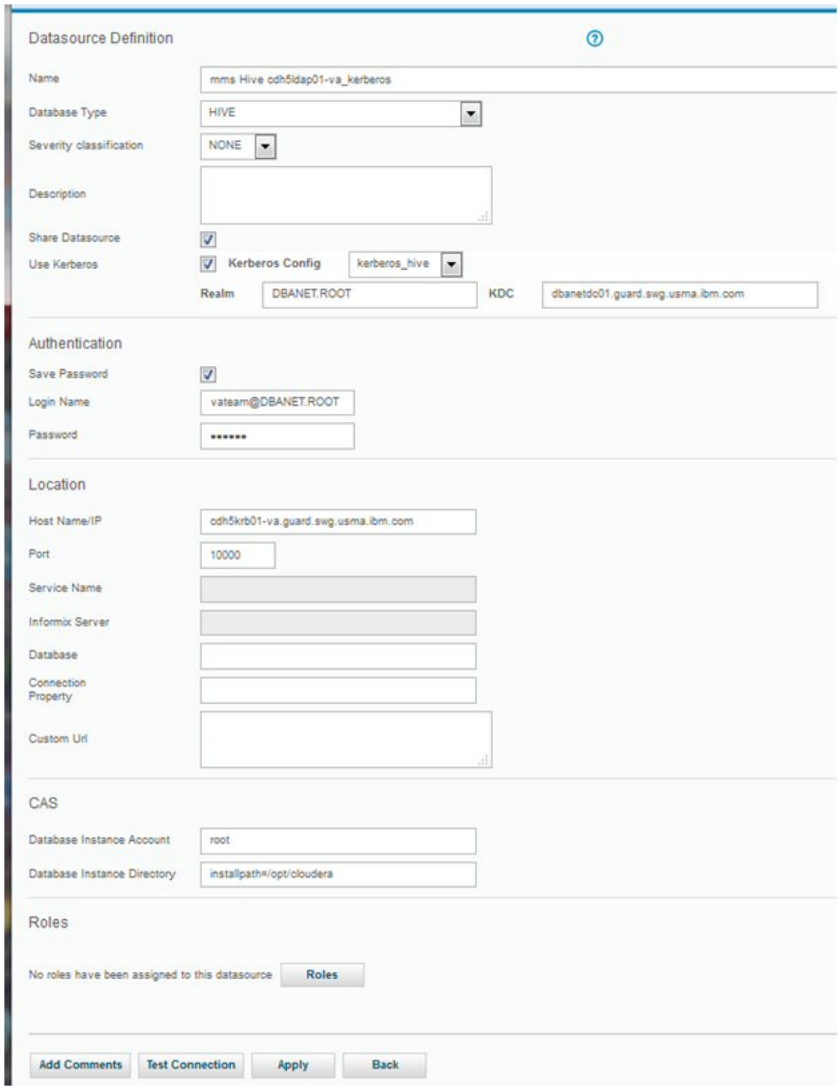
1. Le répertoire doit être le chemin d'installation de Cloudera Manager. Par exemple : installpath=/opt/cloudera
2. Si HDFS est activé pour Kerberos, le nom d'utilisateur de la source de données et le mot de passe associé doivent être ceux d'une combinaison Kerberos valide. Les scripts CAS utilisent cette combinaison pour obtenir un ticket Kerberos.
3. Le compte doit être root. Pour certains tests de paramètres nécessitant CAS, il est important que l'utilisateur CAS soit root, car il doit pouvoir accéder en temps réel à la configuration sous le répertoire du processus de l'agent Cloudera (/var/run/cloudera-scm-agent/process/).

Remarque : Guardium ne modifie en rien vos données de configuration.

Pour Hive

Pour les tests de privilèges, le compte de la source de données doit être un membre du groupe d'administrateurs sentry. Pour les étapes de vérification du groupe d'administrateurs sentry, voyez le script Hive gdmmonitor.

Lors de la configuration des sources de données Hive, seule la source de données pointant sur votre HiveServer2 se prête à un test de connexion JDBC. Pour toutes les autres sources de données Hive, vous pouvez cloner cette source de données spécifique en utilisant le nom du noeud où le service Cloudera est installé. Assurez-vous que le clone de la source de données a un nom d'utilisateur et un mot de passe valides, au même titre que la source de données pointant sur HiveServer2. Pour ces sources de données, vous ne pouvez pas effectuer de test de connexion. Cependant, Guardium compte sur l'exactitude du nom d'utilisateur et du mot de passe de la source de données pour établir une connexion Kerberos en utilisant CAS lorsque Kerberos est activé.



Tests d'évaluation des vulnérabilités

Les tests des privilèges Hive nécessitent que les services Sentry soient installés et configurés. Sans eux, il n'y a pas de sécurité. Tout le monde peut se connecter à Hive et accéder aux données.

Les tests d'évaluation de vulnérabilité CAS des paramètres HDFS sont tirés des fichiers de configuration situés sous le répertoire du processus de l'agent Cloudera (/var/run/cloudera-scm-agent/process/). Les noms de dossier à l'intérieur de ces répertoires changent à chaque démarrage des services de l'agent Cloudera.

Parmi les tests CAS des paramètres HDFS, certains nécessitent que le système de la source de données soit un noeud spécifique (par exemple, NameNode ou DataNode). D'autres nécessitent que Yarn, Mapreduce ou Hive Server soient installés sur ce système. Pour votre évaluation, sélectionnez les tests avec soin, en fonction de la configuration du système de la source de données. Si les besoins d'un test ne sont pas satisfaits, celui-ci renverra une erreur accompagnée de la recommandation d'exécuter les tests sur les services Cloudera corrects. Les besoins à satisfaire sont également mentionnés dans la description du test.

Lorsque vous créez une source de données Hive, il est conseillé d'avoir une source de données par service Cloudera (NameNode, DataNode, HiveServer2, Hive metastore, Yarn NodeManager et Yarn ResourceManager).

Indépendamment du nombre de noeuds dans votre cluster, si vous avez une source de données Guardium Hive couvrant tous ces services, votre environnement est correctement configuré pour l'exécution d'une évaluation de sécurité.

Par exemple

Rubrique parent : Introduction à Guardium Vulnerability Assessment

Tests d'évaluation des vulnérabilités

Guardium fournit plusieurs types de test pour vous permettre d'évaluer vos vulnérabilités.

Tests d'évaluation des vulnérabilités

Guardium fournit plus de deux cents tests prédéfinis permettant de vérifier les vulnérabilités liées aux paramètres de configuration des bases de données, aux privilèges et d'autres vulnérabilités. Vous pouvez également définir vos propres tests.

Une évaluation de vulnérabilités peut contenir un ou plusieurs types de tests parmi les suivants.

Tests prédéfinis

Les tests prédéfinis sont conçus pour illustrer les problèmes de vulnérabilités courants pouvant être détectés dans les environnements de base de données. En raison de la nature extrêmement variable des applications de base de données et des différences sur ce qui est jugé acceptable en fonction des différentes sociétés ou situations, certains de ces tests seront adaptés à certaines bases de données mais seront totalement inadaptés pour d'autres (même au sein de la même société). La plupart des tests prédéfinis sont personnalisables pour répondre aux exigences de votre organisation. En outre, pour conserver les évaluations à jour afin de répondre aux pratiques recommandées des différents secteurs d'activité et se protéger face aux vulnérabilités qui viennent d'être découvertes, Guardium diffuse de nouveaux tests d'évaluation et mises à jour chaque trimestre dans le cadre de son service "Database Protection Subscription Service". Consultez le guide d'administration de Guardium pour plus de détails.

Les types de tests prédéfinis sont les suivants :

- Tests de comportement
- Tests de configuration

Tests de comportement

Cette série de tests évalue l'état de la sécurité de l'environnement de base de données en observant le trafic de la base de données en temps réel et en détectant les vulnérabilités liés à l'accès et à la manipulation des informations.

Par exemple, voici quelques-uns des tests de vulnérabilité liée au comportement inclus :

- Accès des utilisateurs par défaut
- Violations de règle d'accès
- Exécution des commandes Admin, DDL et DBCC directement à partir des clients de base de données
- Nombre excessif d'échecs de connexion
- Nombre excessif d'erreurs SQL
- Connexion en dehors des heures de travail
- Nombre excessif de connexions administrateur
- Vérifications d'appels de procédures mémorisées étendues
- Test vérifiant si les ID utilisateurs sont accessibles à partir de plusieurs adresses IP

Tests de configuration

Cette série d'évaluations vérifie les paramètres de configuration liés à la sécurité des bases de données cible, à la recherche d'erreurs ou de défauts de configuration pouvant être à l'origine de vulnérabilités.

Par exemple, les catégories actuelles, avec quelques tests de haut niveau, pour détecter les vulnérabilité liées à la configuration comprennent :

- Privilège
  - Création d'objet / droits d'utilisation
  - Octrois de privilèges aux administrateurs de base de données et à des utilisateurs individuels
  - Droits au niveau système
- Authentification
  - Utilisation de compte utilisateur
  - Utilisation de connexion à distance
  - Réglementation concernant les mots de passe
- Configuration
  - Paramètres spécifiques à une base de données
  - Paramètres de niveau système
- Version
  - Versions de base de données
  - Niveau de correctif de la base de données
- Objet
  - Exemples de base de données installés
  - Dispositions de base de données recommandées
  - Propriété de base de données

Tests basés sur une requête

Un test basé sur une requête est soit un test prédéfini ou un test défini par l'utilisateur pouvant être rapidement et facilement créé en définissant ou en modifiant une requête SQL, qui sera exécutée pour une source de données de la base de données et dont les résultats seront comparés à une valeur de test prédéfinie. Voir Définir un test basé sur une requête pour plus d'informations sur la génération d'un test basé sur une requête défini par l'utilisateur.

Tests basé sur CAS

Un test basé sur CAS est soit un test prédéfini ou un test défini par l'utilisateur basé sur un élément de modèle CAS de type commande de script de système d'exploitation et qui utilise des données collectées par CAS.

Les utilisateurs peuvent spécifier l'élément de modèle et le test par rapport au contenu des résultats CAS. Voir Créer un élément de jeu de modèles pour obtenir de l'aide sur la création d'un modèle CAS de type Script de système d'exploitation.

Guardium est préconfiguré avec des éléments de modèle CAS de type Script de système d'exploitation qui peuvent être utilisés pour la création d'un test basé sur CAS. Ces tests sont visibles dans le panneau Définition de jeu de modèles CAS et ont un nom comportant le mot *Assessment*. Par exemple, le jeu Unix/Oracle pour les

évaluations est nommé Guardium Unix/Oracle Assessment. En outre, un modèle ajouté qui est assorti à des droits d'accès aux fichiers sera également utilisé pour la vérification des autorisations et de l'appartenance. Voir Modifier un élément de jeu de modèles pour afficher ces jeux de modèles et voir les éléments de type Scripts de système d'exploitation.

Que vous utilisiez les tests préconfigurés de Guardium ou définissiez vos propres tests, une fois définis, ces tests apparaissent dans la sélection lors de la création ou de la modification de tests basés sur CAS. Voir Définir un test basé sur CAS pour plus d'informations.

Tests CVE

Guardium surveille en permanence les données CVE (Common Vulnerabilities and Exposures) à partir de MITRE Corporation et ajoute ces tests pour rechercher les vulnérabilités associées aux bases de données pertinentes.

- Définition d'un test basé sur une requête
  Créez un test basé sur une requête qui exécute une instruction SQL.
- Définition d'un test basé sur CAS
  Les évaluations des vulnérabilités utilisent le mécanisme CAS pour exécuter des tests au niveau du système d'exploitation sur le serveur de base de données et identifier les vulnérabilités.

Rubrique parent : Evaluation et renforcement

Définition d'un test basé sur une requête

Créez un test basé sur une requête qui exécute une instruction SQL.

Pourquoi et quand exécuter cette tâche

Vous pouvez créer un test basé sur une requête en utilisant l'une des approches suivantes :

Nouveau
: Démarrer depuis le début et définir tous les champs.

Cloner
: Cloner un test basé sur une requête existant.

Modifier
: Modifier un test basé sur une requête existant.

Procédure

1. Ouvrez le Générateur d'évaluation en cliquant sur Renforcement > Vulnerability Assessment > Générateur d'évaluation.
2. Dans les tests définis par l'utilisateur, cliquez sur Tests basés sur une requête.
3. Cliquez sur Nouveau, Cloner ou Modifier pour ouvrir le Générateur de test basé sur une requête.
4. Entrez un Nom de test unique.
5. Sélectionnez un Type de base de données.
6. Sélectionnez une Catégorie.
7. Sélectionnez une Gravité.
8. Facultatif : Entrez une Brève description pour le test.
9. Facultatif : Entrez une Référence externe pour le test.
10. Entrez le Texte de résultat pour réussite qui sera affiché en cas de réussite du test.
11. Entrez le Texte de résultat pour échec qui sera affiché en cas d'échec du test.
12. Entrez l'Instruction SQL qui sera exécutée pour le test.

    Utilisez la convention suivante pour ajouter et référencer des membres de groupe dans une instruction SQL :

    Par exemple :

    Pour référencer un groupe d'utilisateurs définis pour le groupe nommé MyUsersGroup et le remplacer par les membres effectifs du groupe, utilisez :

    ```
    Select ... from DBA_GRANTS where ... AND USER in (~~G~MyUsersGroup~~) and ...
    ```

    Vous obtiendrez une instruction SQL de ce type où U1, U2, etc sont les membres du groupe MyUsersGroup :

    ```
    Select ... from DBA_GRANTS where ... AND USER in ('U1','U2','U3',...) and ...
    ```

    Si le groupe n'a pas de membre, la base de données renvoie une erreur. Dans ce cas, la référence est remplacée par une simple paire de guillemets, comme suit :

    ```
    Select ... from DBA_GRANTS where ... AND USER in ('') and ...
    ```

    Utilisez la convention suivante pour remplacer une référence à un alias spécifique (d'un type de groupe spécifique) par l'alias réel :

    Par exemple :

    Select ... from USER_OBJECTS where ... AND OBJECT_TYPE = '~~A~GroupType~TYPE~~'

    S'il existe un alias de TYPE pour le type de groupe GrouptType, il remplacera la chaîne et l'instruction SQL ressemblera à ceci :

    Select ... from USER_OBJECTS where ... AND OBJECT_TYPE = 'TYPE'

    où TYPE est l'ALIAS réel

13. Facultatif : Entrez une Instruction SQL pour détail, il s'agit d'une instruction SQL qui extrait une liste de chaînes en vue de générer une chaîne de détails avec le préfixe Detail + liste de chaînes. Voir l'exemple indiqué à la section Préfixe Detail.
    Remarque : Le détail généré s'affiche uniquement en cas d'échec du test basé sur une requête, ce qui permet à l'utilisateur d'entrer une instruction SQL pouvant extraire les informations ayant entraîné l'échec du test et pouvant aider à identifier la cause de l'échec.
    Remarque : La chaîne "Detail" est visible dans les résultats d'évaluation de la sécurité en cliquant sur le nom du test d'évaluation et peut être également interrogée via l'attribut Détails des résultats de l'entité Résultats de test.

14. Facultatif : Entrez une instruction SQL Pre-test check. Cette instruction est exécutée avant d'effectuer le test. Si elle renvoie 0, le test n'est pas exécuté. Si le test renvoie 1 ou une erreur, le test est exécuté.
15. Facultatif : Entrez un message "Pre-test fail"). Ce message est inséré dans les résultats d'évaluation si le test n'est pas exécuté en raison de la valeur 0 renvoyée par l'instruction SQL.
16. Facultatif : Dans Bases de données en boucle, entrez une liste de bases de données que le test doit parcourir en boucle. Le test renvoie l'union ou la somme des résultats renvoyés par toutes les bases de données spécifiées. Vous ne pouvez exécuter cette fonction que si le test renvoie une valeur entière et uniquement avec ces types de base de données : Informix, SQL Server, Sybase SE, PostgreSQL et MySQL. L'exécution en boucle s'effectue si la case Indicateur de boucle de base de données est cochée. Il est possible qu'une ou plusieurs bases de données spécifiées soient indisponibles lors de l'exécution du test. Dans ce cas, le test ignore cette base de données et continue son exécution ou s'arrête et émet un message d'échec, selon que la case Ignorer en cas d'erreur soit cochée ou pas.
17. Facultatif : Entrez un préfixe Detail qui apparaîtra au début de la chaîne des détails.

```
Example for SQL Statement for Detail & Detail prefix:
Test that checks for objects with certain grants.
Detail prefix: "Objects found with certain GRANT:"
SQL Statement for Detail: SELECT object FROM....--returning 4 records:
      Obj1
      Obj2
      Obj3
      Obj4
==> Details: Objects found with certain GRANT: Obj1, Obj2, Obj3, Obj4
```

18. Facultatif : Sélectionnez la case à cocher Associer variable de sortie si le texte saisi dans l'instruction SQL est un bloc de procédure qui renverra une valeur devant être associée à une variable Guardium interne qui sera utilisée dans la comparaison avec la valeur indiquée dans le paramètre Compare to.

```
Example (Oracle):
declare
    retval integer := 0;
    strval varchar2(255) := '';
    nver number;
    sver varchar2(255) := '';
begin
    select VERSION
    into sver
    from V$INSTANCE;
    nver := to_number(substr(sver,1,(instr(sver,'.',1,2) - 1)));
    if nver >= 11.1 then
        select VALUE
        into strval
        from V$PARAMETER
        where NAME = 'sec_case_sensitive_logon';
    end if;
    if (nver < 11.1 or strval = 'TRUE') then
        retval := 0;
    else
        retval := 1;
    end if;
    ? := retval;
end;
```

19. Sélectionnez le Type de retour qui sera renvoyé par l'instruction SQL.
20. Sélectionnez l'opérateur qui sera utilisé pour la condition.
21. Entrez une Valeur cible de comparaison qui sera utilisée pour la comparaison avec la valeur renvoyée par l'instruction SQL utilisant l'opérateur de comparaison. C'est cette comparaison qui détermine si le test a réussi ou échoué. Vous pouvez aussi cliquer sur RE (regex) en vue de définir une expression régulière pour la valeur de comparaison.
22. Effectuez l'une des opérations suivantes :
    - Cliquez sur Retour pour annuler les changements et revenir à l'écran précédent.
    - Cliquez sur Appliquer pour sauvegarder le test basé sur une requête.

Résultats

Vous pouvez ajouter ce nouveau test basé sur une requête à une évaluation.

Que faire ensuite

Rubrique parent : Tests d'évaluation des vulnérabilités

Définition d'un test basé sur CAS

Les évaluations des vulnérabilités utilisent le mécanisme CAS pour exécuter des tests au niveau du système d'exploitation sur le serveur de base de données et identifier les vulnérabilités.

Avant de commencer

Pourquoi et quand exécuter cette tâche

Vous pouvez créer un test basé sur CAS en modifiant un test de ce type existant ou en commençant depuis le début et en définissant tous les champs.

Procédure

1. Ouvrez le Générateur d'évaluation en cliquant sur Renforcement > Vulnerability Assessment > Générateur d'évaluation.
2. Dans Tests définis par l'utilisateur, cliquez sur Tests basés sur CAS pour ouvrir le panneau Localiseur de test basé sur CAS.
3. Cliquez sur Nouveau ou sur Modifier pour créer un nouveau test.
4. Entrez un Nom de test unique.
5. Sélectionnez une base de données dans le menu Type de base de données.
6. Sélectionnez une catégorie dans le menu Catégorie.

7. Sélectionnez un niveau de gravité dans le menu Gravité.
8. Facultatif : Entrez une Brève description pour le test.
9. Facultatif : Entrez une Référence externe pour le test.
10. Entrez un Texte de résultat pour réussite qui sera affiché en cas de réussite du test.
11. Entrez un Texte de résultat pour échec qui sera affiché en cas d'échec du test.
12. Entrez un Texte de recommandation pour réussite qui sera affiché en cas de réussite du test.
13. Entrez un Texte de recommandation pour échec qui sera affiché en cas d'échec du test. Texte de recommandation pour échec - Afin d'éviter tout piratage intersite, tout nom figurant dans cette liste, utilisé dans la zone de texte Texte de recommandation pour échec, fera l'objet d'une réécriture : expression, fonction, code JavaScript, script, alerte; eval <img, ContentType
14. Sélectionnez un modèle à utiliser dans le menu Modèle CAS.
15. Sélectionnez un opérateur à utiliser dans le menu opérateur.
16. Entrez une chaîne de recherche qui sera utilisée avec l'opérateur pour la comparaison au résultat renvoyé par le modèle CAS. C'est cette comparaison qui détermine la réussite ou l'échec du test. Vous pouvez également cliquer sur l'icône RE pour définir une expression régulière pour la chaîne de recherche.
17. Facultatif : Sélectionnez la case à cocher Echec en cas de correspondance si le test doit échouer si une correspondance est trouvée avec la chaîne de recherche.
18. Cliquez sur Appliquer pour sauvegarder le test basé sur CAS.

Résultats

Vous pouvez ajouter ce nouveau test basé sur CAS à une évaluation.
Rubrique parent : Tests d'évaluation des vulnérabilités

Evaluations

Les évaluations constituent un groupe de tests qui analysent les infrastructures de base de données à la recherche des vulnérabilités et fournissent une évaluation de l'état de santé de la sécurité des données et des bases de données avec des mesures en temps réel et des historiques de mesures.

- Création d'une évaluation
  Créez une évaluation, ou modifier/cloner une évaluation existante.
- Création d'une exception de test VA
  Utilisez une exception de test pour exclure des membres de groupe spécifiques d'une évaluation de sécurité. Exécutez l'évaluation de sécurité par rapport à ce groupe d'exceptions pour voir si un membre spécifique du groupe a une incidence sur vos résultats d'évaluation. C'est pratique si vous ne souhaitez pas changer les paramètres du groupe ou si vous n'êtes pas autorisé à le faire.
- Comment créer une évaluation de sécurité
  Exécutez des évaluations de la sécurité sur des sources de données sélectionnées afin d'identifier et de traiter les vulnérabilités de manière proactive, d'améliorer les configurations et de renforcer les infrastructures.
- Exécution d'une évaluation
  Pour obtenir les résultats d'une évaluation, elle doit être exécutée dès sa création.
- Affichage des résultats d'évaluation
  Vous pouvez effectuer différentes actions lorsque vous affichez les résultats d'une évaluation.
- Récapitulatif VA
  Le tableau suivant répertorie les informations par test et clé de base de données affichées dans le tableau Récapitulatif VA : résultat de test par identificateur unique, âge d'échec cumulé, date de premier échec/date de dernier échec, date de dernière réussite et date de dernière analyse. Ces informations sont suivies et les utilisateurs peuvent créer un rapport à partir de ces informations.

Rubrique parent : Evaluation et renforcement

Création d'une évaluation

Créez une évaluation, ou modifier/cloner une évaluation existante.

Avant de commencer

Ouvrez le Générateur d'évaluation en cliquant sur Renforcement > Vulnerability Assessment > Générateur d'évaluation.

Pourquoi et quand exécuter cette tâche

Procédure

1. Dans le panneau Localiseur d'évaluation de sécurité, cliquez sur Nouveau pour créer une évaluation de toute pièce. Cliquez sur Cloner ou Modifier pour utiliser une évaluation existante. Cliquer sur l'un de ces boutons ouvre le panneau Localiseur d'évaluation de sécurité. Si vous créez une évaluation de toute pièce, suivez toutes les étapes suivantes. Si vous clonez ou modifiez une évaluation existante, entrez une nouvelle description, puis modifiez uniquement les champs que vous souhaitez changer.
2. Entrez une description unique pour l'évaluation.
3. Ajoutez une source de données en cliquant sur Ajouter une source de données, en entrant les informations requises, puis en cliquant sur Ajouter.
4. Ajoutez des tests à l'évaluation en cliquant sur Configurer tests.
   a. Dans la sous-fenêtre Tests disponibles pour être ajoutés, sélectionnez l'onglet approprié pour la source de données que vous avez ajoutée précédemment.
   b. Sélectionnez les tests que vous souhaitez et cliquez sur Ajouter des sélections pour les ajouter à l'évaluation. Une fois ajoutés, vos sélections s'affichent dans la sous-fenêtre Sélection des tests d'évaluation.
   c. Utilisez la sous-fenêtre Sélection des tests d'évaluation pour gérer les tests de votre évaluation. Supprimez un test sélectionné ou cliquez sur Ajuster cette optimisation de test pour un test afin de personnaliser les paramètres du test.
5. Ajoutez des rôles à l'évaluation.
   Remarque : Vous ne pouvez pas affecter de rôles à une évaluation tant que vous n'avez pas affecté des rôles aux sources de données sur lesquelles elle s'appuie.
6. Cliquez sur Appliquer pour sauvegarder l'évaluation.

   Cliquez sur Support CAS pour fournir les données appropriées pour réaliser une évaluation.

   Vous pouvez également Ajouter des commentaires pour une évaluation afin de documenter ou de consigner les changements apportées à cette évaluation et indiquer pourquoi.

Résultats

Votre nouvelle évaluation est prête à être exécutée.
Rubrique parent : Evaluations

Création d'une exception de test VA

Utilisez une exception de test pour exclure des membres de groupe spécifiques d'une évaluation de sécurité. Exécutez l'évaluation de sécurité par rapport à ce groupe d'exceptions pour voir si un membre spécifique du groupe a une incidence sur vos résultats d'évaluation. C'est pratique si vous ne souhaitez pas changer les paramètres du groupe ou si vous n'êtes pas autorisé à le faire.

Procédure

1. Ouvrez le panneau Générateur de groupe en cliquant sur Configurer > Outils et vues > Générateur de groupe.
2. Sélectionnez Exception tests VA dans le menu Type de groupe pour afficher la liste des groupes d'exceptions prédéfinis.
3. Sélectionnez un groupe dans le menu Modifier groupes existants et cliquez sur Modifier.
4. Ajoutez les membres de groupe que vous souhaitez exclure du test VA.
5. Ouvrez le Générateur d'évaluation en cliquant sur Renforcement > Vulnerability Assessment > Générateur d'évaluation. Sélectionnez une évaluation dans le Localiseur d'évaluation de sécurité et cliquez sur Configurer tests.
6. Recherchez le test auquel vous souhaitez ajouter l'exception et cliquez sur le bouton Ajuster cette optimisation de test pour ce test dans la colonne Optimisation.
7. Sélectionnez votre groupe d'exceptions dans le menu et cliquez sur Sauvegarder. Exécutez à nouveau l'évaluation pour voir si le groupe d'exceptions affecte le résultat du test.
   Remarque : Par défaut, Guardium inclut un groupe d'exceptions appelé "IBM iSeries Profile User Exclusions". Vous pouvez cloner et modifier ce groupe pour répondre à vos besoins.

   Tous les tests de privilèges sur les objets de base de données excluent les schémas système par défaut des groupes Guardium.

Rubrique parent : Evaluations

Comment créer une évaluation de sécurité

Exécutez des évaluations de la sécurité sur des sources de données sélectionnées afin d'identifier et de traiter les vulnérabilités de manière proactive, d'améliorer les configurations et de renforcer les infrastructures.

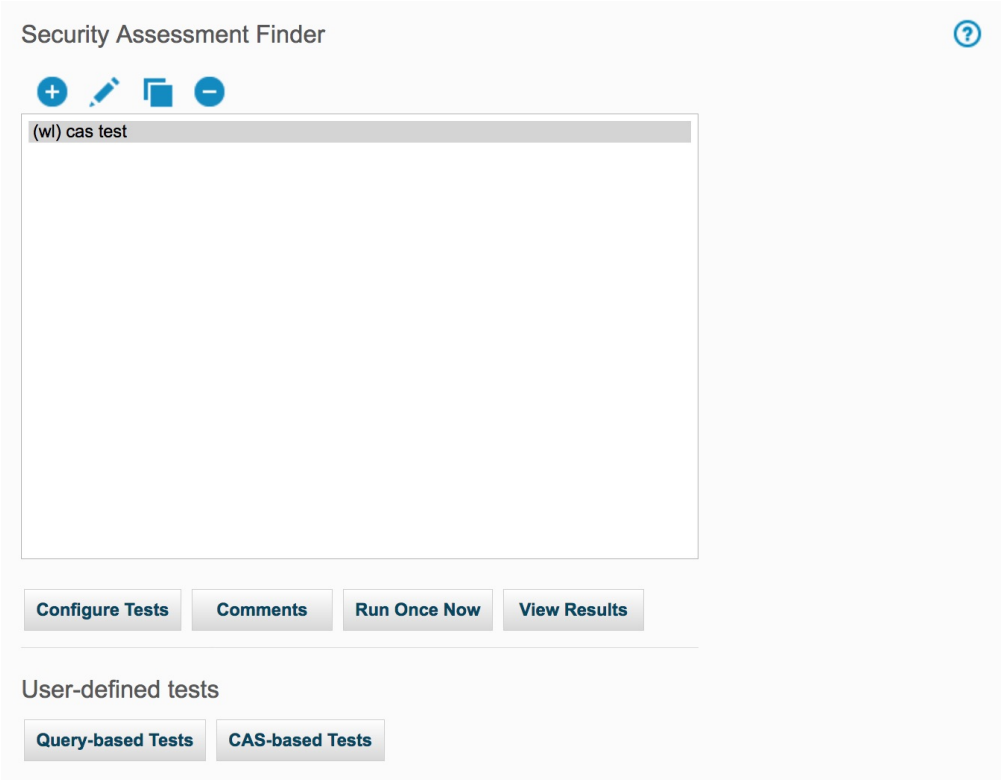
Pourquoi et quand exécuter cette tâche

Voici la procédure de base pour la création d'une évaluation de sécurité :

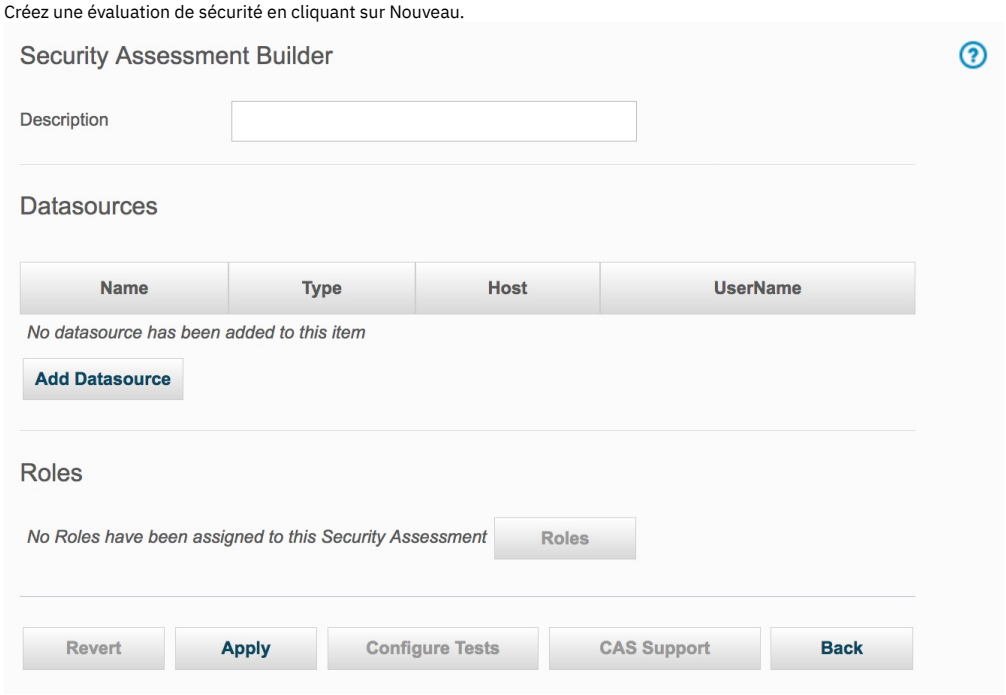
1. Créer une évaluation
2. Ajouter des sources de données à l'évaluation
3. Ajouter des tests à l'évaluation

Procédure

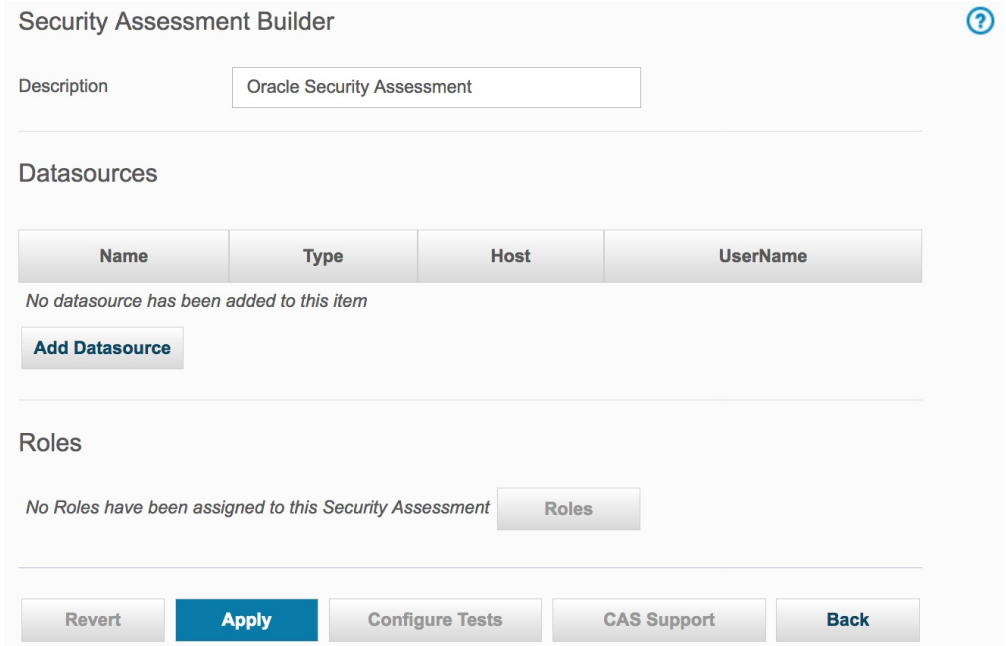
1. Créez ou modifiez une évaluation en ouvrant le Générateur d'évaluation. Ouvrez le Générateur d'évaluation en cliquant sur Renforcement > Vulnerability Assessment > Générateur d'évaluation.



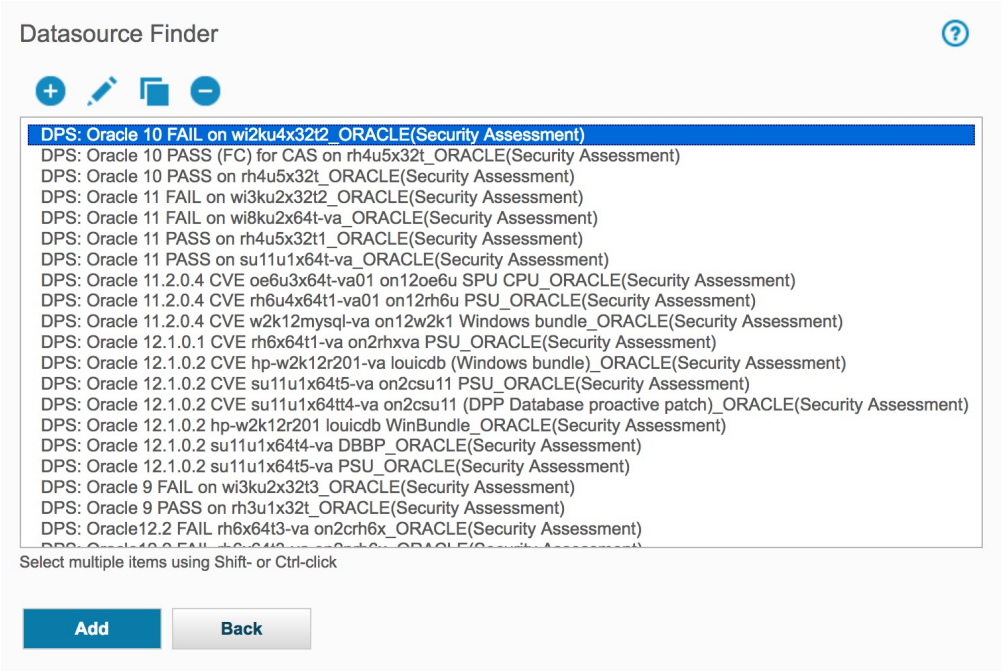
2. Créez une évaluation de sécurité en cliquant sur Nouveau.



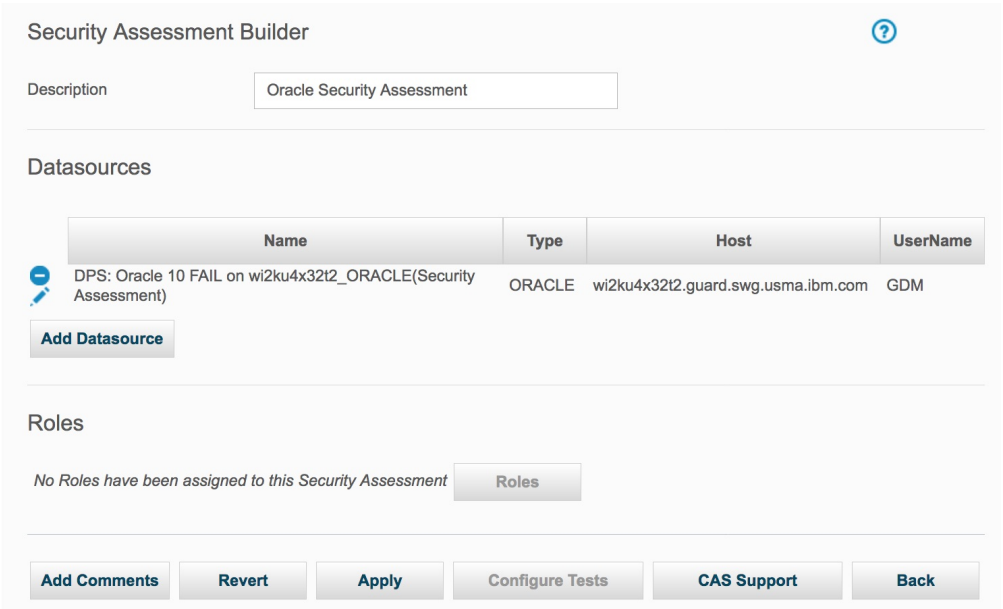
3. Entrez un nom unique pour l'évaluation dans Description et cliquez sur Appliquer pour sauvegarder l'évaluation.



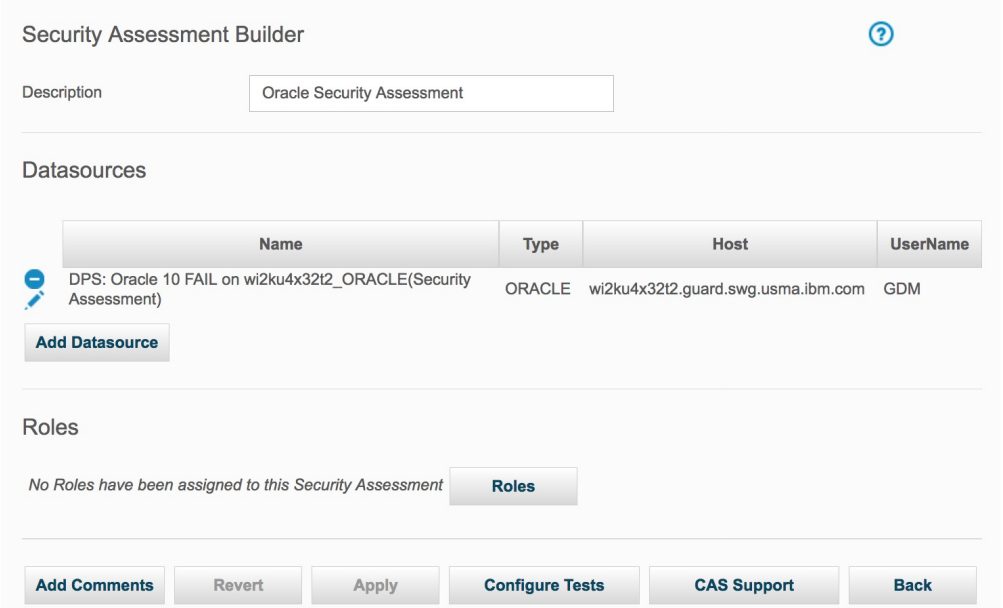
4. Ajoutez une source de données à l'évaluation en cliquant sur Ajouter une source de données. Sélectionnez une source de données dans le Localiseur de source de données et cliquez sur Ajouter. Ajoutez une nouvelle source de données en cliquant sur , en complétant les informations dans la fenêtre Définition de base de données, puis en cliquant sur Appliquer. Voir *Sources de données* pour obtenir de l'aide.



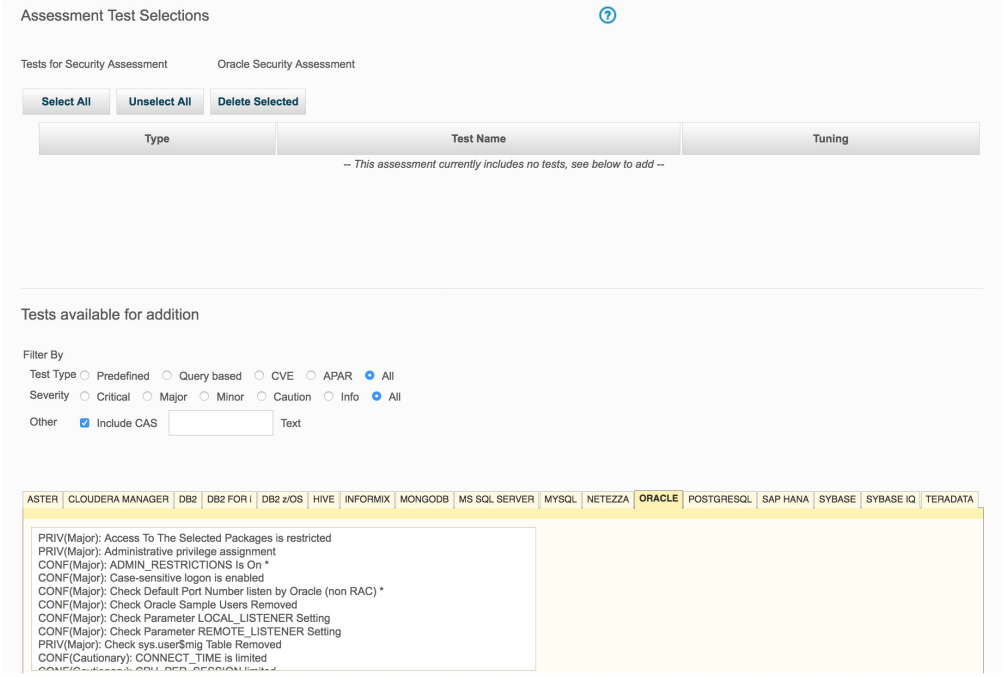
Après avoir cliqué sur le bouton Ajouter, la source de données apparaît dans la section Sources de données du Générateur d'évaluation de sécurité.

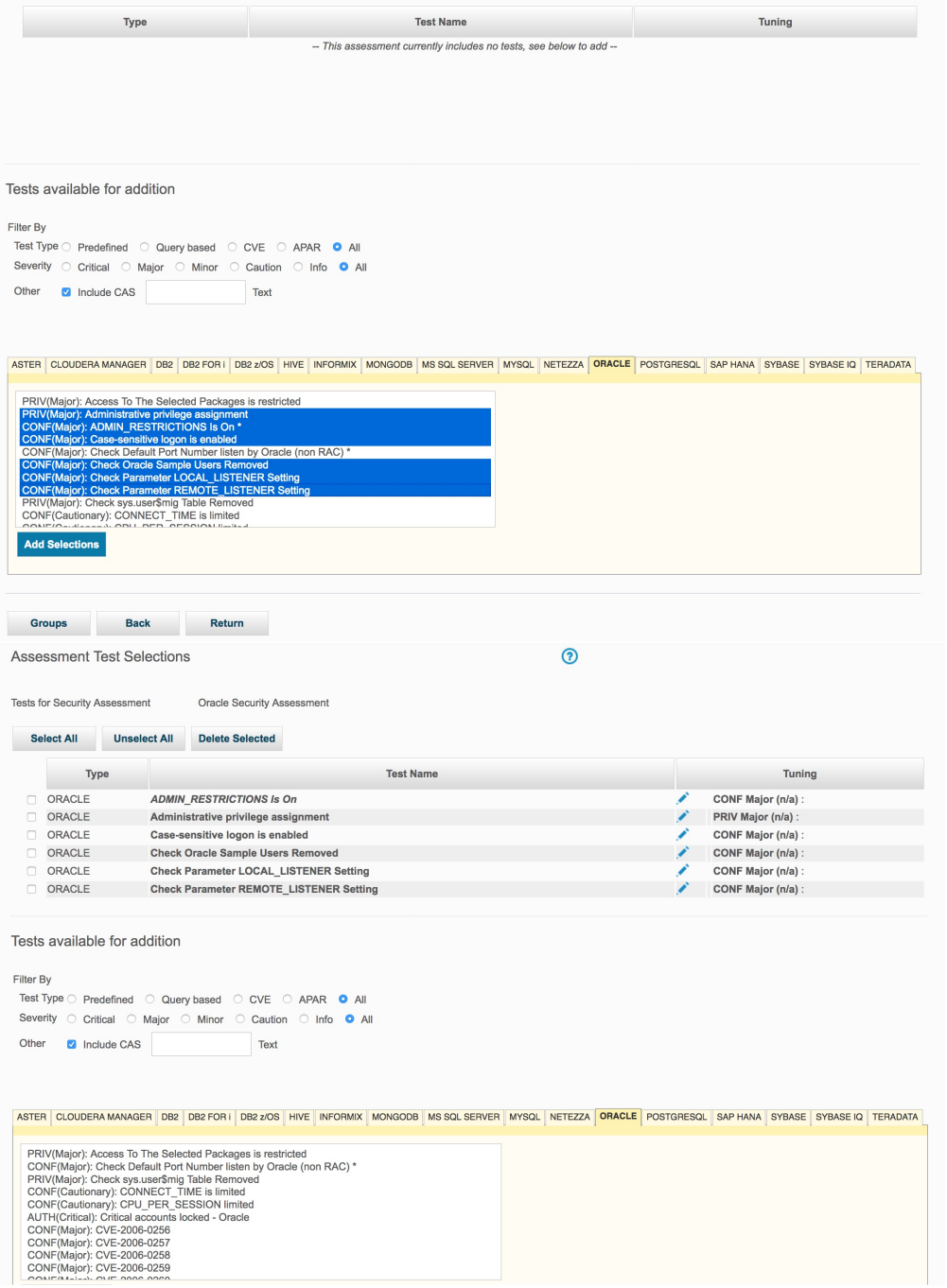


5. Cliquez sur Appliquer pour sauvegarder l'évaluation.



6. Cliquez sur Configurer tests pour ajouter des tests à l'évaluation. Dans le panneau Tests disponibles pour être ajoutés, cliquez sur l'onglet correspondant à la ressource appropriée que vous avez créée, sélectionnez les tests que vous souhaitez ajouter à l'évaluation et cliquez sur Ajouter des sélections. Utilisez les boutons d'option pour filtrer les tests à ajouter. Voir Tests prédéfinis, Tests basés sur une requête, Tests CVE ou Tests APAR pour obtenir de l'aide.





7. Cliquez sur Retour pour revenir au Générateur d'évaluation de sécurité et cliquez sur Rôles pour ajouter des rôles à l'évaluation.
   Remarque : Vous ne pouvez pas affecter de rôles à l'évaluation tant que vous n'avez pas affecté des rôles aux sources de données sur lesquelles s'appuie l'évaluation.
8. Sauvegardez votre évaluation en cliquant sur Appliquer. L'évaluation peut maintenant être exécutée sur les sources de données sélectionnées.

Rubrique parent : Evaluations

Exécution d'une évaluation

Pour obtenir les résultats d'une évaluation, elle doit être exécutée dès sa création.

Les évaluations s'exécutent en mode sérialisé l'une après l'autre. Si l'exécution de plus d'une évaluation est planifiée, les évaluations devront être placées en file d'attente. Cette file d'attente est visible dans le rapport File d'attente de travaux Guardium.

Cliquer sur le bouton Exécuter une fois maintenant fera entrer l'évaluation dans la file d'attente pour une exécution immédiate. Une courte période est nécessaire pour que le travail s'exécute et puisse s'afficher. Voir Affichage des résultats d'évaluation pour plus d'informations sur les résultats d'une évaluation.

Vous pouvez éventuellement définir et planifier un processus automatisé pour l'exécution d'une définition d'évaluation. Le panneau Localiseur de processus d'audit est le point de départ pour la création et la modification d'une planification de processus d'audit. Créez une planification pour exécuter automatiquement vos évaluations en accédant au panneau Localiseur de processus d'audit. Voir Automatisation du flux de travail de conformité pour obtenir de l'aide sur la définition d'un processus d'audit

Rubrique parent : Evaluations

Affichage des résultats d'évaluation

Vous pouvez effectuer différentes actions lorsque vous affichez les résultats d'une évaluation.

Afficher les résultats d'une évaluation

Affichez les résultats d'une évaluation dans le Générateur de rapport. Ouvrez le Générateur de rapport en cliquant sur Renforcement > Rapports > Générateur de rapport et utilisez les filtres pour trouver le rapport que vous recherchez.

Interprétation des résultats d'une évaluation

Une évaluation s'appuie sur plusieurs tests basés sur plusieurs rapports. Les résultats globaux s'affichent dans une fenêtre de navigateur distincte intitulée Résultats d'évaluation de sécurité avec les sections suivantes :

Identité de l'évaluation

Les résultats de l'évaluation identifient :

- le nom de l'évaluation
- la date et l'heure d'exécution de l'évaluation
- la période de l'évaluation
- les adresses IP client et serveur ou les sous-réseaux

Sélection de l'évaluation

Utilisez le menu déroulant pour sélectionner et afficher les résultats antérieurs d'une évaluation. Le dernier résultat est affiché par défaut.

Historique des résultats d'évaluation

La section Historique des résultats d'évaluation affiche le pourcentage de tests effectués sur une période. D'autres recommandations pour augmenter le pourcentage de réussite des tests sont fournies à la section Résultats de test d'évaluation.

Afficher journal

Lorsque vous cliquez sur cette option, le Journal d'exécution s'affiche dans une nouvelle fenêtre qui présente l'exécution du test d'évaluation. Un horodatage, ainsi que des événements, et des messages peuvent faciliter le débogage des erreurs pouvant être à l'origine de l'échec de certains tests.

Récapitulatif des résultats

Un graphique tabulaire récapitule tous les tests qui ont été exécutés dans le cadre de cette évaluation. L'axe des X représente la gravité du test (CRITICAL, MAJOR, MINOR, CAUTION ou INFO). L'axe des Y représente le type de test (Privilège, Authentification, Configuration, Version ou Autre). Dans la grille figure la représentation du nombre de tests à l'état de réussite ou d'échec ou pour lesquels des erreurs ont été détectées lors de leur tentative d'exécution. Ces nombres sont directement liés aux détails des tests d'évaluation indiqués à la section Résultats de test d'évaluation.

Filtrage en cours appliqué

Si vous souhaitez modifier le filtrage appliqué, utilisez les deux options pour filtrer les résultats comme vous le voulez :

Réinitialiser le filtrage - Supprime toutes les options de filtrage sélectionnées via les options Contrôles filtrage/tri.

Contrôles filtrage/tri - Utilisez cette option pour ouvrir les options de filtrage et de tri du rapport. Ces options vous permettent d'effectuer un filtrage par Gravité, Classification de gravité de la source de données, Score (réussite, échec ou erreur) et Type de test (Observé/Type de base de données). L'option de tri vous permet d'effectuer le tri sur des combinaisons de gravité, score et source de données. Cliquez sur Appliquer lorsque vous souhaitez que ces options de filtrage et de tri soient appliquées.

Résultats de test d'évaluation

La section Résultats de test d'évaluation fournit une description détaillée du test effectué, des informations sur la source de données cible et la classification des niveaux de gravité, ainsi que le statut de réussite ou d'échec, la gravité, la référence externe et le motif du statut actuel. Vous pouvez cliquer sur chaque nom de test et filtrer toutes les informations issues du rapport à l'exception des informations concernant ce test particulier. Une fonction à survoler avec la souris dans le champ Motif affiche les recommandations pour aider à résoudre les tests ayant échoué ou comportant des erreurs.

Les résultats d'évaluation comprennent le nombre de tests et le nombre de tests réussis dans chacune de ces catégories :

- Tests CIS
- Tests CVE
- Tests STIG

Ces valeurs sont affichées dans l'afficheur des résultats d'évaluation et disponibles pour la création de rapport dans le domaine des résultats de VA.

Détails de la source de données

Lorsqu'elle est développée, la section Détails de la source de données affiche toutes les sources de données référencées dans l'évaluation, y compris les informations environnementales spécifiques à la source de données.

Informations CVE et CVSS

Des enregistrements CVE et des informations CVSS s'affichent dans l'afficheur des résultats de test d'évaluation.

Vous pouvez cliquer sur les liens de référence (qui s'ouvrent dans une nouvelle fenêtre). Il se peut que l'une ou l'autre de ces sections soient absentes s'il n'y a aucun enregistrement correspondant à un résultat.

Les champs CVSS présentant un intérêt sont :

- Score CVSS
- Complexité des accès
- Impact sur la disponibilité
- Impact sur la confidentialité
- Impact sur l'intégrité
- Authentification
- Fournisseur d'accès
- Source
- Généré le (date et heure)

Utilisation de tests ayant échoué

Si certains tests dans votre évaluation ont un statut d'échec, vous pouvez envisager d'effectuer l'une des actions suivantes :

Ajouter une exception au test
: Cette action entraîne la réussite du test sur une période définie. Par exemple, vous pouvez disposer d'un groupe de serveurs qui font échouer le test qui vérifie que les dernières mises à jour du service disponibles ont été appliquées. Vous ne pouvez pas appliquer les mises à jour pendant la période de maintenance qui a lieu durant le week-end. Vous ne voulez pas que le test échoue jusque-là. Cliquez avec le bouton droit de la souris sur le mot Echec dans le panneau des résultats. Un menu en incrustation Ajouter une exception au test s'affiche. Indiquez une date et une heure de fin pour l'exception en ajoutant éventuellement un commentaire. Le test réussira sur toutes les sources de données, même s'il est effectué avant expiration de l'exception, qu'il soit effectué dans le cadre de cette évaluation ou d'une autre évaluation.

Ajouter des éléments ayant échoué à un groupe d'exceptions
: Lorsqu'un test échoue, vous pouvez afficher des informations supplémentaires en cliquant sur le nom du test. Le nouveau panneau affiche une zone intitulée Détails. Les éléments du test ayant échoué sont affichés après cet intitulé. Si des éléments s'affichent, vous pouvez les ajouter à un groupe d'exceptions pour ce test. Pour cela, cliquez sur l'en-tête Détails : pour ouvrir une nouvelle boîte de dialogue. Cette boîte de dialogue affiche les éléments ayant échoué, avec une case à cocher en regard. Sélectionnez les cases à cocher des éléments que vous souhaitez ajouter au groupe d'exceptions et effacez les autres cases à cocher. Sélectionnez ensuite un groupe. Si un groupe d'exceptions par défaut est défini pour ce test, il apparaît pré-sélectionné dans la boîte de dialogue. Une liste déroulante affiche les autres groupes d'exceptions au test de type VA qui ont été définis. Pour choisir un groupe dans la liste, cliquez sur le bouton d'option en regard de la liste, et choisissez le groupe dans cette liste. Cliquez sur Sauvegarder pour implémenter votre sélection. Pour ajouter des éléments restants à un autre groupe, cliquez à nouveau sur Détails.

Exportation au format PDF ou au format XML SCAP ou AXIS

Vous pouvez générer une version PDF du résultat de l'évaluation en cliquant sur Télécharger PDF.

Utilisez le bouton Télécharger XML pour ouvrir deux options de menu : Télécharger au format XML SCAP et Télécharger au format XML AXIS. Choisissez l'une de ces sélections pour télécharger sur votre poste de travail un fichier XML représentant les résultats d'évaluation affichés. Le fichier peut correspondre au format XML de Security Content Automation Protocol (SCAP) ou d'Apache EXtensible Interaction System (AXIS), utilisé par QRadar.

Rubrique parent : Evaluations

Récapitulatif VA

Le tableau suivant répertorie les informations par test et clé de base de données affichées dans le tableau Récapitulatif VA : résultat de test par identificateur unique, âge d'échec cumulé, date de premier échec/date de dernier échec, date de dernière réussite et date de dernière analyse. Ces informations sont suivies et les utilisateurs peuvent créer un rapport à partir de ces informations.

Récapitulatif VA

La clé peut comporter, en plus des trois éléments d'origine, le nom de la source de données. La valeur par défaut est Hôte, port et Nom d'instance.

Utilisez le suivi du récapitulatif VA dans le générateur de requête pour définir des requêtes et des rapports.

Ce tableau peut être exporté/importé. L'importation de données remplacera les données existantes sur le système Guardium (par clé).

Tableau 1. Récapitulatif VA

Colonne du tableau	Type	Description
VA_SUMMARY_ID	Int	Incrémentation automatique – clé principale
DATA_SOURCE_HASH	Varchar(40)	Hachage de la clé
DB_TYPE	Varchar	Type de base de données
SERVICE_NAME	Varchar	Nom d'instance de la base de données (s'il fait partie de la clé, "N/A" autrement)
DB_PORT	Varchar	Port de la base de données (s'il fait partie de la clé, "N/A" autrement)
DB_HOST	Varchar	Hôte / Adresse IP (s'ils font partie de la clé, "N/A" autrement)
TEST_ID	Int	ID du test
FIRST_EXECUTION	DateTime	Première fois que le test a été exécuté
LAST_EXECUTION	DateTime	Dernière fois que le test a été exécuté
FIRST_FAIL	DateTime	Première fois que le test a échoué sur cette base de données
LAST_FAIL	DateTime	Dernière fois que le test a échoué sur cette base de données

Colonne du tableau	Type	Description
FIRST_PASS	DateTime	Première fois que le test a réussi sur cette base de données
LAST_PASS	DateTime	Dernière fois que le test a réussi sur cette base de données
CURRENT_SCORE	varchar	Réussite/ Echec / Erreur
CURRENT_SCORE_SINCE	Datetime	Date depuis laquelle le test est à l'état en cours
CUMULATIVE_FAIL_AGE	Int	Age d'échec cumulé (en jours)
CUMULATIVE_PASS_AGE	Int	Age de réussite cumulé (en jours)

Les commandes de l'interface CLI sont : store va_test_show_query et show va_test_show_query. Utilisez la commande export va_summary pour exporter ces informations.

Les commandes GuardAPI permettant de changer ou d'afficher la clé sont : grdapi modify_va_summary_key et grdapi reset_va_summary_by_key. La commande GuardAPI à utiliser pour réinitialiser les âges cumulés (à la fois pour la réussite et l'échec), est grdapi reset_va_summary_by_id. Utilisez la commande grdapi export_va_summary pour exporter ces informations.

Un autre paramètre, datasourceName, a été ajouté aux commandes grdapi reset_va_summary_by_key et grdapi modify_va_summary_key.

L'entité VA Summary comporte l'attribut supplémentaire Datasource Name, rempli UNIQUEMENT si le nom de la source de données fait partie de la clé.

Remarque : La commande GrdAPI, modify_va_summary_key, permet à la clé d'être vide si elle est appelée avec l'ensemble des quatre paramètres : useHost, usePort, useServiceName, useDatasourceName, ayant la valeur false. Dans ce cas, lorsque la clé est vide, le calcul du récapitulatif VA est désactivé (aucune donnée récapitulative n'est calculée, mise à jour ou sauvegardée).
Rubrique parent : Evaluations

Changement obligatoire de schéma

Le schéma utilisé pour les tests d'évaluation des vulnérabilités sur IBM DB2 for z/OS a changé dans Guardium, version 9.1. Si vous effectuez une mise à niveau à partir d'une version antérieure à 9.1, vous devez mettre à jour la base de données pour pouvoir continuer à utiliser ces tests.

Pourquoi et quand exécuter cette tâche

Lorsque vous effectuez une mise à niveau de votre système Guardium vers la version 10.x, vous devez créer de nouvelles tables de base de données sur votre serveur de base de données. Ces tables permettent de prendre en charge une nouvelle série de tests, mais vous devez les créer que vous utilisiez ou non ces nouveaux tests.
Dans les versions antérieures, vous avez créé et rempli des tables dans le schéma gdmmonitor :

- GDMMONITOR.OS_GROUP
- GDMMONITOR.OS_USER

Ces tables sont remplacées par des tables dans le schéma CKADBVA :

- CKADBVA.CKA_OS_GROUP
- CKADBVA.CKA_OS_USER

Procédure

1. Installez Guardium 10.x
2. Copiez le fichier create_CKADBVA-schema_tables_zOS.sql du répertoire /var/log/guard/gdmmonitor_scripts sur votre système Guardium vers votre serveur de base de données. Exécutez la commande fileserver sur votre serveur de base de données pour extraire le fichier.
3. Le script contient des instructions qui décrivent la procédure à suivre avant et après l'exécution du script. Lisez ces instructions et exécutez le script.
4. Remplissez les nouvelles tables avec des données semblables à celles stockées dans les anciennes tables.

Résultats

Votre système est désormais configuré pour utiliser les tests d'évaluation des vulnérabilités actuels.

Que faire ensuite

Rubrique parent : Evaluation et renforcement

Evaluation des vulnérabilités RACF

Si vous utilisez IBM DB2 for z/OS, vous pouvez recourir à des test d'évaluation des vulnérabilités pour évaluer les vulnérabilités liées à votre fonction de contrôle d'accès RACF. Vous devez disposer au minimum de la version 9.1 de Guardium pour réaliser des évaluations RACF.

Pourquoi et quand exécuter cette tâche

Evaluez vos privilèges RACF (Resource Access Control Facility) pour savoir s'ils sont octroyés dans la base de données ou s'ils sont externes à la base de données. Les tests, qui comprennent l'évaluation des vulnérabilités RACF, identifient le contrôle d'accès des privilèges sur les objets, des privilèges sur les bases de données et des privilèges système.

Pour utiliser ces tests, vous devez obtenir et installer IBM Security zSecure Audit, version 2.1. Ce produit active les commandes qui sont utilisées dans ces tests pour interagir avec RACF.

Les tests qui examinent les autorisations ne renvoient pas de résultat de type réussite/échec, mais une liste d'utilisateurs autorisés. Des exemples de rapports de ce type comprennent les privilèges sur les tables et les vues octroyés à des bénéficiaires et les privilèges sur les packages octroyés à des bénéficiaires. Dans un environnement important incluant un très grand nombre d'utilisateurs et d'applications, ces rapports génèrent une immense quantité de données. Lorsque vous exécutez ces rapports

dans un environnement de ce type, le processus peut s'exécuter pendant longtemps et consommer de grandes quantités de ressources et il peut en définitive dépasser le temps imparti.

Procédure

1. Mettez à niveau le schéma de base de données utilisé pour prendre en charge Vulnerability Assessment sur votre serveur de base de données.
2. Installez zSecure Audit sur votre serveur de base de données. Utilisez les instructions et les outils fournis avec zSecure Audit pour savoir comment remplir environ 24 tables dans le schéma CKADBVA pour prendre en charge les nouveaux tests zSecure.
3. L'équipe zSecure émettra une modification provisoire de logiciel (PTF) pour permettre à zSecure Audit d'utiliser Guardium Vulnerability Assessment. Récupérez cette PTF et appliquez-la en suivant les instructions qui l'accompagnent.

Résultats

Votre système est désormais configuré pour bénéficier des nouveaux tests zSecure.

Que faire ensuite

Choisissez les nouveaux tests que vous souhaitez utiliser pour évaluer les vulnérabilités de votre fonction de contrôle d'accès RACF. Configurez et exécutez les tests.

Rubrique parent : Evaluation et renforcement

Configuration Auditing System (CAS)

CAS procède au suivi des changements de configuration et génère des rapports. Les données sont disponibles sur le système Guardium et peuvent être utilisées pour les rapports et les alertes.

Présentation de Configuration Auditing System (CAS)

Les bases de données peuvent être affectées par des changements apportés à l'environnement serveur. Par exemple, en changeant les fichiers de configuration, les variables d'environnement ou de registre, ou d'autres composants de base de données ou de système d'exploitation, y compris des fichiers exécutables ou des scripts utilisés par le système de gestion de base de données ou le système d'exploitation. CAS procède au suivi de ces changements et génère des rapports. Les données sont disponibles sur le système Guardium et peuvent être utilisées pour les rapports et les alertes.

Remarque : Vulnerability Assessment (VA) et Configuration Auditing System (CAS) ne sont pris en charge qu'en anglais.

Agent CAS

CAS est un agent installé sur le serveur de base de données qui génère des rapports sur le système Guardium dès qu'une entité surveillée a changé, soit au niveau de son contenu, de sa propriété ou de ses droits d'accès. Vous installez un client CAS sur le système de serveur de base de données à l'aide du même utilitaire employé pour l'installation de S-TAP. CAS partage les informations de configuration avec S-TAP, bien que les composants s'exécutent indépendamment les uns des autres. Une fois le client CAS installé sur l'hôte, vous configurez les fonctions d'audit des changements à partir du portail Guardium.

Serveur CAS

Le serveur CAS est un composant de Guardium et s'exécute sur le système Guardium. Il s'exécute comme un processus autonome, indépendamment du serveur d'applications Tomcat. Il est contrôlé via le fichier innittab.

Le serveur CAS est configuré pour n'utiliser que quelques-uns des processeurs disponibles sur le système Guardium. Le nombre de processeurs utilisés par CAS est déterminé à l'aide du paramètre *divide_num_of_processors_by*. Ce paramètre est stocké dans le fichier cas.server.config.properties et sa valeur par défaut est 2. Le nombre de processeurs disponibles sur le système Guardium est divisé par cette valeur. Lorsque CAS utilise 100 % de l'UC sur les processeurs attribués, cela permet de garantir la disponibilité des processeurs restants pour d'autres applications.

Authentification du serveur CAS

En plus de la sécurité de base fournie par SSL, Guardium offre un support d'authentification pour le serveur CAS sur le client CAS qui s'exécute sur le serveur de base de données. Cela garantit que le client CAS communique uniquement avec le serveur CAS de Guardium. Les connexions non authentifiées et les non concordances de noms communs (CN) seront consignées dans le fichier journal de CAS.

Lorsque cette authentification est configurée, au démarrage du serveur CAS, un certificat signé ainsi qu'une clé privée sont chargés et sont affectés à un socket de serveur sur lequel les connexions sont acceptées. Sur la base de données côté serveur, le client CAS prend en charge les modes de connexion suivants :

1. Connexion non sécurisée (use_tls='0')
2. Connexion sécurisée sans authentification (use_tls ='1', guardium_ca_path=NULL). Ce mode force l'utilisation de SSL comme moyen de communication avec le serveur CAS (c'est-à-dire l'utilisation de SSL sans authentification de serveur).
3. Connexion sécurisée avec authentification de serveur (use_tls ='1', guardium_ca_path=<emplacement de la clé publique>). La clé publique est utilisée par le client CAS pour authentifier le serveur CAS. La clé publique (ca.cert.pem) sera située dans <rép_installation>/etc/pki/certs/trusted.

   ca.cert.pem - est un fichier contenant des certificats d'autorités de certification racine (qui sont autosignés). Ils sont l'équivalent des certificats de l'autorité de certification (CA) approuvés pour les navigateurs, tels que Verisign, etc.

   Tous les certificats gmachine sont émis/signés par l'autorité de certification racine - c'est ainsi qu'ils sont validés et que la chaîne d'approbation est établie.

   Il est possible de définir guardium_ca_path avec le chemin complet comprenant le nom de fichier de clé publique effectif, ou juste avec le nom du répertoire (<rép_installation>/etc/pki/certs/trusted), dans lequel toutes les clés publiques qui s'y trouvent seront utilisées afin d'authentifier le serveur. Si guardium_ca_path est défini avec un fichier ou un répertoire qui ne contient pas la clé publique, la tentative de connexion échouera.

4. Connexion sécurisée avec authentification de serveur et vérification de nom commun. Ce mode fournit une vérification supplémentaire où le nom commun (CN) du certificat provenant du serveur est comparé à celui défini dans le paramètre sqlguard_cert_cn. Si sqlguard_cert_cn a la valeur NULL ou s'il est vide, cette vérification est désactivée. Autrement, il doit être défini avec le même nom commun (CN) utilisé par le certificat autosigné de Guardium ('gmachine').

Remarque : Tous les paramètres mentionnés proviennent du fichier guard_tap.ini.

Utilisation de SSL avec CAS

Vous pouvez configurer l'agent CAS afin d'utiliser une connexion Secure Sockets Layer (SSL) pour envoyer des données au serveur CAS. Le serveur CAS installé avec la version 10.1 est conforme aux exigences de la norme US Federal Information Processing Standard 140-2 (FIPS 140-2). Seul un agent CAS conforme à la norme FIPS peut communiquer avec ce serveur CAS à l'aide de SSL. Si vous voulez utiliser cette approche, vous devez mettre à niveau vos agents CAS à la version livrée avec ce correctif. Vous devez également disposer d'IBM Java installé sur le serveur sur lequel s'exécute l'agent CAS et l'agent CAS doit être configuré pour l'utiliser. Pour recourir à la communication FIPS, l'authentification basée sur des certificats doit être utilisée.

Si vous tentez d'utiliser un ancien agent CAS pour communiquer avec le serveur CAS mis à jour avec SSL, vous verrez ce message dans le fichier journal sur le système d'agent CAS :

```
javax.net.ssl.SSLHandshakeException: Received fatal alert: handshake_failure
```

Vous pourrez également voir ce message dans le fichier journal de CAS sur le système Guardium

```
javax.net.ssl.SSLHandshakeException: Client requested protocol SSLv3 not
enabled or not supported
```

Pour utiliser une autre connexion que SSL entre les agents CAS et le serveur CAS, vous pouvez continuer à utiliser vos agents CAS existants.

Jeu de modèles

Un jeu de modèles CAS contient une liste de modèles d'élément, regroupés ensemble, qui partagent un objectif commun, tel que la surveillance d'un type particulier de base de données (Oracle sur Unix, par exemple), et un des deux types suivants :

- Operating System Only (Unix ou Windows)
- Database (Unix-Oracle, Windows-Oracle, Unix-Db2, Windows-Db2, etc.)

Un jeu de modèles de base de données est toujours spécifique au type de base de données et au type de système d'exploitation.

Elément de modèle CAS

Définition ou ensemble d'attributs d'une tâche surveillée sur une entité surveillée (Monitored Entity) unique. Les utilisateurs peuvent définir de nouveaux tests CAS en créant des modèles CAS ou utiliser des modèles CAS prédéfinis pouvant être modifiés.

Un élément de modèle (template item) est un fichier ou un modèle de fichier spécifique, une variable d'environnement ou de registre, la sortie d'un script de système d'exploitation ou d'un script SQL, ou la liste des utilisateurs connectés. L'état de ces éléments est répercuté par les données brutes, c'est-à-dire le contenu d'un fichier ou la valeur d'une variable de registre. CAS détecte les changements en vérifiant la taille des données brutes ou en calculant une somme de contrôle des données brutes. Pour les fichiers, CAS peut également rechercher les changements au niveau du système, tels que la propriété, les droits d'accès et le chemin d'accès à un fichier.

Dans un environnement fédéré où toutes les unités (collecteurs et regroupeurs) sont gérées par un gestionnaire, tous les modèles sont partagés par les collecteurs et les regroupeurs et les données CAS peuvent être utilisées dans la production de rapports ou les évaluations de la sécurité. Lorsque le collecteur et le regroupeur (ou l'hôte sur lequel les données archivées sont restaurées) ne fait pas partie du même cluster de gestion, les modèles ne sont pas partagés et par conséquent, les données CAS ne peuvent pas être utilisées par les évaluations de vulnérabilités même si elles sont présentes. Pour y remédier, utilisez l'exportation/importation des définitions pour copier les modèles du collecteur vers le regroupeur (ou la cible de restauration).

Remarque : Vous ne devez pas demander à CAS de surveiller plus de 10 000 fichiers par client.
Remarque : Il n'est pas recommandé de configurer CAS pour traiter plus de 1 000 fichiers surveillés par heure.

Entité surveillée

L'entité réelle surveillée peut être un fichier (son contenu et ses propriétés), la valeur d'une variable d'environnement ou d'une variable de registre Windows, la sortie d'une commande ou d'un script de système d'exploitation ou la sortie d'une instruction SQL.

Instance CAS

Application d'un jeu de modèles CAS sur un hôte spécifique (création d'une instance de ce jeu de modèles et application de cette instance sur un hôte spécifique)

Configuration CAS

Une configuration CAS définit une ou plusieurs instances CAS, chacune identifiant un jeu de modèles à utiliser pour surveiller un ensemble d'éléments sur cet hôte.

Jeux de modèles par défaut

Pour chaque type de système d'exploitation et de base de données pris en charge, Guardium fournit un jeu de modèles par défaut préconfiguré pour surveiller toute une variété de bases de données sur des plateformes Unix ou Windows. Un jeu de modèles par défaut sera utilisé comme point de départ d'un nouveau jeu de modèles défini pour ce type de jeu de modèles. Un type de jeu de modèles est soit un système d'exploitation seul (Unix ou Windows) ou un système de gestion de base de données (Db2, Informix, Oracle, etc.), qui est toujours qualifié par un type de système d'exploitation (par exemple, UNIX-Oracle ou Windows-Oracle. Bon nombre de jeux de modèles par défaut préconfigurés sont utilisés dans l'application Vulnerability Assessments de Guardium, où, par exemple, les paramètres connus, les emplacements des fichiers et les droits d'accès aux fichiers peuvent être vérifiés.

Vous ne pouvez pas modifier un jeu de modèles par défaut Guardium, mais vous pouvez le cloner et modifier la version clonée. Chaque jeu de modèles par défaut de Guardium définit un ensemble d'éléments à surveiller. Veillez à bien comprendre la fonction et l'utilisation de chaque élément surveillé par ce jeu de modèles par défaut et à utiliser les éléments adaptés à votre environnement. Après avoir défini votre propre jeu de modèles, vous pouvez le désigner comme valeur par défaut pour ce type de jeu de modèles. Après cette opération, tous les nouveaux jeux de modèles définis pour ce type de système d'exploitation et de base de données seront définis avec votre nouveau jeu de modèles par défaut comme point de départ. Le jeu de modèles par défaut de Guardium correspondant à ce type ne sera pas retiré. Il restera défini mais ne sera pas marqué en tant que valeur par défaut.

Justification de la création de jeux de modèles pour répondre à des configurations de base de données spécifiques

Bien que Guardium fournissent des jeux de modèles CAS pour chaque type de base de données, la grande variété des configurations de base de données possibles permet de personnaliser les jeux de modèles prédéfinis ou d'en créer de nouveaux pour répondre à tous vos besoins dans un environnement de production (notamment

en matière de logiciels de base de données et d'emplacements des fichiers de données). Vous devez envisager de créer d'autres modèles si vous voulez que CAS surveille la propriété, les droits d'accès et les changements apportés à vos fichiers de base de données.

Par exemple, le jeu de modèles prédéfini CAS pour Oracle contient, entre autres, les modèles suivants :

- $ORACLE_HOME/oradata/../.*dbf
- $ORACLE_HOME/oradata/../.*ctl
- $ORACLE_HOME/oradata/../.*log
- $ORACLE_HOME/../init.*.ora

Comme vous pouvez le voir, ces modèles de masque de fichiers commencent tous par la même racine, $ORACLE_HOME (REMARQUE : Il ne s'agit pas forcément de la variable d'environnement $ORACLE_HOME définie sur votre serveur de base de données. CAS utilise de préférence le champ de source de données "Database Instance Directory" comme valeur pour $ORACLE_HOME).

Il se peut que dans un environnement de production, vos fichiers de données Oracle ne soient pas dans la même arborescence de répertoires, ou même sur la même unité, que vos fichiers journaux et que vos fichiers de configuration Oracle se trouvent encore à un autre emplacement.

Vous pouvez créer d'autres modèles CAS en utilisant des chemins absolus pour permettre à CAS de rechercher et de surveiller tous vos fichiers Oracle, par exemple :

- /u01/oradata/mydb/*.dbf
- /u02/oradata/mydb/*.dbf
- /u03/oradata/mydb/*.dbf
- /u01/oradata/mydb/*.ctl
- /u02/oradata/mydb/*.ctl
- /u03/oradata/mydb/*.ctl
- /home/oracle11/admin/mydb/bdump/*.log
- /home/oracle11/product/11.1/db_1/dbs/init*.ora

Vous pouvez même utiliser des variables d'environnement supplémentaires définies dans le compte de votre instance Oracle. Par exemple, si les variables $ORA_DATA1, $ORA_DATA2 et $ORA_SOFT sont définies, vous pouvez utiliser :

- $ORA_DATA1/mydb/*.dbf
- $ORA_DATA2/mydb/*.dbf
- $ORA_DATA1/mydb/*.ctl
- $ORA_DATA2/mydb/*.ctl
- $ORA_SOFT/admin/mydb/bdump/*.log
- $ORA_SOFT/product/11.1/db_1/dbs/init*.ora

Approvisionnement de fichiers à partir d'emplacements différents

Les modèles CAS supposent que certains fichiers, par exemple les profils utilisateur se trouvent à certains emplacements. Vous pouvez configurer CAS pour rechercher ces fichiers à d'autres emplacements que vous spécifiez en utilisant une expression régulière. Pour utiliser cette fonction, ajoutez le paramètre user_profile_files dans le fichier cas.client.config.properties qui se trouve dans le répertoire config. Le format de chaque entrée est

```
identifying_string=liste de fichiers séparés par des virgules
```

Par exemple, supposons que vous voulez trouver des fichiers .profile dans le répertoire de base d'un utilisateur Db2. Pour cet exemple, il est supposé que les noms de tous les répertoires de base comprennent la chaîne "db2". Ajoutez cette ligne dans le fichier de propriétés :

```
user_profile_files=.*db2.*=.profile
```

Si vous devez spécifier plusieurs masques, utilisez le symbole barre (|) pour les séparer. Pour ajouter les profils de vos utilisateurs mysql à cette entrée, remplacez l'exemple précédent par ceci :

```
user_profile_files=.*db2.*=.profile|.*mysql.*=.profile
```

- Démarrage et reprise en ligne CAS
  Plusieurs paramètres de reprise en ligne et de connexion peuvent être modifiés via la fonction S-TAP Control Change Auditing.
- Modèles CAS
  Guardium fournit un jeu de modèles CAS, un pour chaque type de référentiel de données.
- Utilisation des modèles CAS
  Cette section décrit comment gérer les modèles CAS
- Hôtes CAS
  Une configuration d'hôte Configuration Auditing System (CAS) définit une ou plusieurs instances CAS.
- Production de rapports CAS
  Cette section présente la production de rapports de Configuration Auditing System (CAS).
- Statut CAS
  Ouvrez le panneau Statut du système d'audit de configuration en cliquant sur Gestion > Surveillance des changements > Statut CAS

Rubrique parent : Evaluation et renforcement

Démarrage et reprise en ligne CAS

Plusieurs paramètres de reprise en ligne et de connexion peuvent être modifiés via la fonction S-TAP Control Change Auditing.

Lorsque le client CAS démarre sur l'hôte, il recherche un fichier de point de contrôle qu'il a pu écrire sur le système. Ce fichier indique à CAS ce qu'il effectuait au cours de sa dernière exécution. CAS se connecte ensuite à son système Guardium. S'il a trouvé un fichier de point de contrôle, CAS demande au système Guardium de vérifier la version de son affectation de surveillance par rapport à ce qui est stocké dans la base de données Guardium. Lorsque le client CAS et le système Guardium ont été déconnectés, l'affectation a pu changer. Lorsque les différences sont résolues, CAS reprend la surveillance. Si CAS ne trouve pas de fichier de point de contrôle, il demande au système Guardium ce qu'il doit faire. Si le système Guardium trouve l'hôte CAS dans sa base de données, les jeux de modèles associés sont envoyés au client CAS, développés en éléments surveillés et la surveillance peut commencer. S'il ne trouve pas l'hôte CAS dans sa base de données, le système Guardium l'ajoute dans la base de données et envoie le jeu de modèles par défaut pour le système d'exploitation hôte CAS.

En cas de perte de connectivité entre le client CAS et le système Guardium, le client CAS et le système Guardium peuvent mettre jusqu'à 5 minutes (temps d'attente d'un client CAS pour recevoir un message du système Guardium) pour découvrir que le contact a été perdu avec le système Guardium principal, mais ce temps d'attente peut être plus court si l'erreur de communication est détectée.

En cas de perte de connexion du client CAS au système Guardium, ou si aucune connexion initiale ne peut être établie, le client ouvre un fichier de reprise en ligne et commence à écrire les messages qu'il était censé envoyer au système Guardium, dans le fichier de reprise en ligne. Le chemin d'accès à ce fichier se trouve dans guard_tap.ini avec le nom cas_fail_over_file. Une fois la communication rétablie, le client CAS s'arrête et redémarre, envoie tous les messages stockés dans le fichier de reprise en ligne au système Guardium et supprime le fichier. Si le client CAS a été incapable d'établir la connexion initiale, il utilise le fichier de point de contrôle pour déterminer ce qu'il y a à surveiller et continue les opérations qui étaient en cours avant l'échec de la communication.

Lorsque la communication est perdue, le client démarre également une unité d'exécution qui tente régulièrement de se reconnecter au système Guardium principal. Le nombre de tentatives de reconnexion de CAS et la durée moyenne entre deux tentatives de reconnexion sont des paramètres configurables. Les tentatives de reconnexion s'effectuent dans un délai défini dans le fichier guard_tap.ini avec le nom cas_server_failover_delay. Une fois ce délai échu, le client essaie également de se connecter à un serveur secondaire identifié dans guard_tap.ini. Les serveurs secondaires seront essayés dans l'ordre de la valeur de l'attribut principal répertorié dans les sections SQL_Guard de guard_tap.ini. Lorsque le serveur principal est différent de 1, il s'agit d'un serveur secondaire. Lorsque le client est connecté à un serveur secondaire, il réitère les tentatives de reconnexion au serveur principal.

Si le nombre limite de tentatives de connexion est atteint, le client CAS n'essaie plus de se reconnecter mais continue à écrire des données dans un fichier de reprise en ligne. Pour limiter l'espace disque nécessaire sur le serveur de base de données, il existe en fait deux fichiers de reprise en ligne. CAS écrit dans un fichier jusqu'à ce qu'il atteigne la taille maximale du fichier de reprise en ligne (qui est configurable), puis bascule sur l'autre, écrasant toutes données précédentes figurant dans ce fichier. La taille par défaut du fichier de reprise en ligne est de 50 Mo (pour chaque fichier).

Vous pouvez indiquer un ou plusieurs systèmes Guardium secondaires lors de la configuration du client CAS. En mode de reprise en ligne, CAS tente uniquement de se reconnecter au serveur principal jusqu'au nombre de fois indiqué par le paramètre cas_server_failover_delay dans le fichier guard_tap.ini. Une fois cette limite atteinte, CAS essaie de se connecter à l'un des serveurs secondaires, ainsi qu'au serveur principal (qui est toujours le premier serveur utilisé lors d'une tentative de reconnexion). Lorsqu'il est connecté à un serveur secondaire, CAS réitère les tentatives de reconnexion au serveur principal.

Les changements apportés à la configuration du client CAS ne peuvent s'effectuer qu'à partir du serveur principal et uniquement lorsque l'hôte est en ligne. Dès que la configuration du client CAS est changée sur le serveur principal et que le système Guardium est en mode de configuration autonome, un fichier d'exportation est sauvegardé sur l'hôte. Si le client CAS se connecte à un serveur secondaire, le fichier d'exportation sauvegardé est importé de l'hôte vers le serveur secondaire.

Il n'est pas nécessaire de gérer les configurations séparément à la fois sur le serveur principal et sur le serveur secondaire. Toutefois, si sur le serveur principal, les paramètres d'un élément surveillé individuel ont changé par rapport à ceux définis dans le modèle, ces changements ne seront pas transférés sur le serveur secondaire. Par exemple, même si l'intervalle de test sur un fichier particulier est passé de la valeur par défaut du modèle de 1 h à 10 mn, l'intervalle de test sur le serveur secondaire sera toujours de 1 h. En fait, les éléments surveillés sont régénérés à partir des modèles de la configuration importée. Le délai avant la recherche des serveurs secondaires est basé directement sur la durée plutôt que sur la taille du fichier de reprise en ligne. Le délai est défini avec le paramètre cas_server_failover_delay dans le fichier guard_tap.ini et sa valeur par défaut est de 60 minutes.

Plusieurs paramètres de reprise en ligne et de connexion peuvent être modifiés via la fonction S-TAP Control Change Auditing.

Comme avec S-TAP, les problèmes de connectivité CAS génèrent des exceptions sur le système Guardium, de sorte que des alertes puissent être émises dès que le problème est détecté.

Configuration et gestion des serveurs secondaires

Dans le fichier de configuration S-TAP/CAS sur le système de serveur de base de données, un ou plusieurs serveurs secondaires Guardium peuvent être définis. Si le serveur Guardium principal devient indisponible, CAS sur ce système de serveur de base de données se connectera à un système Guardium secondaire (comme indiqué précédemment, voir Démarrage et reprise en ligne).

Règles de reprise en ligne

Règle N°	Système Guardium	Bascule sur	Valide
1	autonome	autonome	Oui
2	géré	géré (même gestionnaire)	Oui
3	géré	géré (autre gestionnaire)	Non
4	géré	autonome	Non
5	autonome	géré	Non

Limites de la reprise en ligne CAS

1. Les instances de CAS ne seront pas relocalisées sur le système Guardium de reprise en ligne lorsque le système Guardium source est une unité gérée et que le système Guardium cible est soit :
   - un système Guardium autonome
   - une unité gérée dont la gestion est assurée par un autre gestionnaire
2. L'option d'importation/exportation de CAS sera limitée uniquement au gestionnaire et aux machines autonomes.

Exportation d'hôtes CAS

1. Cliquez sur Gestion > Agrégation & Archive > Exporter pour ouvrir le panneau Exportation de définitions. Sélectionnez Hôtes CAS dans le menu Type, sélectionnez les définitions à exporter dans le menu Définitions à exporter et cliquez sur Exporter
2. Un fichier nommé exp_<date>_<heure>.sql est sauvegardé sur votre système. Ce fichier contient les définitions de tous les hôtes CAS sélectionnés, ainsi que les définitions des jeux de modèles utilisés par ces hôtes.

Importation d'hôtes CAS

1. Cliquez sur Gestion > Agrégation & Archive > Importer pour ouvrir le panneau Importation de définitions.
2. Utilisez les boutons Parcourir et Télécharger pour sélectionner les fichiers et les télécharger, puis sélectionnez la définition dans la sous-fenêtre Importer les définitions téléchargées.

3. Cliquez sur Importer ce jeu de définitions pour importer la définition.
4. Confirmez l'action sélectionnée (ou pas).
   Remarque : Une opération d'importation n'écrase pas une définition existante. Si vous tentez d'importer une définition avec le même nom qu'une définition existante, vous êtes averti que l'élément n'a pas été remplacé. Pour écraser une définition existante avec une définition importée, vous devez supprimer la définition existante avant d'effectuer l'opération d'importation.

Gestion des serveurs secondaires pour un hôte CAS

Les configurations CAS peuvent également être gérées en utilisant des opérations d'importation et d'exportation. Comme l'opération d'importation ne remplace pas une définition existante, sur chaque serveur secondaire, vous devez supprimer l'ancienne définition d'hôte CAS avant d'importer la nouvelle.

Assurez-vous d'effectuer cette procédure uniquement lorsque l'hôte CAS sélectionné est connecté à son serveur principal.

1. Exportez la définition de l'hôte CAS (voir la section précédente).
2. Sur chaque serveur secondaire :
   - Supprimez l'ancienne définition d'hôte CAS que vous souhaitez remplacer.
   - Importez les définitions qui avaient été exportées du serveur principal (voir la section précédente Importation d'hôtes CAS).

Installation d'un client CAS

En principe, l'agent du client CAS est installé avec l'agent S-TAP . Il peut être installé ultérieurement sous Windows à partir d'un DVD d'installation, ou sous Unix en exécutant le script d'installation install_cas.sh, qui se trouve dans le répertoire d'installation S-TAP, qui est par défaut : /usr/local/guardium/guard_stap.

Paramètre ignore-change-alerts du client CAS

L'agent du client CAS peut éviter d'envoyer des notifications de changements au serveur CAS en fonction d'un paramètre prédéfini.

L'agent du client CAS va maintenant rechercher un nouveau paramètre ignore_change_alerts dans son fichier de configuration cas.client.config.properties.

Si le paramètre est introuvable ou s'il n'est pas défini, le client CAS fonctionnera sans changements et la fonctionnalité Ignore change alerts ne sera pas activée (par exemple, le client CAS générera des alertes à chaque changement du fichier).

Si le nouveau paramètre est défini, l'agent du client CAS ignore l'envoi des notifications concernant les changements en fonction des types de changement (change-types) indiqués dans la valeur du paramètre.

Les valeurs possibles de types de changement sont :

PERMISSION, SIZE, OWNER, GROUP, TIMESTAMP

Pour ignorer plusieurs types de changement, vous pouvez délimiter la concaténation en indiquant + pour un type de changement indiqué.

Par exemple :

Pour éviter l'envoi de notification relative à des changement de propriétaire (OWNER) et de groupe (GROUP), configurez le paramètre comme suit :

ignore_change_alerts=OWNER+GROUP

Remarque : Dans l'installation initiale ou lorsque vous définissez un nouveau modèle, la PREMIERE analyse des fichiers sera effectuée et ces fichiers apparaîtront dans le rapport des changements CAS quelles que soient les valeurs du paramètre Ignore change alerts.

Correction d'un nom d'hôte non IP

Si l'utilisateur installe l'agent CAS avec un paramètre erroné tap_ip, guard_tap.ini param ou CAS_TAP_IP (paramètre GIM), les sources de données Windows définies pour cet hôte peuvent s'avérer inexploitables (si elles sont utilisées pour une activité qui nécessite l'accès à la base de données distante).

Si ce scénario se produit, l'utilisateur devra supprimer la source de données et remplacer le paramètre tap_ip par le nom d'hôte ou l'adresse IP valide du serveur de base de données.

Rubrique parent : Configuration Auditing System (CAS)

Modèles CAS

Guardium fournit un jeu de modèles CAS, un pour chaque type de référentiel de données.

Modèles CAS - Db2

Script de système d'exploitation

Désigne un script de système d'exploitation à exécuter. Il doit commencer par la variable $SCRIPTS, qui se rapporte au répertoire scripts situé sous le répertoire de base CAS et identifier le script à exécuter, par exemple, `$HOME/ db2_spm_log_path_group_test.sh`". Bien entendu, le script même doit résider dans le répertoire CAS $SCRIPTS. La sortie du script est stockée dans la base de données Guardium pour être utilisée par les évaluations de la sécurité. Il peut s'agir d'un script shell ou d'un script de commandes, ou d'un ensemble de commandes pouvant être saisies sur la ligne de commande. Etant donné la nature changeante de l'analyse syntaxique de Java, il est suggéré que les commandes (à l'exception des plus simples) soient insérées dans un script au lieu d'être exécutées directement. Sous Unix, le script est exécuté dans l'environnement de l'utilisateur du système d'exploitation indiqué. Trois variables d'environnement seront définies pour l'environnement d'exécution. L'utilisateur pourra les utiliser dans l'écriture des scripts : $UCAS est le nom d'utilisateur de la base de données, $PCAS est le mot de passe de la base de données et $ICAS est le nom d'instance de la base de données. Pour Windows, ces trois valeurs seront ajoutées pour constituer les trois derniers arguments dans l'exécution du fichier de commandes. Par exemple, si vous disposez d'un modèle Script de système d'exploitation `%SCRIPTS%\MyScript.bat my-arg1 my-arg2`, les variables %3, %4 et %5 correspondent respectivement au nom d'utilisateur, au mot de passe et au nom d'instance de la base de données.

Fichier

Désigne un fichier dont le suivi et la surveillance seront assurés par les évaluations de la sécurité. Le chemin d'accès au fichier peut être absolu ou relatif à la variable $INSTHOME. Définissez la valeur de la variable $INSTHOME dans la zone Répertoire d'instance de base de données dans le panneau Définition de source de données. Un

seul fichier est censé être nommé. Il est possible d'utiliser des variables d'environnement de l'environnement de l'utilisateur du système d'exploitation dans le nom du fichier et de les développer. Par exemple, $HOME/START.sh nommera le script de démarrage dans le répertoire de base de l'utilisateur Db2.

Modèle de fichier

Désigne un groupe de fichiers dont le suivi et la surveillance seront assurés par les évaluations de la sécurité. Le chemin d'accès à ces fichiers peut être absolu ou relatif à la variable $INSTHOME. Définissez la valeur de la variable $INSTHOME dans la zone Répertoire d'instance de base de données dans le panneau Définition de source de données. Dans le chemin, la présence de .. indique qu'il y a un ou plusieurs répertoires entre la partie du chemin située avant et la partie du chemin située après. .+ dans le chemin indique qu'il y a exactement un répertoire entre la partie du chemin située avant et la partie du chemin située après. Par exemple `$INSTHOME/sqllib/../db2.*` est juste un raccourci pour créer des identifications de fichier unique à partir d'une seule chaîne d'identification, un modèle de fichier qui correspondra à tous les fichiers figurant dans le répertoire. Un modèle de fichier peut être affiché sous la forme d'une série d'expressions régulières séparées par des barres obliques /. Un fichier correspond si chaque élément de son chemin complet peut correspondre à l'une des expressions régulières dans l'ordre indiqué. Si un élément du modèle est une variable d'environnement, elle est développée avant le début de la recherche de correspondance. Si .. est l'un des éléments du modèle, il correspond à un niveau de répertoire égal à zéro ou plus. Par exemple, /usr/local/../foo correspondra à /usr/local/foo et /usr/local/gunk/junk/bunk/foo. L'utilisation de plus d'un élément .. dans un modèle de fichier ne doit pas être nécessaire. Elle est déconseillée car elle rend le modèle très lent à développer. En raison de la confusion avec son utilisation dans les expressions régulières, | ne peut pas être utilisé comme délimiteur comme cela peut être le cas dans Windows.

De plus, l'ensemble Guardium Unix/DB2 Assessment: UNIX - DB2 for Unix comprend les modèles suivants :

Db2govd Setuid Bits Is Not Set (Le bit SETUID sur Db2gov n'est pas défini)

Ce test vérifie que le bit SETUID sur DB2GOVD a été désactivé

Db2start Setuid Bits Is Not Set (Le bit SETUID sur Db2start n'est pas défini)

Ce test vérifie que le bit SETUID sur DB2START a été désactivé

Db2stop Setuid Bits Is Not Set (Le bit SETUID sur Db2stop n'est pas défini)

Ce test vérifie que le bit SETUID sur DB2STOP a été désactivé

Propriété des fichiers

Ce test vérifie la propriété des fichiers et les modifications associées pour les fichiers Db2.

Droits d'accès aux fichiers

Ce test vérifie les droits d'accès aux fichiers et les modifications associées pour les fichiers Db2.

Modèles CAS - Informix

Script de système d'exploitation

Désigne un script de système d'exploitation à exécuter. Il doit commencer par la variable $SCRIPTS, qui se rapporte au répertoire scripts situé sous le répertoire de base CAS et identifier le script à exécuter, par exemple, `$HOME/ informix_rootpath_owner.sh`". Bien entendu, le script même doit résider dans le répertoire CAS $SCRIPTS. La sortie du script est stockée dans la base de données Guardium pour être utilisée par les évaluations de la sécurité. Il peut s'agir d'un script shell ou d'un script de commandes, ou d'un ensemble de commandes pouvant être saisies sur la ligne de commande. Etant donné la nature changeante de l'analyse syntaxique de Java, il est suggéré que les commandes (à l'exception des plus simples) soient insérées dans un script au lieu d'être exécutées directement. Sous Unix, le script est exécuté dans l'environnement de l'utilisateur du système d'exploitation indiqué. Trois variables d'environnement seront définies pour l'environnement d'exécution. L'utilisateur pourra les utiliser dans l'écriture des scripts : $UCAS est le nom d'utilisateur de la base de données, $PCAS est le mot de passe de la base de données et $ICAS est le nom d'instance de la base de données. Pour Windows, ces trois valeurs seront ajoutées pour constituer les trois derniers arguments dans l'exécution du fichier de commandes. Par exemple, si vous disposez d'un modèle Script de système d'exploitation `%SCRIPTS%\MyScript.bat my-arg1 my-arg2`, les variables %3, %4 et %5 correspondent respectivement au nom d'utilisateur, au mot de passe et au nom d'instance de la base de données.

Fichier

Désigne un fichier dont le suivi et la surveillance seront assurés par les évaluations de la sécurité. Le chemin d'accès au fichier peut être absolu ou relatif à la variable $INFORMIXDIR. Définissez la valeur de la variable $INFORMIXDIR dans la zone Répertoire d'instance de base de données dans le panneau Définition de la source de données. Un seul fichier est censé être nommé. Il est possible d'utiliser des variables d'environnement de l'environnement de l'utilisateur du système d'exploitation dans le nom du fichier et de les développer. Par exemple, $HOME/START.sh nommera le script de démarrage dans le répertoire de base de l'utilisateur Informix.

De plus, l'ensemble Guardium Unix/Informix Assessment for Unix comprend les modèles suivants :

Recherche d'erreurs dans les fichiers journaux

Ce test recherche les erreurs dans le fichier online.log

Propriété des fichiers

Ce test vérifie la propriété des fichiers et les modifications associées pour les fichiers Informix.

Droits d'accès aux fichiers

Ce test vérifie les droits d'accès aux fichiers et les modifications associées pour les fichiers Informix.

Modèles CAS - Oracle

Script de système d'exploitation

Désigne un script de système d'exploitation à exécuter. Il doit commencer par la variable $SCRIPTS, qui se rapporte au répertoire scripts situé sous le répertoire de base CAS et identifier le script à exécuter, par exemple, $SCRIPTS/oracle_user.sh. Bien entendu, le script même doit résider dans le répertoire CAS $SCRIPTS. La sortie du script est stockée dans la base de données Guardium pour être utilisée par les évaluations de la sécurité. (Il peut s'agir d'un script shell ou d'un script de commandes, ou d'un ensemble de commandes pouvant être saisies sur la ligne de commande. Etant donné la nature changeante de l'analyse syntaxique de Java, il est suggéré que les commandes (à l'exception des plus simples) soient insérées dans un script au lieu d'être exécutées directement. Sous Unix, le script est exécuté dans l'environnement de l'utilisateur du système d'exploitation indiqué. Trois variables d'environnement seront définies pour l'environnement d'exécution. L'utilisateur pourra les utiliser dans l'écriture des scripts : $UCAS est le nom d'utilisateur de la base de données, $PCAS est le mot de passe de la base de données et $ICAS est le nom d'instance de la base

de données. Pour Windows, ces trois valeurs seront ajoutées pour constituer les trois derniers arguments dans l'exécution du fichier de commandes. Par exemple, si vous disposez d'un modèle Script de système d'exploitation $SCRIPTS/mysql_mysqld_user.sh, les variables %3, %4 et %5 correspondent respectivement au nom d'utilisateur, au mot de passe et au nom d'instance de la base de données.)

Fichier

Désigne un fichier à suivre et surveiller. Le chemin d'accès au fichier peut être absolu ou relatif à la variable $ORACLE_HOME. La valeur de la variable $ORACLE_HOME correspond à la valeur définie dans la zone Répertoire d'instance de base de données du panneau Définition de source de données. (Un seul fichier est censé être nommé. Il est possible d'utiliser des variables d'environnement de l'environnement de l'utilisateur du système d'exploitation dans le nom du fichier et de les développer. Par exemple, $HOME/START.sh nommera le script de démarrage dans le répertoire de base de l'utilisateur Oracle.)

Modèle de fichier

Désigne un groupe de fichiers à suivre et surveiller. Le chemin d'accès à ces fichiers peut être absolu ou relatif à la variable $ORACLE_HOME. Définissez la valeur de la variable $ORACLE_HOME dans la zone Répertoire d'instance de base de données dans le panneau Définition de source de données. Dans le chemin, la présence de .. indique qu'il y a un ou plusieurs répertoires entre la partie du chemin située avant et la partie du chemin située après. .+ dans le chemin indique qu'il y a exactement un répertoire entre la partie du chemin située avant et la partie du chemin située après. Par exemple : $ORACLE_HOME/oradata/../*.dbf (Il s'agit d'un raccourci pour créer de nombreuses identifications de fichier unique à partir d'une seule chaîne d'identification, un modèle de fichier). Un modèle de fichier peut être affiché sous la forme d'une série d'expressions régulières séparées par des barres obliques /. Un fichier correspond si chaque élément de son chemin complet peut correspondre à l'une des expressions régulières dans l'ordre indiqué. Si un élément du modèle est une variable d'environnement, elle est développée avant le début de la recherche de correspondance. Si .. est l'un des éléments du modèle, il correspond à un niveau de répertoire égal à zéro ou plus. Par exemple, /usr/local/../foo correspondra à /usr/local/foo et /usr/local/gunk/junk/bunk/foo. L'utilisation de plus d'un élément .. dans un modèle de fichier ne doit pas être nécessaire. Elle est déconseillée car elle rend le modèle très lent à développer. En raison de la confusion avec son utilisation dans les expressions régulières, \ ne peut pas être utilisé comme délimiteur comme cela peut être le cas dans Windows. Le modèle de fichier affiché précédemment n'est pas correct car *.dbf n'est pas une expression régulière valide. On devrait avoir .*dbf.

De plus, le jeu de modèles par défaut Guardium Unix/Oracle comprend les modèles suivants :

ADMIN_RESTRICTIONS est activé

Ce test vérifie que le paramètre ADMIN_RESTRICTIONS dans le fichier listener.ora est défini correctement.

Propriété des fichiers

Ce test vérifie la propriété des fichiers et les modifications associées pour les fichiers de données, les journaux, les exécutables Oracle, etc.

Droits d'accès aux fichiers

Ce test vérifie les droits d'accès aux fichiers et les modifications associées pour les fichiers de données, les journaux, les exécutables Oracle, etc.

Recherche d'erreurs dans les fichiers journaux

Ce test analyse les fichiers journaux Oracle pour rechercher les chaînes avec des erreurs.

SPOOLMAIN.LOG n'existe pas

Ce test vérifie l'existence du fichier SPOOLMAIN.LOG d'Oracle.

Modèles CAS - MongoDB

MongoDB est utilisé en principe comme un système opérationnel et comme back end pour les applications Web car il facilite la programmation des données non relationnelles, telles que les documents JSON.

Utilisez le modèle Unix/MongoDB pour indiquer plusieurs chemins et plusieurs répertoires dans la source de données afin d'analyser divers composants comme indiqué dans la définition de la source de données MongoDB.

Analysez un modèle de fichier en sélectionnant des éléments de modèle commençant par "$".

Ne sélectionnez pas l'élément $SCRIPTS/mongodb_unmask_value.sh - il s'agit d'un élément de réserve Guardium.

Si l'élément de modèle n'est pas indiqué dans la zone Répertoire d'instance de base de données dans la définition de la source de données MongoDB, il sera ignoré et ne sera pas analysé.

Remarque : Pour que les scripts CAS fonctionnent, vous devez activer la connexion pour le compte MongoDB sur le serveur MongoDB. Pour activer la connexion, connectez-vous en tant que superutilisateur (root), exécutez la commande chsh mongod, puis, lorsque le système vous demande un nouveau shell, entrez `/bin/bash`.
Remarque : Vous pouvez créer votre propre modèle avec plusieurs chemins d'accès aux fichiers pour n'importe quel type de source de données. Dans ce cas, nous vous recommandons d'utiliser Unix/MongoDB comme référence. Pour créer un nouveau modèle pour une source de données MongoDB, vous pouvez cloner et modifier le modèle Unix/MongoDB.
Remarque : Les sources de données MongoDB prennent en charge les connexions SSL serveur et client/serveur avec des certificats client SSL. Les connexions MongoDB utilisent un pilote Java au lieu d'une connexion de base de données JDBC.
Remarque : La solution VA pour les clusters MongoDB peut s'exécuter sur mongos, un noeud principal et tous les noeuds secondaires pour les jeux de répliques.

Modèles CAS - Netezza

Propriété des fichiers

Ce test vérifie la propriété des fichiers et leur appartenance au groupe adéquat conformément à la définition figurant dans le modèle CAS.

Droits d'accès aux fichiers

Ce test vérifie si les droits d'accès aux fichiers sont définis correctement conformément à la définition figurant dans le modèle CAS.

Recherche d'erreurs dans les fichiers journaux

Ce test recherche les événements (FATAL, ERROR, DEBUG, ABORT et PANIC) dans ces deux fichiers journaux. /nz/kit/log/postgres/pg.log et /nz/kit/log/startupsvr/startupsvr.log

Modèles CAS - Oracle

Script de système d'exploitation

Désigne un script de système d'exploitation à exécuter. Il doit commencer par la variable $SCRIPTS, qui se rapporte au répertoire scripts situé sous le répertoire de base CAS et identifier le script à exécuter, par exemple, $SCRIPTS/oracle_user.sh. Bien entendu, le script même doit résider dans le répertoire CAS $SCRIPTS. La sortie du script est stockée dans la base de données Guardium pour être utilisée par les évaluations de la sécurité. (Il peut s'agir d'un script shell ou d'un script de commandes, ou d'un ensemble de commandes pouvant être saisies sur la ligne de commande. Etant donné la nature changeante de l'analyse syntaxique de Java, il est suggéré que les commandes (à l'exception des plus simples) soient insérées dans un script au lieu d'être exécutées directement. Sous Unix, le script est exécuté dans l'environnement de l'utilisateur du système d'exploitation indiqué. Trois variables d'environnement seront définies pour l'environnement d'exécution. L'utilisateur pourra les utiliser dans l'écriture des scripts : $UCAS est le nom d'utilisateur de la base de données, $PCAS est le mot de passe de la base de données et $ICAS est le nom d'instance de la base de données. Pour Windows, ces trois valeurs seront ajoutées pour constituer les trois derniers arguments dans l'exécution du fichier de commandes. Par exemple, si vous disposez d'un modèle Script de système d'exploitation $SCRIPTS/mysql_mysqld_user.sh, les variables %3, %4 et %5 correspondent respectivement au nom d'utilisateur, au mot de passe et au nom d'instance de la base de données.)

Fichier

Désigne un fichier à suivre et surveiller. Le chemin d'accès au fichier peut être absolu ou relatif à la variable $ORACLE_HOME. La valeur de la variable $ORACLE_HOME correspond à la valeur définie dans la zone Répertoire d'instance de base de données du panneau Définition de source de données. (Un seul fichier est censé être nommé. Il est possible d'utiliser des variables d'environnement de l'environnement de l'utilisateur du système d'exploitation dans le nom du fichier et de les développer. Par exemple, $HOME/START.sh nommera le script de démarrage dans le répertoire de base de l'utilisateur Oracle.)

Modèle de fichier

Désigne un groupe de fichiers à suivre et surveiller. Le chemin d'accès à ces fichiers peut être absolu ou relatif à la variable $ORACLE_HOME. Définissez la valeur de la variable $ORACLE_HOME dans la zone Répertoire d'instance de base de données dans le panneau Définition de source de données. Dans le chemin, la présence de .. indique qu'il y a un ou plusieurs répertoires entre la partie du chemin située avant et la partie du chemin située après. .+ dans le chemin indique qu'il y a exactement un répertoire entre la partie du chemin située avant et la partie du chemin située après. Par exemple : $ORACLE_HOME/oradata/../*.dbf (Il s'agit d'un raccourci pour créer de nombreuses identifications de fichier unique à partir d'une seule chaîne d'identification, un modèle de fichier). Un modèle de fichier peut être affiché sous la forme d'une série d'expressions régulières séparées par des barres obliques /. Un fichier correspond si chaque élément de son chemin complet peut correspondre à l'une des expressions régulières dans l'ordre indiqué. Si un élément du modèle est une variable d'environnement, elle est développée avant le début de la recherche de correspondance. Si .. est l'un des éléments du modèle, il correspond à un niveau de répertoire égal à zéro ou plus. Par exemple, /usr/local/../foo correspondra à /usr/local/foo et /usr/local/gunk/junk/bunk/foo. L'utilisation de plus d'un élément .. dans un modèle de fichier ne doit pas être nécessaire. Elle est déconseillée car elle rend le modèle très lent à développer. En raison de la confusion avec son utilisation dans les expressions régulières, \ ne peut pas être utilisé comme délimiteur comme cela peut être le cas dans Windows. Le modèle de fichier affiché précédemment n'est pas correct car *.dbf n'est pas une expression régulière valide. On devrait avoir .*dbf.

De plus, le jeu de modèles par défaut Guardium Unix/Oracle comprend les modèles suivants :

ADMIN_RESTRICTIONS est activé

Ce test vérifie que le paramètre ADMIN_RESTRICTIONS dans le fichier listener.ora est défini correctement.

Propriété des fichiers

Ce test vérifie la propriété des fichiers et les modifications associées pour les fichiers de données, les journaux, les exécutables Oracle, etc.

Droits d'accès aux fichiers

Ce test vérifie les droits d'accès aux fichiers et les modifications associées pour les fichiers de données, les journaux, les exécutables Oracle, etc.

Recherche d'erreurs dans les fichiers journaux

Ce test analyse les fichiers journaux Oracle pour rechercher les chaînes avec des erreurs.

SPOOLMAIN.LOG n'existe pas

Ce test vérifie l'existence du fichier SPOOLMAIN.LOG d'Oracle.

Configuration des systèmes Oracle RAC

Voici la configuration requise pour les systèmes Oracle RAC.
Modifiez guard_tap.ini sur chaque noeud installé avec S-TAP :
unix_domain_socket_marker=<key>
où la valeur <key> se trouve dans le fichier listener.ora dans la définition du protocole IPC
Exemple 1 :
Si la ligne suivante correspond à une description dans le fichier listener.ora
LISTENER=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=ORCL))))
Modifiez le paramètre suivant en conséquence
unix_domain_socket_marker=ORCL
Exemple 2 :
Dans le cas où il y aurait plusieurs lignes IPC dans le fichier listener.ora, utilisez un dénominateur commun de toutes les clés LISTENER=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=LISTENER)))) LISTENER_SCAN1=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=LISTENER_SCAN1)))) LISTENER_SCAN2=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=LISTENER_SCAN2)))) LISTENER_SCAN3=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=LISTENER_SCAN3))))
Guardium utilise une recherche de chaîne dans le chemin de sorte que LISTENER fonctionne pour toutes ces quatre lignes, et qui est à utiliser dans ce cas :
unix_domain_socket_marker=LISTENER

Modèles CAS - PostgreSQL

Remarque : Il est très important que les variables d'environnement PostgreSQL_BIN et PostgreSQL_DATA soient définies correctement. Une valeur non valide peut entraîner l'échec ou le dysfonctionnement des tests d'évaluation CAS.

Propriété des fichiers

Ce test vérifie la propriété des fichiers et leur appartenance au groupe adéquat conformément à la définition figurant dans le modèle CAS.

Droits d'accès aux fichiers

Ce test vérifie si les droits d'accès aux fichiers sont définis correctement conformément à la définition figurant dans le modèle CAS.

Variable d'environnement PostgreSQL_BIN définie

Ce test vérifie si la variable d'environnement $PostgreSQL_BIN est définie dans votre serveur de base de données. Cette variable doit être définie sous le compte root pour Unix/Linux ou vous pouvez l'ajouter à .profile pour la connexion root. Pour le système d'exploitation Windows, elle doit être définie pour la connexion Administrateur. Pour Red Hat Linux, le dossier PostgreSQL BIN se trouve en général dans /usr/bin. Pour Solaris, il s'agit en principe d'un répertoire de ce type /data/postgres/postgres/8.3-community/bin/64. La définition de cette variable d'environnement est très importante car d'autres tests d'évaluation dépendent de l'emplacement de ce dossier.

Variable d'environnement PostgreSQL_DATA définie

Ce test vérifie si la variable d'environnement $PostgreSQL_DATA est définie dans votre serveur de base de données. Cette variable doit être définie sous le compte root pour Unix/Linux ou vous pouvez l'ajouter à .profile pour la connexion root. Pour le système d'exploitation Windows, elle doit être définie pour la connexion Administrateur. Pour Red Hat Linux, la valeur par défaut pour le dossier DATA se trouve en général dans /var/lib/pgsql/data. Pour Solaris, il n'y a pas d'emplacement régulier. La définition de cette variable d'environnement est très importante car d'autres tests d'évaluation dépendent de l'emplacement de ce dossier pour rechercher les fichiers de configuration adéquats.

Modèles CAS - SQL Server

Script de système d'exploitation

Désigne un script de système d'exploitation à exécuter. La sortie du script est stockée dans la base de données Guardium. Il peut s'agir d'un script shell ou d'un script de commandes, ou d'un ensemble de commandes pouvant être saisies sur la ligne de commande.

Variable de registre

Recherchez une valeur de clé spécifique dans le registre Windows nécessaire au test d'évaluation de la sécurité.

Modèles CAS - Sybase

Script de système d'exploitation

Désigne un script de système d'exploitation à exécuter. Il doit commencer par la variable $SCRIPTS, qui se rapporte au répertoire scripts situé sous le répertoire de base CAS et identifier le script à exécuter, par exemple, $HOME/sybase_sysdevice_type_test.sh. Bien entendu, le script même doit résider dans le répertoire CAS $SCRIPTS. La sortie du script est stockée dans la base de données Guardium pour être utilisée par les évaluations de la sécurité. Il peut s'agir d'un script shell ou d'un script de commandes, ou d'un ensemble de commandes pouvant être saisies sur la ligne de commande. Etant donné la nature changeante de l'analyse syntaxique de Java, il est suggéré que les commandes (à l'exception des plus simples) soient insérées dans un script au lieu d'être exécutées directement. Sous Unix, le script est exécuté dans l'environnement de l'utilisateur du système d'exploitation indiqué. Trois variables d'environnement seront définies pour l'environnement d'exécution. L'utilisateur pourra les utiliser dans l'écriture des scripts : $UCAS est le nom d'utilisateur de la base de données, $PCAS est le mot de passe de la base de données et $ICAS est le nom d'instance de la base de données. Pour Windows, ces trois valeurs seront ajoutées pour constituer les trois derniers arguments dans l'exécution du fichier de commandes. Par exemple, si vous disposez d'un modèle Script de système d'exploitation %SCRIPTS%\MyScript.bat my-arg1 my-arg2, les variables %3, %4 et %5 correspondent respectivement au nom d'utilisateur, au mot de passe et au nom d'instance de la base de données.

Fichier

Désigne un fichier dont le suivi et la surveillance seront assurés par les évaluations de la sécurité. Le chemin d'accès au fichier peut être absolu ou relatif à la variable $SYBASE. La valeur de la variable $SYBASE correspond à la valeur définie dans la zone Répertoire d'instance de base de données du panneau Définition de source de données. Un seul fichier est censé être nommé. Il est possible d'utiliser des variables d'environnement de l'environnement de l'utilisateur du système d'exploitation dans le nom du fichier et de les développer. Par exemple, $HOME/START.sh nommera le script de démarrage dans le répertoire de base de l'utilisateur Sybase.

Modèle de fichier

Désigne un groupe de fichiers dont le suivi et la surveillance seront assurés par les évaluations de la sécurité. Le chemin d'accès au fichier peut être absolu ou relatif à la variable $SYBASE. La valeur de la variable $SYBASE correspond à la valeur définie dans la zone Répertoire d'instance de base de données du panneau Définition de source de données. Dans le chemin, la présence de .. indique qu'il y a un ou plusieurs répertoires entre la partie du chemin située avant et la partie du chemin située après. .+ dans le chemin indique qu'il y a exactement un répertoire entre la partie du chemin située avant et la partie du chemin située après. Par exemple : $SYBASE/../.*dat" Il s'agit d'un raccourci pour créer de nombreuses identifications de fichier unique à partir d'une seule chaîne d'identification, un modèle de fichier. Un modèle de fichier peut être affiché sous la forme d'une série d'expressions régulières séparées par des barres obliques /. Un fichier correspond si chaque élément de son chemin complet peut correspondre à l'une des expressions régulières dans l'ordre indiqué. Si un élément du modèle est une variable d'environnement, elle est développée avant le début de la recherche de correspondance. Si .. est l'un des éléments du modèle, il correspond à un niveau de répertoire égal à zéro ou plus. Par exemple, /usr/local/../foo correspondra à /usr/local/foo et /usr/local/gunk/junk/bunk/foo. L'utilisation de plus d'un élément .. dans un modèle de fichier ne doit pas être nécessaire. Elle est déconseillée car elle rend le modèle très lent à développer. En raison de la confusion avec son utilisation dans les expressions régulières, \ ne peut pas être utilisé comme délimiteur comme cela peut être le cas dans Windows.

De plus l'ensemble Guardium Unix/Sybase Assessment: UNIX - SYBASE comprend les modèles suivants :

Recherche d'erreurs dans les fichiers journaux

Ce test recherche les erreurs dans les fichiers journaux Sybase.

Le propriétaire de l'unité système est sysbase

Ce test vérifie la propriété de sysdevice.

Propriété des fichiers

Ce test vérifie la propriété des fichiers et les modifications associées pour les fichiers Sybase.

Droits d'accès aux fichiers

Ce test vérifie les droits d'accès aux fichiers et les modifications associées pour les fichiers Sybase.

Modèles CAS - Teradata

Propriété des fichiers

Ce test vérifie la propriété des fichiers et leur appartenance au groupe adéquat conformément à la définition figurant dans le modèle CAS.

Droits d'accès aux fichiers

Ce test vérifie si les droits d'accès aux fichiers sont définis correctement conformément à la définition figurant dans le modèle CAS.

Aster Data

Teradata a fait l'acquisition d'Aster Data en 2011, utilisé en principe pour les applications d'entrepôts de données et de traitement analytique (OLAP). Aster Data a créé une infrastructure nommée SQL-MapReduce qui permet d'utiliser SQL (Structured Query Language) avec Map Reduce. Aster Data est associé le plus souvent aux types d'applications à parcours de navigation.

Une base de données Aster nCluster comprend trois groupes de noeuds : Queen, Worker et Loader. Un agent CAS est installé sur ces trois groupes de noeuds.

Une évaluation de la sécurité doit être créée pour exécuter tous les tests sur le noeud Queen. Toutes les connexions de base de données pour Aster Data passent uniquement par le noeud Queen.

Les tests sur les noeuds Worker et Loader sont requis uniquement lors de l'exécution des tests CAS (Droits d'accès aux fichiers et Propriété des fichiers).

Les tests de privilèges sont effectués en boucle sur toutes les bases de données d'une instance donnée.

Lorsque vous effectuez des tests VA qui nécessitent un accès à CAS et que vous complétez les options de configuration de source de données CAS, indiquez le nom d'utilisateur sous lequel est installé Aster dans la zone Compte d'instance de base de données. Le nom d'utilisateur est nommé en principe beehive.

Pour l'option Répertoire d'instance de base de données, il s'agit du répertoire de base de l'utilisateur beehive. La valeur par défaut est en principe /home/beehive.

Lorsque vous exécutez des tests VA qui n'utilisent pas CAS, le client doit créer sa source de données pointant vers le noeud QUEEN au sein du cluster.

Lorsque vous exécutez des tests VA qui dépendent de CAS, si le noeud que vous testez est l'un du groupe Worker, vous devez dans ce cas configurer l'"URL personnalisée" dans la source de données pour qu'elle pointe vers le noeud Queen utilisé comme mode d'écoute.

Exemple

Nom d'hôte/IP = Worker.guard.xxx.xxx..com ou 1xx.1xx.111.111 (Il s'agit de l'hôte Worker réel même si Worker n'écoute pas dessus. CAS en a besoin pour envoyer et recevoir des données à partir du noeud Worker)

Port = 2046 ou n'importe quel port utilisé.

Base de données = beehive

URL personnalisée = jdbc:ncluster://aster6q:2406/beehive (Cet exemple JDBC montre que nous sommes en train de nous connecter réellement à aster6q qui correspond au noeud Queen sur le port 2406 et la base de données beehive)

Compte d'instance de base de données = beehive

Répertoire d'instance de base de données = /home/beehive

Rubrique parent : Configuration Auditing System (CAS)

Utilisation des modèles CAS

Cette section décrit comment gérer les modèles CAS

Définir un modèle/jeu de modèles

- Créer un jeu de modèles
- Modifier un jeu de modèles
- Cloner un jeu de modèles
- Supprimer un jeu de modèles

Créer un jeu de modèles

1. Ouvrez le Navigateur de configuration CAS en cliquant sur Renforcement > Contrôle des changements de configuration (Application CAS) > Configuration de jeu de modèles CAS.
2. Cliquez sur Nouveau pour ouvrir le panneau Définitions de modèle d'élément surveillé.
3. Sélectionnez le type de système d'exploitation.
4. Sélectionnez le type de base de données. Si le jeu de modèles ne nécessite pas de type de base de données, sélectionnez N_A comme type de base de données.
5. Entrez un nom unique pour Nom de jeu de modèles.
   Remarque : Les noms de jeu de modèles dépassant 128 caractères seront tronqués
6. Cliquez sur Appliquer pour sauvegarder la définition du jeu de modèles CAS.
7. Pour ajouter des éléments à ce nouveau jeu de modèles, cliquez sur Ajouter au jeu et reportez-vous à la section Définir un élément de jeu de modèles.

Rechercher le panneau Guardium CAS

Par défaut, l'accès aux fonctions de configuration CAS est limité à l'administrateur et aux utilisateurs auxquels le rôle CAS a été affecté.

Cliquez sur Renforcement. La liste des fonctions CAS est répertoriée dans l'en-tête Contrôle des changements de configuration (Application CAS).

Ouvrir le Navigateur de configuration CAS

Le panneau Navigateur de configuration CAS est le point de départ pour la création ou la modification des jeux de modèles CAS.

Ouvrez le panneau Navigateur de configuration CAS en cliquant sur Renforcement > Contrôle des changements de configuration (Application CAS) > Configuration de jeu de modèles CAS.

Vous pouvez filtrer la liste par type de système d'exploitation et type de base de données.

Modifier un jeu de modèles

Utilisez le panneau Navigateur de configuration CAS pour modifier un jeu de modèles CAS existant. Dès qu'un jeu de modèles est en cours d'utilisation sur un hôte CAS, les modifications que vous pouvez apporter à ce jeu sont limitées. Vous ne pourrez effectuer que des changements mineurs à différents éléments de la définition, mais vous ne pourrez pas ajouter ou retirer des modèles.

1. Ouvrez le panneau Navigateur de configuration CAS en cliquant sur Renforcement > Contrôle des changements de configuration (Application CAS) > Configuration de jeu de modèles CAS.
2. Filtrez la liste des jeux de modèles par type de système d'exploitation ou par type de base de données.
3. Sélectionnez le jeu de modèles que vous souhaitez modifier et cliquez sur Modifier pour ouvrir le panneau Définition de jeu de modèles CAS.
4. Effectuez les changements souhaités et cliquez sur Appliquer pour les sauvegarder.

Cloner un jeu de modèles

1. Ouvrez le panneau Navigateur de configuration CAS en cliquant sur Renforcement > Contrôle des changements de configuration (Application CAS) > Configuration de jeu de modèles CAS.
2. Filtrez la liste des jeux de modèles par type de système d'exploitation ou par type de base de données.
3. Sélectionnez le jeu de modèles que vous souhaitez cloner et cliquez sur Cloner pour ouvrir le panneau Définition de jeu de modèles CAS.
4. Une fois le clone créé, modifiez-le pour répondre à vos besoins.

Remarque : Les modèles prédéfinis ne sont pas modifiables. Ils ont les mêmes restrictions que les modèles utilisés par un hôte CAS. Le client doit les cloner, puis éditer les copies clonées s'il souhaite les modifier.

Supprimer un jeu de modèles

1. Ouvrez le panneau Navigateur de configuration CAS en cliquant sur Renforcement > Contrôle des changements de configuration (Application CAS) > Configuration de jeu de modèles CAS.
2. Filtrez la liste des jeux de modèles par type de système d'exploitation ou par type de base de données.
3. Sélectionnez le jeu de modèles que vous souhaitez supprimer et cliquez sur Supprimer.

Définir un élément de jeu de modèles

Dès qu'un jeu de modèles est en cours d'utilisation sur un hôte CAS, les modifications que vous pouvez apporter à ce jeu sont limitées. Vous ne pourrez effectuer que des changements mineurs à différents éléments de la définition, mais vous ne pourrez pas ajouter ou retirer des modèles.

- Créer un élément de jeu de modèles
- Modifier un élément de jeu de modèles
- Supprimer un élément de jeu de modèles

Créer un élément de jeu de modèles

1. Ouvrez le panneau Navigateur de configuration CAS en cliquant sur Renforcement > Contrôle des changements de configuration (Application CAS) > Configuration de jeu de modèles CAS.
2. Cliquez sur Nouveau pour ouvrir le panneau Définitions de modèle d'élément surveillé.
3. Entrez un nom de jeu de modèles, sélectionnez un type de système d'exploitation et un type de base de données, puis cliquez sur Appliquer.
4. Cliquez sur Ajouter au jeu pour créer un nouvel élément.

Modifier un élément de jeu de modèles

1. Ouvrez le panneau Navigateur de configuration CAS en cliquant sur Renforcement > Contrôle des changements de configuration (Application CAS) > Configuration de jeu de modèles CAS.
2. Filtrez la liste des jeux de modèles par type de système d'exploitation ou par type de base de données.
3. Sélectionnez le jeu de modèles que vous souhaitez modifier et cliquez sur Modifier pour ouvrir le panneau Définition de jeu de modèles CAS.
4. Sélectionnez les éléments que vous souhaitez modifier et cliquez sur Editer sélection.... Effectuez les changements souhaités et cliquez sur Appliquer pour les sauvegarder.

Supprimer un élément de jeu de modèles

1. Ouvrez le panneau Navigateur de configuration CAS en cliquant sur Renforcement > Contrôle des changements de configuration (Application CAS) > Configuration de jeu de modèles CAS.
2. Filtrez la liste des jeux de modèles par type de système d'exploitation ou par type de base de données.
3. Sélectionnez le jeu de modèles que vous souhaitez modifier et cliquez sur Modifier pour ouvrir le panneau Définition de jeu de modèles CAS.
4. Sélectionnez les éléments que vous souhaitez supprimer et cliquez sur Supprimer l'élément sélectionné....

Panneau Définition de modèle d'élément CAS

Composant	Description
Type de système	Type de système d'exploitation : Windows ou Unix. Vous pouvez changer cette sélection lorsque le jeu de modèles est vide, mais vous ne pouvez pas le faire si le jeu de modèles contient un ou plusieurs éléments.

d'exploitation	
Type de base de données	Type de base de données (Oracle, MS-Sql, Db2, Sybase, Informix, etc.) ou N/A pour un jeu de modèles du système d'exploitation. Vous pouvez changer cette sélection lorsque le jeu de modèles est vide, mais vous ne pouvez pas le faire si le jeu de modèles contient un ou plusieurs éléments.
Description	Nom facultatif de l'élément utilisé dans les rapports et qui permet d'identifier l'élément dans d'autres panneaux CAS (Définition de jeu de modèles CAS par exemple). S'il est omis, le nom de l'élément prend par défaut la valeur du nom ou du modèle de fichier, du nom de la variable ou du script (en fonction du type).
Type	Il peut s'agir d'un des types suivants : Requête SQL, Script de système d'exploitation, Variable d'environnement, Variable de registre, Modèle de variable de registre et Modèle de fichier. Voir Types de modèle et d'audit pour plus d'informations. Remarque : S'il est utilisé avec des tests d'évaluation CAS, il doit s'agir du script de système d'exploitation.
Contenu	Texte dépendant du type définissant l'élément spécifique à surveiller ou comment le générer. Voir Types de modèle et d'audit pour plus d'informations. Remarque : S'il s'agit d'un script de système d'exploitation, CAS attendra la fin du script. Pour limiter la durée d'exécution autorisée pour un script de système d'exploitation et autoriser CAS à interrompre le script, utilisez le paramètre cas_command_wait dans guard_tap.ini. La durée d'attente par défaut est de 300 secondes ou 5 minutes. Lorsque vous changez ce paramètre, vous n'avez pas besoin de redémarrer CAS.
Limite des autorisations	Pour les types Fichier et Modèle de fichier uniquement. Utilisé pour Unix uniquement - il s'agit des autorisations auxquelles ce fichier est limité.
Propriétaire de fichier	Pour les types Fichier et Modèle de fichier uniquement. Propriétaire du ou des fichiers.
Groupe de fichiers	Pour les types Fichier et Modèle de fichier uniquement. Propriétaire du groupe de fichiers.
Période	Intervalle maximal entre les tests, indiqué par un nombre de minutes (m), heures (h) ou jours (d). Les données sont accessibles après la période initiale écoulée et jusqu'au début de la prochaine période.
Conserver les données	Si cette option est sélectionnée, une copie des données réelles est sauvegardée avec chaque changement. Par exemple : pour un élément de fichier, une copie du fichier est sauvegardée. Si cette option est sélectionnée mais que la taille des données brutes de l'élément est supérieure au paramètre Raw Data Limit configuré pour cet hôte CAS, aucune donnée ne sera sauvegardée.
Utiliser MD5	Indique si une autre comparaison est effectuée en calculant un total de contrôle des données brutes à l'aide de l'algorithme MD5. Le calcul du total de contrôle MD5 prend du temps pour les objets CLOB. Toutefois, c'est un meilleur indicateur de changement que la simple utilisation de la taille. La valeur par défaut consiste à ne pas utiliser MD5. Si MD5 est utilisé, mais que la taille des données brutes est supérieure au paramètre MD5 Size Limit configuré pour l'hôte CAS, le calcul MD5 et la comparaison seront ignorés.
Activé	Sélectionné par défaut. Indique si une recherche de changement sera effectuée pour l'élément.

Modèle et types d'audit

Type	Description
Requête SQL	Le contenu doit être une instruction SQL valide. Le résultat renvoyé par l'instruction sera comparé au résultat renvoyé lors de la dernière exécution de la requête. La requête sera exécutée avec les paramètres spécifiés dans la source de données utilisée : nom d'utilisateur, port de base de données, etc. Ces paramètres doivent être renseignés avec soin dans la source de données pour que la requête renvoie un résultat.
Script de système d'exploitation	Le contenu peut être une entrée de ligne de commande valide ou le nom d'un fichier contenant un script exécutable de système d'exploitation. Le script est exécuté dans l'environnement de l'utilisateur du système d'exploitation indiqué dans le champ Compte d'instance de base de données de la définition de la source de données.
Variable d'environnement	Le contenu doit nommer une variable d'environnement définie dans le contexte de l'utilisateur du système d'exploitation indiqué dans le champ Compte d'instance de base de données de la définition de la source de données.
Variable de	Le contenu est interprété sous forme de chemin d'accès à une variable dans le registre Windows de l'hôte. La valeur trouvée dans ce chemin est comparée à celle trouvée lors du dernier suivi de chemin.

registre	
Modèle de variable de registre	Le contenu est une séquence d'expressions régulières utilisées pour correspondre aux composants des chemins dans le registre Windows. Le modèle est utilisé pour développer des éléments surveillés de type variable de registre qui seront traités comme indiqué précédemment. Les expressions régulières sont liées par / de sorte que le modèle ressemble à un chemin d'accès au registre. Le caractère \ plus courant, ne peut pas être utilisé car il s'agit d'un caractère spécial dans la syntaxe des expressions régulières Java™. Si une barre oblique / est nécessaire dans l'une des expressions régulières, elle doit être indiquée avec le caractère d'échappement \. (Par exemple U\/235 doit être utilisé pour représenter U/235). Le modèle .. peut être utilisé pour représenter aucun ou plusieurs composants dans un chemin. Par exemple, HKLM/Software/../buzz pourra correspondre à HKLM\Software\buzz ou HKLM\Software\one\two\three\buzz. Ce type de modèle peut occasionner une recherche particulièrement complexe en terme de calculs dans le registre, donc utilisez-le avec précaution. Mises à part ces exceptions, les expressions régulières suivent la syntaxe des expressions régulières Java.
Fichier	Le contenu est interprété sous forme de chemin de fichier absolu sur l'hôte. Les caractéristiques du fichier trouvé dans le chemin seront comparées à celles du dernier suivi du chemin. Le chemin peut comporter des variables d'environnement qui seront développées dans le contexte de l'utilisateur du système d'exploitation indiqué dans la source de données. Le chemin peut également commencer par une variable de substitution, comme "$SYBASE_HOME", qui sera remplacée par la valeur entrée dans le champ Répertoire d'instance de base de données dans la définition de la source de données.
Modèle de fichier	Le contenu est une séquence d'expressions régulières utilisées pour correspondre aux composants des chemins de fichier et pour générer des éléments surveillés de type Fichier. Les expressions régulières sont liées par / de sorte que le modèle ressemble à un chemin d'accès à un fichier. Comme pour les modèles de registre, le caractère \ ne peut pas être utilisé pour les fichiers Windows en raison de la syntaxe des expressions régulières. Si le modèle commence par *?:* sur une machine Windows, les correspondances du modèle seront démarrées sur chaque unité d'une machine à plusieurs lecteurs. La construction .. décrite dans les modèles de registre doit être également utilisée avec précaution dans un modèle de fichier. Les variables d'environnement du contexte de l'utilisateur du système d'exploitation peuvent être utilisées dans un modèle de fichier et seront développées avant le développement des expressions régulières.

Commandes GuardAPI

create_cas_template_set

create_cas_template

create_datasource

create_cas_host_instance

Rubrique parent : Configuration Auditing System (CAS)

Hôtes CAS

Une configuration d'hôte Configuration Auditing System (CAS) définit une ou plusieurs instances CAS.

Lorsque vous avez défini un ou plusieurs jeux de modèles CAS et que vous avez installé CAS sur un serveur de base de données, vous êtes prêt à configurer CAS sur cet hôte. Une configuration d'hôte CAS définit une ou plusieurs instances CAS. Chaque instance CAS spécifie un jeu de modèles CAS et définit les paramètres nécessaires pour se connecter à la base de données. Pour chaque serveur de base de données sur lequel est installé CAS, il y a une seule configuration d'hôte CAS, qui contient en principe plusieurs instances CAS (par exemple, une instance CAS pour surveiller les éléments du système d'exploitation et des instances CAS supplémentaires pour surveiller des instances de base de données individuelles).

- Définir une instance CAS
- Modifier une instance CAS
- Supprimer une instance CAS
- Désactiver une instance CAS

Définir une instance CAS

1. Ouvrez le Navigateur de configuration CAS en cliquant sur Renforcement > Contrôle des changements de configuration (Application CAS) > Configuration hôte CAS.

   Le menu répertorie tous les serveurs de base de données sur lesquels a été installé CAS et sur lesquels cet hôte s'est connecté au système Guardium.

2. Utilisez cette liste pour effectuer un filtrage par type de système d'exploitation ou type de base de données et rechercher l'hôte que vous souhaitez utiliser.
3. Mettez en évidence l'hôte que vous souhaitez modifier et cliquez sur Modifier.
4. Sélectionnez un jeu de modèles dans le menu.
   Remarque : Une instance CAS ne peut pas être définie si l'hôte est hors ligne ou s'il s'agit d'un système Guardium secondaire pour l'hôte.
5. Cliquez sur Ajouter une source de données pour ouvrir le panneau Localiseur de source de données.
   Remarque : Si aucune source de données compatible n'est disponible pour ce jeu de modèles sur cet hôte, vous pouvez cliquer sur Nouveau pour ouvrir le panneau Définition de source de données et ajouter une source de données.
6. Sélectionnez la source de données que vous souhaitez ajouter au jeu de modèles et cliquez sur Ajouter.

Rechercher le panneau Guardium CAS

L'accès aux fonctions de configuration CAS est limité à l'administrateur et aux utilisateurs auxquels le rôle CAS a été affecté.

Cliquez sur Renforcement. Toutes les fonctions CAS sont répertoriées dans l'en-tête Contrôle des changements de configuration (Application CAS).

Ouvrir le Navigateur de configuration CAS

Le panneau Navigateur de configuration CAS est le point de départ pour la création ou la modification d'hôtes CAS.

Ouvrez le panneau Navigateur de configuration CAS en cliquant sur Renforcement > Contrôle des changements de configuration (Application CAS) > Configuration hôte CAS.

Modifier une instance CAS

1. Ouvrez le panneau Navigateur de configuration CAS
2. Utilisez cette liste pour effectuer un filtrage par type de système d'exploitation ou type de base de données et rechercher l'instance que vous souhaitez utiliser.
3. Mettez en évidence l'hôte que vous souhaitez modifier et cliquez sur Modifier.

Une liste d'instances CAS définies associées à l'hôte sélectionné s'affiche avec les informations et options d'édition suivantes :

Tableau 1. Modifier une instance CAS

Composant	Description
Icône Désactiver/Activer une instance	Cliquez sur l'icône Désactiver une instance pour désactiver/activer l'instance CAS
Icône Supprimer une instance	Cliquez sur l'icône Supprimer une instance pour supprimer l'instance CAS
Source de données	Identifie la source de données utilisée par l'instance. Cliquez sur **Source de données** pour ouvrir le panneau Définition de source de données pour éditer la définition de la source de données
Jeu de modèles	Identifie le jeu de modèles CAS utilisé par l'instance. Cliquez sur ce lien pour ouvrir le panneau Définitions de modèle d'élément surveillé afin d'afficher ou modifier la définition du jeu de modèles. Voir Utilisation des modèles CAS pour plus d'informations
Eléments surveillés	Nombre d'éléments actuellement surveillés par l'instance. Cliquez sur ce lien pour ouvrir le panneau Définitions d'élément surveillé qui affiche la liste de tous les éléments surveillés actuellement. Voir Afficher les listes d'éléments surveillés pour plus d'informations. Remarque : Par défaut, il y a 10 000 éléments surveillés pouvant être affichés dans les rapports, quel que soit le nombre d'éléments surveillés définis. Il est suggéré de définir plusieurs instances lorsque le nombre d'éléments surveillés approche cette limite.

Supprimer une instance CAS

1. Ouvrez le Navigateur de configuration CAS
2. Utilisez cette liste pour effectuer un filtrage par type de système d'exploitation ou type de base de données et rechercher l'instance que vous souhaitez utiliser.
3. Cliquez sur Supprimer une instance pour supprimer une instance CAS. Toutes les données modifiées collectées seront également supprimées.

Désactiver une instance CAS

1. Ouvrez le Navigateur de configuration CAS.
2. Utilisez cette liste pour effectuer un filtrage par type de système d'exploitation ou type de base de données et rechercher l'instance que vous souhaitez utiliser.
3. Mettez en évidence l'hôte que vous souhaitez modifier et cliquez sur Modifier, ou cliquez deux fois pour ouvrir le panneau Définitions d'instance d'hôte.
4. Cliquez sur l'icône Désactiver une instance pour désactiver une instance CAS. Les données modifiées ne seront pas collectées tant que l'instance n'est pas activée en cliquant à nouveau sur l'icône.

Afficher les listes d'éléments surveillés

Dans le panneau Définitions d'instance d'hôte, cliquez sur un lien Eléments surveillés pour afficher la liste complète des éléments surveillés dans le panneau Définitions d'élément surveillé. Le tableau suivant présente les composants visibles dans le panneau Définitions d'élément surveillé correspondant à cette configuration d'hôte.

Tous les éléments surveillés se réfèrent à des données brutes, à un objet caractère sur l'hôte, au résultat d'une requête SQL, à la sortie d'un script de système d'exploitation ou au contenu d'un fichier. La taille de l'objet caractère est calculée. Si l'élément est un fichier, les droits d'accès, le propriétaire, le groupe et la date de dernière modification sont également vérifiés. Si l'un de ces éléments a changé depuis la dernière vérification de l'élément, les changements seront notés.

Tableau 2. Afficher les listes d'éléments surveillés

Composant	Description
Case de sélection	Cochez la case de sélection si vous souhaitez éditer un élément surveillé individuellement ou en tant que groupe. Cliquez deux fois sur un élément surveillé pour l'éditer.
Elément	Nom de l'élément surveillé à partir de la description figurant dans le panneau Définition de modèle d'élément CAS
Type	Un des types suivants : Script de système d'exploitation, Requête SQL, Fichier, Variable d'environnement ou Variable de registre Script de système d'exploitation ou Script SQL : texte réel ou chemin d'accès à un script de système d'exploitation ou à un script SQL, dont la sortie sera comparée à celle produite à la prochaine exécution du script Fichier ou Modèle de fichier : fichier ou modèle spécifique permettant d'identifier un ensemble de fichiers Variable d'environnement ou Variable de registre : variable d'environnement ou variable de registre (Windows)
Période	Intervalle moyen entre les tests, indiqué par un nombre de secondes (s), minutes (m), heures (h) ou jours (d).
Conserver les données	Si cette option est marquée, une copie des données réelles est sauvegardée avec chaque changement. Par exemple, pour un élément de fichier, une copie du fichier est sauvegardée. Si cette option est marquée mais que la taille des données brutes de l'élément est supérieure au paramètre de limite des données brutes (Raw Data Limit) configuré pour cet hôte CAS, aucune donnée ne sera sauvegardée.
Utiliser MD5	Indique si la comparaison est effectuée en calculant un total de contrôle des données brutes à l'aide de l'algorithme MD5. Le calcul du total de contrôle MD5 prend du temps pour les objets CLOB. Toutefois, c'est un meilleur indicateur de changement que la simple utilisation de la taille. La valeur par défaut consiste à ne pas utiliser MD5. Si MD5 est utilisé alors que la taille des données brutes est supérieure à la taille limite MD5 (MD5 Size Limit) configurée pour l'hôte CAS, le calcul et la comparaison avec MD5 sont ignorés.

Commandes GuardAPI

delete_cas_host

list_cas_hosts

create_cas_host_instance

delete_cas_host_instance

list_cas_host_instances

update_cas_host_instance

Rubrique parent : Configuration Auditing System (CAS)

Production de rapports CAS

Cette section présente la production de rapports de Configuration Auditing System (CAS).

L'administrateur a accès à tous les générateurs de requête et rapports par défaut. Le rôle d'administrateur permet d'accéder aux rapports CAS par défaut, mais pas aux générateurs de requête CAS. Le rôle CAS permet d'accéder à la fois aux rapports CAS par défaut et aux générateurs de requête.

- Accès aux générateurs de requête CAS
- Accès aux rapports CAS par défaut
- Domaines de production de rapports CAS

Accès aux générateurs de requête CAS

Cette section décrit comment accéder aux générateurs de requête CAS à partir des portails de l'administrateur et de l'utilisateur. Pour obtenir de l'aide sur l'utilisation des générateurs de requête ou des générateurs de rapport, voir Requêtes ou Rapports.

Depuis l'interface utilisateur :

1. Ouvrez le panneau Générateur de rapport en cliquant sur Examen > Générateur de rapport.
2. Cliquez sur Nouveau, choisissez une requête dans le menu, indiquez un titre de rapport, cliquez sur Suivant, et remplissez les options restantes dans Générateur de rapport selon vos besoins.

Accès aux rapports CAS par défaut

Affichez les rapports par défaut relatifs à CAS en cliquant sur Renforcement > Rapports.

Domaines de production de rapports CAS

Domaine	Description
CAS Modèles	Suit les définitions de modèle CAS. Les modèles identifient des éléments dont il faut surveiller les changements. Les éléments surveillés peuvent être des fichiers, des variables d'environnement ou de registre, des ensembles de sorties de script SQL ou de scripts de système d'exploitation, ou l'ensemble des utilisateurs connectés.
CAS Config	Suit les configurations hôte CAS, où une configuration représente l'application d'un ou de plusieurs jeux de modèles à un hôte de serveur de base de données spécifique. Dans les instances de configuration, vous pouvez voir quels sont les éléments des jeux de modèles activés ou désactivés, ou quels sont exactement les fichiers sélectionnés et surveillés (ou non) par les modèles de masque de nom de fichier.
CAS Historique de l'hôte	Suit les événements hôte CAS, notamment les serveurs ou les clients en service et ceux qui ne sont pas en service.
Changements de CAS	Suit les changements apportés aux éléments surveillés (fichiers, variables de registre, etc.)

Domaine CAS Modèles

Entité	Description
Template Set	Décrit la définition d'un jeu de modèles
Template	Décrit un élément de modèle au sein d'un jeu de modèles

Entité Template Set

Attribut	Description
Template Set ID	Identificateur unique du jeu de modèles, numéroté de manière séquentielle
OS Type	Système d'exploitation : Unix ou Windows
DB Type	Type de base de données (Oracle, MS-SQL, DB2, Sybase, Informix, etc.) ou N/A s'il s'agit d'un modèle de système d'exploitation
Template	Nom du jeu de modèles

Set Name	
IsDefault	Indique s'il s'agit du modèle par défaut pour la combinaison type de système d'exploitation/type de base de données indiquée
Editable	Indique si ce modèle est modifiable. Les modèles Guardium par défaut ne peuvent pas être modifiés. En outre, une fois qu'un jeu de modèles a été utilisé dans une instance CAS, il ne peut plus être modifié. Cependant, un jeu de modèles peut toujours être cloné et le jeu cloné peut alors être modifié.
Timestamp	Date et heure de dernière mise à jour du modèle

Entité Template

Attribut	Description
Template ID	Identificateur unique du jeu de modèles, numéroté de manière séquentielle
Access Name	En fonction du type d'audit, il s'agit du script de système d'exploitation ou du script SQL, de la valeur d'une variable d'environnement ou de registre, ou d'un nom de fichier ou d'un masque de nom de fichier
Audit Type	Type d'élément surveillé
Audit Frequency (minutes)	Intervalle maximal (en minutes) entre les tests
Use MD5	Indique si la comparaison est effectuée en calculant une somme de contrôle à l'aide de l'algorithme MD5 et en comparant cette valeur à celle qui a été calculée lors de la dernière vérification de l'élément. La valeur par défaut consiste à ne pas utiliser MD5. Si MD5 est utilisé mais que la taille des données brutes est supérieure à la taille limite MD5 configurée pour l'hôte CAS, le calcul et la comparaison avec MD5 sont ignorés. Peu importe si MD5 est utilisé ou non, la valeur actuelle de l'horodatage de dernière modification et la taille de l'élément sont comparées avec les valeurs sauvegardées lors de la dernière vérification de l'élément.
Save Data	Indique si la case Conserver les données a été cochée. Dans ce cas, les versions précédentes de l'élément peuvent être comparées à la version actuelle.
Description	Description facultative du modèle
Timestamp	Date et heure de dernière mise à jour du modèle

Rapports par défaut de domaine CAS Templates

Rapport par défaut	Description
Rapport CAS Modèles	Affiche la liste des modèles CAS

Rapport CAS Modèles

Entité	Attribut	Opérateur	Valeur par défaut
Template	Access_Name	Like	%
Template Set	Template_Set_Name	Like	%
Template	Audit_Type	Like	%

Domaine CAS Config

Entité	Description
Host	Identifie un hôte CAS (serveur de base de données) et le statut en cours de CAS (en ligne/hors ligne). Cette entité est également disponible dans le domaine CAS Historique de l'hôte
Instance Config	Pour chaque hôte, une entrée Configuration d'instance (Instance Config) décrit une instance CAS, qui contient les paramètres de connexion à la base de données (si nécessaire) et identifie le jeu de modèles utilisé par l'instance. Elle fournit le statut en cours de l'instance (in use, enabled ou disabled) et la date de dernière révision.
Monitored Item Details	Identifie un élément (par exemple un fichier ou une variable d'environnement) surveillé par une instance CAS. Contient la définition de l'élément et indique s'il est activé ou non.

Entité Host

Entité	Description
Host Name	Nom d'hôte du serveur de base de données (peut afficher une adresse IP)
OS Type	Système d'exploitation : UNIX ou WIN
Is Online	Statut en ligne (yes ou no) lorsque l'enregistrement a été écrit

Entité Instance Config

Attribut	Description
DB Type	Type de base de données (Oracle, MS-SQL, DB2, Sybase, Informix, etc.) ou N/A s'il s'agit d'une instance de système d'exploitation
Instance	Nom de l'instance
User	Nom d'utilisateur utilisé par CAS pour se connecter à la base de données ou N/A pour une instance de système d'exploitation.
Port	Numéro de port utilisé par CAS pour se connecter à la base de données. Il peut être vide pour une instance de système d'exploitation
DB Home Dir	Répertoire de base de la base de données. Il peut être vide pour une instance de système d'exploitation
Template Set ID	Identifie le jeu de modèles utilisé par cette instance

Entité Monitored Item Details

Attribut	Description
Template ID	Type de base de données (Oracle, MS-SQL, DB2, Sybase, Informix, etc.) ou N/A s'il s'agit d'une instance de système d'exploitation
MonitoredItem	Nom de l'instance
AuditType	Nom d'utilisateur utilisé par CAS pour se connecter à la base de données ou N/A pour une instance de système d'exploitation.
Enabled	Numéro de port utilisé par CAS pour se connecter à la base de données. Il peut être vide pour une instance de système d'exploitation
InSynch	Répertoire de base de la base de données. Il peut être vide pour une instance de système d'exploitation
AuditFrequency	Identifie le jeu de modèles utilisé par cette instance
UseMD5	Indique si la comparaison est effectuée en calculant une somme de contrôle à l'aide de l'algorithme MD5 et en comparant cette valeur à celle qui a été calculée lors de la dernière vérification de l'élément. La valeur par défaut consiste à ne pas utiliser MD5. Si MD5 est utilisé mais que la taille des données brutes est supérieure à la taille limite MD5 configurée pour l'hôte CAS, le calcul et la comparaison avec MD5 sont ignorés. Peu importe si MD5 est utilisé ou non, la valeur actuelle de l'horodatage de dernière modification et la taille de l'élément sont comparées avec les valeurs sauvegardées lors de la dernière vérification de l'élément.
SaveData	Lorsque cette option est cochée, la version précédente de l'élément peut être comparée à la version actuelle
Description	Description facultative de l'instance
TemplateContent	Entrée du modèle qui constitue la base de cet élément surveillé, définie à partir de l'attribut Template entity Access Name lors de la création de l'instance. En principe, elle est identique à l'élément surveillé, mais si un modèle de fichier a été utilisé dans le modèle, il s'agira de ce modèle de fichier

Rapports par défaut du domaine CAS Config

Rapports par défaut	Description
CAS Instances	Affiche la liste des instances CAS
CAS Configuration d'instance	Affiche la liste des changements de configuration de l'instance CAS

Rapport CAS Instances

Entité	Attribut	Opérateur	Valeur par défaut
Host	Host_Name	Like	%
Host	OS_Type	Like	%
Instance Config	DB_Type	Like	%
Instance Config	Instance	Like	%

Rapport CAS Configuration d'instance

Entité	Attribut	Opérateur	Valeur par défaut
Host	Host_Name	Like	%
Host	OS_Type	Like	%
Monitored Item Details	Template_Id	Like	%

Rapports d'exploration en aval

Rapport	Description
Détails de rapport	Affiche les éléments surveillés inclus dans le nombre indiqué dans la colonne des éléments surveillés

Domaine CAS Historique de l'hôte

Liste d'entités	Description du domaine
Host	Identifie un hôte CAS (serveur de base de données) et le statut en cours de CAS (en ligne/hors ligne). Cette entité est également disponible dans le domaine Configuration CAS
Host Event	Date et heure d'un événement dans une relation CAS client/serveur, détails d'un client ou d'un serveur qui passe à l'état en service ou hors service.

Entité Host

Attribut	Description
Host Name	Nom d'hôte du serveur de base de données
OS Type	Système d'exploitation : Unix ou Windows
Is Online	Statut en ligne en cours (Yes/No)

Entité Host Event

Attribut	Description
Event Time	Date et heure d'enregistrement de l'événement
Event Type	Identifie l'événement enregistré : "Client Down" : CAS s'est arrêté sur l'hôte du serveur de la base de données "Client Up" : CAS a démarré sur l'hôte du serveur de la base de données "Failover Off" : Un serveur est disponible (suite à une interruption), de sorte que les données CAS soient écrites sur ce serveur "Failover On" : Le serveur n'est pas disponible, les données CAS sont alors écrites dans le fichier de reprise en ligne "Server Down" : Le serveur de base de données s'est arrêté "Server Up" : Le serveur de base de données est démarré

Rapports par défaut CAS Host History Domain

Rapport par défaut	Description
Rapport CAS Historique de l'hôte	Affiche la liste des événements CAS pour chaque hôte CAS

Rapport CAS Historique de l'hôte

Entité	Attribut	Opérateur	Valeur par défaut
Host	Host_Name	Like	%
Host	OS_Type	Like	%
Host Event	Event_Type	Like	%

Domaine Changements de CAS

Entité	Description
Monitored Changes	Créé à chaque changement d'un élément surveillé
Host Configuration	Créé à chaque changement d'un élément surveillé
Saved Data	Contient les données sauvegardées des changements effectués

Entité Monitored Changes

Attribut	Description
Change Identifier	Identificateur unique correspondant au changement
Sample Time	Horodatage (date et heure sur l'hôte) de prélèvement de l'échantillon
Saved Data ID	Identifie l'entité Saved Data correspondant à ce changement
Audit State Label ID	Identifie l'entité Host Configuration correspondant à ce changement
Timestamp	Date et heure de création de l'enregistrement du changement sur le serveur (horloge du serveur de dispositif Guardium)
Owner	UNIX uniquement. Si le type d'élément est un fichier, il s'agit du propriétaire du fichier
Permissions	UNIX uniquement. Si le type d'élément est un fichier, il s'agit des droits d'accès au fichier
Size	Taille de fichier, mais il existe des valeurs spéciales, comme suit : -1, le fichier existe mais avec zéro octet 0, le fichier n'existe pas, mais ce nom de fichier fait l'objet d'une surveillance (il n'a jamais existé ou a éventuellement été supprimé)
Last Modified	Horodatage de la dernière modification, prélevée sur le système de fichiers au moment de l'échantillonnage
Last Modified Date	Date de la dernière modification
Last Modified Weekday	Jour de la semaine correspondant à la dernière modification
Last Modified Year	Année où a été effectuée la dernière modification
Group	UNIX uniquement. Si le type d'élément est un fichier, il s'agit du propriétaire du groupe

Entité Host Configuration

Attribut	Description
Audit State Label ID	Identificateur numérique unique de l'élément de configuration
Host Name	Nom d'hôte ou adresse IP du serveur de base de données
OS Type	Système d'exploitation : Unix ou Windows
DB Type	Type de base de données (Oracle, MS-SQL, DB2, Sybase, Informix, etc.) ou N/A si la modification concerne une instance de système d'exploitation
Instance Name	Nom d'instance du jeu de modèles
Type	Type d'élément surveillé ayant été modifié. Script de système d'exploitation ou script SQL : changement déclenché par le script de système d'exploitation inclus dans la définition de modèle de l'élément surveillé. Variable d'environnement : variable d'environnement (Unix uniquement) Variable de registre : variable de registre (Windows uniquement) Fichier : fichier spécifique. Il n'y a pas d'entité de configuration hôte pour un modèle de fichier défini dans le jeu de modèles utilisé par l'instance. Il existe à la place une entité de configuration hôte distincte pour chaque fichier correspondant au modèle.
Monitored Item	Nom de l'élément modifié, à partir de la description (si elle a été indiquée), autrement nom par défaut dépendant du type (par exemple, un nom de fichier).

Entité Saved Data

Attribut	Description
Saved Data ID	Identificateur numérique unique de l'élément Saved Data
Saved Data	Données réelles sauvegardées
Timestamp	Horodatage correspondant à l'enregistrement de l'entité Saved Data dans la base de données du serveur

Change Identifier	Identifie l'entité Monitored Changes correspondant à cette entité Saved Data

Rapports par défaut du domaine CAS Changes

Rapport par défaut	Description
CAS Change Details	Pour chaque élément surveillé, affiche la liste des modifications par propriétaire. Ce rapport répertorie les modifications des propriétés du fichier, par exemple le propriétaire ou les droits d'accès. Il n'indique pas les modifications apportées au contenu du fichier.
CAS Saved Data	Pour les éléments surveillés dont la case facultative Conserver les données est cochée, affiche les données de chaque modification détectée. Ce rapport affiche la liste des modifications apportées au contenu du fichier et non à ses propriétés.

Détails de CAS Changes

Entité	Attribut	Opérateur	Valeur par défaut
Host Configuration	DB_Type	Like	%
Host Configuration	Host_Name	Like	%
Host Configuration	Instance_Name	Like	%
Host Configuration	Monitored_Item	Like	%
Host Configuration	OS_Type	Like	%
Host Configuration	Type	Like	%

Rapports d'exploration en aval

Rapport	Description
Détails de l'enregistrement	Affiche les données sauvegardées incluses dans la colonne Nombre de données sauvegardées

CAS Données sauvegardées

Entité	Attribut	Opérateur	Valeur par défaut
Host Configuration	Host_Name	Like	%
Host Configuration	Monitored_Item	Like	%
Monitored Changes	Saved_Data_Id	Like	%

Rapports d'exploration en aval

Rapport	Description
Afficher la différence	Affiche la différence entre les données sélectionnées et la version précédente

Rubrique parent : Configuration Auditing System (CAS)

Statut CAS

Ouvrez le panneau Statut du système d'audit de configuration en cliquant sur Gestion > Surveillance des changements > Statut CAS

Pour chaque serveur de base de données sur lequel CAS est installé et s'exécute, et sur lequel ce système Guardium est configuré en tant qu'hôte Guardium actif, ce panneau affiche le statut CAS et le statut de chaque instance CAS configurée pour ce serveur de base de données.

Si vous rencontrez des difficultés pour effectuer la distinction entre les couleurs des voyants de statut, déplacez la souris sur ces voyants et une zone de texte affichera le statut en cours.

Composant	Description
Voyant de statut du système CAS	Le voyant trouvé sur ce panneau indique si CAS s'exécute de manière active sur le système Guardium. Rouge : CAS n'est pas en cours d'exécution sur ce système Guardium. Vert : CAS est actif sur ce système Guardium.
Voyants de statut de l'agent CAS	Ces voyants de statut indiquent si l'agent individuel CAS est connecté au système Guardium. Identifiez chaque agent CAS en référençant l'adresse IP qui apparaît avant la ligne des voyants de statut **Rouge** : l'hôte et/ou l'agent CAS est hors ligne ou inaccessible. **Vert** : l'hôte et l'agent CAS sont en ligne. **Jaune :** le système Guardium est un système secondaire pour l'hôte CAS.
Réinitialiser	Réinitialiser l'agent CAS sur ce système surveillé. Cette opération, arrête et redémarre l'agent CAS sur le serveur de base de données. Remarque : Les fichiers de point de contrôle sont eux aussi réinitialisés, ce qui permet de repartir sur de nouvelles bases et de réanalyser les fichiers en partant de zéro.
Supprimer (X)	Retirer ce système surveillé de CAS et supprimer également les données sur le système Guardium qui étaient associées au client CAS.

	Ce bouton est désactivé si l'agent CAS s'exécute sur ce système. Vous devez arrêter l'agent CAS pour pouvoir effectuer la suppression. Voir Arrêt et redémarrage de l'agent CAS pour plus d'informations.
Voyant rouge/jaune/vert	Chaque ensemble de voyants indique le statut d'une instance CAS sur le système surveillé. Si le statut du système surveillé propriétaire est rouge (ce qui indique que l'agent CAS est hors ligne), ignorez cet ensemble de voyants de statut. **Rouge** : l'instance est désactivée. **Vert** : l'instance est activée et en ligne. Sa configuration est synchronisée avec celle du système Guardium. **Jaune** : l'instance est activée, mais sa configuration sur le système Guardium ne correspond pas à la configuration de l'instance sur le système surveillé (elle a été mise à jour sur le système Guardium, mais cette mise à jour n'a pas été appliquée sur le système surveillé).
Actualiser	Cliquez sur Actualiser pour vérifier à nouveau le statut de tous les serveurs dans la liste. Ce bouton n'arrête pas et ne redémarre pas CAS sur un serveur de base de données (il ne fait que vérifier la connexion entre CAS sur le système Guardium et CAS sur chaque serveur de base de données).

Remarque : L'entrée TAP_IP dans le fichier guard_tap.ini est obligatoire. Si l'entrée TAP_IP est manquante, CAS ne démarre pas et un message d'erreur est consigné dans le fichier journal sur le client CAS.

Arrêt et démarrage de l'agent CAS

Il existe plusieurs situations où vous serez peut-être amené à arrêter ou démarrer l'agent CAS sur un système surveillé.
Remarque : Si vous voulez arrêter et redémarrer l'agent CAS, vous pouvez le faire en cliquant sur Gestion > Surveillance des changements > Statut CAS.

Arrêt de CAS sur un hôte UNIX

1. Editez le fichier /etc/inittab.
2. Recherchez la ligne CAS respawn :

```
cas:2345:respawn:/usr/local/guardium/guard_stap/cas/bin/run_wrapper.sh /usr/local/guardium/guard_stap/cas/bin
```

3. Mettez en commentaire cette ligne en insérant le caractère # à l'emplacement du premier caractère.
4. Sauvegardez le fichier.
5. Entrez la commande suivante : init -q
6. Entrez la commande suivante : ps -er | grep cas
7. Notez l'ID de processus (PID) de chaque processus répertorié.
8. Pour chaque processus répertorié, exécutez la commande suivante : kill -9 <pid>
9. Dans le panneau Statut de Configuration Auditing System du portail d'administration Guardium, le voyant de statut de cet hôte CAS doit être rouge et le bouton Retirer doit être activé. Cela vous permet de retirer les données de cet hôte CAS à partir de la base de données interne du système Guardium.

Démarrage de CAS sur un hôte Unix

Utilisez cette procédure pour redémarrer l'agent CAS uniquement lorsqu'il a été arrêté en éditant le fichier /etc/inittab comme indiqué précédemment.

1. Editez le fichier /etc/inittab.
2. Recherchez la ligne :

```
#cas:2345:respawn:/usr/local/guardium/guard_stap/cas/bin/run_wrapper.sh /usr/local/guardium/guard_stap/cas/bin
```

3. Supprimez la mise en commentaire de la ligne (voir notre exemple à l'étape 2.), en retirant # à l'emplacement du premier caractère. En fonction du système d'exploitation, le caractère de mise en commentaire peut être différent.
4. Sauvegardez le fichier.
5. Entrez la commande suivante pour redémarrer l'agent CAS : init -q

Démarrage et arrêt de CAS sur un hôte Windows

Sur Windows, CAS s'exécute en tant que service système.

1. Dans le panneau Services, mettez en évidence l'élément Configuration Auditing System Client.
2. Sélectionnez Démarrer ou Arrêter dans le menu Action.

Rubrique parent : Configuration Auditing System (CAS)

Configuring your Guardium system

You can configure several aspects of your Guardium system to enable you to meet your business goals effectively and efficiently.

- System Configuration
  Most of the information on the System Configuration panel is set by using the CLI at installation time.
- Inspection Engine Configuration
  An inspection engine monitors the traffic between a set of one or more servers and a set of one or more clients using a specific database protocol (Oracle or Sybase, for example).
- Portal Configuration
  You can keep the Guardium® appliance Web server on its default port (8443) or reset the portal. We strongly recommend that you use the default port.
- Managing the TLS version
  You can disable TLS 1.0/1.1, and enable TLS 1.2 on all appliances, S-TAP agents, CAS and GIM clients.
- Generate New Layout
- Configure Authentication
  By default, Guardium user logins are authenticated by Guardium, independent of any other application.
- Global Profile
  The Global Profile panel defines defaults that apply to all users.
- Alerter Configuration
  No e-mail messages, SNMP traps, or alert related Syslog messages will be sent until the Alerter is configured and activated.
- Anomaly Detection
  The Anomaly Detection process runs every polling interval to create and save, but not send, correlation alert notifications that are based on an alert's query.

- Session Inference
  Session Inference checks for open sessions that have not been active for a specified period of time, and marks them as closed.
- Block S-TAP connection to Guardium (S-TAP Certification)
  Use this function to control the specific S-TAP hosts whose clients are allowed access to the Guardium system.
- IP to Hostname Aliasing
  The IP-to-Hostname Aliasing function accesses the Domain Name System (DNS) server to define hostname aliases for client and server IP addresses.
- System Backup
  Use the System Backup function to define a backup operation that can be run on demand or on a scheduled basis. Use the Patch Backup function to create the backup profile settings.
- Configuring patch backup
  Use this feature to store backup profile information.
- Configure Permission to Socket connection
  This topic applies to Custom Alerting Classes.

System Configuration

Most of the information on the System Configuration panel is set by using the CLI at installation time.

For instructions on how to configure the system, or to modify any other System Configuration settings, see Modify the System Configuration.

There must be a valid license to use various functions within the appliance. When a license is entered after the system starts, a restart of the GUI is needed.

About System Shared Secret

The Guardium® administrator defines the system shared secret in the System Configuration. The system shared secret is used for two general purposes:

- To encrypt files that are exported from the appliance by archive/export activities
- To establish secure communications between Central Managers and managed units

If you are using Central Management and/or aggregation, you must set the System Shared Secret for all related systems to the same value.

The system shared secret value is null at installation time. Depending on a company's security practices, it may be necessary to change the system shared secret on a periodic basis. Each appliance maintains a shared secret keys file, containing an historical record of all shared secrets defined on that appliance. The same system thus will have no problem at a later date decrypting information that has been encrypted on that system.

When information is exported or archived from one system, and imported or restored on another, the latter must have access to the shared secret used by the former. For these cases, there are CLI commands that can be used to export the system shared secrets from one Guardium system, and import them on another.

See the following commands in the CLI appendix:

- aggregator backup keys file
- aggregator restore keys file

Modifying the System Configuration

1. Click Setup > Tools and Views > System to open the System Configuration.
2. Make your changes.
3. Click Apply to save the updated system configuration.

Note: The applied changes do not take effect until the Guardium system is restarted. After you apply configuration changes, click Restart to stop and restart the system.

Table 1. System Configuration Panel Reference

Field or Control	Description
Unique Global Identifier	This value is used for collation and aggregation of data. The default value is a unique value that is derived from the MAC address of the machine. Do not change this value after the system begins monitoring operations.
System Shared Secret	Any value that you enter here is not displayed. Each character you type is masked. The system shared secret is used for archive/restore operations, and for Central Management and aggregation operations. When used, its value must be the same for all units that will communicate. This value is null at installation time, and can change over time. The system shared secret is used: • When secure connections are being established between a Central Manager and a managed unit. • When an aggregated unit signs and encrypts data for export to the aggregator. • When any unit signs and encrypts data for archiving. • When an aggregator imports data from an aggregated unit. • When any unit restores archived data. Depending on your company's security practices, you might be required to change the system shared secret from time to time. Because the shared secret can change, each system maintains a shared secret keys file, containing a historical record of all shared secrets defined on that system. This allows an exported (or archived) file from a system with an older shared secret to be imported (or restored) by a system on which that same shared secret has been replaced with a newer one. **Caution**: When used, be sure to save the shared secret value in a safe location. If you lose the value, you will not be able to access archived data.
Retype Secret	When you enter or change the system shared secret, retype the new value a second time. Any value that you enter here is not displayed. Each character you type is displayed as an asterisk.

Field or Control	Description
License Key	The license key is inserted in the configuration during installation. Do not modify this field unless you are instructed to do so by Technical Support. You might need to paste a new product key here if optional components are being added. If you install a new product key on the central management unit, when you click Apply, you will receive a warning message that reads: `Warning: changing the license on a Central Management Unit requires refreshing all managed units`. After you click OK to close the message window, you must click Apply a second time to install the new product key. You will know that the new license has been installed when you receive the message: `Data successfully saved`. If you install a new product key on a Central Management Unit, you might get a warning that states the license applied to the CM must be refreshed on the managed unit. This requires a refresh done from the Central Manager and is done by pressing the refresh icon from the Central Manager to each of the collectors listed. License entitles user to access products and the corresponding features. License can be appended or overridden. Active license is stored in LICENSE_KEY in ADMINCONSOLE_PARAMETER Product types DAM; FAM; VA Edition for product types: Express; Standard; Advanced
Number of Datasources	If a limited license is applied, the maximum number of datasources permitted per datasource license is displayed.
Metered Scans Left	If a limited license is applied, the number of vulnerability assessment scans permitted (datasource metering) per metering license is displayed. Each time a vulnerability assessment is triggered, the scan counter decreases by one.
License valid until	If a limited license is applied, a fixed date when the license will be disabled is displayed.
# of Licenses	This value indicates the number of licenses remaining.
Note: Configure Network Address, Secondary Management Interface and Routing settings using the CLI	These settings cannot configured through the GUI and appear grayed-out on the System Configuration user interface.
System Hostname	The resolvable host name for the Guardium system. This name must match the DNS host name for the primary System IP Address.
Domain	The name of the DNS domain on which the Guardium system resides.
System IP Address	The primary IP address that users and S-TAP® or CAS agents use to connect to the Guardium system. It is assigned to the network interface labeled ETH0.
SubNet Mask	The subnet mask for the primary System IP Address.
Hardware (MAC) Address	The MAC address for the primary network interface.

Field or Control	Description

System IP Address (Secondary)	Optional: A port can also be configured to team with the primary interface in order to provide high-availability failover IP teaming.
	
	Alternatively, a port on the device can be configured as a secondary management interface with a different IP address, network mask, and gateway from the primary.
	
	These two options are mutually exclusive.
	
	There are two different, and mutually exclusive, kinds of secondary management connections, both controlled by options to the same CLI command:
	
	Bonding or teaming
	Turns eth0 and another specified network interface card (NIC) into a bonded pair with standby failover. To implement this option, use the CLI command store network interface high-availability on <nic>, where nic is an available NIC.
	Secondary interface
	Allows the GUI and CLI to be accessible from another NIC in the Guardium system. To implement this option, use the CLI command store network interface secondary on <nic> <ip> <mask> <gateway> to specify the secondary NIC, its IP address and network mask, and optionally a gateway.
	
	BOTH physical and VM systems have the same capabilities. dependent on the number of NICs installed on the Guardium system or VM.
	
	To display the network interfaces installed on the unit, use the **show network interface inventory** CLI command. For example:
	
	`show network interface inventory`
	`Current network card configuration:`
	`Device | Mac Address |Member of`
	`----------`
	`eth0 | 00:50:56:3b:c3:73 |`
	`eth1 | 00:50:56:8a:0d:fa |`
	`eth2 | 00:50:56:8a:0d:fb |`
	`eth3 | 00:50:56:8a:00:c1 |`
	
	Note: The "Member of" will show which NICs are in a bond pair, if a bonding exists.
	
	To locate the eth connectors on your appliance, use the **show network interface port** CLI command, which will blink the orange light on that port, 20 times. For example:
	
	guard14.xyz.com> sho net int port 3
	
	The orange light on port eth5 will now blink 20 times.
	
	Note: The secondary IP address and its associated port are NOT related to the high availability feature, which provides fail-over support via IP Teaming for the primary connection. For more information about the high-availability option, see the **store network interface** commands in the CLI Appendix.

SubNet Mask (Secondary)	Optional. The subnet mask for the secondary System IP Address.
Default Route/ Secondary Route	The IP address of the default router for the system./ The IP address of the Secondary Router
Primary Resolver Secondary Resolver Tertiary Resolver	The IP address for the Primary Resolver (DNS) is required. The secondary and tertiary are optional.
Test Connection	Click Test Connection to test the connection to the corresponding DNS (Domain Name System) server. This only tests that there is access to port 53 (DNS) on the specified host. It does not verify that this is a working DNS server. You will receive a message box indicating if the DNS server responded.
Stop	Click Stop to shut down the system.
Restart	Click Restart to stop and then restart the system. You will be prompted to confirm the action.
Apply	Click Apply to save the changes. The changes will be applied the next time the system restarts.

Parent topic: Configuring your Guardium system

Inspection Engine Configuration

An inspection engine monitors the traffic between a set of one or more servers and a set of one or more clients using a specific database protocol (Oracle or Sybase, for example).

The inspection engine extracts SQL from network packets; compiles parse trees that identify sentences, requests, commands, objects, and fields; and logs detailed information about that traffic to an internal database.

You can configure and start or stop multiple inspection engines on the Guardium® appliance.

Inspection engines cannot be defined or run on a Central Manager unit. However, you can start and stop inspection engines on managed units from the Central Manager control panel.

Inspection engines are also defined on S-TAPs. If S-TAPs report to this Guardium appliance, be sure the appliance does not monitor the same traffic as the S-TAP®. If that happens, the analysis engine will receive duplicate packets, will be unable to reconstruct messages, and will ignore that traffic.

Selecting IP addresses

Each inspection engine monitors traffic between one or more client and server IP addresses. In an inspection engine definition these are defined using an IP address and a mask. You can think of an IP address as a single location and a mask as a wild-card mechanism that allows you to define a range of IP addresses.

IP addresses have the format: n.n.n.n, where each n is an eight-bit number (called an octet) in the range 0-255.

For example, an IP address for your PC might be: 192.168.1.3. This address is used in the examples. Since these are binary numbers, the last octet (3) can be represented as: 00000011.

The mask is specified in the same format as the IP address: n.n.n.n. A zero in any bit position of the mask serves as a wildcard. Thus, the mask 255.255.255.240 combined with the IP address 192.168.1.3 matches all values from 0-15 in the last octet, since the value 240 in binary is 11110000. But it only matches the values 192.168.1 in the first three octets, since 255 is all 1s in binary (in other words, no wildcards apply for the first three octets).

Specifying binary masks can be a little confusing. However, for the sake of convenience, IP addresses are usually grouped in a hierarchical fashion, with all of the addresses in one category (desktop computers, for example) grouped together in one of the last two octets. Therefore, in practice, the numbers you see most often in masks are either 255 (no wildcard) or 0 (all).

Thus a mask 255.255.255.255 (which has no zero bits) identifies only the single address specified by IP address (192.168.1.3 in the example).

Alternatively, the mask 255.255.255.0, combined with the same IP address matches all IP addresses beginning with 192.168.1.

Selecting all addresses

The IP address 0.0.0.0, which is sometimes used to indicate all IP addresses, is not allowed by Guardium. To select all IP addresses when using an IP address/mask combination, use any non-zero IP address followed by a mask containing all zeroes (for example: 1.1.1.1/0.0.0.0). However, 0.0.0.0/0.0.0.0 is a valid combination.

Configure Settings that apply to all Inspection Engines

1. Click Manage > Activity Monitoring > Inspection Engines to open the Inspection Engine Configuration.
2. Refer to the table and make any changes desired.
3. Click Apply to save the updated system configuration when you are done making changes.
4. Optionally add comments to the Inspection Engine Configuration.
5. Click Restart Inspection Engines.

Note: The applied changes do not take effect until the inspection engines are restarted. After applying inspection engine configuration changes, click the Restart button to stop and restart the system (using the new configuration settings).
Note: For HTTP support, there are Inspection Engine configuration limitations. The following Inspection Engine settings are not supported for HTTP: Default Capture Value; Default Mark Auto Commit; Log Sequencing; Log Exception Sql String; Log Records Affected; Compute Avg. Response Time; Inspect Returned Data; Record Empty Sessions.

Table 1. Settings that Apply to All Inspection Engines

Control	Description
Default Capture Value	Default value is false. Used by Replay function to distinguish between transactions and capture values, meaning that if you have a prepared statement, assigned values will be captured and replayed. If you want to replay your captured prepared statements as prepared statements the check box should be checked for the captured data.
Default Mark Auto Commit	Default value is true. Due to various auto-commit models for different databases, this value is used by Replay function to explicitly mark up the transactions and auto commit after each command. Note: If the check box is checked then commits and rollbacks will be ignored. Databases currently supported include DB2®, Informix®, and Oracle.
Log Sequencing	If marked, a record is made of the immediately previous SQL statement, as well as the current SQL statement, provided that the previous construct occurs within a short enough time period.
Log Exception Sql String	If marked, when exceptions are logged, the entire SQL statement is logged.
Log Records Affected	Records affected - Result set of the number of records which are affected by each execution of SQL statements. If marked, the number of records affected is recorded for each SQL statement (when applicable). Default value for log records affected is FALSE (0). Note: When using JDBC, this must be marked to properly log Oracle bind variable traffic Note: The records affected option is a sniffer operation which requires sniffer to process additional response packets and postpone logging of impacted data which increases the buffer size and might potentially have a adverse effect on overall sniffer performance. Significant impact comes from really large responses. To prevent large amount of overhead associated with this operation, Guardium uses a set of default thresholds that allows sniffer to decide to skip processing operation when exceeded. Note: Usually, Records Affected is set correctly when the user turns on Log Records Affected via Inspection Engines > Log Records Affected. However using MS-SQL via stored procedure will set Records Affected as -1. Refer to Configuration and Control CLI Commands store max_results_set_size, store max_result_set_packet_size and store max_tds_response_packets, to set levels of granularity. Example of result set values: • Case 1, record affected value, positive number - this represents correct size of the result set. • Case 2, record affected value, -2 - This means number of records exceeded configurable limit (This can be tuned through CLI commands). • Case 3, record affected value, -1 - This shows any unsupported cases of packets configurations by Guardium. • Case 4, record affected value, -2 - If the result set is sent by streaming mode. • Case 5, record affected value, -2 - Intermediate result during record count to update user about current value, ends up with positive number of total records. Note: Records Affected feature is not supported in DB2 when streaming to used to send the results.
Compute Avg Response Time	When marked, for each SQL construct logged, the average response time will be computed.
Inspect Returned Data	Mark to inspect data returned by SQL requests as well as update the ingress and egress counts. If rules will be used in the security policy, this checkbox must be marked.
Record Empty Sessions	When marked, sessions containing no SQL statements will be logged. When cleared, these sessions will be ignored.

Control	Description
Parse XML	The Inspection Engine will not normally parse XML traffic. Mark this checkbox to parse XML traffic.
Logging Granularity	The number of minutes (1, 2, 5, 10, 15, 30, or 60) in a logging unit. If requested in a report, Guardium summarizes request data at this granularity. For example, if the logging granularity is 60, a certain request occurred n times in a given hour. If the check box is not marked, exactly when the command occurred within the hour is not recorded. But, if a rule in a policy is triggered by a request, a real time alert can indicate the exact time. When you define exception rules for a policy, those rules can also apply to the logging unit. For example, you might want to ignore 5 login failures per hour, but send an alert on the sixth login failure.
Max. Hits per Returned Data	When returned data is being inspected, indicate how many hits (policy rule violations) are to be recorded.
Ignored Ports List	A list of ports to be ignored. Add values to this list if you know your database servers are processing non-database protocols, and you want Guardium to not waste cycles analyzing non-database traffic. For example, if you know the host on which your database resides also runs an HTTP server on port 80, you can add 80 to the ignored ports list, ensuring that Guardium will not process these streams. Separate multiple values with commas, and use a hyphen to specify an inclusive range of ports. For example: 101,105,110-223
Buffer Free: n %	Display only. **n** is the percent of free buffer space available for the inspection engine process. This value is updated each time the window is refreshed. There is a single inspection engine process that drives all inspection engines. This is the buffer used by that process.
Restart Inspection Engines	Click Restart Inspection Engines to stop and restart all inspection engines.
Add Comments	Click Comment to add comments to the Inspection Engine Configuration.
Apply	Click the Apply to save the configuration. Note: Any global changes made (and saved by using Apply) do not take effect until you restart the inspection engines. However, individual inspection engine attributes, such as exclude, sequence order, etc., take effect immediately.

Create an Inspection Engine

1. Click Manage > Activity Monitoring > Inspection Engines to open Inspection Engines.
2. Click Add Inspection Engine to expand the panel.
3. Enter a name in the Name box. It must be unique on the appliance. We recommend that you use only letters and numbers in the name, as the use of any special characters prevents working with this inspection engine via the CLI.
4. From the Protocol box, select either the protocol to be monitored (Aster, Cassandra, CouchDB, DB2, DB2 Exit, exclude IE, FTP, GreenPlumDB, Hadoop, HIVE, HTTP, HUE, IBM ISERIES, IMPALA, Informix, iNFORMIX Exit, KERBEROS, Maria,DB, MongoDB, MS SQL, Mysql, Named Pipes, Netezza, Oracle, PostgreSQL, SAP Hana, Sybase, Teradata, WebHDFS or Windows File Share) or the keyword exclude IE. Select exclude IE if you want all traffic between the specified clients and servers to be ignored.
   Note: Exclude IE only works on ports, IP does not matter. Enter a range of ports to ignore. To exclude a specific IP for this port, the exclude DB Client IP can be used within the inspection engine created. If there is a need not to pick up packets on a certain port range, define a separate inspection engine of the type Exclude IE (IGNORE). The only values that have to be defined in that engine are PORT_RANGE_START and PORT_RANGE_END. This kind of exclusion might be needed, for instance, when an all-inclusive Oracle Inspection Engine is defined with ports range 1024-65535, but certain ports have to be excluded. When using Oracle for Windows, expand the port range to 1000 to 65535.
   Note: When sending IPC traffic from the GreenPlum database, it will be logged on the Guardium system as PostgresSQL traffic. When sending TCP traffic from the GreenPlum database, it will be logged on as GreenPlum database with the inspection engine. For TCP traffic, Guardium determines the database according to the Port (port 5432 for GreenPlum). For IPC traffic, Guardium is using named pipe, and for GreenPlum database, the Guardium system is using PostgresSQL as the name of the database. When both PostgresSQL and Greenplum database are on the same system, their IPC traffic will log in DB_PROTOCOL according to the first PostgresSQL/Greenplum database IE set in the guard_tap.ini file.
5. In the DB Client IP/Mask boxes, enter a list of clients (a client host from which the database connection was initiated) to be monitored (or excluded if the Exclude DB Client IP box is marked). The clients are identified by IP addresses and subnet masks. There are detailed instructions on how to use these fields in the overview.

   Click the plus sign to add additional IP address and subnet mask. Click the minus sign to remove the last IP address and subnet mask.

6. In the DB Server IP/Mask boxes, enter a list of database servers (where a database sits) to be monitored. The servers are identified by IP addresses and subnet masks. There are detailed instructions on how to use these fields in the overview.

   Click the plus sign to add additional IP address and subnet mask. Click the minus sign to remove the last IP address and subnet mask.

7. In the Port box, enter a single port or a range of ports over which traffic between the specified clients and database servers will be monitored. Most often, this should be a single port.

   Warning: Do not enter a wide range of ports, just to be certain that you have included the correct one! You may cause the inspection engine to bog down attempting to analyze traffic on ports that carry no database traffic or traffic that is of no interest for your environment.

8. Mark the Active on startup box if this inspection engine should be started automatically on start-up.
9. Mark the Exclude DB Client IP box if you want the inspection engine to monitor traffic from all clients except for those listed in the DB Client IP/Mask list. Be sure that you understand the difference between this and the Ignore protocol selection. This includes all traffic except for the from IP addresses. To ignore a specific set of clients without including all other clients, define a separate inspection engine for those clients and use the Ignore protocol.
10. Click Add to save the definition.
11. Optionally reposition the inspection engine in the list of inspection engines. Filtering mechanisms defined in the inspection engines are executed in the order. If necessary, reposition the new inspection engine configuration, or any existing configurations, using the Up and/or Down buttons in the border of the definition.
12. Optionally click Start to start the inspection engine just configured. The Start button will be replaced by a Stop button, once the engine has been started.
13. Note: If you provide a value for TAP_IDENTIFIER and the value contains spaces, Guardium will automatically replace the spaces with hyphens. For example, the value "Sample description" will become "Sample-description".

Start or Stop an Inspection Engine

Click Manage > Activity Monitoring > Inspection Engines to open the Inspection Engines. To start an inspection engine, click Start. To stop an inspection engine, click Stop.

Remove an Inspection Engine

If you are no longer using an inspection engine, we suggest that you remove the definition, so that it is not restarted accidentally.

1. Click Manage > Activity Monitoring > Inspection Engines to open the Inspection Engines.
2. If the inspection engine to be removed has not been stopped, click Stop.
3. To remove an inspection engine, click Delete.

Parent topic: Configuring your Guardium system

Portal Configuration

You can keep the Guardium® appliance Web server on its default port (8443) or reset the portal. We strongly recommend that you use the default port.

1. Click Setup > Tools and Views > Portal to open the Portal.
2. If it is not marked, mark the Active on Startup checkbox (this should never be disabled).
3. Set the HTTPS Port to an integer value between 1025 and 65535.
4. Click Apply to save the value. (The Guardium security portal will not start listening on this port until it is restarted.) Or click Revert to restore the value stored by the last Apply operation.
5. Click Restart to restart the Guardium Web server if you have made and saved any changes. You can now connect to the unit on the newly assigned port.
   Note: To re-connect to the unit after it has restarted with the new port number, you must change the URL used to open the Guardium Login Page on your browser.

The Guardium Portal Configuration is used to define the way user passwords are authenticated when logging into the Guardium appliance. There are three choices.

These choices are Local (Guardium Default), RADIUS or LDAP.

The Portal configuration screen under Setup > Tools and Views > Portal is used for the following:

1. To define the best way to authenticate a user password.
2. To restart GUI to reset the authentication type.

The Local connection will work when a password for a given user is defined from a login. The login is defined using the accessmgr role. By default login into the **accessmgr** account which has the accessmgr role. This role gives a user the ability to add or uploaded user accounts and create passwords.

When you define your username and password using the accessmgr role type, the defined password per user will be used when logging into the Guardium appliance.

The RADIUS connection allows login authentication through a radius server. The Radius/RSA server can be defined using both a password and a SecurID token number. The SecurID token numeric password is displayed via a hardware token.

The Radius/RSA server is defined on a Windows server. The security RSA SecurID token is also defined and stored on the Radius server and does not have to be downloaded in order for the Radius portal to work.

In addition, a Radius server connection can be defined using a UNIX platform. Radius is also defined as FreeRadius. User account and passwords are defined on the Radius servers and do not have to be downloaded. In order to use FreeRadius, the client (Guardium server), username and passwords are defined on the FreeRadius UNIX servers and used when the Radius Portal connection is defined.

The default portal is set to Local.

The LDAP connection will work when the password is defined and stored on a given LDAP server. In order for a user to use the LDAP portal and to login, a user account name must be imported from **the LDAP server** first. Use the User LDAP Import function available from the accessmgr account to define the LDAP location and then import the LDAP users. The password does not have to be uploaded.

Parent topic: Configuring your Guardium system

Managing the TLS version

You can disable TLS 1.0/1.1, and enable TLS 1.2 on all appliances, S-TAP agents, CAS and GIM clients.

About this task

This feature was introduced in v10.1.4.

To increase the security of the Guardium system, from Guardium release v10.1.4, communications protocols TLS 1.0/1.1 can be optionally disabled. Disabling TLS 1.0/1.1 results in only the TLS 1.2 protocol being enabled. Communications may be less secure when using TLS 1.0/1.1.

You must disable TLS 1.0/1.1 from the Central Manager and/or standalone unit using the CLI. Your Guardium appliances, S-TAP agents, CAS and GIM clients must be at specific versions to enable this feature.

The disablement of TLS 1.1 automatically checks to make sure managed units and S-TAPs are at specific versions, but cannot check CAS client versions. Customers using CAS need to make sure their CAS clients are at version 10.1.4 and their database servers have Java 7 enabled. Lack of doing this will result in the inability to see CAS connections to database servers.

You must also make sure all managed units have version 10.1.4 installed, and GIM Clients and S-TAPs are at a minimum version of 10.1.2. Failure to meet all requirements will mean that TLS 1.0/1.1 will not be disabled.

To get information about, and to disable TLS1.0/1.1 on all units in a managed environment, (Central Manager, Aggregator, Managed units), the following commands should be run on the Central Manager.

Procedure

1. Access the CLI as admin.
2. Enter the following command.

```
grdapi get_secured_protocols_info
```

Running this command from a Central Manager to propagate down to all managed units. The system outputs the enabled protocols (TLS 1.0/1.1 and TLS 1.2) and indicates if the TLS 1.0/1.1 protocols can be disabled. Error codes 1000+ indicate an issue with a component that needs to be addressed by the admin before TLS 1.0/1.1 can be disabled. Messages are displayed indicating which component(s) do not meet the requirements for disabling TLS 1.0/1.1. Warning messages are generated for managed units that are offline or unreachable. Offline units must be managed individually when they come back online.

3. To disable TLS 1.0/1.1, enter:

```
grdapi disable_deprecated_protocols
```

Running this command from a Central Manager to propagate down to all managed units. This command firsts run the version checks described above. If the requirements for disablement are met, then this command changes the configuration settings for each service on the Central Manager as well as all managed units. If the requirements for disablement are not met, then the system indicates that the deprecated protocols are enabled and must be kept enabled until all managed units and/or components are upgraded.

4. For any managed unit that was offline during the disablement of depreciated protocols, Guardium users with admin role must manually start a CLI session on the managed unit and execute local_disable_depreciated_protocols to make the configuration changes.

   ```
   grdapi local_disable_deprecated_protocols
   ```

5. To revert to TLS 1.0/1.1, enter

   ```
   grdapi enable_deprecated_protocols all=true
   ```

   This GuardAPI command is a fallback that changes back the configuration settings and restart services on the Central Manager and all managed units to enable the deprecated protocols. This GuardAPI command can be run with the all=true argument from a Central Manager to enable deprecated protocols on the Central Manager and all managed units. Absence of the parameter all=true enable deprecated protocols on the appliance running the GuardAPI only.
6. Guardium users with admin role should check that communications between Central Managers and managed units are stable and working properly.

Parent topic: Configuring your Guardium system

Generate New Layout

Generate a new layout for a role based on a user layout

The Guardium® administrator or access manager can generate, via CLI, a default layout for a role. After that, any new user who is assigned that role will have that layout after logging in for the first time.

Note: Default .psml structures for user and role can be defined, via the GUI, by the admin user. See Portlet Editor for further information.

Use the generate-role-layout CLI command to generate a new layout for an existing role, based on the layout for the specified user. Once the new role layout has been defined, any users who are assigned that role before they log in for the first time, will receive the layout for that role.

generate-role-layout

Syntax generate-role-layout <user> <role>

Note: user (login name) and role are not case-sensitive.

Parameters

If either of the following parameters contains spaces (John Doe is user , or DBA Managers is role), replace the space characters with underscore characters.

For example:

generate-role-layout John_Doe DBA_Managers

user - The name of the user whose layout will be used as a model for the role layout. If the user does not exist, you will receive the following error message: `No such user '<user>'.`

role - The role to which the new layout will be attached.

Parent topic: Configuring your Guardium system

Configure Authentication

By default, Guardium® user logins are authenticated by Guardium, independent of any other application.

For the Guardium admin user account, login is always authenticated by Guardium alone. For all other Guardium user accounts, authentication can be configured to use either RADIUS or LDAP. In the latter cases, additional configuration information for connecting with the authentication server is required.
Note: FreeRadius client software is supported.

When an alternative authentication method is used, all Guardium users must still be defined as users on the Guardium appliance. It is only the authentication that is performed by another application.

While user accounts and roles are managed by the accessmgr user, the authentication method used is managed by the admin user. This is a standard separation-of-duties best practice.

To configure authentication, see the proceeding topic.

Configure Guardium Authentication

1. Click Setup > Tools and Views > Portal to open the Authentication Configuration.
2. Select the Guardium radio button in the Authentication Configuration panel.
3. Click Apply.

Configure RADIUS Authentication

1. Click Setup > Tools and Views > Portal to open the Authentication Configuration.
2. Select the RADIUS radio button in the Authentication Configuration panel. Additional fields will appear in the panel.
3. In the Primary Server box, enter host name or IP address of the primary RADIUS server.
4. Optionally enter the host name or IP address of the secondary and tertiary RADIUS servers.
5. Enter the UDP Port used (1812 or 1645) by RADIUS.
6. Enter the RADIUS server Shared Secret, twice.
7. Enter the Timeout Seconds (the default is 120).
8. Select the Authentication Type:
    - PAP - password authentication protocol
    - CHAP - Challenge-handshake authentication protocol
    - MS-CHAPv2 - Microsoft version 2 of the challenge-handshake authentication protocol
9. Optionally click Test to verify the configuration. You will be informed of the results of the test. The configuration will also be tested whenever you click the Apply button to save changes.
10. Click Apply. Guardium will attempt to authenticate a test user, and inform you of the results.

Configure LDAP Authentication

1. Click Setup > Tools and Views > Portal to open the Authentication Configuration.
2. Select the LDAP radio button in Authentication Configuration.
3. In the Server box, enter the host name or IP address of the LDAP server.
4. Enter the Port number (the default is 636 for LDAP over SSL).
5. Enter the User RDN Type (relative distinguished name type) type, which is uid by default.
   Note:

   This attribute identifies a user for LDAP authentication. The Access Manager should be made aware of what attribute is used here, since the Access Manager performs the LDAP User Import operation. Click on this help link LDAP User Import for further information on Importing LDAP Users.

   If a user is using SamAccountName as the RDN value, the user must use either a =search or =[domain name] in the full name.

   Examples: SamAccountName=search, SamAccountName=dom

6. Enter the User Base DN (distinguished name).
7. Mark or clear the Use SSL checkbox, as appropriate for your LDAP Server.
8. Optional. To inspect one or more trusted certificates, click Trusted Certificates and follow the instructions in that panel.
9. Optional. To add a trusted certificate, click Add Trusted Certificates and follow the instructions in that panel.
10. Optional. Click Test to verify the configuration. You will be informed of the results of the test. The configuration will also be tested whenever you click Apply to save changes.
11. Click Apply. Guardium will attempt to authenticate a test user, and inform you of the results.

Parent topic: Configuring your Guardium system

Global Profile

The Global Profile panel defines defaults that apply to all users.

Override the Default Aliases Setting

By default, for any new report, or for any report that is contained in a default layout, aliases are not used.

An alias provides a synonym that substitutes for a stored value of a specific attribute type. It is commonly used to display a meaningful or user-friendly name for a data value. For example, Financial Server might be defined as an alias for IP address 192.168.2.18.

If you want to see aliases by default, you can change the default aliases setting for all reports, as follows:

- Click Setup > Tools and Views > Global Profile to open the Global Profile.
- Mark the Use Aliases in Reports unless otherwise specified check box.
- Click Apply.

Customize the PDF Page Footer

PDF files created by various Guardium® components (audit tasks, for example) have a standard page footer. To customize that footer:

1. Click Setup > Tools and Views > Global Profile to open the Global Profile.
2. In the PDF Footer Text field, enter the text to be printed at the foot of each page.
   Note: PDF footer text is not distributed from the Central Manager/ Aggregator to the Managed Units.
3. Click Apply.

Edit the Alert Message Template

To customize the message template used to generate alerts:

1. Click Setup > Tools and Views > Global Profile to open the Global Profile.
2. In the Message Template text box, edit the alert template text.

   You can mark the no wrap check box to see where the line breaks appear in the message.

3. Click Apply when you are done.
4. Changes will not take effect until the inspection engines are restarted. To do that now, click Manage > Activity Monitoring > Inspection Engines to open the Inspection Engines. Click Restart Inspection Engines.

Table 1. Alert Message Template Variables

Variable	Description
%%addBaselineConstruct	To add to baseline Attention: The Baseline Builder and related functionality is deprecated starting with Guardium V10.1.4.
%%AppUserName	Application user name
%%AuthorizationCode	Authorization code
%%category	Category from the rule definition
%%classification	Classification from the rule definition
%%clientHostname	Client host name
%%clientIP	Client IP address
%%clientPort	Client port number
%%DBName	Database name
%%DBProtocol	Database protocol
%%DBProtocolVersion	Database protocol version
%%DBUser	Database user name
%%lastError	Last error description; available only when a SQL error request triggering an exception rule contains a last error description field
%%netProtocol	Network protocol, for K-TAP on Oracle, this may display as either IPC or BEQ
%%OSUser	Session information. (OS_USER in GDM_ACCESS)
%%receiptTime	Timestamp representing the time when the alert occurred
%%receiptTimeMills	Numeric representing the time when the alert occurred, in milliseconds since the fixed date of Jan 1 1900
%%requestType	Request type
%%ruleDescription	The rule description from the policy rule definition
%%ruleID	The rule number from the rule definition
%%serverHostname	Server hostname
%%serverIP	Server IP address
%%serverPort	Server port number
%%serverType	The database server type
%%serviceName	Service name
%%sessionStart	Session start time (login time)
%%sessionStartMills	Numeric representing the start of the session where the alert occurred, in milliseconds since the fixed date of Jan 1 1900
%%severity	Severity from the rule definition
%%SourceProgram	Source program name
%%SQLNoValue	SQL string with masked values. The value of SQL will be replaced by ? in the syslog.
%%SQLString	SQL string (if any)
%%SQLTimestamp	The time on the packet/request (TIMESTAMP in GDM_CONSTRUCT_TEXT)
%%Subject[ ]	If this variable is used in the message template, all that appears between [ ] (for example, file name, email sender, description) will be the subject line of the email sent to user.
%%violationID	Numeric representing the POLICY_VIOLATION_LOG_ID of this alert in GDM_POLICY_VIOLATION_LOG (this is the same as the Violation Log ID in the Policy Violations / Incident Management report)

Named Template

Message templates are used to generate alerts.

The feature defines multiple message templates and facilitates the use of different templates on different rules. In the past, only a single message template was available for all rules, all receiver types, etc.

To add, modify and delete named message templates, click Edit. When creating a new named template, the starting value of the string is a copy of whatever is currently in the Message template of the Global Profile. "R/T Alert" is the only level of severity permitted.

Predefined message templates have been created for the SIEM solutions, ArcSight, EnVision, and QRadar. The Guardium system comes preloaded with two certified (agreed upon) templates to integrate with these two SIEM solutions.

The Named Template builder can select from two template types - Real-time Alerts and Audit Process Report.

Use the Audit Process Report to audit process tasks.

Click Edit Named Templates. Choose an SIEM and then click Modify. Select Real-time Alerts or Audit Process Report.

After editing, the multiple message templates can be selected from within the Policy Builder menu. See Policies.

Adding the QRadar template allows sending real-time alerts or Audit Process Report to QRadar using the LEEF Format (this is QRadar's format).

Follow the steps to send real-time alerts or Audit Process Results to the QRadar SIEM.

Real-time alert, Guardium to QRadar

1. Create an real-time alert.
2. Write to syslog
3. Select Template type (Read-time Alert)
4. Forward to Q1 Labs QRadar SIEM (via LEEF mapping/ predefined message template) - choose QRadar Named Template from Global Profile
5. From the CLI, run the CLI command "store remotelog" to forward the syslog messages to QRadar.

Audit Process Report, Guardium to QRadar

Click Harden > Vulnerability Assessment > Audit Process Builder to open the Audit Process Builder.

1. Create an Audit Process report (Audit Process Builder)
2. Write to syslog
3. Select Template type (Audit Process Report)
4. Forward to Q1 Labs QRadar SIEM (via LEEF mapping/ predefined message template) – choose QRadar Named Template from Global Profile
5. From the CLI, run the CLI command "store remotelog" to forward the syslog messages to QRadar.

For example, here is the default LEEF template for the Databases Discovered report:

```
LEEF:0|IBM|Guardium|9.0|Databases Discovered|Time Probed=${1}|Server IP=${2}|Server Host Name=${3}|DB
Type=${4}|Port=${5}|Port Type=${6}
```

Here are the report columns that are mapped to the template:

```
Time Probed      Server IP    Server Host Name    DB Type    Port    Port Type
```

1. Check Export to CSV file and Write to Syslog.
2. Select the Named Template, LEEF Discovered Databases
3. Configure Remote Syslog by using the store remotelog command. For example:

   ```
   store remotelog add user.info 9.70.145.68 udp
   ```

   This will now push all records from the audit process to the supplied IP address.

Sender Encoding

To encode outgoing messages (email and SNMP traps) in an encoding scheme other than UTF8, use the CLI command, store sender_encoding.

Filter templates of one type

There is a filter mechanism to select all Real Time Alerts or Audit Process Report. Check or clear each selection.

Envision 2 message template

GUARDIUM_ALERT:
rule-id=%%ruleID^^category=%%category^^classification=%%classification^^severity=%%severity^^session-start-time=%%sessionStart^^client-hostname=%%clientHostname^^client-ip=%%clientIP^^server-type=%%serverType^^server-ip=%%serverIP^^src-program=%%SourceProgram^^os-user=%%OSUser^^db-user=%%DBUser^^app-user=%%AppUserName^^service-name=%%serviceName^^req-type=%%requestType^^rule-desc=%%ruleDescription^^sql=%%SQLNoValue

Threshold Default Template

As in real-time alerts, you can choose a template for the message that is sent when the threshold is reached. The template uses a predefined list of variables that are replaced with the appropriate value for the specific alert.

Those variables are:

%%alertName - alert name

%%description - alert description

%%alertQueryValue - query value that caused the alert

%%alertThreshold - alert threshold

%%alertQueryFromDate - start of the query period

%%alertQueryToDate - end of the query period

%%alertBaseQueryValue - base query value of the alert

%%classification - alert classification

%%category - alert category

%%severity - alert severity

%%recommendation - recommended action for the alert

%%Subject[] - subject of the message

The default template for threshold alerts is as follows (can be cloned and edited):

%%Subject[Guardium Alert. Severity: (%%severity), Alert Name: %%alertName]

Alert Name: %%alertName. Alert Description: %%description.

Current value: %%alertQueryValue

Base query value: %%alertBaseQueryValue

Threshold: %%alertThreshold

Query period: %%alertQueryFromDate - %%alertQueryToDate

Alert Classification: %%classification

Category: %%category

Severity: %%severity

Recommended Action: %%recommendation

Customize real-time alerts and email

Control appearance of Prefix email subject with Guardium appliance name.
Control appearance of email subject in email body.
Add naming template parameter %%applianceHostName so Guardium users can add appliance hostname to Name Templates (any position subject or body).
To accomplish this, use two fields in ADMINCONSOLE_PARAMETERS table:
APPEND_APPLIANCENAME_SUBJECT
APPEND_SUBJECT_IN_BODY
Use the following CLI commands to control the content of these fields:
show alerter email append_name_subject
store alerter email append_name_subject
show or store the flag to append the appliance name in email subject
show alerter email append_subject_body
store alerter email append_subject_body show or store the flag to append email subject in the beginning of the email body
Each time the value in CLI changes, it takes effect immediately on the outgoing emails.

CSV Separator

To define a separator to be used in the audit process:

1. Click Setup > Tools and Views > Global Profile to open the Global Profile.
2. Choose Comma, Semicolon, Tab, or define your own in Other box to define the CSV Separator that is used.
3. Click Apply.

Add other HTML content to the Guardium Window

To add other HTML content to the Guardium window:

1. Click Setup > Tools and Views > Global Profile to open the Global Profile.
2. In the HTML - Left and HTML - Right text boxes, enter the HTML for the text or any other items you want to include on the window.
3. Optionally click the preview button to verify that your HTML is displayed as you expect.
4. Click Apply.

Add or Disable a Login Message

To add a message to display in a message box, each time a user logs in:

1. Click Setup > Tools and Views > Global Profile to open the Global Profile.
2. In the Login Message text box, enter the text that you want to display when each user logs in.
3. Mark the show login message box to enable the display of the login message (or clear the box to disable the display).
4. Click Apply.

Enable or Disable Concurrent Same-user Logins

By default, the same Guardium user can log in to an appliance from multiple IP addresses. You can disable concurrent logins from the same user. When disabled, each Guardium user will be allowed to log in from only one IP address at a time. If a user closes their browser without logging out, the connection will time out due to inactivity, so the user account will not be blocked for long.

To change this setting:

1. Click Setup > Tools and Views > Global Profile to open the Global Profile.
2. Locate the field Concurrent login from different IP.
3. Click Enable or Disable, depending on the current status, to change the setting.
   Note: When the feature is disabled, an Unlock button appears next to the Enable button. You can click Unlock to allow a second user to log in with this user account, from a different IP address. This is provided for support purposes.

Enable Data Level Security at the Observed Data Level

This feature assumes that specific Guardium users are responsible for certain specific databases. Therefore a mechanism exists that will filter results, system-wide, in a way that each user will only be able to see the information from those databases that the user is responsible for.

Restriction: Data Level Security and the Investigation Dashboard cannot be enabled concurrently.

To change this setting:

1. Click Setup > Tools and Views > Global Profile to open the Global Profile.
2. Click the Enable or Disable button for the Data level security filtering option
   Note: The datasec-exempt role is activated when data level security is enabled and the datasec-exempt role has been assigned to a user.
3. Additional choices include:

- Show-all - Permits the logged-in viewer to see all the rows in the result regardless of who these rows belong to. When used with the Datasec-exempt role permits an override of the data level security filtering.
- Include indirect records - Permits the logged-in viewer to see the rows that belong to the logged-in user, but also all rows that belong to users under the logged-in user in the user hierarchy.

Note: If data level security at the observed data level is enabled, then audit process escalation is allowed only to users at a higher level in the user hierarchy.

Default Filtering

Online viewer default setting and for audit process results distribution.

Show-all. The default setting is disabled.

Escalate result to all users

Escalate result to all users - A check mark in this check box escalates audit process results (and PDF versions) to all users, even if data level security at the observed data level is enabled. The default setting is enabled. If the check box is disabled (no check mark in the check box), then audit process escalation is allowed only to users at a higher level in the user hierarchy and to users with the datasec-exempt role. If the check box is disabled, and there is no user hierarchy, then no escalation is permitted.

Custom database table maximum size

Set the size of the custom database table (in MB). The Default value is 4000 MB.

At this point in the Global Profile menu is a button to see Current usage. Click on the Current Usage button to show values for INNODB, MYISAM and Total.

Note: The custom size limit is tested before importing data. The import can exceed the maximum size limit. After the limit is exceeded, the next import will be prevented.

SCP and FTP files via different ports

Change the ports that can be used to send files over SCP and FTP.

For Global Profile - Export and Patch Backup can be changed. The default port for ssh/scp/sftp is 22. The default port for FTP is 21.
Note: Seeing a zero 0 in the Guardium GUI as the port indicates that the default port is being used and that there is no need to change.

Add a logo to the Guardium Window

To add a company logo graphic to the Guardium window, or to add other HTML content to the Guardium window:

1. Click Setup > Tools and Views > Global Profile to open the Global Profile.
2. In Upload Logo Image, if you want to include a logo image in the portal window, enter an image file name or click Browse to select a file to upload to the Guardium appliance, and then click Upload.
3. Refresh your browser window. The new logo appears.

Note: The name of the uploaded logo file cannot contain a single quotation mark, double quotation mark, less than sign, or greater than sign.

Encrypt Must Gather

Encrypt Must Gather was added to the Global Profile. Default value is cleared (Do not encrypt). If it is cleared, must gather output is just compressed and not encrypted. When the check box is checked, all future must gather output will be encrypted. Encryption can be also set on by using the store encrypt_must_gather on CLI command and set off by using store encrypt_must_gather off.

Check for Guardium updates

Adding a checkmark will display relevant ad-hoc Guardium patches, GPUs/CFPs/Bundles, Sniffer patches and security patches that are available for the customer to download. Once the patch has been installed, it will disappear from the list.

Datasource connection timeout

Set the Datasource connection timeout in seconds. The default is 60 seconds.

The corresponding GrdAPI command to update this value is: grdapi update_datasource_connection_timeout timeoutInSecond=80

Parent topic: Configuring your Guardium system

Alerter Configuration

No e-mail messages, SNMP traps, or alert related Syslog messages will be sent until the Alerter is configured and activated.

Other components create and queue messages for the Alerter. The Alerter checks for and sends messages based on the polling interval that has been configured for it.

To configure, enable or disable individual correlation alerts, see Correlation Alerts. For correlation alerts and appliance alerts to be produced, Anomaly Detection must also be started. For real-time alerts to be produced, a security policy must be installed.

Mail/SNMP/SYSLOG messages are sent out according to their priority.

Automatically activate the Alerter on startup

1. Click Setup > Tools and Views > Alerter to open the Alerter or click Protect > Database Intrusion Detection > Alerter to open the Alerter.
2. Mark the Active on Startup checkbox. Each time the appliance restarts, the Alerter will be activated automatically.
3. Click Apply.
4. If the Alerter is not running, and you want to start it, click Restart.

Set the frequency that the Alerter checks for and sends messages

1. Click Setup > Tools and Views > Alerter to open the Alerter or click Protect > Database Intrusion Detection > Alerter to open the Alerter.
2. Enter the Polling Interval, in seconds.
3. Click Apply.

Configure the Alerter to send SMTP (email) messages

1. Click Setup > Tools and Views > Alerter to open the Alerter or click Protect > Database Intrusion Detection > Alerter to open the Alerter.
   Note: All remaining items in this topic are in the SMTP section of the Alerter panel.
2. Enter the IP address for the SMTP gateway, in the IP Address box.
3. Enter the SMTP port number (it is almost always 25) in the Port box.
4. Optional: Click the Test Connection hypertext link to verify the SMTP address and port. This only tests that there is access to specified host and port. It does not verify that this is a working SMTP server. A dialog box is displayed, informing you of the success or failure of the operation.
   Note: If this SMTP server uses authentication, you must supply a valid User Name and Password for that mail server in the following two fields. Otherwise, those fields can be blank.
5. Enter a valid user name for your mail server in the User Name box if your SMTP server uses authentication.
6. Enter the password for the user in the Password box if your SMTP server uses authentication. Re-enter it in the Re-enter Password box.
7. In the Return E-mail Address box, enter the return address for e-mail sent by the system. This address is usually an administrative account that is checked often.
8. Select Auth in the Authentication Method if your SMTP server uses authentication. Otherwise, select None. When Auth is selected, you must specify the user name and password to be used for authentication.
9. Click Apply to save the configuration.
   Note: The Alerter will not begin using a new configuration until it is restarted.
10. Click Restart to restart the Alerter with the new configuration.

Configure the Alerter to send SNMP traps

1. Click Setup > Tools and Views > Alerter to open the Alerter or click Protect > Database Intrusion Detection > Alerter to open the Alerter.
   Note: All remaining items in this topic are in the SMTP section of the Alerter panel.
2. In the IP Address box, enter the IP address to which the SNMP trap will be sent.
3. Optional: Click the Test Connection hypertext link to verify the SNMP address and port (162). This only tests that there is access to specified host and port. It does not verify that this is a working SNMP server. A dialog box is displayed, informing you of the success or failure of the operation.
4. In the "Trap" Community box, enter the community name for the trap. Retype the community in the Retype Community box.
5. Click Apply to save the configuration.
   Note: The Alerter will not begin using a new configuration until it is restarted.
6. Click Restart to restart the Alerter with the new configuration.

Parent topic: Configuring your Guardium system

Anomaly Detection

The Anomaly Detection process runs every polling interval to create and save, but not send, correlation alert notifications that are based on an alert's query.

This notification is run according to the schedule defined for each alert. See Alerter Configuration for more information about sending notifications.

The Anomaly Detection process uses the results of a correlation alert's query, which looks back over a specified period of time, and the correlation alert's threshold, to determine whether a condition is satisfied (an excessive number of failed logins, for example). See Correlation Alerts for more information.

In a Central Manager environment, the Anomaly Detection panel for each Guardium system can be used to turn off correlation alerts that are not appropriate for that particular Guardium system. Under Central Management, all correlation alerts are defined on the Central Manager, regardless of which Guardium system they were created or updated. These correlation alerts are the same for all Guardium system, and when activated, are activated on all Guardium system by default.

Note: The Alerter component must be configured and started to send a saved alert message to SYSLOG, email, or an SNMP trap.
Note: Anomaly Detection does not play a role in the production of real-time alerts, which are produced by security policies.

Automatically activate Anomaly Detection on startup

1. Click Setup > Tools and Views > Anomaly Detection to open Anomaly Detection.
2. Mark the Active on Startup check box. Each time the Guardium system restarts, Anomaly Detection is activated automatically.
3. Click Apply.

Set the frequency that Anomaly Detection checks for appliance issues

1. Click Setup > Tools and Views > Anomaly Detection to open Anomaly Detection.
2. Enter the Polling Interval in minutes.
3. Click Apply.

Enable or Disable Active Alerts

To disable an alert globally in a Central Manager environment, it is easier to clear the Active check box in the Modify Alert panel.

To enable or disable an alert on a single Guardium system in a Central Management environment, follow these steps:

1. Log in to the UI of the Guardium system on which you want to disable one or more alerts.
2. Click Setup > Tools and Views > Anomaly Detection to open Anomaly Detection.
3. To disable an alert, select it from the Active Alerts box, and click Disable.
4. To enable an alert, select it from the Locally Disabled Alerts box, and click Enable.

Stop or Restart Anomaly Detection

1. Click Setup > Tools and Views > Anomaly Detection to open Anomaly Detection.
2. Click Stop to stop Anomaly Detection, or click Restart to restart it.

Parent topic: Configuring your Guardium system

Session Inference

Session Inference checks for open sessions that have not been active for a specified period of time, and marks them as closed.

To configure the Session Inference options:

1. Click Setup > Session Inference to open Session Inference.
2. Mark the Active On Startup box to start Session Inference on startup of the Guardium® system.
3. In the Polling Interval box, enter the frequency (in minutes) with which Session Inference checks for open sessions. The default is 120 (minutes).
4. In the Max Inactive Period box, enter the number of minutes of inactivity after which a session is marked closed. The default is 720 (minutes).
5. Click Applyto store the values in the configuration database. Session Inference will not begin using a new configuration until it is restarted.
6. Click Restart to restart Session Inference with the new configuration.

To stop Session Inference, open the Session Inference panel and click Stop.

Parent topic: Configuring your Guardium system

Block S-TAP connection to Guardium (S-TAP Certification)

Use this function to control the specific S-TAP hosts whose clients are allowed access to the Guardium system.

About this task

When enabled, only the specified S-TAP clients are allowed to access the Guardium system.

You can also control this feature with the CLI command store stap approval or with the GuardAPI command, grdapi store_stap_approval.

If you use the CLI command store stap approval, the new configuration takes effect after you run the command restart inspection-core.

View approved STAPs in Manage > Reports > Change Monitoring > Approved Tap Clients or Reports > Real-Time Guardium Operational Reports > Approved Tap Clients.

Procedure

1. Access Manage > Activity Monitoring > S-TAP Certification.
2. Select S-TAP Approval Needed.
3. Specify the approved S-TAP client host IP addresses (not host name) in the Approved S-TAP Clients section, and click Add.
4. Repeat for each S-TAP client.

Results

Note: In a Central Managed environment, after you add the IP addresses to approved S-TAPs, there is a wait time for synchronization that might take up to an hour. After synchronization is complete, the status of the approved S-TAPs appears green in Manage > Activity Monitoring > S-TAP Control
Parent topic: Configuring your Guardium system

IP to Hostname Aliasing

The IP-to-Hostname Aliasing function accesses the Domain Name System (DNS) server to define hostname aliases for client and server IP addresses.

There are two separate sets of IP addresses: one for clients, and one for servers. When IP-to-Hostname Aliasing is enabled, alias names will replace IP addresses within Guardium® where appropriate.

1. Click Protect > Database Intrusion Detection > IP-to-Hostname Aliasing to open IP-to-Hostname Aliasing.
2. Mark the check box for Generate Hostname Aliases for Client and Server IPs (when available) to enable hostname aliasing.

   A second check box can now be accessed. The name of this check box is Update existing Hostname Aliases if rediscovered.

3. Mark the check box to update a previously defined alias that does not match the current DNS hostname (usually indicating that the hostname for that IP address has changed). You may not want to do this if you have assigned some aliases manually. For example, assume that the DNS hostname for a given IP address is dbserver204.guardium.com, but that server is commonly known as the QA Sybase Server. If QA Sybase Server has been defined manually as an alias for that IP address, and the check box for Update existing Hostname Aliases if rediscovered is marked, that alias will be overwritten by the DNS hostname.
4. Click Apply to save the IP-to-Hostname Aliasing configuration.
5. Do one of the following:
   - Click Run Once Now to generate the aliases immediately.
   - Click Define Schedule to define a schedule for running this task. See Scheduling for more information.

To view the aliases defined, see Aliases.

Parent topic: Configuring your Guardium system

System Backup

Use the System Backup function to define a backup operation that can be run on demand or on a scheduled basis. Use the Patch Backup function to create the backup profile settings.

System Backup

System backups are used to backup and store all the necessary data and configuration values to restore a server in case of hardware corruption.

All configuration information and data is written to a single encrypted file and sent to the specified destination, using the transfer method configured for backups on this appliance.

To restore backed up system information, use the restore system CLI command. The CLI command, diag, can also be used, provided that diag is defined as a role for given user.

System backup supports the following methods:

- SCP - defined by default and accessible via CLI and the GUI
- FTP - defined by default and accessible via CLI and the GUI
- Centera - can be added to the GUI by logging into CLI and running the following command, store storage centera backup on
- TSM - can be added by logging into CLI and running the following command, store storage tsm backup on
- AMAZON S3 - is defined by default and accessible via CLI and GUI. It is accessible from CLI as long as it is defined in the GUI.
- Softlayer - Softlayer cloud backup
- Cleversafe - CleverSafe Functionality: Storing backups in a similar fashion to Amazon S3. Will draw a list of available buckets for you directly to the GUI. The first listed name is the name of the bucket you saved to the DataBase. Note: You cannot make new buckets nor delete any buckets (from the Guardium UI/CLI).

Note: System restore must be done to the same patch level of the system backup. For example, if a customer backed up the appliance when it was on Version 7.0, Patch 7 and then wants to restore this backup into a newly-built appliance, then there is a need to first install Version 7.0, Patches 1 to 7 on the appliance and only then to restore the file.

To back up system information:

1. Click Manage > Data Management > System Backup to open System Backup.
2. Select storage method radio button from the list. Depending on how the Guardium system has been configured, one or more of these buttons may not be available. For a description of how to configure the archive and backup storage methods, see the description of the show storage-system and store storage-system commands in Configuration and Control CLI Commands.
    - EMC CENTERA
    - TSM
    - SCP
    - FTP
    - AMAZON S3
    - Softlayer
    - Cleversafe
3. Perform the appropriate procedure depending on the storage method selected:
    - Configure SCP or FTP Archive or Backup
    - Configure EMC Centera Archive or Backup
    - Configure TSM Archive or Backup
    - Configure AMAZON S3 Archive or Backup
    - Configure Softlayer object storage cloud backup
    - Cleversafe - Enter> Valid Endpoint, Valid Bucket name, Valid Access Key, Valid Secret Key
4. Mark one or both of the Backup check boxes:
    - Mark the Configuration check box to back up all definitions.
    - Mark the Data check box to back up all data. (If you are archiving data on a regular basis, this is unnecessary.)
5. Use the Scheduling section to define a schedule for running this operation on a regular basis.
6. Click Save to verify and save the configuration changes. The system will attempt to verify the configuration by sending a test data file to that location.
    - If the operation fails, an error message will be displayed and the configuration will not be saved.
    - If the operation succeeds, the configuration will be saved.
7. Click Run Once Now to run the operation once.

Note: During a SCP/FTP/TSM/Centera/AMAZON S3/Softlayer file transfer, if the backup file transfer fails, the last file of each set of backup/archive files (system backup, configuration backup, archive, CSV archive, etc.) will be saved in the diag/current folder. Then when the backup file destination is again online, a manual transfer of the backup files can be made from the diag/current folder to the destination. The set of backup/archive files will only be saved in the diag/current folder if the file transfer is unsuccessful. If during another backup file transfer there is a file transfer failure, the set of backup/archive files will again be saved in the diag/current folder. However, in order to avoid saving too many files and running out of disk space, ONLY the latest file of each type will be saved. The earlier backup files will be overwritten.
Note: When performing a system backup and restore from one server, which has GIM defined, to another server, then the user must configure a GIM failover to the restore server. This GIM configuration applies to a Backup Central Manager or a System backup and restore.

SCP and FTP files via different ports

Change the ports that can be used to send files over SCP and FTP.

For System Backup or Patch Backup - Set the protocol (SCP or FTP) and specify Host, Directory and Port. The default port for ssh/scp/sftp is 22. The default port for FTP is 21.

Prevent backup/archive scripts from filling up /var

The backup process will check for room in /var before running and fail. This process will also warn the user if there is insufficient space for backup.

The archive process will check the size of the static tables and make sure there is room in /var to create the archive.

An error is logged in the logfile and GUI if the backup is over 50%. For example:

```
ERROR: /var backup space is at 60% used. Insufficient disk space for backup.
```

Amazon S3 Archive and Backup in Guardium

Use this feature to archive and backup data, from Guardium, to Amazon S3.

Amazon S3 (Amazon Simple Storage Service) provides a simple web service interface that can be used to store and retrieve any amount of data, at any time, from anywhere on the web. It gives any developer access to the same highly scalable, reliable, secure, inexpensive infrastructure that Amazon uses to run its own websites.

Prerequisites

1. An Amazon account.
2. Register for S3 service
3. Amazon S3 credentials are required in order to access Amazon S3. These credentials are:
    - Access Key ID - identifies user as the party responsible for service requests. It needs to be included it in each request. It is not confidential and does not need to be encrypted. (20-character, alphanumeric sequence).
    - Secret Access Key - Secret Access Key is associated with Access Key ID calculating a digital signature included in the request. Secret Access Key is a secret, and only the user and AWS should have it (40-character sequence). This key is just a long string of characters (and not a file) that is used to calculate the digital signature that needs to be included in the request.

There are two archive operations available on the Administration Console, in the Data Management section of the menu:

- Data Archive backs up the data that has been captured by the appliance, for a given time period.
- Results Archive backs up audit tasks results (reports, assessment tests, entity audit trail, privacy sets and classification processes) as well as the view and sign-off trails and the accommodated comments from work flow processes.

When Guardium data is archived, there is a separate file for each day of data.

Archive data file name format:

```
 <time>-<hostname.domain>-w<run_datestamp>-d<data_date>.dbdump.enc
```

The archive function creates signed, encrypted files that cannot be tampered with. The names of the generated archive files should not be changed. The archive operation depends on the file names created during the archiving process.

System backups are used to backup and store all the necessary data and configuration values to restore a server in case of hardware corruption.

All configuration information and data is written to a single encrypted file and sent to the specified destination, using the transfer method configured for backups on this appliance.

Backup system file format:

```
<data_date>-<time>-<hostname.domain>-SQLGUARD_CONFIG-9.0.tgz
<data_date>-<time>-<hostname.domain>-SQLGUARD_DATA-9.0.tgz
```

The Aggregation/Archive Log report can be used to verify that the operation completes successfully. There should be multiple activities listed for each Archive operation, and the status of each activity should be Succeeded.

Regardless of the destination for the archived data, the Guardium catalog tracks where every archive file is sent, so that it can be retrieved and restored on the system with minimal effort, at any point in the future.

A separate catalog is maintained on each appliance, and a new record is added to the catalog whenever the appliance archives data or results.

Catalog entries can be transferred between appliances by one of the following methods:

- Aggregation - Catalog tables are aggregated, which means that the aggregator will have the merged catalog of all of its collectors
- Export/Import Catalog - These functions can be used to transfer catalog entries between collectors, or to backup a catalog for later restoration, etc.
- Data Restore - Each data restore operation contains the data of the archived day, including the catalog of that day. So, when restoring data, the catalog is also being updated.

When catalog entries are imported from another system, those entries will point to files that have been encrypted by that system. Before restoring or importing any such file, the system shared secret of the system that encrypted the file must be available on the importing system.

Enable Amazon S3 from the Guardium CLI

Amazon S3 archive and backup option is enabled by default in the Guardium GUI. To enable Amazon S3 via Guardium CLI, run the following CLI commands:

```
store storage-system amazon_s3 archive on
store storage-system amazon_s3 backup on
```

Amazon S3 requires that the clock time of Guardium system to be correct (within 15-minutes). Otherwise, this will result in an Amazon error. If there is too large a difference between the request time and the current time, the request will not be accepted.

If the Guardium system time is not correct, set the correct time using the following CLI commands:

```
show system ntp server
store system ntp server (An example is ntp server: ntp.swg.usma.ibm.com)
store system ntp state on
```

User Interface

Use the System Backup screen (Manage > Data Management > System Backup) to configure the backup. After enabling Amazon S3 through the CLI commands, Amazon S3 will appear in the list of protocols.

User input requires:

- S3 Bucket Name (Every object stored in Amazon S3 is contained in a bucket. Buckets partition the namespace of objects stored in Amazon S3. Within a bucket, you can use any names for your objects, but bucket names must be unique across all of Amazon S3.
- Access Key ID
- Secret Access Key

If bucket name does not exist, it will get created.

Secret Access Key is encrypted when saved into the database.

Check that files got uploaded on Amazon S3

1. Log onto AWS Management Console using your email address and password.

http://aws.amazon.com/console/

1. Click on S3.
2. Click on the bucket that you specified in Guardium UI.

Softlayer Object Storage

SoftLayer Object Storage is a redundant and highly scalable cloud storage service. Use it to easily store, search, and retrieve data across the Internet. It is based on the OpenStack Swift platform and may be accessed through a RESTful API and Web Portal.

Information needed beforehand:

- Authentication Endpoints - Authentication requests should be sent to the endpoint associated with the location of your Object Storage account. https://dal05.objectstorage.softlayer.net/auth/v1.0
- Container - The basic storage unit for all the data within Object Storage is a container. It stores data/files and must be associated with an Object Storage account.
- X-Auth-User - Username to authenticate with: Tenant value:username
- X-Auth-Key - API key (Password) to authenticate with.

Account credentials can be retrieved by logging onto https://control.softlayer.com/

System Backup by Softlayer from GUI

1. Click Manage > Data Management > System Backup, Manage > Data Management > Data Archive, or Manage > Data Management > Results Archive.
2. Select the Softlayer protocol.
3. Fill in Authentication Endpoint URL (example, https://dal05.objectstorage.softlayer.net/auth/v1.0)
4. Specify an Object Storage container name (example, yourname_Container)
5. Specify the X-Auth-User (Tenant value: Username) (example, username)
6. Fill in the X-Auth Key (example, password)
7. Specify what to Backup - Configuration or Data
8. Modify Scheduling or Run Once Now.

System Backup via CLI (Configuration)

Access CLI.

CLI> backup system.

1. DATA

2. CONFIGURATION

Please enter the number of your choice: (q to quit) 1

1. SCP

2. CONFIGURED DESTINATION

Please enter the number of your choice: (q to quit) 2

Make sure destination is configured in the GUI under the <System Backup> option

Please wait, this may take some time.

Performing a DEFAULT backup, config=

System Backup and System Restore

Access CLI.

CLI> restore system

1. SCP

2. FTP

3. TSM

4. CENTERA

5. AMAZONS3

7. SOFTLAYER

8. SFTP

Please enter the number of your choice: (q to quit) 7

Enter the SoftLayer Authentication Endpoint URL:

Enter Softlayer Object Storage Container name:

Enter Softlayer X-Auth-User:

Enter X-Auth-Key:

Enter a file name from list:

Authenticate success!

Download file success!

Select your recovery type, for most cases, use the normal option:

1. normal

2. upgrade

System Backup > Cleversafe

Prerequisite

The Guardium server must be set to the correct local time. Use NTPserver to change if necessary.

System Backup selections:

Authentication endpoint URL

(AWS) Access key

(AWS) Secret access key

Bucket name

Answer yes to all certificate questions.

Parent topic: Configuring your Guardium system

Configuring patch backup

Use this feature to store backup profile information.

Procedure

1. Click Setup > Patch Backup to open the Patch Backup panel.
2. Choose the method of file transfer.
3. Enter the name of the host and the directory where the information is to be stored.
4. Enter a user name and password to own the file on the destination host.
5. Click Apply when you are finished.

Parent topic: Configuring your Guardium system

Configure Permission to Socket connection

This topic applies to Custom Alerting Classes.

Follow this procedure to configure permissions for socket all connections that are used by custom classes.

1. Click Setup > Evaluations > Communication Permissions to open the Communication Permissions.
2. Click Add permission To Socket Connection to expand that pane.
3. Enter the IP address or Host name for the host.
4. Enter a Port number for the socket connection.
5. Enter a description.
6. Click Save.

Parent topic: Configuring your Guardium system

Access Management Overview

Access management consists of four tasks: account administration, maintenance, monitoring, and revocation.

Access Management is separate from system administration duties.

There are two predefined users on a Guardium® appliance: accessmgr and admin.

- *accessmgr* is the user name assigned to the access manager. By default, the access manager is the only user authorized to manage user accounts and security roles.

- *admin* is the user name assigned to the (primary) Guardium administrator. By default, the administrator does not have authority to manage user accounts or security roles. The admin user has a more extensive set of privileges.

Note:

Admin and accessmgr roles can not be assigned to the same user. The same user may contain both of these roles through a legacy situation or as a result of an upgrade. However, current use will not allow the two roles to be assigned to the same user.

In the past, when a unit was upgraded, the accessmgr role was assigned to the admin user, and the accessmgr user was disabled. In this upgrade situation, it was necessary to first log in as admin and enable the accessmgr user, then log in as accessmgr (with initial password "accessmgr", the system prompted the user to change it), and remove the accessmgr role from the admin user.

Access Management Selection

- User Browser - Manage users
- Role Browser - Manage permissions and customize layouts for roles
- Role Permissions - Manage application permissions
- LDAP User Import - Import users from LDAP

Data Security Selection

- Datasources Associated
- Datasources Not Associated
- Servers Associated
- Servers Not Associated
- User Hierarchy
- User-DB Association

Predefined Reports from Accessmgr

The following predefined reports are available from the Accessmgr user.

User and Role Reports

Defining and modifying users (see Manage Users) involves deciding both who will be using the Guardium system and to what roles (see Manage Roles) they will be assigned. A role is a group of users, all of whom are granted the same access privileges.

The User and Role Reports consist of reports:

- User - Role -- a report that shows, by user, the number of roles that user belongs to.
- All Roles - User -- a report that shows, by role, the number or users that belong to that role.

Note: admin and access manager are pre-existing, other roles are created by the Access manager.

The following reports are available on a Central Manager or a standalone unit. If trying to use on a managed machine, an error message will appear. Servers Not Associated will show servers from ALL managed units in Central Manager systems.

Datasources Associated

This report identifies Datasource Name, Host, Service Name, Login Name and Association Type. This information comes from the choices made in the User-Database Associations activity. See the Data User Security - Hierarchy and Associations help topic.

Datasources Not Associated

This report is a list of datasources not associated with any users. This report identifies Datasource Name, Datasource Type, Host, and Service Name. This information comes from the choices made in the User-Database Associations activity. See the Data User Security - Hierarchy and Associations help topic.

Servers Associated

This report identifies Server IP, Service Name, Login Name and Association Type. This information comes from the choices made in the User-Database Associations activity. See the Data User Security - Hierarchy and Associations help topic.

Servers Not Associated

This report is a list of servers not associated with any users. This report identifies Server IP and Service Name. This information comes from the choices made in the User-Database Associations activity. See the Data User Security - Hierarchy and Associations help topic.

- Understanding Roles
  Assign a role to a Guardium user to grant them specific access privileges. Some examples of roles are: CLI, admin, accessmgr, CAS, and user.
- Managing roles and permissions
  Roles and permissions provide different levels of access to users based on their job duties.
- How to create a role with minimal access
  This topic explains how to create a new role with minimal access permissions, for example an auditor role that can only access the Audit Process To-Do List and view specific reports.
- Manage Users
  Use the access manager, assigned the user name *accessmgr*, to add user accounts, enable or disable user accounts, import members from LDAP, or edit user permissions. Open the User Browser and browse the user accounts by clicking Access > Access Management > User Browser
- How to create a user with the proper entitlements to login to CLI
  Use this task to create a user who has the proper roles and entitlements to use CLI to run GuardAPI commands.
- Importing Users from LDAP
  You can import Guardium user definitions from an LDAP server by configuring an import operation to obtain the appropriate set of users.

- Data Security - User Hierarchy and Database Associations
  You can use data security features to create a hierarchy of users and associate users to specific databases and servers. Guardium data security features report on which users accessed what information, and ensure that only specific users see information that they are responsible for.
- How to define User Hierarchies
  Use the UI from an access manager account to easily define user hierarchies.
- Guardium UI Login using a Smart card
  Guardium Smart card support meets the United States government mandate that all vendors must support multi-factor authentication for user access. Smart card authentication is supported only for access to the web-based Guardium user interface (UI).

Understanding Roles

Assign a role to a Guardium user to grant them specific access privileges. Some examples of roles are: CLI, admin, accessmgr, CAS, and user.

The access manager defines roles and assigns them to users and applications. When a role is assigned to an application or the definition of an item (a specific query, for example), only those Guardium users who are also assigned that role can access that component.

When user definitions are imported from an LDAP server, the groups to which they belong can optionally be defined as roles. For more information, see Importing Users from LDAP.

Note: When assigning roles to a user, the admin and access manager role cannot be assigned to the same user.
Note: Custom-created roles cannot be combined with default-provided roles (examples are user, admin, accessmgr, cli, inv, datasec-exempt, review-only).
Note: Admin role and object owner have access to all objects by default.
Note: Taking a base role and customizing (with additional navigation items), and then copying this customized role, will result in a loss of the customization if the customized or copied role is reset to default.

Default Roles

The Guardium system is pre-configured to support users who fall into four broadly defined default roles: admin, user, access manager, and investigations. The Guardium access manager can create new roles as well.
Note: Note: If data level security at the observed data level is enabled (see Global Profile settings), then audit process escalation is allowed only to users at a higher level in the Data Hierarchy (see Access Manager). The Datasec-exempt user can escalate, without restrictions, to anyone.

Table 1. Default Roles

Default Role	Description
user	Provides the default layout and access for all common users. This role can not be deleted.
admin	Provides the default layout and access for Guardium administrators. Do not confuse the admin role with the admin user, which is a special user account having the admin role, but also having additional powers that are reserved for the admin user account only. This role can not be deleted.
accessmgr	Provides the default layout and access for the access manager. This role can not be deleted.
cli	Provides access to CLI. The admin user has default access to CLI. Everyone else must be given permission when users are created by access manager and roles specified. The access manager can define as many users in the system and give them the CLI role. These users have access to the CLI and all activities of their CLI sessions are associated with this user. To run GrdAPI or CLI commands without admin rights, click the role CLI for Admin Console in the User Role Permissions selection. See the topic, diag CLI Command, on how to manage the diag role.
inv	Provides the default layout and access for investigation users. An investigation user must have the restore-to database name of INV_1, INV_2 or INV_3, as the Last Name in their user definition. This is not enforced by the GUI, but is required for the application to function properly. When assigned, the user role must also be assigned. This role can not be deleted. Note: The Ad-Hoc Process for run once now button is available on all report screens for all users except investigation (INV) user.
datasec-exempt	Data Security - Exempt. This role is activated when Data level security is enabled (see Global Profile in Administration Console) and the datasec-exempt role has been assigned. If the user has this role, a Show all check box appears in all reports. If checked, all sniffed data records are shown (no filter is applied). This role cannot be deleted in the Role Browser.
review-only	A user that is specified by this role can view only results (Audit, Assessment, Classifier), Audit Results and the To Do List. This role cannot be deleted in the Role Browser. Users with this role is allowed to enter comments in the audit process viewer (not workflow or comments/data per row, but comments at process/result level). Users with this role cannot perform any changes/actions on any workflow automation result (escalate, reassign, etc).

Sample Roles

In addition to the default roles, a set of sample roles is also defined.

Table 2. Sample Roles

Sample Role	Description
dba	Users who have a database-centric view of security, allowing access to database-related reports and tracking of database objects
infosec	Users who have an information security focus, including tracking access to the database, and handling network requests, audits, and forensics
netadm	Users who have a network-centric view, including IP sources for database requests
appdev	Application developers, architects, and QA personnel who have an application-centric focus and want to track and report on SQL streams generated by an application

Sample Role	Description
audit	Auditors and others who need to view audit reports Note: If trying to copy this role, an embedded message will appear explaining that not all aspects of this role can be copied. The message is: "Create a new role using the layout and permission from the "audit" role. Special privileges and actions associated with the "audit" role will not be copied."
audit-delete	This role is used to track or log when an audit process result has been deleted. Users with the audit-delete role can delete reports. Admin users can also delete reports. Tracking is done through the User Activity Audit Trail report.
admin-console-only	A user that is specified by this role can only access the admin console tab.
cas	Configuration Auditing System (CAS)
vulnerability-assess	A user that is specified by this role can view only vulnerability results.
diag	A user that is specified by this role can access and run the diag commands in CLI.
workload-replay-admin	A user that is specified by this role can define and modify the workload-replay functions.
workload-replay-user	A user that is specified by this role can run the workload-replay functions.
fam	A user that is specified by this role can define and modify the File Activity Monitor functions.
BaselII	Accelerator - Basel II. This role can not be deleted. Basel II Part 2 Sections 4 and 5 require that banking institutions must define a Securitization Framework around financial information and estimate the associated operational risk.
DataPrivacy	Accelerator - DataPrivacy. This role can not be deleted. The Data Privacy Accelerator delivers a portfolio of pre-configured policies, real-time alerts, and audit reports that are specifically tailored to the challenges of identify theft and based on industry best practices. With the Data Privacy Accelerator, security managers, privacy officers, and database administrators begin by defining combinations of data elements – called "privacy sets" – whose access may indicate hacking or inappropriate activities by internal users.
GDPR	Accelerator - GDPR. This role can not be deleted. The Guardium GDPR accelerator provides predefined reports based on GDPR groups and policies. To begin working with the GDPR accelerator, assign the GDPR role to a Guardium user, then navigate to Accelerators > GDPR with that user account.
pci	Accelerator - PCI. This role can not be deleted. The PCI DSS is a set of technical and operational requirements designed to protect cardholder data and applies to all organizations who store, process, use, or transmit cardholder data. Failure to comply can mean loss of privileges, stiff fines, and, in the case of a data breach, severe loss of consumer confidence in your brand or services. The IBM Guardium accelerator helps guide you through the process of complying with parts of the standard using predefined policies, reports, group definitions, and more.
sox	Accelerator - SOX. This role can not be deleted. SOX Section 404 requires that companies must establish and maintain an adequate internal control structure and procedures for financial reporting.

Roles in a Central Manager Environment

In Central Manager environments, all User Accounts, Roles, and Permissions are controlled by the Central Manager. To administer any of these definitions, you must be logged in to the Central Manager (and not to a managed unit).

Create a Role

1. Login as accessmgr, and open the User Role Browser by clicking Access > Access Management > Role Browser.
2. Click Add Role to open the Role Form panel.
3. Enter a unique name for Role Name and click Add Role.

Remove a Role

1. Open the User Role Browser by clicking Access > Access Management > Role Browser.
2. Click Delete for any role (some roles cannot be removed, and do not have the Delete option). This opens the Role Form for the role.
3. Click Confirm Deletion. A message displays informing you that all references to the role are removed, and you will be asked to confirm the action.
4. Click OK to confirm the deletion, or Cancel to abort the operation.

Parent topic: Access Management Overview

Managing roles and permissions

Roles and permissions provide different levels of access to users based on their job duties.

Examples of roles include user, admin, and audit. Using roles allows you to easily define permissions for an entire group of users. Only access managers can create new roles and assign users to that role. As part of role creation, access managers can also customize the navigation menu and permissions for that role.

Creating customized roles involves several processes:

- Creating a new role
- Managing permissions for the role to limit what users can access
- Optionally customizing the navigation menu for the role to further limit what users can see

- Adding users to the role

There are two ways to limit access to specific applications:

Limit access from the application

Limit access from the application by deselecting the All Roles check box on the Role Permissions > Edit Application Role Permissions screen. Next, select the individual roles that should have access to the application.

The process is the same if you find that the All Roles check box is already deselected: simply select or deselect the individual roles to grant or revoke access to the application.

When All Roles is selected for a particular application, every currently-defined role will have access to that application.

Limit access from the role

Limit access from the role by navigating to the Role Browser > Manage Permissions screen and move individual applications from the Accessible applications list to the Inaccessible applications list.

When managing permissions or customizing the navigation menu for a new role, the defaults shown in the Accessible applications list reflects any application with the All Roles check box selected on the Role Permissions > Edit Application Role Permissions screen.

When working with roles and permissions, removing permissions for an application also changes the default permissions for new roles. That is, removing permissions for an application means that any subsequent roles you create will also lack permissions for that application. If you want a new role to have permissions for an application that no longer appears in the Accessible applications list by default, you will need to move the desired application from the Inaccessible applications list to the Accessible applications list for the new role.

It is also possible to restrict access to specific tools by hiding menu items using the Role Browser > Customize Navigation Menu tool. This approach limits access without altering the default application permissions, but it may be less secure than a permissions-based approach.

Best Practices:

- After editing permissions for a role, review the navigation layout for that role as shown on theRole Browser > Customize Navigation Menu screen. Add or remove items from the Navigation Menu list as needed to create a layout appropriate for the role.
- Copy and edit predefined roles to establish the desired permissions and navigation menu. This approach allows you to revert to the original role if needed.

Parent topic: Access Management Overview
Related tasks:
How to create a role with minimal access
Related information:
Customizing the user interface
Managing users, roles, and the Guardium system (video)

How to create a role with minimal access

This topic explains how to create a new role with minimal access permissions, for example an auditor role that can only access the Audit Process To-Do List and view specific reports.

Procedure

1. Create a new role.
   a. Log in as *accessmgr*, navigate to Access > Access Management, and select the Role Browser.
   b. Click the Add Role button, give the role a name, and click the Add Role button to create the new role.
2. Manage permissions so the new role can only access the Audit Process To-Do List and the Report Builder (which is required for viewing reports).
   a. From the Role Browser, click the Manage Permissions link for the new role.
   b. Select the checkbox in the header of the Accessible Items list and use the arrow to move all items to the Inaccessible Items list. When creating a highly restricted role, it is easier to begin by removing permissions.
   c. In the Inaccessible items list, select the Audit Process To-Do List and the Report Builder, and use the arrow to move them back to the Accessible items list. The new role now has access to only these two specific applications.
   d. Click the OK button to commit your changes.
3. Customize the menus and navigation by defining which reports and applications are available to the new role.
   a. From the Role Browser, click the Customize Navigation Menu link for the new role.
   b. In the Navigation Menu list, select the Reports group so it is highlighted. The selected group acts as the destination for menu items added in subsequent steps.
   c. In the Available Tools and Reports list, expand the Reports section or use the Filter to identify specific reports, select the check box next to each item that should be available to the new role, and use the arrow to add the items to the Navigation Menu list. Items moved into the Navigation Menu list will become visible to users assigned to this role.
   d. In the Navigation Menu list, remove access to the Report Builder by clicking the  icons next to the Reports > Report Configuration Tools and Investigate groups. This further simplifies the menu structure for this role and removes access to the Report Builder tool without also removing application permissions that are required to access reports.
   e. Click the OK button to commit your changes. You have now created a new role with very minimal privileges that can be assigned to users.
4. Optionally specify a custom home page for the new role.
   a. From the Role Browser, click the Customize Navigation Menu link for the new role.
   b. In the Navigation Menu list, specify a new default home page by selecting Comply > Tools and Views > Audit Process To-Do List and clicking the  icon in the toolbar. Users assigned to this role will now see the Audit Process To-Do List as the default screen after logging in.
   c. Click the OK button to commit your changes.
5. Create a new user and add that user to the new role.
   a. Navigate to Access > Access Management and select User Browser.
   b. Click Add User, provide the required information, and click Add User to create the new user. You will now see the user you created listed in the User Browser.

When a new user is created, the account is disabled by default. Deselect the Disabled check box if you want the user to have immediate access to their account.

c. From the User Browser, click the Roles link for the new user to view a list of available roles.
d. Select the Assign check box next to the custom role you created earlier. This will assign the user to the new role.
e. Deselect the Assign check box next to the *user* role. Deselecting the *user* role prevents the new user from inheriting the default *user* access and permissions.
f. Click Save to commit your changes.

Parent topic: Access Management Overview
Related concepts:
Managing roles and permissions

Manage Users

Use the access manager, assigned the user name *accessmgr*, to add user accounts, enable or disable user accounts, import members from LDAP, or edit user permissions. Open the User Browser and browse the user accounts by clicking Access > Access Management > User Browser

Defining and modifying users involves deciding both who will be using the Guardium® system and to what roles they will be assigned. A group of users can all have the same role and the same access privileges if you so choose. For more information on roles, see Understanding Roles.

Note: A default layout can be defined for a role, so that any new user assigned that role will have that layout. See Generate New Layout in the CLI Reference.

User definitions can be imported from an LDAP server, on demand or on a schedule.

Regardless of how users are defined to the Guardium system, the Guardium administrator can configure the system to authenticate users via Guardium, LDAP, or Radius.

When getting started with your Guardium system, an important early task is to identify which groups of users will use the system, and what their function will be. For example, an information security group might use Guardium for alerting and troubleshooting purposes while a database administrator group might use Guardium for reporting and monitoring. When deciding who will access the Guardium system, keep in mind that sensitive company data can be picked up by the system. Therefore, be very aware of who will be able to access that data.

Once you decide which groups of users will use the Guardium system (and for what purpose), collect the following information for each user:

- User's first and last name
- User account name (the name they will use to log in)
- User's email address
- User's function/role with Guardium

User Account Security

Several settings can be changed to provide additional security for user accounts. You can enable or disable these settings using the show and store password CLI commands (see User Account, Password and Authentication CLI Commands in the CLI Reference).

- By default, password validation is enabled. This means that a minimum of eight characters is required, and the password must contain at least one character from each of the following categories:
  - Uppercase letters: A-Z
  - Lowercase letters: a-z
  - Digits: 0-9
  - Special characters: @#$%^&.;!-+=_

  Note: If password validation is disabled, any characters are allowed.
- By default, password expiration is enabled. Passwords can be configured to expire after a designated number of days.
- By default, account lockout following a specified number of failed login attempts is enabled. Lockout can be configured to occur after a fixed number of attempts in a given time, or after a total number of attempts for the life of the account.

Locked Accounts

1. Open the User Browser by clicking Access > Access Management to view the list of users.
2. Click Edit for any user, clear the Disabled check box, and click Update User to save changes.
   Note: If the admin user account becomes locked, use the unlock admin CLI command to unlock it (see Configuration and Control CLI Commands in the CLI Reference).

Create a User Account

1. Open the User Browser and click Add User to open the User Form panel.
2. Enter a unique name for Username. Do not include apostrophe characters in the name. User names are not case sensitive.
   Note: When adding a user manually, from either the Add User panel or User LDAP Import, if there is no first name and/or last name, the login name will be used.
3. Enter a password and confirm it again in the Password (confirm) box. The password you assign will be temporary, and the user will be required to change it following their first login.
   Note: Passwords are case sensitive. When password validation is enabled (the default), the password must be eight or more characters in length, and must include at least one uppercase alphabetic character (A-Z), one lowercase alphabetic character (a-z), one digit (0-9), and one special character from the following set: @$%^&.;!-+=_
   Note: Non-Latin characters, for example, Chinese, Japanese, are not supported in the username.
4. Enter the user's first and last name in the respective fields.
   Note: Restrictions apply to the last name for those users assigned the Investigation Data Restore role (inv). If you want to assign a user the investigator role, their last name must be INV_1, INV_2, INV_3. The UI will not restrict you from entering something different in this field, but the application will not function properly unless the last name is entered as shown. Further, the investigator cannot be assigned any additional roles - they must be inv only. This is the only case where it is not required to have a user or admin role.
5. (Optional) Enter the user's email address.
6. (Caution) The Disabled check box is checked by default. We suggest that you defer clearing the check box and enabling the account until after the correct set of roles have been assigned for the user.

It is much simpler to assign the roles first, so that the user has all components in their layout the first time they log in. When a user logs in for the first time, their layout is built using all of the roles assigned at that time. If roles are added later, the user has access to everything available to that role, but will have to add reports or applications particular to that role manually.

7. Click Add User to save the new user account definition and close the panel.

This completes the user definition. We suggest that you add the appropriate roles for the user before informing them of their password for the initial login. See Understanding Roles for more information.

Enable/disable many users

Open the User Browser and click Search Users to easily filter users by role. When you select a user, you have the option to enable or disable the user. Because users are disabled by default, this menu can be very useful to easily change the status of many users.

Update a User Account

1. Open the User Browser and click Edit for the user you want to modify.
2. Replace any values in the User Form panel.
3. Click Update User to save changes.

Note: Changing a user's password will require the user to change it following their next login.

Enable a Disabled User Account

1. Open the User Browser and click Edit for the user you want to enable.
2. Clear the Disabled check box.
3. If the user has forgotten their password, enter a new password in both the Password and Password (confirm) boxes.
4. Click Update User.

Remove a User Account

1. Open the User Browser by clicking Access > Access Management .
2. Click Delete for the user you want to remove.
3. Click Confirm Deletion.

Note: Alerts that were sent to deleted user will be sent now to the admin; however this will not take effect until the access policy is re-installed.

Define the Data Security User Hierarchy

1. Click Data Security > User Hierarchy.
2. Select a user from the User menu to refresh the screen and display the selected user's current hierarchy in the user pane.
3. Right-click a user node for the following op:
   - Add User - Clicking Add User displays the Add User dialogue. Search or filter by role, and add a user as a descendent of the selected user.

     This can create a measure of data-level security, by permitting the parent of a hierarchy to look at specified servers and databases, but not the children of the hierarchy. Depending on the configuration, inheritance can also take place in that the parent inherits the data-level security of the child.

     Note: Many-to-many relationships are permitted where a user may have more than one parent and a parent may have more than one user.
   - Unlink User from parent - will sever the descendent from the parent
   - Remove all descendents - will sever all descendents from the parent
4. Click Refresh Cached Hierarchy to apply the recent changes to the user hierarchy map.
5. Click Full Update Active User-DB Map to fully apply all recent changes to the active User-DB association map.
   Note: Best practices dictate a Full Update Active User-DB Map after changing the User Hierarchy.

   When you make a change to a hierarchy or to a database association (via UI or GuardAPI), this change DOES NOT take effect automatically. The Periodic Update will NOT pick up this change, unless it is the FIRST time the Periodic Update has run. Otherwise, the user MUST click Full Update or run the Full Update GuardAPI command for their changes to take effect.

   A periodic update of the user hierarchy is run every 10 minutes automatically. This cannot be run manually. This is an incremental update, meaning that it is only looking at new server IPs or Service Names that have been sniffed since the last time the periodic update was run. It compares the existing hierarchy and associations against the new IPs/Service Names and determines what users should have access to these IPs/Service Names.

   A full update of the user hierarchy is NOT run automatically. It is only run when the user executes it, either via the UI or GuardAPI function. This compares ALL IPs/Service Names to the existing hierarchy and associations to determine who has access to what.

Define the Data Security User to Database Association

Use the Data Security User-DB Association to find, assign, or remove users from available servers and service names (databases).

1. Open the User-DB Association panel by clicking Data Security > User-DB Association.
2. Select the check boxes of the Server & Service Name Suggestion to find databases and service names to associate to users. Choices include:
   - Observed Accesses - Observed traffic from Guardium internal database table GDM_Access
   - Datasource Definitions - Existing datasource definition information such as name, database type, authentication information, and location of datasource.
   - S-TAP® Definitions - Existing S-TAP definition information such as the IP address of the database server and the IP address of the Guardium host that will receive data from S-TAP.
   - Auto-Discovered Hosts - Hosts discovered by the Guardium Auto-discovery process that were not previously known. Guardium's Auto-discovery application can be configured to probe the network, searching for and reporting on all databases discovered.
   - Guardium Install Manager (GIM)-Discovered Systems - Hosts discovered by the GIM that were not previously known.
3. Click Go to find and display available servers, service names, and currently associated users.
   Note: When traversing the node tree, numerical indicators are displayed next to each server and service name to provide a count of direct and descendant users that have been associated. The indicators take the format of [nn] for direct association and (mm) for descendant association (a server or service name within the

current server has a user associated to it for example). Likewise, when viewing the users associated to a server or service name, if there is a user associated to a larger level node in the tree, that user will be displayed.

4. Click a server or service name node to display associated users. With any node selected, you can do one of the following:
   - Click Add User to add a new user-DB association, click any users you want to add, and then click Add.
   - Click Add Group to add a new group-DB association. When Add Group is selected, groups that were created using the Group Builder for group type Guardium Users will be displayed. Select the group you'd like to add and click Add.
   - Right-click any server or service name node to do one of the following:
5. Right-click any server or service name node, and you are presented with options to do one of the following:
   - Highlight the server
   - Expand or collapse the server
   - Find a server
   - Add server, service name, or unnamed service
   - Delete the server
6. Add an IP or IP/Service Name pair using the IP and Service Name fields before the tree structure.
   Note: The Find button can be used to search the IP/Service Name tree structure. IP strings may be entered as partials or include the wild card * such that 192.168 and 192.168.*.* are both valid. Numeric values cannot trail the use of any wild card or be used with the wild card to form an octet. Service Name names may include the wild card % anywhere within their name.
7. Click Full Update Active User-DB Map to fully apply all recent changes to the active User-DB association map.
   Note: Best practices dictate a full update of the active User-DB map after changing the User-DB Association.

   A full update of the user hierarchy is NOT run automatically. It is only run when the user executes it, either via the Full Update Activer User-DB Map button or the GuardAPI function. This compares ALL IPs/Service Names to the existing hierarchy and associations to determine who has access to what.

   A periodic update of the user hierarchy is run every 10 minutes automatically (cannot be run manually). This update is only looking at new server IPs or Service Names that have been sniffed since the last time the periodic update was run. It compares the existing hierarchy and associations against the new IPs/Service Names and determines what users should have access to these IPs/Service Names.

   When you make a change to a database association (via UI or GuardAPI), this change DOES NOT take effect automatically. The periodic update will NOT pick up this change, unless it is the FIRST time the periodic update has run. Otherwise, the user MUST click the Full Update Activer User-DB Map button, or run the full update GuardAPI command for the changes to take effect.

Parent topic: Access Management Overview

How to create a user with the proper entitlements to login to CLI

Use this task to create a user who has the proper roles and entitlements to use CLI to run GuardAPI commands.

About this task

This how-to topic is important since (1) GuardAPI commands can be executed only through CLI, and (2) Most GuardAPI commands are associated with a specific application and therefore with its roles; meaning that the standard CLI user (who has a hard coded "admin" role) cannot run many of the GuardAPI commands because that user does not have the appropriate roles.

Procedure

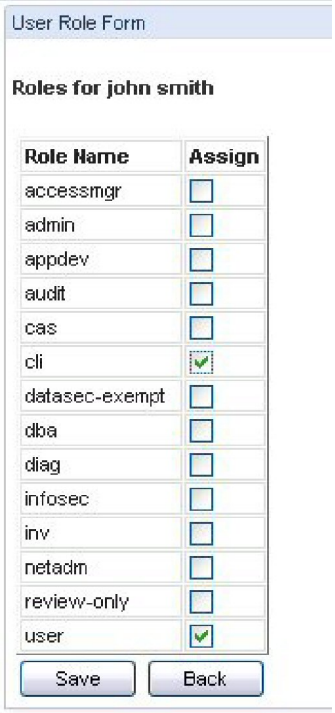
1. Login as the accessmgr and open the User Browser by clicking Access > Access Management > User Browser.
2. Click Add User from the User Browser panel

3. Fill in the User Form, clear the Disabled check box to enable the user upon creation, and click Add User.

When a user is initially created they do not have the privilege to login to CLI and execute any of the GuardAPI commands. As an example, if we try and use one of the CLI accounts (guardcli1,...,guardcli5) under the newly created user we are quickly disconnected and told that the user does not have the necessary role defined.

```
$ ssh -l guardcli1 192.168.1.89  guardcli1@192.168.1.89's password:
Last login: Tue Aug 10 18:37:25 2010 from 192.168.1.14
Welcome guardcli1 - your last login was Tue Aug 10 18:37:26 2010
Please enter your GUI login (one with ADMIN or CLI role defined):johnsmith
No such user or user does not have the necessary role defined.
Connection to 192.168.1.89 closed.
```

4. From the User Browser panel, click Roles for any user to bring up the User Role Form panel.
5. Check the CLI check box, and click Save to grant the user CLI access



Now when the user tries to use one of the CLI accounts (guardcli1,...,guardcli5) under the newly created user we are asked for a password and granted access to the CLI.

```
$ ssh -l guardcli1 192.168.1.89
guardcli1@192.168.1.89's password:
Last login: Tue Aug 10 18:39:01 2012 from 192.168.1.14
Welcome guardcli1 - your last login was Tue Aug 10 18:39:02 2011
The 'set guiuser' command must be run (successfully) before any other commands will work
set guiuser admin
Enter current password
192.168.1.89>
```

6. Grant any additional roles, if desired, to allow access to the user to execute GuardAPI functions.

For example, if the user johnsmith were to issue the following GuardAPI command, he would find out he does not have any API commands to execute:

```
192.168.1.89 >grdapi commands user
ID=0
Matching API Function list:
ok
```

But if we were to grant johnsmith the accessmgr role (previously in step 5) the same GuardAPI command would result in the following API commands being available:

```
192.168.1.89> grdapi commands user
ID=0  Matching API Function list :
create_db_user_mapping
create_user_hierarchy
delete_allowed_db_by_user
delete_db_user_mapping
delete_user_hierarchy_by_entry_id
delete_user_hierarchy_by_user
execute_ldap_user_import
list_allowed_db_by_user
list_db_user_mapping
list_user_hierarchy_by parent_user
update_user_db
ok
```

Parent topic: Access Management Overview

Importing Users from LDAP

You can import Guardium® user definitions from an LDAP server by configuring an import operation to obtain the appropriate set of users.

You can run the import operation on demand, or schedule it to run on a periodic basis. You can elect to have only new users imported, or you can have existing user definitions replaced. In either case, LDAP groups can be imported as Guardium roles.

When importing LDAP users:

- The Guardium admin user definition will not be changed in any way.
- Existing users will not be deleted (in other words, the entire set of users is not replaced by the set imported from LDAP).
- Guardium passwords will not be changed.
- New users being added to Guardium:
  - Will be marked inactive by default
  - Will have blank passwords
  - Will be assigned the user role

Note:

Special characters in a user name is not supported.

When adding a user manually via Access Management (either from Add User or LDAP user import), if there is no first name and/or last name, the login name will be used.

This LDAP configuration menu screen has tool tips for certain menu choices. Move the cursor over a menu choice (such as Object Class for user), and a short description will appear.

Guardium CLI users can not authenticate in the LDAP environment, as there is no privilege separation for the CLI users.

Configure LDAP User Import

The attribute that will be used to identify users is defined by the Guardium administrator, in the User RDN Type box of the LDAP Authentication Configuration panel. See Configure LDAP Authentication for further information. The default is uid, but you should consult with your Guardium administrator to determine what value is being used. If a user is using SamAccountName as the RDN value, the user must use either a =search or =[domain name] in the full name. Examples: SamAccountName=search, SamAccountName=dom

Note: In order to configure LDAP user import, accessmgr user must have the privilege to run Group Builder. In certain situations, when changes are made to the role privilege, accessmgr's privilege to Group Builder can be taken away. This results in an inability to save or run successfully LDAP user import. Go to the access management portal, select Role Permissions from the choices. Choose the Group Builder application and make sure that there is a checkmark in the all roles box or a checkmark in the accessmgr box.

1. Open the LDAP User Import panel by clicking Access > Access Management > LDAP User Import.

   See Example of Tivoli® LDAP Configuration at the end of this help topic for reference in filling out the required information.

2. For LDAP Host Name, enter the IP address or host name for the LDAP server to be accessed.
3. For Port, enter the port number for connecting to the LDAP server.
4. Select the LDAP server type from the Server Type menu.
5. Check the Use SSL Connection check box if Guardium is to connect to your LDAP server using an SSL (secure socket layer) connection.
6. For Base DN, specify the node in the tree at which to begin the search. For example, a company tree might begin like: DC=encore,DC=corp,DC=root
7. For Attribute to Import, enter the attribute that will be used to import users (for example: cn). Each attribute has a name and belongs to an objectClass.
8. Check the Clear existing group members before importing check box if you want to delete all existing group members before importing.
9. For Log In As and Password, enter the user account information that will connect to the Guardium server.
10. For Search Filter Scope, select One-Level to apply the search to the base level only, or select Sub-Tree to apply the search to levels beneath the base level.
11. For Limit, enter the maximum number of items to be returned. We recommend that you use this field to test new queries or modifications to existing queries, so that you do not inadvertently load an excessive number of members.
12. **Optional:** For Search Filter, define a base DN, scope, and search filter. Typically, imports will be based on membership in an LDAP group, so you would use the memberOF keyword. For example: memberOf=CN=syyTestGroup,DC=encore,DC=corp,DC=root
13. Click Apply to save the configuration settings.
    Note: The Status indicator in the Configuration - General section will change to *LDAP import currently set up for this group as follows* and the Modify Schedule and Run Once Now buttons will be enabled. You can now import from your LDAP server.

Schedule LDAP User Import

If LDAP Import has not yet been configured, you must perform Configure LDAP User Import before performing this procedure.

1. Open the LDAP User Import panel by clicking Access > Access Management > LDAP User Import.

Run LDAP User Import

When you run LDAP user import on demand, you have the opportunity to accept or reject each of the users returned by the query. This is especially useful for testing purposes. If LDAP Import has not yet been configured, you must perform Configure LDAP User Import before performing this procedure.

1. Open the LDAP User Import panel by clicking Access > Access Management > LDAP User Import.
2. Click Run Once Now. After the task completes, the set of members satisfying your selection criteria will be displayed in the LDAP Query Results panel.
3. In the LDAP Query Results panel, mark the check box for each user you want added, and click Import (or click Cancel to return without importing any users).
4. To view the added users, open the User Browser by clicking Access > Access Management > User Browser. Verify that the correct user accounts have been added.

Example of Tivoli LDAP Configuration

Table 1. Example of Tivoli LDAP Configuration

LDAP Host Name	Values
Port	389
Server Type	Tivoli Directory

LDAP Host Name	Values
Use SSL connection	
Base DN	cn=sample realm,o=sample
Import Mode	Choose Override existing attributes
Disable user if not on import list	
Enable new Imported Users	
Log in as	cn=root
Password	
Search filter scope	Sub-Tree
Limit	
Attribute to Import as User Login	cn (Configurable through Portal)
Search filter	
Object Class for User	Fill with Default Value - |(objectClass=organizationalPerson)(objectClass=inetOrgPerson)(objectClass=person)
Import Roles	Add a Checkmark
Attribute to Import as Role	cn
Role Search Base DB	Fill with Default Value - cn=sample realm,0=sample
Role filter	
Object Class for Role	Fill with Default Value - |(objectClass=groupOfNames)(objectClass=group)(objectClass=groupOfUniqueNames)
Attribute in User to Associate Role	Fill with Default Value - memberOf
Attribute in Role to Associate User	Fill with Default Value - member

Parent topic: Access Management Overview

Data Security - User Hierarchy and Database Associations

You can use data security features to create a hierarchy of users and associate users to specific databases and servers. Guardium® data security features report on which users accessed what information, and ensure that only specific users see information that they are responsible for.

Follow these steps to enable and use Guardium data security features:

1. Enable Data Security
2. Create a User Hierarchy
3. Create a User to Database Association
4. Filter Results

When data security features are used with the Classification feature (which discovers and classifies sensitive data found in multiple places of the database), the Data Level Security prevents a specified user from seeing classifier results from a specified datasource (datasource definition). Using Data Level Security can also prevent a specified user from seeing Audit Task results when the task type is Classifier.

Enable Data Security

Restriction: Data Level Security and the Investigation Dashboard cannot be enabled concurrently.

1. Log in as the admin user and open the Global Profile by clicking Setup > Global Profile.
2. Click Enable for Data level security filtering.

   Note: The status indicator icon for Data level security filtering will now appear as  .

   You can verify that Data level security filtering is enabled by referencing the Services Status panel (Setup > Services Status).

- With data level security filtering enabled, log in as the accessmgr to use the User Hierarchy and User-DB Association features.

Create a User Hierarchy

The User Hierarchy shows you the parent-child relationships between all users. User hierarchies permit the parent of the relationship to look at specified servers and databases, but not the children.

Log in as accessmgr and open the User Hierarchy by clicking Data Security > User Hierarchy.

Do one of the following:

- Click Full Update Active User-DB Map to view the full hierarchy of users.
- Use the Roles and Users filters to view the hierarchy for a specific user or role. Right-click a node in the hierarchy to expand or collapse the tree, or add a user to a specific hierarchy.
- Click Refresh Cached Hierarchy to update the hierarchy.

Note: Depending on the configuration, inheritance can also take place where the parent inherits the data-level security of the child.

Create a User to Database Association

The User-DB Association feature maps users to specific databases to ensure that users see only data that they are permitted to view.

Log in as accessmgr and open the User-DB Association by clicking Data Security > User-DB Association.

Do one of the following:

1. View the current mapping of users to databases by clicking Full Update Active User-DB Map.
2. Create a new User-DB association map by selecting options from the Server & Service Name Suggestion list and clicking Go.
   Note: Once the map is fully updated, you will see a tree listing all your servers. Click any node in the tree to view which users are currently associated with that node.

   If you are using dual-stack configuration, there is a root node, and two trees of addresses to choose from. One tree is for the IPV4 address, and the longer tree is for the IPV6 address.

   Add a user or group to a node by selecting the node and clicking Add user or Add group.

Central Management

On a Central Management appliance, there is also a box on the User-Database Associations screen that allows a user to create database associations based on data from a managed node. Select a remote source from only a box that appears for Central Management appliances. Also, there is a check box to get data from ALL managed nodes.

Filter Results

Data level security at the observed data level requires the filtering of data for specific users and the specific databases they are responsible for.

Filtering at the system level is based on the User Hierarchy and User-DB Association so that users will see only information from their assigned databases for the various reports, audit processes, security assessments, and so on, within the Guardium system.

Log in as the admin user and use the Global Profile to filter results. Open the Global Profile by clicking Setup > Global Profile.

- Default filtering:
  - Show all - This option is available only if the user logged in has the special role *datasec-exempt* defined, which allows the user to see all data as if there was no data level security.
  - Include indirect records - This check box shows the viewer not only the rows that belong to the user logged in, but also all the rows that belong to other users within that hierarchy.
- Audit Process Escalation: Escalation is allowed for tasks on this type only to users who have the datasec-exempt role. Users without the datasec-exmpt role are not shown in the escalation list.

  Escalate results to all users - A check mark in this check box escalates audit process results (and PDF versions) to all users, even if data level security at the observed data level is enabled. The default setting is enabled. If the check box is disabled (no check mark in the check box), then audit process escalation only will be allowed to users at a higher level in the user hierarchy and to users with the datasec-exempt role. If the check box is disabled, and there is no user hierarchy, then no escalation is permitted.

- PDF and CSV generation for results (attached to email) distribution will use the default global profile values set in Administration Console parameters.
- PDF and CSV generated from the viewer will use the same filtering as in the screen.

Note:

The Data Security User to Database Association filters reports only from the following domains: Access; Exception; and, Policy Violations (as well as custom domains using these domains or tables from these domains). All other domains (reports) are not filtered by the Data Security User to Database Association.

Users with admin role will be able to see event types on all roles (the information will still be filtered based on observed data level security parameters).

If Data Level Security is turned on, predefined entities added to a custom domain need to be in the same domain(s) for the data level security filtering to work properly.

If Data Level Security is on, and two predefined entity subjects are trying to send data from two domains (not Custom Domains) that are using a filtering policy, then the sending of the two predefined entity subjects will not be permitted. Data Level Security can only enforce one kind of filtering policy (for example, there can be only one policy depending on server_ip/service_name and one policy depending on datasource).

Parent topic: Access Management Overview

How to define User Hierarchies

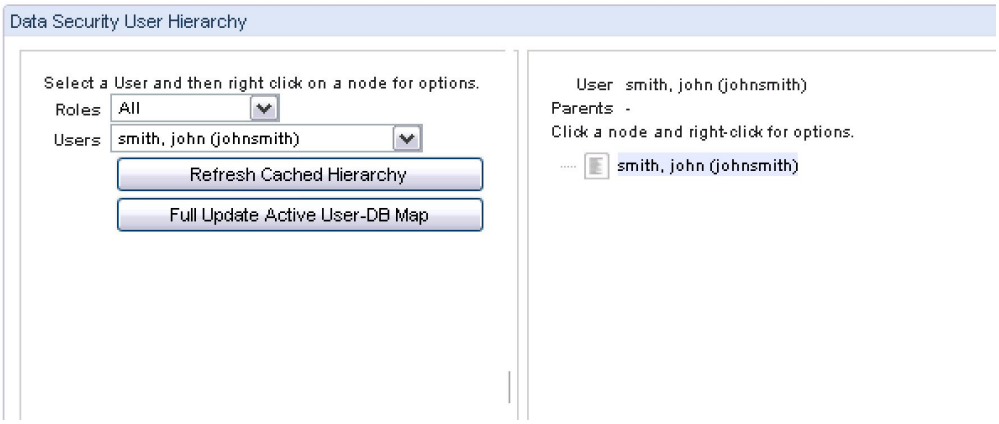
Use the UI from an access manager account to easily define user hierarchies.

About this task

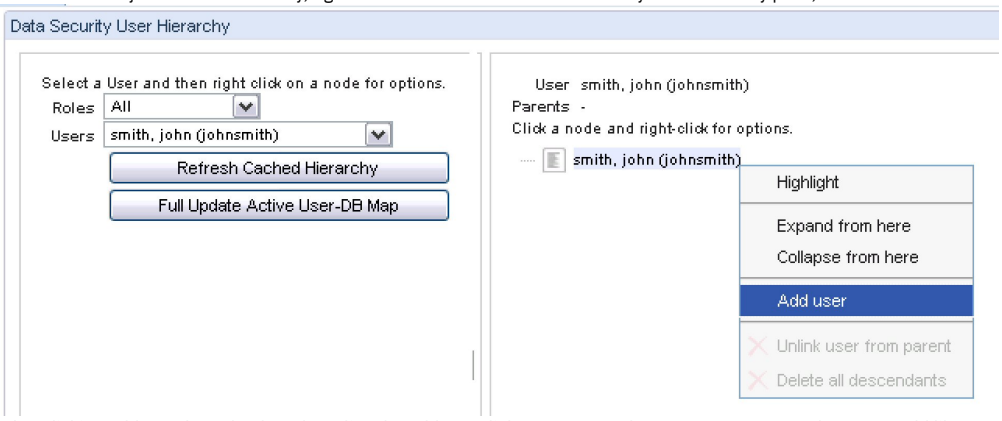
The Data Security User Hierarchy represents the parent-child relationships between users; allowing for the creation and enforcement of a data-level security by permitting the parent of a hierarchy to look at specified servers and databases, but not the children. Depending on the configuration, inheritance can also take place in that the parent inherits the data-level security of the child.

Procedure

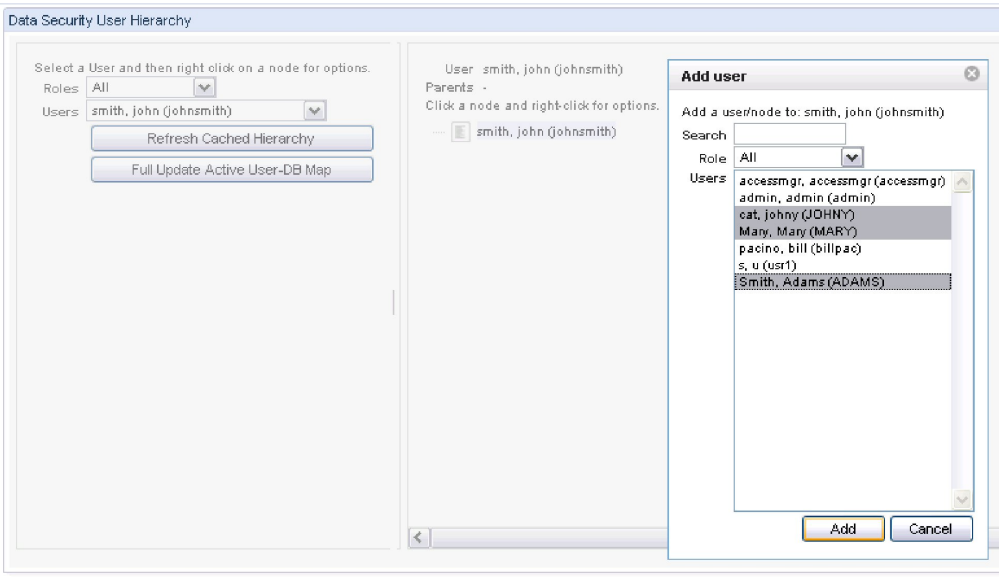
1. Login as accessmgr and click Data Security > User Hierarchy.
2. Select a user from the Users drop-down menu to display it in the Data Security User Hierarchy pane. This example uses john smith as a user.



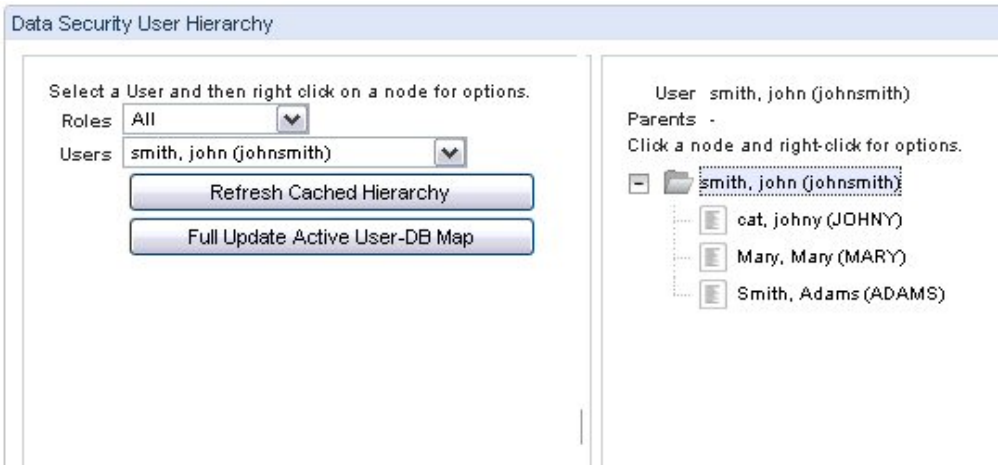
3. To add a user to john smith's hierarchy, right-click on the user in the Data Security User Hierarchy pane, and select Add user from the drop-down menu.



4. After clicking Add user from the drop down list, the Add user dialog appears. Select one or more users that you would like to add to the user's hierarchy, and then click Add.



5. After adding the users to a hierarchy, the Data Security User Hierarchy panel will be refreshed; allowing the user to drill down and see the new hierarchy.



6. Repeat the steps until all required users are defined to the data security user hierarchy.

Parent topic: Access Management Overview

Guardium UI Login using a Smart card

Guardium Smart card support meets the United States government mandate that all vendors must support multi-factor authentication for user access. Smart card authentication is supported only for access to the web-based Guardium user interface (UI).

Before you begin

Details of the multi-factor authentication requirement are found in the Identification and Authentication (Organizational Users) (IA-2) section the Security and Privacy Controls for Federal Information Systems and Organizations (NIST Special Publication 800-53) document. NIST 800-53 is available through the NIST web site: https://www.nist.gov .

Government applications refer to Personal Identification and Verification Cards (PIV). Civilian applications refer to Common Access Cards (CAC). PIV and CAC cards have different certificate authorities, but the cards are otherwise the same.

Guardium Smart card support meets the HIGH confidence PIV assurance level described in the PIV Cardholder Authentication (6) section of the Personal Identity Verification (PIV) of Federal Employees and Contractors (FIPS Publication 201-2) document. FIPS 201-2 is available through this NIST web site: https://www.nist.gov .

Prerequisites

The device requires the following:

- Access to the Guardium UI via a web browser that can access the Smart card certificate
- A Smart card reader
- A valid PIV/CAC card

About this task

This task describes how to correctly associate the information on a Smart card with a Guardium user.

Create Guardium users to associate with Smart cards. If you want to associate existing users with Smart cards, you do not need to create any new users. For more information about user creation and access management, see Access Management Overview.

1. Login to the Guardium UI as the admin user.
2. Navigate to Setup > Tools and Views > Portal.
3. Under the Authentication Configuration section, select the Smart Card option. If the Smart Card option is not present, verify that the Smart card patch is installed.
4. In the Regex Match Pattern field, provide a regular expression (regex) that matches user information on a Smart card.

Example

Create Users

The Guardium application provide various ways for users to be created. It doesn't matter how your users are created, and once you configure your web to use the Smart card for authentication it only uses the Smart card credential to establish SSL/TLS communication (Guardium site uses https).

Here is an example how to manually create a user:

1. Login as Accessmgr on CM
2. Select AccessUser Browser.
3. Click Add.
4. Add Username Test Cardholder X
5. Add password twice
6. Enter first name and last name same as user
7. Click Add.

Now you will configure the mapping, so when a Smart card is present, the information on the Smart card will be correctly mapped to a user in the system.

1. Login as Admin from CM or standalone.
2. After you login, navigate to Setup > Tools and Views > Portal.

If you see a menu screen titled Authentication Configuration, then you have the Smart card support patch installed.

Now use a regular expression, in the Regex Match Pattern, to match the user information on the Smart card. Here is an example of a Regex Match Pattern:

CN ?= ?(.*?), ?OU ?= ?Test Agency, ?OU ?= ?Test Department, ?O ?= ?Test Government, ?C ?= ?US

This works with a Smart card with client certificate, the client certificate you selected to send to the webserver to establish HTTPS. On the Smart card you selected, this client certificate gives to the webserver when the server requests it, which is exactly what happens when this feature is enabled. An example of the client certificate has the details: Version, Serial number, Signature algorithm, Signature hash algorithm, Issuer, Valid from, Valid to, Subject.

In this example you can use one of the following patterns. They both will match the mapping. Pattern 1 is more exact. Pattern 2 depends on your purpose, you can write your own to match your needs. You need to work with someone who is familiar with the data on the Smart card to write efficient mapping patterns.

Pattern 1:

CN ?= ?(.*?), ?OU ?= ?Test Agency, ?OU ?= ?Test Department, ?O ?= ?Test Government, ?C ?= ?US

Pattern 2:

CN ?= ?(.*?)

Both of the examples will get the value for CN attribute in the certificate subject which you can see by examine the detail of the certificate from the browser. In this case it is Test Cardholder X. Configure this pattern correctly is probably the most important part to make sure the authentication on Smart card is successful.

Note that the regex validation tool currently available for other modules is not available for this purpose. (see Troubleshooting section, items 2 and 3).

Now save it. Note, you are not done yet and you need to enable it from CLI since part of the enablement can only be done after the server is shut down, during which there is no GUI.

Before you leave GUI for the CLI part, you need to upload the root CA certificate to the trust store.

Upload the root CA certificate to web server trust store

This part describes how you upload the root CA's certificate into the trust store used by the GUI. Use the Import Certificate selection from the Guardium Portal and Authentication Configuration screens.

If you do not have the root certificate of the CA that signed the certificates on the Smart cards, you can export a root certificate from a CA-signed user certificate or a Smart card that contains one.

We assume you obtained the certification either by having it given to you by the customer or exporting it from a Smart card using certification management tools such as certMgr.exe or tools like open SSL.

The public root certificate of a trusted CA. This is the most common source of a root certificate in environments that already have a Smart card infrastructure and a standardized approach to Smart card distribution and authentication.

Select a certificate to use for Smart card authentication. The signing chain lists a series of signing authorities. The best certificate to select is usually the intermediate authority above the user certificate.

Enabling the feature from CLI (can only be done in CLI)

To check the status, use the CLI command,

```
show system websmartcard
```

To turn on this CLI command, use

```
store system websmartcard on
```

To turn off this CLI command, use

```
store system websmartcard off
```

When the feature is turned off, the GUI is automatically restarted with the system using local authentication. This is also useful when you first deploy the system and the regular expression you set is not quite right and you see errors.

Note: While the Smart card authentication is used to authenticate, the access control (for example, what module a user has access, what navigation the user has) is still done through the same way as without Smart card authentication.

After enabling the feature

Once the feature is enabled, you can only access the site with a valid Smart card (PIV, CAC etc.)

Now when you visit the GUI site, you'll see an authentication prompt, asking you to choose a certificate.

The above details are for an administrator to set it up. As for end user, if it is set right, the user just needs to put the card in and the user will go straight to the site content.

For a user with a valid Smart card, when the user load the websites, the browser will prompt for a Smart card pin. This pin allows the client certificate on the card is access when requested.

After the pin is provided, the regular Guardium login page will display with the user field pre-filled with the login extracted from the Smart card. Note there is no password used here. The only thing you see in the user field is the extracted user place holder for mapping.

For example, if the certificate are valid and the root CA of the Smart card issuer for Test Cardholder X is loaded in Guardium web server (See section Upload the root CA's certificate for how to do it), the user field will be pre-filled with Test Cardholder X and prompt you for the Smart card pin. This is to access the client certificate on the Smart card. The client certificate stays on the Smart card and you cannot export it into a file. You may see the prompt twice and just provide the pin.

What to do next

Troubleshooting or recovery scenarios

After the feature is enabled, when you load Guardium URL, you see an error page.

Diagnostic: Most likely, your configuration of the matching regular expression is not right or you don't have a valid certificate on the card.

You created a matching Regex and it does not seem to be working. You remember that Guardium has a regex validation tool and used it thinking that if it works in the tool, it's a good Regex. Unfortunately, while the test is successful in that tool, the Regex pattern doesn't work for Smart Card Configuration.

Diagnostic: That tool is to find if an expression can be found inside a text paragraph. So it won't work in this case. This configuration is to extract a piece of text from the certificate text as displayed in the subject as shown in certificate details.

You didn't get prompt from the browser to select a certificate at all.

Diagnostic: PC/laptop is able to install the card reader and the Smart card. A copy of the certificate in the Smart card gets copied to the certmgr in Windows OS. However, when accessing the site, browser (IE or Firefox or Chrome) does not read the certificate. In other words, all the three browsers are unable to read the certificate and there is no prompt to choose the certificate.

This has been noted on all browsers on some laptops we tested. If this is the case, it's not only happening to Guardium site. Other sites that require Smart cards to operate will also experience this. This is rare.

Solution: Contact the department that manages your Smart card.

Parent topic: Access Management Overview

Aggregation and Central management

Aggregation enables you to bring together data from multiple Guardium systems for a consolidated view. Central management enables you to maintain consistency among your Guardium systems.

- Aggregation
  Collect and merge information from multiple Guardium® units into a single Guardium Aggregation appliance to facilitate an enterprise view of database usage.
- Central Management
  In a central management configuration, one Guardium unit is designated as the Central Manager. That unit can be used to monitor and control other Guardium units, which are referred to as managed units. Un-managed units are referred to as stand-alone units.
- Investigation Center
  Investigation Center is an extension of the Aggregation Servers. Investigation Users (once defined) can restore data and results of selected historic dates and perform forensic investigation. Once the days (dates) are restored, the investigation users can define and view reports using the standard Guardium UI, only in the scope of the investigated dates.

Aggregation

Collect and merge information from multiple Guardium® units into a single Guardium Aggregation appliance to facilitate an enterprise view of database usage.

Aggregation Process

- Accomplished by exporting data on a daily basis from the source appliances to the Aggregator (copying daily export files to the aggregator).
- Aggregator then goes over the uploaded files, extracts each file and merges it into the internal repository on the aggregator.

For example, if you are running Guardium in an enterprise deployment, you may have multiple Guardium servers monitoring different environments (different geographic locations or business units, for example). It may be useful to collect all data in a central location to facilitate an enterprise view of database usage. You can accomplish this by exporting data from a number of servers to another server that has been configured (during the initial installation procedures) as an aggregation appliance. In such a deployment, you typically run all reports, assessments, audit processes, and so forth, on the aggregation appliance to achieve a wider view, not always an enterprise view. Note: The Aggregator does not collect data, but it is used to present the data from the collectors.

Pre-defined aggregation reports can be located on the Guardium Monitor tab, Enterprise Buffer Usage Monitor, and the Daily Monitor tab, Logging Collectors.

Appliance Types

Collector
: Used to collect database activity, analyze it in real time and log it in the internal repository for further analysis and/or reacting in real-time (alerting, blocking, etc.). Use this unit for the real-time capture and analysis of the database activity.

Aggregator (see notes 1, 2)
: Used to collect and merge information from multiple appliances (collectors and other aggregators) to produce a holistic view of the entire environment and generate enterprise-level reports. The Aggregator does not collect data itself; it just aggregates data from multiple sources.

Central Manager (see notes 1, 3, 4)
: Use this Appliance to manage and control multiple Guardium appliances.
With Central Manager (CM), manage the entire Guardium deployment (all the collectors and aggregators) from a single console (the CM console).
This includes patch installation, software updates and the management and configuration of queries, reports, groups, users, policies, etc.

Note:

In many environments, the Central Manager is also the Aggregator. Central Manager and Aggregator can be installed on the same appliance.

Guardium appliance needs to be configured as an Aggregator at install time, in order to be promotable to a Central Manager.

One Central Manager per federated environment

Central Manager/Aggregator enforcement
: Starting with v9.5 (v9.0 patch 500), the application will enforce that a Central Manager has to be an Aggregator-type appliance. This would mean that starting with v9.5, only aggregator-type appliances would be promotable to the Central Manager appliance. Pre-existing pre-v9.5 CM appliances are not subject to this change.

Solution for unit showing as down after upgrade

Issue: When upgrading the Aggregator with search mode in CM_only or Local_only mode, this unit shows as down in search post upgrade. Also, if after upgrade, user chooses to change search mode to all_machines search will not be available from the Aggregator.

Solution: Once the Aggregator unit has been upgraded and the user does not want to see the aggregator unit to show as down on the search tooltip, User can run the two commands below

1. grdapi enable_quick_search schedule_interval=2 schedule_units=MINUTE
2. restart network

Note: If the environment was in and will be in cm_only or local_only mode, this step will not enable search from aggregator, just make it so that aggregator does not show as down.

Terminology

Table 1.

Term	Description
Guardium Appliance	The physical or virtual Guardium box; can be either a “collector” or an “aggregator” (with or without central management)
Guardium Unit	See Guardium Appliance
Manager Unit	An appliance configured as Central Manager
Managed Unit	An appliance managed by the Central Manger
Standalone Unit	An appliance not in a Central Manager environment
Purge	For the best performance, purge all data that is not needed. Purge to free disk space.
Archive	Compress the data of a single day into an encrypted file and send it to the aggregator.

Hierarchical Aggregation

Guardium also supports hierarchical aggregation, where multiple aggregation appliances merge upwards to a higher-level, central aggregation appliance. This is useful for multi-level views. For example, you may need to deploy one aggregation appliance for North America aggregating multiple units, another aggregation appliance for Asia aggregating multiple units, and a central, global aggregation appliance merging the contents of the North America and Asia aggregation appliances into a single corporate view. To consolidate data, all aggregated Guardium servers export data to the aggregation appliance on a scheduled basis. The aggregation appliance imports that data into a single database on the aggregation appliance, so that reports run on the aggregation appliance are based on the data consolidated from all of the aggregated Guardium servers.

About the System Shared Secret

The Guardium administrator defines the System Shared Secret on the System Configuration panel, which is described in the following section. The system shared secret is used for archive/restore operations, and for Central Management and Aggregation operations. When used, its value must be the same for all units that will communicate. This value is null at installation time, and can change over time.

The system shared secret is used:

- When secure connections are being established between a Central Manager and a managed unit.
- When an aggregated unit signs and encrypts data for export to the aggregator.
- When any unit signs and encrypts data for archiving.
- When an aggregator imports data from an aggregated unit.
- When any unit restores archived data.

Depending on your company’s security practices, you may be required to change the system shared secret from time to time. Because the shared secret can change, each system maintains a shared secret keys file, containing an historical record of all shared secrets defined on that system. This allows an exported (or archived) file from a system with an older shared secret to be imported (or restored) by a system on which that same shared secret has been replaced with a newer one. Shared secrets (current and historic ones) can be exported from one appliance and imported to another through the CLI.

For aggregation to work, the shared secret must be set and be the same for aggregator and all aggregated collectors.

Aggregating, Archiving, and Purging Operations

Scheduled export operations send data from Guardium collector units to a Guardium aggregation appliance. On its own schedule, the aggregation appliance executes an import operation to complete the aggregation process. On either or both units, archive and purge operations are scheduled to back up and purge data on a regular basis (both to free up space and to speed up access operations on the internal database). The export, archive, and purge functions can work on the same data, but not the same date ranges. For example, you may want to export and archive all information older than one day and purge all information older than one month, thereby always leaving one month of data on the sending unit.

Note:

When setting the schedule of import on an aggregator, it should be planned to run after export is completed on all collectors.

CAS data is also aggregated and archived.

Note: The alert for no traffic is inactive for aggregator servers.

Managing Data on an Aggregator

- Exporting Data
  - Stopping Export
- Importing Data
  - Stopping Import
- Archiving and Purging

- Stopping Archiving and Purging
- Verify Archiving and Purging Process
- Reporting on Aggregation and Archiving Activity
- Restoring

Exporting Data

Table 2. Exporting Data

Topic	Description
Function	Compress the data of a single day (midnight to midnight, typically - yesterday) into an encrypted file and send it to the aggregator (or to an external repository on Archive).
Schedule	Executed on a daily basis. Starts immediately after midnight (00:10) to include full day's data. Assumed to take up to 2 hours to complete (Average – dependent on amount of data).
High Level Process	Create a temporary database. Load the relevant data (last day's activity) to the tmp db. Update auto-increment IDs in tmp db to ensure uniqueness. Create an encrypted compressed export file of the tmp database. Copy the export file to the aggregator (or to an external repository on Archive).

To export data to an aggregation appliance, follow the procedure. You can define a single export configuration for each Guardium unit.

1. Click Manage > Data Management > Data Export to open Data Export.
2. Check the Export box as this will open additional options for exporting data.
3. In the boxes following Export data older than, specify a starting day for the export operation as a number of days, weeks, or months prior to the current day, which is day zero. These are calendar measurements, so if today is April 24, all data captured on April 23 is one day old, regardless of the time when the operation is performed. To archive data starting with yesterday's data, enter the value 1.
4. Optionally, use the boxes following Ignore data older than to control how many days of data will be archived. Any value specified here must be greater than the Export data older than value, so you always export at least two days of data. If you leave the Ignore data older than blank, you export data for all days older than the value specified in the Export data older than row; It is recommended to always set the Ignore older than value, otherwise you will be exporting the exact same days over and over again; overloading the network and the aggregator with redundant data (that will be ignored).
5. The Export Values box is checked by default. In some cases, where the collector resides in a country that prohibits the export of data, and the aggregation appliance resides in another country, you would want to clear the Export Values check box, which would mask all fields containing database values.
6. In the Host box, enter the IP address or DNS host name of the aggregation appliance to which this system's encrypted data files will be sent. There is also an option to enable a secondary aggregation for export data over more then one aggregator. There are two Host boxes available, the first one is required, while the Secondary Host is an option. This unit and the aggregation appliance to which it is sending data must have the same System Shared Secret. If not, the export operation works, but the aggregation appliance that receives the data is not able to decrypt the exported file and the Import will fail. See System Shared Secret in System Configuration for more information. The Shared Secret is required to be identical on both exporting system and receiving system. The reason for this is that unless they have same shared secret, the configuration on the exporting system will not be set and there will be a message for a test file that can not be sent to the receiving system.
7. Use the Scheduling section to define a schedule for running this operation on a regular basis.
8. Click the Save button to save the export and purge configuration for this unit. When you click the Apply button, the system attempts to verify that the specified aggregator host will accept data from this unit. If the operation fails, the following message is displayed and the configuration will not be saved: A test data file could not be sent to this host. Please confirm the hostname or IP address is entered correctly and the host is online.
9. Click Run Once Now to run the operation one time.

Stopping Export

To stop the export of data to an aggregation appliance:

1. Click Manage > Data Management > Data Export to open Data Export.
2. Clear the Export checkbox.
3. Click Save.

Note: Stopping an export after the Run Once Now button has been clicked is impossible.

Importing Data

The Guardium collector units export encrypted data files to another Guardium appliance configured as an aggregation appliance. The encrypted data files reside in a special location on the aggregation appliance until the aggregation appliance executes an import operation to decrypt and merge all data to its own internal database.

Note: To avoid the possibility of importing files that have not completely arrived, the aggregation appliance will not import files that have changed in the last two minutes.

Table 3. Importing Data

Topic	Description
Function	Import and merge the imported data into the internal databases of the Aggregator.
Schedule	Executed on a daily basis. Do not run more than once a day. Starts at 02:00 (or after export has ended). Assumed to take up to 3 hours to complete.
High Level Process (for each purged day)	Construct the delete command for each purged table (tables and the purge conditions defined in AGG_TABLES). Execute the delete commands for each of the tables.

Follow the procedure to define the Data Import operation on an aggregation appliance. You can define only a single Data Import configuration on each unit.

1. Click Manage > Data Management > Import to open Import.
2. Check the Import checkbox which causes the appearance of an additional non-modifiable field indicating the location of the data files to be imported.
3. Click Apply to save the configuration. The Apply button is only available when you toggle the Import data from checkbox on or off.
4. Click Run Once Now to run the operation once.
5. Click Modify Schedule to schedule the operation to open the general-purpose task scheduler and run on a regular basis. This aggregation appliance and all units exporting data to it must have the same System Shared Secret. If not, the export operations will still work, but the aggregation appliance will not be able to decrypt the files of exported data.

Stopping Import

To stop importing data sent from other Guardium units:

1. Click Manage > Data Management > Import to open Import.
2. Clear the Import data box.
3. Click Apply to save the configuration. Stopping importing does not stop other Guardium units from exporting data to this system. To stop that, you must stop the Export operation on each sending unit.

Note: Stopping an import once the RUN ONCE NOW button is clicked is impossible.

Archiving and Purging

Archiving and purging data on a regular basis is essential for the health of your Guardium system. For the best performance, we strongly recommend that you archive and purge all data that is not needed. Important - purge to free disk space. For example, if you only need three moths of data on the Guardium appliance, archive and purge all data that is older than 90 days.

The archive and purge process frees space and preserves information for future use. You should periodically archive and purge data from standalone units and from aggregation units. The Guardium's archive function creates signed, encrypted files that cannot be tampered with. Archive files are transferred and stored on external systems such as file servers or storage systems.

Note:

If both Archive and Purge are scheduled, Purge will run after Archive.

Data that was archived on a collector can be restored either on another collector or an aggregator server. Restoring of data that was archived on an aggregator to a collector machine is not supported.

Archiving data on aggregator system - on the first day of the month, all static tables are archived. On all other days, only additional data added to archived data will be archived. This methodology is the same as used by collectors. Adding the static tables to the normal purge process eliminates the existence of orphans, freeing up disk space and improving report performance.

Archive and export of static tables on an aggregator includes full static data only on the first day of the month (archive) or when the export configuration changes (export). Use the CLI commands, store archive_table_by_date [enable | disable] or show archive_table_by_date. Other relevant CLI commands are store aggregator clean orphans or show aggregator clean orphans.

Scheduling Data Management tasks - Default schedule times are supplied when the unit is built and these can be amended accordingly. The Data Management tasks should be scheduled at less busy times, for example, overnight. They should be spaced out so as not to overlap (for example, the start of one task should not run into the start of another before finishing.)

Aggregator Data Archive, when dealing with an Aggregator/ Central Manager that performs Data Imports and Data Archives. A default or common setting is to have the Data Archive perform an Archive of data older than one day ignoring data older than two days. If it happens that the Data Archive is scheduled to run BEFORE the Data Imports from other Collector(s)/Aggregator(s), then the Archive will NOT contain the Imports meant for that days Archive. Imagine the following schedule: Data Archive to run at 30 minutes past Midnight; Data Imports to run at 6:00 AM for data older than 1 day - ignoring older than 2 days. When the Archive happens - it will not Archive any relevant yesterday data - no Imports for that days data have yet occurred. In this example, the Data Archive should be re-scheduled to occur AFTER the Data Import(s) have finished. This way the Archive would correctly contain data for yesterday.

Table 4. Archiving and Purging Data

Topic	Description
Purge Function	Delete old records from appliance (typically - older than 60 days) to free up space and speed up access operation to the internal database. Purging is based on dates (deleting whole days' worth of data), but will not delete records that are still "in use" (for example: open sessions).
Schedule	The default purge activity is scheduled every day at 5:00 AM. Collectors, after the export/archive. Aggregator, after the import. Assumed to take up to 2 hours to complete.
High Level Process (for each purged day)	Purge configuration is used by both Data Archive and Data Export. Use the Purge data older than field to specify a starting day for the purge operation as a number of days, weeks, or months prior to the current day, which is day zero.

Topic	Description
Default Purging	The default value for purge is 60 days The default purge activity is scheduled every day at 5:00 AM. For a new install a default purge schedule will be installed that is based on the default value and activity When a unit type is changed between manager managed or back to standalone the default purge schedule will be applied The purge schedule will not be affected during an upgrade

It may be necessary to run reports or investigations on this data at some point. For example, some regulatory environments may require that you keep this information for three, five, or even seven years in a form that can be queried within 24-hours. This functionality is supported by the Guardium restore capability, which allows you to restore archived data to the unit.

The following sections describe how to define and schedule archiving and how to restore from an archive.

Note: The archive and restore operations depend on the file names generated during the archiving process. DO NOT change the names of archived files.

Archive data files can be sent to an SCP or FTP host on the network, or to an EMC Centera or TSM storage system (if configured). You can define a single archiving configuration for each unit To archive data to another host on the network and optionally purge data from the unit, follow the procedure.

1. Click Manage > Data Management > Data Archive to open Data Archive.
2. Check the Archive checkbox to expose additional fields for the archive process.
3. In the boxes following Archive data older than, specify a starting day for the archive operation as a number of days, weeks, or months prior to the current day, which is day zero. These are calendar measurements, so if today is April 24, all data captured on April 23 is one day old, regardless of the time when the operation is performed. To archive data starting with yesterday's data, enter the value `1`.
4. Optionally, use the boxes following Ignore data older than to control how many days of data will be archived. Any value specified here must be greater than the value in the Archive data older than field. If you leave the Ignore data older than row blank, you archive data for all days older than the value specified in the Archive data older than row. This means that if you archive daily and purge data older than 30 days, you archive each day of data 30 times (before it is purged on the 31st day). Depending on the archive options configured for your system (using the store storage-system CLI command), you may have EMC Centera or TSM options on your panel. If you select one of those archive destinations, see the appropriate topic.
    a. EMC Centera Archive and Backup
    b. TSM Archive and Backup
5. Enter the IP address or DNS Host name of the host to receive the archived data
6. In the Directory box, identify the directory in which the data is to be stored. How you specify this depends on whether the file transfer method used is FTP or SCP. For FTP, specify the directory relative to the FTP account home directory. For SCP, specify the directory as an absolute path.
7. In the Username box, enter the user name to use for logging onto the host machine. This user must have write/execute permissions for the directory specified in the Directory box.
8. In the Password box, enter the password for the user, then enter it again in the Re-enter Password box.
9. Data Purge
10. Check the Purge checkbox to purge data, whether or not it is archived. When this box is marked, the Purge data older than fields display. It is important to note that the Purge configuration is used by both Data Archive and Data Export. Changes made here will apply to any executions of Data Export and vice-versa. In the event that purging is activated and both Data Export and Data Archive run on the same day, the first operation that runs will likely purge any old data before the second operation's execution. For this reason, any time that Data Export and Data Archive are both configured, the purge age must be greater than both the age at which to export and the age at which to archive.
11. If purging data, use the Purge data older than fields to specify a starting day for the purge operation as a number of days, weeks, or months prior to the current day, which is day zero. All data from the specified day and all older days will be purged, except as noted otherwise. Any value specified for the starting purge date must be greater than the value specified for the Archive data older than value. In addition, if data exporting is active (see Exporting Data to an aggregation appliance), the starting purge date specified here must be greater than the Export data older than value. There is no warning when you purge data that has not been archived or exported by a previous operation. The purge operation does not purge restored data whose age is within the do not purge restored data timeframe specified on a restore operation. For more information, see Restoring Archived Data.
12. Use the Scheduling section to define a schedule for running this operation on a regular basis.
13. Click Save to verify and save the configuration changes. When you click the Save button, the system attempts to verify the specified Host, Directory, Username, and Password by sending a test data file to that location.
14. Click Run Once Now to run the operation once.

Orphan cleanup on aggregators

When the aggregator includes restored data, orphans cleanup related to the restored data will be set to run according to the expiration date set when data was first restored.

If any changes are done through GuardAPI commands related to the expiration date, this will not affect the date restored data that is available for Orphans cleanup.

For example: The user restores data and wants to keep this data for 7 days. This means the expiration date of this data will be in 7 days from today and this data will be available for orphan cleanup after 7 days.

If the expiration date is changed (set to keep the data for shorter/longer period - it won't affect the date this data is available for orphan cleanup. Customer should pay attention for this especially if they change the expiration period to be longer - in order not to lose data), then the rest of the data on the machine will be available for orphan cleanup as first designed.

EMC Centera Archive and Backup

To use EMC Centera:

1. Click Manage > Data Management > Data Archive to open Data Export.
2. Click on the Data Archive or System Backup in the Data Management section. Initially, the Network radio button is selected by default, and the Network backup parameters are displayed
3. Select the EMC Centera radio button. The EMC Centera parameters will be displayed on the panel.
4. In the Retention box, enter the number of days to retain the data. The maximum is 24855 (68 years). If you want to save if for longer, you can restore the data later and save it again.
5. In the Centera Pool Address box, enter the Centera Pool Connection String; for example: `10.2.3.4,10.6.7.8/var/centera/profile1_rwe.pea`

6. Click Upload PEA to upload a Centera PEA file to be used for the connection string.
7. Click Save to save the configuration. The system will attempt to verify the Centera address by opening a pool using the connection string specified. If the operation fails, you will be informed and the configuration will not be saved.

TSM Archive and Backup

When you select TSM as an archive or backup destination, the TSM portion of the archive or backup configuration panel expands. Before setting TSM as an archive or backup destination, the Guardium system must be registered with the TSM server as a client node. A TSM client system options file (dsm.sys) must be created (on your PC, for example) and uploaded to Guardium. Depending on how that file is defined, you may also need to upload a dsm.opt file. For help creating a dsm.sys file for use by Guardium, consult with your company's TSM administrator. To upload a TSM configuration file, use the CLI command, import tsm config.

The TSM (or Spectrum Protect client) lifecycle is defined by the Spectrum Protect product terms.

To use TSM:

1. Click Manage > Data Management > Data Archive to open Data Archive.
2. Select the TSM radio button. The TSM parameters will be displayed on the panel.
3. In the Password box, enter the TSM password that this Guardium unit uses to request TSM services, and re-enter it in the Re-enter Password box.
4. Optionally enter a Server name matching a servername entry in your dsm.sys file.
5. Optionally enter an As Host name.
6. Click Save to save the configuration. When you click the Apply button, the system attempts to verify the TSM destination by sending a test file to the server using the dsmc archive command. If the operation fails, you will be informed and the configuration will not be saved.

Stopping Archiving and Purging

1. Click Manage > Data Management > Data Archive to open Data Archive.
2. Clear the Archive or Purge box.
3. Click Save.

Verify Archiving and Purging Process

1. Click Reports > Guardium Operational Reports > Aggregation/Archive Log to open the Aggregation/Archive Log.
2. Check to ensure that each Archive/Purge operation has a status of Succeeded.

Reporting on Aggregation and Archiving Activity

1. Navigate to Manage > Reports > Data Management > Aggregation/Archive Log to open the Aggregation/Archive Log.
2. Define a query and build a report.

Restoring

As described previously, archives are written to a SCP or FTP host, or to a Centera or TSM storage system. To restore archives, you must copy the appropriate file(s) back to the Guardium system on which the data is to be restored. There is a separate file for each day of data. Depending on how your archive/purge operation is configured, you may have multiple copies of data archived for the same day. Archive and export data file names have the same format: <daysequence>-<hostname.domain>-w<run> datestamp>-d<data_date>.dbdump/TAR file. To restore file for archived data (and not backup system), you need to use the GUI screen called Catalog Archive. The archive and restore operations depend on the file names generated during the archiving process. DO NOT change the names of archived files. If a generated file name is changed, the restore operation will not work.

For example: 732423-g1.guardium.com-w20050425.040042-d2009-04-22.dbdump/TAR file.

Unless you are restoring data from the first archive created during the month, you will need to restore multiple days of data. That is because when restoring data, Guardium needs to have all of the information that it had when the data being restored was archived. After the archive was created, some of that information may have been purged due to a lack of use. All information needed for a restore operation is archived automatically, the first time that data is archived each month. So, when restoring data, you can restore the first day of the month and all the following days until the desired day or restore the desired day and then the first day of the following month

For example, to restore June 28th, either restore June 1st through June 28th, or restore June 28th and July 1st.

To restore file for archived data (and not backup system), you need to use the GUI screen called Catalog Archive. The archive and restore operations depend on the file names generated during the archiving process. DO NOT change the names of archived files. If a generated file name is changed, the restore operation will not work.

1. Click Manage > Data Management > Data Restore to open Data Restore.
2. Enter a date in the From box, to specify the earliest date for which you want data.
3. Enter a date in the To box, to specify the latest date for which you want data.
4. In the Host Name box, optionally enter the name of the Guardium appliance from which the archive originated.
5. Click Search.
6. In the Search Results panel, mark the Select box for each archive you want to restore.
7. In the Don't purge restored data for at least box, enter the number of days that you want to retain the restored data on the appliance.
8. Click Restore.
9. Click Done when you are finished.

Troubleshooting

On an escalation to technical support, please supply a detailed log from the time when the problem occurred. Navigate to Manage > Reports > Data Management > Aggregation/Archive Log and define a report for the time period in question.

Calculating maximum number of Collectors per Aggregator

When a Guardium system is built from an .ISO, a default value of 10 for the maximum number of collectors per aggregator is set.

When a customer upgrades the Guardium system, the system calculates the maximum number of collectors using the following logic:

1. Get number of collectors according to data in internal Guardium table. The default value is 10.
2. If results of step 1 is 0 (no collectors are found), the system sets this value to 10.
3. If a different number of collectors is found, the system will add 20 percent more to the number determined in step 2.
4. For example, if Step 1 did not find any collectors, then Step 2 will set a value of 10, and then Step 3 will add 20% to it and will make it 12.
5. Another example, in Step 1 the system found five collectors exporting to an aggregator. In this case, the value is set to 5. Step 2 is not relevant as result was 5 and not 0. Step 3 will add 20% to 5 and will set this value to 6.

Parent topic: Aggregation and Central management

Central Management

In a central management configuration, one Guardium® unit is designated as the Central Manager. That unit can be used to monitor and control other Guardium units, which are referred to as managed units. Un-managed units are referred to as stand-alone units.

The concept of a local machine can refer to any machine in the Central Management system. There are some applications (Audit Processes, Queries, Portlets, etc.) which can be run on both the Managed Units and the Central Manager. In both cases, the definitions come from the Central Manager and the data comes from the local machine (which might also be the Central Manager).

Once a Central Management system is set up, customers can use either the Central Manager or a managed unit to create or modify most definitions. Keep in mind that most of the definitions reside on the Central Manager, regardless of which machine does the actual editing.

Note:

- Using the Remote Source function, a user on the Manager can run any report on the managed unit (the user must have the correct role privileges) and view data and information of that managed unit.
- CAS template definitions are shared between all units of a federated environment just like all other definitions (reports, policies, alerts, etc.)
- It is recommended that a user run CAS Reports on a manager, especially CAS Reports relating to CAS configurations, hosts, and templates.
- If you use the Custom Domain Builder to create a report that uses some or all remote tables (tables that live on the manager in a Central Manager environment, such as Datasource or Comments), this report does not work on a managed node. No data will be returned.
- The Central Management page of a manager will no longer automatically refresh itself based on a certain interval. This page will timeout based on the GUI timeout of the system.
- After some time of inactivity, the system will log you out automatically and ask you to sign in again. The length of the GUI timeout can be set via the CLI command show/store session timeout (default is 900 seconds). Status lights will refresh every five minutes when the session is active.
- If a user is attempting to synchronize or upload any data from the Central Manager to managed nodes, all nodes that are involved in this type of activity MUST be on the SAME version of Guardium.
- During the Central Management Redundancy Transition, it can take up to five minutes for the Unit type Sync to occur depending on how many units are defined in the Central Management environment.

- Guardium Component Services
  Identify Guardium components and the locations from which they are taken in a central management environment.
- Implementing Central Management
  Make one machine into a Central Manager, connect the other machines into a Central Management system, and register the Managed Units to communicate with the Central Manager.
- Using Central Management Functions
  Use Central Management functions to synchronize portal user accounts, monitor managed units, and install security policies on managed units.

Parent topic: Aggregation and Central management

Guardium Component Services

Identify Guardium components and the locations from which they are taken in a central management environment.

That unit can be used to monitor and control other Guardium units, which are referred to as managed units. Unmanaged units are referred to as stand-alone units.

Table 1. Guardium Component Services

Component	Description
Users, Roles and Permissions	Central Manager controls the definition of users, roles, groups and datamart tables for all managed systems. The Central Manager exports the complete set of user, security role, group, and datamart tables definitions on a scheduled basis or on demand. The managed units update their internal databases on an hourly basis. As a result, there might be a delay of up to an hour between the time users, roles, permissions or datamart tables are added or modified on the Central manager and the time that the managed unit applies those updates. Note: If you have Guardium® users or security roles that are defined on an existing stand-alone unit that is about to be registered for central management, those definitions will not be available after the system is registered, unless those users and security roles have also been defined on the Central Manager. You cannot administer users or security roles on a managed unit. Those definitions can be administered only when logged on to the Central Manager. When a unit is unregistered for central management, all added users and security roles are removed leaving only the default users (admin, accessmgr). When installing an Accelerator add-in product (PCI, SOX, etc.), in a Central Manager environment, install it first on the Central Manager and then on the managed unit. Add any roles and users as required for the Accelerator on the Central Manager (and those will be synchronized with the managed unit from there). Accelerator documentation is contained within the Accelerator module. See an overview of PCI Accelerator at the end of this Component Services table.
Aliases and Groups	On all processes that automatically generate aliases or groups, for example: import user groups from LDAP, group generation from queries, alias generation from queries, classifier, etc. if the same group or alias is automatically generated on more than one managed machine (managed by the same manager), then it might conflict with an existing group or alias, which will not be replaced.

Component	Description
Audit Processes	The definitions of the Audit Process itself and all of its corresponding tasks are saved to the Central Manager and available to all managed units. However, Schedules, Results, and To-Do lists are saved on the local machine. This means that the same Audit Process tasks can be run on all Managed Units, plus the Central Manager. But it can be run at different times on different machines, which can be useful if the Managed Units have different peak load periods. Each machine has its own set of results, which are based on the data that the machine has collected; and each machine has its own set of To-Do lists for all users. Audit Process definitions are exported from the Central Manager to the managed units as part of the user synchronization process (see Synchronizing Portal User Accounts). When audit process results have been produced, the results are available to users, but on managed units, there might be a delay of up to an hour before reports or monitors such as Outstanding Audit Process Reviews are updated.
Queries	Each query can get only database information from a single machine. Queries that require access information including both Central Manager definitions and Managed Unit data show no data, or missing data.
Policies	Policy definitions are saved on the Central Manager. However, when you install a policy on a Managed Unit, a local copy is made and saved on the Managed Unit. The reason for that is that the Managed Unit is needed to keep on monitoring the database activity and using the policy even when the Central Manager is not available for any reason. Note: Installing a policy on a managed node will not upload this policy to the Central Manager until the Refresh on the Central Manager is clicked. Versions must be the same between Central Manager and Managed Unit when installing policies else policies will not install and errors are generated.
Reports	Report definitions are saved on the Central Manager. When regenerate portlet is called on a Central Manager, it also sends a management (https) request to all managed units to regenerate the portlet (with the report ID). When regenerate is called on a managed unit - if it is called from the screen (not the management request), then it should send a management request to the manager to refresh the portlet (this would also send it to all units). There is a persistence mechanism for management requests for the case a unit is down - see sections within this topic on registration and policy installation. From the Central Manager, reports and audit processes can use data from a managed unit but not managed aggregators. The managed unit is selected as a run-time parameter, is referred to as a remote datasource, and presented as a filtered drop-down selection list containing only managed units. When an audit process references a remote datasource, that audit process can be run from the Central Manager only, so it will not appear in a list of audit processes that are displayed on a managed unit. Note: Certain reports, on a Central Manager, of domain Sniffer Buffer Usage (for example, Request Rate, CPU Usage, Buffer Usage Monitor) will NOT display any data. The reports will be empty.
Security Assessment	Like the Audit Process, the definition of the Security Assessment itself is saved to the Central Manager. But the results are saved on the local machine. This means that the same Security Assessment can be run on all Managed Units, plus the Central Manager.
Baselines	Baselines are always saved on the Central Manager. However, baselines are GENERATED using the logged data that is local to the machine on which it is generated. Therefore, if you want to include constructs from all Managed Units, you must regenerate the baseline on ALL Managed Units and merge the new results into the existing baseline. Attention: The Baseline Builder and related functionality is deprecated starting with Guardium V10.1.4.
Comments	Comments can be saved on either the local machine or the Central Manager, depending on what the comment is associated with. If the Comment is associated with a definition that resides on the Central Manager, then it is also saved on the Central Manager. If the Comment is associated with a Result on the local machine, OR something specific to a Managed Unit (like an Inspection Engine), the Comment is also saved on the local machine.
Schedules	Schedules are always saved on the local machine, even when the definition is saved on the Central Manager.
Non-Central Manager Tasks	When a server is configured as a Central Manager, you must be aware of the tasks that cannot be performed on that unit, but rather must be performed on other (non-Central Manager) units. Inspection engines cannot be defined on the Central Manager and can be created only on the Managed Units. But Inspection engines can be viewed from the Central Manager.
Upgrade Considerations	It is recommended to have your Central Manager and managed units on the same version. The Central Manager should be upgraded first and then the managed units should follow. Having a manager in a different version than its managed units should be a temporary thing and it is highly recommended to upgrade all managed units to the same version as the manager. Run Sync (Refresh) on all managed nodes after upgrading, in order for these managed nodes to recognize the proper software version that they are.

Component	Description
PCI Accelerator for Compliance	The PCI Data Security Standard consists of twelve basic requirements. Much of the requirements are focused on protecting physical infrastructure (for instance, Requirement 1: Install and maintain a firewall configuration to protect data) or implementing procedural best practices (for instance, Requirement 5: Use and regularly update anti-virus software). However, an extra emphasis is placed on real-time monitoring and tracking of access to cardholder data and continuous assessment of database security health status (for instance, Requirement 10: Track and monitor all access to network resources and cardholder data). Guardium's PCI Accelerator for Database Compliance is tailored to simplify organizational processes that are needed to support these monitoring and tracking mandates and to allow for cardholder data security. The Accelerator report templates can be customized to directly reflect specific organizational and regulatory requirements. You can access these templates using the tabs that are provided: • PCI Data Security Standard overview • Plan and Organize • PCI Req. 10: Track and Monitor Access • PCI Req. 11: Regularly Test and Validate • PCI Policy Violations Monitoring Other tools in the Guardium family of solutions are available to help meeting regulations include the following: • PCI Compliance Report Card - A detailed view of cardholder databases access security health that is used to automate the compliance processes with continuous real-time snapshots customized for user-defined tests, weights, and assessments. The Report Card can be generated using security assessment. • Full Audit Trail - The non-intrusive generation of a full audit trail for data usage and modifications that are required by regulatory compliance. • Automated Scheduling - Automated scheduling of PCI work flows, audit tasks, and dissemination of information to responsible parties across the organization.

The following table can help identify which components are taken from which location in a central management environment.

Table 2. Components and Location in Central Manager Environment

Central Manager	Managed Unit
Users	System Configuration
Security Roles	Inspection Engines
Application Role Permissions	Alerter (configuration)
Queries	Anomaly Detection
Reports	Session Inference
Time Periods	IP-to-Hostname Aliasing
Alerts	System Backup
Security Assessments	Aggregation / Archiving
Audit Process Definitions	Custom Alerting
Privacy Sets	Custom Identification Procedures
Baselines Attention: The Baseline Builder and related functionality is deprecated starting with Guardium V10.1.4.	Exported csv Output
Policies	Schedules
Groups	DB Auto-discovery Configurations
Aliases	Audit Process Results

Users, Security Roles, Audit Process Definitions, and Groups are exported from the Central Manager to all managed units on a scheduled basis, as described later.

From the Central Manager, the administrator can:

- Register Guardium units for management
- Monitor managed units (unit availability, inspection engine status, etc.)
- View system log files (syslogs) of managed units
- View reports using data on managed units
- View main statistics for managed units
- Install Guardium security policies on managed units
- Restart managed units
- Manage Guardium inspection engines on managed units
- Maintain the complete set of Users, Security Roles, Groups, and Application Role Permissions that are used on all managed systems
- Patch distribution
- Distribute Uploaded JAR files
- Distribute Patch Backup Settings
- Distribute Authentication Config
- Distribute Configurations

Note: Application Role Permissions can also be changed by the administrator from any managed unit. When this happens, the permissions are changed for all managed units.

Parent topic: Central Management

Implementing Central Management

Make one machine into a Central Manager, connect the other machines into a Central Management system, and register the Managed Units to communicate with the Central Manager.

- Implementing Central Management in a New Installation
- Implementing Central Management in an Existing Installation
- If the Central Management Unit is unavailable

- Implementing Central Management in a New Installation
  Make one Machine the Central Manager, use the same shared secret, register units, and group managed units.
- Implementing Central Management in an Existing Installation
  Implement Central Management in an existing Guardium environment and migrate a CAS collector with active instances to be managed.

Parent topic: Central Management

Implementing Central Management in a New Installation

Make one Machine the Central Manager, use the same shared secret, register units, and group managed units.

Make one machine the Central Manager

The first thing is to make one machine into a Central Manager. Select a machine. Then, complete the following steps.

1. Log in to the CLI of the Machine that you want to make the Central Manager.
2. Enter store unit type manager. This step makes the machine a Central Manager; however, it is not yet managing anything.

Use the Same Shared Secret

After you have a Central Manager, you must connect the other machines into a Central Management system. For security reasons, it is a requirement that the communications between the machines be encrypted by using the same shared secret. To do this step, do the following action items.

1. Click Setup > Tools and Views > System to open System.
2. Set the shared secret to the same string on all systems.

- Registering Units
  Register managed units to communicate with the Central Manager.
- Unregistering a Managed Unit
  When a unit is unregistered, always unregister from the Central Manager. This method is the only way that the Central Manager decrements its count of managed units.
- Synchronizing Portal User Accounts
  Manage portal user synchronization by using the Central Manager.

Parent topic: Implementing Central Management

Registering Units

Register managed units to communicate with the Central Manager.

You can register Guardium units for central management either from the Central Manager or from the unit itself. Regardless of how the registration is done, the Central Manager and all managed units must have the same system shared secret. If the unit to be managed is already registered for central management with another manager, unregister the unit from that central manager before you register it with the new manager. Be sure to understand exactly what happens to that unit when it is registered and unregistered for central management.

Note: If the user that is logged in to a managed unit does not exist on the Central Manager, the session is invalidated. It remains invalidated until the unit is registered with a Central Manager.

What Happens during Registration

The following actions happen on registration.

- The unit type is set to managed and manager IP is stored.
- Product key of manager is applied. (License key is not propagated with Ping or User sync. It is sent on registration or when the system refreshes.)
- All job scheduling is reset to default.
- All psml files (portal GUI customizations) are removed.
- All local users and roles are removed.
- List of threshold alerts that is not be evaluated is reset.
- Users roles, permissions from manager are loaded.
- Custom classes, user uploaded JARs, LDAP truststore from manager are uploaded.
- Database connection from managed to manager is enabled.
- Database connection from manager to managed is enabled.
- CAS listener is started if needed.

After registration all definitions of reports, queries, groups, policies, audits, and more are retrieved from the Central manager.

If the Registered Unit Status Remains Offline

If you know the unit that is registered is online and accessible from the Central Manager, but its status remains offline, then complete the following steps.

- Verify that the unit to be managed is online, accessible, and operational by using a browser window to log in to the Guardium system on that unit.
- Click Refresh for the unit.
- Check that you entered the correct IP address for the unit.
- Check that the unit has the same shared secret as the Central Manager.

Note: If the registration of a unit is offline, the registration request persists. It is resent to the IP/port specified on a set interval until the unit registers. A registration request that does not succeed expires after seven days.

Registering from a Managed Unit

On a managed unit, you can use the GUI to register the unit with the Central Manager. Otherwise, you can use the CLI register command as described in Registering a Managed Unit with the CLI.

1. Click Setup > Central Management > Registration and Load Balance to open Central Management Registration.
2. For Host IP, enter the IP address of the Central Manager.
3. For Port, enter the https port for the Central Manager (usually 8443).
4. Click Register.

After you register on the managed unit, it initiates communication with the Central Manager, and nothing more needs to be done.

Note: The central management unit must be online and accessible by this unit when you register for central management. In contrast, when you register units for management from the central management unit, you can register units that are not currently accessible.

Registering a Managed Unit with the CLI

1. On the managed unit, log in to the CLI.
2. Type `register management <Manager IP> <Manager Port>`

After you register on the managed unit, it initiates communication with the Central Manager, and nothing more needs to be done.

Registering units from the Central Manager

You can register units that are not currently accessible.

1. Navigate to Manage > Central Management > Central Management to open Central Management.
2. Click Register New. The unit Registration page opens.
3. Enter the Unit IP and port, and click Save. The Central Management page refreshes with the new unit.

Parent topic: Implementing Central Management in a New Installation

Unregistering a Managed Unit

When a unit is unregistered, always unregister from the Central Manager. This method is the only way that the Central Manager decrements its count of managed units.

Unregistering from the managed unit does NOT unregister the unit on the Central Manager. The Central Manager still counts that unit as a managed unit for licensing purposes and treats the unit as managed. It might not allow another unit to be registered with the Central Manager. The unregister function on the managed unit is included for emergency use ONLY. If a manager is no longer in service, then you must unregister the unit before you can register it to another manager.

If you unregister a unit from the managed unit, it still shows on the Central Manager screen. Pressing refresh for that unit reregisters it. Pressing any other operation for that unit gives out a message that the unit is no longer managed and removes it from the manager.

On a managed unit, you can use the GUI to unregister the unit with the Central Manager. Also, you can use the CLI unregister command as described in Unregistering a Managed Unit with the CLI.

1. Log in as admin to the Guardium UI of the unit to be managed.
2. Click Set > Central Management > Registration and Load Balance to open Central Management Registration.
3. Click Unregister.

What Happens during Unregistration

The following actions take place upon unregistration.

- The unit type is set to standalone.
- The manager IP is cleared.
- The product key is cleared (license is null until registration to new manager or a license is loaded manually).
- The list of threshold alerts that is not evaluated is reset.
- All job scheduling is reset to default.
- Psml files are removed.
- All users but the default users (admin, accessmgr) are removed.
- The database connection from managed to manager is disabled.
- The GUI is restarted.

After unregistration all definitions of reports, queries, groups, policies, audits, and more are retrieved from the local database, the definitions that are stored on Central Manager are no longer accessible.

If you are unsure about how to verify, contact Guardium Support before you unregister the unit.

Unregistering a Unit from the Central Manager

1. Log in, as admin, to the Central Manager.
2. Click Manage > Central Management > Central Management to open Registration.
3. Mark the check box for the managed unit you want to unregister.

4. Click Unregister.

Unregistering a managed unit from the Central Manager screen removes it from the managed unit list and sets the unit to be a stand-alone unit.

Note: The product key of the unit is removed and unless the unit is registered to another manager the product key is placed in manually.

Unregistering from a Managed Unit

On a managed unit, you can use the UI to unregister the unit with the Central Manager. Also, you can use the CLI unregister command as described in Unregistering a Managed Unit with the CLI.

1. Log in, as admin, to the managed unit.
2. Click Setup > Central Management > Registration and Load Balance to open Registration.
3. Click Unregister.

To unregister a Managed Unit by using the CLI, complete the following steps.

1. On the Managed Unit, log in to the CLI.
2. Enter `unregister management`.

After you have unregistered from the Managed Unit, it severs communication with the Central Manager, and nothing more needs to be done.

Parent topic: Implementing Central Management in a New Installation

Synchronizing Portal User Accounts

Manage portal user synchronization by using the Central Manager.

About this task

As mentioned earlier, the Central Manager controls the definition of Users, Security Roles, Groups, and datamart tables for all managed units. The Central Manager makes an encrypted and signed copy of its complete set of User and Security Roles. In addition, the Central Manager transmits that information to all managed units. Furthermore, some other definitions that are required for local processing (Groups and Group members, Audit processes, Aliases, and more) are also copied. The managed units then update their internal databases on an hourly basis. This process means that there might be a delay of up to an hour before using these roles or datamart tables.

A full user synchronization cycle occurs on registration or by pressing Refresh from the Central management screen. In both cases, the synchronized information is sent from the manager and loaded on the managed units immediately.

Note: Use caution when setting the schedule so that it does not interfere with other scheduled jobs like Import which can fail to start.

Procedure

Click Manage > Central Management > Portal User Sync to manage portal user synchronization.

a. Click Modify Schedule to change the user synchronization task schedule by using the standard task scheduler.
b. If the task is actively scheduled, click Pause to stop further scheduled executions.
c. If the task is paused, click Resume to start running the task again (according to the defined schedule).
d. Click Run Once Now to run the synchronization task immediately.
   Note: The task that is scheduled or Run Once Now refers to the collection of data and its transmission to the managed units only. The managed units might not use that data to update their user tables until up to 1 hour after it is received.

Parent topic: Implementing Central Management in a New Installation

Implementing Central Management in an Existing Installation

Implement Central Management in an existing Guardium environment and migrate a CAS collector with active instances to be managed.

In an existing Guardium environment, refer to the procedure outlined to develop a plan for implementing central management. If you are converting an existing Guardium unit to a Central Manager, keep in mind that a Central Manager cannot monitor network traffic. For example, inspection engines cannot be defined on a Central Manager.

1. Select a system shared secret to be used by the Central Manager and all managed units. For more information, see the system shared secret in System Configuration.
2. Install the Central Manager unit or designate one of the existing systems as the Central Manager. In either case, use the store unit type command to set the manager attribute for the Central Manager.
3. Any definitions from the stand-alone unit that you want to have available in the central management environment must be exported before the stand-alone unit is registered for management. Later, those definitions are imported on the Central Manager. BEFORE exporting or importing any definitions, follow the procedure that is outlined for each stand-alone unit that is to become a managed unit. Read through the introductory information under Export/Import Definitions.
   - Decide which definitions from the standalone system you want to have available after the system becomes a managed unit. Ignore any components on the stand-alone system you do not want to have available.
   - Compare the security roles and groups that are defined on the stand-alone unit with those defined on the Central Manager. Under central management, a single version of these definitions applies to all units. If a security role with the same name exists on both systems and it is used for different purposes, add a new role on the Central Manager and assign the new role to the appropriate definitions after they are imported.
   - If the same group name exists on the stand-alone unit and the Central Manager but it has different members, create a new duplicate group on the stand-alone system, taking care to select a group name that does not exist on the Central Manager. In all of the definitions to be exported, change the old group name references to new group name references.
   - All security roles that are assigned to all definitions that are exported from the stand-alone system. When definitions are imported, they are imported WITHOUT roles, so you must add them manually.
   - Check the application role permissions on each system. If any security roles assigned to an application on the stand-alone unit are missing from the Central Manager, add them to the Central Manager.

- Export all definitions from the stand-alone system that you want to have available after the system becomes a managed unit. (See Export/Import Definitions) Do not export users or security roles. If you are unsure about a definition, export it in a separate export operation so that you can decide in the future whether to import that definition to the Central Manager. After you register for central management, none of the old definitions from the stand-alone unit are available.
- On the stand-alone unit, create PDF versions audit process results and store them in an appropriate location. Under central management, only the audit results produced under central management are available.
- On the stand-alone unit, instruct all users to remove all portlets that contain custom report, and to not create any new reports until the conversion to central management is complete.
- On the Central Manager, manually add all users from the stand-alone unit.
- On the stand-alone unit, delete all user definitions except for the admin user (which cannot be deleted).
- Register the stand-alone unit for central management. See Registering Units for Central Management.
- On the Central Manager, import all definitions that are exported from the stand-alone system. Check to make sure that references to included items (receivers in alert notifications, for example) are correct. Reassign security roles, as necessary, to all imported definitions.
- Inform users of the managed unit that they must use the Report Builder application to regenerate the portlets for any custom reports they want to display in their layouts.

Migrating a stand-alone CAS collector to managed

Use the following steps when you migrate a CAS collector with active instances to managed.

1. Export the CAS host definitions from the stand-alone collector.
2. Manage the stand-alone collector.
3. Restart the CAS host from the GUI of the now managed collector.
4. Import the CAS host definition to the manager.
5. Restart the CAS host from the GUI of the managed collector again.

After these steps are performed, the CAS collector has the same instances and monitor the same files that it did when it was a stand-alone.

Note: The CAS data that was collected when it was a standalone is deleted. There is no collected CAS data unless a file changes.
Parent topic: Implementing Central Management

Using Central Management Functions

Use Central Management functions to synchronize portal user accounts, monitor managed units, and install security policies on managed units.

- Deployment health views
  The deployment health views gather and display information about your entire Guardium environment in powerful, easily consumed graphical views.
- Enterprise load balancing
  The enterprise load balancer dynamically allocates managed units to S-TAP agents based on system load and availability.
- Deployment inventory
  The inventory view provides centralized view of all database servers and any installed S-TAPs or GIM clients.
- Resource deployment view
  The resource deployment view provides a centralized view of all database servers and their associated collectors, aggregators, and central managers.
- Creating managed unit groups
  Organize managed units into groups and then take actions on those groups.
- Monitoring Managed Units
  Monitor managed units by using Central Management.
- Installing Security Policies on Managed Units
  Install a security policy on a manage unit.
- Central Patch Management
  Provide visibility and control over patch installation, status, and history.
- Working with configuration profiles
  Configuration profiles allow you to define configuration and scheduling settings from a central manager and distribute those settings to managed unit groups without altering the configuration of the central manager itself.
- Distribute Configuration
  Configurations and their schedules, can be distributed, either all or individually, between the Central Manager and the managed units.
- Distribute Authentication Configuration
  Instead of configuring authentication on each appliance separately, Central Management authentication (Configure Authentication) can be configured once on the central manager and then distributed to all managed units. This way, information is entered once and it applies to some or all units; some of the units may have a different type of authentication.
- Central Manager Redundancy
  Use Central Manager Redundancy or Backup Central Manager (CM) to configure a secondary or backup CM in case the Primary CM becomes unavailable.

Parent topic: Central Management

Deployment health views

The deployment health views gather and display information about your entire Guardium environment in powerful, easily consumed graphical views.

The deployment health views help you investigate system-utilization trends and quickly identify ailing or down systems. These views decrease reaction times and reduce risks from problems in your Guardium deployment. The deployment health views are designed to work together by consolidating several different sources of information into unique but related views.

Deployment health topology and table views

The deployment health topology and table views show the data flow relationships between systems in your environment. These views make it easy to identify problematic systems and investigate the underlying issues.

Access the topology view by navigating to Manage > System View > Deployment Health Topology. Access the table view by navigating to Manage > System View > Deployment Health Table.

Deployment health dashboard

The deployment health dashboard provides an at-a-glance summary of issues that are found across a Guardium deployment. The dashboard is especially useful for identifying patterns and trends in the health data before investigating individual systems where problems are identified.

Access the dashboard by navigating to Manage > System View > Deployment Health Dashboard.

The following table summarizes the types of data available to each of the deployment health views.

Table 1. Summary of deployment health views

	Dashboard	Topology	Table
Unit utilization	✔	✔	✔
Correlation alerts	✔		
Self-monitoring	✔		
System requirements	✔		
Aggregation		✔	✔
Inspection engines (S-TAP verification data)		✔	
Connectivity		✔	✔
S-TAP connectivity		✔	

Attention: The deployment health views present data gathered from an entire Guardium environment and are only available from a central manager.

- Configuring a central manager for the deployment health views
  To use the deployment health views, enable the collection of unit utilization data, configure correlation alerts, and configure data import and export for your environment.
- Deployment health topology and table views
  Learn more about how the deployment health topology and table views present the configuration of your Guardium environment and its data.
- Deployment health dashboard
  Learn more about how the deployment health dashboard presents data from your entire Guardium deployment.
- Scenario: Troubleshooting overloaded systems using the deployment health topology view
  This topic describes using the deployment health topology view to identify and fix an overloaded system in your environment.

Parent topic: Using Central Management Functions

Configuring a central manager for the deployment health views

To use the deployment health views, enable the collection of unit utilization data, configure correlation alerts, and configure data import and export for your environment.

About this task

From a central manager, the deployment health views display data from across a Guardium environment. The ability to display data about an entire deployment requires the collection of unit utilization data, the configuration of correlation alerts, and that data import, export, and S-TAP verification is correctly configured. For a summary of data that is displayed on the deployment health views, see Deployment health views.

It is likely that your deployment is already configured to support the deployment health views. Verify the configuration steps that are described in this procedure if you notice any of the following issues on any of the deployment health views:

- CM buffer usage report not scheduled
- Unit utilization report not scheduled
- Export not scheduled
- Import not scheduled
- No issues found
- Status unavailable

Procedure

1. Configure the collection and processing of unit utilization data from the central manager. For more information, see Configuring unit utilization data processing.
2. Enable correlation alerts for inclusion on the deployment health dashboard.
   a. Open Protect > Database Intrusion Protection > Alert Builder.
   b. Select an existing alert and click the icon, or create a new alert by clicking the icon.
   c. Provide a Category for the alert. Alerts without a specified category are displayed as Uncategorized.
   d. Select the View in deployment health dashboard check box to include the alert on the dashboard.
   Attention: Alerts must have the Severity set to LOW, MED, or HIGH to be included on the deployment health dashboard.
   For more information about defining alerts, see Building alerts.
3. Configure data import and export from the central manager. For more information, see, Aggregation.
   Tip: Use the distribute configuration profiles tool to simplify the process of configuring data import and export for a Guardium deployment. For more information, see Working with configuration profiles.
4. Configure S-TAP verification for all supported S-TAPs. For more information, see Windows Inspection engine verification and UNIX Inspection engine verification.

Results

After you complete the configuration procedures and allow the data to update, the deployment health topology and deployment health table views will predominately show status except for systems with preexisting health issues. The deployment health dashboard will include any preexisting unit utilization issues and begin showing new correlation alert conditions.

When altering the unit utilization or data import and export schedules, wait up to 1 hour to allow the deployment health views to update with new information. The availability of new correlation alert data depends on the notification frequency that is specified for an alert.

Parent topic: Deployment health views
Related concepts:
Aggregation
Related tasks:
Configuring unit utilization data processing
Working with configuration profiles
Related information:
Correlation Alerts

Deployment health topology and table views

Learn more about how the deployment health topology and table views present the configuration of your Guardium environment and its data.

The deployment health topology view is accessible from any central manager and provides an at-a-glance visualization of the entire Guardium environment that is connected to that central manager. In addition to showing relationships between nodes in the environment, the deployment health topology view also provides health information about all connected aggregators, collectors, and S-TAPs. Several investigation and resolution actions are available directly from the deployment health topology view to help quickly address health issues that are discovered in your environment.

The default deployment health topology view is a data flow view that shows the data import and export relationships between aggregators and managed units. Open the deployment health topology view at Manage > System View > Deployment Health Topology.

A sortable table view of the deployment health data is also available at Manage > System View > Deployment Health Table.

Data availability

Several factors influence that availability of system data and how that data is displayed on the deployment health topology and table views. For information about configuring your system to use the deployment health views, see Configuring a central manager for the deployment health views.

Types of data

When correctly configured, the deployment health topology and table views display data that is collected from several different sources. The specific types of data that are displayed depend on the unit type, as summarized in the following sections.

Connectivity

The connectivity category indicates whether systems in a Guardium environment are able to communicate.

- Applies to central managers, aggregators, collectors, and S-TAPs
- Examples include unit not responding and S-TAP not responding

Unit utilization

The unit utilization category provides information about how heavily Guardium systems are being loaded.

- Applies to central managers, aggregators, and collectors
- Examples include CPU load, free buffer space, and MySQL disk usage
- For more information, see Unit Utilization Level.

Aggregation

The aggregation category provides information about data import and export flow between Guardium systems.

- Applies to central managers (if configured as aggregators), aggregators, and collectors
- Examples include import failed, export failed, and export not scheduled
- For more information, see Predefined admin reports and Aggregation.

Inspection engines

The inspection engines category provides S-TAP verification information.

- Applies to S-TAPs
- Examples include S-TAP verification failed
- For more information, see Configuring the S-TAP verification schedule, and Viewing S-TAP verification results.

Click the  icon to open the Customize Settings dialog to define the types of data shown on the deployment health topology and table views.

Data latency

Several preset and user-defined schedules determine the latency of data that is displayed on the deployment health topology view. These schedules are summarized in the following table.

Table 1. Deployment health topology view data latency

Health category	Node type	Latency
Connectivity	Aggregator or collector	Less than 15 minutes
Connectivity	S-TAP	Less than 15 minutes if enterprise load balancing is enabled Less than 1 hour if enterprise load balancing is not enabled

Health category	Node type	Latency
Aggregation	Central manager, aggregator, or collector	Less than 1 hour
Verification	S-TAP	Less than 1 hour
Unit utilization	Central manager, aggregator, or collector	1 - 2 hours, based on the recommended configuration. For more information, see Configuring unit utilization data processing.

Observe the following latencies for specific environment and configuration changes:

- Newly registered aggregators or collectors become available to the deployment health views within 15 minutes.
- Deleting the data export schedule or data export configuration from a collector are reflected on the deployment health views within 2 hours.

Data presentation

Health status

The deployment health topology view displays three categories of health information for Guardium systems: connectivity, unit utilization, and aggregation. Metrics under these categories are assigned one of the following health statuses: status unavailable (least severe), no health issues, low severity, medium severity, and high severity (most severe). The overall status is determined by the most severe status of any individual metric included under any of the health categories being displayed. Data that has been excluded using the Customize Settings dialog is not used for determining the overall status of a system.

For example, if the Restarts metric under the Unit utilization category is assigned a High severity status, but no health issues exist under another category, the Overall status for that system is High severity. This behavior ensures that the most severe condition is always visible at-a-glance as the overall status of a system.

At the Manage > System View > Deployment Health Topology view, detailed statuses for the available health categories are only displayed when at least one low, medium, or high severity issue is found.

At the Manage > System View > Deployment Health Table view, detailed statuses for the available health categories are always displayed.

Health status roll-up

The deployment health topology view implements a health status roll-up strategy to efficiently display health information for an entire Guardium environment. Using this strategy, child nodes are collapsed under their parent nodes, and the child's health status is rolled-up to the parent. The rolled-up status is expressed as a small icon attached to the parent node.

Attention: Health status roll-up is only supported for S-TAP nodes rolling-up status to their parent collector.

For example,  indicates a collector with no health issues, but the small red circle indicates that one or more S-TAPs that are associated with that collector has high severity issues. Clicking the collector expands the node and reveals the associated S-TAPs and their health status. For example,

indicates four S-TAPs that are associated with the collector: two S-TAPs have high severity health issues, and two S-TAPs have low severity health issues.

Only the most severe status is rolled-up from the child to the parent node when the child nodes are collapsed. In the previous example, the parent node shows a small red circle because one or more of its children has high severity issues. However, if one or more child nodes contain low severity issues but all the other child nodes have no health issues, the parent node would display a small yellow circle.

Deployment presentation

Some deployment configurations display unexpectedly on the deployment health topology view. Several of these configuration scenarios are described in the following sections.

Managed units before Guardium V10.1.3

Managed units before Guardium V10.1.3 may display incorrect or inconsistent unit utilization data when connected to a central manager at or after V10.1.3. To correct the problem, log in to the CLI of the central manager and run the following command for each managed unit:

```
grdapi change_tracker_reset host=[managed unit host name or IP address]
```

Best practice: In a managed environment, it is recommended that all units operate at the same Guardium version level.

Managed units before Guardium V10.1

Managed units before Guardium V10.1 display Status unavailable under the Aggregation health section when viewed from either the Deployment Health Topology page or the Deployment Health Table.

Best practice: In a managed environment, it is recommended that all units operate at the same Guardium version level.

Unsupported S-TAPs

The deployment health topology view displays any S-TAPs that are configured for S-TAP verification or that participate in enterprise load balancing. If an S-TAP cannot be configured for S-TAP verification or to participate in enterprise load balancing, the S-TAPs will not be displayed.

S-TAP load balancing

If S-TAP load balancing is configured with the participate_in_load_balancing parameter and an S-TAP is configured to balance traffic across multiple collectors, the deployment health topology view displays that S-TAP as a child node of each collector. For example, if *S-TAP 1* is load balancing with *Collector A* and *Collector B*, both *Collector A* and *Collector B* display *S-TAP 1* as a child in the deployment health topology view.

Unmanaged units

If a collector exports data to a central manager or to an aggregator that is configured as a central manager, but that collector is not designated as a managed unit of that central management cluster, the Overall status of the collector in the deployment health topology view is shown as Health status unavailable. No additional information about the collector is made available through the deployment health topology view unless the collector is designated as a managed unit of the central manager.

Collector exporting data to primary and secondary hosts

When a collector is configured to export data to both primary and secondary hosts, only the primary host is used for the deployment health topology view.

Parent topic: Deployment health views
Related tasks:
Configuring a central manager for the deployment health views

Deployment health dashboard

Learn more about how the deployment health dashboard presents data from your entire Guardium deployment.

Data availability

Several factors influence that availability and latency of health data and how that data is displayed on the deployment health dashboard. The following table summarizes the data included on the dashboard, trigger criteria, and data latency and purge information.

Table 1. Summary of deployment health dashboard data

Data source	Information type	Trigger criteria	Data latency	Data purge interval
System resources	System configuration, such as CPU cores, system memory, /var disk capacity	System does not meet minimum requirements	Updated whenever the user-interface server is started or restarted	Not applicable
Unit utilization	Unit utilization data such as sniffer restarts, MySQL disk usage, and CPU load.	Value exceeds unit utilization thresholds	Updated within 1 - 2 hours, based on the recommended configuration. For more information, see Configuring unit utilization data processing.	Unit utilization data is purged after 60 days Sniffer buffer usage data is purged after 14 days
System self-monitoring	MySQL disk usage and system disk usage	Usage meets or exceeds default thresholds (75% for high severity, 90% for critical severity)	Updated every 5 - 10 minutes. For high-severity, if the same event occurs multiple times in a 15 minute period, the timestamp is updated to reflect the most recent instance. If the same event occurs after a 15 minute interval, a new entry is created with the most recent timestamp. For critical issues, every instance of an event is created with a unique timestamp.	High-severity issues are purged after 7 days Critical issues are never purged
Correlation alerts	Triggered correlation alerts	An alert threshold is reached	Updated based on the alert notification frequency. For more information, see Correlation Alerts.	Data is purged after 7 days

Important:

- Only data from systems that are running Guardium V10.1.2 and later are included on the deployment health dashboard.
- When you change the host name of a system, preexisting data that is associated with the original host name is no longer displayed on the deployment health dashboard.
- When a primary central manager transfers data to a backup central manager during a failover scenario, up to 30 minutes of data is unavailable to the deployment health dashboard.

Data presentation

The deployment health dashboard formats and presents data through various tiles or small window-like containers. The following table summarizes the data that is presented on each dashboard tile.

Table 2. Summary of deployment health dashboard tiles

	Tile name						
Data source	**Resource requirements**	**Unit utilization issues**	**Unit utilization timecharts**	**Alerts (by category, name, severity, or system)**	**Events**	**High severity**	**Critical**
System resources	✔					✔	
Unit utilization		✔	✔		✔	✔	
System self-monitoring					✔	✔ (When usage meets or exceeds 75% threshold)	✔ (When usage meets or exceeds 90% threshold)
Correlation alerts				✔	✔	✔	
The following tiles are displayed by default: *alerts by name*, *critical issues*, *events timeline*, *high severity issues*, and *unit utilization issues*.							

Dashboard filter

The dashboard filter allows quick filtering of the data based on Guardium systems, issue severity, and time period. Filter settings affect the data displayed on the entire dashboard unless noted otherwise.

The Guardium systems filter allows filtering the dashboard by unit type or by groups defined at Manage > Central Management > Managed Unit Groups.

By default, the dashboard displays all available issues: low, medium, high, and critical. Use the Severity menu to filter data on the dashboard by severity. Selecting high filters the entire dashboard to display only high-severity issues. Selecting critical filters the entire dashboard to display only critical issues. It is possible to select both high and critical issues to filter out all lower-severity data.
Notes:

- Outstanding or unresolved critical issues are displayed on the dashboard regardless of the Severity filter setting.
- For the *unit utilization issues* tile, the dashboard Severity filter is based on the overall unit utilization severity. For more information about how unit utilization severity is assigned, see Unit utilization issues.

The time filter determines the range of data that is displayed on the dashboard. Default settings allow time periods from 1 hour to 3 weeks, but custom time periods are also supported. The time filter does not apply to critical issues: critical issues are always displayed, regardless of the time filter setting.

Use the Add chart menu to add tiles to the dashboard or replace default tiles that you previously removed.

Dashboard summary

The dashboard summary provides overall counts of health issues that are detected in your Guardium deployment. The Collectors with issues and Aggregators with issues counts indicate the number of systems--collectors and aggregators--that are detected with health issues. The Critical and High counts indicate the number of issues detected from all systems that are included on the dashboard.
Note:

- The Critical and High counts are not affected by adding or removing tiles from the dashboard.
- The counts on the dashboard summary bar reflect the dashboard filter settings.

Alerts by category, name, severity, or system

The deployment health dashboard supports several tiles based on Guardium correlation alerts: *Alerts by category*, *Alerts by name*, *Alerts by severity*, and *Alerts by system*. Add correlation alert tiles to the dashboard by using the Add chart menu.

Correlation alerts must be explicitly configured for inclusion on the deployment health dashboard. For information about configuring alerts for the dashboard, see Configuring a central manager for the deployment health views.

Resource requirements

The *resource requirements* tile indicates whether systems in a Guardium deployment meet the minimum hardware requirements for CPU, memory, and /var disk capacity. Any system resource that does not meet the minimum requirement is designated as a high-severity issue and displayed on both the *resource requirements* tile and the *high severity issues* tile.

Use the Include healthy systems check box on the details view of the tile to include all available data for the systems and time frame that are indicated on the dashboard filter bar. By including all available data, the Include healthy systems check box overrides the Severity setting of the overall dashboard filter. Systems without any detected health issues are excluded by default.

A table that displays all met and unmet resource requirements in your Guardium deployment is also available at Manage > Central Management > System Resources.
Note:

- System resource issues are not displayed in the *Events* timeline because they are not associated with a specific time stamp

Unit utilization issues

The *unit utilization issues* tile displays issues based on unit utilization thresholds. The issues that are displayed on the tile represent individual metrics that exceed their respective thresholds. The overall severity is assigned based on the highest severity issue that is found in all available metrics for an individual system in a specified time period. For more information about unit utilization thresholds, see Unit Utilization Level.

The details view of the *unit utilization issues* tile includes both a Period start time and a Timestamp:

- The Period start time indicates that the *CM buffer usage monitor* data is rolled-up into hourly periods, for example periods starting at 13:00, 12:00, and 11:00.
- The Timestamp indicates when the unit utilization levels data is added to the deployment health dashboard, either based on the unit utilization levels schedule or by using *run once now*.

For more information, see Configuring unit utilization data processing.
The first time that unit utilization data is brought into the deployment health dashboard, all the unit utilization data has the same *timestamp* but different *period start* times. Over time, the time stamps will appear at intervals based on the unit utilization levels schedule. For example, if the unit utilization levels data is collected every hour at 40 minutes after the hour, you will see *period start time* and *timestamp* values as follows:

Table 3. Example unit utilization period start time and timestamp values

Period start	Timestamp
13:00	14:40
12:00	13:40
11:00	12:40

Use the Include healthy systems check box on the details view of the tile to include all available data for the systems and time frame that are indicated on the dashboard filter bar. By including all available data, the Include healthy systems check box overrides the Severity setting of the overall dashboard filter. Systems without any detected health issues are excluded by default.

Unit utilization timecharts

Unit utilization timecharts allow the observation of trends in unit utilization data over time. *Unit utilization timecharts* can be configured to show multiple unit utilization metrics for a single Guardium system or to show a single unit utilization metric for multiple Guardium systems.

Unit utilization timecharts are structured based on the following criteria:

- The x-axis represents the *period start* time
- When multiple metrics are being charted and the values for the metrics are in the same range, one y-axis is drawn. For example, both *MySQL disk usage* and */var disk usage* are expressed as percentages and are drawn with the same y-axis.
- When multiple metrics are being charted and the values of the metrics are not similar, two y-axes are drawn. For example, *MySQL disk usage* is expressed as a percentage and *flat log requests* is expressed as an integer, so two y-axes are drawn: one displaying percentages and one displaying integers.
- If the value of a metric falls outside the range of a y-axis, that value is displayed at the bottom of the chart. This behavior accommodates scenarios where different metrics are expressed with similar units but significantly different values: for example, integers in the range of thousands versus millions.
  Tip: Create multiple time charts when values are in significantly different ranges.

Note: Systems are not included on Timechart settings > Host name menu when unit utilization data does not exist for that system in the time frame that is specified on the dashboard filter bar.
Parent topic: Deployment health views
Related tasks:
Configuring a central manager for the deployment health views
Configuring unit utilization data processing

Scenario: Troubleshooting overloaded systems using the deployment health topology view

This topic describes using the deployment health topology view to identify and fix an overloaded system in your environment.

About this task

This scenario involves identifying health issues from the deployment health topology view, assessing the root cause, and correlating that assessment with additional data before resolving the problem and verifying the fix. The example described here involves an overloaded collector, but the process is applicable for other cases.

Procedure

1. On a central manager, navigate to Manage > System View > Deployment Health Topology.
2. Review the deployment topology and assess the overall health of systems in the environment. At a high level,  icons indicate healthy systems while  and  icons indicate systems with some health issues.
3. If you notice systems with  or  status icons, click the node to view an overlay with additional health information.
4. Use the information presented on the node overlay to begin diagnosing any health problems. For example, a collector with high or medium severity statuses for /var disk usage, Restarts, Analyzer queue, and Logger queue indicates that the collector is overloaded.
5. After initially assessing health issues from the deployment health topology view, try to correlate your findings with additional data. For example, if you suspect that a system is overloaded, begin monitoring the traffic for that system.
6. When you are confident that you have diagnosed the underlying health issues, take corrective actions. In the example of an overloaded system, you could establish Enterprise load balancing or reassign S-TAPs to another collector. Typically, this set of symptoms would not occur if enterprise load balancing was already configured and in use.
7. After taking corrective actions, the status of the node on the deployment health topology view will be updated following the next refresh of unit utilization and central manager buffer usage monitor data. This refresh interval depends on your schedule for processing unit utilization data.

Parent topic: Deployment health views
Related concepts:
S-TAP user's guide
S-TAP user's guide

Enterprise load balancing

The enterprise load balancer dynamically allocates managed units to S-TAP agents based on system load and availability.

Overview

Load balancing automatically allocates managed units to S-TAP agents when new S-TAPs are installed and during fail-over when a managed unit is unavailable. The load balancing application also dynamically re-balances loaded or busy managed units by relocating S-TAP agents to less-loaded managed units.

The enterprise load balancing application automates several tasks:

- It removes the need to manually evaluate the load of managed units before assigning those managed units to an S-TAP agent.
- It eliminates the need to define fail-over managed units as part of post-installation S-TAP configuration because the load balancer dynamically manages fail-over scenarios.
- It removes the need to manually relocate S-TAP agents from loaded managed units to less loaded managed units.

Important: When using the enterprise load balancing application, the Guardium system assumes control over the allocation of managed units to S-TAP agents. This is an automated and dynamic process: the S-TAPs change their associations based on the relative load of available manged units. Use the Load Balancer Events report to review all load balancing activity.
Note: When configuring the S-TAP to use enterprise load balancing, the F5-based load balancing cannot be used.

Prerequisites

The enterprise load balancer runs on a central manager or managed unit, listens to port 8443, and uses Transport Layer Security (TLS). No new firewall or additional system setup is required. S-TAPs must be at V10.1 or higher.

Load balancing is disabled by default on Guardium systems. For information about enabling S-TAPs to participate in load balancing, see Windows General parameters and UNIX General Parameters.

How it works

The enterprise load balancing application works by collecting and maintaining up-to-date load information from all its managed units.

It uses the load information from managed units to create a load map. This load map provides the data that directs load balancing and managed unit allocation activities. Use the GuardAPI command grdapi get_load_balancer_load_map to view the current load map at any time.

Load information is only collected from managed units that are online and configured with the parameter LOAD_BALANCER_ENABLED=1. Setting LOAD_BALANCER_ENABLED=0 disables load balancing and prevents that managed unit from being dynamically allocated to S-TAP agents during load balancing activities.

Load collection errors from specific managed units are recorded in the Load Balancer Events report but do not interfere with the overall load collection and load balancing processes. However, failure to collect load information from a managed unit excludes that managed unit from participation in load balancing processes.

- Associating an S-TAP with managed units for enterprise load balancing
  Learn how to use enterprise load balancing by creating and associating S-TAP groups with groups of managed units.
- Viewing the enterprise load balancing load map
  Learn how to view the current enterprise load balancer load map.
- Viewing an enterprise load balancing activity report
  View a report of enterprise load balancing events and activities.
- Enterprise load balancing Guardium configuration parameters
  This reference information provides detailed descriptions of the load balancer configuration parameters. On a CM, access from Manage > Central Management > Enterprise Load Balance > Enterprise Load Balance Properties. On an MU, access from Setup > Central Management > Registration and Load Balance.

Parent topic: Using Central Management Functions

Associating an S-TAP with managed units for enterprise load balancing

Learn how to use enterprise load balancing by creating and associating S-TAP groups with groups of managed units.

About this task

Load balancing creates associations between S-TAP groups and groups of managed units such that S-TAPs within a group are allowed to be reallocated to the most-available managed unit within a group. This task introduces you to the process of establishing associations between S-TAP groups and managed unit groups for the purposes of enterprise load balancing.

Procedure

1. On a Central Manager, navigate to Manage > Central Management > Enterprise Load Balancer > Associate S-TAPs and Managed Units.
2. If an S-TAP group has not already been created or a new one is required, create a new S-TAP group.
   a. Click the  icon to open the Create New S-TAP Group dialog.
   b. Provide a name in the Group Name field. For example, `North_American_S-TAPs`.
      Recommendation: To ensure compatibility with other Guardium components, do not use spaces or special characters in group names.
   c. Add group members by selecting from existing host names or adding new members using the Group Member field. S-TAPs indicated with a  icon are included with the new S-TAP group.
   d. Click Create New Group to create the S-TAP group.
3. Associate the S-TAP group with a group of managed units.
   a. Select the S-TAP group you want to associate. For example, `North_American_S-TAPS`.
   b. Click Associate Managed Units to open the Associate Managed Unit Group dialog.
   c. If necessary, create a new group of managed units.
      i. Navigate to Manage > Central Management > Managed Unit Groups.
      ii. Click the  icon to open the Create New Managed Unit Group dialog.
      iii. Provide a name in the Group Name field. For example, `North_American_MUs`.
      Recommendation: To ensure compatibility with other Guardium components, do not use spaces or special characters in group names.
      iv. Add group members by selecting from existing Managed Unit IP addresses.
      v. Click Create New Group to create the new group of managed units.
   d. Select the group(s) of managed units to associate with the S-TAP group. For example, `North_American_MUs`.
   e. Click Apply.
4. Click Save to complete the association between an S-TAP group and a group of managed units.
5. (Optional) Associate the S-TAP group with a failover group of managed units.
   a. Select the S-TAP group you want to associate, that already is associated to a managed units group. For example, North_American_S-TAPS.
   b. Click Associate Failover Groups to open the Associate Failover Group dialog.
   c. If necessary, create a new group of managed units same as described above. Both Regular managed unit groups and failover groups are the same until specified during association with S-TAP group.
   d. Select the group(s) of managed units to associate with the S-TAP group. For example, North_American_MUs_failover.
   e. Click Apply.
6. Click Save to complete the association between an S-TAP group and a group of managed units.

Parent topic: Enterprise load balancing

Viewing the enterprise load balancing load map

Learn how to view the current enterprise load balancer load map.

About this task

The enterprise load balancing application uses the load information from managed units to create a load map. This load map provides the data that directs load balancing and managed unit allocation activities.

Procedure

1. To view the current load map as a report in the Guardium UI, navigate to Manage > Reports > Unit Utilization > Load Balancer.
2. It is also possible to view the current load map using the Guardium API. Issue the following GuardAPI command: grdapi get_load_balancer_load_map.

The load map should look like the following example:

```
ID=0

************ LOAD MAP *************

****************  LOADED MU LIST ************************

****************  VACANT MU LIST ************************
  {
   MU=myguard_01.domain.com
   MU_QUEUE_SIZE(MB)=25.0
   MU_TIMES_REBALANED=0
   MU_EFFECTIVE_MAX_USED_QUEUE(%)=0.0
   MU_MAX_LOAD_CONTIB_BY_STAP(MB)=0.0
   MU_ADJUSTED_STAP_CONTRIB_IN_MB=0.0
   MU_BASE_MAX_USED_QUEUE_IN_MB=0.0
   IS_REBALANCABLE=true
   INSTALLED_POLICIES=log full details|
   APPLIANCE_RESOURCE_INFO={NUM_PROCESSORS=4,CPU_SPEED=2800,CPU_CACHE=25600,CPU_CORES=4,
      CACHE_READ_RATE=7870,HARD_DRIVE_READ_RATE=186,MEMORY_SIZE=24607}
   STAP_LIST=
      {
      STAP_IP=01_gct1.domain.com, STAP_HOST=01_gct1.domain.com, CONNECTED_TO_MU=gct1.domain.com,
         PARTICIPATES_IN_LOAD_BALANCING=false, MAX_STAP_CONTIBUTION_TO_LOAD_IN_MB=0.0,
         AVG_STAP_CONTIBUTION_TO_LOAD_IN_MB=0.0
      }
      {
      STAP_IP=02_gct1.domain.com, STAP_HOST=02_gct1.domain.com, CONNECTED_TO_MU=gct1.domain.com,
         PARTICIPATES_IN_LOAD_BALANCING=false, MAX_STAP_CONTIBUTION_TO_LOAD_IN_MB=0.0,
         AVG_STAP_CONTIBUTION_TO_LOAD_IN_MB=0.0
      }
      {
      STAP_IP=03_gct1.domain.com, STAP_HOST=03_gct1.domain.com, CONNECTED_TO_MU=gct1.domain.com,
         PARTICIPATES_IN_LOAD_BALANCING=false, MAX_STAP_CONTIBUTION_TO_LOAD_IN_MB=0.0,
         AVG_STAP_CONTIBUTION_TO_LOAD_IN_MB=0.0
      }
  }

****************  STAP -> MUS ALLOCATION TABLE ************************
03_gct1.domain.com ----> gct1.domain.com
02_gct1.domain.com ----> gct1.domain.com
01_gct1.domain.com ----> gct1.domain.com
ok
```

Parent topic: Enterprise load balancing

Viewing an enterprise load balancing activity report

View a report of enterprise load balancing events and activities.

About this task

The Enterprise Load Balancer Events report shows all load balancing events and activities, including successful associations between S-TAP agents and managed units, changes in managed unit load, and failed associations.

Procedure

To view the report, navigate to Manage > Reports > Activity Monitoring > Enterprise Load Balancer Events.
Parent topic: Enterprise load balancing

Enterprise load balancing Guardium configuration parameters

This reference information provides detailed descriptions of the load balancer configuration parameters. On a CM, access from Manage > Central Management > Enterprise Load Balance > Enterprise Load Balance Properties. On an MU, access from Setup > Central Management > Registration and Load Balance.

Parameter	Default value (valid values)	Description

STATIC_LOAD_COLLECTION_INTERVAL	720 (≥10)	Static managed unit load collection interval (in minutes). If ENABLE_DYNAMIC_LOAD_COLLECTION is set to `0`, the load balancer collects the load from all the managed units at the interval specified by STATIC_LOAD_COLLECTION_INTERVAL.
LOAD_BALANCER_ENABLED	1 (0 or 1)	Controls the load balancer feature. • `0` disables the feature • `1` enables the feature If disabled on the managed unit, the load balancer (running on the central manager) does not collect load information from that managed unit. All the S-TAPs connected to that managed unit do not participate in load balancing. On the CM, enabling this parameter (after it was disabled) triggers an immediate full load collection from all the managed units enabled for load balancing.
ENABLE_DYNAMIC_LOAD_COLLECTION	1 (0 or 1)	Controls the load collection method. • `0` disables the dynamic load collection interval (uses STATIC_LOAD_COLLECTION_INTERVAL as the collection interval) • `1` enables dynamic load collection interval When this parameter is enabled (set to `1`), the collection interval is proportional to the number of managed units (1 hour per 10 connected managed units). Changes to this parameter triggers an immediate recalculation of the next full load collection time.
USE_APPLIANCE_HW_PROFILE_FACTOR	1 (0 or 1)	The load balancer can use managed units' hardware profile indicators (specified by the parameter APPLIANCE_HW_PROFILE_INDICATORS) when evaluating vacant managed units for relocating S-TAPs. • `0` ignores hardware profile indicators • `1` uses managed unit hardware profile indicators
MAX_RELOCATIONS_BETWEEN_FULL_LOAD_COLLECTIONS	3 (≥-1)	Defines the maximum number of S-TAP relocations (between managed units) allowed after a full load collection. Negative values means unlimited relocations are allowed.
ALLOW_POLICY_MISMATCH_BETWEEN_APPLIANCES	1 (0 or 1)	The load balancer can take into account managed units' installed policies. • `0`: does not allow S-TAP relocation to an MU that has a different policy. • `1`: allows an S-TAP relocation to an MU that has a different policy.
TIME_TO_IGNORE_STAP_CONNECTION_RELATED_LOAD	10 (≥5)	When collecting the load statistics for S-TAPs of each managed unit, we want to avoid including data that represents the initial S-TAP connection to the managed unit. This data can indicate traffic spikes that create a false-positive for the load balancer. The TIME_TO_IGNORE_STAP_CONNECTION_RELATED_LOAD parameter tells the load balancer to ignore S-TAP load for the specified number of minutes after the S-TAP has connected to the managed unit.
ENABLE_RELOCATION	1 (0 or 1)	Relocation of resources (rebalancing) is a process that the load balancer executes after full load collection. Relocation here means transferring S-TAPs from loaded managed units to vacant manged units. • `0` does not allow relocating S-TAPs to vacant managed units • `1` allows relocating S-TAPs to vacant managed units
LOADED_SNIFFER_QUEUE_USAGE_THRESHOLD	0.6 (0.1 to 1 in increments of 0.1)	A managed unit is considered loaded if its sniffer has at least one queue whose size reaches the LOADED_SNIFFER_QUEUE_ USAGE_THRESHOLD. This parameter should not be changed under normal circumstances.
DEFAULT_STAP_MAX_QUEUE_USAGE	0.15 (0.10 to 1 in increments of 0.10)	When an S-TAP is initially assigned to a managed unit, the load balancer does not have load information about it. The value of this parameter defines the temporary sniffer max used queue until the real load is collected from the managed unit (after the interval defined by the TIME_TO_IGNORE_STAP_CONNECTION_RELATED_LOAD parameter). This parameter should not be changed under normal circumstances.
DEFAULT_STAP_MAX_CONTRIBUTION_TO_MAX_QUEUE_USAGE	0.1 (0.1 to 1 in increments of 0.1)	When an S-TAP is initially assigned to a managed unit, the load balancer does not have load information about it. The value of this parameter defines the temporary max S-TAP load contribution to the temporary max used queue until the real load is collected from the managed unit (after the interval defined by the TIME_TO_IGNORE_STAP_CONNECTION_RELATED_LOAD parameter). This parameter should not be changed under normal circumstances.
REBALANCE_IF_MU_CLASSIFIED_AS_LOADED_N_TIMES_IN_M_HOURS	1:168 (≥0 : ≥0)	Loaded managed units can be rebalanced only if they have been classified as loaded a specified number of instances over a specified period of hours. For example, a value of `1:168` requires that a managed unit be classified as loaded at least `1` time during a period of `168` hours.
APPLIANCE_HW_PROFILE_INDICATORS	NUM_PROCESSORS: CPU_SPEED: CPU_CACHE: CPU_CORES: MEMORY_SIZE (Columns names from the table *APPLIANC*	The load balancer can take into account managed units' hardware profile indicators. A colon delimited list of indicators (column names from the table *APPLIANCE_RESOURCE_INFO*) are used by the load balancer to evaluate the hardware profile. This parameter should not be changed under normal circumstances.

	E_RESOURCE_INFO)	
MAX_CONCURRENT_LOAD_COLLECTIONS	10 (≥1)	The maximum number of concurrent load collection processes the load balancer runs at any given point in time. That is, the number of concurrent, non-persistent, remote SQL connections from the Central Manager to the managed unit.
MAX_RELOCATIONS_PER_MU_BETWEEN_FULL_LOAD_COLLECTIONS	3 (≥-1)	The maximum number of S-TAP relocations allowed from a specific managed unit during any one period of full load. This parameter is the maximum number of STAPs that can be relocated per MU. If you have 2 loading S-TAPs, and the value is set to 1, then only one of these S-TAPs can be moved for a specific MU. If the value is set to 0 then STAP does not relocate. Negative values allow unlimited relocations.
ENABLE_FAILOVER_GROUPS_REBALANCE	0 (0 or 1)	Controls automatic relocation of S-TAP from the failover group back to the main MU group once an MU is available again in the main MU group. 0: does not allow automatic relocation of an S-TAP back to main MU group. 1: allows automatic relocation of an S-TAP back to main MU group.

Parent topic: Enterprise load balancing
Related reference:
GuardAPI Enterprise Load Balancing Functions

Deployment inventory

The inventory view provides centralized view of all database servers and any installed S-TAPs or GIM clients.

Parent topic: Using Central Management Functions

Resource deployment view

The resource deployment view provides a centralized view of all database servers and their associated collectors, aggregators, and central managers.

Parent topic: Using Central Management Functions

Creating managed unit groups

Organize managed units into groups and then take actions on those groups.

About this task

Managed unit groups allow you to organize managed units into meaningful groups and then take actions on those groups. For example, you might create managed unit groups for specific unit types, geographies, or lines of business. Actions you might take include installing policies or distributing patches or configurations to a group of managed units.

Procedure

1. Navigate to Manage > Central Management > Managed Unit Groups.
2. From the Managed Unit Groups page, click  to create a new managed unit group or  to edit an existing group.
3. From the Create new managed unit group dialog, type a name for the group in the Group name field.
   Recommendation: To ensure compatibility with other Guardium components, do not use spaces or special characters in group names.
4. Use the ☐ icons to select managed units to include in the group.
5. When you have finished selecting managed units to include in the group, click the Save button. The new managed unit group will be saved and appear on the Managed Unit Groups page.
6. Optionally, from the Managed Unit Groups page, click the ⊞ icon to expand a group and view its managed units.

Results

Once defined, a managed unit group is available from the Manage > Central Management > Central Management page, the Manage > Central Management > Distribute Configuration Profiles page, as a managed unit group within the Manage > Central Management > Enterprise Load Balance > Associate S-TAPs and Managed Units tool, and in other locations where managed unit groups are used.
Parent topic: Using Central Management Functions

Monitoring Managed Units

Monitor managed units by using Central Management.

To monitor managed units:

1. Log in to the Guardium® GUI of the unit to be managed as the admin user.
2. Click Reports > Guardium Operational Reports > Managed Units to open Managed Units.

Each component of the Central Management pane is described in the table.

Table 1. Monitoring Managed Units

Control	Description

Control	Description
Select all check box	Mark this box in the shaded area of column one to select all managed units.
Unselect all	Clear all managed units.
Check box	Mark this box to select the unit for wanted operation.
Refresh unit information	Refreshes all information that is displayed in the expanded view of that unit and issues new requests to that unit. This action also causes a full user synchronization cycle.
Reboot unit	Reboots the unit at the operating system level. By default, the Guardium portal is started at startup.
Restart unit portal	Restarts the Guardium application portal on the managed unit. You can then log in to that unit to do Guardium tasks (defining or removing inspection engines, for example).
View unit SNMP attributes	Opens the SNMP Viewer pane in a separate window. Clicking the refresh icon in the SNMP Viewer pane refreshes the data in the window.
View unit syslog	Opens the Syslog Viewer in a separate window, displaying the last 64 KB of syslog messages. Clicking the Refresh icon in the Syslog Viewer pane refreshes the data in the window.
Shortcut to unit portal	Opens the Guardium login page for the managed unit, in a separate browser window.
Unit Name	The host name of the managed unit. If you hold the mouse pointer over the unit name, its IP address displays as a tooltip. If the host name changes on the unit, the Central Manager no longer sees that unit when automatically refreshing the Online status. If you suspect the host name was changed, use Refresh on the toolbar. Obtain the changed host name and update the displayed current Online status and other information for that unit.
Online	Indicates whether the unit is online. If the green indicator is lit, the unit is online; if the red indicator is lit, the unit is offline. The Central Manager refreshes this status at the refresh interval that is specified in the central management configuration (1 minute by default). If an error occurred connecting to a unit, the error description can be viewed as a tooltip. Hover the mouse indicator over that unit's record in the management table.
Inspection Engines	Click the ⊞ icon to expand the list of inspection engines; click the ⊟ icon to hide the list of inspection engines. From here, depending on status, you might stop or start the inspection engine. The information that is displayed for each inspection engine is as follows (This information is fetched from the managed unit when the Refresh is pressed, not on every ping): Name - The name of the inspection engine. Protocol - The protocol that is monitored by the inspection engine: Oracle, MSSQL, Sybase, Informix®, or DB2® Active on Startup - Indicates if the inspection engine starts on system startup Exclude From IP - Indicates if the list of from-IP addresses is to be excluded (not examined). From-IP/Mask - A list of the IP addresses and subnet masks of the clients whose database traffic to the To-IP/Mask addresses the inspection engine monitors. Ports - The ports on which database clients and servers communicate; can be a single port, a list of ports, or a range of ports To-IP/Mask - A list of IP addresses and subnet masks of servers whose traffic from the corresponding client machine (From-IP/Mask) is monitored.
Installed Security Policy	The name of the security policy that is installed on the managed unit. This field is updated on every ping.
Model	The Guardium model number of the managed unit.
Version	The Guardium version number of the managed unit.
Last Patch	The last patch installed.
Last Ping Time	The last time that the unit was pinged by the Central Manager to determine the managed unit's online/offline status.
Selected Units	
Group Setup	Group Setup opens a new window that allows the user to maintain groups; creating new groups, removing groups, and associating managed units with groups.
Unregister	Unregister all selected units.
Restarting	
Reboot	Reboot the selected units.
Restart portal	Restart the selected portal.
Restart Inspection Engines	Restart the inspection engines of the selected units.
Distribution	
Refresh	Refresh the selected units.
Install Policy	The policy name is a link that opens a new window with the policy's detail.
Patch Distribution	Patch Distribution opens a new screen, display an available patch list with dependencies, and allow for the selecting of a patch and installing it to all selected units. Schedule a patch up to one year in the future.

Control	Description
Distribute Uploaded JAR files	Click Harden > Vulnerability Assessment > Customer Uploads. Then, enter the name of the file to be uploaded. Otherwise, click the Browse to locate and select that file. Upload one driver at a time. Click Upload. You are notified when the operation completes, and the file that is uploaded is displayed. This action brings the uploaded file to the Central Manager. Select a check box of the managed unit or units where these JAR files are to be distributed. Click Distribute Uploaded JAR files.
Distribute Patch Backup Settings	This setting distributes the following to selected units: PATCH_BACKUP_FLAG; PATCH_AUTOMATIC_RECOVERY_FLAG; PATCH_BACKUP_DEST_HOST; PATCH_BACKUP_DEST_DIR; PATCH_BACKUP_DEST_USER; PATCH_BACKUP_DEST_PASS
Distribute Authentication Config	Select the managed units that receive the distribution of the Central Management authentication. Click Distribute Authentication Config to distribute the authentication configuration to all managed units selected.

Control	Description
Distribute Configurations	The following configurations are distributed to sync parameters between the Central Manager and the managed units: • Anomaly Detection - Active on startup, Polling interval • Alerter - all fields • Data Archive - all fields • Global profile - Concurrent Logins, Data Level Security, all fields except Named Templates (which are already synced), PDF footer text, and logo image • IP-to-Hostname Aliasing - both check boxes • Results Archive - all fields • Results export - all fields • Session Inference - all fields • System Backup - all fields • Data export - all fields Some of these configurations do not take effect until the portal is restarted (Anomaly Detection, Session Inference). Other processes, such as the Alerter, need to be restarted, either directly through the admin portal of the managed unit, or by rebooting all relevant managed units from the manager. The Distribute Configurations does not restart the managed units. There is a separate icon for each managed unit to be restarted. Restart Portal restarts all of the selected units. After Distribution, a message will display saying that the managed units will need to be restarted for all the configurations to take effect on managed units. Each parameter that has scheduling has a second check box. When this second box is checked, this parameter's scheduling is distributed. See Distribute Configuration for information on selectively distributing configurations. Reboot or restart portal? Alerter Active on Startup check box. Each time the appliance restarts, the Alerter is activated automatically. GUI restart does not take the Active on Startup value. Distributing configuration from Central Manager to managed units needs a reboot on managed units to take full effect The Alerter to be manually restarted on the managed units through the admin portal (Admin Console/ Alerter). Since this restart cannot be done from the Central Manager, restart the managed units from Admin Console and get the same effect. Anomaly Detection Active on Startup check box. Each time the appliance restarts, Anomaly Detection is activated automatically. GUI restart takes the Active on Startup value. Distributing configuration from Central Manager to managed units needs restart portal on managed units to take full effect Session Inference Active On Startup check box to start Session Inference on startup of the Guardium appliance. GUI restart takes the Active on Startup value. Distributing configuration from Central Manager to managed units needs restart portal on managed units to take full effect Results Export/System Backup/Data Archive/Result Archive/Data export Distributing configuration from Central Manager to managed units takes effect without restart of portal on managed units Global profile Distributing configuration from Central Manager to managed units takes effect without restart of portal on managed units (Though using a different named template applies only when policy is installed.)
Register New	Opens the Unit Registration pane to register a new unit for management.
Patch Installation Status	The Patch Installation Status screen displays, for each unit, failed installations and discrepancies. For example, having one patch installed on part of the units only, regardless if it failed on other units or was not installed.

Use the Central Manager to assign correlation alerts to individual managed units or managed unit groups

This new feature is for a managed environment.

It allows the central manager to assign correlation alerts to individual managed units or managed unit groups. You can either assign it to a unit or group or you can exclude it from a unit or group. You must also specify whether to run it on the Central Manager itself. The groups used are managed unit groups, the same types of groups that are used on the Central Manager page.

In the managed environment, on the Central Manager, the alert builder has a new section for "Managed Units". In this section, you specify either single units or groups of managed units to either include or exclude from an alert. You also specify with a checkbox whether that Central Manager itself is included or excluded. The default behavior matches the existing behavior: alerts run everywhere. If you specify that alerts should not run everywhere, verify that the alerts run where you specify. The UI includes four options for including/excluding single units or groups, and dialogs for selecting from the list of management groups and if desired, creating new management groups, or editing existing managed unit groups.

On the individual managed units, the alert builder does not show any section on managed units, only the Central Manager can assign alerts to units and groups.

If there are entries in the alert table on a given managed unit, there will automatically be a system generated group created to exclude that unit for each alert it is excluded from. This will occur when the alerts are started on that managed unit.

The alert panes on the anomaly detection page under admin console were used to enable/disable alerts locally. For this feature, the alert panes appear only on the Central Manager.

On the managed units, there is now a table showing active alerts and whether they are enabled.

Parent topic: Using Central Management Functions

Installing Security Policies on Managed Units

Install a security policy on a manage unit.

About this task

To install a security policy on a managed unit:

Procedure

1. Click Setup > Tools and Views > Policy Installation to open Currently Installed Policies and the Policy Installer.
2. From the Policy list, select the policy that you want to install.
3. From the list, select an installation action. After you select an installation action, you are informed of the success (or failure) of each policy installation. If a selected unit is not available (it might be offline or a link might be down), the Central Manager informs you of that fact. It continues attempting to install the new policy for a maximum of seven days (on the condition that unit remains registered for central management).
4. From the Policy list, select the policy that you want to install.
5. The available installation actions include the following items:
    a. Install and Override - delete all installed policies and install the selected one instead
    b. Install last - installing the selected policy as the last one in the sequence; installing the policy after all currently installed policies and having the lowest priority
    c. Install first - installing the selected policy as the first one in the sequence; installing the policy before all currently installed policies.

   Note: If you install a policy from the Central Manager, the selection of Run Once Now (and scheduler) updates existing groups within the installed policies.

   To load changes to rules, including addition and subtraction of groups, you must either:

    a. Initially install policies from the Collector, or
    b. Reinstall policies from the Collector or Central Manager.

Parent topic: Using Central Management Functions

Central Patch Management

Provide visibility and control over patch installation, status, and history.

About this task

Provide visibility and control over patch installation, status, and history. On a Central management cluster provides a way to install patches on managed units from the Central Manager.

When you install a patch, a date and time request can be specified to indicate when the patch is installed. If no date and time is entered or if now is entered, the installation request time is immediate.

Note: A patch that is installed successfully can be installed again. This fact is important for batched patches. A warning informs you if the patch is already installed.

Log in to the Guardium® GUI of the unit to be managed as the admin user:

Procedure

1. Click Manage > Central Management > Central Management.
2. Select the units that need the patch, and click Patch Distribution
3. From the Patch Distribution screen select the patch you want to distribute and click Install Patch Now or Schedule Patch.
4. To see the status of the installation, click Manage > Central Management > Central Management and then select the units and click Patch Installation Status. The Patch Installation Status screen displays, for each unit, failed installations and discrepancies. For example, having one patch installed on part of the units only, regardless if it failed on other units or was not installed. To remove patches from the Patch Distribution screen, click the delete icon (red x) next to the patch. This does not delete the patch from the patch distribution directory on the appliance, but will remove it from the display.

Parent topic: Using Central Management Functions

Working with configuration profiles

Configuration profiles allow you to define configuration and scheduling settings from a central manager and distribute those settings to managed unit groups without altering the configuration of the central manager itself.

Before you begin

Before creating and distributing configuration profiles, verify the following prerequisites:

- allow communication over port 8447 between the central manager and its managed units
- the central manager and the managed units that will receive configurations must be at or above Guardium V10.1

About this task

Configuration profiles contain two types of information: one or more sets of configuration and scheduling settings, and a list of managed unit groups to be updated with the configuration and scheduling settings. Once defined, configuration profiles can be stored, modified, and reused to distribute specific sets of configuration and scheduling settings to specific groups of managed units.

Configuration profiles are defined independently of the local settings on the central manager. This allows you to quickly define configuration settings and deploy those settings to managed unit groups without disrupting the configuration of your central manager or configuring each managed unit individually.

This task describes how to create, distribute, and save a configuration profile.

Procedure

1. Navigate to Manage > Central Management > Distribute Configuration Profiles.
2. Click  or select an existing profile to begin working with a configuration profile.
3. From the Name and description panel, provide a name and optionally provide a description for the profile. Click Next to continue.
   Optional: click the Roles button to specify security roles that can use the configuration profile.
4. From the What to distribute panel, click  to define a new configuration, or select an existing configuration and click  to edit.
   a. From the Configuration type menu, select a configuration type to add to the profile.
   b. Specify configuration and scheduling details for the selected configuration type. For more information about configuration settings, see the product documentation for the configuration type you are defining.
      Restriction: Distributing data export configuration settings to an aggregator will not distribute any purge settings. The existing purge settings on an aggregator will be retained. Purge settings, including retention periods, will be distributed to and replace existing purge settings on collectors.
   c. Click Save to finish editing the configuration details.

   Continue adding or editing configurations as needed. Click Next to continue.
5. From the Where to distribute panel, select groups from the Managed unit groups table and use the  icon to add the groups to the Selected groups table. Click Next to continue.

   Note: click  to create a new managed unit group or  to edit an existing group. Managed unit groups can also be defined and edited at Manage > Central Management > Managed Unit Groups.
6. From the Distribute configurations panel, click Run Now to distribute the configuration profile to the selected groups. When the status indicates that distribution is complete, click Next to continue.
7. From the Review results panel, review a summary of the distribution process and its results.
   Optional: click Run Log to view a detailed log of the distribution process.
8. Click Save to save the configuration profile for reuse.

What to do next

If you need to move configuration profiles between central managers, use Manage > Data Management > Definitions Export and Manage > Data Management > Definitions Import and select Configuration profile from the Type menu.

Parent topic: Using Central Management Functions

Related concepts:

Aggregation
Alerter Configuration
Export/Import Definitions
IP to Hostname Aliasing
Scheduling

Distribute Configuration

Configurations and their schedules, can be distributed, either all or individually, between the Central Manager and the managed units.

Procedure

1. Select the managed units that receive the configurations.
2. Click Distribute Configurations to display the Distribute Configurations window.
3. Check the appropriate boxes for those Configurations that you would like distributed. Use the check box in the header to select all configurations.
4. Check the appropriate boxes for those Schedules that you would like distributed. Use the check box in the header to select all schedules. If a configuration is not scheduled, there is not a check box for it and displays 'n/a' instead.
5. Click Distribute to distribute the configurations and schedules.
6. Option: Click Cancel to abort distribution.

Results

If using the command, Central Management > Distribute Configurations > Global Profile, the following values are distributed:

- ACTIVATE_ALIASES
- CUSTOM_DB_MAX_SIZE
- CHECK_CONCURRENT_LOGIN
- HTML_BOTTOM_RIGHT
- HTML_BOTTOM_LEFT
- DISPLAY_LOGIN_MESSAGE
- LOGIN_MESSAGE
- CSV_DELIMETER
- FILTERING_ENABLED
- INCLUDE_CHILDREN_ON_FILTER
- SHOW_ALL_RECORDS
- ACCORDION_DISABLED
- SCHEDULER_RESTART_INTERVAL
- SCHEDULER_RESTART_WAIT_SHUTDOWN
- ESCALATE_TO_ALL
- MESSAGE_TEMPLATE

Parent topic: Using Central Management Functions

Distribute Authentication Configuration

Instead of configuring authentication on each appliance separately, Central Management authentication (Configure Authentication) can be configured once on the central manager and then distributed to all managed units. This way, information is entered once and it applies to some or all units; some of the units may have a different type of authentication.

Procedure

1. Ensure authentication (Configure Authentication) on both the central manager and the managed unit. So if LDAP authentication is being used, ensure that LDAP is configured on the central manager and the managed unit.
2. Select the managed units to receive the distribution of the central management authentication.
3. Click Distribute Authentication Config to distribute the authentication configuration to all managed units selected.

Parent topic: Using Central Management Functions

Central Manager Redundancy

Use Central Manager Redundancy or Backup Central Manager (CM) to configure a secondary or backup CM in case the Primary CM becomes unavailable.

Central Manager redundancy supports the following:

1. Backup Central Manager - Make Primary CM link will be available after Primary Central Manager loses connection.
2. User Layouts will be retained.
3. User and roles are in the synch backup and will not rely on Portal User Sync.
4. User Group Roles Data will be retained.
5. A GuardAPI function make_primary_cm, has been added to allow switch to Central Manager from CLI.
6. Data is retained from Audit Process Builder processes after switching Primary Central Manager to Backup Central Manager.
7. Central Management backup includes all the definitions (reports, queries, alerts, policies, audit processes etc.), users and roles as it did before.
8. It includes the schedules for enterprise reports, distributed reports and LDAP.
9. It includes schedules for all audit processes, schedules and settings for data management processes such as archive, export, backup, and import.
10. It includes settings for Alerter and Sender.
11. User's GUI customization's, custom classes and uploaded JDBC drivers are included.

Note: Data, either collected data, audit results and custom tables data, is not included.
Note:

To list status of cm_sync_file(s) on Backup CM, use the CLI command, show local_cm_sync_file. To list the value of Backup CM IP for each managed unit, use the GuardAPI command, grdapi show_backup_cm_ip (this API command can only run on a Central Manager).

Note: Failover with Central Manager load balancing - After failover, if the new Managed Units connect and then disconnect right away, the correct DB_USER will not be sent until the failover message is received.

Perform these steps on your development or secondary servers and test. If successful, then perform these steps on your Primary or live Guardium Servers.

Install Patches on Central Manager

1. From the now Primary CM, login as CLI.
2. Install patches with the following CLI command, store system patch install scp
3. This CLI command will copy the files over to your Guardium Server and give you the ability to install them.
4. Watch these patches being installed with the following CLI command, show system patch install

5. Wait until the patch status shows “DONE: Patch installation Succeeded.” for both patches.

Install Patches on Backup CM

1. Login into the now Primary CM GUI as admin.
2. Select the Setup > Tools and Views and then choose Central Manager.
3. Click check boxes for the Backup CM managed unit ONLY on the Central Manager.
4. Click Patch Distribution and install all of the patches that you just installed onto the Primary CM.

Example to install a patch

1. Click Patch Distribution.
2. Click Install Patch Now.
3. Wait approximately 15 minutes to be sure the patch is installed on all managed servers.
4. To verify, login as CLI on the Backup CM and run CLI command, show system patch install, from Backup CM server.

Install Patches on all other managed servers (optional steps)

1. Repeat the previous steps to install patches on all managed servers.
2. Verify that all patches have been installed before going to the next procedure.

After all Patches have been installed on the CM and managed servers

1. Login as admin onto the now Primary CM.
2. Select Setup > Tools and Views and then choose Central Manager. Click Designate Backup CM.
3. Select Backup CM server from the returned list of eligible Backup CM candidates.
4. Click Apply.
5. Wait approximate two minutes for the Backup CM to sync and the NEW Backup CM file to be created and copied to the Backup CM.
6. Wait for two complete rounds of backups to complete (approximate 1 hour) for two Backup CM sync files that will be copied to the Backup CM and can be viewed from the Guardium Monitor tab - Aggregation Archive Log Report.
7. Select Guardium Monitor and select Aggregation/Archive Log Report to view the progress of the creation of the Backup CM sync file.
8. Verify the Activity Backup has started and the cm_sync_file.tgz file has been created from the Aggregation/Archive Log Report.
    a. Login as Admin from the GUI.
    b. Select Guardium Monitor tab.
    c. Select Aggregation/Archive Report.
    d. Look for Backup Types.
9. When complete:
    a. The patches have been installed on the CM.
    b. The patches have been installed on the Backup CM.
    c. Option: The patches have been installed on all other managed units.
    d. Two Backup CM Sync files have been completed (see Aggregation/Archive Log file under Guardium Monitor Tab).
    e. The following steps outline the process to convert the now Primary CM and its managed nodes to the Backup CM.

Note:

- IMPORTANT: Wait approximately one hour to be sure at least TWO of the Backup CM sync files supporting Backup CM have completed.
- The backups schedule for Backup CM sync files is approximately every 30 minutes.
- The process will run on the CM to create a backup CM file and copy that file to the directory on the Backup CM.

Start the Backup CM Process after two sync file process have completed

Shutdown the Primary CM Guardium Server

If you have no access to shutdown the Primary CM, then go directly to the Backup CM and login as Admin. (select Setup > Tools and Views and then choose Central Management) and click Make Primary CM). Skip to section “Steps to start the Backup CM configuration to become the Primary CM” in this document.

1. Wait approximate five minutes and login again as admin in the GUI of the Backup CM.
2. Once the Primary CM is shutdown completely, you can continue onto the next step

Note:

If you are logged into the Primary CM and it goes down, you get a message indicating that the connection has timed out.

Steps to start the Backup CM configuration to become the Primary CM

The secondary CM will not be responsive for approximately five minutes. Login after five minutes and the Make Primary CM link will be available. The link is available under the admin login and (Setup > Tools and Views > Central Management).

1. When the Primary Server goes down, you will get a message on the Backup CM “Unable to connect to Remote Manager, consider switching to (the name of the backup CM)".
2. If you decide to switch:
    a. Login as admin
    b. Select Setup > Tools and Views.
    c. Click Make Primary CM (do not click the “Make Primary CM” link more than once. Also stay on this screen and do not select anything else during the running of this process. A log file will be created that you can view to see the progress and completion of this process.) Be patient as this process will take awhile to complete. There is a safeguard that if you do click this button more than once nothing will change with the current running process.
    d. Within seconds you should get a message “Are you sure you want to make this unit the primary CM? Click OK.
    e. Within a few seconds more you will get a message stating “This may take a few minutes”. The time it takes for the Backup CM to become the primary CM depends on the amount of data backed up from the Backup CM sync file and the amount of managed nodes that switch to the Backup CM which will become the Primary CM. Click OK.

       As soon as we click OK a log file will be created called load_secondary_cm_sync_file.log that will allow you to view the progress of the switch to the completion of the Backup CM switch process. This file can be viewed from your GUI. The following steps indicate how to view this log file.
    f. The last message will take a while to be presented to the screen. It will be the last message before the Backup CM switch has completed. The message is “GUI will restart now. Try to login again in a few minutes and the Backup CM will now become the Primary CM”. Click OK.

       Wait a few minutes for the Backup CM to become Primary and for all the managed nodes to complete switching over to the new Primary CM.

While the CM Backup Process is running – viewing the progress log file

From the Backup CM while the Make Primary CM process is running, you can do the following to view the progress of the Backup CM becoming the Primary CM.

Prerequisite: You will need the IP of the server you are connected to in order to view the log files.

1. Login as CLI from your Backup CM server from a Putty.exe session
2. From CLI run Fileserver <IP> “enter your IP number” 3600", for example: fileserver 9.70.32.122 3600
3. From the GUI, enter the value: http://yourserver.x.x.x.com (will display in the CLI screen after entering the command, example: http://joe.server.guardium.com (the server name will be the Backup CM server).

   Fileserver Window on the UI will open to select file – Select Sqlguard logs
4. Select the file: load_secondary_cm_sync_file.log. (The file will display in a list of files from Step #3.) This will allow you to view the progress of the Backup CM becoming the Primary CM.

   Locate log file for viewing

   CM Backup Process is complete when you see this line in the load_secondary_cm_sync_file.log

   Import CM sync info - DONE
5. Wait approximately 10 minutes for all the Managed units to become available to the New Primary CM.

After the Backup CM becomes the Primary and all Managed nodes are now managed by the Backup CM server

You can now bring up the old CM server. Once it is up and running, perform the following steps to add it as the Backup CM server.

1. Reboot Old Primary CM.
2. Once the Server is up, login as CLI.
3. Delete the manager unit type, enter delete unit type manager.
4. After it completes and you get an OK message from CLI.
5. VERY IMPORTANT: Wait approximately five minutes for the GUI to completely restart even after the deleted unit type displays a successful message and the GUI restart message.
6. After five minutes, log into the New Primary CM to register Old CM as a managed unit.
7. Login as admin on New Primary CM.
8. Select Setup > Tools and Views > Central Management.
9. Click Register New.
10. Enter IP of the Old Primary CM that you just rebooted.
11. Enter 8443 as Port.
12. Click Save. (IMPORTANT: Be patient, do not click this button twice).
13. Wait a minute for the Old Primary CM to become registered.
14. Make the Old Primary CM a New Backup CM.
15. Click Designate Backup CM.

16. Click on Old Primary CM server.
17. Click Apply.
18. Old Primary CM server is NOW the New Backup CM server.
19. Refresh Central Management screen to see the New Unit type Backup CM defined.
20. This task is complete.

Report Data After Backup CM Process is complete

The following data is missing after the Backup CM process is completed. This is related to only the "first" switch from the Primary to the Secondary CM.

Missing Data:

1. Audit Process Results
2. Custom Table Data
3. Custom Report Data
4. VA Results
5. Classifier Results
6. DSD Results
7. CAS results
8. Datamart Data
9. Collected Data
10. Entitlement Data

The reports will be populated again is once you run these reports again on the New Primary CM. If you switch back to the old Primary CM, the data for these reports will be presented.

Parent topic: Using Central Management Functions

Investigation Center

Investigation Center is an extension of the Aggregation Servers. Investigation Users (once defined) can restore data and results of selected historic dates and perform forensic investigation. Once the days (dates) are restored, the investigation users can define and view reports using the standard Guardium® UI, only in the scope of the investigated dates.

Each Guardium appliance maintains a Catalog of all the data and results archived. The Catalog contains information about the archive, its location and credentials to access them. The Catalog is exported from the collectors and merged into a complete Catalog on the Aggregation Server as part of the aggregation process. With the Catalog in place, investigation users can now select the desired dates for restoration and these dates will automatically be uploaded to the Investigation Center and merged into that investigation user's view. In addition to merging collectors' Catalogs through the Aggregation Server, it is also possible to Export and Import Catalogs from Setup > Tools and Views.

Users and Roles

In a Guardium aggregation server there is a special investigation role (inv). Users with the inv role can perform forensic investigations on historic data.

An investigation user for the most part utilizes the same query and report definitions as any other user would. The biggest difference is that the investigation user sees only data selected for his investigation database (multiple investigators can be configured to share an INV database). Selected data can be restored from archive or viewed from the current database in the case of data that was not purged yet. An investigation user can also restore archived audit process results and view them.

Caution: Role inv is a special role which will cause the user to be connected to a separate, investigation-only internal database. It should be combined with the role user and in general it is incompatible with all other roles.

Note: To correctly configure an investigation user, the user's Last Name must be set to the name of one of the three investigation databases, INV_1, INV_2, or INV_3 (case-sensitive).

When creating an investigation user, it is suggested that the user's name correspond or have some representation that denotes which investigation database that will be used. For instance, if a user will be using the INV_1 database, the user's name could be john1 or inv1.

Note: The Run an Ad-Hoc Audit Process button is available on all report screens for all users except investigation (INV) user.

Audit Process and INV role

If the user is INV, then the audit process finder will show audit processes according to roles and ownership, but will only allow Clone or New for all audit processes not owned by INV.

If the user is INV, then the audit process definition menu screen will permit the following:

- Only Investigation users and/or specific email addresses are allowed as receivers (no regular users, no groups, no roles other than INV are permitted as receivers).
- The Events and Additional Columns button within a saved Report Audit Task is always disabled. No API automation can be specified.
- No schedule can be specified. Audit process on INV, data can be run only manually using the Run Now button.
- Only audit tasks of type Report are allowed.
- Active is disabled, Keep Days and Keep Runs fields are disabled.

If the user is not INV, the audit process finder will not display any audit process owned by an investigation user (regardless of the roles assigned).

When an audit process is ran on INV data, the result title is appended with the words Executed on Investigation center by and the name of the INV user.

A comment is attached to the results specifying the dates and source hosts of the data mounted on the Investigation database at execution time.

The results can be viewed either from the Audit Process Builder or for the result navigation list.

Results of audits run on Investigation center cannot be archived and the results are discarded when investigation data is discarded.

Investigation Context

Guardium's Investigation Center supports one to three concurrent investigation periods, dubbed INV_1, INV_2 and INV_3, each can hold separate historic data and provides means to forensic investigation of that period. When creating an investigation user, the user's last name is must be either INV_1, INV_2, or INV_3 to associate that user with one of the investigation databases. When logged into the Investigation Center (using one of the investigation users) a label specifies the selected investigation period.

GUI

A user with the investigation role will see two additional tabs that are particular to the Investigate Center.

- Auditing tab gives access to restored audit process results
- Volume management tab allows the user to set or modify the investigation period, select audit process results to restore and discard data at the end of an investigation.

Working with Investigation Center

- Restore an Investigation Period
- Restore Audit Results
- View Restore Log
- Viewing Restored Audit Results

Restore an Investigation Period

After logging into the Guardium interface as a user with the inv role:

1. Click Manage > Data Management > Data Restore to open the Data Restore Search Criteria.
2. C
3. Click Data Restore to open the Restored Data panel. If a prior restore was performed, this panel will display the currently mounted data periods being used. At this point, you may click Discard Data to un-mount all previously mounted data periods.
4. Click Re-Select Investigation Period to open the Data Restore Search Criteria panel.
5. Enter the start date in the From: box for the beginning time period you wish to search
6. Enter the end date in the To: box for the ending time period you wish to search
7. Optionally, enter a Host name to aid in filtering the result set on the host name
8. Click Search to view the result set - this will search the catalog for all archives matching the search criteria.
9. From the result set produced, check the Select box(es) of those periods you wish to restore. You may also click Select All or Unselect All to speed the selection process.
10. Click Restore to restore the selected periods. Depending on the number of periods to restore, and whether the datasets are local to the system, the restore process could take long time.
11. You can monitor the progress of the restore process in the View Restore Log panel.

Note: Data of any day restored to Investigation Center that falls within the merge period is also merged into the Guardium application database and is visible by non-inv users.

Restore Audit Results

A checkbox in Audit Process builder allows to specify if results of a process should be archived or not. Only results of processes marked for archive for which all signers had signed are archived. Results of a specific runs are packed, zipped and stored, the location is recorded in the catalog and is used by the Restore Audit Results for selection and restore. Archived results from the Guardium Audit process can be restored to an Investigation Center and contain the results, the view and signoff trails as well as the comments associated with these results.

After logging into the Guardium interface as a user with the inv role:

1. Click the Volume Management tab.
2. Click Audit Results Restore to open the Restored Results panel. If a prior restore was performed, this panel will display the currently restored results being used. At this point, you may click Discard Data to un-mount all previously mounted results.
3. Click Audit Results Restore to open the Results Restore Search Criteria panel.
4. Enter the start date in the From: box for the beginning time period you wish to search.
5. Enter the end date in the To: box for the ending time period you wish to search.
6. Optionally, enter a Host name, Audit Process, or Run No to aid in filtering the result set.
7. Click Search to view the result set.
8. From the result set produced, check the Select box(s) of those results you wish to restore. You may also click Select All or Unselect All to speed the selection process.
9. Click Restore to restore the selected results. Depending on the number of results to restore, and whether the datasets are local to the system, the restore process could take long time.
10. You can monitor the progress of the restore process in View Restore Log.

View Restore Log

The restore log provides a view to the Archive/Restore of past and current restore attempts and filtered for the user currently logged in. This log enables the user to validate a successful restore for both data and audit results.

After logging into the Guardium interface as a user with the inv role: Click Restore Log to open My Restore Log. From this panel you will be able to see the status of all restore attempts.

Viewing Restored Audit Results

After logging into the Guardium interface as a user with the inv role:

1. Click the Auditing tab.
2. Click the Results Navigation link to open the Audit Process Finder panel.
3. From the drop down list (if there are audit processes), select a process.
4. Click View to open another window and view the available reports for the audit results.

Parent topic: Aggregation and Central management

Managing your Guardium system

Management tasks include monitoring your system's health and managing artifacts such as groups, domains, and notifications.

- Guardium Administration
  Guardium® administrators perform various administration and maintenance tasks.
- Certificates
  Check certificates periodically to avoid loss of function. Use CLI commands to obtain and install new certificates.
- Unit Utilization Level
  Use unit utilization reports to identify under- and over-utilized systems in your Guardium environment.
- Customer Uploads
  Database Activity Monitor Content Subscription (previously known as Database Protection Subscription Service) supports the maintenance of predefined assessment tests, SQL based tests, CVEs, APARs, and groups such as database versions and patches.
- Services Status panel
  The Services Status panel is a centralized place to check status of services such as CAS or alerter, and if necessary, investigate each service further. Open the Services Status panel by clicking Setup > Tools & Views > Services Status. Each time the Services Status panel is opened, the status of each service is refreshed.
- Archive, Purge and Restore
  Archive and purge operations should be run on a scheduled basis. Use Data Archive and Results Archive to store captured and information for auditing. Amazon S3 Archive and Backup in Guardium also appears at the end of this topic.
- Guardium catalog
  When you archive data from your Guardium system, the Guardium catalog tracks where every archive file is sent, so that it can be retrieved and restored.
- How to manage backup and archiving
  Establish data retention practices; control activity volume; manage scheduling of data archive and purge, and monthly backups.
- Exporting Results (CSV, CEF, PDF)
  CSV, CEF, and PDF files can be created by workflow processes. This function exports all such files that are on the Guardium system.
- Export/Import Definitions
  If you have multiple systems with identical or similar requirements, and are not using Central Management, you can define the components that you need on one system and export those definitions to other systems, provided those systems are on the same software release level.
- Distributed Interface
  Use this configuration screen to define the Distributed Interface and upload the Protocol Buffer (.proto) file to the DIST_INT database.
- Manage Custom Classes
  Upload and maintain custom classes used in alerts or evaluations. Manage custom classes by clicking Setup > Custom Classes.
- SSH Public Keys
  Use this information to create, modify or remove an SSH Public Key.
- How to install an appliance certificate to avoid a browser SSL certificate challenge
  Use IBM Security Guardium CLI commands to create a certificate signing request (CSR), and to install server, certificate authority (CA), or trusted path certificates on your Guardium system.
- Self Monitoring
  The Guardium solution monitors itself to minimize disruptions and correct problems automatically whenever possible.
- Groups
  Using groups makes it easy to create and manage classifier, policy and query definitions, as well as roll out updates to your S-TAP's and GIM clients. Rather than having to repeatedly define a group of data objects for an access policy, put the objects into a group to easily manage them.
- Security Roles
  Security roles are used to grant access to data (groups, queries, reports, etc.) and to grant access to applications (Group Builder, Report Builder, Policy Builder, CAS, Security Assessments, etc).
- Notifications
  Use the Alerter and Alert Builder to create notifications. When email or other notifications are required for alerting actions, follow this procedure for each type of notification to be defined.
- How to create a real-time alert
  Send a real-time alert to the database administrator whenever there are more than three failed logins for the same user within five-minutes.
- Custom Alerting Class Administration
  Use a custom alert class to send alerts to a custom recipient. Upload the custom class, then use the Alert Builder to designate the custom class as an alert notification receiver.
- Predefined Alerts
  Table describing the predefined alerts found in the Alert Builder.
- Scheduling
  The general purpose scheduler is used to schedule many different types of tasks (archiving, aggregation, workflow automation, etc.).
- Aliases
  Create synonyms for a data value or object to be used in reports or queries.
- Dates and Timestamps
  Use a calendar tool to select an exact date, and a relative date picker to select a date that is relative to the current time.
- Time Periods
  Use the Time Period Builder to create time periods that can be used for policy rules and query conditions.
- Time Periods
  Policy rules and query conditions can test for events that occur (or not) during user-defined time periods.

- Comments
  Comments apply to definitions and to workflow process results.
- How to install patches
  Install a single patch or multiple patches as a background process.
- Support Maintenance
  The Support Maintenance feature is password protected and can be used only as directed by Technical Support. Contact Technical Support if you require more information.

Guardium Administration

Guardium® administrators perform various administration and maintenance tasks.

Any user assigned the admin role is referred to as a Guardium administrator. This is distinct from the admin user account.

Admin role Privileges

The Guardium admin role has privileges that are not explicitly assigned to that role. For example, when a user with the admin role displays a list of privacy set definitions, all privacy sets defined on the Guardium system display, and the user with the admin role can view, modify, or delete any of those definitions. When a user without the admin role accesses the list of privacy sets, that user will see only those privacy sets that he or she owns (i.e. created), and all privacy sets that have been assigned a security role that is also assigned to that user.

CLI diag Command Access

Use of the diag CLI command requires an additional password, which can be the password of any user with the admin role.

If automatic account lockout is enabled (a feature that locks a user account after a specified number of login failures), the admin user account may become locked after a number of failed login attempts. If that happens, use the unlock admin CLI command to unlock it.

Note: The access manager (accessmgr) can unlock accounts from the User Browser. Open the User Browser by clicking Access > Access Management > User Browser.

Admin user Privileges

The admin user has additional privileges that are not granted to the admin role, as follows:

- Access to all users' to-do lists
- Owner of imported definitions
- Access management functions

Admin User To-Do List Powers

The To-do List is a workflow automation feature that controls the distribution of audit process results to users. The admin user has special privileges and responsibilities in this area. If a user account is disabled, all audit process results for that user will be reassigned to the admin user automatically. If a user is unavailable for any other reason, audit process results may be installed in that user's to-do list, i.e., awaiting sign-off before being released to the next results receiver. The admin user can open any user's to-do list, and take any actions available to that user. When the admin user performs any actions on another user's to-do list, that fact is noted in the audit process activity log, for example, `User admin signed results on behalf of user x`.

Imported Definition Ownership

When definitions are exported, all roles are removed, and the owner is changed to the admin user. This is the only way to control how the definition will be used on the importing system.

Access Management and the Administrator

For security purposes, there is a separation of duties for the access manager and admin. Admin users cannot have access manager privileges, and vice versa.

The next time the admin user logs in, access manager functionality will be available to them. This is possible for the admin user only (and not for other users having the admin role).

Note:

The same user may contain both of these roles through a legacy situation or as a result of an upgrade. However, current use will not allow the two roles to be assigned to the same user.

In the past, when a unit was upgraded, the accessmgr role was assigned to the admin user, and the accessmgr user was disabled.

In this situation, to configure the accessmgr and admin, log in as admin and enable the accessmgr user, then log in as accessmgr (the default initial password is`guardium`), and remove the accessmgr role from the admin user.

Parent topic: Managing your Guardium system

Certificates

Check certificates periodically to avoid loss of function. Use CLI commands to obtain and install new certificates.

Certification Expiration

Expired certificates will result in a loss of function. Run the show certificate warn_expire command periodically to check for expired certificates. The command displays certificates that will expire within six months and certificates that have already expired. The user interface will also inform you of certificates that will expire. To see a summary of all certificates, run the command show certificate summary.

For more information, see the full list of Certificate CLI Commands.

New Certificates

To obtain a new certificate, generate a certificate signed request (CSR) and contact a third-party certificate authority (CA) such as VeriSign or Entrust. Guardium does not provide CA services and will not ship systems with different certificates than the ones that are installed by default. The certificate format must be in PEM and include BEGIN and END delimiters. The certificate can either be pasted from the console or imported through one of the standard import protocols.

You can generate a certificate signed request (CSR) with one of the following commands:

- create csr alias - This command creates a certificate request with an alias.
- create csr gui - This command creates a certificate request for the tomcat.
- create csr sniffer - This command creates a certificate request for the sniffer.

Note: Do not perform this action until after the system network configuration parameters have been set.
To install a new certificate through the command line interface, use one of the following commands:

- store certificate gim - This command stores GIM certificates in the keystore.
- store certificate gui - This command stores tomcat certificates in the keystore.
- store certificate keystore - This command asks for a one-word alias to uniquely identify the certificate and store it in the keystore.
- store certificate mysql - This command stores mysql client and server certificates.
- store certificate stap - This command stores S-TAP certificates.
- store certificate sniffer - This command stores sniffer certificates.

To install a new certificate key through the command line interface, use one of the following commands:

- store cert_key mysql - This command stores the certificate key of a mysql client and server.
- store cert_key sniffer - This command stores the sniffer certificate key.

Backup and Default Options

You can choose to restore certificates and certificate keys with the backup or default parameter. Use the backup parameter to restore a certificate to the last saved certificate. Use the default parameter to restore a certificate to the original certificate that Guardium supplied.

Changes in Commands

Some certificate commands have been changed.

- csr is now create csr gui.
- create system csr is now create csr sniffer.
- restore keystore is now restore certificate keystore backup.
- restore system-certificate is now restore certificate sniffer default.
- show system certificate is now show certificate sniffer.
- store system certificate is now store certificate sniffer.
- store trusted certificate is now store certificate keystore.
- store certificate console is now store certificate gui.

New Commands

The following commands are available for use.

- create csr alias
- restore certificate keystore default
- restore certificate sniffer backup
- show certificate all
- show certificate gim
- show certificate gui
- show certificate keystore alias
- show certificate keystore all
- show certificate mysql client
- show certificate mysql server
- show certificate summary
- show certificate warn_expired

Deprecated Commands

The following commands have been deprecated.

- csr
- store certificate console
- store system key
- show system key
- store system certificate
- show system certificate

Full List of Commands

Use the following commands to create, restore, show, or store certificates.

- create csr gui
- create csr alias

- create csr sniffer
- restore certificate keystore default
- restore certificate keystore backup
- restore certificate sniffer backup
- restore certificate sniffer default
- show certificate all
- show certificate gim
- show certificate gui
- show certificate keystore alias
- show certificate keystore all
- show certificate mysql client
- show certificate mysql server
- show certificate sniffer
- show certificate summary
- show certificate warn_expired
- store certificate sniffer
- store certificate gui

Parent topic: Managing your Guardium system

Unit Utilization Level

Use unit utilization reports to identify under- and over-utilized systems in your Guardium environment.

Open the unit utilization reports by clicking Manage > Reports > Unit Utilization, and then selecting one of the reports.

The default unit utilization reports include the following:

- Buff Usage Monitor
- CPU Tracker
- Enterprise Buffer Usage Monitor
- Unit Utilization

Utilization Parameters

Most parameters are averaged for a specific unit over a specific time range. The number of restarts is a count of the sniffer restarts during a specific time range based on the different PIDs.

The parameters supported are:

- Number of restarts
- Sniffer memory
- Percent MySQL memory
- Free buffer space
- Analyzer queue
- Logger queue
  Restriction: There is a limit of 500 SQLs in the logger queue. If more than 500 SQLs try to fill this queue at the same time, any additional SQLs beyond the queue limit will log `RA=-1`.
- MySQL disk usage
- System CPU load
- System var disk usage
- Number of requests
- Number of full SQL
- Number of exceptions
- Number of policy violations
- Quick search disk usage
- Quick search number of documents
- Flat log requests

Thresholds

For each parameter there are two thresholds defined that separate three utilization levels: Low, Medium, and High.

Utilization levels:

- Low: value is less than Threshold1
- Medium: value is greater than Threshold1, and less than Threshold2
- High: value is greater than Threshold2

There is also an overall utilization level for each unit. For each period of time, this level is the highest level for all levels during that period.

Reporting

View the available unit utilization reports by clicking Manage > Reports > Unit Utilization.

The Unit Utilization Levels tracking option allows you to create custom queries and reports.

Using aliases is recommended when using unit utilization data in custom and predefined reports. Otherwise, utilization levels will display as numbers: 1, 2, 3, instead of Low, Medium, High.

The list of attributes includes:

- Host name
- Period start
- Number of restarts
- Number of restarts level
- Sniffer memory
- Sniffer memory Level
- Percent MySQL memory
- Percent MySQL memory level
- Free buffer space
- Free buffer space level
- Analyzer queue
- Analyzer queue level
- Logger queue
- Logger queue level
- MySQL disk usage
- MySQL disk usage level
- System CPU load
- System CPU load level
- System var disk usage
- System var disk usage level
- Overall unit utilization level
- Number of requests
- Number of requests level
- Number of full SQLs
- Number of full SQLs level
- Number of exceptions
- Number of exceptions level
- Number of policy violations
- Number of policy violations level
- Number of flat log requests
- Number of flat log requests level

Note: Each parameter has a value and a level which is calculated based on the value and the thresholds.

Throughput information available in Unit Utilization

Throughput data is collected on each collector unit. The CM consolidates all throughput data and creates an enterprise custom table that is added to predefined utilization reports.

Throughput information collected:

- Number of requests (for the period) (from construct instance)
- Number of full SQLs (for the period) (from construct text)
- Number of exceptions
- Number of policy violations

By default, throughput information is collected every hour.

GuardAPI and CLI commands for Unit Utilization

Guard APIs:

- listUtilizationThresholds

  updateUtilizationThresholds

  reset_unit_utilization

CLI commands:

- store monitor gdm_statistics
- show monitor gdm_statistics

- Configuring unit utilization data processing
  This procedure describes how to configure Guardium systems for processing and displaying unit utilization data.

Parent topic: Managing your Guardium system

Configuring unit utilization data processing

This procedure describes how to configure Guardium systems for processing and displaying unit utilization data.

About this task

For a centrally managed environment, viewing unit utilization information requires scheduling two processes on the central manager: uploading data for the central manager buffer usage monitor, and processing the unit utilization data.

For a standalone system, viewing unit utilization information only requires scheduling the processing of unit utilization data. There is no need to schedule data upload for a central manager buffer usage monitor when working with a standalone system.

Procedure

1. For a centrally managed environment, define a schedule on the central manager for uploading the central manager buffer usage monitor data.
    a. Navigate to Reports > Report Configuration Tools > Custom Table Builder.
    b. From the Custom Tables screen, select CM Buffer Usage Monitor and click Upload Data to continue.
    c. From the Upload Data screen, click Modify Schedule to define a schedule for uploading the central manager buffer usage monitor data. Click Save after defining a schedule, then click Back to return to the Upload Data screen. Scheduling the process to run once every hour is a reasonable starting point for many deployments, but you may want to adjust the interval around your available resources or data-currency needs.
    Important: To ensure that the most recent data is available for unit utilization reports, define a schedule that processes the buffer usage monitor data before processing the unit utilization data. Additionally, the buffer usage monitor data should not be scheduled to run exactly on the hour.
    Best practice: Define schedules that process the buffer usage monitor data at 10-minutes after the hour and unit utilization data at 40-minutes after the hour.
    d. From the Upload Data screen, optionally click Run Once Now to immediately upload the data.
2. For a centrally managed environment or for a standalone system, define a schedule for processing unit utilization data. In a centrally managed environment, you only need to define the unit utilization schedule on the central manager.
    a. Navigate to Manage > Unit Utilization > Unit Utilization Levels.
    b. From the Unit Utilization Levels screen, click Modify Schedule to define a schedule for processing unit utilization data. Click Save after defining a schedule, then click Back to return to the Unit Utilization Levels screen. Scheduling the process to run once every hour is a reasonable starting point for many deployments, but you may want to adjust the interval around your available resources or data-currency needs.
    Important: To ensure that the most recent data is available for unit utilization reports, define a schedule that processes the unit utilization data after processing the buffer usage monitor data.
    Best practice: Define schedules that process the buffer usage monitor data at 10-minutes after the hour and unit utilization data at 40-minutes after the hour.
    c. From the Unit Utilization Levels screen, optionally click Run Once Now to immediately process the data.

Results

After completing these steps, navigate to Manage > Reports > Unit Utilization to view unit utilization reports. In a centrally managed environment, data will be available for the central manager and its managed units. For a standalone system, data will only be available for that individual system. If you did not use the Run Once Now option when defining the schedules, you must wait until those processes run before the unit utilization reports will update with the latest data.
Parent topic: Unit Utilization Level

Customer Uploads

Database Activity Monitor Content Subscription (previously known as Database Protection Subscription Service) supports the maintenance of predefined assessment tests, SQL based tests, CVEs, APARs, and groups such as database versions and patches.

Uploads are used to keep information current and within industry best practices to protect against newly discovered vulnerabilities. Distribution of updates is done on a quarterly basis.

Use Customer Uploads to upload the following: DPS update files; Oracle JDBC drivers; MS SQL Server JDBC drivers; and, DB2 for z/OS license jar.

Note: If a custom group exists with the same name as a predefined Guardium® group, the upload process will add Guardium in front of the name for the predefined group.

1. Open Customer Uploads by clicking Harden > Vulnerability Assessment > Customer Uploads.
2. For DPS Upload, click Browse to locate and select the file to be uploaded.
   Note: Reference the Import DPS pane to see what files have been uploaded.
3. For Upload DB2 z/OS License jar, click Browse to locate and select the file.
4. Use Upload Oracle JDBC driver or Upload MS SQL Server JDBC driver to upload open source drivers. After uploading, you will see the databases added to the Datasource finder. Upload one driver at a time.
   Note: There are two instances where open source drivers are recommended over Oracle Data Direct drivers or MS SQL Data Direct drivers.
    a. To support Windows Authentication for MS SQL Server. In all other uses, the Data Direct driver pre-loaded in the Guardium appliance is sufficient.
    b. When using the Value Change Tracking application for Oracle version 10 or higher, the open source driver is recommended in order to support using streams instead of triggers.

   Use keywords to search and download open source JDBC drivers (for example: *open source JDBC driver for MS SQL*).
5. Use the Central Manager to distribute the .jar file to managed units. After the file is successfully uploaded, the GUI needs to be restarted on the Central Manager and the managed units.

Note:

If you will be exporting and importing definitions from one unit to another, be aware that subscribed groups are not exported. When exporting definitions that reference subscribed groups, you must ensure that all referenced subscribed groups are installed on the importing unit (or central manager in a federated environment).

When uploading DB2® z/OS® license jar files, the license will take effect after restart of the GUI.

Note: If the DPS stops for any reason (for example, a server restart or a GUI restart), it is recommended to wait 30 minutes before starting the DPS upload process again.

Enable ASO on the Oracle server using latest Oracle DataDirect driver

Refer to the following when enabling ASO on the Oracle server using the latest Oracle DataDirect driver.

SQLNET.CRYPTO_CHECKSUM_SERVER = required

SQLNET.ENCRYPTION_SERVER = required

SQLNET.ENCRYPTION_TYPES_SERVER = (AES256, AES192, AES128)

#SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER = (SHA256)

SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER = (SHA1)

The Oracle JDBC driver will work and does not require specifying a connection property.

But the latest Oracle JDBC driver must be downloaded from Oracle. The filename is ojdbc7.jar. Use keywords to search and download open source JDBC drivers (for example: open source JDBC driver for Oracle). Then upload that driver to the appliance using the Guardium Customer Uploads function.

If you continue to use Oracle DataDirect driver, then you need to specify a connection property to the datasource.

Use the following when defining the Oracle DataDirect driver connection property:

DataIntegrityLevel=required;EncryptionLevel=required;DataIntegrityTypes=(MD5,SHA1)

Note: The current Oracle DataDirect driver does not support SHA-256. So SHA-1 has to be used. That is why sqlnet.ora reference (#SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER = (SHA256)) had to be commented out. However, if a Guardium customer must connect using SHA-256, they should use the Oracle JDBC driver instead.

Data Direct references:

https://www.progress.com/documentation/datadirect-connectors

Download the Oracle database JDBC User' Guide PDF for a list of command references.

Use a TAB Delimited file (.TXT) when creating and saving a Datasource Upload file from the Customer Upload functionality

If you choose to use a comma delimited file structure (.CSV), it will not behave as intended if any column value contains a comma.

Follow these steps

1. If using EXCEL, save file as a TAB Delimited (.TXT) file.
2. If using OpenOffice or Libre Office then save a (.CSV) file with TAB Delimiters.
3. Log in as admin and open Customer Uploads by clicking Harden > Configuration Change Control (CAS Application) > Customer Uploads.
4. For Upload CSV to Create/Update Datasources, click Browse..., and select the tab delimited file.

Create Datasource for CSV uploaded via the Upload CSV menu

Follow the proceeding steps to create a Tab Delimited .TXT formatted file containing datasource information. This Tab Delimited .TXT file can then be used with the Customer Upload function in the Guardium application to many datasource types.

Use the function to import datasources was not always compatible with each Guardium Software Release. This procedure will enable the uploading of any datasource.

The following is a list of Header Columns that should be added to an Excel spreadsheet when creating the .TXT tab delimited datasource upload file:

Column Values (accepted for .CSV datasource upload file)

Table 1. create_datasource

Parameter	Description
application	Required. Identifies the application for which the datasource is being defined. It must be one of the following: ChangeAuditSystem Access_policy MonitorValues DatabaseAnalyzer AuditDatabase CustomDomain Classifier AuditTask SecurityAssessment Replay Stap_Verification
compatibilityMode	Compatibility Mode: Choices are Default or MSSQL 2000. The processor is told what compatibility mode to use when monitoring a table.
conProperty	Optional. Use only if additional connection properties must be included on the JDBC URL to establish a JDBC connection with this datasource. The required format is property=value, where each property and value pair is separated from the next by a comma. For a Sybase database with a default character set of Roman8, enter the following property: charSet=utf8
customURL	Optional. Connection string to the datasource; otherwise connection is made using host, port, instance, properties, etc. of the previously entered fields. As an example this is useful for creating Oracle Internet Directory (OID) connections.
dbInstanceAccount	Optional. Database Account Login Name (software owner) that will be used by CAS
dbInstanceDirectory	Optional. Directory where database software was installed that will be used by CAS
dbName	Optional. For a DB2 or Oracle datasource, enter the schema name. For others, enter the database name.
description	Optional. Longer description of the datasource.
host	Required. Can be the host name or the IP address.
name	Required. Provides a unique name for the datasource on the system.

Parameter	Description
owner	Required. Identifies the Guardium user account that owns the datasource.
password	Optional. Password for owner. If used, user must also be used.
port	Optional (integer). Port number.
serviceName	Required for Oracle, Informix®, DB2, and IBM® ISeries. For a DB2 datasource enter the database name, for others enter the service name.
severity	Optional. Severity Classification (or impact level) for the datasource.
shared	Optional (boolean). Set to **true** to share with other applications. To share the datasource with other users, you will have to assign roles from the GUI.
type	Required. Identifies the datasource type; it must be one of the following: DB2 DB2 for i DB2 for z/OS Informix MS SQL Server MS SQL Server (DataDirect) MySQL NA Netezza Oracle (DataDirect) Oracle (Service Name) Oracle (SID) PostgreSQL Sybase Sybase IQ Teradata The following can be used when the application is CustomDomain or Classifier: TEXT TEXT:FTP TEXT:HTTP TEXT:HTTPS TEXT:SAMBA
user	Optional. User for the datasource. If used, password must also be used.
environmentTitle	Required for cloud database service protection. Account name.
region	Required for cloud database service protection. The AWS region.
objectLimit	Required for cloud database service protection. The maximum number of objects found in the classification process that are added automatically to the list of audited objects. See Cloud database service protection
primaryCollector	Relevant for cloud database service protection. The collector that extracts the audit data from the cloud database.

Notes:

1. Each of the column names must be included in the Excel spreadsheet SAVED as a TAB delimited (.TXT) file.
2. The Created Datasource name (what is shown when looking for the datasource) is made up of both the name column and the type column.
3. Upload file MUST be saved as a Column Tab Delimited file type.

Steps to create and upload txt file in a Text CSV format file and add Datasource Data

1. Create the Excel spreadsheet file save as a Tab Delimited .TXT file with the following headers and datasource data to support the datasource import capability.
2. Create and save your .txt file to your PC or UNIX/Linux device for uploading into the Guardium application.
3. Login as admin and open Customer Uploads by clicking Harden > Configuration Change Control (CAS Application) > Customer Uploads
4. From Upload CSV to Create/Update Datasources, click Browse and select the .txt file containing the tab delimited datasource information.
5. Click Upload.

A message will display showing which values from the .txt file were uploaded:

1. **New**: Per file upload (if save file and added New Datasource member(s), these members will be have the status of NEW.
2. **Update**: Upload SAME datasource that you made changes on will give an Update status.
3. **Fail**: Displayed failed datasource or errors

Parent topic: Managing your Guardium system

Services Status panel

The Services Status panel is a centralized place to check status of services such as CAS or alerter, and if necessary, investigate each service further. Open the Services Status panel by clicking Setup > Tools & Views > Services Status. Each time the Services Status panel is opened, the status of each service is refreshed.

Say that you set up a policy that sends a real-time alert whenever there are more than three failed log-ins in 5 minutes. To protect against this possible intrusion, you must make sure that the policy was installed, and that the alerter is on.

Use the Services Status panel to verify that both of these services are configured properly.

Clicking any service takes you to its configuration page, where you can, as relevant, turn the service off or on, restart a service, configure a service, etc.

If for some reason the policy didn't install correctly, click Setup > Tools & Views > Policy Installation to go to Policy Installer, view the currently installed policies, and make the necessary changes.

Each service displays one of the following icons:

- Service is running/scheduled: 
- Service is paused: 
- Service is off: 

Parent topic: Managing your Guardium system

Archive, Purge and Restore

Archive and purge operations should be run on a scheduled basis. Use Data Archive and Results Archive to store captured and information for auditing. Amazon S3 Archive and Backup in Guardium also appears at the end of this topic.

Data Archive and Results Archive can be found by clicking Manage > Data Management.

- Data Archive backs up the data that has been captured by the Guardium system, for a time period. When configuring Data Archive, a purge operation can also be configured. Typically, data is archived at the end of the day of everyday to ensure that in the event of a catastrophe, only one day of data is lost. The purging of data depends on the application and is highly variable, depending on business and auditing requirements. In most cases, data can be kept on the Guardium systems for more than six months.
- Results Archive backs up audit tasks results (reports, assessment tests, entity audit trail, privacy sets, and classification processes) as well as the view and sign-off trails and the accommodated comments from workflow processes. Results sets are purged from the system according to the workflow process definition.

In an aggregation environment, data can be archived from the collector, from the aggregator, or from both locations. Most commonly, the data is archived only once, and the location from where it is archived varies depending on your requirements.

Scheduled export operations send data from Guardium® collector units to a Guardium aggregation server. On its own schedule, the aggregation server executes an import operation to complete the aggregation process. On either or both units, archive and purge operations are scheduled to back up and purge data regularly (both to free up space and to speed up access operations on the internal database).

Archive files can be sent using SCP or FTP protocol, or to an EMC Centera or TSM storage system (if configured). You can define a single archiving configuration for each Guardium system.

Guardium's archive function creates signed, encrypted files that cannot be tampered with. DO NOT change the names of the generated archive files. The archive and restore operations depend on the file names that are created during the archiving process.

Archive and export activities use the system shared secret to create encrypted data files. Before information encrypted on one system can be restored on another, the restoring system must have the shared secret that was used on the archiving system when the file was created.

Whenever archiving data, be sure to verify that the operation completes successfully. To do this, open the Aggregation/Archive Log by clicking Manage > Reports > Data Management > Aggregation/Archive Log. There should be multiple activities that are listed for each archive operation, and the status of each activity should as completed.

Perform System Backup tasks by clicking Manage > Data Management > System Backup. You can also perform backup tasks from the CLI. See File handling CLI commands for further information.

Default Purging

- The default value for purge is 60 days
- The default purge activity is scheduled every day at 5:00 AM.
- For a new install, a default purge schedule is installed that is based on the default value and activity.
- When a unit type is changed to a managed unit or back to a standalone unit, the default purge schedule is applied.
- The purge schedule will not be affected during an upgrade.
- When purging a large number of records (10 million or higher), a large batch size setting (500k to 1 million) is the most effective way to go. Using a smaller batch size or NULL causes the purge to take hours longer. Smaller purges finish quickly, so a large batch size setting is only relevant for large purges.

Note: Setting batch size is not available in the UI. Use the GuardAPI command grdapi set_purge_batch_size batchSize to set batch size.

How to determine what days are not archived

Use the Report Builder to view the list of all files with archive dates. Open the Report Builder by clicking Manage > Reports > Report Builder. From the Query menu, select Location View. Dates not on this report indicate that those dates have not been archived. Run archive for the dates not on the list, if required.

Configure Data Archive and Purge

1. Open the Data Archive by clicking Manage > Data Management > Data Archive.
2. To archive, check the Archive check box. Additional fields will appear in the Configuration panel.
3. For Archive data older than, enter a value and select a unit of time from the menu. To archive data starting with yesterday's data, enter the value `1`, and select Day(s) from the menu.
4. Use Ignore data older than to control how many days of data is archived. Any value that is specified here must be greater than the Archive data older than value. Note: If you leave this field blank, you archive data for all days older than the value specified in Archive data older than. This means that if you archive daily and purge data older than 30 days, you archive each day of data 30 times (before it is purged on the 31st day).
5. Check the Archive Values check box to include values from SQL strings in the archived data. If this box is cleared, values are replaced with question mark characters on the archive (and hence the values will not be available following a restore operation).
6. Select a Protocols option, and fill in the appropriate information. Depending on how your Guardium system has been configured, one or more of these buttons might not be available. For a description of how to configure the archive and backup storage methods, see the description of the show and store storage-system commands.
7. Perform the appropriate procedure, depending on the storage method selected:
   - Configure SCP or FTP Archive or Backup
   - Configure EMC Centera Archive or Backup
   - Configure TSM Archive or Backup
8. Check the Purge check box to define a purge operation.

   IMPORTANT: The Purge configuration is used by both Data Archive and Data Export. Changes that are made here apply to any executions of Data Export and vice versa. In the event that purging is activated and both Data Export and Data Archive are run on the same day, the first operation that runs will likely purge any old data before the second operation's execution.

   For this reason, any time that Data Export and Data Archive are both configured, the purge age must be greater than both the age at which to export and the age at which to archive.

9. If purging data, use the Purge data older than field to specify a starting day for the purge operation as a number of days, weeks, or months before the current day, which is day zero. All data from the specified day and all older days are purged, except as noted. Any value that is specified for the starting purge date must be greater than the value specified for the Archive data older than value. In addition, if data exporting is active, the starting purge date that is specified here must be greater than the Export data older than value. See the IMPORTANT note.
   Note:

   There is no warning when you purge data that has not been archived or exported by a previous operation.

   The purge operation does not purge restored data whose age is within the do not purge restored data timeframe that is specified on a restore operation.

10. Use the Scheduling section to define a schedule for running this operation on a regular basis.
11. Click Save to save the configuration changes. The system attempts to verify the configuration by sending a test data file to that location.
    - If the operation fails, an error message is displayed and the configuration will not be saved.
    - If the operation succeeds, the configuration is saved.
12. Click Run Once Now to run the operation once.

Configure SCP or FTP Archive or Backup

After selecting SCP or FTP in an archive or backup configuration panel, the following information must be provided:

1. For Host, enter the IP address or host name of the host to receive the archived data.
2. For Directory, identify the directory in which the data is to be stored. How you specify this depends on whether the file transfer method used is FTP or SCP.
   - For FTP: Specify the directory relative to the FTP account home directory.
   - For SCP: Specify the directory as an absolute path.
3. For Port that can be used to send files over SCP and FTP. The default port for ssh/scp/sftp is 22. The default port for FTP is 21.
   Note: Seeing a zero (0) for port indicates that the default port is being used and that there is no need to change.
4. For Username and Password, enter the credentials for the user logging on to the SCP or FTP server. This user must have write/execute permissions for the directory that is specified in Directory.

   For Windows, a domain user is accepted with the format of domain\user

5. Click Save to save the configuration.

Configure EMC Centera Archive or Backup

This backup or archiving task copies files to an EMC Centera storage system off-site. A license is needed with user name and password from EMC. Four main actions are needed for this task:

1. Establish account with an EMC Centera on the network (IP addresses and a ClipID are needed)
2. Configure the data and/or configuration files from a Guardium system
3. Define and export a library
4. Confirm that your files are stored on the EMC Cetera storage system.

CLI action

From the CLI, run these commands:

```
store storage-system centera backup ON
show storage-system
```

Configure Centera Archive or Backup

Open System Backup by clicking Manage > Data Management > System Backup. Select EMC Centera, the following information must be provided:

1. For Retention, enter the number of days to retain the data. The maximum is 24855 (68 years). If you want to save it for longer, you can restore the data later and save it again.
2. For Centera Pool Address, enter the Centera Pool Connection String; for example: 10.2.3.4,10.6.7.8?/var/centera/us1_profile1_rwe.pea txt
   Note: This IP address and the .PEA file comes from EMC Centera. The question mark is required when configuring the path. The .../var/centera/... path name is important as the backup might fail if the path name is not followed. The .PEA file gives permissions, username, and password authentication per Centera backup request.
3. Click Upload PEA File to upload a Centera PEA file to be used for the connection string. The Centera Pool Address is still needed.
   Note: If the message `Cannot open the pool at this address.` appears, check the size of the Guardium system host name. A timeout issue has been reported with Centera when using host names that are fewer than four characters in length.
4. Click Save to save the configuration. The system attempts to verify the Centera address by opening a pool using the connection string specified. If the operation fails, you will be informed and the configuration will not be saved.
5. Click Run Once Now to perform the backup using the downloaded .PEA file.

Confirm that your files have been copied to the EMC Centera. The name of the files and a ClipID are required for this task.

Configure TSM Archive or Backup

Before archiving to a TSM server, a dsm.sys configuration file must be uploaded to the Guardium system, via the CLI. Use the import tsm config CLI command. After you select TSM in an archive or backup configuration panel, provide following information:

1. For Password, enter the TSM password that this Guardium system uses to request TSM services, and re-enter it in the Re-enter Password box.
2. Optionally, enter a Server name matching a servername entry in your dsm.sys file.
3. Optionally, enter an As Host name.
4. Click Save to save the configuration. When you click the Save button, the system attempts to verify the TSM destination by sending a test file to the server using the dsmc archive command. If the operation fails, you will be informed and the configuration will not be saved.
5. Return to the archiving or backup procedure to complete the configuration.

Configure Results Archive

1. Open the Results Archive by clicking Manage > Data Management > Results Archive (Audit).
2. In the files following Archive results older than, specify a starting day for the archive operation as a number of days, weeks, or months before the current day, which is day zero. To archive results starting with yesterday's data, enter the value 1, and select Day(s) from the list.
3. Optionally, use the fields following Ignore results older than to control how many days of results are archived. Any value that is specified here must be greater than the Archive results older than value.
4. Select a storage method from the radio buttons. Depending on how the Guardium system has been configured, one or more of these buttons might not be available. For a description of how to configure the archive and backup storage methods, see the description of the show storage-system and store storage-system commands in Configuration and Control CLI Commands.
   - EMC CENTERA
   - TSM
   - SCP
   - FTP
5. Perform the appropriate procedure depending on the storage method selected:
   - Configure SCP or FTP Archive or Backup
   - Configure EMC Centera Archive or Backup
   - Configure TSM Archive or Backup
   - Amazon S3 Archive and Backup in Guardium
6. Use the Scheduling section to define a schedule for running this operation on a regular basis.
7. Click Save to verify and save the configuration changes. The system attempts to verify the configuration by sending a test data file to that location.
   - If the operation fails, an error message is displayed and the configuration will not be saved.
   - If the operation succeeds, the configuration is saved.
8. Click Run Once Now to run the operation once.

Restore Data

If this system is not the system that generated the archive to be restored, you must create a location entry in the catalog via Catalog Archive, then click Add (reference: Guardium catalog) or GuardAPI (reference: CLI and API > GuardAPI Reference > GuardAPI Catalog Entry Functions). When the Data Restore is started this information is used to transfer the file to the system before processing the data.

Before Restoring Data

- Before restoring from TSM, a dsm.sys configuration file must be uploaded to the Guardium system, via the CLI. Use the import tsm config CLI command.
- Before restoring from EMC Centera, a pea file must be uploaded to the Guardium system, via the Data Archive panel.
- Before restoring or importing a file that was encrypted by a different Guardium system, make sure that the system shared secret used by the Guardium system that encrypted the file is available on this system (otherwise, it will not be able to decrypt the file). See About the System Shared Secret in System Configuration.
- Before restoring on a Guardium collector run the CLI command stop inspection-core to stop the inspection-core process.
  Note: The data cannot be captured during the restore process.

To restore data:

1. Open Data Restore by clicking Manage > Data Management > Data Restore.
2. Enter a date in From to specify the earliest date for which you want data.
3. Enter a date in To to specify the latest date for which you want data.
4. For Host Name, optionally enter the name of the Guardium system from which the archive originated.
5. Click Search.
6. In the Search Results panel, check the Select check box for each archive you want to restore.
7. In the Don't purge restored data for at least field, enter the number of days that you want to retain the restored data on the system.
8. Click Restore.
9. Click Done when you are finished.

Note: The restore of data archived from a collector should be done only to: the same collector; an aggregator; or, a different collector dedicated to investigation that is not part of an aggregation cluster. In the case of a crashed collector, a system backup can be restored onto a new, clean collector.

Amazon S3 Archive and Backup in Guardium

Use this feature to archive and backup data, from Guardium, to Amazon S3.

Amazon S3 (Amazon Simple Storage Service) provides a simple web service interface that can be used to store and retrieve any amount of data, at any time, from anywhere on the web. It gives any developer access to the same highly scalable, reliable, secure, inexpensive infrastructure that Amazon uses to run its own web sites.

Prerequisites

1. An Amazon account.
2. Register for S3 service
3. Amazon S3 credentials are required in order to access Amazon S3. These credentials are:
    - Access Key ID - identifies user as the party responsible for service requests. It needs to be included it in each request. It is not confidential and does not need to be encrypted. (20-character, alphanumeric sequence).
    - Secret Access Key - Secret Access Key is associated with Access Key ID calculating a digital signature included in the request. Secret Access Key is a secret, and only the user and AWS should have it (40-character sequence). This key is just a long string of characters (and not a file) that is used to calculate the digital signature that needs to be included in the request.

- Data Archive backs up the data that has been captured by the system, for a given time period.
- Results Archive backs up audit tasks results (reports, assessment tests, entity audit trail, privacy sets, and classification processes) as well as the view and sign-off trails and the accommodated comments from work flow processes.

When Guardium data is archived, there is a separate file for each day of data.

Archive data file name format:

```
<time>-<hostname.domain>-w<run_datestamp>-d<data_date>.dbdump.enc
```

Guardium's archive function creates signed, encrypted files that cannot be tampered with. The names of the generated archive files should not be changed. The archive operation depends on the file names that are created during the archiving process.

System backups are used to backup and store all the necessary data and configuration values to restore a server in case of hardware corruption.

All configuration information and data is written to a single encrypted file and sent to the specified destination, using the transfer method that is configured for backups on this system.

Backup system file format:

```
<data_date>-<time>-<hostname.domain>-SQLGUARD_CONFIG-9.0.tgz
<data_date>-<time>-<hostname.domain>-SQLGUARD_DATA-9.0.tgz
```

Use the Aggregation/Archive Log report in Guardium to verify that the operation completes successfully. Open the Aggregation/Archive Log by clicking Manage > Reports > Data Management > Aggregation/Archive Log. There should be multiple activities that are listed for each Archive operation, and the status of each activity should be *Succeeded*.

Regardless of the destination for the archived data, the Guardium catalog tracks where every archive file is sent, so that it can be retrieved and restored on the system with minimal effort, at any point in the future.

A separate catalog is maintained on each system, and a new record is added to the catalog whenever the system archives data or results.

Catalog entries can be transferred between appliances by one of the following methods:

- Aggregation - Catalog tables are aggregated, which means that the aggregator will have the merged catalog of all of its collectors
- Export/Import Catalog - These functions can be used to transfer catalog entries between collectors, or to backup a catalog for later restoration, etc.
- Data Restore - Each data restore operation contains the data of the archived day, including the catalog of that day. So, when restoring data, the catalog is also being updated.

When catalog entries are imported from another system, those entries will point to files that have been encrypted by that system. Before restoring or importing any such file, the system shared secret of the system that encrypted the file must be available on the importing system.

Enable Amazon S3 from the Guardium CLI

Amazon S3 archive and backup option is not enabled by default in the Guardium GUI. To enable Amazon S3 via Guardium CLI, run the following CLI commands:

```
store storage-system amazon_s3 archive on
store storage-system amazon_s3 backup on
```

Amazon S3 requires that the clock time of Guardium system to be correct (within 15-minutes). Otherwise, this results in an Amazon error. If there is too large a difference between the request time and the current time, the request will not be accepted.

If the Guardium system time is not correct, set the correct time using the following CLI commands:

```
show system ntp server
store system ntp server (An example is ntp server: ntp.swg.usma.ibm.com)
store system ntp state on
```

User Interface

Use the System Backup to configure the backup. Open the System Backup by clicking Manage > Data Management > System Backup.

User input requires:

- S3 Bucket Name (Every object that is stored in Amazon S3 is contained in a bucket. Buckets partition the namespace of objects that are stored in Amazon S3. Within a bucket, you can use any names for your objects, but bucket names must be unique across all of Amazon S3.
- Access Key ID
- Secret Access Key

If bucket name does not exist, it will get created.

Secret Access Key is encrypted when saved into the database.

Check that files got uploaded on Amazon S3

1. Log onto AWS Management Console using your email address and password.

http://aws.amazon.com/console/

1. Click S3.
2. Click the bucket that you specified in Guardium UI.

How to purge data from the Guardium appliance

Two areas can get full on a Guardium appliance which can then cause the GUI to stop:

- The internal database
- The filesystem itself (usually the /var partition)

As user CLI, check if the database is full with this CLI command:

support show db-status free %

If this comes back with 10% or less, the database is 90% full or more.

To check if /var partition (filesystem) is 90% full or more. run a must gather command from the CLI:

support must_gather system_db_info

You should be able to use fileserver to check the df -k output within the system_output.txt file that can be seen in fileserver

must_gather/system_logs/system_output.txt

or extracted from the system.<datetime>.tgz file once you have downloaded it

Inside the system_output.txt file you can find the detail.

Here the /var partition is 65% full.

==========2016-11-30 08:36:09 ... Output of df command:==========

Filesystem 1024-blocks Used Available Capacity Mounted on

/dev/sda3 10154020 2272668 7357232 24% /

/dev/sda2 28571320 17384504 9712052 65% /var

/dev/sda1 505604 33476 446024 7% /boot

tmpfs 6169768 0 6169768 0% /dev/shm

The later Guardium versions have a safety catch/feature that will stop the main processes from collecting any more data when the database or filesystem reaches a certain level .

The default is to stop the processes when the database and /or the filesystem reaches a 90% full level. as per this example v10.1 documentation. You can check the current value of the safety catch via CLI:

CLI> show auto_stop_services_when_full

Note: If the auto_stop_services_when_full is switched off the appliance may go on to fill the system to 100% preventing you from accessing the system at all.

You should never need to or want to set the auto_stop_services_when_full to OFF unless used temporarily in the specific circumstance described in the answer below when you should then use it as described before switching it back to ON once you have resolved the space problem.

Note: You must stop inspection-core before switching the auto_stop off - this will avoid the system filling any further .

So in this case the system will automatically stop inspection-core and other processes when the filesystem or database is 90% full. This includes the GUI interface - so you won't be able to connect to the GUI at that point.

If you attempt to restart stopped services with this command below then the system (and GUI interface) is likely to stop again after 5 minutes for the same reason. restart stopped_services

Note: This command should only be used once you are sure that space has been recovered.

Before the database or the filesystem fills to the "auto stop" level you should receive warnings in the system log (messages file)

Alerts can be made to email you about the space problems before the auto stop is triggered. see Guardium Full database Alert

You can run a must_gather command and look inside the compressed file that gets created to check the latest messages file within

support must_gather system_db_info

>>>Purging Data from the internal database when the GUI is down

If the auto stop has been triggered then this stops services such as the GUI - which stops you from making an emergency purge of data via the "Run Once Now " purge option

To make that emergency purge, do the following:

- Make sure that the inspection-core is switched off on Collectors to stop more data flooding into the appliance

stop inspection-core

- Check that NO database commands are running except the show processlist - (if needed let any running commands finish before the next step)

support show db-processlist running

You should be able to simply restart gui to gain access to the GUI to perform the purge as per What can I do if I see my Guardium Appliance getting full?

If there is a problem where GUI keeps going down every 5 minutes - then you can then consider switching the auto_stop_services_when_full to off TEMPORARILY to allow you to restart gui and purge some data. Just restarting GUI on its own might only stay running for 5 minutes - the main nanny process might stop the services again before enough data is purged or before you've had time to set the purge going.

Note: If the auto_stop_services_when_full is switched off the appliance may go on to fill the system to 100% preventing you from accessing the system at all.

You should never need to or want to set the auto_stop_services_when_full to OFF unless used temporarily in the specific circumstance described here when you should then use it as described before switching it back to ON once you have resolved the space problem.

You must stop inspection-core before switching the auto_stop off - this will avoid the system filling any further)

CLI> store auto_stop_services_when_full off

CLI> show auto_stop_services_when_full [off | restart | gui]

Now you can go to the GUI and then Data Management Archive and set a purge running to clear some data.

Keep checking the database full and the Aggregation Archive log will show when the purge process is finished.

Once it is finished and you have space on the system you should set the auto_stop back on and then restart the stopped services thus

store auto_stop_services_when_full on

restart stopped services

If needed, then start the inspection-core.

Now data should start to be collected again.

If the system has filled up it usually means that too much activity is being recorded.

Parent topic: Managing your Guardium system
Related information:
Advanced Guardium system management and configuration (video)
Preventing and reacting to Guardium database full issues (video)

Guardium catalog

When you archive data from your Guardium system, the Guardium catalog tracks where every archive file is sent, so that it can be retrieved and restored.

About this task

A separate catalog is maintained on each Guardium system, and a new record is added to the catalog whenever you archive data or results. Catalog entries can be transferred between appliances by one of the following methods:

- Aggregation: catalog tables are aggregated, which means that the aggregator has the merged catalog of all of its collectors.
- Export/Import Catalog: these functions can be used to transfer catalog entries between collectors, or to back up a catalog for later restoration.
- Data Restore: each data restore operation contains the data of the archived day, including the catalog of that day. When you restore data, the catalog is also updated.

You can archive a catalog, export a catalog to external storage, or import a catalog that has been stored.

When catalog entries are imported from another system, those entries point to files that have been encrypted by that system. Before you restore or import any such file, the system shared secret of the system that encrypted the file must be available on the importing system. You can use the aggregator backup keys file and aggregator restore keys file CLI commands to copy the shared secrets from one Guardium system to another.

Parent topic: Managing your Guardium system

Archiving a catalog

Procedure

1. Click Manage > Data Management > Catalog Archive.
2. You can display available catalog entries for a range of dates, or add a catalog entry. To display catalog entries:
    a. Enter a date in From to specify the earliest date for which you want data.
    b. Enter a date in To to specify the latest date for which you want data.

c. Optional: For Host Name, enter the name of the Guardium® system from which the archive originated.
d. Click Search.

To add a catalog entry:

a. Click Add.
b. Enter a File Name.
c. Enter a Host Name.
d. Enter the Path for the file.
Note:

For FTP: specify the directory relative to the FTP account home directory

For SCP: Specify the directory as an absolute path.

For TSM: Specify the directory as an absolute path of the original location.

e. Enter a User Name and Password for access to this location.
f. In the Retention field, enter the number of days this entry is to be kept in the catalog (the default is 365).
g. Select an option from the Storage System menu on which the file is contained.
h. Click Save.

3. To remove a catalog entry, open the catalog, select the entry, and click Remove Selected.
4. Click Done when you are finished.

Exporting a catalog

Procedure

1. Click Manage > Data Management > Catalog Export.
2. Select a definition type from the Type dropdown list. TheDefinitions to Export list is populated with definitions of the selected type.
3. Select all of the definitions of this type that you want to export and click Export. Depending on your browser security settings, you might see a message that asks whether you want to save the file or open it.
4. Choose a location to save the exported file.

Importing a catalog

Procedure

1. Click Manage > Data Management > Catalog Import.
2. Click Browse to locate and select the file.
3. Click Upload. You are notified when the operation completes and the definitions that are contained in the file are displayed. Repeat to upload more files.
4. Click Import to import the uploaded files or click Remove without Importing to remove the uploaded files without importing the contents.

How to manage backup and archiving

Establish data retention practices; control activity volume; manage scheduling of data archive and purge, and monthly backups.

Value-added: Best Practices. Protect your data from loss. Make your data readily accessible for auditing purposes.

Use the System Backup function to define a backup operation that can be run on demand or on a scheduled basis.

System backups are used to back up and store all the necessary data and configuration values to restore a server in case of hardware corruption.

There are two archive operations available. Go to Manage > Data Management to select the Data Archive or Results Archive functions:

- *Data Archive* backs up the data that has been captured by the Guardium system, for a given time period. When configuring Data Archive, a purge operation can also be configured. Typically, data is archived at the end of the day on which it is captured, which ensures that in the event of a catastrophe, only the data of that day is lost. The purging of data depends on the application and is highly variable, depending on business and auditing requirements. In most cases data can be kept on the machines for more than six months.
- *Results Archive* backs up audit tasks results (reports, assessment tests, entity audit trail, privacy sets, and classification processes) as well as the view and signoff trails and the accommodated comments from workflow processes. Results sets are purged from the system according to the workflow process definition.

In an aggregation environment, data can be archived from the collector, from the aggregator, or from both locations. Most commonly, the data is archived only once, and the location from where it is archived varies depending on the customer's requirements.

Whenever archiving data, be sure to verify that the operation completes successfully. To do this, log in as admin user, and open the Aggregation/Archive Log by clicking Manage > Reports > Data Management > Aggregation/Archive Log. There should be multiple activities listed for each Archive operation, and the status of each activity should be *Succeeded*.

Data backup

There are three types of recommended data backups:

1. Full/system backups:

   a. Weekly or daily full backups of the Central Manager unit (assuming a standalone Central Manager).

   b. Monthly for aggregators and collectors during a quiet off-hour period

2. Daily archives (think of these archives as incremental backups) for aggregators and collectors. The archive files from the aggregators are much larger than those from the collectors. For example, if an aggregator has ten collectors sending data to it, the starting point for the size of the archive file is equal to those of all ten collector archive files. However, it is much larger than the entire combined collector archives because the aggregator archive files contain extra data that is not sent by the collectors every day.

3. Results archive (this is a specialized subset of the data in the daily and full backups) for aggregators. An alternative to using the Results archive is to save a PDF file from the Audit Process after all users complete the review process.

Data retention

The data backup and archive files serve two purposes: disaster recovery, and historical investigation or auditing.

The following suggestions can be modified based on your corporate data retention policy. For example, some organizations are mandated to keep all backups for 18 months.

For disaster recovery

- Keep a rolling three months full backup from each unit
- Keep a rolling 2-weeks worth of daily archives from the managed collectors

Note: If you have stand-alone collectors, the daily archives should be kept according to your data-retention policy.

For historical investigation or auditing purposes

- All daily archives from the aggregators for the period required by your auditing or corporate data-retention policies.

Storage capacity

The following are only estimates/ranges of backup and archive file sizes for auxiliary storage capacity planning purposes.

The actual sizes vary depending on (1) the volume and granularity of the database activity that is logged on the Guardium collectors, and (2) the retention period of the backup files.

Daily Archives

Collector: approximately 40 MB (privileged user monitoring) to 1 GB (Comprehensive monitoring with full details logged on all traffic).

Aggregator: a rough multiple of the number of collectors, for example, Number of collectors multiplied by 40 MB.

Monthly System Backups – assuming a 50% full database on a Dell R610 or IBM xSeries 3550 M4 (600 GB Disks)

Note: The backup gets roughly a 1:8 compression for the backup file.

Collector: 7 – 10 GB

Aggregator: 16 – 20 GB

Central Manager (no aggregation): << 1 GB

Results Archives

Depends on the number and frequency of audit processes implemented.

Control activity volume

Controlling the volume of activity monitored (on the database server) and logged (on the collector) helps to reduce network utilization; reduce the Guardium system's database disk consumption; and improves the overall capacity and performance of the IBM Security Guardium infrastructure.

This control is primarily achieved in the policy rules, and via the inspection engine configuration.

The following are general guidelines:

- Avoid using port ranges in inspection engines
- Identify all trusted applications and batch programs (these programs generally generate the bulk of the database activity) and if possible, ignore/skip their activity by using the Ignore STAP Session or Skip Logging actions.
- Unless necessary, avoid using the Log Full Details action.
- If possible, use the Selective Audit policy (with the Ignore S-TAP session rules) to minimize network traffic.
- If no extrusion rules are used, for example, result sets are not examined, consider using the Ignore Responses per Session action to eliminate result sets being sent to the Guardium system.
- Establish a process to periodically review and update policy rules, including groups, to accommodate new databases and applications.
- Establish a process to periodically monitor SQL Errors and provide to the DBA and Application development teams for remediation.

Scheduling

The following tables provide a summary of the key schedules to be configured on your Guardium systems. Following the tables is a brief explanation of each process.

Use the Aggregation/Archive log to record the time and status of these processes to assist with adjusting your scheduling times.

The following table lists a schedule of tasks for a Guardium system that is deployed as a collector.

Function	Schedule
Data export (to the Aggregators)	Daily*: 12:30 AM
Data Archive and Purge	Daily: 01:30 AM AND Purge for 15 days

Audit/Workflow jobs	Daily: 03:00 AM (if standalone)
CSV/CEF export to the SCP/FTP Server	Daily: 05:00 AM, if configured in the Audit jobs AND after the audit jobs complete.
Host name Aliasing	Daily: 10:00 PM
Policy Reinstallation	Daily: 11:00 PM
System Backups	Monthly: First Sunday of each Month at 6:00 AM

The following table lists a schedule of tasks for a Guardium system that is deployed as an aggregator.

Function	**Schedule**
Data Archive and Purge	Daily: 4:00 AM AND Purge for 30 days
Data Import (from the Collectors)	Daily 1:15 AM
Audit/Workflow jobs	Daily: 03:30 AM
CSV/CEF export to the SCP/FTP Server	Daily: 05:15 AM, if configured in the Audit jobs AND after the audit jobs complete.
Hostname Aliasing	Daily: 10:00 PM
System Backups	Monthly: First Sunday of each Month at 7:00 AM

Note: Avoid scheduling before 12:15 a.m. to avoid any conflicts with the internal start-of-day processing on each Guardium system.

The daily Data Archive should be set to Archive data older than 1-Day and Ignore data older than 2-days. The first run archives all data in the database and subsequent processes will only archive yesterday's data.

The amount of data kept online is constrained by the size of the database on each Guardium system, so the Purge process helps to manage how much data is kept online, and it works with the Daily Archive. Guardium recommends keeping the minimum amount of data necessary to avoid filling up the database and help with database performance.

For collectors, Guardium recommends 15 days for the collector and 30 days for the aggregator. The actual length, however, depends on how much data is recorded (for example, numbers of S-TAPS, policy rules, and collectors).

Data Export and Import

The previous day's logged activities are exported daily (a push process) from the collectors to their assigned aggregators for aggregated-reporting. This activity is the counterpart to the Data Import on the aggregator.

Note: For convenience, purge can be configured on either the Archive or Export setup screens.

The Data Import process is scheduled only on an aggregator. It imports and processes the previous day's data exported from the collectors.

Monthly Backups

As noted previously, the system backups are full backups and used for disaster recovery. Here is an example of the monthly schedule for the first Sunday of each month starting at 6:00 AM.

Parent topic: Managing your Guardium system

Exporting Results (CSV, CEF, PDF)

CSV, CEF, and PDF files can be created by workflow processes. This function exports all such files that are on the Guardium system.

CEF/CSV files that are created by workflow processes can also be written to syslog. When that happens, those files are not available to be exported by the means described here. Those files should be accessed from syslog by other means.

To export CSV, CEF, and PDF files:

1. Open the Results Export (files) by clicking Manage > Data Management > Results Export (Files).
2. Choose an option from the Protocols radio buttons: SCP, FTP, Amazon S3, or Softlayer.
3. For Host, enter the IP address or DNS host name of the host to receive the files.
4. For Directory, identify the directory in which the data is to be stored. How you specify this directory depends on the protocol you selected.
    - For FTP: Specify the directory relative to the FTP account home directory.
    - For SCP: Specify the directory as an absolute path.
5. Change the Port that can be used to send files over SCP and FTP. The default port for SSH, FTP, and SFTP is 22. The default port for FTP is 21.
6. For Username and Password, enter the credentials for the user logging in to the host machine. This user must have write/execute permissions for the directory that is specified in the Directory field.
7. Use the Scheduling section to define a schedule for running this operation on a regular basis.
8. Click Save to save the configuration. The system attempts to verify the configuration by sending a test data file to that location. If the operation fails, it displays an error message.
9. Click Run Once Now to run the operation once.
10. To verify that files have been exported, check the Aggregation/Archive Log. There should be a Send activity for each CSV or CEF file exported.

To define a default separator, open the Global Profile by clicking Setup > Tools and Views > Global Profile.

To enter a label to be included in all file names, go to Tools > Audit Process Builder.
Note:

The Syslog maximum message size is 4000. CSV results are truncated if they exceed this limit.

Set the encoding to UTF-8 no matter what application is used to read .CSV files. Excel defaults to a different character set and can corrupt the .CSV files. Also, when using Excel, import the .CSV file and select UTF-8 encoding instead of just opening the file and having Excel launch based on file association.

Parent topic: Managing your Guardium system

Export/Import Definitions

If you have multiple systems with identical or similar requirements, and are not using Central Management, you can define the components that you need on one system and export those definitions to other systems, provided those systems are on the same software release level.

You can export one type of definition (reports, for example) at a time. Each element that is exported can cause other referenced definitions to be exported as well. For example, a report is always based on a query, and it can also reference other items, such as IP address groups or time periods. All referenced definitions (except for security roles) are exported along with the report definition. However, only one copy of a definition is exported if that definition is referenced in multiple exported items. An export of policies or queries exports only the groups that are referenced by the exported policies or queries. Previously an export of policies or queries would export all groups.

Export/Import Definitions

Export and Import Definitions are used to save and then restore functional data from a given Guardium system. For example, this function enables you to create a report on one Guardium system and then import that same report onto another server with the same Guardium installed version.
Note: This function is not the same as a full backup of the server. Backups should still be defined and run on a scheduled or manual basis.
Export Definitions - Are used to save and share defined functional values such as Reports/Queries, CAS data, Classifier Data, and so on. The export types are saved onto your PC as a .sql file type.
Import Definitions - This function is used to import the exported definitions onto servers that use the SAME Guardium Software version. For example, if you export definitions from a Guardium V10 system, then you can import those definitions only onto another V10 system.

Note:

- When you export graphical reports, the presentation parameter settings (colors, fonts, titles, and so on) are not exported. When imported, these reports use the default presentation parameter settings for the importing system.
- Subscribed groups are not exported. When you export definitions that reference subscribed groups, the user must ensure that all referenced subscribed groups are installed on the importing appliance (or Central Manager in a federated environment).
- The logs of Export/Import Definitions have the same retention period than the monitored database activity logs.
- Comments are not included in export.
- When audit process definitions of scheduled runs (including schedule time) are exported to another system, the ACTIVE check box in Audit Process Builder is not checked (INACTIVE).
- Schedule Start Time of an audit process defined on one appliance and exported to another (unrelated) appliance - In the case that the original schedule start time is defined, it is retained. If the original schedule start time is not defined (empty), then the imported schedule start time is set to the time it was imported.
- When you export a datasource with an open source driver, the open source driver is not included in the export. The user needs to first upload the open source driver into the new system before importing the datasource definition that was created using it, otherwise the data direct driver will be substituted for the open source driver when it is imported.
- Large complex imports can take a very long time and can exceed the length of the user's session. If this happens and the session times out, the import continues to run in the background until it completes.
- When you export the definition of classifier policies - any custom evaluation classes associated with the policies are not exported with the definition. For the imported policies to work custom evaluation classes must be uploaded separately.
- Exporting/Importing definitions between different languages does not work. For example, trying to export a file from a Guardium® system with a language of Simplified Chinese and import that file to a Guardium system of English will not be successful.

Export to XACML Protocol

Guardium supports export of Policy Rules to a XACML file, and import of XACML files to another Guardium system.

The XACML (eXtensible Access Control Markup Language) is a declarative access control policy language that is implemented in XML and a processing model, describing how to interpret the policies.

The export/Import to standard XACML is used as a bidirectional interface to transfer policies rules between Optim Designer and Guardium.

Optim Designer can convert data values for various purposes and through various means. In the core Optim runtime (z/OS and Distributed) this is achieved through the invocation of data privacy functions that are declared within column maps. In Optim Privacy this is specified, by the user, as the application of a data privacy policy on an attribute, referenced by an entity within a data access plan.

Customers who bought both products, Optim Privacy and Guardium, will be able to Export to XACML the policies and privacy information from one product and Import to the other product.

Note: XACML imports from previous versions of Guardium are not supported.
To export Guardium policies to XACML, follow these steps:

1. Click Manage > Data Management > Export.
2. Select Policy from the Type menu.
3. Check the Export to XACML File check box.
4. Select definitions from the Definitions to Export menu.
5. Click Export.

To Import an XACML file from another Guardium system or Optim Privacy, open the Definitions Import by clicking Manage > Data Management > Import.

Importing Groups

When you import a group that already exists, members may be added, but no members will be deleted.

Importing Aliases

When you import aliases, new aliases may be added, but no aliases will be deleted.

Ownership of Imported Definitions

When a definition is created, the user who creates it is saved as the owner of that definition. The significance of this is that if no security roles are assigned to that definition, only the owner and the admin user have access to it.

When a definition is imported, the owner is always changed to admin.

Roles for Imported Definitions

References to security roles are removed from exported definitions. So any imported definitions will have no roles assigned.

Users for Imported Definitions

A reference to a user in an exported definition causes the user definition to be exported. When definitions are imported, the referenced user definitions are imported only if they do not exist on the importing system. In other words, existing user definitions are never overwritten. This has several implications, as described in Duplicate Role and User Implications.

In addition, imported user definitions are disabled. This means that imported users can receive email notifications that are sent from the importing system, but they are not able to log in to that system, unless and until the administrator enables that account.

Duplicate Group and User Implications

If a group that is referenced by an exported definition exists on the importing system, the definition of that group from the exporting system will not be not imported. This may create some confusion if the group is not used for the same purposes on both systems.

If a user definition exists on the importing system, it may not be for the same person that is defined on the exporting system. For example, assume that on the exporting system the user jdoe with the email address john_doe@aaa.com is a recipient of output from an exported alert. Assume also that on the importing system, the jdoe user already exists for a person with the email address jane_doe@zzz.com. The exported user definition is not imported, and when the imported alert is triggered, email is sent to the jane_doe@zzz,.com address. In either case, when security roles or user definitions are not imported, check the definitions on both systems to see if there are differences. If so, make the appropriate adjustments to those definitions.

Definition Types for Exporting

Table 1. Definition Types for Exporting

Can Be Exported	**Cannot be Exported**
Alert	Custom Alerting Class A check box in the Definitions export screen will Exclude group members. See description in Group line item.
Alias	Custom Assessment Test
Audit Process	Custom Identification Procedure
Auto-discovery Process	
CAS Hosts	
CAS Template Sets	
Classification Process	Access Rule
Classifier Policy	
Custom Class Connection Permission	
Custom Domain	
Custom Table	
Datasource	
Event Type	
Group	A check box in the Definitions export screen will Exclude group members. This check box is visible only for data sets that have groups somewhere in the export hierarchy (for example, export of an alert includes also the query of the alert and the query might include groups in the query conditions). If the export of datasource does not include groups, the checkbox is not visible. When that checkbox is set, the export file includes groups (if groups are linked to the exported definition) but members of the groups are not exported. The checkbox is not set by default, its state is not persistent, and only applies to the current export.
Named Template	
Period (time period)	
Policy (but not an included Baseline)	
Privacy Set	
Query	
Replay	
Report	A check box in the Definitions export screen will Exclude group members. See description in Group line item.
Role	
Security Assessment	
User	
Users database mapping	
Users database permission	
Users Hierarchy	

Export Definitions

1. Open the Definitions Export pane by clicking Manage > Data Management > Export.
2. Select an option from the Type menu. The Definitions to Export menu will be populated with definitions of the selected type.
3. Select all of the definitions of this type to be exported.
   Note: Do not export a Policy definition whose name contains one or more quote characters. That definition can be exported, but it cannot be imported. To export such a definition, make a clone of it, naming the clone without using any quote characters, and export the clone.
4. Click Export. Depending on your browser security settings, you may receive a warning message asking if you want to save the file or to open it using an editor.
5. Save the exported file in an appropriate location.

Import Definitions

1. Open the Definitions Import pane by clicking Manage > Data Management > Import.
2. Click Browse to locate and select the file.
3. Click Upload. You are notified when the operation completes and the definitions contained in the file are displayed. Repeat to upload additional files.
4. Use the Fully synchronize group members checkbox to set the behavior of how to add new group members imported directly or via other datasets such as queries or policies. If not checked, new members that are in the import are added, but members not in the import are not removed. If checked, then group members not in the import are removed. Use the Set as default button next to the checkbox to save the checkbox setting.
5. Click Import this set of Definitions to import a set of definitions, or click Remove this set of Definitions without Importing to remove the uploaded file without importing the definitions.
6. You will be prompted to confirm either action.
   Note: An import operation does not overwrite an existing definition. If you attempt to import a definition with the same name as an existing definition, you are notified that the item was not replaced. If you want to overwrite an existing definition with an imported one, you must delete the existing definition before performing the import operation.

Parent topic: Managing your Guardium system

Distributed Interface

Use this configuration screen to define the Distributed Interface and upload the Protocol Buffer (.proto) file to the DIST_INT database.

From this database, Query Domain metadata is built automatically. After the metadata is built, the user can go to the Custom Domain Builder to modify or clone the data and build custom reports. The distributed interface data uses protocol buffers. Protocol buffers are a flexible, efficient, and automated mechanism for serializing structured data.

For Universal Feed type 3, upload the protocol definition file for configuration of DIST_INT database by clicking Manage > Data Management > Distributed Interface.

Note: Click Maintenance to manage the table engine type and table index. The table engine types for universal feed tables (InnoDB and MyISAM) will appear for all universal feed tables as the data stored on the Guardium internal database is MYSQL-based. See External Data Correlation for further information on InnoDB and MyISAM maintenance.

Configure the Distributed Interface

1. Open the Distributed Interface Finder by clicking Manage > Data Management > Distributed Interface.
2. Click New to create a new Distributed Interface, or select an existing Distributed Interface from the Distributed Interface Finder and click Modify or Delete.
3. For Vendor ID, enter the ID of the vendor (for example, 20000).
4. For Domain name, enter the name of the domain that will be selectable from Custom Domain Builder.
5. Check the Included in aggregation
6. For File Name, click Browse to select a file.
7. Click Apply to save this configuration.
8. Build a custom report in the Custom Domain Builder. Open the Custom Domain Builder by clicking Setup > Tools & Views > Custom Domain Builder.

Example of a .proto file

```
package bim;
option java_package = "com.ibm.infosphere.bim.proto";
option java_outer_classname = "BimEvent";
// NOTE: AssetID and Property_type (== Property name!) are strings.
// For AssetID , it is safest to use a UUID since it provides world-wide unique ID.
// This will be the key to the table of current metrics and property values.
// per each asset, per each property , there will be one value (recent, or min, or max,etc)
message EventTypeID {
    required string eventType                   = 1; //e.g. Schema change
}
message AssetID {
    required string assetId                     = 1;
}
message InfoPropertyID {
    required string assetId                     = 1;
    required string propertyName                = 2;
}
message MetricPropertyID {
    required string assetId                     = 1;
    required string propertyName                = 2;
}
message AssetRelationID {
    // These are asset "native" ids
    required string sourceAssetId               = 1;
    required string targetAssetId               = 2;
}
message RelationPropertyID {
    required string assetRelationId             = 1;
    required string propertyName                = 2;
}
```

```
message Event {
    optional InnerEvent innerEvent              = 1;
}
message InnerEvent {
    // Common for all events
    optional EventTypeID eventTypeId                = 1;
    optional string description                     = 2;
    optional string time                            = 3;
    optional string agentId                         = 4;
    // Event can be for asset info, or metric property
    optional AssetInfoEvent assetInfoEvent          = 5;
    optional MetricPropertyEvent metricPropertyEvent  = 6;
    optional AssetRelationEvent  relationEvent      = 7;
    optional RuleEvent ruleEvent                    = 8;
}
message AssetInfoEvent {
    optional AssetID unique_key__               = 1;
    optional string assetType                   = 2;
    optional string assetName                   = 3;
    optional string gdm_server_ip               = 4;
    optional string gdm_service_name            = 5;
    repeated InfoProperty property              = 6;
}
message InfoProperty {
    optional InfoPropertyID unique_key__        = 1;
    optional string value                       = 2;
}
message MetricPropertyEvent {
    optional AssetID assetId                    = 1;
    repeated MetricProperty property            = 2;
}
message MetricProperty {
    optional MetricPropertyID unique_key__      = 1;
    optional AssetID assetId                    = 2;
    optional string stringValue                 = 3;
    optional double doubleValue                 = 4;

    enum Data_type {
        DOUBLE                                      = 1;
        LONG                                        = 2;
        INT                                         = 3;
        FLOAT                                       = 4;
        DATE                                        = 5;
        BOOLEAN                                     = 6; // convention is to store it
as 0 and 1 in the double_value
        STRING                                      = 7; // stored in string_value
    }
        optional Data_type dataType                 = 5;
    optional string unit                        = 6; // unit for the value
}
message AssetRelationEvent {
    optional AssetRelationID unique_key__       = 1;
    required string relationshipType            = 2;
    repeated RelationshipProperty property      = 3;
    optional bool deleted                       = 4;
}
message RelationshipProperty {
    optional RelationPropertyID unique_key__    = 1;
    optional string value                       = 2;
}
message RuleEvent {
    optional string ruleName                    = 1;
    optional bool enabled                       = 2;
}
// --- Metadata --- All unique identifier must be defined here
message Identifier {
    optional InfoPropertyID infoPropertyId              = 1;
    optional MetricPropertyID metricPropertyId          = 2;
    optional AssetID assetId                            = 3;
    optional AssetRelationID assetRelationId            = 4;
    optional RelationPropertyID relationshipPropertyId  = 5;
}
```

Parent topic: Managing your Guardium system

Manage Custom Classes

Upload and maintain custom classes used in alerts or evaluations. Manage custom classes by clicking Setup > Custom Classes.

After you compile a class, it must be uploaded to the Guardium® system.

Uploading a Custom Class

1. You can upload a custom class for alerts or evaluations. Upload a custom class by clicking Setup > Custom Classes, then either Alerts > Upload or Evaluations > Upload
2. Enter a description for the custom class.
3. Click Browse to locate and select the class file that you want to upload.
4. Click Apply.

Updating a Custom Class

1. Select Setup > Custom Classes, then either Alerts > Update or Evaluations > Update.
2. Select the description of the class to be updated.
3. Click Browse to locate and select the class file that is to be used for the update.
4. Click Apply.

Deleting a Custom Class

1. Select Setup, then either Alerts > Delete or Evaluations > Delete
2. Select the description of the class to be deleted.
   Note: You cannot remove a class that is in use by some other component (the installed policy, for example).
3. Click Delete.

Parent topic: Managing your Guardium system

SSH Public Keys

Use this information to create, modify or remove an SSH Public Key.

1. Click Manage > Activity Monitoring > SSH Public Key Management, and do one of the following:
   - To create a key, click New.
   - To generate a key, click Generate.
   - To modify a key, select it from the list and click Modify.
   - To remove a key, select it from the list and click Remove.
2. Fill in the appropriate information on the SSH Public Key Edit panel and click Apply to save.

Parent topic: Managing your Guardium system

How to install an appliance certificate to avoid a browser SSL certificate challenge

Use IBM Security Guardium CLI commands to create a certificate signing request (CSR), and to install server, certificate authority (CA), or trusted path certificates on your Guardium® system.

About this task

Eliminate the Certificate Error warning screens saying:

```
There is a problem with this website's security certificate.  The security certificate presented by this website was issued  for a different website's address. Security certificate problems may indicate an attempt to fool  you or intercept any data you send to the server.
```

See Certificate CLI Commands for more information on all the certificate commands.

Note: One prerequisite is that you must provide a public certificate from a CA you will be using to sign your certificates (Verisign, Thwate, Geotrust, GoDaddy, Comodo, within-your-company, etc).
Note: Guardium does not provide CA services and will not ship systems with different certificates than the one installed by default. A customer that wants their own certificate will need to contact a third-party CA.
Note: If the certificate is not self-signed, you MUST obtain also the public certificate for each signer up to the lowest level (for example, the certificate that is self-signed). You can use the command, openssl x509 -in t.pem -text -noout, to show contents of a x509 certificate.

Procedure

1. Have available the public certificate from the CA (Certificate Authority) you will be using to sign your certificates (from Verisign, Thwate, Geotrust, GoDaddy, Comodo, in-house, etc).
2. Log into the CLI on the individual Guardium system you wish to have a signed certificate on.

   Before executing the command, obtain the appropriate certificate (in PEM format, not binary format) from your CA, and copy the certificate, including the Begin and End lines, to your clipboard.

3. Enter the command, store certificate keystore. The following prompt will be displayed:

   ```
   What is a one-word alias we can use to uniquely identify this certificate?
   ```

   Enter a one-word name for the certificate and press Enter.

   The following instructions will be displayed:

   ```
   Please paste your CA certificate, in PEM format. Include the BEGIN and END lines, and then press CTRL-D.
   ```

   Paste the PEM-format certificate to the command line, then press CRTL-D. You will be informed of the success or failure of the store operation.

   Now the CA you will sign with is set as trusted on the Guardium system.

4. Next, from the CLI command prompt, type: `create csr gui`.

   Fill in the requested information. If the CN (common name) of the certificate is not set to the hostname.domain of the box, certificate errors from the browser will result.

   There are no parameters, but you will be prompted to supply the organizational unit (OU), country code (C), and so forth. Be sure to enter this information correctly. The last prompt is as follows:

   ```
   What encryption algorithm should be used (1=DSA or 2=RSA)?
   ```

   DSA, or the Digital Signature Algorithm, is a federal information processing standard (FIPS) for digital signatures. RSA is a public-key cryptosystem that involves key generation, encryption, and decryption. The default encryption algorithm is RSA.

After you respond to the last prompt, the system displays a description of the request, followed by the request itself, and followed finally by additional instructions. For example:

```
This is the generated CSR: Certificate Request: Data: Version: 0 (0x0) Subject: C=US, ST=MA, L=Littleton, O=XYZCorp,
OU=Accounting, CN=g2.xyz.com -----BEGIN NEW CERTIFICATE REQUEST-----
MIICWjCCAhcCAQAwVDELMAkGA1UEBhMCVVMxEDAOBgNVBAgTB1dhbHRoYW0xETAPBgNVBAoTCEd1
YXJkaXVtMRUwEwYDVQQLEwxndWFyZGl1bS5jb20xCTAHBgNVBAMTADCCAbgwggEsBgcqhkjOOAQB
MIIBHwKBgQD9f1OBHXUSKVLfSpwu7OTn9hG3UjzvRADDHj+AtlEmaUVdQCJR+1k9jVj6v8X1ujD2
y5tVbNeBO4AdNG/yZmC3a5lQpaSfn+gEexAiwk+7qdf+t8Yb+DtX58aophUPBPuD9tPFHsMCNVQT
WhaRMvZ1864rYdcq7/IiAxmd0UgBxwIVAJdgUI8VIwvMspK5gqLrhAvwWBz1AoGBAPfhoIXWmz3e
y7yrXDa4V7l5lK+7+jrqgvlXTAs9B4JnUVlXjrrUWU/mcQcQgYC0SRZxI+hMKBYTt88JMozIpuE8
FnqLVHyNKOCjrh4rs6Z1kW6jfwv6ITVi8ftiegEkO8yk8b6oUZCJqIPf4VrlnwaSi2ZegHtVJWQB
TDv+z0kqA4GFAAKBgQCONsEB4g4/limbHkuZ5YnLn9CGM3a2evEnqjXZts4itxeTYwPQvdkjdSmQ
kaQlBxmNUsZOJZrq5nC5Cg3X9spa+BzFr+PgR/5zka17nHcxKXCjVjLk451L67KllXv61TUfv/bU
PKmiaGKDttsP2ktG4dBFXQdICJEGo0aNFCYn6qAAMAsGByqGSM44BAMFAAMwADAtAhUAhHTY5z9X NiBAuyAC9PS4GzleYakCFF2kcfxfjX1BFy5I228XWMAU0N95
-----END NEW CERTIFICATE REQUEST-----
```

Note: For Common Name, use hostname in FQDN format (fully qualified domain name). But if you connect to the GUI normally using the short hostname (for example, system1) instead of FDQN (system1.us.ibm.com), you will get a certificate error "Address Mismatch" you will either have to change the CN=system1 or connect with https://system1.us.ibm.com:8443/sqlguard to make use of the certificate.
Note: Country Code must be 2 letters.
Note: Keysize can be 1024 or 2048.

5. Copy and paste the generated hash from ---Begin CSR---- to ---End CSR--- into a text document. Now send this off to your CA for them to return the signed key.

   Before continuing, check the Subject line to verify that you have entered your company information correctly. From this point forward, use whatever procedure you would normally use to obtain a server certificate from your CA.

   Note: • When submitting the request to your CA make sure you request the certificate to be in PKCS#7 PEM format.
6. The CA signs the CSR and sends you back your signed key.
7. Now, go back to the CLI prompt on the Guardium system and have the signed key from the CA handy. Type the following: store certificate gui.

   Enter the command exactly as shown. You will receive the following information and prompt:

   Please paste your new server certificate, in PEM format.

   Include the BEGIN and END lines, and then press CTRL-D.

   Paste the PEM-format certificate to the command line, then press CRTL-D. You will be informed of the success or failure of the store operation.

```
-----BEGIN CERTIFICATE----- MIIDvTCCAqegAwIBAgIBATALBgkqhkiG9w0BAQUwcjELMAkGA1UEBhMCVVMxEzAR
BgNVBAgTCldhc2hpbmd0b24xDzANBgNVBAcTBllha2ltYTEMMAoGA1UEChMDSUJN
MRUwEwYDVQQLEwxHdWFyZGl1bURlbW8xGDAWBgNVBAMTD0d1YXJkaXVtRGVtb19D
QTAeFw0xMTAzMjUxNTM1MTRaFw02OTEyMzEyMzU5NTlaMHIxCzAJBgNVBAYTAlVT
MRMwEQYDVQQIEwpXYXNoaW5ndG9uMQ8wDQYDVQQHEwZZYWtpbWExDDAKBgNVBAoT
A0lCTTEVMBMGA1UECxMMR3VhcmRpdW1EZW1vMRgwFgYDVQQDEw9HdWFyZGl1bURl
bW9fQ0EwggEgMAsGCSqGSIb3DQEBAQOCAQ8AMIIBCgKCAQEAw08aZVJNdnC69LR6
YtvHO+KbsqA89vCezLw7xmEa7F6+io0NofIFX7b7FvSkxzx1SO4eStaQSTDBxOGk
mqK2vk3VeJk9+lItofUuQXl1CZ1R4wQPMRfaWgELt+t94XB3Y1zmI68vwfr1fB32
u3Yjpt4aq27sTMrjEqZIyDqQ7hQ1tpMtoBUqNi54wN+OJjhtpNYDAkCHs+3NPqXE
6HeL7W5X6PJ+YCyyZiXeqQ+T8qdpH0KDVJGJLGX1YC+0WnQz/S2kaaRfxe6Nhe6q
YeYaD09tlWkVrZQm8a76SDULjzjrQ4wNoTJu17JQk7Uc835RE/bF5WMsaN5HGs3s
9zP3uwIDAQABo2QwYjAPBgNVHRMBAf8EBTADAQH/MA8GA1UdDwEB/wQFAwMHBgAw
HQYDVR0OBBYEFINmKThm8tA+Z8cyFC7MOZ7v398SMB8GA1UdIwQYMBaAFINmKThm
8tA+Z8cyFC7MOZ7v398SMAsGCSqGSIb3DQEBBQOCAQEAcXttcJwy1aowq9wtJksK
q6n6laEFR38i+pLJ6kArjoJGP5WxFdaYcDQr5cAw2Q6YFZvQGaYAqiSS6ezF20PT
3BrrP+Mg/SK8jgPvM0ekodmpr385iQqSDneTTwPPrIaQBrrtb2510wHSEyiVcRRI
4vn3ktVahjiSMD92bfmZilPYQ51pD0jFgGFFRvekulPWGWv7iuCT+alCM99/76xR
uWrRc7cxypfxK1yymptizZVrxLHS47VVoXzmZ7yO3kfhhdZbBmoXg1MDM82rVdnp
WVQdlSasn8deHaVG//RsCrWx4PxN8TVIDGbfh0nWRYU4zPORvWst3fa+h9B2W55z /A== -----END CERTIFICATE-----
```

8. For the final step, restart the UI using the command restart gui.

   You have now successfully installed one certificate for one Guardium unit. Repeat the steps for every Guardium system on-site.

Parent topic: Managing your Guardium system

Self Monitoring

The Guardium solution monitors itself to minimize disruptions and correct problems automatically whenever possible.

Guardium uses a three-pronged approach to ensuring that it is available, functioning properly, has not been tampered with, and alerts users of problems:

- Reports - Whether textual or graphical, reports are at the core of the Guardium® solution. By using Guardium's Query Builder and Report Builder, a user can effectively report on any of the self-monitoring data collected through associated domains and entities. Many of the predefined reports can be enhanced through more detailed effort to provide higher levels of granularity. A specific query builder has been created (VA Test Tracking) to report on tests that are available for security assessments.
- Alerts - In addition to building reports, a user can define an alert against those reports through defined thresholds--indicating an exception or policy rule violation. These alerts can either be real-time or determined through historical analysis. These alerts can then trigger notification to users through SMTP, SNMP, syslog, or a custom Java™ class.
- Self-Monitoring Utility - Guardium has implemented an internal self-monitoring demon (always running) service utility on collectors and aggregators that wakes up every 5 minutes and does system scan, checking components for optimal configuration, operational effectiveness, and repairs when necessary. For example if the utility finds the Web Server down, it will first validate a complete shutdown of the service, restart the service, and then alerts an administrative user.

Components Monitored

Table 1. Components monitored

Components	How to access

Components	How to access
System Disk space(%full)	Manage > System View > System Monitor Alert: You can use the Queries and Correlation Alerts, utilizing the Sniffer Buffer domain and Sniffer Buffer Usage entity to create alerts
CPU Load Uptime and Reboots Memory Usage Monitoring Engine (sniffer) - Status: up/down/stuck/overloaded CPU Usage Memory Usage Overload and delays (queues)	Reports > Guardium Operational Reports > Buff Usage Monitor Alert: You can use the Queries and Correlation Alerts, utilizing the Sniffer Buffer domain and Sniffer Buffer Usage entity to create alerts
Failed Logins	Manage > System View > System Monitor. Alert: You can use the Queries and Correlation Alerts, utilizing the Guardium Login domain and Guardium Users Login entity to create alerts
Lost requests	Manage > Reports > Activity Monitoring > Dropped Requests Alert: You can use the Queries and Correlation Alerts, utilizing the Exceptions domain and Exceptions entity to create alerts
Change in data patterns	Reports >Real-time Operational Reports > Values Changed Alert: See Viewing an Audit Process Definition for alert: Data Source Changes - alert on any data source changes
Packets rates Request rates Ignored data	Reports >Guardium Operational Reports > Buffer Usage Monitor Alert: You can use the Queries and Correlation Alerts, utilizing the Sniffer Buffer domain and Sniffer Buffer Usage entity to create alerts
Scheduled Jobs Exceptions	Reports >Guardium Operational Reports > Scheduled Job Exceptions, or See Predefined admin Reports: Alert: You can use the Queries and Correlation Alerts, utilizing the Exceptions domain and Exception Type entity to create alerts.
Audit processes status	Reports >Guardium Operational Reports > Number of Active Audit Processes, or See Predefined admin Reports. Alert: You can use the Queries and Correlation Alerts, utilizing the Audit Process domain and Audit Process entity to create alerts
Inspection Engine Changes	Reports >Activity Monitoring > S-TAP Configuration Change History Alert: See Viewing an Audit Process Definition for alert: Inspection Engines and S-TAP - alert on any activity related to inspection engine and S-TAP configuration
Guardium Users Activity - Login/logout	Reports >Guardium Operational Reports > Logins to Guardium, or See Predefined admin Reports Alert: You can use the Queries and Correlation Alerts, utilizing the Guardium Login domain and SQL Guard Login entity to create alerts
Failed Logins	Reports >Guardium Operational Reports > Logins to Guardium, or See Predefined admin Reports Alert: See Viewing an Audit Process Definition for alert: Failed Logins To Guardium - alert if have more than 5 failed logins in the last 11 minutes, or Select Tools > Report Building > drop-down Report Title: Guardium Logins, See Reports for additional information
User Activity Audit Trail	Reports >Guardium Operational Reports > User Activity Audit Trail, or See Predefined admin Reports Alert: You can use the Queries and Correlation Alerts, utilizing the Guardium Activity domain and SQL Guard User Activity Audit entity to create alerts Note: User activity includes those instances where a user changes to the root shell -- providing a log of their root activity.
Creation/Deletion of Users/Roles	Reports >Guardium Operational Reports > User Activity Audit Trail, or See Predefined admin Reports Alert: See Viewing an Audit Process Definition for alert: Guardium - Add/Remove Users - alert on any Addition or Removal of Guardium User
Permissions monitoring	Reports >Guardium Operational Reports > Guardium Users, Guardium Roles, or Guardium Applications Alert: You can use the Queries and Correlation Alerts, utilizing the Application domain and Application Data entity to create alerts

Components	How to access
S-TAP® Info (Central Manager)	Report: See S-TAP Reports. On a Central Manager, an additional report, S-TAP Info, is available. This report monitors S-TAPs of the entire environment. Upload this data using the Custom Table Builder. This report is the result of uploading data using remote sources on a Central Manager and using that data to see a consolidated view of S-TAPs. S-TAP info is a predefined custom domain which contains the S-TAP Info entity and is not modifiable like the entitlement domain.

Guardium nanny process

The Guardium nanny is an internal process that monitors the system's critical resources and then alert when potential problems are emerging. Nanny alerts go to syslog, can be forwarded and sent as emails to the administrator, and in some cases take remedial actions.

The nanny watches key components and critical resources within the Guardium system—guaranteeing their availability and reliability. These resources and components include:

- Web service monitoring - service port (default 8443) not responding or tomcat service is not up
  - syslog message
  - mail admin
  - will issue restarts of the web service
- Inspection Engine activity - snif overloaded, not responding, or failure
  - syslog message
  - mail admin
  - mail guardium support (optional)
  - will try and fix by restarting the snif under certain conditions
  - will try and respawn snif if process dies
- Diskspace utilization - alerts when > 75% on the critical partitions
  - syslog message
  - alert admin
  - will perform preventive action by cleaning temporary files when over 95%
- Failed login (ssh) to the appliance - checks for ssh daemon's messages and alerts on failed ssh login attempts
  - mail admin (it's already in syslog)
- Monitor internal database (TURBINE) - verify service is up, status, and capacity utilization monitoring
  - syslog message
  - mail admin
  - restart service
- File System utilization - every five minutes, Nanny.pl checks file system at /var, warning alert when > 75% in the /var directory, critical alert and services stopped when >90% in /var directory
  - syslog message
  - alert admin
  - Admin clean-up required, using CLI commands: show filesystem usage, clear filesystem dir, and restart stopped_services

- How to monitor the Guardium system via alerts
  Monitor the capacity, performance and availability of the IBM Security Guardium system using a combination of built-in and custom correlation alerts.
- Monitoring with SNMP
  There is an SNMP agent installed on Guardium systems, and read-only access is provided using the SNMP community name of guardiumsnmp.
- Running Query Monitor
  The Running Query Monitor displays the status of active user queries, and enables you to set a timeout value for all Report/Monitor queries.

Parent topic: Managing your Guardium system

How to monitor the Guardium system via alerts

Monitor the capacity, performance and availability of the IBM Security Guardium system using a combination of built-in and custom correlation alerts.

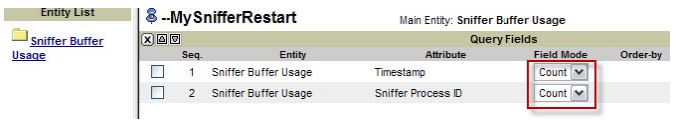
Alert users to issues that may affect system performance, such as: CPU utilization, database disk space, inactive STAPs, and no traffic situations.

The Sniffer Buffer Usage domain is the basis for most of the following alerts.

Sniffer Restart Alert

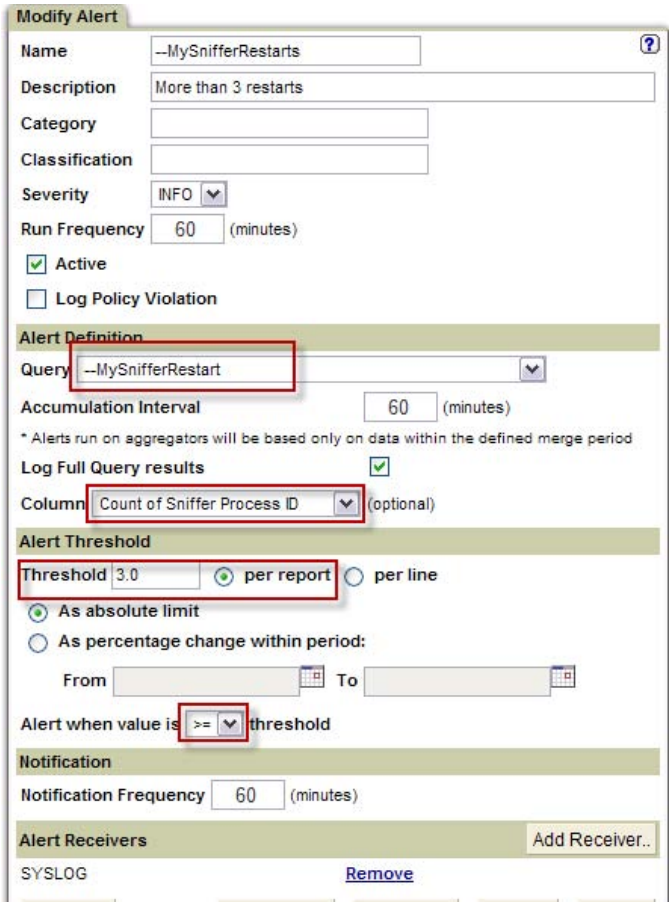
An alert will be sent if the sniffer on a collector has restarted at least three times an hour.

Create a Query using the Sniffer Buffer Usage domain with the columns and Fields as shown – there are no conditions.



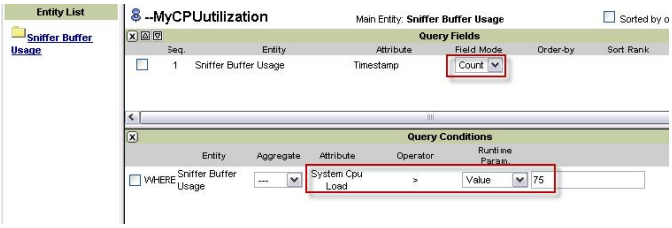
This is an example of the output from the Query:

Define the alert.



High CPU Utilization

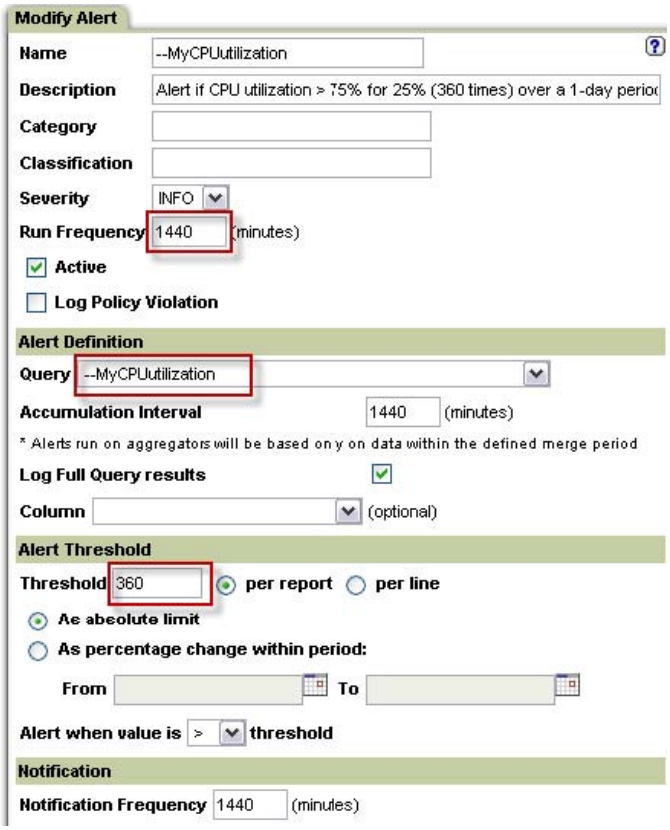
Using the Enterprise Buffer Usage domain, create an alert to monitor system CPU utilization. Here is an example of a query for CPU utilization which exceeds 75%.



The alert will then be setup to fire only if the utilization is exceeded for 360 times in a 24-hour period, for example, 25% of the day.

Note: The Sniffer buffer usage domain is populated once a minute, so there are 1440 entries in a 24-hour period.

To define the alert, click Protect > Database Intrusion Detectioin > Alert Builder..

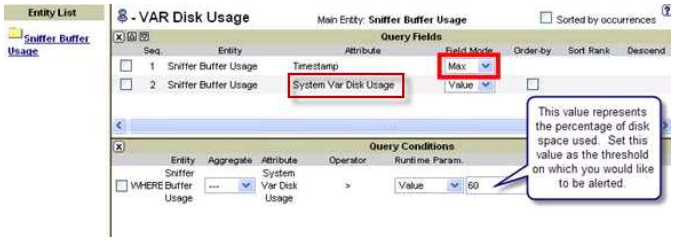


Database Disk Space Alerts

Use the Query Builder to Build two reports (they are similar) and two alerts – one for the collector and the other for the aggregator since the database size is fixed on the collector but dynamic on the aggregator (up to the size of the var partition).

Aggregator Disk Space Alert

1. Create a new Query with Sniffer Buffer Usage as the main entity.
2. Configure the fields and conditions.

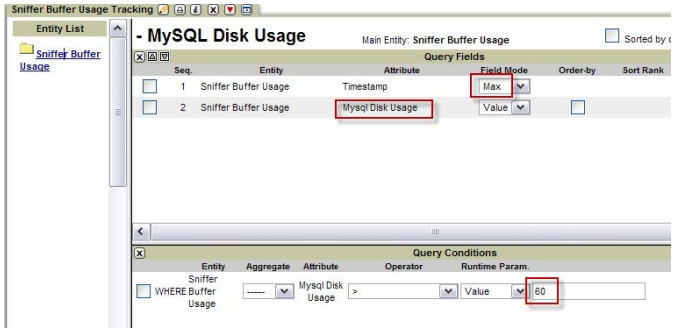


1. Setup a new alert in the Alert Builder. Open the Alert Builder by clicking Protect > Database Intrusion Detection > Alert Builder.

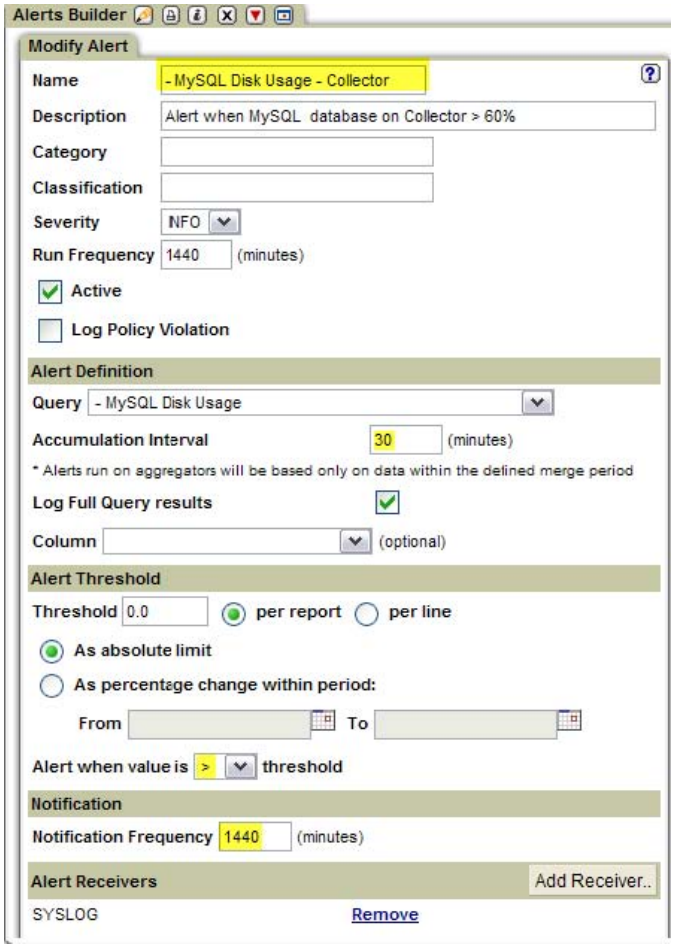
Collector Disk Space Alert

Repeat the previous steps to create an alert for monitoring disk space on the collectors.

1. Create a Query.



1. Use the Alert Builder to set up a new alert.



Data Import, Merge (Aggregation), Archive or Backup Failure Alerts

This is a built-in alert and must be activated and scheduled.

Inactive S-TAP Alerts

This is a built-in alert and needs to be activated and scheduled.

For STAPs configured with a primary and secondary collector, if the STAP cannot communicate with the primary (for example, due to network issues), it will failover to the secondary. Unless the former-primary collector is able to ping the STAP, it will then generate an inactive STAP alert.

Note: STAPs in a cluster configuration can generate false alerts if misconfigured.

No Traffic Alerts

This is a built-in alert and needs to be activated and scheduled.

This alert checks for traffic from an active inspection engine, from which the collector previously received traffic, AND for traffic that is processed by the policy. If both conditions are not satisfied within 48 hours, an alert will be generated.

Application Monitoring via Ad-hoc Reports

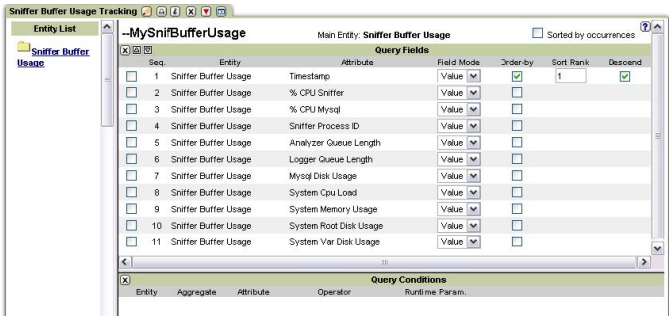
As a general rule, avoid invoking ad-hoc queries/reports on the collector with time spans > 1 hour. Large/long running queries should be invoked on the aggregator and are best scheduled using the Audit Process.

The following two reports should be scheduled, from the Central Manager, to run weekly on each collector.

Note: These reports also need to be scheduled individually on EACH aggregator.

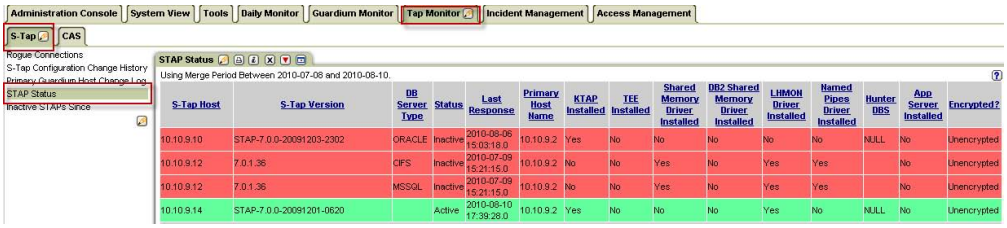
Custom Sniffer Buffer Usage Report

Using the Sniffer Buffer Usage domain, create a report with the following fields:



STAP Status Report

This report displays the key parameters for ALL STAPs and inspection engines for a given collector. The report cannot be modified but can be run on each collector, or from the Central Manager pointing to each collector in turn, or scheduled via the Audit process on each collector.



Parent topic: Self Monitoring

Monitoring with SNMP

There is an SNMP agent installed on Guardium® systems, and read-only access is provided using the SNMP community name of guardiumsnmp.

When querying, a value of -1 (minus one) indicates a NULL in the database. The table at the end of this section lists the available SNMP OIDs.

SNMP Examples

From a Unix session, you can display SQL Guard SNMP information using the snmpget or snmpwalk commands. (Use snmpget -h or snmpwalk -h to display command syntax.) Various UI-based software packages are available for displaying SNMP information. Those alternatives are not described here.

Table 1. SNMP Examples

SNMP Examples
Disk space used and available:
> snmpget -v 2c -c guardiumsnmp a1.corp.com UCD-SNMP-MIB::dskAvail.1
UCD-SNMP-MIB::dskAvail.1 = INTEGER: 1043856
> snmpget -v 2c -c guardiumsnmp a1.corp.com UCD-SNMP-MIB::dskUsed.1
UCD-SNMP-MIB::dskUsed.1 = INTEGER: 914856
To list total memory and used memory:
> snmpget -v 2c -c guardiumsnmp a1.corp.com
HOST-RESOURCES-MIB::hrStorageSize.101
HOST-RESOURCES-MIB::hrStorageSize.101 = INTEGER: 2067352
> snmpget -v 2c -c guardiumsnmp a1.corp.com HOST-RESOURCES-MIB::hrStorageUsed.101
HOST-RESOURCES-MIB::hrStorageUsed.101 = INTEGER: 1017548
To list the available memory:
> snmpwalk -v 2c -c guardiumsnmp a1.corp.com memAvailReal
UCD-SNMP-MIB::memAvailReal.0 = INTEGER: 1049564
To list values relating to cpu usage:
> snmpwalk -v 2c -c guardiumsnmp a1.corp.com ssCpuRawUser
UCD-SNMP-MIB::ssCpuRawUser.0 = Counter32: 89240
> snmpwalk -v 2c -c guardiumsnmp a1.corp.com ssCpuRawSystem
UCD-SNMP-MIB::ssCpuRawSystem.0 = Counter32: 195310
> snmpwalk -v 2c -c guardiumsnmp a1.corp.com ssCpuRawNice

SNMP Examples
UCD-SNMP-MIB::ssCpuRawNice.0 = Counter32: 11
Note: Adding the RawUser, RawSystem, and RawNice numbers provides a good approximation of total CPU usage.
> snmpwalk -v 2c -c guardiumsnmp a1.corp.com ssCpuRawIdle
UCD-SNMP-MIB::ssCpuRawIdle.0 = Counter32: 26734332

Guardium SNMP OID

Table 2. Guardium SNMP OID

SNMP OID	Description
.1.3.6.1.4.1.2021.9.1.7.1 UCD-SNMP-MIB::dskAvail.1	Disk space available in / directory
.1.3.6.1.4.1.2021.9.1.7.2 UCD-SNMP-MIB::dskAvail.2	Disk space available in /var directory
.1.3.6.1.4.1.2021.9.1.8.1 UCD-SNMP-MIB::dskUsed.1	Disk space used in / directory
.1.3.6.1.4.1.2021.9.1.8.2 UCD-SNMP-MIB::dskUsed.2	Disk space used in /var directory
.1.3.6.1.2.1.25.2.3.1.5.1 HOST-RESOURCES-MIB::hrStorageSize.1	Total memory available
.1.3.6.1.2.1.25.2.3.1.6.1 HOST-RESOURCES-MIB::hrStorageUsed.1	Memory in use
.1.3.6.1.4.1.2021.8.1.101.1 UCD-SNMP-MIB::extOutput.1	Open monitored session count
.1.3.6.1.4.1.2021.8.1.101.2 UCD-SNMP-MIB::extOutput.2	Requests logged by the current sniffer process (set to zero for each restart)
.1.3.6.1.4.1.2021.8.1.101.3 UCD-SNMP-MIB::extOutput.3	Last session timestamp
.1.3.6.1.4.1.2021.8.1.101.4 UCD-SNMP-MIB::extOutput.4	Last construct timestamp
.1.3.6.1.4.1.2021.8.1.101.5 UCD-SNMP-MIB::extOutput.5	Memory used by the sniffer process
.1.3.6.1.4.1.2021.8.1.101.7 UCD-SNMP-MIB::extOutput.7	Packets in on ETH1/ out on ETH2; usually only one number (inbound) when a SPAN port or TAP is used
.1.3.6.1.4.1.2021.8.1.101.8 UCD-SNMP-MIB::extOutput.8	Packets in on ETH3/ out on ETH4; usually only one number (inbound) when a SPAN port or TAP is used
.1.3.6.1.4.1.2021.8.1.101.9 UCD-SNMP-MIB::extOutput.9	Packets in on ETH5/ out on ETH6; usually only one number (inbound) when a SPAN port or TAP is used

Other MIBs accessible in the machine are: SNMPv2-MIB, IF-MIB, RFC1213-MIB, and HOST-RESOURCES-MIB.

Parent topic: Self Monitoring

Running Query Monitor

The Running Query Monitor displays the status of active user queries, and enables you to set a timeout value for all Report/Monitor queries.

Open the Running Query Monitor by clicking Manage > Activity Monitoring > Running Query Monitor.

From the Running Query Monitor, you can:

- Set the query timeout for all reports and monitors that are running in a portlet. Other query processes, such as policy simulations, audit processes, and internal processes are not affected by this timeout value. The default is 180 seconds (3 minutes).
- Kill any currently running user query. Some queries that are listed in this panel–audit processes, for example–can exceed the query timeout specified. That is expected, because the Report/Monitor query timeout applies only to reports and monitors running in a portlet.

We do not recommend setting the Query Timeout higher than the default setting (180 seconds) for an extended time. If you set this limit higher, it increases the chances of overloading the system with ad-hoc reporting activity.

To change the timeout setting, type a number of seconds in the Report/Monitor Query Timeout (seconds), and click Update. You will be informed when the update finishes.

Parent topic: Self Monitoring

Groups

Using groups makes it easy to create and manage classifier, policy and query definitions, as well as roll out updates to your S-TAP's and GIM clients. Rather than having to repeatedly define a group of data objects for an access policy, put the objects into a group to easily manage them.

- Groups Overview
  Group together similar data objects and use them in creating query, policy, and classification definitions. Use one of the many predefined groups, or create your own group using the Group Builder.
- Using the group builder
  The group builder provides at-a-glance information about group membership and use and several convenient methods for populating groups.
- Using the group builder (legacy)
- Using groups in queries and policies
  Short overview of conditional operators for queries and where to use groups in policies.
- Example: Using groups to create rules and policies
  Use groups to quickly specify rule conditions in a policy.
- Predefined Groups
  This section details the predefined groups in Guardium®.

Parent topic: Managing your Guardium system

Groups Overview

Group together similar data objects and use them in creating query, policy, and classification definitions. Use one of the many predefined groups, or create your own group using the Group Builder.

There are many places where groups are practical to use. By grouping together similar data objects, you can use the whole set of objects in policies, classifications, queries, and reports, rather than having to select multiple data objects individually.

If you need to make changes to a query or policy, rather than applying those changes to each individual object, you can apply those changes to the group.

S-TAPs and GIM also use groups to make it easier to roll out updates across managed servers.

Group Builder

The Group Builder allows you to create a new group or modify an existing group from the user interface.

Open the Group Builder by clicking Setup > Group Builder.

The Group Filter screen allows you to easily sort through groups based on application type, group type, description or category.

Types of groups

The field Group Type refers to the type of data that will be grouped together. For example, *Server IP* expects data arranged as an IP address and *Users* expects to see names of users on the application.

Tuple groups

A tuple group allows multiple attributes to be combined together to form a single composite group member. Three of an ordered set of values are called 3-tuple. An n-tuple is one with an n-set of value attributes. This simplifies the specification of conditions for reporting and policy rules.

Examples of tuple groups are:

- Tuple groups - Object/Command, Object/Field, Client IP/DB User, Server IP/DB User
- 3-tuple groups - Client IP/Source Program/DB User, DB User/Object/Privilege
- 5-tuple group - Client IP/Source Program/DB User/Server IP/Service Instance
- 7-tuple group - Client IP/Src App/DB User/Server IP/Svc. Name/OS User/DB Name

Tuple supports the use of one slash and a wildcard character (%). It does not support the use of a double slash (//).
Note: Tuple query - If the user tries to use LIKE GROUP condition and the data has '\' in it, the result may not be correct. The user should use IN GROUP instead, if data has '\' in it.

Predefined groups

There are a number of predefined groups that are included with Guardium. Use the Group Filter and Group Type menu to browse the list of groups and find the one that best suits your needs.

Group types *DB User/DB Password* are by default only available to admin users. Modify the group roles if you want to change this default setting.

Overlapping group memberships

Groups members can be in more than one group.

For example, two predefined groups, *Create Commands* and *DDL Commands*, both have a member named CREATE TABLE. If you are querying for either of these groups, all of the CREATE TABLE members from the reporting period will be counted in that group.

In some cases you may want to define a set of groups so that each member belongs to only one group. For example, suppose that for reporting purposes you need to group database users into one of two groups: employees or consultants. You would define each of those groups with the same sub-group type (Employee-Status, for

example). When sub-groups are used, the system will not allow you to add a member to a sub-group if that member has already been added to another group with the same sub-group type.

Wildcards in members

Group members can include wildcard (%) characters for when the group is used in a query condition or policy rule.

Table 1. Wildcards in members

Member	Matches	Does NOT Match
aaa%	aaa aaazzz	zzzaaa aaz
%bbb	bbb,zzbbb	bb bbbzzz
%ccc%	ccc ccczz zzzccczzz	cc zzzcczzz

Managed Unit Groups

There is a distinction between managed unit groups and the groups created through the group builder used for grouping elements to simplify creating and managing policies and to clarify the presentation of reports. For more information about managed unit groups, see Creating managed unit groups.

Parent topic: Groups

Using the group builder

The group builder provides at-a-glance information about group membership and use and several convenient methods for populating groups.

Use the group builder to create and populate groups from a variety of sources including CSV files, external datasources, and existing groupd. In addition, the builder provides at-a-glance information about group membership and where groups are used in security policies, classifier policies, queries, and reports.

Tip:

Guardium V10.1.4 introduces the new group builder interface described in this information. The new group builder is accessible at Setup > Tools and Views > Group Builder.

The original group builder is accessible at Setup > Tools and Views > Group Builder (Legacy) and described at Using the group builder (legacy).

- Creating and editing groups
  Learn how to create and edit groups.
- Viewing group membership and where groups are used
  Learn how to view group membership and identify the policies, reports, and queries where groups are used.
- Populating groups
  The group builder supports several methods of adding members to groups.

Parent topic: Groups

Creating and editing groups

Learn how to create and edit groups.

Parent topic: Using the group builder

Creating a group

Procedure

1. Open the group builder by navigating to Setup > Tools and Views > Group Builder.
2. Click the  icon on the Group Builder table.
3. Use the Create new group dialog to define a new group. Provide a group description and use the Application type and Group type menus to define the group.
4. After defining the new group, use the Members tab to populate the group. For information about populating groups, see Populating groups.
5. Click Save to create finish defining the new group.

Editing a group

Procedure

1. Open the group builder by navigating to Setup > Tools and Views > Group Builder.
2. Select a group from the Group Builder table and click the  icon.
3. Use the Edit group dialog to modify group settings. To add members to the group or modify group membership, use the Members tab. For information about populating groups, see Populating groups.
4. Click Save to finish editing the group.

Viewing group membership and where groups are used

Learn how to view group membership and identify the policies, reports, and queries where groups are used.

Parent topic: Using the group builder

Viewing group membership

About this task

The Members and Populated by columns of the Group Builder table summarize how many members are in a group and how the group is populated. The following procedure describes how retrieve detailed information about group membership and the methods used for populating the group.

Procedure

1. Open the group builder by navigating to Setup > Tools and Views > Group Builder.
2. Open the Edit group dialog by selecting a group from the Group Builder table and clicking the icon.
3. View group membership on the Edit group dialog by clicking the Members tab.

Identify where a group is used

About this task

The Used in classifier, Used in policy, and Used inquery columns of the Group Builder table provide an overview of where groups are used in Guardium. The following procedure describes how retrieve detailed information about the policies, queries, and reports where a group is used.

Procedure

1. Open the group builder by navigating to Setup > Tools and Views > Group Builder.
2. Open the details panel by selecting a group from the Group Builder table and clicking Actions > View details.
   Attention: The View details action is only enabled when the selected group is being used, for example by policies or queries.
3. Use the Policies and Queries tabs on the details panel to view where the selected group is used in security policies, classifier policies, queries, and reports.

Populating groups

The group builder supports several methods of adding members to groups.

Procedure

1. Click the icon to create a new group or select a group from the Group Builder table and click the icon to edit an existing group.
2. Select the Members tab of the Create new group or Edit group dialog.
3. Populate the group using one of the following methods:
   - Use the icon to manually define group members.
   - Use the Import menu to add group members using one of the following methods:
     - From CSV
     - From group
     - From external datasource
     - From query
     - From LDAP

     Tip: Once configured, import actions that can be scheduled will appear as tabs on the Create new group or Edit group dialog. One-time actions such as Import from CSV cannot be scheduled and will not introduce a new tab to the dialog.
   - Some group types also support advanced methods for populating groups, including the following:
     - Using stored procedure analysis on datasources
     - Using database dependencies
     - Using reverse dependencies
     - Using observed procedures
     - Generating selected objects

     Important: Using the group builder introduced with Guradium V10.1.4, advanced import actions are invoked on a target group that is populated based on the results of analysis performed on a user-selected input group. This represent a change in behavior from the legacy group builder, where advanced actions were invoked on a source group containing the input to be analyzed, with the results of the analysis being imported into a user-selected group.

- Importing from external datasources
  Learn how to quickly populate Guardium groups with data from your own databases and keep those groups in sync with your data.

Parent topic: Using the group builder

Importing from external datasources

Learn how to quickly populate Guardium groups with data from your own databases and keep those groups in sync with your data.

About this task

Using Import > From external datasource automates the creation of custom tables, domains, and queries to populate Guardium groups from your own datasources. Once created, these artifacts represent a durable connection between Guardium and your data: updates to your data become reflected in the associated Guardium groups.

Procedure

1. Select Import > From external datasource to open the Import from external datasource dialog.
2. Use the Datasource menu to import data from a datasource. Click the icon to define a new datasource or the icon to edit an existing datasource.
3. Use the Table name and Column name fields to identify the location of data to import from your datasource.
4. Click OK to continue.

Results

Completing the Import from external datasource dialog automatically creates or updates the following Guardium artifacts:

- Custom table
- Custom datasource
- Custom domain
- Custom query
- Group

These artifacts are available through standard Guardium tools using naming conventions described in the following table, where *[table name]* and *[column name]* are taken from the Table name and Column name fields of the Import from external datasource dialog.

Table 1. Import from external datasource: summary of artifacts created.

Artifact	Guardium tool	Naming convention	Example	Scheduled
Custom table	Custom Table Builder > Edit Data	*[table name]_[column name]_[datasource ID]*	`USERS_ADMIN_12345`	
Custom datasource	Custom Table Builder > Upload Data	*[datasource name]_[datasource type](Custom Domain)*	`user_repository(Custom Domain)`	✓
Custom domain	Custom Domain Builder	*[group type]_[table name]_[column name]_[datasource ID]*	`USERS_USERS_ADMIN_12345`	
Custom query	Custom Query Builder	*[group type]_[table name]_[column name]_[datasource ID]*	`USERS_USERS_ADMIN_12345`	
Group	Group Builder > Populate from Query		PCI Admin Users	✓

Attention: Imported names are truncated after 64 characters.

Parent topic: Populating groups

Using the group builder (legacy)

- Creating a new group
  Use the group builder to manually create a group of data objects.
- Modifying a group
  Make modifications to your group, such as adding a member or changing the category of the group. Exercise caution when modifying or deleting a group, as changes made could possibly affect other users or policies.
- Populating groups
  After creating a group or finding the one you want to work with, populate the group with members. Use the Group Builder (Legacy) to manually add members to a group, or through several automated import methods.

Parent topic: Groups

Creating a new group

Use the group builder to manually create a group of data objects.

Procedure

1. Open the Group Builder by clicking Setup > Group Builder (Legacy).
2. Click Next to bypass the filter and create a new group.
3. In the Create New Group panel, select an option from the Application Type menu to determine which application you will use the group with.
4. Enter a unique Group Description for the new group - do not include apostrophe characters in this field.
5. Select a Group Type Description to choose which type of data you are grouping.
6. Enter a Category, which is an optional label that you can filter by and use to group items (that the filter has isolated) of policy violations and reports.
7. Enter a Classification, which is another optional label that you can filter by and use to group items for policy violations and reporting.
8. Select Hierarchical to create a group of groups, where the admin user has access and then passes it along to users in groups in the hierarchy.
9. Click Add to add the group.

Parent topic: Using the group builder (legacy)

Modifying a group

Make modifications to your group, such as adding a member or changing the category of the group. Exercise caution when modifying or deleting a group, as changes made could possibly affect other users or policies.

Procedure

1. Open the Group Builder (Legacy) by clicking Setup > Group Builder (Legacy).
2. Use the Group Filter to find the group you want to modify, or leave the filter empty and click Next to look at the complete list of groups.
3. When modifying a group, a best practice is to clone the group , save it as a new group, and then modify the clone to prevent undesired effects on the rest of your Guardium system.

The Modify Existing Groups pane allows you to:

- Modify, clone, or delete any group
- Assign or modify roles
- Populate your group from a query, LDAP server, or using Auto Generated Calling Prox functionality.

4. With any group selected, click Modify  to be able to:
   - modify the category of the group
   - add a new member to the group
   - rename a group member
   - reset a group's membership to the predefined members
   - add comments
   - create an alias for a group
   - populate a group from LDAP

Parent topic: Using the group builder (legacy)

Modifying group category

Procedure

Select a group from the Group Members list, enter the new category name into the Category field and click Modify Category to save changes.

Adding a group member

Create a new member and add it to a group, or add an existing member to a group.

Procedure

If you have a new member you want to add to a group, enter the member's name into the Create & add a new Member named field and click Add.
Note: When adding to a group of objects, valid member names may be composed of object_name, schema.object_name, use a wildcard such as %object_name, or a combination of all three.
The new member is now added to the Group Members list.

Renaming a group member

Procedure

1. Select the group member to be re-named from the Group Members list. This will also display the current group member name in Rename Selected Member to.
2. Change the name of the group member in the Rename selected Member to field and click Update.

Resetting to the predefined group membership

Click Reset to Predefined for any group to replace the current group members with the set of predefined group members.

Adding a comment to a group

Click Add Comments for any group to add comments for your future reference.

Creating an alias for a group

Procedure

1. Click Aliases to open the Alias Quick Definition window.
2. For each group member you want to create an alias for, enter a value into the Alias column and click Apply.

Populating groups

After creating a group or finding the one you want to work with, populate the group with members. Use the Group Builder (Legacy) to manually add members to a group, or through several automated import methods.

- How to populate a group from LDAP
  How to import data from an LDAP server to use in Guardium® groups.
- Populating a group from a query
  Create a query, and use the results to populate a group. This option of populating groups is most useful after the external data correlation has uploaded a custom table to the Guardium system.
- Populating a group from stored procedures
  There are several different methods for populating command or object groups from stored procedures. The auto-generated calling prox functionality in the Group Builder allows you to analyze command or object groups for specific group members and add those members into a new group.

Parent topic: Using the group builder (legacy)
Related information:
Guardium groups and policies (video)

How to populate a group from LDAP

How to import data from an LDAP server to use in Guardium® groups.

About this task

Configure Guardium with your LDAP server, and then import on demand, or schedule an import in the future.

When importing LDAP users:

- The Guardium admin user account will not be changed in any way.
- You have the option to clear existing members from a group before importing.
- Existing user passwords will not be changed.
- By default, new users are disabled when added, assigned the user role, and have blank passwords.

Note:

Special characters are not supported in user names.

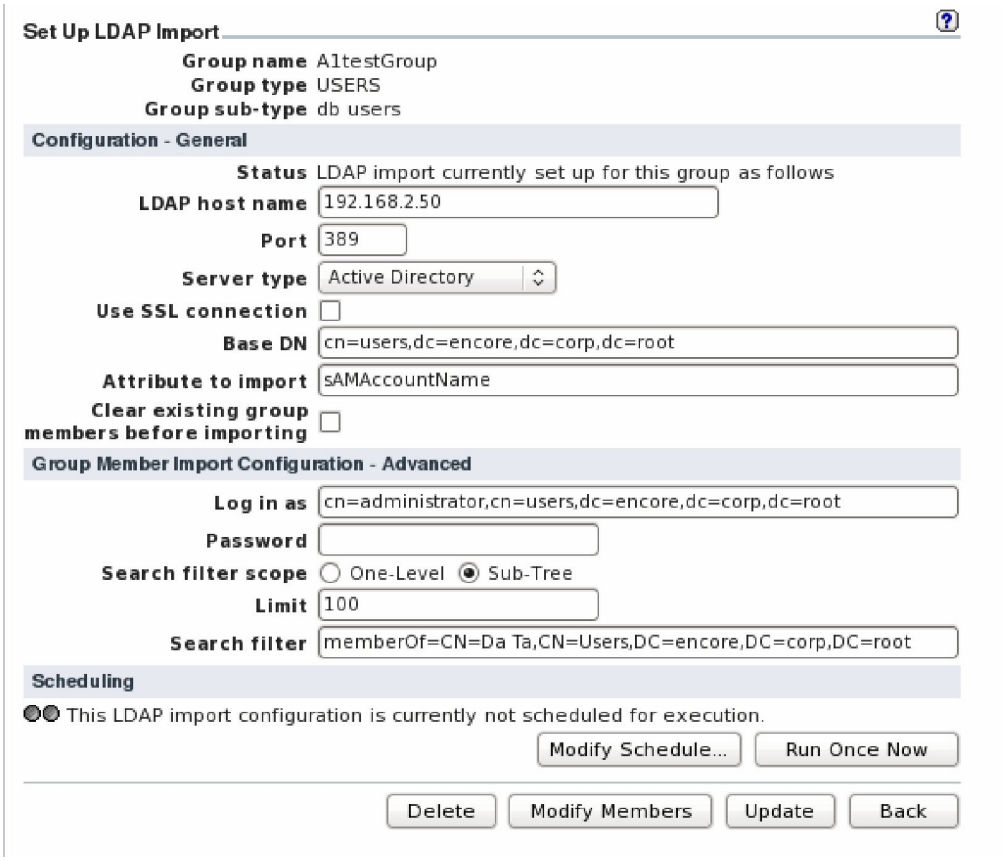
If you are scheduling an import, consider any other scheduled imports you may have at that time, as this will affect the behavior of existing scheduled imports.

Procedure

Configure your LDAP server with your Guardium system. Open the Group Builder by clicking Setup > Group Builder (Legacy), and fill out the required information.

a. For LDAP Host Name, enter the IP address or host name for the LDAP server to be accessed.
b. For Port, enter the port number for connecting to the LDAP server.
c. Select the LDAP server type from the Server Type menu.
d. Check the Use SSL Connection check box if Guardium is to connect to your LDAP server using an SSL (secure socket layer) connection.
e. For Base DN, specify the node in the tree at which to begin the search. For example, a company tree might begin like this: DC=encore,DC=corp,DC=root
f. For Attribute to Import, enter the attribute that will be used to import users (for example: cn). Each attribute has a name and belongs to an objectClass.
g. Check the Clear existing group members before importing check box if you want to delete all existing group members before importing.
h. For Log In As and Password, enter the user account information that will connect to the Guardium server.
i. For Search Filter Scope, select One-Level to apply the search to the base level only, or select Sub-Tree to apply the search to levels beneath the base level.
j. For Limit, enter the maximum number of items to be returned. We recommend that you use this field to test new queries or modifications to existing queries, so that you do not inadvertently load an excessive number of members.
k. Optional: For Search Filter, define a base DN, scope, and search filter. Typically, imports will be based on membership in an LDAP group, so you would use the memberOF keyword. For example: memberOf=CN=syyTestGroup,DC=encore,DC=corp,DC=root
l. Click Apply to save the configuration settings.

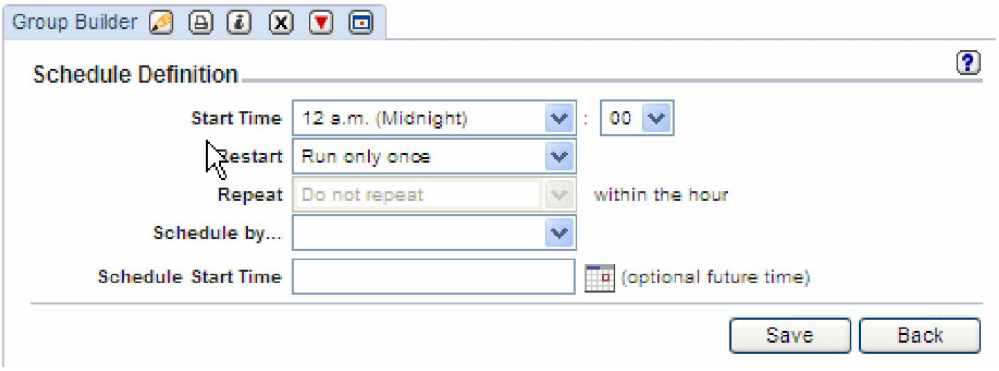
The Status indicator in the Configuration - General section will change to *LDAP import currently set up for this group as follows* and the Modify Schedule and Run Once Now buttons will be enabled. You can now import from your LDAP server.



What to do next

Run or schedule an import.

- Schedule an LDAP import by clicking Modify Schedule, filling out the schedule information, then clicking Save.



- To run the import on demand, click Run Once Now. After the task completes, the set of members satisfying your selection criteria will be displayed in the LDAP Query Results panel.

Note:

When you import on demand, you have the opportunity to accept or reject each entry returned from the LDAP server.

When you schedule an LDAP import, all of the LDAP entries that satisfy your search criteria will be imported.

Verify that members have been added to a group by selecting the group in the Group Builder, then clicking Modify, and looking at the group's membership.

For larger groups, it may be easier to verify members by using the Guardium Group Details report (Reports > Guardium Group Details).

Parent topic: Populating groups

Populating a group from a query

Create a query, and use the results to populate a group. This option of populating groups is most useful after the external data correlation has uploaded a custom table to the Guardium system.

Procedure

1. Open the Group Builder by clicking Setup > Group Builder (Legacy). Use the filter to find the group you want to populate, or click Next and find the group from the list of all groups.
2. With a group selected, click the Populate From Query button to open the Populate Group From Query Set Up panel.
3. From the Query menu, select the query to be run.
    a. Depending on the type of group being populated, different fields will appear. For most group types, the Fetch Member From Column menu will appear.
    b. For paired attribute groups (Object/Command, Object/Field, or Client IP/DB User), two menus will appear: Choose Column for Attribute 1 and Choose Column for Attribute 2.
    c. Select the column (or columns) to be used to populate the group, and any additional parameters for the query. The run-time parameters for the query will then be added to the pane.
4. Select the Clear existing group members before importing box to delete existing group content before importing new members.
5. Optional: Select a remote source (only available from a Central Manager).
6. Click Save to save the definition.
7. Click Run Once Now to run the query immediately, or click Modify Schedule to set a schedule for the query in the future.

Parent topic: Populating groups

Populating a group from stored procedures

There are several different methods for populating command or object groups from stored procedures. The auto-generated calling prox functionality in the Group Builder allows you to analyze command or object groups for specific group members and add those members into a new group.

About this task

The Group Builder (Legacy) can automatically populate command or object group types through two ways:

- By analyzing stored procedure source code. To use this option, Guardium® must access the database on which the stored procedures have been defined, and the stored procedures must not be stored in encrypted format.
- By analyzing stored procedures in database traffic that has been monitored and logged by Guardium. To use this option, the Guardium appliance must be inspecting the appropriate database streams, and logging the information (as opposed to using ignore session or skip logging actions), and the analysis task must run while the data is still on the unit (as opposed to, for example, after an archive/purge operation).

There are two groups involved when populating a group from stored procedures:

- The receiving group is the one to which members will be added.
- The starting group which will be analyzed. This group must be an existing commands or objects group. The search-and-add process is recursive. For example, if the stored procedure named prox_one is added to the receiving group, and prox_one is referenced in prox_two, prox_two will also be added to the receiving group.

Note: Wildcards are not supported in the group members field for stored procedures.

Procedure

1. Open the Group Builder by clicking Setup > Group Builder (Legacy).

2. Choose a starting group to analyze that is either a commands or objects group type.
3. With the starting group selected, click Auto Generated Calling Prox. You will be presented with five options:
    a. Using DB Sources: Populate a group by analyzing the stored procedure definitions from one or more databases.
    b. Using Database Dependencies: Populate a group of objects or a group of qualified objects by analyzing Functions, Java classes, Packages, Procedures, Synonyms, Tables, Triggers and/or Views.
    c. Using Reverse Dependencies: Populate a group by computing a set of objects used when starting from a set of objects.
    Note: The Using Reverse Dependencies option is only available for Oracle.
    d. Using Observed Procedures: Populate a group by analyzing the CREATE PROCEDURE and ALTER PROCEDURE commands as they are observed in the database traffic.
    e. Generate Selected Object: Populate a group by reverse analysis of observed stored procedures. Starting from a set of stored procedures, compute all the tables that these procedures use (directly or indirectly).
    Note: The Generate Selected Object option can only be used with object group type.

- Populating a group using database sources
- Populating a group using database dependencies
  Use this option to populate groups based on Database Dependencies such as Functions, Java classes, Packages, Procedures, Synonyms, Tables, Triggers and/or Views. **This option will only work with Oracle databases on object group types.** This option does not work on *Command* group types because dependency information in the database is only related to objects.
- Populating a group using reverse dependencies
  Generate Selected Object populates the group through reverse analysis of observed stored procedures.
- Populating a group using observed procedures
  Guardium will populate a group by inspecting all changes or additions to stored procedures. This keeps the mapping information up-to-date through continuous analysis of changes to stored procedures.
- Populating a group using generate selected object
  The Generate Select Object option is a part of the Auto Generated Calling Prox functionality that populates an objects group type through reverse analysis of observed stored procedures.

Parent topic: Populating groups

Populating a group using database sources

Before you begin

To use this option:

- You must know where the stored procedures of interest are defined.
- The sources must not be stored in encrypted format.
- You must have access to the stored procedure sources on those databases.

About this task

Guardium will analyze the stored procedure source code, on one or more database servers. Select a group and then run the Auto Generated Calling Prox process to scan your stored procedures. This process will check the selected group to see if any of the objects in that group can be accessed or if any of the commands in that group can be executed. Any matches will be added to a new group. To populate a group using database sources:

Procedure

1. Open the Group Builder by clicking Setup > Group Builder (Legacy). Use the filter to find the group you want to populate, or click Next and find the group from the list of all groups.
   Note: This option can only be used with commands or objects group types.
2. With the group selected, click Auto Generated Calling Prox, and select the Using DB Sources option. This opens the Analyze Stored Procedures panel.
3. Click Add Datasource and select a datasource from the Datasource Finder. The selected datasource will appear in the Datasources pane.
4. Optional: Fill in the Query parameters. Some fields only apply to certain databases.
    - **For Sybase, MS SQL Server, and Informix**, enter a database name to restrict the operation to that database. If it is blank, all stored procedures in the master database will be analyzed.
    - **For MySQL, Oracle or DB2 only**, enter a schema name to restrict the operation to databases owned by that schema. For MySQL only, the Schema Owner is in the form user_name@host, where host can be a specific IP or it can be a % to specify all hosts. To get all hosts, enter the schema name followed by %.
    - **For MySQL, Oracle or DB2 only**, enter a stored procedure name in Object Name. Wildcard characters may be used. For example, if only interested in the procedures beginning with the letters ABC, enter ABC% in the Object Name box.
5. In the Source Detail Configuration section, do one of the following:
    - Add members to an existing group by checking the Append check box, and then selecting a group from the Existing Group Name menu.
    - Add members to a new group by entering the new group name in New Group Name.
      Note: Do not include apostrophe characters in a group name.
6. Select Flatten Namespace to create member names using wildcard characters, so that the group can be used for LIKE GROUP comparisons. For example, if sp_1, is discovered, the member %sp_1% will be added to the group, and in a LIKE GROUP comparison, the values sp_101, sp_102, sss_sp_103, etc. would all match.
7. Click Analyze Database to begin populating the group. The operation may take an extended amount of time to complete.

Parent topic: Populating a group from stored procedures

Populating a group using database dependencies

Use this option to populate groups based on Database Dependencies such as Functions, Java classes, Packages, Procedures, Synonyms, Tables, Triggers and/or Views. **This option will only work with Oracle databases on object group types.** This option does not work on *Command* group types because dependency information in the database is only related to objects.

About this task

When specifying the group type, keep in mind that only *Object* or *Qualified Object* group types work with this option. A qualified object requires five value attributes: server IP, instance, DB name, owner and object. This is also called a 5-tuple object.

An example of what a Qualified Objects group member looks like is 192.168.1.0+guardium+oracle+admin+fininacial object.

Procedure

1. Open the Group Builder by clicking Setup > Group Builder (Legacy). Use the filter to find the group you want to populate, or click Next and find the group from the list of all groups.
2. With the objects or qualified objects group selected, click Auto Generated Calling Prox, and select the Using Database Dependencies option. This opens the Analyze Stored Procedures panel.
3. Click Add Datasource and select a datasource from the Datasource Finder. The selected datasource will appear in the Datasources pane.
4. Optional: Fill in the Query parameters.
5. In the Source Detail Configuration section, do one of the following:
   - Add members to an existing group by checking the Append box, and then selecting a group from the Existing Group Name menu.
   - Add members to a new group by entering the new group name in New Group Name.
     Note: Do not include apostrophe characters in a group name, and make sure that the new group is fully qualified (includes five value attributes: server IP, instance, DB name, owner and object).
6. Select Flatten namespace to create member names using wildcard characters, so that the group can be used for LIKE GROUP comparisons. For example, if sp_1, is discovered, the member %sp_1% will be added to the group, and in a LIKE GROUP comparison, the values sp_101, sp_102, sss_sp_103, etc. would all match.
7. In the Include Types section, select database dependencies: Functions, Java classes, Packages, Procedures, Synonyms, Tables, Triggers and/or Views.
8. Click Analyze Database to populate the group. You will be informed of the results.

Parent topic: Populating a group from stored procedures

Populating a group using reverse dependencies

Generate Selected Object populates the group through reverse analysis of observed stored procedures.

About this task

These options from the Group auto-populate menu compute a set of objects used when starting from a set of objects. For example, starting from a set of stored procedures, compute all the tables that these procedures use (directly or indirectly).

Procedure

1. Open the Group Builder by clicking Setup > Group Builder (Legacy). Use the filter to find the group you want to populate, or click Next and find the group from the list of all groups.
   Note: The Reverse Dependencies option is available only for Oracle.
2. With the group selected, click Auto Generated Calling Prox, and select the Using Reverse Dependencies option. This opens the Analyze Stored Procedures panel.
3. Click Add Datasource and select a datasource from the Datasource Finder. The selected datasource will appear in the Datasources pane.
4. Optional: Fill in the Query parameters.
5. In the Source Detail Configuration section, do one of the following:
   - To add members to an existing group, select Append, and then select the group from the Existing Group Name list.
   - To add members to a new group, enter the new group name in New Group Name.
     Note: Do not include apostrophe characters in a group name.
6. Select Flatten namespace to create member names using wildcard characters, so that the group can be used for LIKE GROUP comparisons. For example, if sp_1, is discovered, the member %sp_1% will be added to the group, and in a LIKE GROUP comparison, the values sp_101, sp_102, sss_sp_103, etc. would all match.
7. In the Include Types section, select database dependencies: Functions, Java classes, Packages, Procedures, Synonyms, Tables, Triggers and/or Views.
8. Click Analyze Database to populate the group. You will be informed of the results.

Parent topic: Populating a group from stored procedures

Populating a group using observed procedures

Guardium will populate a group by inspecting all changes or additions to stored procedures. This keeps the mapping information up-to-date through continuous analysis of changes to stored procedures.

Procedure

1. Open the Group Builder by clicking Setup > Group Builder (Legacy). Use the filter to find the group you want to populate, or click Next and find the group from the list of all groups.
2. With the starting group selected, click Auto Generated Calling Prox, and select the Using Observed Procedures option. This opens the Analyze Observed Stored Procedures panel.
3. To edit an existing configuration, select it from the Source Details menu. To create a new configuration, leave the selection on *New*.
4. In the Access Information section, select all of the database servers to be analyzed. You can choose any combination of the check-boxes.
5. In the Source Detail Configuration section, do one of the following:
   - Add members to an existing group by checking the Append box, and then selecting a group from the Existing Group Name menu.
   - Add members to a new group by entering the new group name in New Group Name.
     Note: Do not include apostrophe characters in a group name.
6. Select Flatten namespace to create member names using wildcard characters, so that the group can be used for LIKE GROUP comparisons. For example, if sp_1, is discovered, the member %sp_1% will be added to the group, and in a LIKE GROUP comparison, the values sp_101, sp_102, sss_sp_103, etc. would all match.
7. Click Save to save the configuration.
8. Set a schedule for the group by doing one of the following:
   - To run the query immediately and get results now, Click Run Once Now.
   - To define a schedule for the operation, click Modify Schedule.

Parent topic: Populating a group from stored procedures

Populating a group using generate selected object

The Generate Select Object option is a part of the Auto Generated Calling Prox functionality that populates an objects group type through reverse analysis of observed stored procedures.

About this task

Guardium will populate the group by inspecting all changes or additions to stored procedures. This keeps the mapping information up-to-date through continuous analysis of changes to stored procedures.

Procedure

1. Open the Group Builder by clicking Setup > Group Builder (Legacy). Use the filter to find the group you want to populate, or click Next and find the group from the list of all groups.
2. With the starting group selected, click Auto Generated Calling Prox, and select the Generate selected object option. This opens the Analyze Observed Stored Procedures panel.
3. To edit an existing configuration, select it from the Source Details menu. To create a new configuration, click *New*.
4. In the Access Information section, select all of the database servers to be analyzed. You can choose any combination of the check-boxes.
5. In the Source Detail Configuration section, enter a name, and choose an option from the Verb menu.
6. Do one of the following:
   - Add members to an existing group by checking the Append box, and then selecting a group from the Existing Group Name menu.
   - Add members to a new group by entering the new group name in New Group Name.
     Note: Do not include apostrophe characters in a group name.
7. Select Flatten namespace to create member names using wildcard characters, so that the group can be used for LIKE GROUP comparisons. For example, if sp_1, is discovered, the member %sp_1% will be added to the group, and in a LIKE GROUP comparison, the values sp_101, sp_102, sss_sp_103, etc. would all match.
8.
9. Click Save to save the configuration.
10. Set a schedule for the group by doing one of the following:
    - To run the query immediately and get results now, Click Run Once Now.
    - To define a schedule for the operation, click Modify Schedule.

Parent topic: Populating a group from stored procedures

Using groups in queries and policies

Short overview of conditional operators for queries and where to use groups in policies.

Queries

Queries use conditional operators with groups. Here are examples of each conditional operator:

- IN GROUP - If the value matches any member of the selected group, the condition is true. IN ALIASES GROUP, this operator works on a group of the same type as IN GROUP, however assumes the members of that group are aliases. Note that the IN GROUP/IN ALIASES GROUP operators expect the group to contain actual values or aliases respectively. Query Builder will look for records with database values matching the aliases value in the group.
- NOT IN GROUP - If the value does not match any member of the selected group, the condition is true. NOT IN ALIASES GROUP, this works on a group of the same type as NOT IN GROUP, however assumes the members of that group as aliases.
- IN DYNAMIC GROUP - If the value matches any member of a group that will named as a run-time parameter, the condition is true. IN DYNAMIC ALIASES GROUP, this works a group of the same type as IN DYNAMIC GROUP, however assumes the members of that group as aliases.
- NOT IN DYNAMIC GROUP - If the value does not match any member of a group that will named as a run-time parameter, the condition is true. NOT IN DYNAMIC ALIASES GROUP, this works a group of the same type as NOT IN DYNAMIC GROUP, however assumes the members of that group as aliases.
  Note: The group may contain either aliases or actual values according to the operator used (IN GROUP OR IN ALIASES GROUP) can not be used at the same time.
- LIKE GROUP - If the value is like any member of the selected group, the condition is true. This condition enables wildcard (%) characters in the group member names.
  Note: A like member value uses one or more wildcard (%) characters, and matches all or part of the value. For a like comparison, alphabetic characters are not case sensitive. For example, %tea% would match tea, TeA, tEam, or steam.

Policies and rules

When creating a rule as part of a policy, groups simplify the process of specifying the parameters you want.

Anywhere there is a Group drop-down menu on the rule definition pane you can select a group.

Further, if you want to create or modify a group on the fly, click the Groups icon  to open a Group Definition window and make your desired changes.

For example: if you want to capture activity occurring on your production servers, rather than typing in full IP addresses each time, you could create a group *Production Servers* and use that.

Parent topic: Groups

Example: Using groups to create rules and policies

Use groups to quickly specify rule conditions in a policy.

About this task

Each policy is composed of one or more rules. Specify which conditions will enact a rule, and then choose one or more actions to take when that rule is triggered. This example shows you how to use groups to identify unauthorized users, log details of their access on a group of sensitive objects, and send an alert indicating that the access occurred.

Procedure

1. Login to your Guardium system, and open the Policy Builder by clicking Setup > Tools and Views > Policy Builder for Data.
2. Create a new policy by clicking the  icon to open the Policy Definition window.
3. Define the policy definition, then click Apply to save the policy.
4. Click Edit Rules to open the Policy Rules window and begin adding rules to the policy.
5. Click Add Rules > Add Access Rule to add a new rule to the policy.
6. Begin by providing a Description for the rule. Optionally provide Category and Classification labels.
7. Specify where to look for data. From the Server IP row, select the (Public) PCI Authorized Server IPs group. The rule will apply to all activity from all PCI servers. Note: You can view the members of any group or modify any group by going to the Group Builder.
8. Specify unauthorized users. From the DB User row, mark the Not check box and select the (Public) Authorized Users group. The rule will apply to all users who are not in the *(Public) Authorized Users* group.
9. Specify sensitive objects. From the Object row, select the (Public) PCI Cardholder Sensitive Objects group. The rule will now apply to all unauthorized users on PCI servers looking to access PCI sensitive objects.
10. Add an action to the rule by clicking Add Action and selecting Action > LOG FULL DETAILS from the menu. Click Apply to save the rule. This action logs details of the access, including an exact timestamp of the access.
11. Add another action to the rule by clicking Add Action and selecting Action > ALERT ONCE PER SESSION from the menu. Specify an alert destination, then click Apply to save the rule. This action sends or logs an alert indicating that the rule was triggered.
12. Click Save to save the rule.
13. Install the policy.
    a. Find the policy that you created. Click Back twice, or click Policy Builder to get to the Policy Finder and browse the list of policies.
    b. With the policy selected, choose Install & Override from the installation action menu.
    c. Click OK to confirm the policy installation, and then check Latest Logs and Violations to verify the policy was installed.

    The policy is now installed and active. Any person not in the *(Public) Authorized Users* group attempting to access an object in the *(Public) PCI Cardholder Sensitive Objects* groups will have their session logged and will trigger an alert indicating the access.

Parent topic: Groups

Predefined Groups

This section details the predefined groups in Guardium®.

The following table describes the predefined groups that are included with your Guardium system. To view the list of all groups, open the Group Builder by clicking Setup > Group Builder. Select *SQL_APP_NAME* from the Applications menu, and click Next. From the next screen, manage members from Selected Groups. The term *Group Type* refers to expectations on the type of data designated by the label. For example, the group type *Server IP* expects data arranged as an IP address (192.168.1.0) and the group type *Users* expects to see names of users of the application.

Additional predefined groups do get added periodically and these additional predefined groups may not be described here. Open the Group Builder to see all existing groups.

Predefined groups of group type DB User/DB Password are allowed only to users with the role of admin. Users can, if preferred, add other roles or even allow the groups to all roles.

Table 1. Predefined Groups

SQL_APP_NAME	GROUP_DESCRIPTION	MEMBERS
DB2® zOS Groups	zOS Audit Dynamic SQL	Group Type for DB2 commands
DB2 zOS Groups	zOS Audit Query	Group Type for DB2 commands
DB2 zOS Groups	zOS Audit Updates	Group Type for DB2 commands
DB2 zOS Groups	zOS Audit Deletes	Group Type for DB2 commands
DB2 zOS Groups	zOS Audit Inserts	Group Type for DB2 commands
DB2 zOS Groups	zOS Audit Utilities	Group Type for DB2 commands
DB2 zOS Groups	zOS Audit Object Maintenance	Group Type for DB2 commands
DB2 zOS Groups	zOS Audit User Maintenance	Group Type for DB2 commands
DB2 zOS Groups	zOS Audit User Authorization Changes	Group Type for DB2 commands
DB2 zOS Groups	zOS Audit DB2 Commands	Group Type for DB2 commands
DB2 zOS Groups	zOS Audit Plan/ Package Maintenance	Group Type for DB2 commands
IMS™ zOS Groups	zOS IMS Audit Query	Group Type for IMS commands
IMS zOS Groups	zOS IMS Audit Updates	Group Type for IMS commands
IMS zOS Groups	zOS IMS Audit Deletes	Group Type for IMS commands
IMS zOS Groups	zOS IMS Audit Inserts	Group Type for IMS commands
IMS zOS Groups	zOS IMS Audit DB Commands	Group Type for IMS commands
Policy Builder	Cardholder Objects	Group Type, Objects
Policy Builder	Financial Objects	Group Type, Objects
Policy Builder	PHI Objects	Group Type, Objects
Policy Builder	Authorized Client IPs	Group Type, Client IP
Policy Builder	Production Users	Group Type, Users
Policy Builder	PII Objects	Group Type, Objects

SQL_APP_NAME	GROUP_DESCRIPTION	MEMBERS
Policy Builder	Production Servers	Group Type, Server IP
Policy Builder	Financial Servers	Group Type, Server IP
Policy Builder	Functional Users	Group Type, Users
Policy Builder	Sharepoint Servers	Group Type, Server IP
Security Assessment Builder	DB2 Database Version+Patches Informix® Database Version+Patches MS Sql Server Database Version+Patches MySql Database Version+Patches Netezza® Version+Patches Oracle Database Version+Patches Postgress Version+Patches Sybase Database Version+Patches Teradata PDE Version+Patches Teradata TDBMS Version+Patches Teradata TDGSS Version+Patches Teradata TGTW Version+Patches	Used for (specific) database version and patch level tests.
Security Assessment Builder	DB2 Allowed Grants to Public Informix Allowed Grants to Publics MS-SQL Allowed Grants to Public MYSQL Allowed Grants to Public Netezza Allowed Grants to Public Oracle Allowed Grants to Public Postgres Allowed Grants to Public Teradata Allowed Grants to Public	TUPLE, Object/Command Application 8 (Security assessment) List of objects/commands for which grants to public are allowed. These objects will be skipped on MS-SQL and Sybase tests that check grants to public. Note: Exceptions group can contain a regular expression or just a member. If regular expression, the group member must start with (R) (case sensitive), and the records in the detail will be checked against the regular expression after the (R). For example if a group member is: (R)SYSTEM.[a-z]+ each detail record will be checked using pattern: SYSTEM.[a-z]+ If the member does not start with (R) the detail record will be considered an exception only if it is equal to the group member. Note a group may contain a mix of regular expressions and specific exceptions.
Security Assessment Builder	MS-SQL Extended Procedures Allowed	Group Type is Objects
Security Assessment Builder	MS-SQL Database Administrators	Group Type is Users
Security Assessment Builder	Teradata Profile	Group Type is Objects
Public	Account Management Commands	Commands used to maintain accounts (users, roles, permissions), examples: REVOKE, GRANT, ALTER/CREATE/DROP USER
Public	Account Management Procedures	Account Management Objects, stored Procedures used to maintain accounts (users, roles, permissions)
Public	Active Users	Group Type is Users
Public	Admin Users	Default administrative users (DBAs and SysAdmins)
Public	Administration Objects	Privileged Objects, objects that only DBA or Sys Accounts should access. These accounts are locked for "public" by default.
Public	Administrative Commands	Privileged Commands, privileged Commands, should be executed only by DBAs. Examples: GRANT, BACKUP, DDL commands
Public	Administrative Programs	Database utilities (clients) that come with database and usually reside on the database server and could used by the server itself
Public	ALTER Commands	Examples, alter database, alter procedure, alter profile, alter session, alter user
Public	Application Privileged Commands	Public privileged commands that should be revoked from "public", but not revoked since they are used by the application
Public	Application Privileged Procedures	Application Privileged Objects, public privileged procedures that should be revoked from "public" but not revoked since they are used by the application

SQL_APP_NAME	GROUP_DESCRIPTION	MEMBERS
Public	Application Schema Users	Application Users, database user used by the application to maintain/user the application tables
Public	Archive Candidates	Group Type is Objects
Public	Authorized Source Programs	Group Type is Source Programs
Public	Authorized Users	Group Type is Users
Public	Connection Profiling List	Group Type is Client IP/Src App/DB User/Server IP/SVC. Name List of allowed connections
Public	CREATE Commands	Examples, create context, create database link, create function, create statistics, create type, create user
Public	Credentials Related Entities	Guardium Audit Types, Self-Monitoring, examples, allowed_role, LDAP_config, Turbine_user_group_role
Public	Data Transfer Commands	Backup Commands, commands dealing with backup/restore of database data
Public	Data Transfer Procedures	Data Transfer Objects, procedures dealing with backup/restore of database data (mostly on MSS and SYB)
Public	DB Predefined Users	Either non-admin predefined users or all predefined users, including administrative ones
Public	DBCC Commands	Group Type is Commands
Public	DDL Commands	Data Definitions Language, schema-privileged commands, examples, ALTER, CREATE, DROP
Public	DML Commands	DML Commands, examples, insert, truncate, update
Public	DROP Commands	Examples, drop_context, drop_event_monitor, drop_procedure, drop_role
Public	DW All Object-Field DW All Objects DW Execute Accessed Objects DW Select Accessed Objects DW Select Accessed Objects/Fields	There are five predefined reports that use monitored data to show object names. These reports all start with the prefix DW (Data Warehouse). See the help topic, How to report on dormant tables/columns, for further information on how to use these predefined reports.
Public	EBS App Servers	Group Type is Client IP
Public	EBS DB Servers	Group Type is Server IP
Public	EXECUTE Commands	Examples, call, execute, execute function
Public	GRANT Commands	Examples, grant, grant objectives, grant system privileges
Public	Guardium Audit Categories for Detailed Reporting	Guardium patches, TURBINE_USER_GROUP_ROLE
Public	ICM App Servers	Group Type is Client IP
Public	ICM DB Servers	Group Type is Server IP
Public	ImportLDAPUser	Group Type is Objects
Public	ImportLDAPUser_bindValues	Group Type is Objects
Public	Inspection Engine Entities	Examples, adminconsole_sniffer, software_tap_db_client, software_tap_db_server
Public	Java™ Commands	Examples, alter java, create java, drop java
Public	KILL Commands	Example, kill
Public	Masked_SP_Executions_MS_SQL_SERVER	For MS SQL Server, a group that includes a collection of stored procedures (SP) names. If there is an execution of an included procedure, than everything will be masked, even if in quotes. Predefined as empty.
Public	Masked_SP_Executions_Sybase	For Sybase, a group that includes a collection of stored procedures (SP) names. If there is an execution of an included procedure, than everything will be masked, even if in quotes. Predefined as empty.
Public	MongoDB Skip Commands	Group Type is Commands
Public	MS-SQL Replication Procedures	Group Type is Objects
Public	MS-SQL Security System Procedures	Group Type is Objects
Public	MS-SQL System Procedures	Group Type is Objects
Public	Oracle EBS HRMS Sensitive Objects	Group Type is Objects
Public	Oracle EBS-PCI	Group Type is Objects
Public	Oracle EBS-SOX	Group Type is Objects
Public	Oracle Predefined Users	Group Type is Users

SQL_APP_NAME	GROUP_DESCRIPTION	MEMBERS
Public	Peer Association Commands	Commands dealing with links/replications of data, examples, links, log shipping, replications, snapshots
Public	Peer Association Procedures	Peer Association Objects, procedures dealing with links/replications of data Examples: Links, log shipping, replications, snapshots
Public	PeopleSoft Objects	Group Type is Objects
Public	PeopleSoft Sensitive Objects	Group Type is Objects
Public	Performance Commands	Examples, analyze, create statistics, update all statistics
Public	Policy Related Entities	Examples, access_rule, gdm_install_policy_header
Public	Potential Overflow Objects	Group Type is Objects
Public	Procedural Commands	Examples, begin, call, execute, exit, repeat, set
Public	PROCEDURE DDL	Examples, alter procedure, create procedure, drop procedure
Public	PSFT App Servers	Group Type is Client IP
Public	PSFT DB Servers	Group Type is Server IP
Public	Public executable procedures	Execute-Only Objects, procedures/functions/Packages that by default granted access to public
Public	Public selectable object	Select-only Objects, tables that by default granted access to public
Public	RESTORE Commands	Examples, restore database, restore log
Public	REVOKE Commands	Examples, revoke object privileges, revoke system privileges
Public	Risk-indicative Error Messages	SQL errors related to security
Public	Sharepoint Servers	
Public	SAP-PCI	Group Type is Objects
Public	SAP App Servers	Group Type is Client IP
Public	SAP DB Servers	Group Type is Server IP
Public	SAP HR Sensitive Objects	Group Type is Objects
Public	Select Command	Examples, select, select list
Public	Sensitive Objects	Examples, activity, sales
Public	SIEBEL App Servers	Group Type is Client IP
Public	SIEBEL DB Servers	Group Type is Server IP
Public	Siebel SIA Sensitive Objects	Group Type is Objects
Public	SPECIAL CASE Source Program	Group Type is Source Programs
Public	Suspicious Objects	Group Type is Objects
Public	Suspicious Users	Group Type is Users
Public	System Configuration Commands	Database configuration commands (subset of Administrative Commands) Examples: ALTER DATABASE, ALTER SYSTEM
Public	System Configuration Procedures	System Configuration Objects (subset of Administration Objects)
Public	Terminated DB Users	Group Type is Users
Public	Vulnerable Objects (with wildcards)	Database objects with reported vulnerabilities
Public	Windows File Share Verbs	Group Type is Commands
Public	DB2 Default Users IBM iSeries Default Users Informix Default Users MS-SQL Server Default Users MYSQL Default Users Netezza Default Users Oracle Default Users PostgreSQL Default Users Sybase Default Users Teradata Default Users	Group Type is DB User/DB Password

SQL_APP_NAME	GROUP_DESCRIPTION	MEMBERS
Public	Hadoop Skip Commands Hadoop Skip Objects Not Hadoop Server	Group Type is Command Group Type is Object Group Type is Server IP
Public	Replay - Exclude from Compare Replay - Include in Compare	Group Type is Objects
Audit Process Builder		Predefined as empty.
Baseline Builder		Predefined as empty. Attention: The Baseline Builder and related functionality is deprecated starting with Guardium V10.1.4.
Classifier		Predefined as empty.
Express Security		Predefined as empty.

Parent topic: Groups

Security Roles

Security roles are used to grant access to data (groups, queries, reports, etc.) and to grant access to applications (Group Builder, Report Builder, Policy Builder, CAS, Security Assessments, etc).

By default, when a component is initially defined, only the owner (the person who defined it) and the admin user (who has special privileges) are allowed to access and modify that component.

You can allow other users to access the components you define by assigning security roles. For example, if you assign a security role named DBA to an audit process, all users assigned the DBA role will be able to access that audit process.

Note: In order to configure LDAP user import, accessmgr user must have the privilege to run the Group Builder. In certain situations, when changes are made to the role privilege, accessmgr's privilege to Group Builder can be taken away. This results in an inability to save or run successfully LDAP user import. Go to the access management portal, select Role Permissions. Choose the Group Builder application and make sure that there is a checkmark in the all roles box or a checkmark in the accessmgr box.

Assign Security Roles

1. Open or select the item to which you want to assign one or more security roles (a policy or report definition, for example).
2. Click Roles.
3. Check all of the roles you want to assign from the Assign Security Roles list. You can only assign roles that are assigned to your account.
4. Click Apply.

Define a new Security Role

By default, only the special accessmgr user is allowed to create or remove security roles.

1. Login as accessmgr and open the User Role Browser by clicking Access > Access Management > User Role Browser.
2. At the end of the role browser, click Add Role.
3. In the Role Form panel, enter a new Role Name and click Add Role.

Remove a Security Role

By default, only the special accessmgr user is allowed to create or remove security roles. To remove a role assigned to a component, see Assign security roles to a component.

1. Login as accessmgr and open the User Role Browser by clicking Access > Access Management > User Role Browser.
2. Click Delete for any role, and then click Confirm Deletion.

Parent topic: Managing your Guardium system

Notifications

Use the Alerter and Alert Builder to create notifications. When email or other notifications are required for alerting actions, follow this procedure for each type of notification to be defined.

Alerter configuration

1. Before you choose alerting actions, you must be configure the email SMTP settings in theAlerter
2. Open the Alerter by clicking Protect > Database Intrusion Detection > Alerter.
3. Fill out the SMTP and/or SNMP information.
4. After filling out each section, click Test Connection, and verify that the connection is working. You will receive a message stating the connection is unreachable if the connection is not working.
5. Click Apply to save the configuration.
6. At a minimum, IP Address/Host name, port, and return email address must be specified.
7. Select *Mail* from the Notification Type menu. If the Severity of the message is *HIGH*, the Urgent flag is set.
8. Select a user (which can be an individual or group) from the Alert Receiver list. Additional receivers for real-time email notification are Invoker (the user that initiated the actual SQL command that caused the trigger of the policy) and Owner (the owner/s of the database). The Invoker and Owner are identified by retrieving user IDs (IP-based) configured by using the Guardium® APIs.

9. Click Add.

Build an alert

1. After configuring the Alerter, open the Alert Builder by clicking Protect > Database Intrusion Detection > Alert Builder.
2. Fill out the information in the Settings, Alert Definition, Alert Threshold, and Notification sections and click Apply.
3. Choose who will receive the notifications by clicking Add Receiver.. and choosing a user.

Parent topic: Managing your Guardium system

How to create a real-time alert

Send a real-time alert to the database administrator whenever there are more than three failed logins for the same user within five-minutes.

About this task

Generate real-time security alerts whenever suspicious activity is detected or access policies are violated.

Follow these steps:

1. Create a policy
2. Add rules to the policy
3. Install the policy
4. Setup a real-time alert when the policy is enacted

Prerequisites

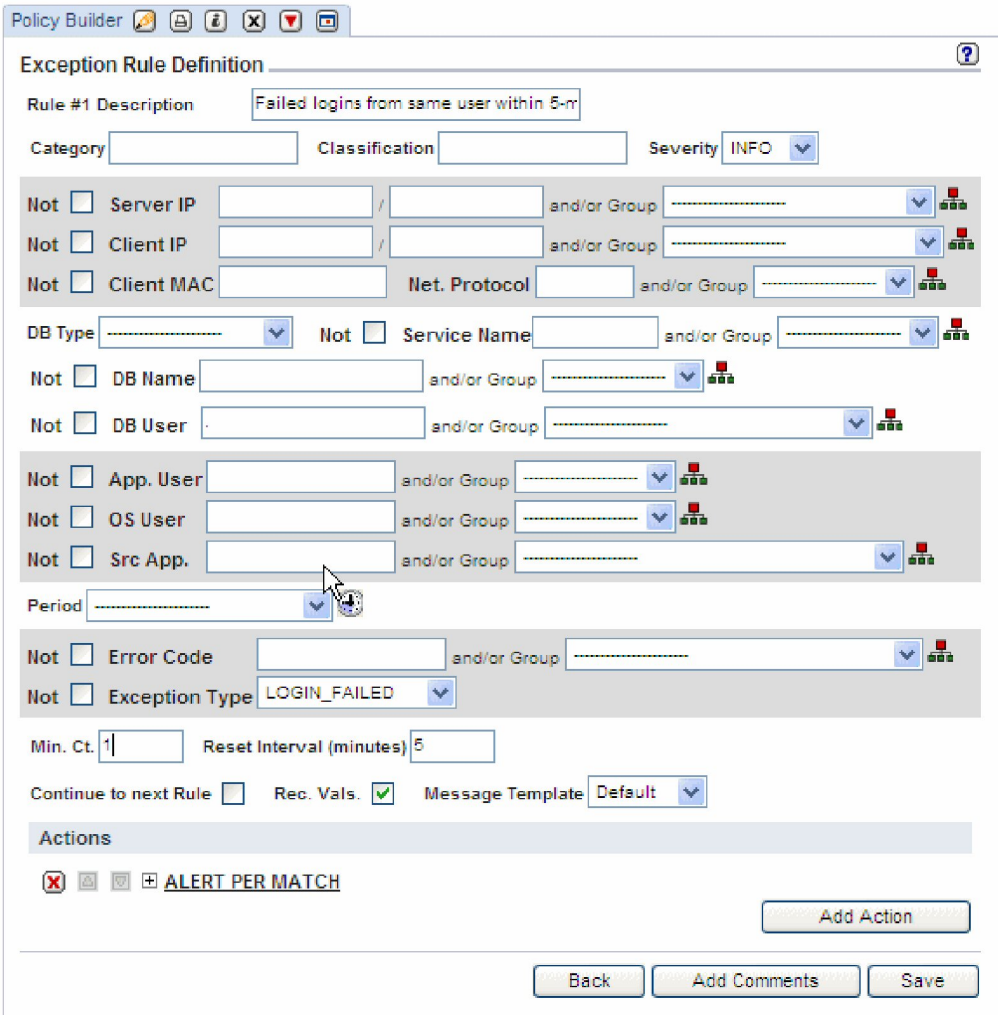
Configure SMTP in the Alerter. Open the Alerter by clicking Protect > Database Intrusion Detection > Alerter, and then fill out the SMTP information.

Note: Policy violations can also be seen as a report in Incident Management See Policies for complete information.

Procedure

1. Create a policy.
   a. Open the Policy Builder by clicking Setup > Tools and Views > Policy Builder for Data or Applications.
   b. Click New, or modify an existing policy by selecting the policy from the Policy Finder and clicking Modify.
   c. Fill out the required information and click Apply to save the policy.
2. Add rules to the policy.
   a. After saving the policy, click Edit Rules to see the existing policy rules.
   b. Click Add Rules... and then you are presented with five rule options.
   c. Choose Add Exception Rule and fill out the required information.

      The Exception Rule Definition screen begins with the following items:



- Description - Enter a short, descriptive name for the rule.
- Category - The category will be logged with violations, and is used for grouping and reporting purposes. If nothing is entered, the default for the policy will be used.
- Classification - (optional) Enter a classification. Like the category, these are logged with exceptions and can be used for grouping and reporting purposes
- Severity - Select a severity code from the menu: INFO, LOW, NONE, MED, or HIGH (the default is INFO).

d. Use the remaining fields to specify how to match the rule - where to search, what to search for, who to search for, and when to search.
e. Enter a period "." in the DB User field to count each individual value separately.
f. From the Excpt. Type (exception type) menu, select LOGIN_FAILED.
g. Use the Minimum Count to set the minimum number of times the rule must be matched before the action will be triggered. For this example, choose 1. The count of times the rule has been met will be reset each time the action is triggered or when the reset interval expires.
h. Use the Reset Interval to set the number of minutes after which the rule counter will be reset to zero. The counter is also reset to zero each time that the rule action is triggered. For this example, choose 5.
i. Check the Cont. to next rule check box to continue testing rules once this rule is satisfied and its action is triggered. If this is not selected, no additional rules will be tested when this rule is satisfied.
j. Check the Rec. Vals. check box to indicate that when the rule action is triggered, the complete SQL statement causing that event will be logged and available in the policy violation report. If not marked, the SQL String attribute will be empty.

3. Add an action when the rule is triggered.
   a. From the Actions section of the Exception Rule Definition screen, click Add Action.
   b. Select an option from the Action menu and click Apply. For this example, choose *ALERT PER MATCH* to get a notification every time the rule is enacted.
   c. Select an option from the Notification Type menu. You must configure the Alerter for mail or SNMP notification types.
   d. Add an alert receiver, and click Apply to save the action.
4. Install the policy.
   a. Click Setup > Tools and View > Policy Installation.
   b. Find the policy from the Policy Installer menu, select an installation action, and click Modify Schedule or Run Once Now. Your policy is now installed. Your alert receiver will receive real-time notifications when the policy rules are enacted.

Parent topic: Managing your Guardium system

Custom Alerting Class Administration

Use a custom alert class to send alerts to a custom recipient. Upload the custom class, then use the Alert Builder to designate the custom class as an alert notification receiver.

- Before you can use a custom class, you must upload it onto the Guardium system. Click Setup > Custom Classes > Alerts > Upload Alerting Class to upload a custom alerting class. Click Browse to select a file, then Apply to save.

- After uploading the custom class, use it in an alert with the Alert Builder. Open the Alert Builder by clicking Manage > Database Intrusion Detection > Alert Builder. Fill out the required information, select *CUSTM* from the Notification Type menu, and click Save.

Parent topic: Managing your Guardium system

Predefined Alerts

Table describing the predefined alerts found in the Alert Builder.

Guardium comes with a set of predefined alerts that can be found in the Alert Builder. Open the Alert Builder by clicking Protect > Database Intrusion Detection > Alert Builder. When you open the Alert Builder, you are presented with a list of all existing alerts in the Alert Finder. Select an alert from the finder and click Modify to edit it.

In the Modify Alert screen, modify any part of the alert, such as receivers or threshold.

You cannot modify the default queries that the alerts are based on. If you want to modify a query, click the Edit this Query icon for any query to open the Query Builder. Once in the builder, clone any query, and then modify the clone to suit your needs.

After making changes to an alert, click Apply to save them.

The following table describes all predefined alerts.

Table 1. Predefined Alerts

Alert	Description
Active S-TAPs Changed	Checks for changes to Active S-TAP® inspection engines done during the last accumulation interval. The alert will trigger if at least one inspection engine has been changed during the period. By default the alert checks every 1/2 hour and checks the last hour.
Aggregation/Archive Errors	Alert once a day on all aggregation or archive tasks that did not complete successfully.
Connection Profiling Alert	Alert runs every 60 minutes and sends notice to predefined group, Connection Profiling List - Name List of allowed connections
CAS Instance Config Changes	Alert once a day on any CAS instance configuration changes.
CAS Templates Changes	Alert once a day on any CAS template configuration changes.
Data Source Changes	Alert once a day on any data source definition changes.
Database disk space	Alert every 10 minutes if internal database is more than 80% filled. See the Self Monitoring help topic for more information on Disk Space (% full) and the Guardium® Nanny process.
Enterprise No Traffic	Enterprise No Traffic Alert runs only on Central Manager systems. It is based on a query similar to the query on the No Traffic alert and retrieves the records with: timestamp between X and Y, when X is a query parameter and Y is query from date generated by the alert mechanism based on the accumulation interval (same way the existing no traffic alert works).
Enterprise S-TAPs changed	This alert will only run Central Manager systems.
Failed Logins to Guardium	Every 10 minutes alert if there have been more than 5 failed login attempts on the Guardium appliance.
Guardium - Add/Remove Users	Alert once a day if any Guardium users have been added or removed.
Guardium - Credential Activity	Alert once a day if there have been any Guardium credential changes, including LDAP configuration changes.
Inactive Managed Unit	Alert runs 30 minutes and sends a notice once a day to the predefined group that is called "Managed Units Alert".
Inactive S-TAPs Since	Alert once an hour on all S-TAPs that have not been heard from.
Inspection Engines and S-TAP	Alert once a day on any activity related to inspection engine and S-TAP configuration.
No Traffic	Alert to Indicate whether there is no traffic from specific database servers. This alert will alert when there is no traffic collected from a server from which the Guardium system was collecting traffic at some point during the last 48 hours. The alert will trigger when there is no traffic within the period defined in the accumulation interval. For example if the accumulation interval is 60 minutes the alert will send an email if there was no traffic from a specific database server in the last hour but there was some traffic in the last 48 hours. The alert will send an email (by default) only every 24 hours. Parameters such as accumulation interval, notification interval, run frequency etc. can be customized. Parameters such as Threshold, Per Line, operator, query etc. should not be changed, as changes to these parameters will cause the alert not to work properly. Note the No Traffic query should not be cloned.
No Traffic by Server/Protocol	Similar to the regular No traffic alert with the following differences: The alert is per service Name/Net Protocol, and will report per line. There is a new additional parameter: Active Traffic Interval that determines when the last request from each server was received. The alert will trigger under the following conditions: There was No traffic during the alert interval from each server/net protocol but there was traffic since: Active Traffic Interval for that combination. Unlike the regular No traffic alert that will trigger if there was no traffic during the alert interval but there was traffic in the previous 48 hours per server IP.
Policy Changes Alert	Alert once a day if there have been any security policy changes.
Queries Running Long Time	Notify if a query takes more than 900 seconds to run.
Scheduled Job Exceptions	Alert every 10 minutes on any scheduled job exception (including assessment jobs).

Parent topic: Managing your Guardium system

Scheduling

The general purpose scheduler is used to schedule many different types of tasks (archiving, aggregation, workflow automation, etc.).

Depending on the type of task being performed, not all of the features described here may be available - for example, the schedules for some types of tasks can be paused, while others cannot be (they can only be stopped or started).

Note: Be aware of scheduling anomalies that can occur when scheduling tasks during Daylight Savings Time.

Define or Modify a Schedule

1. In a task (for example, Audit Process Builder), click Define Schedule or Modify Schedule to open the Schedule Definition panel.
2. Fill in the Start Time. The default is 12 a.m. (Midnight).
3. Optionally, to run the task more than once a day:
   - Select a value from the Restart list (every hour up to every 12 hours). The default is Run only once, meaning the task will not be restarted during the day.
   - Select a value from the Repeat list (every minute up to every 59 minutes). The default is Do not repeat.
4. From the Schedule by list, select one of the following:
   - Day/Week to define a schedule based on one or more days of the week (Monday, Tuesday, Wednesday, etc.).
   - Month to define a schedule based on one or more days of the month, for every month or specific months.

   If you selected Day/Week from the Schedule by list, mark each day of the week you want the task run, or click Every day to select all days (or to clear all days if they are already selected).

   OR

   If you selected Month from the Schedule by list, do one of the following:

   - To select a numbered day (the 15th, for example):
     - Select the Day button.
     - Select a day: 1-31, depending on the month selected.
     - Select Every month, or one or more specific months.
   - To select a weekday occurrence within the month (the first Monday, for example):
     - Select the button.
     - Select a week relative to the start of the month: First, Second, Third, etc.
     - Select a weekday: Sunday, Monday, Tuesday, etc.
     - Select either Every month, or one or more specific months.
5. From the Schedule Start Time list, select the hour and minute at which you want to run the task. If a time is chosen earlier than NOW, the Scheduler Start Time will revert to NOW.
6. Click Apply.

Pause a Schedule

Note: Note that not all types of scheduled tasks provide a pause option.

1. Click Pause and
2. Confirm the action.

Remove a Schedule

After a schedule has been defined, a Remove button appears in the Schedule Definition panel.

1. Click Define Schedule or Modify Schedule to open the Schedule Definition panel.
2. Click the Delete button.

Parent topic: Managing your Guardium system

Aliases

Create synonyms for a data value or object to be used in reports or queries.

Aliases Overview

An alias is used to display a meaningful or user-friendly name for a data value.

For example, *Financial Server* might be defined as an alias for IP address 192.168.2.18. Once an alias has been defined, users can display report results, formulate queries, and enter parameter values using the alias instead of the data value.

Aliases can be defined in a number of ways:

- Through the IP-to-Hostname Aliasing tool - use this tool to generate aliases for discovered client and server IPs.

  Click Protect > Database Intrusion Detection > IP-to-Hostname Aliasing to open the IP-to-Hostname Aliasing tool.

- Through the Alias Builder – use this method to define aliases manually.

  Open the Alias Builder by clicking Comply > Tools and Views > Alias Builder.

- Through a query.
- While using the Group Builder, with the Alias Quick Definition.
-

Note: Aliases changes on the Central Manager or managed units will not be available on other systems until either GUI is restarted or any aliases changes are made through their GUI.

IP-to-Hostname Aliasing

One of the more common applications of aliases is to use them as synonyms for IP addresses. Use this tool to schedule the discovery of client and server IP's and generate aliases for them.

1. Open the IP-to-Hostname Aliasing tool by clicking Protect > Database Intrusion Detection > IP-to-Hostname Aliasing.
2. Check the Generate Hostname Aliases for Client and Server IPs (when available) check box.
3. Check the Update existing Hostname Aliases if rediscovered check box if you want the tool to continually look for and update hostname aliases.
4.
5. Click Apply to save your configuration, then schedule the operation.
    - Click Run Once Now to start the tool immediately.
    - Click Define Schedule... to schedule the tool in the future.
    - Click Pause to pause the generation of client and server IPs aliases.

Alias Builder

Use this method to manually create an alias.

1. Open the Alias Builder by clicking Setup > Tools and Views > Alias Builder.
2. Select the attribute type for which you want to define aliases.
3. Filter your search on that attribute type using the Value and Alias fields and click Search.
4. If any results match your search, they will display in the value and alias table. Click Apply for the search results, or add a new alias by specifying a Value and Alias name, then clicking Add.
5. Add a comment to an alias by clicking the Item Comments icon  . This can be helpful for quickly referencing what an alias refers to in the future.

Define Aliases Using a Query

Use this method to create aliases from a query. When a custom table has been uploaded to Guardium®, that table can be used to map aliases to specific values.

1. Open the Alias Builder by clicking Setup > Tools and Views > Alias Builder.
2. Select the attribute type for which you want to define aliases from the Alias Finder and click Populate from Query to open the Builder Alias From Query Set Up panel.
3. Fill out the required information and click Save to save the alias.
    - Select the query to be run from the Query menu.
    - Choose a value for both Choose Column for Value Column and Choose Column for Alias Column.
    - After selecting column values, more fields display that you must fill in (From Date, To Date, Remote Source, and any additional parameters for the selected query).
    - Check the Clear existing group members before Importing check box to delete the existing content of the group before populating from query.
    - Click Save to save.
    - With the query saved, the Scheduling buttons become active. Click Modify Schedule to run the query in the future, or click Run Once Now to run it immediately.

Alias Quick Definition from Group Builder

Use this method to create an alias for a group on the fly while creating or populating a group.

1. Open the Group Builder by clicking Setup > Group Builder. Select any group from the list, and click Modify.
2. Click Aliases... to open the Alias Quick Definition window. Type in an alias for any group(s), and save the alias by clicking Apply.

GuardAPIs for Aliases

Use these GuardAPI commands to create, update and delete alias functions:

- grdapi create_alias
- grdapi update_alias
- grdapi delete_alias

Parent topic: Managing your Guardium system
Related information:
Advanced Guardium system management and configuration (video)

Dates and Timestamps

Use a calendar tool to select an exact date, and a relative date picker to select a date that is relative to the current time.

There are two tools that are used to populate date fields: a calendar tool to select an exact date, and a relative date picker to select a date that is relative to the current time (now -1 day, for example). In addition, exact or relative dates can be entered manually.

Be aware that when selecting or entering dates, the date on the system on which you are running your browser may not be the same as the date on the Guardium® appliance to which you are connected.

Timestamps in Queries

Caution need to be taken when including Timestamps in queries.

First, be aware of the distinction between a timestamp (lowercase t) and a Timestamp (uppercase T).

- A timestamp (lowercase t) is a data type containing a combined date-and-time value, which when printed displays in the format yyyy-mm-dd hh:mm:ss (e.g., 2005-07-17 15:40:25). When creating or editing a query, most attributes with a timestamp data type display with a clock icon in the Entity List panel.
- A Timestamp (uppercase T) is an attribute defined in many entity types. It usually contains the time that the entity was last updated.

Including a Timestamp attribute value in a query will produce a row for every value of the Timestamp. This may produce an excessive amount of output. To get around this, use the count aggregator when including the Timestamp in a query, and then drill down on a report row, to view the individual Timestamp values for the items included in

that row only, in a drill-down report. See Aggregate Fields in Queries.

When displaying a Timestamp value in a query that contains Timestamp attributes in multiple entities, be careful to select the Timestamp attribute from the appropriate entity type for the report. For example, if the query will display information from both the Client/Server and the Session entities, with the Session selected as the main entity, you can display a Timestamp attribute from one or both entities. If you include the Client/Server Timestamp, you will see the same value printed for every Session for a given client-server connection – it will always be the time at which that particular Client/Server was last updated. If you include the Timestamp attribute from the Session, you will see the time that each Session listed was last updated.

Tip: If your report displays times that are all the same when you expect them to be different, you have probably included a Timestamp attribute from an entity too high in the entity hierarchy for the level of detail you want on the report.

Select an Exact Date from Calendar

To use the Calendar Window to select an exact date:

1. Click the Calendar button for the field where you want to insert a date. This opens a calendar in a separate window.
    - Click the arrow buttons to display the previous or next month in the calendar window.
2. Click on any date to select that day. The calendar window will close and the selected date will be inserted into the date field next to the calendar tool that was clicked.
   Note: The default time for a date selected using the calendar is always 00:00:00 (the start of the day). To specify any other time of day, type over this value, entering the desired time in 24-hour format: hh:mm:ss, where hh is the hour of the day (0-23), and mm and ss are minutes and seconds respectively (both 0-59).

Enter an Exact Date Manually

1. Click the field where you want to enter the date and enter the date in yyyy-mm-dd format, where:
    - yyyy is optional and may be any positive integer value. If omitted, yyyy defaults to the current year. If a one- or two-digit year is entered, the century portion of the date defaults to 19.
    - mm is the month (1-12)
    - dd is the day of the month (1 to 28, 29, 30, or 31, depending on the month)
2. If no time is entered, the time defaults to 00:00:00 (the start of the day). To specify any other time of day, type over this value, entering the desired time in 24-hour format: hh:mm:ss, where hh is the hour of the day (0-23), and mm and ss are minutes and seconds respectively (both 0-59).

Select a Relative Date from Date Picker

Rather than specify an exact date, it is often more convenient to specify dates relative to either the current date (now) or some other date (the first Monday, for example). For example, to always include information from the previous seven days in a query, it's more convenient to define relative dates (e.g., start = now minus seven days and end = now). The Relative Date Picker tool can be used to select a relative date for many types of tasks.

1. Click the Relative Date Picker button next to any field where a relative date is allowed. This opens the Relative Date Picker window.
2. Select Now, Start, or End from the list. Regardless of your choice, the display changes to provide for additional selections.
3. From the middle list, select this, last, or previous, which is relative to the unit (day, week, month, or day of the week selected in the next list) as follows:
    - This is the current unit
    - Last is the current unit minus one
    - Previous is current unit minus two
4. Select the day, week, month, or a specific day: Monday-Friday.
5. Click the Accept button when you are done. The relative date will be inserted into the field next to the Relative Date Picker button that was clicked.
6.

Enter a Relative Date Manually

To enter a relative date manually, follow one of the procedures. The keywords are not case sensitive but each component must be separated from the next by one or more spaces.

There are three general formats you can use to enter a relative date:

NOW minus a specified number of minutes, hours, days, weeks, or months

OR

The Start or End of the current, last or previous day, week, or month

OR

The Past or Previous day of the week (Sunday, Monday, Tuesday, etc.)

Relative to NOW

1. Click in the field where you want to enter the relative date.
2. Enter the keyword NOW.
3. Enter a negative integer specifying the relative number of hours, days, weeks, or months (no space is allowed between the minus sign and the integer).
4. Enter a keyword for the units used: HOUR, DAY, WEEK, or MONTH. Be aware that the plural (hours, days, etc.) is not allowed. Example: now -14 day

Relative to a Day, Week or Month

1. Click in the field where you want to enter the relative date.
2. Enter the keywords START OF or END OF.
3. Enter THIS or LAST, followed by DAY, WEEK, or MONTH. Example: end of last week

Relative to a Day of the Week

1. Click in the field where you want to enter the relative date.

2. Enter the keywords START OF or END OF.
3. Enter LAST or PREVIOUS, followed by SUNDAY, MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY, or SATURDAY. Example: start of previous Tuesday

Parent topic: Managing your Guardium system

Time Periods

Use the Time Period Builder to create time periods that can be used for policy rules and query conditions.

When monitoring database activity, use time periods to specify when you want to monitor. Use the Time Period Builder to create new time periods or modify existing ones.

Add a Time Period

1. Navigate to the Time Period Builder by clicking Setup > Tools and Views > Time Period Builder.
2. Expand the Add Time Period pane by clicking the + button.
3. Fill in the information and click Add to add the time period.
    - Do not include apostrophe characters in the Time Period Description.
    - Check the Contiguous check box to define a single time period that may span multiple days. A workweek is defined as contiguous, whereas a workday is defined as non-contiguous.

Remove a Time Period

1. Navigate to the Time Period Builder by clicking Setup > Tools and Views > Time Period Builder.
2. Check the check box for the time period you want to remove, and click Delete.

Parent topic: Managing your Guardium system

Time Periods

Policy rules and query conditions can test for events that occur (or not) during user-defined time periods.

There is a set of pre-defined time periods (7x24, After Hours Work, Before Hours Work, Evening, Regular Work Day, Saturday, Sunday, and Week End), and users can define their own.

Add a Time Period

1. Navigate to the Time Period panel:
    - Setup> Tools and Views > Time Period builder
2. Expand the Add Time Period pane by clicking the + button.
3. Enter a unique description for the period in the Time Period Description box. Do not include apostrophe characters in the description.
4. Optionally mark the Contiguous box to define a single time period that may span multiple days. Leave this box cleared to define a fixed time period on one or more days.

   Example: Contiguous vs. Non-Contiguous Time Periods

   The following two time periods both begin 09:00 Monday and end 17:00 Friday:
    - Workweek is defined Contiguous.
    - Workday is defined Non-Contiguous.

   The first time period, Workweek, defines a single 164-hour period beginning at 9 AM on Monday and ending at 5 PM on Friday, whereas the second time period, Workday, defines five separate eight-hour time periods (9 AM – 5 PM), on five consecutive days (Monday – Friday)
5. Enter a beginning time in hours (00-24) and minutes (00-59) in the Hour From box.
6. Enter an ending time in hours (00-24) and minutes (00-59) in the Hour To box.
7. Select a beginning day of the week in the Weekday From box.
8. Select an ending day of the week in the Weekday To box.
9. Optionally click the Comments button to add comments (see Commenting).
10. Click the Add button.

Remove a Time Period

1. Navigate to the Time Period panel:
    - Setup> Tools and Views > Time Period builder
2. Mark the Select checkbox for the time period you want to remove.
3. Click the Delete button. You will be prompted to confirm the deletion. Note that you cannot delete a time period that is used by an existing policy rule.

Parent topic: Managing your Guardium system

Comments

Comments apply to definitions and to workflow process results.

Comments can be added or viewed in several places throughout the UI. You can add a comment to a group or alias for reference purposes, or add a comment to report to ease auditing requirements. For example, an auditor may want to know why a configuration change was made on a certain date. Use a comment to easily reference the reason why the change was made.

Comments apply to definitions (groups, aliases, reports, policies), and to workflow process results. You can add multiple comments to a component, and you can add comments to comments, but you cannot modify or delete existing comments.

There are two different kinds of comments:

- **Comments Entities** are stored on the Central Manager, and will be available within that Central management environment, given the usual constraints regarding roles and permissions.
- **Local Comments Entities** are defined on a single unit, and remain local to that unit. Local Comments from the standalone or managed unit are not stored on the Central Manager.

Add or View Comments

1. To view comments, open the User Comments window by clicking Comply > Reports > User Comments.
2. Throughout the UI, there are different ways to add a comment to an entity or report.
   - Add a comment to a group by modifying the group, and clicking Add Comments from the Manage Members for Selected Group screen.
   - Add a comment to an alias by opening the Alias Builder and clicking the Item comments icon  . Open the Alias Builder by clicking Setup > Tools and Views > Alias Builder

Report Comments

View a report of all user comments by clicking Comply > Reports > User Comments.

- The Local Comments entity is used in a Central Manager environment only. Local comments remain local to the system on which they were defined, and are not stored on the Central Manager.
- The Comments entity contains comments that are stored on the Central Manager.

Parent topic: Managing your Guardium system

How to install patches

Install a single patch or multiple patches as a background process.

About this task

Use this topic to provide visibility and control over patch installation, status and history.

See Central Management for more information.

This how-to topic uses a combination of commands from the CLI and choices from the GUI to help you install the latest Guardium patch. The Guardium system must be rebooted after installing a patch.

Important: Patches downloaded in ZIP format must be unzipped outside the Guardium system before uploading and installing. Observe the following restrictions for any patch with database structure changes:

- Perform or schedule the patch installation during quiet time on the Guardium system to avoid conflicts with long-running processes such as heavy reports, audit processes, backups, and imports.
- The exact time required for patch installation depends on database utilization, data distribution, and other considerations.
- Install patches in a top-down manner, first patching a central manager before patching aggregators and finally collectors.

In the procedure below, you will follow these steps from the Guardium system that is designated and configured as the Central Manager:

1. Backup the system profile, using the CLI command store backup profile.
2. Enter the CLI command store system patch install to install a single patch or multiple patches to the Central Manager from a network location.
3. Click Setup > Tools and Views > Patch Distribution to move patches from the CM to managed units.

Procedure

Backup the system profile

1. Using a SSH client, log into the IBM Security Guardium Central Manager as the CLI user.
2. Enter the following command: store backup profile
3. The following dialog will appear:

```
Do you want to setup for automatic recovery? (Y/n)
Enter the patch backup destination host:
Enter the patch backup destination directory:
Enter the patch backup destination user:
Enter the patch backup destination port if you have a special port for SCP operation, or press ENTER to use the default port:
Enter the patch backup destination password:
```

4. Use the following CLI command if the patch installation failed, patch revert failed, and the automatic restore failed or disabled. The following command gets the pre-patch backup file and restore it on the system. If the pre-patch backup file is currently located on the system, enter the file name. Otherwise, the pre-patch backup profile information is used to get the file.

```
CLI>show backup profile patch backup flag is 1 patch backup automatic recovery flag is 1 patch backup dest host is
patch backup dest dir is patch backup dest user is patch backup dest port is patch backup dest pass is CLI>restore pre-patch
backup
```

Install the patch(es) to the Central Manager

Note: A compressed patch file may contain multiple patches, but only one patch can be installed at a time. To install more than one patch, choose all the patches that need to be installed, separated by commas. Internally the CLI submits requests for each patch on the list (in the order specified by the user) with the first patch taking the request time provided by the user and each subsequent patch three minutes after the previous one. In addition, CLI will check to see if the specified patch(es) are already requested and will not allow duplicate requests.

5. Enter the following command:

```
store system patch install <type> <date> <time>
```

where <type> is sys, ftp, scp, or cd and <date> and <time> are the patch installation request date and time formatted as YYYY-mm-dd and hh:mm:ss. If date and time are not entered or if "now" is entered, the installation request time is NOW.

Table 1. Patch install type descriptions and parameters

Name	Description
sys	The sys option is for use when installing a second or subsequent patch from a compressed file that has been copied to the Guardium system by using this command previously. Use this option to apply a second or subsequent patch from a patch file that has been copied to the IBM® Guardium® system by a previous store system patch execution. Install from /var/log/guard/patches

ftp or scp	The ftp and scp options copy a compressed patch file from a network location to the Guardium system. To install a patch from a compressed patch file located somewhere on the network, use the ftp or scp option, and respond to the prompts as shown below.
	Important: Patches downloaded in ZIP format must be unzipped outside the Guardium system before uploading and installing. Observe the following restrictions for any patch with database structure changes:
	• Perform or schedule the patch installation during quiet time on the Guardium system to avoid conflicts with long-running processes such as heavy reports, audit processes, backups, and imports.
	• The exact time required for patch installation depends on database utilization, data distribution, and other considerations.
	• Install patches in a top-down manner, first patching a central manager before patching aggregators and finally collectors.
	
	`Please enter the following information for file transfer:`
	`Host to import patch from:`
	`User on (host name):`
	`Full path to the patch, including name (file name may use wildcard *):`
	`(LDAP password)Password:`
	`Enter the scp/ftp port if you need to use a special port, else just press Enter key to continue:`
	`The file transfer process can take a while to complete.`
	`Leave the terminal open and do not answer any questions until the transfer is complete.`
	`Starting transfer, please wait.`
	`The file transfer is complete.`
	`The backup profile is not set for saving the backup file when patch installation failed.`
	`If you want to save the backup file, please answer NO to the question and run CLI command store backup profile to set up the parameters.`
	`Do you want to continue (yes or no)? yes`
	`List the files in the patches directory:`
	`1. (name of file)`
	`Please choose patches to install (1-1, or multiple numbers separated by ",", or q to quit): 1`
	`Install item 1`
	`Patch has been submitted, and will be installed according to the request time, please check installed patches report or CLI (show system patch installed).`
	`Please don't forget to remove your media if necessary.`

cd	The cd option is for use in installing the patch from a DVD disk. To display a complete list of applied patches, see the Installed Patches report on the Guardium Monitor tab of the administrator portal. There is also an Available Patches report on this same Guardium Monitor tab. To install a patch from a DVD, insert the DVD into the IBM Guardium DVD ROM drive before executing this command. A list of patches contained on the DVD will be displayed.

- To delete a patch install request, use the CLI command `delete scheduled-patch`
- Patches remain after installation only on the Central Manager. Standalone or managed unit patch files ARE deleted after installation.
- To display the available patches: `show system patch available`
- To display the already installed patches and patches scheduled to be installed—showing date/time and the install status: `show system patch installed`
- Use the `fileserver` command to start an HTTPS-based file server running on the Guardium appliance. This facility is intended to ease the task of uploading patches to the unit, or downloading debugging information from the unit. Each time this facility starts, it deletes any files in the directory to which it uploads patches.
  Note: Any operation that generates a file, that the fileserver will access, should finish before the fileserver is started (so that the file is available for the fileserver).
  a. To start the file, enter the fileserver command: `fileserver`
  b. Starting the file server. You can find it at https://(name of unit)
  c. Press ENTER to stop the file server.
  d. Open the fileserver in a browser window, and to one of the following:
     - To upload a patch, click Upload a patch and follow the directions.
     - To download log data, click Sqlguard logs, go to the file you want, right-click on it, and download as you would any other file.
  e. When you are done, return to the CLI session and press **Enter** to terminate the session.

Use the UI to move the patch(es) from Central Manager to managed units

6. Click Setup > Tools and Views > Patch Distribution.

   The Patch Distribution button will open a new screen, display an available patch list with dependencies, and allow for the selecting of a patch and installing it to all selected units. The list of available patches is constructed out of the available patches and evaluating the currently installed patches on each of the selected units along with the dependency list of available patches. Patches available but not installable (a dependent patch is missing) are shown in the list as grayed out and cannot be selected. The selection of patch to install is a single selection - only one patch can be installed at a time. Once a patch is selected and the install button pushed a command is sent to all selected units to install that patch; this process of installing patches will happen in the background.

7. Navigate to Central Management > Central Management > Patch Distribution.
8. Click on Patch Installation Status. The Patch Installation Status screen will display for each unit, failed installations and discrepancies - situations such as having one patch being installed on part of the units only, regardless if it failed on other units or was not installed.

Results

The patched systems are now ready to be used; however, remember that the Guardium system must be rebooted after installing a patch.

Parent topic: Managing your Guardium system
Related information:
How to download and install a Guardium patch (video)

Support Maintenance

The Support Maintenance feature is password protected and can be used only as directed by Technical Support. Contact Technical Support if you require more information.

Parent topic: Managing your Guardium system

Product integration

You can integrate IBM Guardium with other products.

- Configure BIG-IP Application Security Manager (ASM) to communicate with Guardium system
  Use the Big-IP ASM (from F5 Networks) together with Guardium's real-time database activity monitoring to solve the problem of identity propagation between web application and database application server layers.
- Hadoop Integration
  This topic introduces fundamental concepts and processes for monitoring Hadoop data with Guardium.
- PIM Integration with Guardium DAM
  Privileged Information Management (PIM) helps organizations to automate and track the use of shared privileged identities and monitor the usage of these shared privileged identities.
- QRadar and Guardium integration
  QRadar and Guardium can work together in a two-way information flow to have the Guardium data protection policies updated automatically and nearly in real-time in response to security intelligence events from QRadar.
- OPTIM to Guardium Interface
  An OPTIM to Guardium interface, using Protobuf (Universal Feed Agent), sends Optim activity logs to Guardium.
- Combining real-time alerts and correlation analysis with SIEM products
  Distribute contextual knowledge of database activity patterns, structures, and protocols directly to the third-party database of the SIEM system.
- How to transfer sensitive data to InfoSphere Discovery
  Take sensitive data information, identified and classified in IBM Security Guardium and transfer that information to InfoSphere® Discovery.
- CEF Mapping
  The CEF standard from ArcSight defines a set of required fields, and a set of optional fields.
- LEEF Mapping
  Log Event Extended Format (LEEF) from QRadar

Configure BIG-IP Application Security Manager (ASM) to communicate with Guardium system

Use the Big-IP ASM (from F5 Networks) together with Guardium's real-time database activity monitoring to solve the problem of identity propagation between web application and database application server layers.

This solution uses Google's protocol buffers (.protobuf) as the wire format between BIG-IP ASM and the Guardium® system.

Information about configuring the integration between Big-IP ASM and Guardium real-time database activity monitoring is provided at the F5 website: http://www.f5.com/pdf/deployment-guides/ibm-guardium-asm-dg.pdf.

Parent topic: Product integration

Hadoop Integration

This topic introduces fundamental concepts and processes for monitoring Hadoop data with Guardium.

Capacity planning

The following sizing guidelines assume an average volume of audited traffic. Higher volumes of audited traffic may require additional resources.

- 10 management or server nodes per collector
- 20 or more data nodes per collector, where S-TAPs are required for the data nodes (S-TAPs are not required for all components)
- Possibly additional nodes per collector if physical appliances are used

It is also possible to size by the Processor Value Unit (PVU) of the nodes, but this may result in over-sizing if auditing low volumes of traffic. The capacity sizing guideline is 4000 PVU per collector.

Integration scenarios

If you are using SSL encryption with Cloudera, see Hadoop integration using Cloudera Navigator.

If you are using SSL encryption with a Hortonworks Hadoop cluster, see Hadoop integration using Hortonworks and Apache Ranger.
Note: Redaction of returned data using Hive is not supported. If you require data redaction with Hive, see Hadoop integration using a standard Guardium S-TAP.

If you do not require SSL encryption for your Hadoop cluster, see Hadoop integration using a standard Guardium S-TAP.

- Hadoop integration using a standard Guardium S-TAP
  Learn how to integrate Hadoop using a standard Guardium S-TAP for HDFS and MapReduce monitoring.
- Hadoop integration using Cloudera Navigator
  Learn how to integrate Haddop using Cloudera Navigator, Cloudera's native data governance solution.
- Hadoop integration using Hortonworks and Apache Ranger
  Apache Ranger, included with the Hortonworks Data Platform, offers fine-grained access control and auditing over Hadoop components such as Hive, HBASE, and HDFS by using policies.

Parent topic: Product integration
Related information:

S-TAP configuration parameters for Hadoop

Hadoop integration using a standard Guardium S-TAP

Learn how to integrate Hadoop using a standard Guardium S-TAP for HDFS and MapReduce monitoring.

Hadoop deployments include two fundamental components:

- Hadoop Distributed File System (HDFS), which is stores data
- MapReduce or MapReduce 2), which provides a framework for accessing and analyzing data

Capturing activity on these two components covers basic auditing requirements because all data except management console traffic goes through HDFS.

Be aware that HDFS activity is not auditor-friendly, as it is somewhat like monitoring file access in a relational database. Consider monitoring activity from other components used in your environment, such as Hive, Big SQL, or Impala. These components support monitoring that more closely resembles database accesses.

Redaction and blocking policies

Guardium supports redaction using extrusion rules and blocking using S-GATE Terminate for Hive and Impala. Blocking for BigSQL was supported in V9.x when the S-TAP is used.

For detailed instructions on using redaction and blocking policies with Hadoop, see the IBM Security Guardium Deployment Guide for Hadoop Systems.

Kerberos

Guardium supports the use of Kerberos secure clusters with some restrictions. In order to decrypt Kerberos user IDs, Guardium requires that keytab files be generated and placed in a specific location. Detailed instructions are available in the IBM Security Guardium Deployment Guide for Hadoop Systems.

Attention: Kerberos configuration may be required only if you are using HBase or Hive.

- Recommendations and limitations
  Several recommendations and recommendations should guide your Guardium and Hadoop integration.
- S-TAPs and inspection engines with Hadoop
  Deploy Guardium S-TAPs and configure inspection engines for use with Hadoop.
- Guardium policies and rules with Hadoop
  Begin creating Guardium policies and rules for monitoring Hadoop activity.
- Guardium reporting with Hadoop
  Use built-in Guardium reports for Hadoop or define custom reports using Hadoop objects and commands.

Parent topic: Hadoop Integration

Recommendations and limitations

Several recommendations and recommendations should guide your Guardium and Hadoop integration.

Deployment recommendations

To avoid flooding the collector and to make problem diagnosis simpler, consider the followin tactics to reduce the amount and types of traffic processed by the Guardium collector:

- To limit data that must flow across the network to the appliance, restrict the number of inspection engines you configure.
- To limit the amount of data that is logged on the collector, put conditions on the policy.

One strategy might be to configure and test with Hive command line queries before adding additional inspection engines and opening the policy to additional, higher-volume traffic such as HDFS.

For each new inspection engine that is configured, you must restart S-TAP.

Remember to monitor the Guardium system as more services generate traffic. The Guardium deployment redbook includes details on how to monitor the system and make sure the traffic is not excessive for the collector.

Limitations

The following restrictions apply when monitoring Hadoop with a standard Guardium S-TAP:

- SSL encryption is not supported unless using Hortonworks with Ranger or Cloudera with Cloudera Manager. Ranger and Cloudera Manager integration is covered in a separate section of this information.
- UID chaining is not supported.
- Blocking and redaction is only supported for Big SQL, Hive, and Impala.
- Configuration audit system and sensitive data discovery are not supported at this time.
- Guardium currently does not support administration command auditing, for example starting and stopping services.
- Guardium load balancing and failover options are not supported when using Kerberos, however F5 or other load balancing in which a virtual IP address is used may be an option.

Considerations for IBM InfoSphere BigInsights and Big SQL

Unlike most other Hadoop distributions, the following restrictions apply to Hadoop on GPFS and Big SQL.

Hadoop on PGFS (IBM Spectrum Scale)
: The GPFS deployment of BigInsights requires HDFS Transparency Connector.

Big SQL

An S-TAP must be installed on all nodes in which a Big SQL engine is installed. The support for Big SQL is comprehensive and is similar to what Guardium already supports for DB2.

If Kerberos or GPFS is used, you must configure a special communications exit on each Big SQL node. Guardium provides a dynamically loaded shared library that interacts with Big SQL, and Big SQL will invoke functions within that library at run time when it performs SQL and utility requests.
Restriction: Only monitoring and auditing are supported using the exit methodology with Big SQL: redaction and blocking are advanced features that are only supported using an S-TAP.

Parent topic: Hadoop integration using a standard Guardium S-TAP

S-TAPs and inspection engines with Hadoop

Deploy Guardium S-TAPs and configure inspection engines for use with Hadoop.

Deploying S-TAPs and GIM clients

Only S-TAP and GIM clients are needed since Guardium does not yet support CAS and database discovery for Hadoop. As with any S-TAP deployment, be sure to download the correct S-TAP for your operating system and kernel level.

Attention: An S-TAP is recommended for edge nodes, particularly if you are using them as a landing zone for data.

Configuring inspection engines

After S-TAPs are deployed, the appropriate inspection engines must be defined from the Guardium appliance. Inspection engines specify the traffic that is monitored from a particular S-TAP host. For example, on a particular S-TAP host, an inspection engine might indicate that Guardium should monitor traffic from ports 8032 and 60000. Inspection engines also specify the protocol to monitor, such as Hadoop or HTTP.

Before configuring inspection engines, work with the Hadoop administrator to gather the following information for each Hadoop node to be monitored:

- Hadoop node and service to be monitored
- port numbers for the services
- server IP addess (i.e. S-TAP host IP address)

Determine the inspection engine protocol based on the Hadoop node type and service as indicated in the following table.

Table 1. Inspection engine protocols for Hadoop nodes and services.

Hadoop node	Hadoop service	Inspection engine protocol
Namenode	HDFS node name	Hadoop
Namenode	HTTP port for WebHDFS	WEBHDFS
Namenode	Resource manager for YARN	Hadoop
Job tracker Note: This node is required only for MapReduce1.	MapReduce job tracker	Hadoop
HBase master	HBase master	Hadoop
HBase region	HBase region	Hadoop
hiveserver2	Thrift protocol messages	HIVE
Hive metastore	Thrift protocol messages, used for getting Impala and Hive database user from Hue. Note: Requires using a computed attribute.	HADOOP
Impala daemons	Impala	IMPALA
Impala	Impala from Hue	HIVE Note: Impala from Hue uses hiveserver2.
Management node	BigSQL server	DB2
Compute node	BiGSQL server	DB2
Hue node	Hue user interface with Oracle, MySQL, or PGSQL backend	HUE
Solr search node	Solr search	HTTP

For example, an HDFS name node might use port `8020`, the `Hadoop` protocol, and have a host address of `10.0.0.21`.
Given this information, you can configuring an inspection engine by navigating to Manage > Activity > Monitoring > S-TAP Control in the Guardium user interface, or by using Guardium API commands. An example Guardium API command might looks like the following:

```
grdapi create_stap_inspection_engine client=0.0.0.0/0.0.0.0 protocol=HADOOP
    ktapDbPort=8020 portMax=8020 portMin=8020 connectToIp=127.0.0.0 stapHost=10.0.0.21
```

Restrictions:

- Hive CLI is deprecated in Hadoop distributions and is not supported by Guardium.
- Impala requires configuring inspection engines for all nodes running an Impala daemon.
- HBase requires S-TAPs on all data nodes including the master node.
- If you are using Big SQL with Kerberos or GPFS, you must configure the S-TAP with the DB2_Exit, which is a safe and efficient way to capture Big SQL/DB2 encrypted traffic and/or GPFS. However, blocking and redaction are not supported in this scenario. Additional information about Big SQL support is available on IBM developerWorks for Guardium.

Additional examples and more detailed instructions are available in the IBM Security Guardium Deployment Guide for Hadoop Systems.
Parent topic: Hadoop integration using a standard Guardium S-TAP

Guardium policies and rules with Hadoop

Begin creating Guardium policies and rules for monitoring Hadoop activity.

For monitoring purposes, it is useful to think in terms of the user, the data object being monitored, and what actions or commands are being executed. In Guardium terminology, these are the *DB User*, the *object*, and the *verb* or *command*, respectively. These entities can be used in policy rules to trigger particular actions, such as real time alerts.

Guardium policy rule actions allow you to filter traffic for performance in addition to logging or alerting on policy violations. For Hadoop traffic, you cannot use session-level filtering actions such as *ignore S-TAP session*. This is because Hadoop does not do session-management in the same way as relational databases where you log into the database--which establishes a session--and then generate SQL traffic within that session before logging out. With Hadoop, each command is its own session and can spawn many more sessions as work is distributed throughout the cluster.

Guardium cannot usually catch failed logins for command line components, although Guardium can see failed logins from Hue and through IBM BigSQL.

You will get permission exceptions on the file system level, so you report on those using the exceptions domain.

Begin creating policies from the built-in Hadoop policy to ensure traffic is being captured. It's recommended that you test the default policy in a low traffic test environment, and you may even add one more access rules to restrict traffic to a single server type--such as Hive--to reduce the amount of noise you see. Once you are comfortable that traffic is flowing to the collector, you can clone the default policy and create one that aligns with your security and compliance requirements.

For detailed instructions and an example of policies for a production Hadoop environment, see the IBM Security Guardium Deployment Guide for Hadoop Systems.

Parent topic: Hadoop integration using a standard Guardium S-TAP

Guardium reporting with Hadoop

Use built-in Guardium reports for Hadoop or define custom reports using Hadoop objects and commands.

Guardium includes several built-in reports for Hadoop. To see the list of available reports, navigate to My Dashboards > Create a new dashboard and click Add Report. In the Add a Report window, type `hadoop` into the search field to see a list of available Hadoop reports.

Some of the built-in reports provide component-based reporting, which are useful when validating your configuration and that you are sucesfully catching traffic from the component. Other reports are more focused on security and compliance, such as *Hadoop - Permissions report*, *Hadoop - Privileged users accessing sensitive objects*, *Hadoop - Exception report*, and *Hadoop - User login*.

This section includes lists of objects and commands or verbs used with Hadoop. You can cut and paste the commands into a group in Guardium using the Group Builder tool. You will also need to create groups of users and objects based on your own environment.

Hadoop objects

- HDFS files/directories
- MapReduce 2 job name

  Prior to MapReduce 2, the MapReduce job name was not logged as a separate object, but you could obtain it by using the built in MapReduce report and its computed attributes to get the job name from the full message.
- IBM Big SQL, Impala, Hive, HBase table and view names

HDFS commands

Read commands for HDFS:

- getFileInfo
- getBlockLocations
- getFileLocation
- getListing

Write commands for HDFS:

- addBlock
- complete
- create
- delete
- mkdirs
- rename

HBase commands

Read commands for HBase:

- list
- scan

Write commands for HBase:

- createTable
- disableTable
- deleteTable
- multi

Typically, this is an insert/update command. With the Ranger integration deployment option, this is a put command.

- drop

Big SQL, Hive, and Impala objects and commands
: The Big SQL, Hive, and Impala query languages are like SQL and support the normal parsing and logging rules used with most other relational databases in Guardium. Many of these commands are already included in Guardium command groups, such as ALTER commands, CREATE commands, and administrative commands. The extent of SQL syntax support varies greatly among these distributions, with Big SQL having the most extensive support.

Parent topic: Hadoop integration using a standard Guardium S-TAP

Hadoop integration using Cloudera Navigator

Learn how to integrate Haddop using Cloudera Navigator, Cloudera's native data governance solution.

Guardium supports auditing for Cloudera Hadoop using a standard S-TAP. For more information, see Hadoop integration using a standard Guardium S-TAP.

Guardium also provides the capability to subscribe to audit events when Cloudera Navigator is configured with Kafka as an alternative logging destination. Audited activity is sent to a Kafka cluster where the Guardium S-TAP consumes the events and sends them to the Guardium collector appliance for parsing and logging. nce the data is in Guardium, it is highly protected and all normal Guardium functions can be used such as real time alerting and integration with SIEM, reporting and workflow, and analytics.

Compared to integration using a standard Guardium S-TAP, Cloudera Navigator integration supports SSL encryption for clients that access Hadoop data. When using Cloudera Navigator integration, data is decrypted before the Guardium appliance receives it.

Restriction: Guardium-based blocking is not supported for any Hadoop components when using Cloudera Navigator integration.

Prerequisites

Guardium integration with Cloudera Navigator requires the following minimum software release levels:

- IBM Security Guardium and S-TAP at V10.1.2 or later
- CDH 5.7, Cloudera Manager 5.8, and the version of Kafka included with those releases

Architecture and data flow

Rather than having an S-TAP reside on the Hadoop servers, the Cloudera Manager agent sends audit events from the Hadoop component logs to the Cloudera Navigator audit server. At that point, Cloudera Navigator writes the audit events to its audit database. To integrate with Guardium, establish Kafka as an additional logger: Guardium will gather event records from Kafka.

Configuration is quite flexible in that you can install the S-TAP on a node in the Hadoop cluster or on a separate server outside of the Hadoop cluster as long as that server has network connectivity to the Kafka cluster and the Guardium appliance. You can only specify one S-TAP per Kafka cluster, but that S-TAP can send traffic to multiple Guardium systems using standard high availability or load balancing techniques.

In this configuration, Cloudera Navigator produces the log events for each Hadoop component, and the S-TAP consumes those events. Using the Guardium user interface, you will be specifying the message topic identifier that Cloudera Navigator uses so that the Guardium S-TAP knows which events it is supposed to pick up.

Recommendation: Use a secure Kafka cluster to ensure that your audit events are secure.

- Planning the integration with Cloudera Navigator
  Complete and verify the tasks in this topic before configuring the integration.

Parent topic: Hadoop Integration
Related information:
S-TAP configuration parameters for Hadoop

Planning the integration with Cloudera Navigator

Complete and verify the tasks in this topic before configuring the integration.

Integrating with Cloudera Navigator requires gathering some information from the administrators responsible for Cloudera and Kafka as well as from the data security team responsible for Guardium. Gather the following information before you begin:

- Host and ports for the Kafka bootstrap servers
- Whether TLS and Kerberos are used in the Kafka cluster.
- The host and port for the server where the S-TAP is installed. Verify that there is network connectivity between this server and both the Kafka cluster and the Guardium system.
- The operating system and version used on the S-TAP host so you can download and install the correct S-TAP.
- The host for the Guardium system. This is required for installing and configuring the S-TAP.

1. Configure the solution for monitoring
   This section describes how to configure the solution for monitoring.
2. Configure Guardium and Cloudera Navigator communication
   Learn how to establish communication between the Guardium system and Cloudera Navigator using a Kafka cluster.

Parent topic: Hadoop integration using Cloudera Navigator

Configure the solution for monitoring

This section describes how to configure the solution for monitoring.

Procedure

1. Configure the Cloudera Navigator auditing component.

   For more information, see the Cloudera documentation and IBM Security Guardium Activity Monitoring for Cloudera Hadoop Using Navigator Integration.

2. Ensure that TLS/SSL is configured correctly for Kafka.

   The Kafka cluster you use for producing Cloudera audit events must not be configured to require SSL client authentication. For more information, see IBM Security Guardium Activity Monitoring for Cloudera Hadoop Using Navigator Integration.

3. Install the Guardium S-TAP on a server.

   Use any available method to install the S-TAP on the designated server inside or outside of the Hadoop cluster. In Guardium, navigate to Manage > System View > S-TAP Status Monitor to verify connectivity between the S-TAP and the Guardium system.

   For a reference of Hadoop related S-TAP configuration parameters, see S-TAP configuration parameters for Hadoop.

4. Configure publication of Cloudera Navigator audit events to Kafka.

   The Navigator administrator or full administrator must do this task from Cloudera Manager. For more information, see IBM Security Guardium Activity Monitoring for Cloudera Hadoop Using Navigator Integration.

5. Configure Guardium and Cloudera Navigator communication
6. Validate the configuration.

   After configuring the solution, return to Manage > System View > S-TAP Status Monitor and verify that the S-TAP status is still green. Inspection engine verification is not supported for Hadoop sources and will always indicate an *Unverified* status.

7. Install Guardium and Cloudera Navigator policies.

   For monitoring and auditing, there is virtually no difference in policy rules when using the Cloudera Navigator integration than when using the normal S-TAP monitoring for Hadoop. To begin, install a Guardium policy or use the default policy, run HDFS or Hive commands on the Cloudera cluster, and verify that you can see the traffic in a Guardium report. For more information, see IBM Security Guardium Activity Monitoring for Cloudera Hadoop Using Navigator Integration.

Parent topic: Planning the integration with Cloudera Navigator
Next topic: Configure Guardium and Cloudera Navigator communication

Configure Guardium and Cloudera Navigator communication

Learn how to establish communication between the Guardium system and Cloudera Navigator using a Kafka cluster.

About this task

Go to **Setup > Tool and Views > Hadoop Monitoring** then select the plus icon inthe **Add cluster information** tile,

Procedure

1. Navigate to Setup > Tool and Views > Hadoop Monitoring and click the plus icon in the Add cluster information tile.
2. Use the S-TAP host name menu to select an S-TAP that is connected to the Guardium system.
3. Provide a Topic name for the Kafka cluster.

   Unless this was changed in the Kafka cluster configuration settings, use `NavigatorAuditEvents` (default value).

4. Use the Bootstrap servers section to specify one or more Kafka nodes to take the initial connection from the Guardium S-TAP.

   Any nodes that are leaders of a partition for the topic will handle consumer requests. For the initial connections, it's best to specify more than one server to provide a failover in case one of the bootstrap servers is down.

5. If your Kafka cluster is configured with TLS, check the Enable TLS check box.
   Restriction: Guardium does not support Kafka clusters configured to require SSL client authentication.
6. If the Kafka cluster requires Kerberos authentication, check the Use Kerberos check box.
   a. Use the Principal filed to provide the Kerberos principal name for the S-TAP.

      For example, `guardium/FullyQualifiedDomainName@kerberosDomain`.

   b. In the Path to keytab file field, provide the full path to the Kerberos keytab file on the S-TAP server.

      For example, `/etc/krb.keytab`. Make sure the keytab is owned by the S-TAP user and group and is only readable by the user.

7. Click Save.

   The resulting tile will show that you have configured Hadoop monitoring and the S-TAP staus should be green.

Parent topic: Planning the integration with Cloudera Navigator
Previous topic: Configure the solution for monitoring

Hadoop integration using Hortonworks and Apache Ranger

Apache Ranger, included with the Hortonworks Data Platform, offers fine-grained access control and auditing over Hadoop components such as Hive, HBASE, and HDFS by using policies.

The audit data is written to both HDFS and to Solr (recommended). Guardium can integrate with Ranger in two ways:

- For auditing, Guardium acts as another logger source for Ranger Auditing. Audited activity is sent to the Guardium collector where it is parsed and logged. Once the data is in Guardium, it is highly protected in the hardened appliance, and all normal Guardium functions can be used such as real time alerting and integration with SIEM, reporting and workflow, and analytics.
- For blocking, Guardium extends Ranger access control policies, using what is known in Ranger as dynamic policies.

Unlike Hadoop integrations that rely on a standard Guardium S-TAP for monitoring and blocking, integration with Ranger supports SSL encryption between clients and Hadoop data. With Ranger integration, the data is decrypted before it is sent to the Guardium system for auditing. In addition to SSL support, Ranger integration using dynamic policies enables blocking support for more components than is supported using standard S-TAP.

Although you can use both inspection engines and Ranger integration in the same cluster, it is unlikely that you would use both approaches simultaneously. See Hadoop Integration for more information about selecting an integration path.

Prerequisites

Integration with Ranger requires the following:

- IBM Security Guardium 10.1 (S-TAP and Appliance)
- Hortonworks 2.3 or later with Ranger

Architecture and data flow

The important difference with this architecture is that the S-TAP is not collecting audit data directly from the Hadoop component; rather, it is the Ranger plugins that are writing the audit messages to log4j, which forwards them to S-TAP, which then sends the messages to the Guardium collector for logging, alerting, reporting, and analytics.

You must configure the S-TAP, by specifying log4j_reader_enabled=1, to turn on the Ranger integration.

The configuration is quite flexible in that you can install S-TAPs on more nodes. You can configure Ranger to send all component traffic to one S-TAP or you could specify, for example, that all HBase traffic goes to one S-TAP and Hive and HDFS goes to another.

Blocking is implemented by extending Ranger access control policies to honor blocking policy rules that are specified on the Guardium appliance. The actual implementation of blocking is performed as an access denial from Ranger. For more information about how blocking fits into the architecture and data flow and guidance for implementing blocking, see IBM Security Monitoring and Blocking for Hortonworks Hadoop Using Apache Ranger Integration.

- Planning the integration with Hortonworks and Apache Ranger
  Complete and verify the tasks in this topic before configuring the integration.
- Configure the solution for monitoring
  This section describes how to configure the solution for monitoring.

Parent topic: Hadoop Integration
Related information:
S-TAP configuration parameters for Hadoop

Planning the integration with Hortonworks and Apache Ranger

Complete and verify the tasks in this topic before configuring the integration.

Topology of S-TAPs and collectors

Determine the required topology:

- Number of collectors needed
- Components monitored by each S-TAPs

Some customers prefer to have one S-TAP for each component. At a minimum, we recommend one S-TAP for HBase and one S-TAP for everything else.
Tip: An S-TAP is not required to sit on the same node as any particular component. It's possible--and even advisable if supporting Hadoop HA--to establish a dedicated Linux box for an S-TAP.
When configuring the number of connections for an S-TAP, use the following rule of thumb:

- HBase: one plus the number of region servers
- Everything else: one plus one for each component monitored

Attention:

- For blocking, verify access to all HBase region servers, since you will need to copy the Guardium plugin JAR file to each of these region servers.

  For configuring high availability failover scenarios, record the failover node IP addresses or host names.

High availability and failover

Hadoop uses secondary nodes for high availability to handle data requests should the primary node fail. There are several options for S-TAP deployment so that you can continue to collect audit data in a failover scenario.

Install the S-TAP and set it up on a system that is not part of the Hadoop cluster
: This provides a simple configuration where, when the components fail over, the new node automatically uses the S-TAP as a remote logger. No changes are needed to any configurations or S-TAPs.

Use `localhost` for HDFS and Hive S-TAP and a separate system for HBase
: Install an S-TAP for HDFS and Hive using `localhost` in the S-TAP host field, then use a separate system such as an edge node for HBase. This provides an alternative to installing S-TAPs on all nodes and region servers and is the recommended approach.

Install the S-TAP on the nodes in the cluster
: In this model, you install an S-TAP on the primary and standby node for each component.

Using `localhost` in the S-TAP host field, install an S-TAP on every node in the cluster and every region server for HBASE. This is approach is not recommended.

Guardium load balancing

Guardium S-TAP and enterprise load balancing options are supported when Ranger integration is enabled.

Gather Ambari and Ranger information

A significant portion of setup is done through Ambari, the Hadoop administrative interface. To complete configuration, you will need the following information:

Ambari

- A user ID and password who has privileges to update and save the *log4j* configuration, such as a Service Administrator account. For simplicity, refer to this as the admin account and password.
- Port and IP address or hostname.
- Cluster name.

Ranger

The following information is only needed if configuring blocking. For more information about configuring blocking, see IBM Security Monitoring and Blocking for Hortonworks Hadoop Using Apache Ranger Integration.

- A Service Administrator account that can update and save the *log4j* configuration.
- Port and IP address or hostname.

Open the required ports

Ensure that the following ports are opened (assuming use of default ports):

- For monitoring, open port 5555 between the node(s) that S-TAP is on and the Ranger server.
- For blocking, open port 5556 to allow communication between S-TAP and all nodes in the cluster that have the Guardium plugin.

Parent topic: Hadoop integration using Hortonworks and Apache Ranger

Configure the solution for monitoring

This section describes how to configure the solution for monitoring.

Before you begin

Before you begin configuring Guardium communication with Ranger, configure the Ranger plugins using Ambari. Refer to the IBM Security Monitoring and Blocking for Hortonworks Hadoop Using Apache Ranger Integration guide or the Hortonworks documentation for details.

Two Hadoop auditing configuration settings are missing from documentation. Add the following steps to the install manual:

Configure Ranger plugin to write audit logs to log4j

HDFS

In section “Custom ranger-hdfs-audit” add:

xasecure.audit.destination.log4j=true

xasecure.audit.destination.log4j.logger=xaaudit

Hive

In section "Advanced ranger-hive-audit.xml" add:

xasecure.audit.destination.log4j=true

xasecure.audit.destination.log4j.logger=xaaudit

Configuring Ranger using the Python scripts is recommended over configuring Ranger from the GUI.

1. Configure Guardium and Ranger communication
   Learn how to establish communication between the Guardium system and Ranger.
2. Install and configure S-TAPs
   Install and configure S-TAPs for Ranger integration.
3. Enable monitoring for Hadoop services
   Enable monitoring for specific Hadoop components.

What to do next

Once you have completed these setup steps, install Guardium and Ranger policies. For monitoring and auditing, there is virtually no difference in policy rules when using Ranger than when using standard S-TAP monitoring for Hadoop. For more information, see IBM Security Monitoring and Blocking for Hortonworks Hadoop Using Apache Ranger Integration.

Parent topic: Hadoop integration using Hortonworks and Apache Ranger

Configure Guardium and Ranger communication

Learn how to establish communication between the Guardium system and Ranger.

About this task

This task describes how to establish communication between the Guardium system and Ranger.

Procedure

1. Navigate to Setup > Tools and Views > Hadoop Monitoring.
2. Click the  in the Add cluster information section to begin defining a new configuration.
3. Use the Name field to provide a name for the configuration.
4. Select `Hortonworks` from the Hadoop distribution menu.
5. In the Host name/IP field, provide the host name or IP address of the Ambari server.
6. In the Port number field, provide the Ambari server port number. If you leave this field blank, the configuration will use the default port of 8080.
7. In the Cluster name field, provide the Hadoop cluster name.
8. In the User name field, provide an Ambari administrator user name.
9. In the Password field, provide a password for the Ambari administrator account.
10. Click the Test Connection button to verify the configuration.
11. Click Save to save the configuration.

Results

The new configuration will be available from the Hadoop Monitoring page.
Parent topic: Configure the solution for monitoring
Next topic: Install and configure S-TAPs

Install and configure S-TAPs

Install and configure S-TAPs for Ranger integration.

Before you begin

Review Planning the integration with Hortonworks and Apache Ranger for information about S-TAP requirements and deployment options.

Procedure

1. Install S-TAPs and enable them for the Ranger integration. You may need more than one S-TAP to handle the traffic, for example configure one S-TAP on the name node for HDFS, Hive and Kafka traffic and one S-TAP on the HBASE master node for all HBase traffic.
2. Configure guard_tap.ini for auditing.
   a. Open guard_tap.ini in a text editor. You must edit the file directly, as there is no UI or GIM support for these settings.
   b. Add the parameters listed below. Update the values to reflect you

```
; Settings for log4j
logging log4j_reader_enabled=1
log4j_port=5555
log4j_listen_address=0.0.0.0
; Maximum number of connections to support from the log4j service
log4j_num_connections=50
```

   c. Restart the S-TAP after updating any settings.

Parent topic: Configure the solution for monitoring
Previous topic: Configure Guardium and Ranger communication
Next topic: Enable monitoring for Hadoop services
Related information:
S-TAP configuration parameters for Hadoop

Enable monitoring for Hadoop services

Enable monitoring for specific Hadoop components.

About this task

This task describes how to define which Hadoop components are enabled for monitoring with Guardium.

Procedure

1. Navigate to Setup > Tools and Views > Hadoop Monitoring.
2. To begin configuring services, click the  for a Hadoop cluster.
3. Use the Service menu to select the Hadoop component on which to enable monitoring.
4. Use the S-TAP host name / IP menu to select the S-TAP tat should collect audit events from Ranger.
5. In the Port number field, provide the listener port number. If you leave this field blank, the service will use the default port of 5555.
6. Select Activate monitoring immediately to enable monitoring for the selected services.
7. Click the Save button to save the services configuration.
   Attention: The Hadoop administrator must restart the Hadoop service to activate the changes made to the services configuration. Before restarting the service, have the administrator verify the following log4j configuration:

```
# Configuration for Guardium integration with Ranger log4j logging.
log4j.appender.guardlistener=org.apache.log4j.net.SocketAppender
log4j.appender.guardlistener.Port=5555
```

```
log4j.appender.guardlistener.RemoteHost=hw-cl5-01.guard.swg.usma.ibm.com
log4j.logger.xaaudit=ALL,guardlistener
```

Also have the Hadoop administrator verify the following settings in `custom ranger-<service>-audit`:

```
xasecure.audit.destination.log4j=true
xasecure.audit.destination.log4j.logger=xaaudit
```

Results

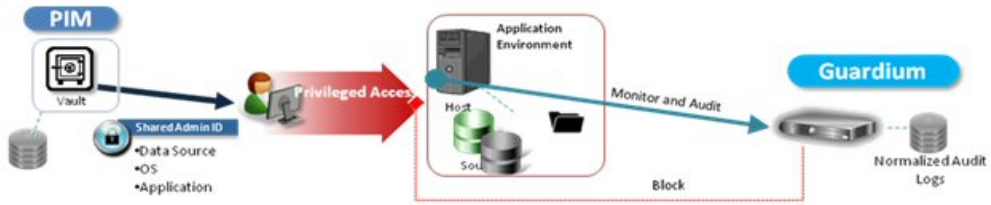
From the Hadoop Monitoring page, verify that the enabled services are marked with a green check mark icon.
Parent topic: Configure the solution for monitoring
Previous topic: Install and configure S-TAPs

PIM Integration with Guardium DAM

Privileged Information Management (PIM) helps organizations to automate and track the use of shared privileged identities and monitor the usage of these shared privileged identities.

The idea is to integrate PIM activity data with Guardium DAM data, in order to allow visibility to the actual user (person) that logged in to the database.

The diagram illustrates the integration.



The main purpose of this integration is:

- Provide visibility in the Guardium appliances to PIM data such as Lease history (who used the shared accounts), credentials and databases managed by PIM.
- Provide DAM information correlated with PIM information, for example, Guardium can show today's Database user along with actual requests issued by a specific user. This integration will allow use of both the Database user and the actual PIM user that leased the shared ID.

Installation

Guardium patch (v10.1p103) can be used to install PIM integration functionality. PIM integration can be used on standalone Guardium systems as well as in federated environments.

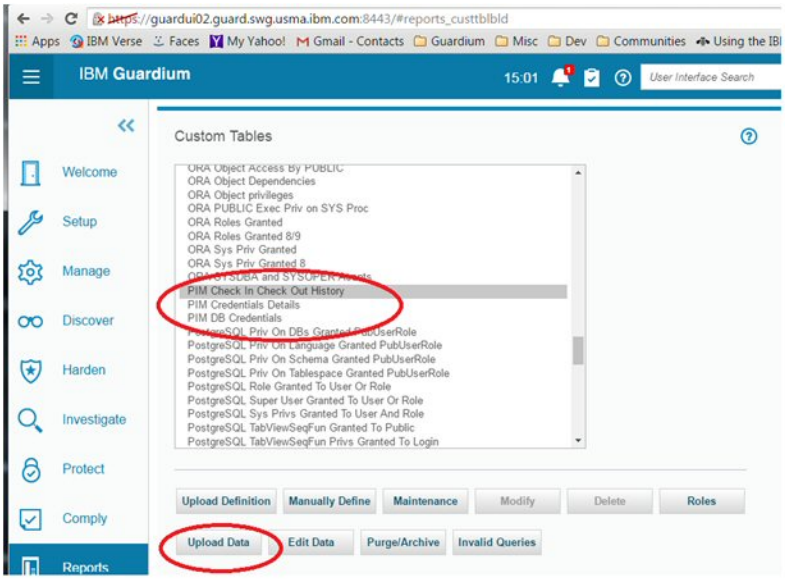
Note: It is assumed that the PIM activity data is already implemented.

Follow these steps

1. Bring data to the Guardium system.

   Select a datasource and then select from the Guardium UI: Reports > Report Configuration Tool > Custom Table Builder.

   Locate and select three PIM predefined tables and, for each one of them, schedule Automatic Data Upload.



   Upload PIM tables to Guardium System

   If using a Guardium Central Manager, select from the Guardium UI: Manage > Central Manager > PIM Data Distribution. Do this to schedule data distribution from the Central Manager to all managed units.

2. Once data is brought to the managed units, use this CLI command, store pim_correlation_mode, to enable correlation of PIM data with Guardium session data.

   CLI command

   store pim_correlation_mode

   Usage: store pim_correlation <state>

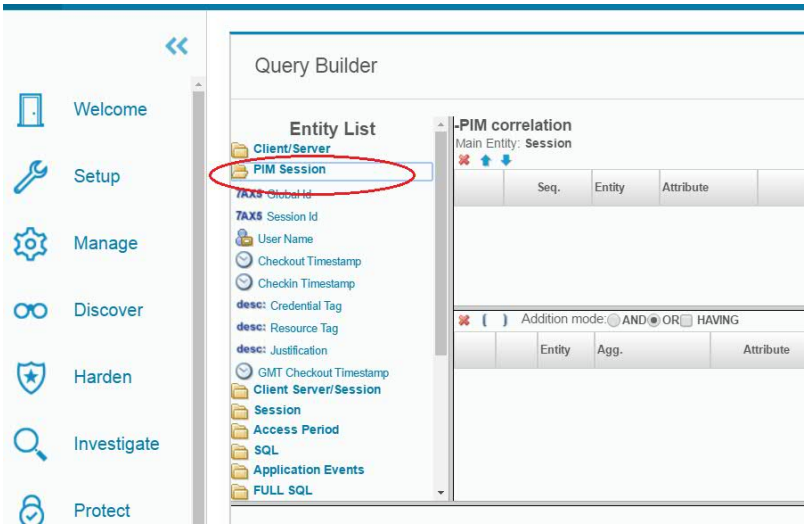
   where state is on/off. On is to enable and off is to disable.

   Show command

   show pim_correlation_mode

3. To run correlation , select from the Guardium GUI:Comply > Custom Reporting > PIM data correlation.

   Correlated data can be seen through reports in Access domain



PIM session in Access Domain

Parent topic: Product integration

QRadar and Guardium integration

QRadar and Guardium can work together in a two-way information flow to have the Guardium data protection policies updated automatically and nearly in real-time in response to security intelligence events from QRadar.

IBM QRadar is a security intelligence tool that provides threat protection by monitoring security information and events, using customizable rules to detect anomalies, as well as providing tools for incident forensics and vulnerability management.

IBM Guardium is a solution for data security and data privacy that helps ensure the integrity of data stored in servers. Guardium uses policies and inclusion/exclusion lists (called Guardium groups) to control access to data.

The QRadar and Guardium solution leverages the QRTrigger framework for triggering actions in response to QRadar security events. Based on configuration settings, QRadar events will cause new members to be added to Guardium groups based on information carried in the event itself. Furthermore the Guardium policy associated with the group is automatically reinstalled so that membership change takes effect immediately.

Note that the QRadar and Guardium solution can be used to update a single Guardium collector, or a group of them being controlled by a Guardium Central Manager (CM).

QRadar and Guardium together

Traditional QRadar and Guardium integration is a one-way information flow where Guardium sends alerts and Vulnerability Assessment (VA) reports to QRadar.

Common alerting use cases for databases:

- Failed logins
- Unauthorized access
- SQL Error codes (for example, SQL injection attacks)
- Users trying to escalate their privileges
- Users creating triggers and views to indirectly access sensitive data

Now QRadar and Guardium can work together in a two-way information flow.

Additional use cases:

- Block access from a machine that became compromised
- Increase audit levels for access by a user ID that became suspicious

- Increase audit levels for access by a privileged shared user ID that was on-boarded in a Privileged Identity Management (PIM) system

Updating Guardium policies based on QRadar events

The steps to deploying the QRadar and Guardium solution are:

1. Install the solution files.
2. Set up a client ID and secret in Guardium.
3. Configure a Forwarding Destination in QRadar.
4. Configure Rules to dispatch QRadar Events to the solution.
5. If necessary, define Guardium Groups and Policies for integration.

Note that Guardium version 10.1 and later has three predefined groups designed to support this integration:

- QRadarBlockingConnection
- QRadarAlertingConnection
- QRadarLogConnection

Each of these groups has the following tuple structure:

<Client IP>,<Src App>,<DB User>,<Server IP>,<Svc. Name>,<OS User>,<DB Name>

There is a predefined Guardium policy called "QRadarPolicy" with three rules: A blocking rule, an alerting rule, and a logging rule. Each rule is tied to its respective group from the list above.

How to install QRadar and Guardium solution

For complete instructions on installing the QRadar and Guardium solution, go to the IBM Developerworks article:

https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/W746177d414b9_4c5f_9095_5b8657ff8e9d/page/QRGuardium

Setting up Guardium

In order for the QRadar and Guardium solution to be able to authenticate to the Guardium REST API, a client ID must be registered in Guardium and the associated client secret retrieved.

Registering a client ID is done using the grdapi command line utility of Guardium. This operation is performed only once. The result of the client ID registration is a JSON entry containing details for the new client, including the client secret.

```
> grdapi register_oauth_client client_id=qrguardium
ID=0
{"client_id":"qrguardium","client_secret":"3ac89782-ce55-
4f24-b795-b6c76ecc4045",
"grant_types":"password","scope":"read,write","redirect_uri"
:"https://joeApp"}
ok
```

Troubleshooting logs

The QRadar and Guardium solution provides a number of log files to assist in managing and troubleshooting operations. These log files include:

Table 1. Log files

Pzrameter name	Description
guardiumEvents_audit.log	This an audit log of all changes made to Guardium based on QRadar events. Each line is a JSON object that includes identifiers, timestamp and details of the Event handled.
QRListener.log	Log output from the Listener process that receives forwarded event data from QRadar.
HANDLER_<event name>.log	Log output from the dedicated handler AL for a specific Event.
RESPONSE_<event name>.log	Log output from a custom response AL if this AL implements logging based on its AssemblyLine name. For example this can be done by setting the Log Appender File Path parameter to be computed using this Javascript: return “logs/” + task.getShortName() + “.log”;

Parent topic: Product integration
Related information:
Directory integrator integrations (video)

OPTIM to Guardium Interface

An OPTIM to Guardium interface, using Protobuf (Universal Feed Agent), sends Optim activity logs to Guardium.

The objective of this interface is to use Guardium auditing capabilities for OPTIM activities. The auditing capabilities include: Reporting tools (user-defined queries and reports); Audit Processes (workflow automation that enables assigning a task to a role/user/group, user-defined status-flow process, escalation, export...): and,

Thresholds Alerts.

The Optim-audit activity information includes the access details, session number, activity type (verb), table (object), details (fields), execution time (response time) and number of errors (records affected).

The data is mapped to the Guardium standard object model.

Enabling OPTIM auditing requires enabling via OPTIM and the steps required in Guardium are: (1) link user to Optim Audit Role; (2) add the predefined reports to the appropriate pane; (3) enable sniffer; and, (4) set policy action to Log Data With Values.

This interface includes an optim-audit role, a default layout (psml file) for the optim-audit role, and seven predefined reports.

These reports are:

- Optim - Failed Request Summary per Optim Server
- Optim - Request Execution per User
- Optim Server Optim - Table Usage Details
- Optim - Request Log
- Optim - Table Usage Summary
- Optim - Request Summary

Note: When creating the optim-audit role and user, only one tab OPTIM Audit will display. Similar to roles with custom layouts that customers can generate, this is a role layout that is meant to be used alone (the optim-audit user has no interest in the other user role tabs) but since the user role is required, layout merging has been turned off when the user has the optim-audit role so that they get only the items of optim interest. Other roles that work in this same way are "review-only" and "inv".
Note: After creating and saving the optim-audit role, click the Generate Layout selection within the User Browser menu and click Reset to get the layout associated with the role. Do this again if changing roles within the User Browser.

Parent topic: Product integration

Combining real-time alerts and correlation analysis with SIEM products

Distribute contextual knowledge of database activity patterns, structures, and protocols directly to the third-party database of the SIEM system.

About this task

Guardium® pre-processes large volumes of database traffic and distills important information. Then, it provides the condensed summary to external SIEM (Security Incident Event Manager) systems such as ArcSight, Envision, and QRadar. Thus, SIEM products do not have to work as hard to process large traffic streams. Rather, it can concentrate on correlating all activity, alerting on unauthorized or suspicious behavior, and helping with the regulatory compliance requirements on event logs.

This Guardium SIEM (Security Incident Event Manager) integration can be done in one of the following ways:

- Syslog forwarding (the most common method for alerts and events)
- Using the CLI command, store remotelog, to specify the Syslog forwarding to facility/priority, and host (destination).
- Using Guardium templates for ArcSight, Envision, and QRadar
- SCP/FTP (CSV or CEF Files sent to an external repository and the SIEM system must upload and parse from this external repository.)

Guardium distributes its contextual knowledge of database activity patterns, structures, and protocols directly to the third-party database of the SIEM system (Guardium has credentials to the SIEM system. It can also write directly to the SIEM database in the SIEM schema. Contact Guardium support as Guardium's entities must be mapped to the third-party schema.

Note: The SIEM system must enable remote logging as well to know to listen for the correct facility/priority which is defined within syslog.

By combining Guardium's real-time security alerts and correlation analysis with SIEM and log management products, companies can enhance their ability to:

- Proactively identify and mitigate risks from external attacks, trusted insiders, and compliance breaches;
- Implement automated controls from Sarbanes-Oxley (SOX), the Payment Card Industry Data Security Standard (PCI-DSS), and data privacy regulations;
- Manage system and network events alongside critical logs and events from the core of their data centers – enterprise databases and applications – for enterprise-wide correlation, forensics, incident prioritization, and reporting.

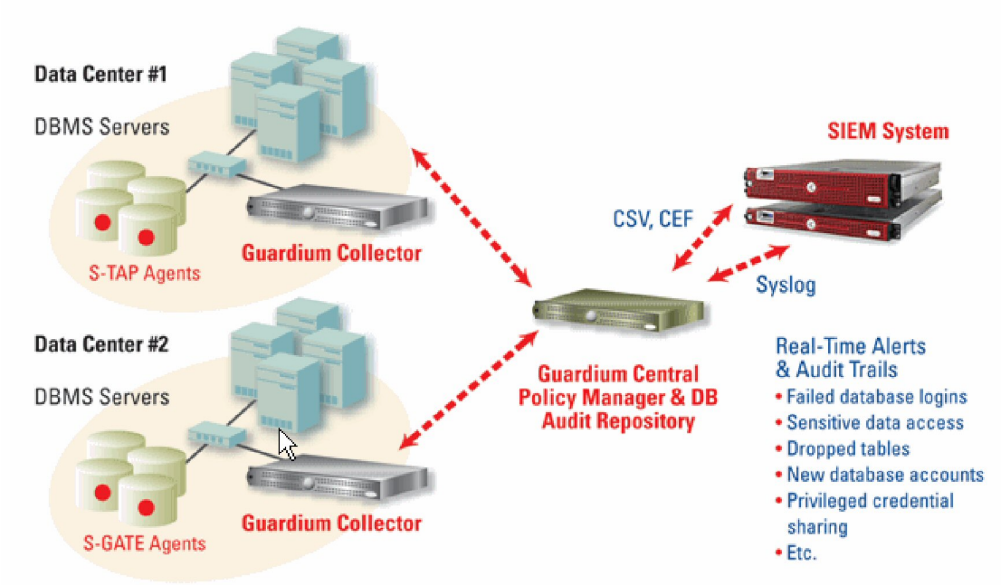
Security Information and Event Management (SIEM) solutions, also referred to as Security Event Management (SEM) solutions, are offered by companies such as QRadar, ArcSight, CA, Cisco MARS, LogLogic, RSA enVision and SenSage. SIEM products are complementary to Guardium's database activity monitoring solution. They can also use Guardium's filtering and preprocessing of database events to provide 100% visibility and database analytics for SOX, PCI-DSS, and data privacy.

SIEM technology provides real-time analysis of security alerts that are generated by network hardware and applications. It helps companies to respond to network attacks faster and to organize the massive amounts of log data that is generated daily. SIEM solutions are log-based correlation engines.

SIEM solutions are primarily focused on detection and security, but not on auditing. They assemble data from other logs and analyze it at a high level. They correlate much more data such as IP addresses and routers but have little database visibility. They do not have forensics-quality, digitally signed, audit monitoring capabilities so they can be used for immediate information, but not historical proof.

Security information and event management (SIEM) users are faced with the challenge of importing raw logs that are generated by internal DBMS utilities. The performance of DBMS logging utilities, the unfiltered information that they produce, and the lack of necessary granular information create challenges.

Through the Guardium user interface, Guardium can be configured easily to integrate with various SIEM tools.



Note: With SIEM integration, the reports and policies do not change on the Guardium system. Users can continue with their existing policies and reports, trigger alerts, and send reports to the SIEM system.

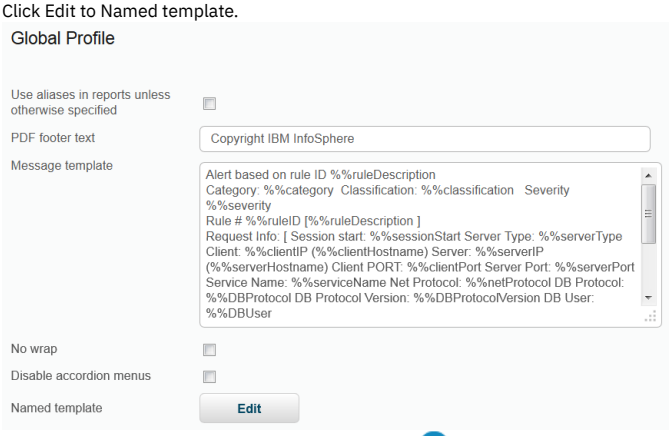
For SIEM-Guardium Integration, there are predefined templates for QRadar, Envision, and ArcSight so you do not need to define them. You can select the appropriate message template within the rule action.

You can change the default message template, specify the parameters for syslog forwarding, and create the CSV or CEF file to export.

Note: CEF is only used for ArcSight. The other SIEM products have a different format and do not use CEF.

In order for the SIEM product to recognize the information that is being sent, the message template must be changed through the Global Profile. This formatting agreement between the SIEM solution and Guardium allows SIEM products to parse incoming messages and update its own database with the new event/data.

1. To open the Global Profile, click Setup > Tools and Views > Global Profile.
2. Click Edit to Named template.



3. Select a template or create a new template with the Icon.

The Guardium appliance can be configured to send Syslog messages to remote systems. Specific types of Syslog messages can be sent to specific hosts. The Syslog message type is determined from the facility-priority of the message.

The following are examples of facility: all, auth, authpriv, cron, daemon, ftp, kern, local0, local1, local2, local3, local4, local5, local6, local7, lpr, mail, mark, news, security, Syslog, user, uucp. The following are examples of priority: alert, all, crit, debug, emerg, err, info, notice, warning.

Reports containing information that can be used by other applications or reports that contain large amounts of data can be exported to a CSV file format. Report, Entity Audit Trail, and Privacy Set task output can be exported to CSV (Delimiter-separated Value) files. Additionally, CSV file output can be written to Syslog. If the remote Syslog capability is used, the output CSV file is forwarded to the remote Syslog locations.

Each record in the CSV or CEF files represents a row on the report. Contact Guardium Support for a tool that permits the reformatting of CSV files before export.

The Guardium appliance can be configured to send Syslog messages to remote systems, using the store remotelog CLI command. Specific types of Syslog messages can be sent to specific hosts. The Syslog message type is determined from the facility-priority of the message.

Examples of facility are: all, auth, authpriv, cron, daemon, ftp, kern, local0, local1, local2, local3, local4, local5, local6, local7, lpr, mail, mark, news, security, Syslog, user, uucp. Examples of priority are: alert, all, crit, debug, emerg, err, info, notice, warning.

Reports containing information that can be used by other applications, or reports containing large amounts of data, can be exported to a CSV file format. Report, Entity Audit Trail, and Privacy Set task output can be exported to CSV (Delimiter-separated Value) files. Additionally, CSV file output can be written to Syslog. If the remote Syslog capability is used, this action results in the immediate forwarding of the output CSV file to the remote Syslog locations.

Each record in the CSV or CEF files represents a row on the report.

To send Syslog messages and export reports to CSV files, complete the following steps.
Note: Do not zip the file within the audit process definition so that the SIEM vendor can parse it correctly.

1. To open the Audit Process Finder, click Comply > Tools and Views > Audit Process Builder.
2. Click the Icon to add a process or select an existing process from the drop-down list.
3. Click New Audit Task under Audit Tasks.
4. Enter a description and select Report.
5. Select a report from the drop-down list and enter the CSV/CEF File Label.
6. Select Export CSV file and Write to Syslog. Choose a named template from the drop-down list.
7. Under Task Parameters, choose the Enter Period From >= and Enter Period To <= by using the calendar icon.
8. Click Apply.

CSV/CEF files can also be exported on a schedule to the SIEM host. Modify or add an audit task.

1. Click Comply > Tools and Views > Audit Process Builder to open the Audit Process Finder and modify or add an audit task.
2. Choose Export CSV file or Export CEF file.
   Note: ACCESS reports can be saved and forwarded in CEF or LEEF format but other reports, such as Guardium Logins, Aggregation Activity Log, and CAS events cannot be mapped to CEF or LEEF.
3. Uncheck the Write to Syslog. Otherwise, Syslog messages will be generated instead of a file.
4. Open the CSV/CEF Export menu by clicking Manage > Data Management > Results Export (Files).
5. Select either the SCP or FTP Protocol. Then enter the Host, Directory, Username, Port, and SCP/FTP password.
6. In the Scheduling section, define the Start Time, Restart frequency, Repeat frequency, Schedule by Day/Week or Month, Schedule Start Time. Check the box to automatically run dependent jobs.
7. Click Save to commit the changes or Reset to clear the fields.

To have a policy alert that is routed to Syslog, exception rules, access rules, and extrusion rules must be modified to trigger notifications to be sent to Syslog. This action can be accomplished by going to the Policy Builder. Policy rules can be sent as email or sent to Syslog and forwarded.

1. To open the Policy Builder, click Setup > Tools and Views > Policy Builder.
2. Select the policy and click Edit Rule.
3. Click Add Rule... > Add Exception Rule.
4. Enter the Description, Category, Classification, and select a Severity level from the drop-down list.

For every policy rule violation logged during the reporting period, the Policy Violations report provides the Timestamp from the Policy Rule Violation entity, Access Rule Description, Client IP, Server IP, DB User Name, Full SQL String from the Policy Rule Violation entity, Severity Description, and a count of violations for that row. With this report, users can group violations and create incidents, set the severity of each violation, and assign incidents to users.

Parent topic: Product integration

How to transfer sensitive data to InfoSphere Discovery

Take sensitive data information, identified and classified in IBM Security Guardium and transfer that information to InfoSphere® Discovery.

Both IBM Guardium and InfoSphere Discovery have the capability to identify and classify sensitive data, such as Social Security Numbers or credit card numbers.

A customer of the IBM Guardium product can use a bidirectional interface to transfer identified sensitive data information from one product to another.

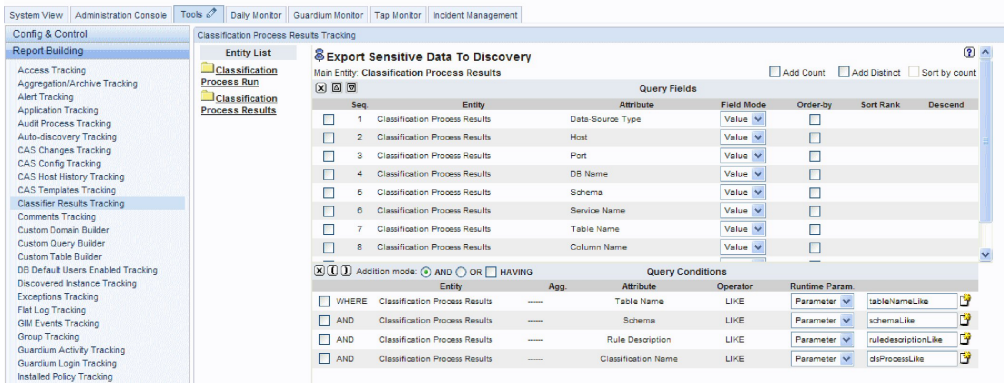
Note: In IBM Guardium , the Classification process is an ongoing process that runs periodically. In InfoSphere Discovery, Classification is part of the Discovery process that usually runs once.
Note: The data will be transferred via CSV files.

The summary of Export/Import procedures is as follows:

- Export from Guardium - Run the predefined report (Export Sensitive Data to Discovery) and export as CSV file.
- Import to Guardium - Load to a custom table against CSV datasource; define default report against this datasource.

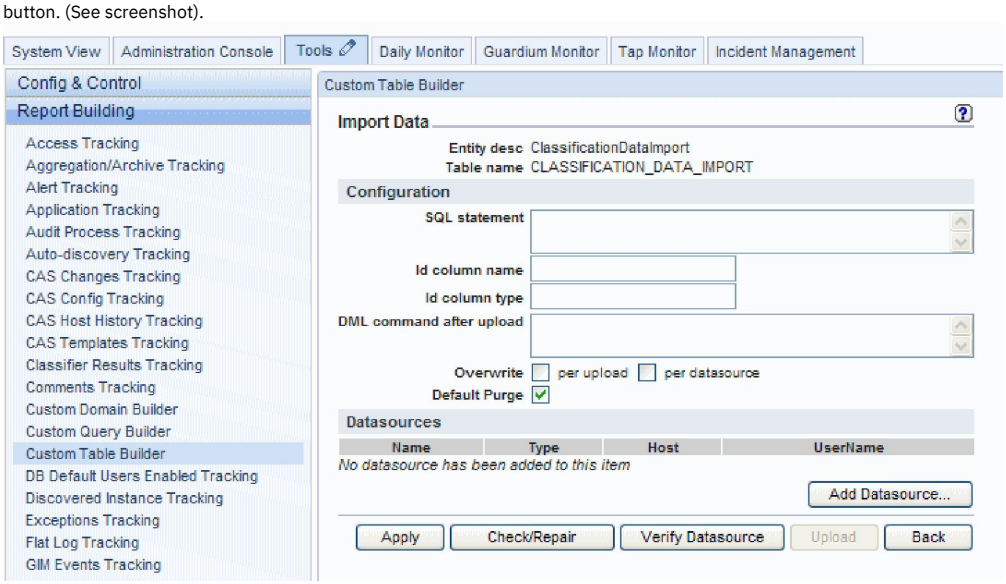
Follow these steps:

1. Export from Guardium - Export Classification Data from IBM Guardium to InfoSphere Discovery
2. As an admin user in the Guardium® application, go to Tools > Report Building >Classifier Results Tracking > Select a Report > Export Sensitive Data to Discovery (See screenshot).
   Note: Add this report to the UI pane (it is not by default).

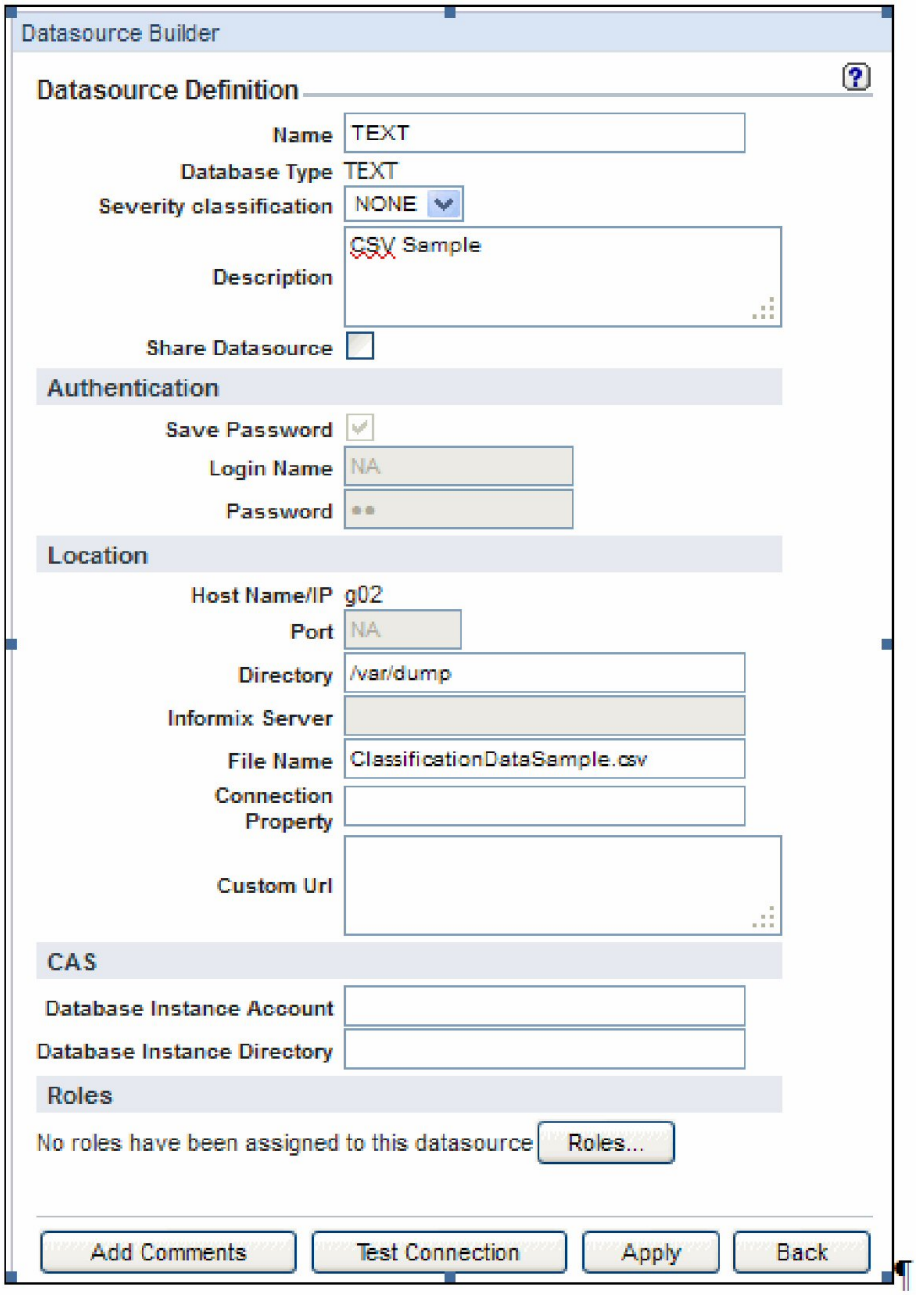


3. Click on Customize icon on Report Result screen and specify the search criteria to filter the classification results data to transfer to Discovery.
4. Run the report and click on Download All Records icon.
5. Save as CSV and import this file to Discovery according to the InfoSphere Discovery instructions.
6. Import to Guardium - Import Classification Data from InfoSphere Discovery to IBM Guardium

7. Export the classification data as CSV from InfoSphere Discovery based on InfoSphere Discovery instructions.
8. As an admin user in the Guardium application, go to Tools > Report Building >Custom Tables screen, select ClassificationDataImport and click on Upload Data button. (See screenshot).



9. In Upload Data screen, click on Add Datasource, click on New button, define the CSV file imported from Discovery as new datasource (Database Type = Text). See the following screenshot of CSV Datasource definition.



Note: Alternatively you can load the data directly from Discovery database if you know how to access the Discovery database and Classification results data.

10. After defining the CSV as Datasource, click on Add button in Datasource list screen.
11. In Upload data screen click on Verify Datasource and then Apply.
12. Click on Run Once Now button to load the data from the CSV.
13. Go to Report Builder, select Classification Data Import report, Click on Add to Pane to add it to your Portal and then navigate to the report.
14. Access the Report, click on Customize to set the From/To dates and execute the report.

The report result has the classification data imported from InfoSphere Discovery. Double click to invoke APIs assigned to this report. The data imported from Discovery can be used for the following:

- Add new Datasource based on the result set.
- Add/Update Sensitive Data Group.
- Add policy rules based on datasource and sensitive data details.
- Add Privacy Set.

Table 1. CSV Interface signature

Interface Signature	Example
Type	DB2®
Host	9.148.99.99
Port	50001
dbName (Schema name for DB2 or Oracle, db name for others)	cis_schema
Datasource URL	

Interface Signature	Example
TableName	MK_SCHED
ColumnName	ID_PIN
ClassificationName	SSN
RuleDescription	Out-of-box algorithm of InfoSphere Discovery
HitRate	70% - not available for export in Guardium Vers. 8.2
ThresholdUsed	60% - not available for export in Guardium Vers. 8.2

Parent topic: Product integration

CEF Mapping

The CEF standard from ArcSight defines a set of required fields, and a set of optional fields.

The latter are called extensions in the CEF standard. Data is mapped to these fields from Guardium® configuration information and reports. Note that not all Guardium fields map to a CEF field, so there may not be a one-to-one relationship between the rows of a printed report and the CEF file produced for that report. Also note that this facility is intended to map data from data access domains (Data Access, Exceptions, and Policy Violations, for example), and not from Guardium self-monitoring domains (Aggregation/Archive, Audit Process, Guardium Logins, etc.).

Note: Analyzed Client IP has a map for CEF source. If the query used for the CEF does NOT contain the Client IP but contains the analyzed client IP, the analyzed client IP will be used for the source. If both included in the query, then Client IP takes precedence.

The CEF fields in the following table are always present.

Table 1. Required CEF Fields Mapping

CEF Field	Guardium Mapping
Version	0 (zero); Currently the only version for the CEF format
Device Vendor	Guardium
Device Product	Guardium
Device Version	Guardium software version number
Signature ID	ReportID
Name	Report Title
Severity	Numeric severity code in the range 0-10, with 10 being the most important event. If not reset in the report, 0 (zero, which translates to Info for Guardium).

The CEF extension fields are optional, and will be present only when the mapping applies. For example, if the report does not contain an access rule description, the act field (the first extension field) will not be present. For more detailed information about the Guardium entities and attributes, see the appropriate entity reference topic.

Table 2. CEF Mapping, Guardium Version 8.2

CEF Field	Entity	Attribute
severity	Policy Rule Violation	Severity
act	Policy Rule Violation	Access Rule Description
app	Client/Server	DB Protocol
app	Exception	Database Protocol
dst	Client/Server	Server IP
dst	Exception	Destination Address
dhost	Client/Server	Server Host Name
dpt	Session	Server Port
dpt	Exception	Destination Port
dproc	Client/Server	Source Program
duid	Client/Server	OS User
duser	Client/Server	DB User Name
duser	Exception	User Name
end	Exception	Exception Timestamp
end	Policy Rule Violation	Timestamp
end	Access Period	Period End
end	Session	Session End
msg	Exception	Exception Description
msg	Message Text	Message Text
msg	Message Text	Message Subject
src	Client/Server	Client IP
src	Client/Server	Analyzed Client IP

CEF Field	Entity	Attribute
src	Exception	Source Address
shost	Client/Server	Client Host Name
smac	Client/Server	Client MAC
spt	Session	Client Port
spt	Exception	Source Port
start	Exception	Exception Timestamp
start	Policy Rule Violation	Timestamp
start	Access Period	Period Start
start	Session	Session Start
proto	Client/Server	Network Protocol
request	FULL SQL	Full Sql
request	SQL	Sql
cs1	Session	Uid Chain
cs2	Session	Uid Chain Compressed

Table 3. CEF Mapping, Guardium Version 9.0

CEF Field	Entity	Attribute
severity	Policy Rule Violation	Severity
act	Policy Rule Violation	Access Rule Description
app	Client/Server	DB Protocol
app	Exception	Database Protocol
dst	Client/Server	Server IP
dst	Exception	Destination Address
dhost	Client/Server	Server Host Name
dpt	Session	Server Port
dpt	Exception	Destination Port
dproc	Client/Server	Source Program
duid	Client/Server	OS User
duser	Client/Server	DB User Name
duser	Exception	User Name
end	Exception	Exception Timestamp
end	Policy Rule Violation	Timestamp
end	Access Period	Period End
end	Session	Session End
msg	Exception	Exception Description
msg	Message Text	Message Text
msg	Message Text	Message Subject
src	Client/Server	Client IP
src	Client/Server	Analyzed Client IP
src	Exception	Source Address
shost	Client/Server	Client Host Name
smac	Client/Server	Client MAC
spt	Session	Client Port
spt	Exception	Source Port
start	Exception	Exception Timestamp
start	Policy Rule Violation	Timestamp
start	Access Period	Period Start
start	Session	Session Start
proto	Client/Server	Network Protocol
request	FULL SQL	Full Sql
request	SQL	Sql
cs1	Session	Uid Chain
cs2	Session	Uid Chain Compressed

For more information about CEF, search the web for Common Event Format: Event Interoperability Standard, or visit the ArcSight Website: www.arcsight.com.

Parent topic: Product integration

LEEF Mapping

Log Event Extended Format (LEEF) from QRadar

The LEEF format consists of an optional syslog header, an LEEF header and a collection of attributes describing the event.

Syslog_Header(optional) LEEF_Header|Event_Attributes

The LEEF header is pipe ('|') separated and attributes are tab separated

Example

Jan 18 11:07:53 host LEEF:Version|Vendor|Product|Version|EventID|Key1=Value1<tab>Key2=Value2<tab>Key3=Value3<tab>...<tab>KeyN=ValueN

Table 1. LEEF Parameters

Parameters	Description
LEEF: Version	Version Integer identifying the version of LEEF used for the log message
Vendor	String identifying the vendor of the device or application sending the event log
Product	Product String identifying product sending the event log Note: The combination of vendor and product must be unique
Version	String identifying the version of the device or application Sending the event log
EventID	ID that uniquely identifies the event
Attributes 1..N	A set of key value pairs attributes for the event separated by the tab character. Order is not enforced. A pre defined set of keys are defined and should be used when possible. LEEF format is extensible and allows for additional key value pairs to be added to the event log. Keys must not contain spaces or equal signs Values must not contain tabs

Example:

```
Jan 18 11:07:53 192.168.1.1 LEEF:1.0|QRadar|QRM|1.0|NEW_PORT_DISCOVERD|src=172.5.6.67 dst=172.50.123.1 sev=5 cat=anomaly msg=there are spaces in this message
```

Character Encoding

UTF8

Predefined Attributes

Table 2. Predefined Attributes

Key Name	Data Type	Max Length	Description
Cat	string		Event category
devTime	date		Time the device or application emitted the event
devTimeFormat	string		Defined by the java SimpleDateFormat. This is only required if using a customized date format. See Date Format section for further details.
proto	integer		Transport protocol
sev	integer (1-10)		Severity of this event
src	IPv4 or IPv6 address		Source address
dst	IPv4 or IPv6 address		Destination address
VSrc	IPv4 or IPv6 address		Virtual source address
srcPort	integer		Source Port. The valid port numbers are between 0 and 65535.
dstPort	integer		Destination Port. The valid port numbers are between 0 and 65535.
srcPreNat	IPv4 or IPv6 address		Source address for the message before Network Address Translation (NAT) occurred
dstPreNat	IPv4 or IPv6 address		Destination address for the message before Network Address Translation (NAT) occurred
srcPostNat	IPv4 or IPv6 address		Source address for the message after Network Address Translation (NAT) occurred
dstPostNat	IPv4 or IPv6 address		Destination address for the message after Network Address Translation (NAT) occurred
usrName	string	255	User name associated with the event
srcMAC	MAC address		Six colon-separated hexadecimal numbers. Example: `1:2D:67:BF:1A:71`
dstMAC	MAC address		Six colon-separated hexadecimal numbers. Example: `11:2D:67:BF:1A:71`

Key Name	Data Type	Max Length	Description
srcPreNATPort	integer		Source Port. The valid port numbers are between 0 and 65535.
dstPreNATPort	integer		Destination Port. The valid port numbers are between 0 and 65535.
srcPostNATPort	integer		Source Port. The valid port numbers are between 0 and 65535.
dstPostNATPort	integer		Destination Port. The valid port numbers are between 0 and 65535.
identSRC	IPv4 or IPv6 address		
identHostName	string	255	Host name associated with the event. Typically, this parameter is only associated with identity events
identNetBios	string	255	NetBIOS name associated with the event. Typically, this parameter is only associated with identity events
identGrpName	string	255	Group name associated with the event. Typically, this parameter is only associated with identity events.

Custom Attributes

In some cases custom attributes may be required to identify more information about the event being generated. In these cases vendors may define their own custom attributes and include them in the event log. Custom attribute fields should be used only when there is no acceptable mapping in to a predefined field.

Custom attributes keys must be:

- Single word no spaces
- Alphanumeric
- Clear and concise
- Cannot be named the same as any predefined attribute key

Custom attributes may be used for viewing in the QRadar Event Viewer by creating custom properties.

Custom attributes may be used by the QRadar reporting engine by creating customer properties.

Custom attributes can NOT be used for event correlation

Note: Add databaseName=%%DBname to the LEEF template in order to capture the MS-SQL database name. Update the existing LEEF template or make a new template by cloning.

Date Formats

You can use any of these predefined formats:

1. Milliseconds since January 1, 1970 (integer)
2. MMM dd yyyy HH:mm:ss, for example, Jun 06 2012 16:07:36
3. MMM dd yyyy HH:mm:ss.SSS, for example, Jun 06 2012 16:07:36.300
4. MMM dd yyyy HH:mm:ss.SSS zzz, for example, Jun 06 2012 02:07:36.300 GMT

If these formats are not suitable, you can define a custom date format in the dTime field by specifying the date format using the dTimeFormat key.

For further information on specifying a date format, visit the SimpleDateFormat page at: http://java.sun.com/javase/6/docs/api/java/text/SimpleDateFormat.html

Parent topic: Product integration

Troubleshooting problems

To isolate and resolve problems with your IBM products, you can use the troubleshooting and support information. This information contains instructions for using the problem-determination resources that are provided with your IBM products, including IBM Guardium.

- Techniques for troubleshooting problems
  Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem. Certain common techniques can help with the task of troubleshooting.
- Problems and solutions
  Search here for solutions to problems that you encounter.

Techniques for troubleshooting problems

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem. Certain common techniques can help with the task of troubleshooting.

The first step in the troubleshooting process is to describe the problem completely. Problem descriptions help you and the IBM technical-support representative know where to start to find the cause of the problem. This step includes asking yourself basic questions:

- What are the symptoms of the problem?
- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can the problem be reproduced?

The answers to these questions typically lead to a good description of the problem, which can then lead you to a problem resolution.

What are the symptoms of the problem?

What is the problem? This question might seem straightforward, however, you can break it down into several more-focused questions that create a more descriptive picture of the problem. These questions can include:

- Who, or what, is reporting the problem?
- What are the error codes and messages?
- How does the system fail? For example, is it a loop, hang, crash, performance degradation, or incorrect result?

Where does the problem occur?

Determining where the problem originates is not always easy, but it is one of the most important steps in resolving a problem. Many layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few of the components to consider when you are investigating problems.

The following questions help you to focus on where the problem occurs to isolate the problem layer:

- Is the problem specific to one platform or operating system, or is it common across multiple platforms or operating systems?
- Is the current environment and configuration supported?
- Do all users have the problem?
- (For multi-site installations.) Do all sites have the problem?

If one layer reports the problem, the problem does not necessarily originate in that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some time to completely describe the problem environment, including the operating system and version, all corresponding software and versions, and hardware information. Confirm that you are running within an environment that is a supported configuration; many problems can be traced back to incompatible levels of software that are not intended to run together or have not been fully tested together.

When does the problem occur?

Develop a detailed timeline of events leading up to a failure, especially for those cases that are one-time occurrences. You can most easily develop a timeline by working backward: Start at the time an error was reported (as precisely as possible, even down to the millisecond), and work backward through the available logs and information. Typically, you need to look only as far as the first suspicious event that you find in a diagnostic log.

To develop a detailed timeline of events, answer these questions:

- Does the problem happen only at a certain time of day or night?
- How often does the problem happen?
- What sequence of events leads up to the time that the problem is reported?
- Does the problem happen after an environment change, such as upgrading or installing software or hardware?

Responding to these types of questions can give you a frame of reference in which to investigate the problem.

Under which conditions does the problem occur?

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These questions about your environment can help you to identify the root cause of the problem:

- Does the problem always occur when the same task is being performed?
- Does a certain sequence of events need to happen for the problem to occur?
- Do any other applications fail at the same time?

Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Remember that just because multiple problems might have occurred around the same time, the problems are not necessarily related.

Can the problem be reproduced?

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem can be reproduced you have a larger set of tools or procedures at your disposal to help you investigate. Consequently, problems that you can reproduce are often easier to debug and solve.

However, problems that you can reproduce can have a disadvantage. If the problem is of significant business impact, you do not want it to reoccur. If possible, recreate the problem in a test or development environment, which typically offers you more flexibility and control during your investigation.

- Can the problem be re-created on a test system?
- Are multiple users or applications encountering the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

- Getting fixes from Fix Central
  You can use Fix Central to find the fixes that are recommended by IBM Support for a variety of products, including Guardium. With Fix Central, you can search, select, order, and download fixes for your system with a choice of delivery options. A product fix might be available to resolve your problem.
- Contacting IBM Support
  IBM Support provides assistance with product defects, answers FAQs, and helps users resolve problems with the product.
- Basic information for IBM Support
  Before you call IBM Support, collect basic information about IBM Guardium (collector, aggregator, Central Manager; UNIX/Linux S-TAP; Windows S-TAP).
- Exchanging information with IBM
  To diagnose or identify a problem, you might need to provide IBM Support with data and information from your system. In other cases, IBM Support might provide you with tools or utilities to use for problem determination.
- Subscribing to Support updates
  To stay informed of important information about the IBM products that you use, you can subscribe to updates.

Parent topic: Troubleshooting problems

Getting fixes from Fix Central

You can use Fix Central to find the fixes that are recommended by IBM Support for a variety of products, including Guardium. With Fix Central, you can search, select, order, and download fixes for your system with a choice of delivery options. A product fix might be available to resolve your problem.

About this task

Procedure

To find and install fixes:

1. Obtain the tools that are required to get the fix. If it is not installed, obtain your product update installer. You can download the installer from Fix Central. This site provides download, installation, and configuration instructions for the update installer.
2. Select Guardium as the product, and select one or more check boxes that are relevant to the problem that you want to resolve.
3. Identify and select the fix that is required.
4. Download the fix.
    a. Open the download document and follow the link in the Download Package section.
    b. When downloading the file, ensure that the name of the maintenance file is not changed. This change might be intentional, or it might be an inadvertent change that is caused by certain web browsers or download utilities.
5. Apply the fix.
    a. Follow the instructions in the Installation Instructions section of the download document.
    b. For more information, see the Installing fixes with the Update Installer topic in the product documentation.
6. Optional: Subscribe to receive weekly email notifications about fixes and other IBM Support updates.

Parent topic: Techniques for troubleshooting problems

Contacting IBM Support

IBM Support provides assistance with product defects, answers FAQs, and helps users resolve problems with the product.

Before you begin

After trying to find your answer or solution by using other self-help options such as technotes, you can contact IBM Support. Before contacting IBM Support, your company or organization must have an active IBM *maintenance contract name*, and you must be authorized to submit problems to IBM. For information about the types of available support, see the Support portfolio topic in the "*Software Support Handbook*".

Procedure

To contact IBM Support about a problem:

1. Define the problem, gather background information, and determine the severity of the problem. For more information, see the Getting IBM support topic in the *Software Support Handbook*.
2. Gather diagnostic information.
3. Submit the problem to IBM Support in one of the following ways:
    - Online through the IBM Support Portal: You can open, update, and view all of your service requests from the Service Request portlet on the Service Request page.
    - By phone: For the phone number to call in your region, see the Directory of worldwide contacts web page.

Results

If the problem that you submit is for a software defect or for missing or inaccurate documentation, IBM Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM Support website daily, so that other users who experience the same problem can benefit from the same resolution.

Parent topic: Techniques for troubleshooting problems

Related information:

How to upload data to a support ticket (PMR) (video)

Guardium troubleshooting and support (video)

Basic information for IBM Support

Before you call IBM Support, collect basic information about IBM Guardium (collector, aggregator, Central Manager; UNIX/Linux S-TAP; Windows S-TAP).

Use support must_gather commands, which can be run through the CLI to generate specific information about the state of any Guardium system. This information can also be collected through the Guardium GUI.

This information can be uploaded from the Guardium system and sent to IBM Support whenever a Problem Management Report (PMR) is logged.

Gathering support information results

To gather support information, click Manage > Maintenance > Support Information Gathering. Complete the following sections.

1. Describe the support information gathering session.
2. Complete the PMR number.
3. To send the results to an email address, specify email: and complete the email address.
4. Schedule a start time by clicking the calendar icon.
5. Check off gather log information that is related to the following categories:
    - Aggregation
    - User Interface
    - Backup
    - DB User
    - Scheduler
    - System DB
    - Network

- Deployment Health
- Alert
- Audit
- Central Manager
- Purge
- Sniffer
- Patch Install
- Advance Threat Scanning
- Entitlement Optimization

6. Input a value to gather information for a certain amount of time in minutes. The default value is 10 minutes. This value is the time period the logs will be gathered for. If you specify an email, the logs are gathered for 10 minutes from the time you start the process and an email is sent afterwards. You must reproduce the problem and generate the log information during the specified time period so that the logs can contain the debug information that is needed to troubleshoot problems.
7. Input the maximum number of rows that appears in the result log file.
8. When you are finished with the configuration, click Start.
9. Go to Support Information Results to view the results. You can open or save the .tgz file.

Must Gather for Guardium Appliance with CLI

IBM Guardium Collector, Aggregator, or Central Manager

The must_gather commands can be run at any time by the user through the CLI. Complete the following steps.

1. Open a putty session (or similar) to the appropriate collector, aggregator, or Central Manager.
2. Log in as user `cli`.
3. Depending on the type of issue, paste the relevant must_gather commands into the CLI prompt. More than one must_gather command might be needed to diagnose the problem. The commands are listed and described in the following list.
   - support must_gather agg_issues (aggregation process)
   - support must_gather alert_issues (alerts)
   - support must_gather app_issues (application)
   - support must_gather audit_issues (audit process)
   - support must_gather backup_issues (backup process)
   - support must_gather cm_issues (Central Manager)
   - support must_gather datamining_issues (data mining)
   - support must_gather miss_dbuser_prog_issues (system database user)
   - support must_gather en (entitlement optimization)
   - support must_gather network_issues (network architecture)
   - support must_gather ocr_issues
   - support must_gather patch_install_issues (patch installation and upgrades)
   - support must_gather purge_issues (purge process)
   - support must_gather scheduler_issues (scheduler function)
   - support must_gather sniffer_issues (sniffer function)
   - support must_gather system_db_info (Guardium system database or operating space performance)

   The output is written to the must_gather directory with a file name such as the following example:

   must_gather/system_logs/.tgz

4. Send the resulting output to IBM Support.

   By using fileserver <ip address>, you can upload the .tgz files and send to IBM Support.

   Send the file through email or upload to ECUREP by using the standard data upload. Specify the PMR number and file to upload.

Must Gather for UNIX/Linux S-TAP

The guard_diag script produces statistics on the server that helps Guardium with diagnostics.

Explanation of guard_diag:

Diagnostic Script (guard_diag)

General Overview:

There is now a diagnostics script (guard_diag) that runs out of /usr/local/guardium/guard_stap/guard_diag when S-TAP logging is set to level 7 from the GUI. It is also possible to transfer this script to a machine that is running S-TAP.

Usage: ./guard_diag output_dir

The script prompts for the location if the script cannot automatically determine where S-TAP is installed. The run time is about 1.5 minutes and if no output directory is specified, the script places the generated .tar file in /tmp. When the script runs and enables logging from the GUI, the .tar file is placed in /var/tmp. The file name is derived from the machine name, and the time/date run; it always starts with diag.ustap.

General System Data Collected:

- Uname -a
- List of kernel modules installed
- Output for one cycle
- Uptime
- Processor number and type
- Dump of most recent syslog
- Netstat output
- IPC list

- Disk free statistics
- copy of /etc/services
- Directory listing of /etc
- Various platform-specific information
- Contents of /etc/inittab

S-TAP Data Collected:

- S-TAP version
- Contents of guard_tap.ini
- Ls -l on the K-TAP device nodes
- 30s trace of S-TAP
- K-TAP statistics
- List of all the files in the installation directory
- K-TAP khash
- Verbose debug log for K-TAP (2) and S-TAP(4)

Known Issues:

- Tusc is not installed on all HP-UX operating systems, so tracing the S-TAP PID does not work.
- gzip isn't always installed on the system. The fall back is to compress (final extension of .tar.Z) and failing that, the .tar file is placed in the output directory.
- Topas output on AIX is best interpreted by the terminal since it contains control codes that makes it mostly unintelligible when it is opened in an editor.
- The non-root S-TAP has a number of issues concerning the diagnostics script.
- In Linux, /var/log/messages is only readable by the root.
- Some Solaris operating systems might not be configured correctly and causes netstat to print an error.
- The path for the non-root user is rather basic, and as a result, some commands might not run at all. Notably, this known issue happens on HP-UX with gzip.

Platforms Supported:

- Linux
- HP-UX
- AIX
- Solaris

Requirements for STAP: None

Requirements for Linux: None

Requirements for AIX: topas

Requirements for Solaris: top, prtdiag, psrinfo

Requirements for HP-UX: tusc

Must Gather for Windows S-TAP

Running this script generates the following text files in the current directory:

- stap.txt
- tasks.txt
- system.txt
- evtlog.txt or evtlog2008.txt
- reg.txt

Notes:

1. This diag script can be run with any S-TAP version.
2. Rename the diag script to diag.bat and place it under directory where S-TAP was installed. Then, you can run it manually. It generates text files with diagnostic information.
3. Submit the results to Guardium L3 Support or Research & Development.

The script collects the following data:

- Content of %system%guard_tap.ini.
- The Guardium S-TAP installation log
- All running tasks
- List of all installed kernel drivers
- OS information that is collected from the system information utility
- ipconfig /all
- netstat -nao
- Ping and trace results from the database server to the Guardium system
- CPU usage for guardium_stapr
- Overall system CPU usage
- Guardium_stapr process handle count and memory usage
- Event log messages that are generated by S-TAP
- System event log messages
- The following registry entries:
  - HKLMSOFTWAREMicrosoftWindowsCurrentVersionUninstall?
  - HKLMSYSTEMCurrentControlSetServices?
  - HKLMSYSTEMCurrentControlSetControlGroupOrderList?
  - HKEY_LOCAL_MACHINESOFTWAREMicrosoftMSSQLServer

Encrypt Must Gather

Encrypt Must Gather was added to the Global Profile screen. To go to the Global Profile screen, click Setup > Global Profile.. The default value is cleared (Do not encrypt). If it is cleared, must gather output is compressed and not encrypted (current function). When the check box is checked, all future must gather output is encrypted. Encryption can be also set by store encrypt_must_gather on CLI command and cleared by using the command store encrypt_must_gather off.

GuardAPI Must Gather

Use the GuardAPI command to run the GuardAPI Must Gather collection of information from a script.

grdapi must_gather --help=true.

The following function parameters are listed.

```
ID=0
function parameters :
commandsList - String -required - Constant values list
description - String
email - String
maxLogLength - Integer - Constant values list
pmrNumber - String
runDuration - Integer - Constant values list
startRun - Date
To get a Constant values list for a parameter, call the function with --get_param_values=<param-name>
```

The --commandsList requires a string. The --description is also a required string. The --runDuration indicates how long the must_gather runs. Type in an email address to send the must_gather report. The --maxLogLength parameter is a required integer that sets the maximum length of the log report. The --pmrNumber is the problem management report number that is used by IBM Support to track and resolve customer reports. The --startRun is a required date such as now. You can get a list of values for each parameter by calling the function grdapi must_gather --get_param_values=<param-name>.

Parent topic: Techniques for troubleshooting problems
Related information:
Guardium troubleshooting and support (video)

Exchanging information with IBM

To diagnose or identify a problem, you might need to provide IBM Support with data and information from your system. In other cases, IBM Support might provide you with tools or utilities to use for problem determination.
Parent topic: Techniques for troubleshooting problems

Sending information to IBM Support

To reduce the time that is required to resolve your problem, you can send trace and diagnostic information to IBM Support.

Procedure

To submit diagnostic information to IBM Support:

1. Open a problem management record (PMR).
2. Collect the diagnostic data that you need. Diagnostic data helps reduce the time that it takes to resolve your PMR. You can collect the diagnostic data manually or automatically:
   - Collect the data manually.
   - Collect the data automatically.
3. Compress the files by using the .zip or .tar file format.
4. Transfer the files to IBM. You can use one of the following methods to transfer the files to IBM:
   - The Service Request tool
   - Standard data upload methods: FTP, HTTP
   - Secure data upload methods: FTPS, SFTP, HTTPS
   - Email

   All of these data exchange methods are explained on the IBM Support website.

Receiving information from IBM Support

Occasionally an IBM technical-support representative might ask you to download diagnostic tools or other files. You can use FTP to download these files.

Before you begin

Ensure that your IBM technical-support representative provided you with the preferred server to use for downloading the files and the exact directory and file names to access.

Procedure

To download files from IBM Support:

1. Use FTP to connect to the site that your IBM technical-support representative provided and log in as `anonymous`. Use your email address as the password.
2. Change to the appropriate directory:
   a. Change to the /fromibm directory.

      ```
      cd fromibm
      ```

   b. Change to the directory that your IBM technical-support representative provided.

      ```
      cd nameofdirectory
      ```

3. Enable binary mode for your session.

```
binary
```

4. Use the get command to download the file that your IBM technical-support representative specified.

   ```
   get filename.extension
   ```

5. End your FTP session.

   ```
   quit
   ```

Subscribing to Support updates

To stay informed of important information about the IBM products that you use, you can subscribe to updates.

About this task

By subscribing to receive updates about Guardium, you can receive important technical information and updates for specific IBM Support tools and resources. You can subscribe to updates by using one of two approaches:

RSS feeds and social media subscriptions
: The following RSS feeds and social media subscriptions are available for Guardium:

  - *RSS feed 1*
  - *RSS feed 2*
  - *RSS feed 3*

  For general information about RSS, including steps for getting started and a list of RSS-enabled IBM web pages, visit the IBM Software Support RSS feeds site.

My Notifications
: With My Notifications, you can subscribe to Support updates for any IBM product. (My Notifications replaces My Support, which is a similar tool that you might have used in the past.) With My Notifications, you can specify that you want to receive daily or weekly email announcements. You can specify what type of information you want to receive (such as publications, hints and tips, product flashes (also known as alerts), downloads, and drivers). My Notifications enables you to customize and categorize the products about which you want to be informed and the delivery methods that best suit your needs.

Procedure

To subscribe to Support updates:

1. Subscribe to the Guardium RSS feeds.
2. Subscribe to My Notifications by going to the IBM® Support Portal and click My Notifications in the Notifications portlet.
3. Sign in using your IBM ID and password, and click Submit.
4. Identify what and how you want to receive updates.
   a. Click the Subscribe tab.
   b. Select the appropriate software brand or type of hardware.
   c. Select one or more products by name and click Continue.
   d. Select your preferences for how to receive updates, whether by email, online in a designated folder, or as an RSS or Atom feed.
   e. Select the types of documentation updates that you want to receive, for example, new information about product downloads and discussion group comments.
   f. Click Submit.

Results

Until you modify your RSS feeds and My Notifications preferences, you receive notifications of updates that you have requested. You can modify your preferences when needed (for example, if you stop using one product and begin using another product).

Parent topic: Techniques for troubleshooting problems

Related Information

- IBM Software Support RSS feeds
- Subscribe to My Notifications support content updates
- My Notifications for IBM technical support
- My Notifications for IBM technical support overview

Problems and solutions

Search here for solutions to problems that you encounter.

- User Interface
- Policies
- Reports
- Assess and Harden
- Configuring your Guardium system
- Access Management
- Aggregation
- Central Management
- S-TAPs and other agents
- GIM
- File activity troubleshooting
- Installing Your Guardium System

Parent topic: Troubleshooting problems

User Interface

- Changes are not saved when you add an inspection engine
  If your changes are not saved when you add an inspection engine, check that the parameters are valid.
- HTTP error 403
  If you receive a HTTP error 403, you can disable the Cross-Site Request Forgery (CSRF) protection feature to prevent the error.
- Java.lang.IllegalStateException
  If you receive a java.lang.IllegalStateException error, clean up the Java servlets.
- Pages are not loading correctly
  If pages do not load correctly, restart the GUI or use a different browser.

Parent topic: Problems and solutions

Changes are not saved when you add an inspection engine

If your changes are not saved when you add an inspection engine, check that the parameters are valid.

Symptoms

When you add an inspection engine, the new settings remain for a few minutes and then disappear.

Causes

There is an error in one or more parameter values with either the new inspection engine or a different inspection engine in the S-TAP configuration file guard_tap.ini.

Environment

The Guardium collector user interface is affected.

Resolving the problem

Check that every parameter that must be set for the inspection engine is set to a valid value. For example, some database types require that you set db_install_dir to the path of the installation directory on the server. However, for other database types, this parameter must not be set or must be set to NULL. Check the specific requirements for your database type in the S-TAP Help Book and make sure that everything is correctly set.

Parent topic: User Interface

HTTP error 403

If you receive a HTTP error 403, you can disable the Cross-Site Request Forgery (CSRF) protection feature to prevent the error.

Symptoms

When you refresh the IBM Security Guardium GUI from the system main page, you receive in the following error:

```
HTTP Status 403-
type Status report
message
description Access to the specified resource () has been forbidden
```

Causes

The cause is a feature in Guardium designed to prevent Cross-Site Request Forgery (CSRF). CSRF protection is enabled by default.

Environment

All Guardium configurations (collector, aggregator, central manager) are affected.

Resolving the problem

You can disable this feature by using the following CLI command: store gui csrf_status off

Note: If you turn off CSRF protection, the security level of the Guardium system is reduced.

The following command enables protection against Cross-Site Request Forgery. It is enabled by default: store gui csrf_status on

You can check the status by running this CLI command: show gui csrf_status

Parent topic: User Interface

Java.lang.IllegalStateException

If you receive a java.lang.IllegalStateException error, clean up the Java servlets.

Symptoms

You receive the following error message.

```
There has been an Error. Please Contact your System Administrator
(java.lang.IllegalStateException)
```

Causes

The error is raised when a method is invoked and the Java VM is in a state that is inconsistent with the method. There might also be corrupted Java servlets that are caused by deadlocks.

Environment

The Guardium system is affected.

Resolving the problem

Wait a few minutes and retry. If the error persists, restart the GUI by logging in as user cli and executing the command restart GUI.

To clean up the Java servlets, run the command support clean sevlets.

If the problem is not resolved, please collect the following tomcat logs and contact IBM Security Guardium Technical Support.

```
tomcat_log/localhost.<date_stamp>.log
tomcat_log/catalina.<date_stamp>.log
```

Parent topic: User Interface

Pages are not loading correctly

If pages do not load correctly, restart the GUI or use a different browser.

Symptoms

You might see a blank screen or other errors. The problem appears to happen with certain browsers on specific systems but not with others.

Causes

The cause might be restricted to a localized browser or there is a Java virtual machine issue.

Environment

The collector, aggregator, and central manager are affected.

Resolving the problem

To resolve the problem, run restart GUI from the CLI prompt on the Guardium system. If that does not help, try the following actions.

- Restart the system.
- Uninstall and reinstall the Java virtual machine.
- Uninstall and reinstall the browser.
- Use a different browser.

Parent topic: User Interface

Policies

- Query does not appear in the co-relation alert definition
  If the query does not appear in the co-relation alert definition, check the count field and sort by time stamp.
- Rule does not trigger
  If a rule with a value in the policy command field does not trigger as expected, reconfigure the rule.
- Redact function causes overly masked result
  If the redact function causes an overly masked result, use the regular expression [\x0c]{1}[0-9]{8}([0-9]{4}).
- SSH sessions and automated CRON jobs that log in to your Oracle database are shown as failed logins
  If SSH sessions and automated CRON jobs that log in to your Oracle database are shown as failed logins, amend the policy.
- The Guardium internal database is filling up
  If the Guardium internal database is filling up, you can purge the data manually or as part of the regular purge strategy.

Parent topic: Problems and solutions

Query does not appear in the co-relation alert definition

If the query does not appear in the co-relation alert definition, check the count field and sort by time stamp.

Symptoms

You created an access query for creating a co-relation alert. However, in the co-relation alert definition, this query does not appear in the drop-down list.

Causes

The co-relation alert search in the report is based on the time stamp.

Environment

The collector and aggregator are affected.

Resolving the problem

Mark the Add Count check box and sort by time stamp.

Parent topic: Policies

Rule does not trigger

If a rule with a value in the policy command field does not trigger as expected, reconfigure the rule.

Symptoms

Rules with a value in the policy Command field do not trigger as expected.

Causes

The cause is a misconfiguration in the command field. The Guardium parser does not consider the command modifiers to be a part of a command.

Environment

Guardium Collectors. The command field in the policy rule is also affected when it is used with wildcard (%).

Resolving the problem

The value in the Command field of the rule must match a value exactly that is shown in SQL Verb, plus a wildcard (%) as needed. This example is correct.

```
GRANT
GRANT%
```

This example is incorrect.

```
GRANT% TO PUBLIC
%GRANT% ADMIN OPTION%
```

ADMIN OPTION and TO PUBLIC do not match and cannot trigger a rule because the Guardium parser does not recognize them as a part of a command. Generally, the parser does not consider command modifiers to be part of a command. Instead, create a report to inspect the traffic that the policy monitors and include the SQL Verb field from the Command entity in that report. Anything that is listed in the SQL Verb field is recognized by the parser and can be used in the Command field of a policy rule. Several commands can be added to a group and the group can be used in the rule instead of a single command. In this case, each group member must match an entry in SQL Verb. Guardium includes several such command groups that you can use or clone.
Parent topic: Policies
Parent topic: Reports

Redact function causes overly masked result

If the redact function causes an overly masked result, use the regular expression [\x0c]{1}[0-9]{8}([0-9]{4}).

Symptoms

The redact function causes an overly masked result or an ORA-03106 error in Oracle traffic.

Causes

The redact function in the Guardium policy rule is doing a pattern match with the result set. It has a feature to replace the matched string with the user specified character.

Environment

Guardium collectors are affected.

Resolving the problem

Use the regular expression `[\x0c]{1}[0-9]{8}([0-9]{4})`. This regular expression ensures that it starts with the length of the column followed by 12 digits and replaces the last 4 digits.

Parent topic: Policies

SSH sessions and automated CRON jobs that log in to your Oracle database are shown as failed logins

If SSH sessions and automated CRON jobs that log in to your Oracle database are shown as failed logins, amend the policy.

Symptoms

SSH sessions and automated CRON jobs that log in to your Oracle database through SQLPLUS and RMAN with `/as sysdba` show as failed logins.

Causes

Oracle responds to these logins with the following error on such attempts, even if it is not shown on the screen.

```
ORA-01-17: invalid username/password; logon denied.
```

This error triggers the failed login alert. For example, if the database user WRONGLOGIN is a member of the DBA group, and logs as `sqlplus WRONGLOGIN as sysdba`, the database authentication of WRONGLOGIN fails. This failure causes the ORA-01-17 error alert to trigger and is reflected in the Guardium log. However, users with sysdba privileges can connect to the database without database authentication so the session is allowed to continue. Both events are captured and recorded.

Environment

Guardium collectors are affected.

Resolving the problem

You can amend the policy to include an allow action before the rule that alerts about failed logins. Create an exception rule in the policy with the following conditions.

```
Client IP=<Server IP>
Source program = SQLPLUS
DB user in trusted group
OS user in group of Oracle DBAs
Net protocol = BEQUEATH (if local BEQUEATH, not TCP)
```

This rule skips the failed login alerts that are caused by the ORA-01-17 error but are still logged. To filter the failed login alerts out of the reports, add these conditions to the end of the conditions list:

```
AND
       (
    client IP<>server IP OR
    src prg <> SQLPLUS OR
    db user NOT IN group of trusted OR
    os user NOT IN group of oracle DBAs OR
    net protocol <>BEQUEATH (if this is local BEQUEATH, not TCP )
   )
```

Parent topic: Policies

The Guardium internal database is filling up

If the Guardium internal database is filling up, you can purge the data manually or as part of the regular purge strategy.

Symptoms

The Guardium internal database is filling up and most of the data is in the GDM_POLICY_VIOLATIONS_LOG table.

Causes

A change to the policy can cause a policy violation rule to be triggered frequently. You might find that most of the data is stored in the GDM_POLICY_VIOLATIONS_LOG table.

Environment

The Guardium collector is affected.

Diagnosing the problem

Run the CLI command support show db-top-tables all.

Resolving the problem

Check the Policy Violations / Incident Management report to identify which policy rule is getting triggered constantly. Then, adjust the policy rule to prevent it from getting triggered as often.

The excess data in the GDM_POLICY_VIOLATIONS_LOG table is purged as part of the regular purge strategy. However, if you would like to manually clean data from GDM_POLICY_VIOLATIONS_LOG table, you can use the command support clean DAM_data policy_violations<start_date><end_date>.

Parent topic: Policies

Reports

- Cannot modify the receiver table for an Audit Process after it has been executed at least once
  If you cannot modify the receiver table for an audit process, clone the audit process and replace the original.
- Cannot see multi-byte characters
  If you export a Guardium report to PDF and the characters are not correct, switch the PDF font configuration.
- File system is almost full
  If the Guardium file system is almost full, change the log rotation strategy.
- Guardium audit reports viewed in Microsoft Excel have rows with unexpected characters
  If you view an Audit report in .csv and see rows with unexpected characters, use another .csv viewer or view it as a .pdf file.
- Reports show IP address as 0.0.0.0

- Request was interrupted or quota exceeded error message
  If you receive an error message that states the request was interrupted or the quota was exceeded when you run a report, divide the report into pieces of shorter reporting interval.
- Rule does not trigger
  If a rule with a value in the policy command field does not trigger as expected, reconfigure the rule.
- Scheduled Job Exceptions every 5 minutes
  If you receive a Scheduled Job exception every 5 minutes, deactivate the alert from the Anomaly Detection page.
- Scheduled jobs exception: merge required, delay executing process
  If you receive an error message that states merge required, delay executing process, reschedule the Audit process.
- The database user is not shown correctly in Guardium reports when you monitor Teradata
  If Guardium reports do not show the database user correctly when you monitor Teradata, configure the Teradata Database.
- Unexpected results in Guardium reports with embedded commands
  If you receive unexpected results in Guardium reports, configure your policy rules to handle depth by using tuples.

Parent topic: Problems and solutions

Cannot modify the receiver table for an Audit Process after it has been executed at least once

If you cannot modify the receiver table for an audit process, clone the audit process and replace the original.

Symptoms

After an audit process runs at least once, you can neither remove nor add a receiver. You can also not modify the following properties for a receiver.

- Action Req.
- Cont.
- Appv. if Empty

Causes

After an Audit Process runs at least once, the receiver table is locked and you cannot modify most of the properties.

Environment

All Guardium configurations (collector, aggregator, central manager) are affected.

Resolving the problem

The following steps enable you to modify the receiver table.

1. Clone the audit process.
2. Make changes to the cloned audit process.
3. Delete the original audit process. However, if you do not want to lose the audit process history, you can rename the audit process.
4. Rename the cloned audit process to the name of the original one.

Parent topic: Reports

Cannot see multi-byte characters

If you export a Guardium report to PDF and the characters are not correct, switch the PDF font configuration.

Symptoms

You can view reports in the GUI. However, when you export the report to PDF, the characters are not correct or missing. The characters appear as question marks or other symbols in the PDF report.

Causes

The default font in Guardium PDF exports does not show multi-byte characters correctly. For example, Greek, Cyrillic, and Chinese characters do not display correctly.

Environment

The collector, aggregator, and central manager are affected.

Resolving the problem

In version 9 and later, switch the PDF font configuration to resolve the problem.

1. Log in as a user in the CLI.
2. Run the command store pdf-config multilanguage_support
3. Select 2 Multi-language.

Parent topic: Reports

File system is almost full

If the Guardium file system is almost full, change the log rotation strategy.

Symptoms

The file system is filling up and approaching 100%.

Causes

Alerts and reports are sent to the syslog and can fill up the file system.

Environment

The collector or aggregator might be affected.

Resolving the problem

By default, the log files rotate weekly and keep five files. However, you can change the log rotation strategy for the log files. Use the following command to keep fewer messages in the system.

```
store logrotate [agg|message] [daily|weekly|monthly] [# of rotations]
```

Parent topic: Reports

Guardium audit reports viewed in Microsoft Excel have rows with unexpected characters

If you view an Audit report in .csv and see rows with unexpected characters, use another .csv viewer or view it as a .pdf file.

Symptoms

When you view an Audit report (in .csv format) in Microsoft Excel, you notice that certain rows are filled with unexpected characters. The characters might look similar to what you find in the full SQL column. The problem is not seen in .pdf reports or in GUI reports.

Causes

Microsoft Excel has a limit on what a cell can contain of 32,767 characters. If your captured SQL is longer than this limit, it will spill over onto the next row.

Environment

The Collector, Aggregator, and Central Manager are affected.

Resolving the problem

Use another .csv viewer that has a larger limit on characters per cell or view the audit report as a .pdf file instead.

Parent topic: Reports

Reports show IP address as 0.0.0.0

Symptoms

The IP address shows as 0.0.0.0. in Guardium.

Causes

While Guardium is decrypting the traffic, the IP address is initially recorded as 0.0.0.0 because the sniffer does not know what the actual IP address is. After the decryption is completed, a separate thread repopulates the session tables with the correct IP address.

Environment

Any database that encrypts the database traffic is affected.

Resolving the problem

Run the same report after a few minutes. To view the correct client IP for newer traffic, add the field Analyzed Client IP from the client/server domain to the report. It is possible that for some rows, the Analyzed Client IP is blank. If it is blank, the decryption for that piece of traffic is not completed.

Parent topic: Reports

Request was interrupted or quota exceeded error message

If you receive an error message that states the request was interrupted or the quota was exceeded when you run a report, divide the report into pieces of shorter reporting interval.

Symptoms

When you run a report in Guardium, you receive the following error message.`Request was interrupted or quota exceeded`.

Causes

The error message `Request was interrupted or quota exceeded` appears when an interactive report does not complete within the 3-minute time limit. The underlying cause is generally the size of the report.

Environment

The collector and aggregator are affected.

Resolving the problem

To resolve the problem, complete one of the following options.

- Divide the report into pieces of a shorter reporting interval. This action is the most recommended method. If a report exceeds 4 GB, it causes a MYSQL table data pointer size exhaustion.
- Increase the query timeout value to a larger value. Click Manage > Activity Monitoring > Running Query Monitor to open the Running Query Monitor.
- Uninstall and reinstall the browser. Type a number of seconds in the Report/Monitor Query Timeout box, and click Update.
- Run the report in the background. Reports that run in the background are not subject to the query timeout.
- Run the report as an audit process.

Parent topic: Reports

Rule does not trigger

If a rule with a value in the policy command field does not trigger as expected, reconfigure the rule.

Symptoms

Rules with a value in the policy Command field do not trigger as expected.

Causes

The cause is a misconfiguration in the command field. The Guardium parser does not consider the command modifiers to be a part of a command.

Environment

Guardium Collectors. The command field in the policy rule is also affected when it is used with wildcard (%).

Resolving the problem

The value in the Command field of the rule must match a value exactly that is shown in SQL Verb, plus a wildcard (%) as needed. This example is correct.

```
GRANT
GRANT%
```

This example is incorrect.

```
GRANT% TO PUBLIC
%GRANT% ADMIN OPTION%
```

ADMIN OPTION and TO PUBLIC do not match and cannot trigger a rule because the Guardium parser does not recognize them as a part of a command. Generally, the parser does not consider command modifiers to be part of a command. Instead, create a report to inspect the traffic that the policy monitors and include the SQL Verb field from the Command entity in that report. Anything that is listed in the SQL Verb field is recognized by the parser and can be used in the Command field of a policy rule. Several commands can be added to a group and the group can be used in the rule instead of a single command. In this case, each group member must match an entry in SQL Verb. Guardium includes several such command groups that you can use or clone.

Parent topic: Policies
Parent topic: Reports

Scheduled Job Exceptions every 5 minutes

If you receive a Scheduled Job exception every 5 minutes, deactivate the alert from the Anomaly Detection page.

Symptoms

You receive the same message in the Scheduled Jobs Exceptions report at regular short intervals, typically every 5 minutes. This interval is the same as the polling interval that anomaly detection runs on.

An example of the Scheduled Jobs Exceptions report might look like the following.

```
Timestamp            Exception Description                              Count of Exceptions
2013-12-05 15:51:22.0 java.lang.NumberFormatException: empty String     1
```

The same exception appears every 5 minutes.

Causes

One of the active alerts is causing the error.

Environment

Guardium collectors and the Aggregator are affected.

Diagnosing the problem

You can check the polling interval and active alerts in the Anomaly Detection page. Click Protect > Database Intrusion Detection > Anomaly Detection to open the Anomaly Detection page.

Resolving the problem

Identify the exact alert that is causing the problem and deactivate it.

1. Deactivate one alert from the Anomaly Detection page.
2. Wait for the length of the polling interval to elapse.
3. Check to see whether the errors stop with that alert deactivated.
4. If not, reactivate the alert and deactivate the next one.
5. Repeat steps 2-5 until you try all alerts.

If you find the alert that is causing the problem and need assistance to understand or stop the error, contact IBM Guardium Technical Support and provide the following items:

1. The exact error text and screen capture.
2. Output of the following CLI commands. If requested, specify the length of one polling interval.

   support must_gather app_issues

   support must_gather alert_issues

Parent topic: Reports

Scheduled jobs exception: merge required, delay executing process

If you receive an error message that states merge required, delay executing process, reschedule the Audit process.

Symptoms

You receive the following message. `Merge required, delay executing Process`. You might receive several of these messages over a short period.

Causes

The audit process requires the merge process to finish before it can run.

Environment

The aggregator is affected.

Diagnosing the problem

Click Reports > Guardium Operational Reports > Aggregation/Archive Log to open the Aggregation/Archive Log. You can also diagnose the problem in agg_progress.log.

Resolving the problem

Reschedule the audit process to run at least 10 minutes after the merge process.

Parent topic: Reports

The database user is not shown correctly in Guardium reports when you monitor Teradata

If Guardium reports do not show the database user correctly when you monitor Teradata, configure the Teradata Database.

Symptoms

When you view records from the monitored Teradata Database in Guardium reports, the database user name field does not show up as expected. The user name is truncated or missing.

Causes

The Teradata Database is not enabled to return the full user name.

Environment

Any Guardium collector that captures data from the Teradata database is affected.

Resolving the problem

Use the following command to enable the Teradata Database to return the full user name, in the correct character set, to the monitoring application. Other applications are not affected.

gtwcontrol -u yes -d

The -d command displays the updated GDO settings.

Note: This setup returns the user name in unencrypted form. If encryption is enabled, the system returns an error message.
Parent topic: Reports

Unexpected results in Guardium reports with embedded commands

If you receive unexpected results in Guardium reports, configure your policy rules to handle depth by using tuples.

Symptoms

You see results in your reports that you do not expect or that you believe should be filtered out by the policy. Conversely, you do not capture statements that you expect to capture.

Causes

The SQL usually has several objects and commands that are embedded in the statement. The policy or report definition is not configured to deal with objects or commands at different depths.

Environment

Guardium collectors are affected.

Resolving the problem

Verify that your conditions match the correct object name. Use the correct main entity to show objects or SQL verbs at different depths. If you still see unexpected behavior, use the group builder to define a group of tuples to use in the policy. A tuple allows multiple attributes to be combined to form a single group member.

Note: Tuple supports the use of one slash and a wildcard character (%). It does not support the use of a double slash.
Parent topic: Reports

Assess and Harden

- CAS is not working with Java 1.7 on Windows
  If Guardium change audit system is not working with Java version 1.7 on Windows, copy msvcr100.dll to your CAS bin folder.
- Vulnerability Assessment exception group members appear in failed test
  If members of a test exception group appear in a failed vulnerability assessment test, use an escape sequence for the backslash character.

Parent topic: Problems and solutions

CAS is not working with Java 1.7 on Windows

If Guardium change audit system is not working with Java version 1.7 on Windows, copy msvcr100.dll to your CAS bin folder.

Symptoms

Guardium CAS works with older Java versions but not with Java 1.7.

Causes

msvcr100.dll is missing from <GUARDIUM STAP directory>\cas\bin\

Environment

Guardium CAS on Windows is affected.

Resolving the problem

To resolve the problem, complete the following steps.

1. Find the path where Java 1.7 is installed on your system such as C:\Program Files (x86)\Java\jre7\bin
2. Find the location of the library jvm.dll within the Java path found in the previous step.
3. Edit the cas.cfg file in the <CAS directory>\conf directory. For example, C:\Program Files (x86)\GUARDIUM_STAP\cas\conf\cas.cfg is a typical file path.
4. Find the line corresponding to the JVM such as ;JVM=c:\program files\java\jre1_2_3\bin\client\jvm.dll.
5. Remove the semicolon from the beginning of the line. Then, set the JVM to the path of the library jvm.dll in step 2. `JVM=C:\Program Files (x86)\Java\jre7\bin\server\jvm.dll`.
6. Copy msvcr100.dll from the bin folder in your Java 7 installation directory to your <CAS directory>\bin folder. For example, copy C:\Program Files (x86)\Java\jre7\bin\msvcr100.dll to C:\Program Files (x86)\Guardium\GUARDIUM_STAP\cas\bin\msvcr100.dll.
7. Restart the change audit system.

Note: This is only needed for Java version 1.7. For older versions of Java, this step is not needed.
Parent topic: Assess and Harden

Vulnerability Assessment exception group members appear in failed test

If members of a test exception group appear in a failed vulnerability assessment test, use an escape sequence for the backslash character.

Symptoms

Some members of a test exception group appear in the details field when you run a vulnerability assessment. The group contains members with a backslash character and a REGEX tag such as `(R)US\John Doe`.

Causes

Special characters can trigger errors when Guardium parses the exception group.

Environment

Guardium collectors are affected.

Resolving the problem

Use an escape sequence for the backslash character or do not use the REGEX tag (use an exact match). Either of these examples work.

```
US\John Doe
```

```
(R)US\\John Doe
```

The REGEX tag (R) is used to trigger a regular expression search of the details field to remove any string that matches the regular expression. A backslash or any other character that has a meaning in a regular expression needs a backslash escape sequence to avoid parsing errors. If you do not use the (R) tag, the group member must exactly match the entire line in the details field for Guardium to make a match. To pass the vulnerability test, the details field of the test must be empty.

Parent topic: Assess and Harden

Configuring your Guardium system

Parent topic: Problems and solutions

Cannot configure STAP after upgrade

Configure S-TAP in Guardium after you upgrade S-TAP.

Symptoms

After you upgrade S-TAP using the Guardium Installation Manager (GIM), you cannot configure the database path parameters in the Inspection Engine in Guardium even though the installation results for the module show as successful.

Causes

K-TAP is not properly upgraded if the new S-TAP is installed as a fresh module. Because the old K-TAP module is not removed, there is a protocol mismatch between the old K-TAP module and the new S-TAP.

Environment

S-TAP installed in UNIX and Linux such as AIX, HP-UX, Linux, and Solaris.

Diagnosing the problem

To diagnose the problem, run the guard_diag utility to collect must gathering data for Guardium S-TAP.

The following lines are seen in the syslog file.

```
STAP and KTAP Protocol Version Mismatch,
Exit!!!!!: No such file or directory
Tap_controller::init failed
GUARD-01: Error Initializing STap
```

The modules log file lists the old K-TAP. For example: `ktap_24276 338760 0`

Resolving the problem

To resolve the problem, follow these steps in the GIM modules installation pane.

1. Set K-TAP Live Update to Y.

2. Set K-TAP_ENABLED to Y and reinstall the new S-TAP.

Parent topic: Configuring your Guardium system

Guardium fails to recognize the network device VMXNET x

If Guardium fails to recognize the network device VMXNET x, install Guardium on a virtual machine and add the network adapter.

Symptoms

Guardium fails to recognize the network device VMXNET x during the installation on VMware. You receive the error `eth0: unknown interface: No such device` when you install Guardium on VMware as a guest. The error message appears after you restart the system.

Causes

VMXNET x virtual network adapter requires a specific driver that is only contained in VMware tools and no operating system has the driver. Guardium is running on Linux and the installer does not have a driver for VMXNET x.

Environment

The Guardium system is affected.

Resolving the problem

Resolve the problem by completing the following steps.

1. Create a virtual machine on VMware by using a default network adapter such as E1000 or Flexible.
2. Install Guardium on the virtual machine.
3. Install the current GPU cumulative patch for Guardium.
4. After the installation, log on to the CLI console and run the command setup vmware_tools install to install VMware tools.
5. Shut down the Guardium system from the CLI console with the command stop system.
6. Edit the virtual machine settings with a VMware client tool such as VMware Infrastructure Client. Select the current network adapter and remove it.
7. Add the network adapter called VMXNET.
8. Restart the Guardium system.

Parent topic: Configuring your Guardium system

Guardium network interface error after system board replacement

If you receive an error message after a hardware repair, reset the network parameters.

Symptoms

After a hardware repair such as replacing the system board on the Guardium appliance, the network connectivity is lost. The following error message occurs for each network interface when the appliance is rebooted.

```
rtnetlink answers: no such device
```

Causes

After you replace the system board, the MAC address will change. This change causes a disparity between the actual MAC address and what is stored in the interface configuration files.

Environment

Any Guardium appliance (collector, aggregator, or central manager) on which the system board has been replaced and all Guardium versions are impacted.

Resolving the problem

Log in to the appliance from the console as user CLI and reset the network parameters by running the following commands.

```
store network interface inventory
restart network
store network interface ip<IP_address>
store network interface mask<netmask>
store network routes defaultroute<gateway_address>
restart network
```

If the problem is still not resolved, contact Guardium Support for manual intervention.

Parent topic: Configuring your Guardium system

Guardium virtual machine is not accessible from the network

If the Guardium virtual machine is not accessible from the network, run the command store network interface inventory and restart the system.

Symptoms

You implemented a new Guardium system as a virtual machine and performed all the required initial network configuration. However, you cannot ping the system using the IP address and the system is not accessible in the network.

Causes

The MAC address assigned to the virtual machine by the virtual environment does not match the MAC address in Guardium.

Environment

The collector, aggregator, and central manager are affected.

Diagnosing the problem

To diagnose the problem, ping the IP address on a network. Use the command ping<appliance's ip address>. If it fails, show the MAC address for the system.

1. Log in as user "cli" .
2. Run the command show network macs to show the MAC address stored in the Guardium configuration.
3. From the administration utility for your virtual environment, check the MAC address for the virtual machine.
    a. Open the VMWare Workstation.
    b. Right-click the virtual machine and select Settings or Properties to open the Virtual Machine Settings.
    c. Select Network Adapter under Hardware.
    d. Click Advanced to open the Network Adapter Advanced Settings.
    e. Compare the MAC address from steps 2 and 3.

Resolving the problem

To resolve the problem, complete the following steps.

1. Log in to the Guardium system as user "cli".
2. Run the command store network interface inventory.
3. Enter `y` to reset the NICs.
4. Restart the system with the command restart system.

Parent topic: Configuring your Guardium system

SSLv3 is enabled

If you receive a warning that `SSLv3 is enabled`, disable SSLv3 to prevent the POODLE exploit.

Symptoms

You receive the following warning: `SSLv3 is enabled`.

Causes

SSLv3 contains a protocol vulnerability known as Padding Guardium® On Downgraded Legacy Encryption (POODLE). If SSLv3 is enabled on your system, this vulnerability allows attackers to force an SSL/TLS fallback to SSLv3, break the encryption, and intercept network traffic in plaintext. The vulnerability is detailed in the National Vulnerability Database as CVE-2014-3566.

Guardium recommends disabling SSLv3 on all systems to prevent the POODLE exploit, and SSLv3 is disabled by default on new Guardium systems. However, older systems and some upgrade scenarios may leave SSLv3 enabled.

This topic describes how to check the status of SSLv3 and disable it if necessary.

Attention: Disabling SSLv3 can disrupt connectivity between a Guardium v10 Central Manager and some managed units running Guardium v9 before GPU 500. If you have a mixed environment with managed units running Guardium v9 before GPU 500, either upgrade the managed units to GPU 500 or apply patch 9501 before disabling SSLv3.

Resolving the problem

1. Verify the status of SSLv3 using the following CLI command: `show sslv3`.
    - If the output indicates `SSL setting is disabled`, SSLv3 is disabled. No additional steps are required to disable SSLv3.
    - If the output indicates `SSL setting is enabled`, SSLv3 is enabled. Continue with this procedure to disable SSLv3.
2. Disable SSLv3 using the following CLI command: `store sslv3 off`. The command output should be similar to the following:

```
Current SSL setting is enabled.  Will change to disabled.
Restarting gui
Changing to port 8443
From port 8443
Stopping.......
ok
```

3. Verify that SSLv3 is now disabled: `show sslv3`. The output should now indicate `SSL setting is disabled`.

Parent topic: Configuring your Guardium system

Access Management

- Cannot log in to Guardium except as admin or accessmgr
  If you cannot log in to the Guardium GUI except admin or accessmgr, check the authentication configuration settings.
- Guardium accessmgr password reset
  If you lose the accessmgr password and cannot log in, contact Guardium support.

Parent topic: Problems and solutions

Cannot log in to Guardium except as admin or accessmgr

If you cannot log in to the Guardium GUI except admin or accessmgr, check the authentication configuration settings.

Symptoms

You are unable to log in to Guardium with any user except admin or accessmgr. You see an invalid user name or password error despite using the correct user and password as defined by accessmgr. You receive the following error message. `Invalid user name and/or password. Please reenter your credentials..`

Causes

The authentication setting is not configured as local.

Environment

The collector, aggregator, and central manager are affected.

Resolving the problem

To solve the problem, change the authentication setting to local. This action enables you to log in as any user defined in the accessmgr.

Parent topic: Access Management

Guardium accessmgr password reset

If you lose the accessmgr password and cannot log in, contact Guardium support.

Symptoms

You lost the Guardium accessmgr password and cannot log in to the GUI. The account is also locked after successive failed attempts.

Causes

Guardium prohibits multiple failed login attempts.

Environment

The collector, aggregator, and central manager are affected.

Resolving the problem

Log in to the CLI and run the following command: support reset-password accessmgr<N>|random.

You can use <N> or random where <N> is a number in the range of 10000000 - 99999999. Random automatically generates a number in the range of 10000000 - 99999999. Open a PMR with IBM Guardium support and send the following output.

```
G10.ibm.com> support reset-password accessmgr random
Password for accessmgr account have been successfully reset using keyword:<passkey>
Please provide these number to Guardium Customer Service to receive actual account password.
ok
```

After you receive the new password, unlock the account.

1. Use the following command to unlock the account. unlock accessmgr.
2. Log in as accessmgr and edit the accessmgr details to enter a temporary password.
3. Log in again with the temporary password.
4. When you are prompted, enter a new password.

Parent topic: Access Management

Aggregation

- Cannot convert Guardium collector to aggregator
  If you cannot convert a Guardium collector to a Central Manager aggregator, reinstall Guardium and select aggregator during installation.
- Data Export configuration change from a Guardium managed system's GUI fails with error
  If a Data Export configuration change fails, make sure that the shared secret key is the same on the collector and aggregator.
- Difference between audit process results and report
  If there is a difference between your audit process results and the report, check that all appliances are set to the same timezone.
- HY000 errors after restoring the configuration in an aggregator
  If you receive HY000 errors after you restore the configuration in an aggregator, run a dummy import.

Parent topic: Problems and solutions

Cannot convert Guardium collector to aggregator

If you cannot convert a Guardium collector to a Central Manager aggregator, reinstall Guardium and select aggregator during installation.

Symptoms

You try to convert a Guardium collector to an aggregator with the command store unit type manager aggregator.

However, the following command shows that the unit type is still listed as manager.

```
> show unit type
Manager
```

Causes

A collector cannot be converted to an aggregator with a CLI command.

Environment

Guardium collectors are affected.

Resolving the problem

To convert a collector to an aggregator, reinstall the Guardium product and select aggregator as the unit type during installation. After you install the aggregator, you can convert it to a central manager aggregator with the command store unit type manager.

Central Manager/Aggregator enforcement
: Starting with v9.5 (v9.0 patch 500), the application will enforce that a Central Manager has to be an Aggregator-type appliance. This would mean that starting with v9.5, only aggregator-type appliances would be promotable to the Central Manager appliance. Pre-existing pre-v9.5 CM appliances are not subject to this change.

Parent topic: Aggregation

Data Export configuration change from a Guardium managed system's GUI fails with error

If a Data Export configuration change fails, make sure that the shared secret key is the same on the collector and aggregator.

Symptoms

You attempt to save new settings for the data export and get the error when you click Apply to save the configuration:

```
Please correct the following errors and try again:
A test data file could not be sent to this host with the parameters given. Please confirm the hostname or IP address is entered
correctly, the host is online, the target directory exists and can be written to by the user given, and the password given is
correct for that user.
```

Causes

Guardium attempts to log in with scp to the target host with the user and password that are specified in the Data Export configuration. Then, Guardium attempts to copy a test file to the target directory. The shared secret on this system does not match the Shared Secret on the aggregator you are trying to set this system to export to.

Environment

The Guardium configurations: collector and aggregator are affected.

Resolving the problem

Make sure that the shared secret key is the same on the collector and aggregator. You can use one of the following methods:

1. If you know the shared secret on the aggregator, set the shared secret on the collector to the same value. You can use one of these methods:
   - From CLI: use command store system shared secret to set the Shared secret key
   - From GUI, set the shared secret key under Setup > System > System Configuration.
2. Back up the current shared secret on the aggregator and restore it to the collector.
   - On the aggregator, run the CLI command.

     ```
     aggregator backup keys file <user@host:/path/filename>
     Parameters
     user@host:/path/filename
     ```

     For the file transfer operation, specify a user, host, and full path name for the backup keys file. The user that you specify must have the authority to write to the specified directory.
   - On the collector, run this command to restore the shared secret key:

     ```
     aggregator restore keys file<user@host:/path/filename>
     ```
3. Reset the shared secret for both appliances to be the same.
   Note: If you change the shared secret for the aggregator, you need to reset the shared secret for all other Guardium systems that export to it.

Parent topic: Aggregation

Difference between audit process results and report

If there is a difference between your audit process results and the report, check that all appliances are set to the same timezone.

Symptoms

You set a report to run on the aggregator as part of an audit process with time parameters, for example, Start of Last Day and End of Last Day. When you look at the results of that report, the first time stamps are always at a set tme after 00.00 for example, 02.00. Additionally the last time stamps are always at a set time before 23.59 for example, 21.59. However, when you run the report interactively, the time stamps are shown as expected.

Causes

The collector and aggregator time zones might not be set the same.

Environment

The aggregator is affected.

Diagnosing the problem

Check that all appliances are set to the same timezone. Use the following command. `show system clock timezone.`

Resolving the problem

If the collector and aggregator are not set in the same timezone, configure the timezone of the appliances with the CLI.

```
store system clock timezone list
store system clock timezone <timezone>
```

Verify that the time is correct on the appliance with the following commands.

```
show system clock datetime
store system clock datetime
```

The datetime can also be synchronized by using an NTP server with the following commands.

```
show system ntp all
store system ntp state
store system ntp server
```

Parent topic: Aggregation

HY000 errors after restoring the configuration in an aggregator

If you receive HY000 errors after you restore the configuration in an aggregator, run a dummy import.

Symptoms

When you restore the configuration of an aggregator or the Central Manager, you receive one or both of these messages.

```
ERROR 1031 (HY000) at line 1: Table storage engine for 'GUARD_USER_ACTIVITY_AUDIT' doesn't have this option
ERROR 1031 (HY000) at line 1: Table storage engine for 'AGGREGATOR_ACTIVITY_LOG' doesn't have this option
```

Causes

This error condition can occur if there is a temporary mismatch in the internal databases.

Environment

The collector and aggregator are affected.

Resolving the problem

To resolve the problem, run a dummy import.

Parent topic: Aggregation

Central Management

- A user is disabled in a Guardium managed unit, but shows as enabled on Central Manager
  If a user is disabled in a Guardium managed unit but shows as enabled on Central Manager, run the Portal User Sync.
- Central Manager does not recognize the new version of upgraded units
  If the Central Manager does not recognize the new version of upgraded units, select the upgraded units and refresh the page.
- Scheduled tasks do not fire at the scheduled time
  If scheduled tasks do not fire at the scheduled time, schedule the import time to run after the portal user sync.
- Torque exception in Central Management view of GUI
  If there is a torque exception in Central Management, delete the custom group and create a new group.

Parent topic: Problems and solutions

A user is disabled in a Guardium managed unit, but shows as enabled on Central Manager

If a user is disabled in a Guardium managed unit but shows as enabled on Central Manager, run the Portal User Sync.

Symptoms

A user is disabled in the managed unit. The user's account is re-enabled in the Central Manager but the user is still showing as disabled in the managed unit. The user's account shows as enabled in the Central Manager.

Causes

The user's account in the Central Manager is not synchronized with the managed unit.

Environment

A combination of the Central Manager, collector, or aggregator might be affected.

Resolving the problem

To synchronize the current user status between the Central Manager and the managed unit, run a Portal user sync.

1. Log in to the Central Manager as an admin user.
2. Click Manage > Central Management > Portal User Sync to open the Portal User Synchronization.
3. Click Run Once Now.

If the user's account between the managed unit and the Central Manager is still not synchronized, contact the IBM Guardium Technical Support for assistance.

Parent topic: Central Management

Central Manager does not recognize the new version of upgraded units

If the Central Manager does not recognize the new version of upgraded units, select the upgraded units and refresh the page.

Symptoms

The Central Manager might not immediately recognize the new version of an upgraded aggregator or collector it manages. Pushing a patch from the Central Manager, which requires the new version, can result in an error that shows the unit is still at the previous version.

The managed unit's old version still displays in the Central Management view of the GUI. The unit ping times in that view, which implies good communication between the Central Manager and managed units.

Causes

The GUI needs to be refreshed to pull the new version information.

Environment

The Guardium Central Manager is affected.

Resolving the problem

In the Central Management view of the GUI, select the upgraded units and push Refresh. This action pulls the new version information from the units.

Parent topic: Central Management

Scheduled tasks do not fire at the scheduled time

If scheduled tasks do not fire at the scheduled time, schedule the import time to run after the portal user sync.

Symptoms

Import fails and you receive the following message in agg_progress.log.

```
* 05/20 04:00:01 --- Import cannot start
(guard_agg|turbine_backup.sh|restore_from_file.pl already running)
* 05/20 20:00:46 --- Merge cannot start - aggregation still active
```

Causes

There is a conflict with the Central Manager portal user sync.

Environment

The aggregator is affected.

Diagnosing the problem

Find out which task is running in the background. Click Reports > Guardium Operational Reports > Aggregation/Archive Log to open the Aggregation/Archive Log.

Resolving the problem

To resolve the problem, schedule the import time to run after the portal user sync. Run the portal user sync every hour and the import time 30 minutes after that time.

Parent topic: Central Management

Torque exception in Central Management view of GUI

If there is a torque exception in Central Management, delete the custom group and create a new group.

Symptoms

Selecting a certain custom group in the Central Management view of the Guardium GUI displays an error instead of the managed units in the group.

```
org.apache.torque.TorqueException: Failed to select one and only one row.
```

After the exception appears, it shows for any group or view under the Central Management tab. The exception even appears for groups that were previously working until you log out of the GUI and log back in.

Causes

This torque exception might occur if one of the managed units in the group was unregistered from the managed unit instead of the Central Manager.

Environment

Guardium Central Manager is affected.

Resolving the problem

Delete the custom group and create a new group that contains the same members.

Parent topic: Central Management

S-TAPs and other agents

- AIX 6.1 fails when you install or upgrade IBM Security Guardium S-TAP
  If the operating system fails when you install or upgrade Guardium S-TAP on AIX 6.1, apply the Fix Packs AIX 6.1.
- Error opening shared memory area when you configure Guardium COMM_EXIT_LIST for DB2
  If you receive an error message when you configure Guardium COMM_EXIT_LIST, authorize the DB2 instance owner with the guardctl command.
- Guardium fails to collect shared memory traffic from Informix
  If Guardium fails to collect shared memory traffic from Informix, check the inspection engine configuration.
- High CPU and I/O Use in Guardium STAP host
  If you observe a high CPU or I/O usage, review the configuration for all of the inspection engines.
- Missing information from the login packet
  If you are missing information from the login packet, collect the S-TAP debug trace and slon trace.
- Nanny process is killing sniffer
  If the nanny process is killing the sniffer, you might have too much traffic coming in.
- Sniffer cannot connect to UNIX S-TAP
- UNIX S-TAP cannot start
  If a UNIX S-TAP cannot start, its buffer size might be too large.
- S-TAP does not start automatically on Linux
  If the S-TAP agent for DB2 or Oracle does not start automatically on Linux, check for the /etc/event.d/ directory.
- S-TAP returns not FIPS 140-2 compliant
  If you receive an error that about FIPS 140-2, change the configuration through the S-TAP Control page.
- The K-TAP kernel module is still present after the uninstallation of S-TAP
  If the K-TAP kernel module is still present after the uninstallation of S-TAP, manually remove it.
- UNIX S-TAP cannot read more than 16 inspection engines
  If UNIX S-TAP cannot read more than 16 inspection engines, change listening port parameters or use PCAP.
- Windows S-TAP service crashes on startup with error ID 1000
  If the S-TAP crashes with error ID 1000, check the SOFTWARE_TAP_IP parameter in the guard_tap_ini configuration file.
- z/OS S-TAP fails to show active the Guardium system
  If z/OS S-TAP fails to show active on the Guardium system, restart the inspection-core.

Parent topic: Problems and solutions

AIX 6.1 fails when you install or upgrade IBM Security Guardium S-TAP

If the operating system fails when you install or upgrade Guardium S-TAP on AIX 6.1, apply the Fix Packs AIX 6.1.

Symptoms

The operating system fails when you install or upgrade Guardium S-TAP on AIX 6.1. The AIX crash memory dump shows the following stack trace.

```
Error ID: DD11B4AF Resource Name: SYSPROC
Detail Data: 00007FFFFFFFD080 0000000000473260
0000000000020000 8000000000029032

Symptom Information:
Crash Location: [0000000000473260] execvex_common+1880
Component: COMP Exception Type: 131

Stack Trace:
```

```
[0000000000473260] execvex_common+1880
[000000000047744C] execve+A8
[F1000000C083E84C] my_execve+424
```

Causes

This crash is a known issue in AIX version 6.1 due to a system crash in the execvex_common code path.

Environment

Any S-TAP to be installed in AIX 6.1 Operating System is affected.

Resolving the problem

To apply the Fix Pack AIX 6.1 6100-08-04 and resolve the problem, see http://www-01.ibm.com/support/docview.wss?uid=isg1IV50179

Parent topic: S-TAPs and other agents

Error opening shared memory area when you configure Guardium COMM_EXIT_LIST for DB2

If you receive an error message when you configure Guardium COMM_EXIT_LIST, authorize the DB2 instance owner with the guardctl command.

Symptoms

After you configure DB2 COMM_EXIT_LIST to use Guardium libguard and restart the DB2 server, you get the following error in the DB2 diag log.

```
2013-06-28-11.41.12.306169-300 E870950E486 LEVEL: Severe
PID : 15764 TID : 139905833363200 PROC : db2sysc 0
INSTANCE: db2001 NODE : 000
APPHDL : 0-16
HOSTNAME: dbhost1
EDUID : 54 EDUNAME: db2agent () 0
FUNCTION: DB2 UDB, DRDA Communication Manager, sqljcCommexitLogMessage,
probe:234
DATA #1 : String with size, 91 bytes
WARNING: Shmem_access /.guard_writer0 failed Error opening shared memory area errno=2 err=8
```

Causes

The following message indicates that the Guardium library was unable to create the shared memory device that it requires.

```
Shmem_access /.guard_writer0 failed
Error opening shared memory area
errno=2
err=8
```

The DB2 instance owner must be added as an authorized user using the guardctl command.

Environment

Guardium collectors that use DB2 Exit (Version 10) Integration with S-TAP are affected.

Resolving the problem

The DB2 instance owner must be added as an authorized user by using the guardctl command.

1. Stop the DB2 instance.
2. Authorize the DB2 instance owner.
3. Start the DB2 instance.

If the Guardium Installation Manager (GIM) is not installed, authorize the DB2 instance owner with the following command.

```
<guardium_installdir>/bin/guardctl authorize-user<db2 instance owner>
```

If the Guardium Installation Manager (GIM) is installed, authorize the DB2 instance owner with the following command.

```
<guardium_installdir>/modules/ATAP/current/files/bin/guardctl authorize-user<db2 instance owner>
```

For example, if the DB2 instance owner is db2001 and GIM is installed in /usr/local/guardium, the command is `/usr/local/gim/modules/ATAP/current/files/bin/guardctl authorize-user db2001`.

Parent topic: S-TAPs and other agents

Guardium fails to collect shared memory traffic from Informix

If Guardium fails to collect shared memory traffic from Informix, check the inspection engine configuration.

Symptoms

Guardium S-TAP does not collect shared memory traffic from Informix.

Causes

The inspection engine is not correctly configured.

Environment

Any S-TAP collection from any Informix system can be affected.

Resolving the problem

Check the inspection engine configuration under Manage > Activity Monitoring > S-TAP Control. Ensure that the value in the Process Name field matches the result of the following command on the database server.

```
ls -lrt /INFORMIXTMP/.inf.*
```

Informix: /INFORMIXTMP/.inf.sqlexec Applies to all Informix platforms but Linux. For Informix with Linux, example: /home/informix11/bin/oninit

Informix must be running for this command to return a value.

For Linux servers using A-TAP, A-TAP must be configured to collect any shared memory traffic. Set the value to the same value as the --db-info parameter in the A-TAP configuration before you activate A-TAP.

Parent topic: S-TAPs and other agents

High CPU and I/O Use in Guardium STAP host

If you observe a high CPU or I/O usage, review the configuration for all of the inspection engines.

Symptoms

You observe a high CPU or I/O usage by the Guardium S-TAP process.

Causes

The following items are common causes.

1. An error in the configuration of one of the inspection engines. If there are errors in an inspection engine, the S-TAP process restarts frequently or tries to reconnect to the inspection engine repeatedly.
2. The K-TAP portion of the S-TAP is sending connection information along with a confirmation request to the S-TAP. This step is causing delays.
3. ORACLE RAC is used, but the unix_domain_socket_marker parameter is not set in the S-TAP configuration file to avoid monitoring potentially large amounts of Oracle RAC traffic.
4. The User ID Chain (UID chain) feature is enabled, for example, parameter hunter_trace=1 in the S-TAP configuration file. Hunter trace is used for UID chain and can be quite CPU intensive for S-TAP.
5. The firewall is enabled (firewall_installed=1). This firewall forces S-TAP to request verdicts for each new session that is observed which can hurt S-TAP performance.

Environment

S-TAP installed in AIX

Resolving the problem

Based on the cause, take the corresponding actions.

1. Review the configuration for all of the inspection engines and make sure that there are no errors in any of the parameters. For example, make sure the database installation directory, executable, ports, and any other parameters applicable to your inspection engine are correctly set with no misspellings or wrong values.
2. Set S-TAP configuration parameter ktap_fast_tcp_verdict to 1 (ktap_fast_tcp_verdict = 1 in the guard_tap.ini configuration file) and restart the S-TAP. Here are the possible settings.

   ktap_fast_tcp_verdict=0: KTAP confirms that the session is the database connection that the inspection engine configured by checking ports and Ips.

   ktap_fast_tcp_verdict=1: KTAP does not send the request to S-TAP while the session's ports are in the range.

3. Disable the UID Chain feature if not needed by setting hunter_trace=0 and restarting the S-TAP.
4. Set firewall_installed=0 if SGATE is not needed and restart the S-TAP.

Parent topic: S-TAPs and other agents

Missing information from the login packet

If you are missing information from the login packet, collect the S-TAP debug trace and slon trace.

Symptoms

You encounter issues in Guardium relating to missing information from the login packet such as database user name, source program, or database name.

Causes

Login packets might miss information when the session is too short.

Environment

The Guardium collector is affected.

Resolving the problem

Collect the S-TAP debug trace on the database server where the Guardium S-TAP is installed and the slon trace on the collector.

Refer to the Technotes in the Related URL section for details on collecting each of these traces.

1. Run both traces at the same time.
2. Generate a new database session that re-creates the issue while both traces are running. Login packets are only sent when the database connection is open.
3. Add session start, client port, and server port to your existing report. Refresh the report after you re-create the issue with the new connection.
4. Confirm that the traces are running during the session by checking the session start.
5. Leave the session open for at least 5 minutes to allow the sniffer to analyze the login packets.
6. Send the session with the missing fields. State the application name you used to generate the session, database name, DB user you connected as, type of connection, SQL statement, and any other pertinent details.
7. Collect the S-TAP debug trace file on the database server, the slon trace on the Guardium collector, and the current sniffer must gather.

Parent topic: S-TAPs and other agents

Nanny process is killing sniffer

If the nanny process is killing the sniffer, you might have too much traffic coming in.

Symptoms

A message similar to the following is reported one or more times in Guardium system log (messages) or Alerts:

```
Nanny process error condition. The nanny process killed the sniffer. VmData was number and was over the limit.
```

Causes

The sniffer memory usage reached over 90% of the available memory and the nanny process has restarted it, which is expected behavior of the product.

Environment

Guardium collector

Resolving the problem

If you are observing this message frequently, there is too much traffic coming to the Guardium system. Reduce traffic to this Guardium system to resolve this message. For example, you may move some STAPs to a collector with less load, ignore some traffic in your policy, or implement load balancing to spread the traffic among more than one collector.

If the message is observed on very few occasions, it is most likely a momentary spike in traffic. To resolve the message, identify the reason for the spike and avoid the trigger. For example, you can review which processes were running at that time, identify the ones generating more traffic. If this message always coincides with a particular process or processes running, reduce the concurrent traffic at that time. For example, you can move heaviest process to run at a different time, or ignore some of this traffic through a policy.

Parent topic: S-TAPs and other agents

Sniffer cannot connect to UNIX S-TAP

Symptoms

When you specify a different number of threads, such as 20, by using the command snif -t 20, the sniffer cannot connect to the UNIX S-TAP. In the GUI console, the status of the S-TAP is inactive.

Causes

The sniffer starts with six threads by default. When the number of threads exceeds the limitation, the sniffer cannot connect to the UNIX S-TAP because of undefined behavior.

Environment

UNIX S-TAP is affected.

Resolving the problem

Reduce the number of threads to make sure that the connection can be established successfully.

Parent topic: S-TAPs and other agents

UNIX S-TAP cannot start

If a UNIX S-TAP cannot start, its buffer size might be too large.

Symptoms

The S-TAP cannot start and issues the following messages:

```
mmap: Not enough space
Can't initialize: Can't mmap buffer file /tmp/stapbuf/192.168.100.107.0.buf
Error Initializing: Stap cannot initialize SQLGuard queue
```

Causes

The S-TAP is unable to allocate enough memory to match the buffer file.

Resolving the problem

Reduce the buffer file size for the S-TAP. The size is specified in the buffer_file_size parameter in the guard_tap.ini file.

Parent topic: S-TAPs and other agents

S-TAP does not start automatically on Linux

If the S-TAP agent for DB2 or Oracle does not start automatically on Linux, check for the /etc/event.d/ directory.

Symptoms

The S-TAP process does not automatically start on Linux even though the /etc/inittab file shows a correct U-TAP entry.

Causes

Various Linux distributions such as RedHat 6 deprecated the use of the traditional init daemon that uses the etc/inittab file. They replaced it with an init process called upstart. Upstart uses the /etc/event.d and /etc/init directories for the automated start, stop, and respawn of processes such as U-TAP.

The S-TAP installer now checks for the existence of the /etc/event.d directory. If it exists, then entries in /etc/init are created for use by upstart. If it does not exist, then entries in /etc/inittab are created for use by the traditional init daemon.

If /etc/event.d is missing for any reason on a system with upstart, the inittab file is populated instead. The S-TAP process does not start or respawn when needed.

Environment

S-TAPs running on Linux are affected.

Resolving the problem

Check for the existence of the /etc/event.d/ directory.

If the /etc/event.d/ directory does not exist, complete the following steps to resolve the situation.

1. Uninstall the existing S-TAP installation.
2. Create the /etc/event.d dir as user root (mkdir /etc/event.d) .
3. Install the S-TAP.

Parent topic: S-TAPs and other agents

S-TAP returns not FIPS 140-2 compliant

If you receive an error that about FIPS 140-2, change the configuration through the S-TAP Control page.

Symptoms

Supported: - Solaris X86 - Linux x86/64 - Linux x86/32 - Linux S390X - Linux IA64
Not Supported: - Solaris SPARC - AIX PowerPC - HPUX RISC - HPUX IA64 - Linux PowerPC

You see the following message in the S-TAP event log.

```
LOG_ERR: To enable FIPS 140-2 mode set use_tls=1
```

Causes

FIPS 140-2 is a U.S. government security standard for cryptographic modules. If you see this message, it indicates that the S-TAP configuration does not meet government requirements.

Note: This message does not indicate that there is an error with the S-TAP.

Environment

Guardium S-TAP is affected.

Supported: Solaris X86; Linux x86/64; Linux x86/32; Linux S390X; Linux IA64

Not Supported: Solaris SPARC; AIX PowerPC; HPUX RISC; HPUX IA64; Linux PowerPC

Resolving the problem

To enable FIPS compliance, the guard_tap.ini file must have the following settings.

```
use_tls=1
```

You can change the configuration by using one of the following methods.

1. Click Manage > Activity Monitoring > S-TAP Control.
2. Modify the details section for the relevant S-TAP and use the TLS check boxes.
3. Restart the S-TAP.

You can also edit the guard_tap.ini file on the DB server directly and restart the S-TAP.

Parent topic: S-TAPs and other agents

The K-TAP kernel module is still present after the uninstallation of S-TAP

If the K-TAP kernel module is still present after the uninstallation of S-TAP, manually remove it.

Symptoms

The K-TAP kernel module is still present after the uninstallation of S-TAP on a Solaris server.

Causes

The server did not restart properly to remove the K-TAP kernel module on Solaris servers.

Environment

The Solaris server after the uninstallation of S-TAP is affected.

Diagnosing the problem

Check on the Solaris server by running both modinfo | grep ktap and ls -al /dev/*tap*.

Resolving the problem

Manually remove the K-TAP kernel with the following steps.

1. Check that /etc/init.d/upguard is removed.
2. Remove /kernel/drv/sparcv9/ktap* and /kernel/drv/ktap*.
3. Run modinfo | grep ktap to get the name of the loaded driver.
4. Then, run rem_drv<loaded driver>. For example: `rem_drv ktap_36821`.
5. Remove /dev/ktap* and `/dev/guard_ktap`.
6. Restart the server.
7. Run modinfo | grep ktap to make sure that the driver is no longer loaded.
8. Remove GIM and gsvr entries from /etc/inittab (if you are using GIM only).
9. Manually clean up remaining files in /usr/local/guardium.

Parent topic: S-TAPs and other agents

UNIX S-TAP cannot read more than 16 inspection engines

If UNIX S-TAP cannot read more than 16 inspection engines, change listening port parameters or use PCAP.

Symptoms

UNIX S-TAP reads only the first 16 `port_range` definitions in the inspection engine settings.

Causes

By design K-TAP can read only 16 `port_range` definitions.

Environment

UNIX S-TAP that uses K-TAP and defines more than 16 inspection engines is affected.

Resolving the problem

Use `port_range_start` and `port_range_end` parameters to include all of the required ports in the first inspection engine definition. This action intercepts all of the traffic from the specified port range. If you need to ignore some ports in the range, you can define a policy to ignore the unnecessary server ports.

The following example defines listening ports 50000 - 50020 as target ports to be monitored.

```
[DB_0]
port_range_end=50020
port_range_start=50000
```

Otherwise, use PCAP for TCP connections by setting `ktap_local_tcp=1` and `devices=<device_name>`.

```
[TAP]
ktap_local_tcp=1
devices=<Network Device Name>
```

Parent topic: S-TAPs and other agents

Windows S-TAP service crashes on startup with error ID 1000

If the S-TAP crashes with error ID 1000, check the SOFTWARE_TAP_IP parameter in the guard_tap_ini configuration file.

Symptoms

The S-TAP on a Windows server does not start. The Windows event log shows errors from Guardium S-TAP with event ID 1000.

```
Log Name:      Application
Source:        Application Error
Event ID:      1000
Task Category: (100)
Level:         Error
Keywords:      Classic
Description:
Faulting application name: guardium_stapr.exe, version: 9.0.0.0
Exception code: 0x40000015
```

Causes

S-TAP cannot connect to the Windows system because the wrong SOFTWARE_TAP_IP is specified in the guard_tap.ini file.

Environment

Any Guardium S-TAP for Windows is affected.

Resolving the problem

Ensure the `SOFTWARE_TAP_IP` parameter in the guard_tap.ini configuration file matches the correct IP address of the Windows server. This parameter is passed on the installation CLI or in the IBM Guardium Installation Manager (GIM) parameters.

Parent topic: S-TAPs and other agents

z/OS S-TAP fails to show active the Guardium system

If z/OS S-TAP fails to show active on the Guardium system, restart the inspection-core.

Symptoms

z/OS S-TAP fails to show active on the Guardium system after you start it for the first time. The policy is correctly configured with a DB2 or IMS Collection Profile and installed. The z/OS S-TAP is properly configured to use port 16022. All messages on the mainframe indicate connectivity.

Causes

If the collector has not been actively used as a collector since being built and configured, the sniffer appears to time out port 16022.

Environment

z/OS is affected.

Resolving the problem

Restart the inspection-core by using the CLI command restart inspection-core.

Parent topic: S-TAPs and other agents

GIM

- Error installing the Guardium Installation Manager (GIM)
  If GIM does not install properly, create the directory manually.
- Guardium Installation Manager (GIM) service does not start in Windows
  If the Guardium Installation Manager (GIM) service does not start in Windows, reinstall GIM in a folder that is reserved for 32-bit applications.

Parent topic: Problems and solutions

Error installing the Guardium Installation Manager (GIM)

If GIM does not install properly, create the directory manually.

Symptoms

When you attempt to install the Guardium Installation Manager (GIM) on RHEL6, you see the following error message.

```
cp: cannot stat `/usr/local/GIM/modules/central_logger.log': No such file or directory Installation failed
```

Causes

Various Linux distributions such as RedHat 6 deprecated the use of the traditional init daemon that uses the etc/inittab file. They replaced it with an init process called Upstart. Upstart uses the /etc/event.d and /etc/init directories for the automated start, stop, and respawn of processes.

Environment

The Guardium Installation Manager (GIM) is affected.

Resolving the problem

To fix the issue, complete the following steps.

- Remove the partial GIM installation.
- Create the /etc/event.d directory manually with the command mkdir /etc/event.d
- Run the GIM installer.

Parent topic: GIM

Guardium Installation Manager (GIM) service does not start in Windows

If the Guardium Installation Manager (GIM) service does not start in Windows, reinstall GIM in a folder that is reserved for 32-bit applications.

Symptoms

After you successfully installed the Guardium Installation Manager (GIM) on Windows, you notice that the service is not running.

Causes

GIM is a 32-bit application. If you are using a Windows 64 bit, GIM might be installed in Program Files instead of Program Files(x86).

Environment

GIM is affected.

Resolving the problem

Install GIM in Program Files(x86) because it is a Windows folder that is reserved for 32-bit applications.

Parent topic: GIM

File activity

Parent topic: Problems and solutions

File activity is not logged in investigation dashboard or reports

Symptoms

There is no file activity logged in the investigation dashboard or predefined reports, such as: File Activities, File Entitlement, Files Count of Activity Per Client, Files Count of Activity Per Server, Files Count of Activity Per User, Files Privileges

Resolving the problem

Check the following:

- Verify the FAM license is installed and the S-TAP is active
- Make sure you are not logged in as root in your file server for activities. Activities from root, (UID0) are not logged by default.
- On Linux/AIX, check the file path specified in your policy rule. For example, /testdir/ monitors a file called testdir and not the files in a directory called testdir. Specify /testdir/* to monitor files in the testdir directory.
- On Windows, if you use domains and your policy rule specifies a user, make sure the domain is specified. For example, svldev\Maryjane instead of just Maryjane.

Parent topic: File activity troubleshooting

File activity from removable disk is not logged in investigation dashboard

Symptoms

File activity from removable disk is not logged in investigation dashboard

Environment

FAM_SCAN_EXCLUDE_REMOTE_DIRECTORIES is set to true

Resolving the problem

Install the file activity monitoring policy *before* mounting the removable disk.
Parent topic: File activity troubleshooting

File activity appears in reports but not the investigation dashboard

Symptoms

You see file activity in the predefined reports, but not in the investigation dashboard.

Resolving the problem

Verify the configuration using the guard API:

- To send crawled data to quick search: grdapi enable_fam_crawler activity_schedule_interval=2 activity_schedule_units=MINUTE entitlement_schedule_interval=10 entitlement_schedule_units=MINUTE
- To enable quick search (with option to also include violations): grdapi enable_quick_search includeViolations=true schedule_interval=2 schedule_units=MINUTE

Parent topic: File activity troubleshooting

Some files missing from classification results

Symptoms

Some files are missing in the classification results.

Causes

The following are file types are *not* supported for classification: DAT, JPG, JPEG, GIF, TIF, TIFF, BMP, WAV, MOV, MP3, MP4, AVI, MPG, WMA, WMV, P7S, XFDL, XFD, FRM, JAR

Parent topic: File activity troubleshooting

Partial file discovery (entitlement) results in reports and investigation dashboard

Reports and investigation dashboard are not showing complete discovery (entitlement) results.

Symptoms

The discovery (entitlement) results that appear in reports and investigation dashboard is incomplete. Results for some files do not appear.

Resolving the problem

Verify that the document types and locations are included in your GIM configurations for discovery. Check the following GIM configuration parameters:

- FAM_SCAN_EXCLUDE_FILES
- FAM_SCAN_EXCLUDE_DIRECTORIES
- FAM_SCAN_EXCLUDE_EXTENSIONS
- FAM_SCAN_EXCLUDE_FILES
- FAM_SCAN_MAX_DEPTH

Parent topic: File activity troubleshooting

File classification results are missing from reports and investigation dashboard

Symptoms

File classification results are missing from reports and investigation dashboard.

Causes

Classification is an additional process that goes beyond metadata discovery.

Resolving the problem

Assuming your software requirements are met for the IBM Content Classification engine (http://www-01.ibm.com/support/docview.wss?uid=swg27020838) that is used for classification, verify the following GIM configurations:

- Ensure that the GIM parameter FAM_IS_DEEP_ANALYSIS= TRUE
- Verify that Decision Plan names are correct in FAM_ICM_CLASS_DECISION_PLANS setting and that the list of Decision Plans is delimited with a semicolon
- Verify that all listed Decision Plans (.dpn) files exist in the following location on the file server: %FAM_HOME%\conf\ContentClassification

User response: Optional. When you have particular actions that are performed by particular users, use one or more of the ts*Response elements.

Parent topic: File activity troubleshooting

FAM bundle fails to install

After installing the GIM client, the FAM bundle installation fails.

Symptoms

When attempting to install the FAM bundle, the system responds with a message similar to:

```
-1,GIM - Failure point : dependancy_violation (Dependancy violation (FAM) : Missing mandatory dependency - STAP at GIM.pm line
3176, <MYFILE> line 20.
```

Causes

The S-TAP bundle must be installed before installing the FAM bundle.

Resolving the problem

Verify the S-TAP for FAM is installed, then install the FAM bundle. See Installing and activating file activity monitoring components.

Parent topic: File activity troubleshooting

Installing Your Guardium System

- Checksum error during S-TAP installation
  If you receive a checksum error, set the transfer mode to binary on the FTP client.
- Guardium S-TAP returns an illegal cp: option - f error message
  If the S-TAP installation fails with cp: illegal option - f, run the command which cp and change the file path.
- Installing a new Guardium patch does not complete
  If you cannot complete the installation of a new Guardium patch, stop the interfering process and reinstall the patch.
- Missing file or directory after new Guardium S-TAP installation
- Partition error installing Guardium
  If you receive a partition error, select Custom installation and specify the disk location and size explicitly.
- Patch installation fails: No such file or directory
  If the patch installation fails, check that the file matches the MD5SUM of the downloaded patch.

Parent topic: Problems and solutions

Checksum error during S-TAP installation

If you receive a checksum error, set the transfer mode to binary on the FTP client.

Symptoms

You receive an error similar to the following when you run the S-TAP installer to install Guardium S-TAP on UNIX or Linux.

```
./guard-stap-v81_r26808_1-aix-6.1-aix-powerpc.sh
Verifying archive integrity...Error in checksums: 2082112805 is
different from 3728267449
```

Causes

The installer file is corrupted. The file became corrupted when the file was transferred to the database server or when the product was downloaded.

Environment

S-TAP on UNIX or Linux is affected.

Resolving the problem

To resolve the problem, make sure that the transfer mode is set to binary on the FTP client. Then, try the transfer to the database server again. If the process fails, download the product again.

Parent topic: Installing Your Guardium System

Guardium S-TAP returns an illegal cp: option - f error message

If the S-TAP installation fails with cp: illegal option - f, run the command which cp and change the file path.

Symptoms

The S-TAP installation fails with the following error message.

```
A directory called 'guardium' containing Guardium software needs to be created under a path provided.
Enter the path prefix [/usr/local]? /opt/guardium
Directory /opt/guardium/guardium/guard_stap does not exist, would you like to create it [Y/n]? Y
Run STAP as root, or as user 'guardium' [R/u]? R
Please be patient... This might take more than a minute.
```

```
Copying installation files...
cp: illegal option -- f
UX:vxfs cp: INFO: V-3-21462: Usage: cp [-i] [-p] f1 f2
cp [-i] [-p] f1 ... fn d1
cp [-i] [-p] [-r|-R] [-e { force | ignore | warn}] d1 d2
```

Causes

The path to/usr/bin/cp is different from what the installer expects.

Environment

The UNIX/Linux database server is affected.

Resolving the problem

Run the command which cp

If which cp returns a value other than /usr/bin/cp, run the command export PATH=/usr/sbin:/usr/bin:$PATH.

Rerun the command which cp to confirm that the path is /usr/bin/cp.

Parent topic: Installing Your Guardium System

Installing a new Guardium patch does not complete

If you cannot complete the installation of a new Guardium patch, stop the interfering process and reinstall the patch.

Symptoms

When you install a new patch it does not complete. The status column in the CLI command show system patch installed shows one of the following messages.

```
STEP: Setting “java” off
STEP: Setting “amei” off
STEP: Setting “sqlw” off
```

Causes

Tomcat, the inspection core, or another process on the machine interfered with the patch installation.

Environment

The Collector, Aggregator, and Central Manager are affected.

Resolving the problem

To install the new Guardium patch, stop any processes from interfering with the installation.

1. Delete the patch that is stuck by using the command delete scheduled-patch.
2. Restart the system by using the command restart system.
3. After the system restarts, stop the GUI and inspection core by using the commands stop gui and stop inspection-core.
4. Reinstall the patch and restart the GUI and inspection core by using the commands restart gui and start inspection-core.

Parent topic: Installing Your Guardium System

Missing file or directory after new Guardium S-TAP installation

Symptoms

When you attempt to install S-TAP, you receive the following error message.

```
Tap_controller::init failed Opening pseudo device /dev/guard_ktap No such file or directory
```

In addition, /dev/*ktap* does not exist.

Causes

There are many possible reasons why the K-TAP device creation can fail. The following are the most common causes.

- You did not use the module files, including the K-TAP module for the Linux kernel.
- You did not specify the Flex Loading option to load the K-TAP module from the module files.
- A previous K-TAP module from an old installation is still running or installed.

Environment

All Linux and UNIX operating systems in which the IBM Guardium S-TAP product can be installed are affected.

Resolving the problem

To resolve the problem, take the following steps.

1. Run these commands as root.

```
<STAP directory>/KTAP/guard_ktap_loader stop
<STAP directory>/KTAP/guard_ktap_loader uninstall
<STAP directory>/KTAP/guard_ktap_loader install
<STAP directory>/KTAP/guard_ktap_loader start
```

2. Check whether the K-TAP device is now created with the command ls /dev/*ktap*. If it was created, issue is resolved. If not, continue to next step.
3. Stop the S-TAP process guard_stap if it is running. You can check whether it is running with command ps -ef | grep guard_stap.
4. Verify that the S-TAP process is not running with the command ps -ef | grep guard_stap.
5. Uninstall the S-TAP.
6. Confirm that the S-TAP directory is gone.
7. Check whether a K-TAP module is still running from an old installation. Use the appropriate command for your operating system.

```
Linux    : lsmod | grep ktap
Solaris  : modinfo | grep  tap
HP-UX    : lsdev | grep tap
AIX      : genkex | grep tap
```

   If a device such as ktap_<release> is listed, then a K-TAP module is running.
8. If you find a K-TAP module is running in previous step, run the following steps to stop and uninstall the K-TAP module.

```
<STAP directory>/KTAP/guard_ktap_loader stop
<STAP directory>/KTAP/guard_ktap_loader uninstall
```

   Restart the server.
9. If you are using the Guardium Installation Manager (GIM), go to Manage > Module Installation > Set up by Client (Legacy), select the client and click Reset Clients. Wait for the server to reappear in the client list.
10. Reinstall the S-TAP. If you are using GIM to install the S-TAP, reinstall the S-TAP bundle with GIM and the following commands.

```
KTAP-ALLOW_COMBOS=Y
KTAP_LIVE_UPDATE=Y
KTAP_ENABLED=Y
```

Parent topic: Installing Your Guardium System

Partition error installing Guardium

If you receive a partition error, select Custom installation and specify the disk location and size explicitly.

Symptoms

When you install the Guardium appliance in VMWare, you receive the following error:

```
Error Partitioning
Could not allocate requested partitions:
Partitioning failed: Could not allocate partitions as primary partitions.
Not enough space left to create partition for /boot.
```

Causes

When you install the Guardium system with VMWare, if you select Typical, VMWare uses configuration parameters that are predefined for the OS type in VMWare. These configuration parameters might not be suitable for this installation.

Environment

All Guardium configurations (collector, aggregator, central manager) are affected.

Resolving the problem

Select Custom installation and specify the disk location and size explicitly. Specify a disk size that is large enough for your monitoring and audit needs. After it is configured, Guardium does not support adding disk space to the system.

Parent topic: Installing Your Guardium System

Patch installation fails: No such file or directory

If the patch installation fails, check that the file matches the MD5SUM of the downloaded patch.

Symptoms

Patch installation in Guardium fails with the error `patch.reg: No such file or directory`.

Causes

The following cases can cause the patch installation to fail.

- The patch was not downloaded in binary mode and corrupted the file.
- The compressed file itself was uploaded to the Guardium system.
- The patch was received from Guardium support and has the PMR number prefixed to the file name.
- The patch was uploaded to the Guardium system from a Windows FTP server.

Environment

The collector, aggregator, and central manager are affected.

Resolving the problem

Verify that the contents of the file match the MD5SUM of the downloaded patch. If the compressed file cannot be extracted or the MD5SUM does not match, download the file in binary mode.

If the compressed file itself was uploaded to the Guardium system, extract the compressed file and upload only the patch.

If there is a PMR number prefixed to the file name, remove the number and then upload the patch to the Guardium system.

If the patch is uploaded from a Windows FTP server, specify the exact file name with the correct case.

Parent topic: Installing Your Guardium System

Windows: S-TAP user's guide

Guardium S-TAP is a lightweight software agent installed on database servers and file servers. The information collected by the S-TAPs is the basis of all Guardium traffic reports, alerts, visualizations, etc.

For data activity monitoring, the S-TAP monitors activity between the client and the database and forwards that information to the Guardium collector. The database traffic is logged into the collector based on criteria specified in the security policy. It is also possible to reduce the amount of traffic that is originally sent to the collector by ignoring trusted connections or ignoring traffic from specific IPs.

For file activity monitoring, unlike data activity, the policy rules are pushed down to the file server and thus only data that is specified in the security policy is forwarded to the collector.

- Windows: Install, Upgrade, Uninstall S-TAP
- Windows: Configuring S-TAP
  Learn to configure the S-TAP.
- Windows: S-TAP operation and performance

Windows: Install, Upgrade, Uninstall S-TAP

- Windows: S-TAP support matrix
  Select your S-TAP setup depending on the data you want to monitor or block. Use this table to identify the monitoring mechanisms that can perform the operations you require, per operating system and database.
- Windows: Prerequisites: installing S-TAP
- Windows: Installing an S-TAP agent
  Install an S-TAP on Windows using the Monitoring Agents tool (from v10.1.3), Guardium Installation Manager (GIM), the interactive installer, or the command line installer.
- Windows: S-TAP installation flow on Oracle RAC
  Configure S-TAPs in an Oracle RAC.
- Windows: Upgrading and Removing an S-TAP
  Learn how to upgrade or remove S-TAPs on Windows.
- Windows: When to restart or reboot the database after S-TAP installation or upgrade
  This topic details the situations, after S-TAP installation, of when to restart and when to reboot the database server or database instance. Restart/reboot requirements are the same for GIM and non-GIM implementations.

Parent topic: Windows: S-TAP user's guide

Windows: S-TAP support matrix

Select your S-TAP setup depending on the data you want to monitor or block. Use this table to identify the monitoring mechanisms that can perform the operations you require, per operating system and database.

For example, you may want to track or perform one or more of the following:

- local traffic only
- local and network traffic
- shared memory
- encrypted data
- monitor and block
- monitor only

This table covers the most common platforms, database types, and protocols, supported by Guardium's monitoring mechanisms. The table presents general guidelines. There may be other combinations that are not presented here that are supported. Some of the supported setups presented here may be dependent on specific configurations. Contact Technical Support to verify the best setup for your specific needs. Empty cells indicate that the combination is not supported.

OS	Database	Network traffic	Local traffic	Encrypted traffic	Protocol	Kerberos	Blocking	Redaction
Windows	MS SQL Server	Supported	Supported	Supported for TCP and NMP	TCP, NMP	Supported	Supported	Supported
Windows	DB2	Supported, also with DB2 Exit	Supported, also with DB2 Exit	DB2 Exit	TCP, SHM		Supported (Except DB2 Exit)	Supported (Except DB2 Exit)
Windows	Oracle	Supported	Supported	Supported (ASO, SSL)	TCP, NMP, BEQ		Supported	Supported

OS	Database	Network traffic	Local traffic	Encrypted traffic	Protocol	Kerberos	Blocking	Redaction
Windows	Informix	Supported	Supported		TCP		Supported	Supported
Windows	Sybase	Supported	Supported		TCP		Supported	Supported
Windows	MySQL	Supported	Supported		TCP		Supported	Supported
Windows	PostgreSQL	Supported	Supported		TCP		Supported	Supported
Windows	MongoDB	Supported	Supported		TCP		Supported	Supported
Windows	CouchDB	Supported	Supported		TCP		Supported	Supported

Parent topic: Windows: Install, Upgrade, Uninstall S-TAP

Windows: Prerequisites: installing S-TAP

- Windows: S-TAP disk space requirements
  Verify the disk space requirements before installing your S-TAP.
- Windows: Guardium port requirements for S-TAP
  If there is a firewall between Guardium® components (for example, between a Guardium system and an S-TAP on a Windows database server), you must verify that the ports used for connections between those components are not being blocked.

Parent topic: Windows: Install, Upgrade, Uninstall S-TAP

Windows: S-TAP disk space requirements

Verify the disk space requirements before installing your S-TAP.

Table 1. Windows S-TAP Disk Space Requirements

Disk Space	Description
S-TAP® Program files	GIM Install: 300 MB non-GIM Install: 180 MB
Buffer file	If you configure the S-TAP to use a buffer file, the size defaults to 50 MB. The size is controlled by the buffer_file_size configuration file parameter.

Parent topic: Windows: Prerequisites: installing S-TAP

Windows: Guardium port requirements for S-TAP

If there is a firewall between Guardium® components (for example, between a Guardium system and an S-TAP on a Windows database server), you must verify that the ports used for connections between those components are not being blocked.

Use your firewall management utility to check, and open as relevant, the ports listed below.

Table 1. Port Requirements for Windows servers

Port	Protocol	Guardium system connection to ...
9500/9501	TCP	Alive messages
9500	TCP	Clear S-TAP®
9501	TLS	Encrypted S-TAP

Parent topic: Windows: Prerequisites: installing S-TAP

Windows: Installing an S-TAP agent

Install an S-TAP on Windows using the Monitoring Agents tool (from v10.1.3), Guardium Installation Manager (GIM), the interactive installer, or the command line installer.

Depending on your license key, you can use the same S-TAP agent for both file and database activity monitoring. There are no specific S-TAP parameters for FAM.

The Base Filtering Engine (BFE) service must be running for the S-TAP installation. If the service exists but is not running, Guardium attempts to start it.

S-TAPs require .NET Framework 4.5 or higher version. If the .NET 4.5 or higher environment does not exist, S-TAP will install .NET 4.5.2.

When installing the Windows S-TAP in a Non-ASCII environment (for example, Japanese), use either the server with that language pack or set the system locale to that location (Japan).

S-TAP installation creates one installation log: C:\IBM Windows S-TAP.ctl.

Auto-discovery of database instances

When installing an S-TAP, you have the option of auto-discovering database instances and creating inspection engines for the discovered instances. The auto-discovery process runs once at the time of S-TAP installation and does not automatically repeat.

Auto-discovery supports these database types: MS SQL Server, DB2, Oracle, Informix, MongoDB, CouchDB. To create inspection engines on other discovered databases, see the Discovered Instances report.

During an upgrade, auto-discovery discovers additional database instances but does not create inspection engines for the new instances. Auto-discovery adjusts any preexisting inspection engines. This means that if you have added an inspection engine for a database that does not exist or specified a port that does not work, the auto-

discovery process adjusts that inspection engine during the upgrade.

If you do not want the S-TAP installation to perform automatic discovery of databases during installation or upgrade, you can prevent it during the S-TAP installation process by following the procedure described for each Windows S-TAP installer.

Enterprise load balancing

During installation of an S-TAP on Windows, you can configure the S-TAP to use Enterprise Load Balancing features. For more information, see Enterprise Load Balancing.

- Windows: Installing S-TAP agent with GIM (v10.1.4)
  The Guardium Installation Manager (GIM) is the recommended method for installing S-TAPs on your database servers. GIM enables you to install, upgrade, and manage agents on individual servers or groups of servers. This includes monitoring processes that were installed under its control, modifying agent parameters, and performing other management tasks.
- Windows: Installing S-TAP agent with GIM (v10.1-10.1.3)
  The Guardium Installation Manager (GIM) is the recommended method for installing S-TAPs on your database servers. GIM enables you to install, upgrade, and manage agents on individual servers or groups of servers. This includes monitoring processes that were installed under its control, modifying agent parameters, and performing other management tasks.
- Windows: S-TAP GIM installation parameters
  Understand the parameters (each with a short description) that are typically used in your GIM installation.
- Windows: Installing S-TAP agent using the interactive installer
  The interactive installer is useful for smaller deployments or whenever a guided, step-by-step installation experience is required.
- Windows: Installing S-TAP agent using the command line interface
  The command-line installer provides a scriptable solution that is especially useful for managing large deployments.
- Windows: S-TAP command line installation parameters
  Understand the parameters (each with a short description) that you can use in your script and GIM installation.

Parent topic: Windows: Install, Upgrade, Uninstall S-TAP
Related concepts:
Quick start for deploying monitoring agents
Guardium Installation Manager

Windows: Installing S-TAP agent with GIM (v10.1.4)

The Guardium Installation Manager (GIM) is the recommended method for installing S-TAPs on your database servers. GIM enables you to install, upgrade, and manage agents on individual servers or groups of servers. This includes monitoring processes that were installed under its control, modifying agent parameters, and performing other management tasks.

Before you begin

Verify the following before you begin:

- Review the Windows S-TAP installation requirements at Windows: Prerequisites: installing S-TAP.
- Verify that your database server and operating system are supported.
- Verify that the intended S-TAP installation directory is empty or does not exist.
- The GIM client is installed on the database server where you will install an S-TAP.
- The GIM client on the database server is communicating with the Guardium system.
- Obtain the S-TAP module from either Fix Central, or your Guardium representative.

About this task

After installing a GIM client on the database server, installation of the S-TAP for Windows is scheduled from the Guardium system.

The only required parameter is WINSTAP_INSTALL_DIR.

The parameter WINSTAP_INSTALL_DIR cannot be modified after the installation. All other parameters can be modified after installation.

You can input any parameter in the Setup by Client page, in the Choose parameters ribbon, using the command WINSTAP_CMD_LINE with the syntax parameter=value for [TAP] parameters, or with the syntax -param value for CLI parameters (Windows: S-TAP command line installation parameters), and they are added or updated in the guard_tap.ini.

CAUTION:
There is no validation of input to this field.

Procedure

1. Upload the Windows S-TAP module for installation.
   a. On the Guardium system, navigate to Manage > Module Installation > Upload Modules.
   b. Click Choose File and select the S-TAP module you want to install.
   c. Click Upload to upload the module to the Guardium system. After uploading, the module will be listed in the Import Uploaded Modules table.
   d. In the Import Uploaded Modules table, click the check box next to the S-TAP module you want to install. The module will be imported and made available for installation. After the module is imported, the Upload Modules page will be reset and the Import Uploaded Modules table will be empty.
2. Follow the GIM instructions in Set up by Client and refer to Windows: S-TAP GIM installation parameters.
   - While the default parameters are acceptable for most installations, you are required to provide a WINSTAP_INSTALL_DIR value. The default value is C:/Program Files/IBM/Windows S-TAP. This is the only required parameter.
   - If WINSTAP_TAP_IP (equivalent to the -taphost command line parameter) is not specified, the GIM_CLIENT_IP value is used.
   - If WINSTAP_SQLGUARD_IP (equivalent to the -appliance command line parameter) is not specified, the GIM_URL value is used.
   - Optionally enable enterprise load balancing. See the parameter description in Windows: S-TAP GIM installation parameters.
   - To enable auto_discovery of database instances, set WINSTAP_NOAUTODISCOVERY to 0.

What to do next

Monitor installation of the S-TAP module using the Module Status table on the Common Modules screen. You can also view the status of the module installation by reviewing the report at Manage > Reports > Install Management > GIM Clients Status.

Verify that the S-TAP is communicating with the Guardium system by navigating to Manage > Activity Monitoring > S-TAP Control and reviewing the S-TAPs status and configuration.

Parent topic: Windows: Installing an S-TAP agent
Related concepts:
Guardium Installation Manager

Windows: Installing S-TAP agent with GIM (v10.1-10.1.3)

The Guardium Installation Manager (GIM) is the recommended method for installing S-TAPs on your database servers. GIM enables you to install, upgrade, and manage agents on individual servers or groups of servers. This includes monitoring processes that were installed under its control, modifying agent parameters, and performing other management tasks.

Before you begin

Verify the following before you begin:

- Review the Windows S-TAP installation requirements at Windows: Prerequisites: installing S-TAP.
- Verify that your database server and operating system are supported.
- Verify that the intended S-TAP installation directory is empty or does not exist.
- The GIM client is installed on the database server where you will install an S-TAP.
- The GIM client on the database server is communicating with the Guardium system.
- Obtain the S-TAP module from either Fix Central, or your Guardium representative.

About this task

After installing a GIM client on the database server, installation of the S-TAP for Windows is scheduled from the Guardium system.

The only required parameter is WINSTAP_INSTALL_DIR.

The parameter WINSTAP_INSTALL_DIR cannot be modified after the installation. All other parameters can be modified after installation.

You can input any parameter in the Setup by Client page, in the Choose parameters ribbon, using the command WINSTAP_CMD_LINE with the syntax parameter=value for [TAP] parameters, , or with the syntax -param value for CLI parameters (Windows: S-TAP command line installation parameters), and they are added or updated in the guard_tap.ini.

CAUTION:
There is no validation of input to this field.

Procedure

1. Upload the Windows S-TAP module for installation.
   a. On the Guardium system, navigate to Manage > Module Installation > Upload Modules.
   b. Click Choose File and select the S-TAP module you want to install.
   c. Click Upload to upload the module to the Guardium system. After uploading, the module will be listed in the Import Uploaded Modules table.
   d. In the Import Uploaded Modules table, click the check box next to the S-TAP module you want to install. The module will be imported and made available for installation. After the module is imported, the Upload Modules page will be reset and the Import Uploaded Modules table will be empty.
2. Select client systems where you want to install an S-TAP.
   a. Navigate to Manage > Module Installation > Setup by Client.
   b. On the Client Search Criteria screen, specify search criteria for the clients where you want to install the S-TAP, then click Search to continue. Search for clients using any combination of the following search criteria:
      - Select a client group.
      - Search by client hostname, IP address, or operating system.
      - Leave all search criteria fields empty to return a list of all available clients.
   c. On the Clients screen, click the check box next to the clients where you want to install the S-TAP, then click Next to continue.
3. Select and configure the S-TAP module before installing to client systems.
   a. From the Modules table on the Common Modules screen, select the S-TAP module for installation, then click Next to continue.
      - Use the Display Latest Versions and Display Bundles Only check boxes to filter the list of available modules.
      - Use the Module Status table to review information about the selected module on the target clients.
   b. From the Client Module Parameters screen, specify installation parameters for the S-TAP.
      - To apply the same parameters to multiple clients, specify installation parameters in the Common Module Parameters fields, click the check box next to clients listed in the Client Module Parameters tables, and then click Apply to Selected.
      - To apply unique parameters to individual clients, specify installation parameters directly in the Client Module Parameters table.

      Attention:
      - While the default parameters are acceptable for most installations, you are required to provide a WINSTAP_INSTALL_DIR value. The default value is C:/Program Files/IBM/Windows S-TAP.
      - If WINSTAP_TAP_IP (equivalent to the -taphost command line parameter) is not specified, the GIM_CLIENT_IP value is used.
      - If WINSTAP_SQLGUARD_IP (equivalent to the -appliance command line parameter) is not specified, the GIM_URL value is used.
   c. Once you have specified installation parameters for the S-TAP, apply those parameters to the selected clients by clicking Apply to Client.
4. Install the S-TAP to the selected clients.
   a. From the Client Module Parameters screen, click Install/Update.
   b. On the Schedule Date dialog, provide a date or time to begin the installation, then click Apply. To begin the installation immediately, use a value of `now` in the Schedule Date field.

What to do next

Monitor installation of the S-TAP module using the Module Status table on the Common Modules screen. You can also view the status of the module installation by reviewing the report at Manage > Reports > Install Management > GIM Clients Status.

Verify that the S-TAP is communicating with the Guardium system by navigating to Manage > Activity Monitoring > S-TAP Control and reviewing the S-TAPs status and configuration.

Parent topic: Windows: Installing an S-TAP agent
Related concepts:
Guardium Installation Manager

Windows: S-TAP GIM installation parameters

Understand the parameters (each with a short description) that are typically used in your GIM installation.

All parameters are listed in Windows: Editing the S-TAP configuration parameters.
CAUTION:
Do not modify advanced parameters unless you are an expert user or you have consulted with IBM Technical Support.

Table 1. Parameters applicable to all .NET installers

GIM parameter	Description
QUIET	Install silently. (Does not require value)
WINSTAP_INSTALL_DIR	This is the install directory. Default install path is C:/Program Files/IBM/Windows S-TAP
WINSTAP_ENABLEGAM	Enables the Guardium Agent Monitor service (GAM).

Table 2. Other S-TAP Parameters

GIM parameter	Description
WINSTAP_ENABLEGAM	Enables the Guardium Agent Monitor service (GAM).
WINSTAP_TAP_IP	The local/client IP. Required for unattended installation.
WINSTAP_SQLGUARD_IP	The SQLGUARD IP. You can set up multiple appliances by specifying this parameter multiple times, each with a unique value.

Table 3. S-TAP Parameters with Applicable Value ON. These parameters are on by default with their value set to ON. Unless described otherwise, setting these parameters to any value other than ON turns the parameter off.

GIM parameter	Description
TCP_DRIVER_INSTALLED	TCP_DRIVER_INSTALLED=1. Use TCP driver.
NAMED_PIPE_DRIVER_INSTALLED	NAMED_PIPE_DRIVER_INSTALLED=1. Specifies the named pipe used by MS SQL Server for local access. If a named pipe is used, but nothing is specified in this parameter, S-TAP attempts to retrieve the named pipe name from the registry.
DB2_TAP_INSTALLED	Enables sniffing DB2 shared memory traffic.
DB2_EXIT_DRIVER_INSTALLED	Enables DB2 Integration with S-TAP.
FAM_DRIVER_INSTALLED	Enables FAM S-TAP.
ORA_DRIVER_INSTALLED	Enables sniffing Oracle ASO and SSL traffic.
KRB_MSSQL_DRIVER_INSTALLED	Deprecated from v10.1.4. It appears in the guard_tap.ini file but it does not affect the configuration. This parameter is used to decrypt MSSQL SSL and Kerberos encrypted traffic. Set to 1 or 2 to collect MSSQL encrypted traffic and Kerberos tickets. If set to 1, when STAP starts, it will pre-collect usernames correlated with SIDs, collecting them for number of seconds defined in krb_mssql_driver_user_collect_time. When set to 2, the pre-collection isn't done and the usernames are correlated at run time.

Table 4. Enterprise Load Balancing parameters

GIM parameter	Description
WINSTAP_LOAD_BALANCER_IP	Required if you are configuring load balancing. This option specifies the IP address of the central manager or managed unit this S-TAP should use for load balancing. • S-TAP parameters cannot be changed via the interactive installer during upgrade. Use the Guardium UI after the upgrade to change S-TAP parameters. • If configuring the enterprise load balancer to run on a managed unit, the S-TAP must be at V10.1 or higher.
WINSTAP_INITIAL_BALANCER_TAP_GROUP	Optional. The application group name that this S-TAP belongs to for enterprise load balancing. Attention: Group names with spaces or special characters are not supported.
WINSTAP_INITIAL_BALANCER_MU_GROUP	Optional. The MU group name the app-group will be associated with. Requires a defined LB-APP-GROUP. An MU group must already exist on the Central Manager before it can be used during installation of S-TAP Attention: Group names with spaces or special characters are not supported.
WINSTAP_LOAD_BALANCER_NUM_MUS	The number of managed units the enterprise load balancer allocates for this S-TAP.

Parent topic: Windows: Installing an S-TAP agent

Windows: Installing S-TAP agent using the interactive installer

The interactive installer is useful for smaller deployments or whenever a guided, step-by-step installation experience is required.

Before you begin

Verify the following before you begin:

- Review the Windows S-TAP installation requirements at Windows: Prerequisites: installing S-TAP.
- Verify that your database server and operating system are supported.
- Identify the IP address of the database server or domain controller where you will install the S-TAP, including any virtual IP addresses.
- Identify the IP address of the Guardium system that will control the S-TAP.
- Verify that the intended S-TAP installation directory is empty or does not exist.
- Obtain the S-TAP module from either Fix Central, or your Guardium representative.

About this task

When installing an S-TAP on a database server, you must provide the IP address or host name of the Guardium system that will receive data from the S-TAP. After the S-TAP has connected to the Guardium system, navigate to the Manage > Activity Monitoring > S-TAP Control page and complete the S-TAP configuration.

Note: Windows S-TAP parameters cannot be changed via the interactive installer during upgrading. The user can use the GUI after the upgrade to change Windows S-TAP parameters.

Procedure

1. Log on to the database server using a system administrator account.
2. Copy the S-TAP module to your database and start the Guardium Windows S-TAP Install Wizard.
   Attention: When installing an S-TAP on Windows 2012 or later, you must use administrative privileges. To do this, right-click the installer and choose Run as Administrator.
3. Read the license agreement on the Guardium License screen. To continue installation, select I accept the terms of the license agreement and click Next.
4. Provide the requested content on the Customer Information screen, then click Next to continue. The default values are appropriate for most installations.
5. Select one of the following installation types, and then click Next to continue:
   - Typical: a typical installation will be appropriate for most users.
   - Compact: a compact installation assumes that additional features such as Enterprise Load Balancing are not required.
   - Custom: a custom installation allows you to modify additional S-TAP installation options such as the software choices, installation directory and the user account that runs the Windows S-TAP process.
6. Optionally, enable Enterprise Load Balancing by selecting the Enable Load Balancing checkbox on the Load Balancing Options screen. Click Next to continue.
   a. If you enable Enterprise Load Balancing, provide the load balancer IP address in the Load Balancer Host Address field.
   b. Click the Advanced Options button to specify any additional Enterprise Load Balancing options. For more information, see Enterprise Load Balancing.
7. Verify the Software Tap Host Address and provide Appliance Address(es) on the Network Addresses screen, then click Next to continue.
   - The Software Tap Host Address specifies the address of the local machine where the S-TAP is being installed.
   - The Appliance Address(es) specify the Guardium system addresses that will control the S-TAP. Provide multiple addresses (typically not more than three) on separate lines to establish failover systems for the S-TAP or when configuring S-TAP load balancing with the participate_in_load_balancing parameter.

   Attention: If you do not want the S-TAP service to be enabled after installation, deselect the Start S-Tap Service checkbox. Deselecting the Start S-Tap Service checkbox also disables the automatic discovery of databases and creation of inspection engines.
   The Install Wizard Completed screen appears following a successful installation.
8. Click Finish to close the installer.

What to do next

Verify that the S-TAP is communicating with the Guardium system by navigating to Manage > Activity Monitoring > S-TAP Control and reviewing the S-TAPs status and configuration.

Parent topic: Windows: Installing an S-TAP agent

Windows: Installing S-TAP agent using the command line interface

The command-line installer provides a scriptable solution that is especially useful for managing large deployments.

Before you begin

Verify the following before you begin:

- Review the Windows S-TAP installation requirements at Windows: Prerequisites: installing S-TAP.
- Verify that your database server and operating system are supported.
- Identify the IP address of the database server or domain controller where you will install the S-TAP, including any virtual IP addresses.
- Identify the IP address of the Guardium system that will control the S-TAP.
- Verify that the intended S-TAP installation directory is empty or does not exist.
- Obtain the S-TAP module from either Fix Central, or your Guardium representative.

Procedure

1. Log on to the database server using a system administrator account.
2. Copy the installer to your database, and using the Windows Command Prompt, navigate to the Windows S-TAP installer directory. For example,

   ```
   cd c:\Windows-STAP-V10.5.0.89
   ```

   You should find a setup.exe executable in the installer directory.
3. Install the S-TAP using the setup.exe executable with the appropriate parameters. The required parameters are:
   - INSTALLPATH, the default is used if you do not specify
   - TAPHOST
   - APPLIANCE

   All parameters, except INSTALLPATH, can be updated after the installation. A typical install command is:

   ```
   setup.exe -UNATTENDED -APPLIANCE 10.0.147.234 -TAPHOST 10.0.145.41
   ```

   where:

- -UNATTENDED (required) invokes the command-line installer.
- -APPLIANCE specifies the IP address of the Guardium system that will control the S-TAP.
- -TAPHOST (required) specifies the client IP address where the S-TAP is being installed.

For a complete description of the setup.exe executable and its parameters, see Windows: S-TAP command line installation parameters

What to do next

Verify that the S-TAP is communicating with the Guardium system by navigating to Manage > Activity Monitoring > S-TAP Control and reviewing the S-TAPs status and configuration.

Parent topic: Windows: Installing an S-TAP agent
Related reference:
Windows: S-TAP command line installation parameters

Windows: S-TAP command line installation parameters

Understand the parameters (each with a short description) that you can use in your script and GIM installation.

In a CLI installation, you install an S-TAP using the setup.exe executable with the appropriate parameters, in this format:

Setup.exe -PARAMETER value

Do not use "=" signs to assign values to the parameters. The only time "=" is used is when you want to add a parameter to the TAP section of the guard_tap.ini file directly as it is typed in the command line.

If you want to add additional parameters not specified here but required in the guard_tap.ini file, you can append the [TAP] section by specifying the parameter and value with an = sign, for example:

setup.exe -UNATTENDED -INSTALLPATH "C:/Program Files/IBM/Windows S-TAP" -APPLIANCE 10.0.148.160 -TAPHOST 10.0.146.160 QRW_INSTALLED=0 QRW_DEFAULT_STATE=0

Important: The TAPHOST, APPLIANCE, INSTALLPATH attributes are required.

Table 1. Parameters applicable to all installers

Command line parameter	GIM parameter	Description
UNATTENDED	QUIET	Install silently. (Does not require value)
INSTALLPATH	WINSTAP_INSTALL_DIR	This is the install directory. Default install path is C:/Program Files/IBM/Windows S-TAP
ENABLEGAM	WINSTAP_ENABLEGAM	Enables the Guardium Agent Monitor service (GAM).
UNINSTALL		Uninstall. A value is not required.
CUSTOMER		To change customer name
COMPANY		To change company name
SERVICEUSER		To specify a user to run the service under
SERVICEPASSWORD		The password for the user

Table 2. Other S-TAP Parameters

Command line parameter	Description
NOAUTODISCOVERY	To prevent Auto-Discovery from running upon install. A value is not required.
ENABLEGAM	Enables the Guardium Agent Monitor service (GAM).
START	Controls whether S-TAP is started or not after installation. Attention: This parameter defaults to on and can be disabled only by setting its value to 0. Any value other than 0 results in this parameter being on.
TAPHOST	The local/client IP. Required for unattended installation.
APPLIANCE	The SQLGUARD IP. You can set up multiple appliances by specifying this parameter multiple times, each with a unique value.

Table 3. S-TAP Parameters with Applicable Value ON. These parameters are on by default with their value set to ON. Unless described otherwise, setting these parameters to any value other than ON turns the parameter off.

Command line parameter	Description
TCP	Use TCP driver.
NMP	Specifies the named pipe used by MS SQL Server for local access. If a named pipe is used, but nothing is specified in this parameter, S-TAP attempts to retrieve the named pipe name from the registry.
DB2SHMEM	Enables sniffing DB2 shared memory traffic.
DB2EXIT	Enables DB2 integration with S-TAP.
FAM	Enables FAM S-TAP.
ORACLEPLUGIN	Enables sniffing Oracle ASO and SSL traffic.
MSPLUGIN	Deprecated from v10.1.4. It appears in the guard_tap.ini file but it does not affect the configuration. This parameter is used to decrypt MSSQL SSL and Kerberos encrypted traffic. Set to 1 or 2 to collect MSSQL encrypted traffic and Kerberos tickets. If set to 1, when STAP starts, it will pre-collect usernames correlated with SIDs, collecting them for number of seconds defined in krb_mssql_driver_user_collect_time. When set to 2, the pre-collection isn't done and the usernames are correlated at run time.

Table 4. Enterprise Load Balancing parameters

Command line parameter	GIM parameter	Description
LOAD-BALANCER-IP	WINSTAP_LOAD_BALANCER_IP	Required if you are configuring load balancing. This option specifies the IP address of the central manager or managed unit this S-TAP should use for load balancing. • S-TAP parameters cannot be changed via the interactive installer during upgrade. Use the Guardium UI after the upgrade to change S-TAP parameters. • If configuring the enterprise load balancer to run on a managed unit, the S-TAP must be at V10.1 or higher.
LB-APP-GROUP	WINSTAP_INITIAL_BALANCER_TAP_GROUP	Optional. The application group name that this S-TAP belongs to for enterprise load balancing. Attention: Group names with spaces or special characters are not supported.
LB-MU-GROUP	WINSTAP_INITIAL_BALANCER_MU_GROUP	Optional. The MU group name the app-group will be associated with. Requires a defined LB-APP-GROUP. An MU group must already exist on the Central Manager before it can be used during installation of S-TAP Attention: Group names with spaces or special characters are not supported.
LB-NUM-MUS	WINSTAP_LOAD_BALANCER_NUM_MUS	The number of managed units the enterprise load balancer allocates for this S-TAP.

Parent topic: Windows: Installing an S-TAP agent

Windows: S-TAP installation flow on Oracle RAC

Configure S-TAPs in an Oracle RAC.

Procedure

1. Install S-TAP on all nodes. In case GIM is used, install GIM client on all nodes, then install S-TAP on all nodes.
2. Configure the STAP parameter STAP_TAP_IP: public IP configured for the node. (Can be configured through GIM UI.)
   - The parameter STAP_ALTERNATE_IPS is not required.
   - If the Oracle database is encrypted (ASO/SSL) make sure the parameter ORA_DRIVER_INSTALLED=1
   - If the Oracle inspection engine is auto-discovered, it should already contain all required parameters including INSTANCE_NAME.

Parent topic: Windows: Install, Upgrade, Uninstall S-TAP

Windows: Upgrading and Removing an S-TAP

Learn how to upgrade or remove S-TAPs on Windows.

Parent topic: Windows: Install, Upgrade, Uninstall S-TAP

Upgrade a Windows S-TAP using the command line

About this task

If a prior version of the Windows S-TAP has been installed, an upgrade can be performed from the command line using the setup program.

Procedure

1. Log on to the database server system using a system administrator account.
2. Change to the directory containing the S-TAP® setup program.
3. Run the setup program with the following options: setup -UNATTENDED
   Attention: Some files from the previous release will not be fully removed until the next scheduled reboot.

Remove a Windows S-TAP using Add/Remove Programs

About this task

This procedure will remove the installed S-TAP while making sure the configuration file is saved for future use.

Procedure

1. Log on to the database server system using a system administrator account.
2. Copy the current S-TAP configuration file to a safe location (a non-Guardium directory). Look for this file in C:Program Files (x86)\IBM\Windows S-TAP\Bin\guard_tap.ini.
3. From the Add/Remove Programs control panel, remove GUARDIUM_STAP.
   Attention: Some files will not be fully removed until the next scheduled reboot.

Remove a Windows S-TAP using the command line

About this task

This procedure will remove the installed S-TAP while making sure the configuration file is saved for future use.

Procedure

1. Log on to the database server system using a system administrator account.

2. Copy the current S-TAP configuration file to a safe location (a non-Guardium directory). Look for this file in C:Program Files (x86)\IBM\Windows S-TAP\Bin\guard_tap.ini.
3. Change to the directory containing the S-TAP setup program.
4. Run the setup program with the following options: setup -UNINSTALL
   Attention: Some files will not be fully removed until the next scheduled reboot.

Windows: When to restart or reboot the database after S-TAP installation or upgrade

This topic details the situations, after S-TAP installation, of when to restart and when to reboot the database server or database instance. Restart/reboot requirements are the same for GIM and non-GIM implementations.

Windows S-TAP installation and upgrade does not require reboot of the database server unless stated otherwise in the release notes or as an exception in this document. If you are not certain about reboot requirement for particular version you are using, you should check with your Technical Support representative.

Reboot database servers only when you need to upgrade the driver

Parent topic: Windows: Install, Upgrade, Uninstall S-TAP

Windows: Configuring S-TAP

Learn to configure the S-TAP.

- Windows: Configure S-TAP from the GUI
  View all S-TAPs managed by this Guardium system, manage individual STAPs, and perform a few operations on all STAPs.
- Windows: Discover database instances
  The Guardium S-TAP Discovery application periodically discovers database instances and sends the details to the primary (current active) S-TAP system.
- Windows: Configuring an Inspection Engine
  Configure or modify an inspection engine in the S-TAP Control pane.
- Windows: Inspection engine verification
  S-TAP verification confirms that the STAPs and their inspection engines in your environment are running and actively monitoring database activity. Understand verification, and define a schedule to regularly verify S-TAPs.
- Windows: S-TAP Load Balancing models and configuration guidelines
  Understand the S-TAP load balancing models, and choose the one appropriate to your setup
- Windows: Set up S-TAP authentication with SSL certificates
  Set up authentication between an S-TAP server and Guardium system.
- Windows: Using DB2 exit library
  The DB2 exit mechanism enables Guardium to pick up all DB2 traffic, whether encrypted or not and whether local or remote. This solution simplifies the S-TAP configuration, and provides native DB2 support.
- Windows: Editing the S-TAP configuration parameters
  You can modify the S-TAP configuration after it is installed using GIM, the UI, or for advanced users, the configuration file on the database.

Parent topic: Windows: S-TAP user's guide

Windows: Configure S-TAP from the GUI

View all S-TAPs managed by this Guardium system, manage individual STAPs, and perform a few operations on all STAPs.

About this task

Prerequisite: You must be logged in to the Guardium system that is the active host for the S-TAP.

Some configuration changes require that the S-TAP agent be restarted manually, as indicated in the parameter descriptions.

Sometimes a user is unable to make a decision during the process of installing an S-TAP or may make the wrong decision and it goes undetected until after the installation process is complete. For instance a user may forget to type in or use the wrong IP address when defining a SQL Guard IP. These types of mistakes can be remedied by modifying the S-TAP configurations.

Parameters in the GUI may be safely changed. Parameters that are not in the GUI rarely need changing and should normally be left unmodified; they are for use by Guardium Technical Support or advanced users.

If you have installed your S-TAP by using the Guardium Installation Manager (GIM), you can update some parameters through the GIM GUI or API.

Procedure

1. Click Manage > Activity Monitoring > S-TAP Control to open S-TAP Control.
2. Perform operations on all S-TAPs in the page.
   - Refresh: refresh display of S-TAPs.
   - Add All to Schedule: add all displayed S-TAPs to the S-TAP verification schedule.
   - Remove All from Schedule: remove all displayed S-TAPs from the S-TAP verification schedule.
   - Comments: add comments. See Comments
3. Identify the S-TAP to be configured by its IP address or the symbolic host name of the database server on which it is installed. View and perform operations on individual S-TAPs.

Option	Description

Option	Description
Delete:	Click Delete to remove an S-TAP. Deleting S-TAPs is useful to clean up your display when you know that an S-TAP has become inactive, or when the Guardium unit is no longer listed as a host in the S-TAP's configuration file. In either of these cases, the S-TAP displays indefinitely with an offline status if you do not delete it. You cannot remove an active S-TAP from the list. Clicking delete does not stop an S-TAP from sending information, nor does it remove the Guardium host from the list of hosts stored in the S-TAP's configuration file.
Refresh:	Click Refresh to fetch a copy of the latest S-TAP configuration from the agent. (There is no auto-refresh of the S-TAP display.)
Send Command:	Opens the S-TAP Commands popup, where you can run various commands on the S-TAP host. • Restart: Restarts the S-TAP. Not usually needed, and if yes, it's easier to simply kill it from the database server. • S-TAP logging • Reinitialize buffer: reset the K-TAP statistics along with deleting the S-TAP buffer • Run Diagnostics: Run the S-TAP diagnostics script (and upload the results to the Guardium system) • Record Replay Log: Records all data to a file on DB server (RECORD) and sends data to collector (REPLAY) • Revoke Ignore: All sessions ignored by a revokable ignore policy will be un-ignored and start capturing the traffic again for those sessions • Run Database Instance Discovery: Runs the discovery process, once immediately. (If enabled to run automatically, it runs, by default, every 24 hours.)
Edit S-TAP configuration:	Opens the S-TAP configuration window. Parameters that do not appear in the GUI are advanced parameters. Do not modify them if you are not an advanced user, or have not been instructed to modify them by Guardium Technical Support. See GUI parameters: • Windows: General parameters • Windows: Configuration Auditing System (CAS) parameters • Windows: Guardium Hosts (SQLGuard) parameters • Windows: Inspection engine parameters
Show S-TAP Event Log:	Click to open the S-TAP event log, where you can see events such as connect, disconnect, GIM server configuration, and so on. This log is very useful for troubleshooting.
Add to Schedule checkbox	Adds the individual S-TAP to the scheduled verification.
Revoke All Ignored Sessions checkbox	A database could be running many sessions, some of which are currently ignored. Clear this option to stop ignoring traffic from that server.

Parent topic: Windows: Configuring S-TAP

Windows: Discover database instances

The Guardium S-TAP Discovery application periodically discovers database instances and sends the details to the primary (current active) S-TAP system.

The Guardium Discovery Agent is a software agent automatically installed with the S-TAP package on a database server. The instance discovery agent reports database instances, listener, and port information to the Guardium system. Discovery does not find and report on every detail of the DB instances on the server.

Auto-discovery is enabled by default. Configure it with the parameter winstap_discovery_interval.

Database types supported by S-TAP Discovery
MS SQL Server, DB2, Oracle, Informix, MongoDB, CouchDB.

Newly discovered database instances can be seen in the Discovered Instances report. From this report, datasources and inspection engines can quickly be added to Guardium using the Actions menu.

If databases on the database server are not operational (started) or are added later, the Discovery Agent can still discover these instances by running the Run Discovery Agent command from the STAP Control window (Manage > Activity Monitoring > S-TAP Control. Click  , and select Run Database Instance Discovery).

S-TAP Discovery can be run manually but this action is not suggested. The main reason to run it manually is for debugging purposes. If a new request comes in from the user interface while a scheduled discovery is running, the new request is ignored.

Note: In order to avoid an instance where S-TAP discovery does not open the Informix database, it is recommended to start Informix databases using the full path to the executable.

The S-TAP Discovery application parameters should be left at their default values, except for advanced users. Discovery application are described in Linux and UNIX systems: Discovery parameters.

Discovery also uses these parameters:

- Software_tap_host: IP address or hostname of the database server on which the S-TAP is installed
- sqlguard_ip: S-TAP discovery results are sent to this IP. (The Guardium system with primary=1 in the SQLguard parameters.)

Parent topic: Windows: Configuring S-TAP

Windows: Configuring an Inspection Engine

Configure or modify an inspection engine in the S-TAP Control pane.

Before you begin

You must be logged in to the Guardium system that manages the S-TAP.

About this task

Do not configure an S-TAP inspection engine to monitor network traffic that is also monitored directly by a Guardium system that is hosting the S-TAP, or by another S-TAP reporting to the same Guardium system. That would cause the Guardium system to receive duplicate information: it would not be able to reconstruct sessions, and would ignore that traffic.

Procedure

1. Navigate to Manage > Activity Monitoring > S-TAP Control.
2. In the row of the S-TAP, click  . The S-TAP Configuration window opens.
3. Scroll to the bottom of the inspection engines, and click  next to Add Inspection Engine....
4. Select the protocol and enter the port range. The window refreshes with the relevant parameters, some with their default values.
5. Configure all required parameters, and click Add. If you are missing parameters, the system informs you what is missing.

Parent topic: Windows: Configuring S-TAP
Related reference:
Windows: Inspection engine parameters

Windows: Inspection engine verification

S-TAP verification confirms that the STAPs and their inspection engines in your environment are running and actively monitoring database activity. Understand verification, and define a schedule to regularly verify S-TAPs.

Verification checks sniffer operation and communication between the Guardium system and the inspection engines. You can enable verification for all S-TAP clients on your system, or individual S-TAP clients, or individual inspection engines.

Verification is supported for these database types:

- DB2
- DB2 Exit (DB2 version 10)
- FTP
- Kerberos
- Mysql
- Oracle
- PostgreSQL
- Sybase
- Windows File Share
- exclude IE
- MSSQL
- named pipes

There are two types of verification:

Standard verification
: Checks the sniffer operation, and the communication between the S-TAP and the inspection engine. It submits invalid login request and verifies that the appropriate error message is returned.

Advanced verification
: Use advanced verification to avoid failed login requests, and manage individual IEs. For avoiding failed login requests, you must identify or create a datasource definition associated with the target database. The datasource definition includes credentials, which the verification process uses to log in to the database. Then it submits a request to retrieve data from a nonexistent table in order to generate an error message.

For both types of verification requests, the results are displayed in a new dialog that provides information about the tests that were performed and recommended actions for tests that failed.

- Windows: S-TAP verification
  The S-TAP verification process checks several configuration parameters and attempts to connect to the inspection engines.
- Windows: Configure standard verification
  Use this task to configure all inspection engines on a specific S-TAP client host.
- Windows: Configure advanced verification
  Use this task to configure all inspection engines on a specific S-TAP client host.
- Windows: Configuring the S-TAP verification schedule
  You can configure the schedule for running S-TAP verification.

Parent topic: Windows: Configuring S-TAP

Windows: S-TAP verification

The S-TAP verification process checks several configuration parameters and attempts to connect to the inspection engines.

Before connecting to the database, the verification process checks whether the sniffer process is running on the Guardium system. The sniffer is responsible for communicating with each S-TAP and processing the data that is received. If the sniffer is not running, responses from the S-TAP are not recognized.

The verification process attempts to log in to your database's STAP client with an erroneous user ID and password, to verify that this attempt is recognized and communicated to the Guardium system.

Next the verification process checks whether it can connect to the selected inspection engine on the database server. It expects to receive a response that indicates a failed login. If a different response is received, you might have to investigate further.

Some error messages from individual databases do not indicate a specific problem. For example, on several supported databases, the error code returned for a wrong port can also mean that the database itself is not started.

View the verification results in the S-TAP Verification page (Manage > Reports > Activity Monitoring > S-TAP Verification page). Failed checks are shown first, with recommendations for next steps. Checks that succeeded are shown in a collapsed section at the end of the list. In some situations, it might be useful to review the successful checks in order to choose among possible next steps.

Parent topic: Windows: Inspection engine verification

Windows: Configure standard verification

Use this task to configure all inspection engines on a specific S-TAP client host.

About this task

As an alternative to this procedure, you can use the GRDAPI command verify_stap_inspection_engine_with_sequence.

Procedure

1. Access Manage > Activity Monitoring > S-TAP Control.
2. Use these options:
   - Add All to Schedule: add all inspection engines for all displayed S-TAPs to verification.
   - Remove All from Schedule: remove all inspection engines for all displayed S-TAPs from verification.
   - Add to Schedule: add all inspection engines of the selected S-TAP client to the schedule.

   If an S-TAP does not have the option All Can Control enabled, you can only change its status if your Guardium system is the primary system for this S-TAP.
3. Click Refresh.
4. To verify now, go to Manage > Activity Monitoring > S-TAP Verification Scheduler and click Run Once Now.

Parent topic: Windows: Inspection engine verification

Windows: Configure advanced verification

Use this task to configure all inspection engines on a specific S-TAP client host.

Before you begin

Use this task to configure verification on individual inspection engines, including advanced verification.

About this task

Procedure

1. Access Manage > System View > S-TAP Status Monitor.
2. Click anywhere in the row of the S-TAP.
   The window refreshes with the individual inspection engines of this host.
3. To verify now, select one or more inspection engines and click Verify.
4. Configure advanced verification.
   a. Click one inspection engine, and click Advanced Verify.
   b. Optionally, under Datasource, select Show only matching S-TAP host or select a name from the Name drop-down list to search for a specific inspection engine.
   c. Click Close.
5. To add to or remove from verification.
   a. Select one or more inspection engines.
   b. Click Add to Schedule or Remove from Schedule

Parent topic: Windows: Inspection engine verification

Windows: Configuring the S-TAP verification schedule

You can configure the schedule for running S-TAP verification.

About this task

The same schedule is used for all S-TAPs that are scheduled for verification.

Once a schedule is defined, you can click the Pause button to temporarily stop the verification process while keeping it active. Use the Run Once Now button to run the verification once in real-time.

Procedure

1. Click Manage > Activity Monitoring > S-TAP Verification Scheduler to open the S-TAP Verification Scheduler.
2. In the S-TAP Verification Scheduler portion of the page, click Modify Schedule.
3. In the Schedule Definition dialog, use the drop-down lists and check boxes to schedule when verification runs. This schedule is applied to all S-TAPs that are scheduled for verification.
4. Click Save to save your changes.

Parent topic: Windows: Inspection engine verification

Windows: S-TAP Load Balancing models and configuration guidelines

Understand the S-TAP load balancing models, and choose the one appropriate to your setup

Each load balancing model is described here, along with its specific parameter requirements.

Note: This topic described S-TAP load balancing, and not Enterprise Load Balancing.

Failover

S-TAP sends traffic to one collector (primary) and fails over to the secondary as needed. The S-TAP agents are configured with a primary and at least one secondary collector IP. If the S-TAP agent cannot send the traffic to the primary collector for various reasons, the S-TAP agent automatically fails over to the secondary. It continues to send data to the secondary host until either the secondary host system becomes unavailable, the primary host becomes available again, or until the S-TAP is restarted (at which point it attempts to connect to its primary host first). If the secondary host system becomes unavailable, it fails over to another secondary if there is one defined. In the second case S-TAP fails over from the secondary Guardium host back to the Primary Guardium host. It's recommend setting up a primary and up to two secondary collectors. You can either define one collector as a standby failover collector only, or a few failover collectors. When using one standby failover, one collector is usually sufficient for 4-5 collectors. When using a few failover collectors, each one should run at a maximum 50% capacity, so that there are always resources for additional load. Choose the setup that works best with your architecture, database, and data center layout. If the primary becomes available, the S-TAP fails back from the secondary Guardium host back to the Primary Guardium host.

The S-TAP restarts each time configuration changes are applied from the active host.

In the S-TAP Control window, Details section: set Load Balancing to 0; In the Guardium Hosts section: add at least one secondary Guardium Host.

Additional failover configuration should be left at the default values, except by advanced users.

Before designating a Guardium system as a secondary host for an S-TAP, verify these items.

- The Guardium system must have connectivity to the database server where S-TAP is installed. When multiple Guardium systems are used, they are often attached to disjointed branches of the network.
- The Guardium system must not have a security policy that will ignore session data from the database server where S-TAP is installed. In many cases, a Guardium® security policy is built to focus on a narrow subset of the observable database traffic, ignoring all other sessions. Either make sure that the secondary host will not ignore session data from S-TAP or modify the security policy on the Guardium system as necessary.

Load balancing

This configuration balances traffic from one database onto multiple collectors. This option might be good when you must monitor all traffic (comprehensive monitoring) of an active database. (Note that for outliers detection, the collectors need to be under the same aggregator and central manager in order for the aggregator to process all related data.) When the generated traffic is large and you need to house the data online on a collector for an extended period, this method might be your best choice because it performs session-based load balancing across multiple collectors. An S-TAP can be configured in this manner with up to 10 collectors.

In the S-TAP Control window, Details section: set Load Balancing to 1 for load balancing.

Grid

With Grid, the S-TAP communicates to the collector through a load balancer, such as f5 and Cisco. The S-TAP agent is configured to send traffic to the load balancer. The load balancer forwards the S-TAP traffic to one of the collectors in the pool of collectors. You also can configure failover between load balancers for continuous monitoring if the load balancer should fail.

S-TAPs in the F5 environment upload their log files and results of running diagnostics (all files from ..\Logs folder except for memory dumps) to the active collector and central manager (if exists) to the location ./var/IBM/Guardium/log/stap_diagnostic/

In the S-TAP Control window, Details section: set Load Balancing to 3 for the grid model.

In addition, set:

- All can control=1
- Guardium Host=<the IP of the Virtual IP of the balancer, to which all S-TAP database clients point to>
- The persistence of S-TAP is configured by the failover parameters:
  - TAP_MIN_TIME_BEFOREFAILOVER: The time interval, in minutes, after which the S-TAP switches to secondary Guardium system if: it cannot connect to its primary Guardium system; it can connect to its primary Guardium system but cannot write to its buffer. Default is 5.
  - TAP_MIN_HEARTBEAT_INTERVAL: Maximum time the S-TAP attempts to write to the primary Guardium system buffer before attempting to write to the secondary Guardium buffer. Default is 30 sec, meaning it tries to write at least 5*60/30 times before failover.

Redundancy

In redundancy, the S-TAP communicates its entire payload to multiple collectors. The S-TAP is configured with more than one collector (often only two) and communicates the identical content to both. This option provides full redundancy of the same logged data across multiple collectors. It can also be used for logging data and alert on activity at different levels of granularity.

In the S-TAP Control window, Details section: set Load Balancing to 2 for redundancy.

Parent topic: Windows: Configuring S-TAP

Windows: Set up S-TAP authentication with SSL certificates

Set up authentication between an S-TAP server and Guardium system.

S-TAPs can be configured to only connect to a certain group of machine(s) that authenticate with a given certificate or set of certificates. These certificates can either be generated locally on the Guardium system and sent off to the Certificate Authority (CA) for signing or can be created at the CA and installed whole on the Guardium system.

- Windows: Generating certificate signing request (CSR) on Guardium system
  Use this procedure to generate a certificate signing request locally on the Guardium system, for sending to the Certificate Authority (CA) for signing.

- Windows: Installing an SSL certificate generated outside of the Guardium system
  Use this procedure to install the SSL certificate that was created by the CA.
- Windows: Configuring the S-TAP to use x.509 certificate authentication

Parent topic: Windows: Configuring S-TAP

Windows: Generating certificate signing request (CSR) on Guardium system

Use this procedure to generate a certificate signing request locally on the Guardium system, for sending to the Certificate Authority (CA) for signing.

Procedure

1. Log into your Guardium system with CLI.
2. Enter: cli> create csr sniffer
3. Enter the requested data.

```
temp4> create system csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:CA
State or Province Name (full name) [Berkshire]:BC
Locality Name (eg, city) [Newbury]:
Organization Name (eg, company) [My Company Ltd]:QA_Sample1
Organizational Unit Name (eg, section) []:Sample_QA
Common Name (eg, your name or your server's hostname) []:sample1_qa.victoria
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
```

When you've finished, it looks like:

```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=CA, ST=BC, L=Newbury, O=QA_Sample1, OU=Sample_QA, CN=sample1_
qa.victoria
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:e9:5e:a2:81:53:dc:e9:b5:f7:54:33:17:6f:15:
                    9c:00:5c:ff:b2:64:c6:e5:48:be:36:a7:a4:55:f4:
                    b1:df:c9:81:a4:41:fe:29:80:d6:fd:d4:c4:b5:97:
                    b7:c1:3d:42:6c:c0:f8:09:cd:ea:36:f6:3b:b9:d9:
                    ce:15:87:2d:2f:b3:f2:5f:f9:42:06:e2:a0:62:56:
                    06:6d:cc:65:69:62:db:36:34:09:95:5b:c3:d0:e6:
                    85:ee:64:76:3e:ed:d6:47:bb:49:f2:08:81:14:c2:
                    e3:93:db:20:ba:86:e7:60:24:80:01:7f:3d:b7:60:
                    16:ba:06:d4:a1:e0:18:39:73:ca:1e:24:15:56:6d:
                    97:79:81:04:f7:fd:37:06:42:d7:15:82:34:aa:51:
                    2c:cc:e2:f0:d1:42:dd:b5:71:bb:10:19:a0:0a:5c:
                    4f:77:b9:bb:36:95:ed:a4:77:07:e3:50:f9:36:20:
                    13:e2:e1:78:d2:0a:36:8a:b9:39:90:1f:a4:82:12:
                    4f:50:29:3f:19:7d:16:a6:b3:23:7b:b8:7b:85:60:
                    04:21:39:84:1d:9e:81:e5:20:2c:8a:51:f3:52:f7:
                    3c:4f:e6:f2:a5:88:dc:2e:99:0a:b3:65:1e:bf:33:
                    5f:be:dc:53:1c:a6:69:18:c4:c7:75:bf:20:e3:cf:
                    29:af
                Exponent: 65537 (0x10001)
        Attributes:
            challengePassword        :guardium
    Signature Algorithm: sha1WithRSAEncryption
        06:4a:b9:db:04:a1:8d:4c:f7:3f:8f:24:fa:7c:ec:a6:70:77:
        8b:b9:38:7c:b6:e6:51:aa:ed:96:20:16:37:85:a7:44:26:2b:
        87:4c:a4:db:0c:f3:d3:87:e3:68:4a:8e:de:f6:0a:09:58:8f:
        68:98:4f:f3:8a:e2:37:5c:d6:42:32:8f:d9:01:56:41:88:df:
        1a:ba:63:03:62:08:89:06:13:88:74:6f:cd:eb:26:f0:67:a4:
        26:9b:a3:4c:ff:7b:c9:19:2c:12:58:06:ce:22:3c:e6:cd:52:
        b0:d0:da:6a:c9:02:df:02:e6:25:77:39:cf:50:80:e7:1d:01:
        fc:40:17:a2:98:04:bf:8b:24:f6:55:46:99:7b:17:05:01:d3:
        09:3d:a2:f0:e0:ba:5d:15:b8:28:74:d2:a3:fe:fd:86:7d:e0:
        60:e8:e4:38:6a:17:9c:80:80:e3:50:11:5e:35:f5:02:2b:65:
        60:41:2a:dc:ed:a8:a9:9a:6f:24:b4:7a:9c:39:01:a4:fc:cf:
        e6:94:86:f1:18:3a:f5:99:6b:f8:66:a2:ff:04:08:7e:ca:6b:
        2a:aa:cf:72:26:d0:c9:96:a0:98:fd:91:bb:b1:e4:8d:6d:10:
        08:ea:56:de:07:20:d3:e6:9a:bf:de:cf:c3:a4:e8:43:60:4f:
        b4:53:aa:d5
-----BEGIN CERTIFICATE REQUEST-----
MIIC0TCCAbkCAQAwczELMAkGA1UEBhMCQ0ExCzAJBgNVBAgTAkJDMRAwDgYDVQQH
EwdOZXdidXJ5MRMwEQYDVQQKDApRQV9TYW1wbGUxMRIwEAYDVQQLDAlTYW1wbGVf
UUExHDAaBgNVBAMME3NhbXBsZTFfcWEudmljdG9yaWEwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQDpXqKBU9zptfdUMxdvFZwAXP+yZMblSL42p6RV9LHf
yYGkQf4pgNb91MS117fBPUJswPgJzeo29ju52c4Vhy0vs/Jf+UIG4qBiVgZtzGVp
Yts2NAmVW8PQ5oXuZHY+7dZHu0nyCIEUwu0T2yC6hudgJIABfz23YBa6BtSh4Bg5
c8oeJBVWbZd5gQT3/TcGQtcVgjSqUSzM4vDRQt21cbsQGaAKXE93ubs2le2kdwfj
UPk2IBP14XjSCjaKuTmQH6SCEk9QKT8ZfRamsyN7uHuFYAQhOYQdnoHlICyKUfNS
9zxP5vKliNwumQqzZR6/M1++3FMcpmkYxMd1vyDjzymvAgMBAAGgGTAXBgkqhkiG
9w0BCQcxChMIZ3VhcmRpdW0wDQYJKoZIhvcNAQEFBQADggEBAAZKudsEoY1M9z+P
JPp87KZwd4u5OHy251Gq7ZYgFjeFp0QmK4dMpNsM890H42hKjt72CglYj2iYT/OK
4jdc1kIyj9kBVkGI3xq6YwNiCIkGE4h0b83rJvBnpCabo0z/e8kZLBJYBs4iPObN
UrDQ2mrJAt8C5iV3Oc9Qg0cdAfxAF6KYBL+LJPZVRpl7FwUB0wk9ovDgul0VuCh0
0qP+/YZ94GDo5DhqF5yAg0NQEV419QIrZWBBKtztqKmabyS0epw5AaT8z+aUhvEY
OvWZa/hmov8ECH7Kayqqz3Im0MmWoJj9kbux5I1tEAjqVt4HINPmmr/ez8Ok6ENg
T7RTqtU=
-----END CERTIFICATE REQUEST-----
ok
temp4>
```

4. Copy from the -----BEGIN CERTIFICATE REQUEST----- to the -----END CERTIFICATE REQUEST----- into a file and send this to your CA for signing.

   The CA will sign the certificate and send you back a public key that looks something like:

```
enance@enance1 Latest $ cat sample1_qa.victoria.pem
-----BEGIN CERTIFICATE-----
MIID1jCCAsCgAwIBAgIBCDALBgkqhkiG9w0BAQUwgYAxCzAJBgNVBAYTAkNBMRkw
FwYDVQQIExBCcml0aXNoIENvbHVtYmlhMREwDwYDVQQHEwhWaWN0b3JpYTEUMBIG
A1UEChMLUUFfdGVzdF92aWMxFDASBgNVBAsTC1ZpY3Rvcmlhx1FBMRcwFQYDVQQD
Ew5WaWN0b3JpYV9RQV9DQTAeFw0xMDExMDEyMTA5MzhaFw0xNTExMDEyMTA5Mzha
MHMxCzAJBgNVBAYTAkNBMQswCQYDVQQIEwJCQzEQMA4GA1UEBxMHTmV3YnVyeTET
MBEGA1UECgwKUUFfU2FtcGxlMTESMBAGA1UECwwJU2FtcGxlX1FBMRwwGgYDVQQD
DBNzYW1wbGUxX3FhLnZpY3RvcmlhMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA6V6igVPc6bX3VDMXbxWcAFz/smTG5Ui+NqekVfSx38mBpEH+KYDW/dTE
tZe3wT1CbMD4Cc3qNvY7udnOFYctL7PyX/lCBuKgYlYGbcxlaWLbNjQJlVvD0OaF
7mR2Pu3WR7tJ8giBFMLjk9sguobnYCSAAX89t2AWugbUoeAY0XPKHiQVVm2XeYEE
9/03BkLXFYI0qlEszOLw0ULdtXG7EBmgClxPd7m7NpXtpHcH41D5NiAT4uF40go2
irk5kB+kghJPUCk/GX0WprMje7h7hWAEITmEHZ6B5SAsilHzUvc8T+bypYjcLpkK
s2UevzNfvtxTHKZpGMTHdb8g488prwIDAQABo2swaTAfBgNVHSMEGDAWgBR0SB68
8syKm4CUQ27LGB9ftHRZyTAMBgNVHRMBAf8EAjAAMA8GA1UdDwEB/wQFAwMHuAAw
JwYDVR0lBCAwHgYIKwYBBQUHAwQGCCsGAQUFBwMCBggrBgEFBQcDATALBgkqhkiG
9w0BAQUDggEBAJe1Dlh623uD9mBjfB3YDKO3agm3vbdMd2vcdKI8TA5dsxMhmHvm
8E+gVsVOrNVbupLoc6OYeJLPvWQ54j9wZnKavBbma067C1QJJ2jEhOhjzoiEDIqT
l/qBhvqabhTG3vIMFSIwOu0zmQD/2iFu9cykKiru8A8djfZWjjfZiHO4dkkiCInP
/dor+Cm5RokGZ+OXhZ/5hxTuGeSAWJIhObVnrnPLZ2c2uYGh6LYip+2GU6L/rp8z
tmLYfldjtTMGYeP4Ivo1s7KHJqqDlATOBwe2XVR9808SrHI7toSpAbdIqP+f77zv
pb5xvOSfmqLuV6eUvJW8d/Wj2mvgw1qLvqY=
-----END CERTIFICATE-----
```

5. Have this file handy to either copy its contents or import it to the Guardium system. Enter: cli> store certificate sniffer [console | import]
6. If console, copy-paste from **-----BEGIN CERTIFICATE-----** all the way to **-----END CERTIFICATE-----** (including those within the copy) and paste into the CLI when prompted. If choosing import, tell the Guardium system where to import the file from.

```
temp4 > store system certificate console
Please paste your new system certificate, in PEM format.
Include the BEGIN and END lines, then press CTRL-D.

-----BEGIN CERTIFICATE-----
MIID1jCCAsCgAwIBAgIBCDALBgkqhkiG9w0BAQUwgYAxCzAJBgNVBAYTAkNBMRkw
FwYDVQQIExBCcml0aXNoIENvbHVtYmlhMREwDwYDVQQHEwhWaWN0b3JpYTEUMBIG
A1UEChMLUUFfdGVzdF92aWMxFDASBgNVBAsTC1ZpY3Rvcmlhx1FBMRcwFQYDVQQD
Ew5WaWN0b3JpYV9RQV9DQTAeFw0xMDExMDEyMTA5MzhaFw0xNTExMDEyMTA5Mzha
MHMxCzAJBgNVBAYTAkNBMQswCQYDVQQIEwJCQzEQMA4GA1UEBxMHTmV3YnVyeTET
MBEGA1UECgwKUUFfU2FtcGxlMTESMBAGA1UECwwJU2FtcGxlX1FBMRwwGgYDVQQD
DBNzYW1wbGUxX3FhLnZpY3RvcmlhMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA6V6igVPc6bX3VDMXbxWcAFz/smTG5Ui+NqekVfSx38mBpEH+KYDW/dTE
tZe3wT1CbMD4Cc3qNvY7udnOFYctL7PyX/lCBuKgYlYGbcxlaWLbNjQJlVvD0OaF
7mR2Pu3WR7tJ8giBFMLjk9sguobnYCSAAX89t2AWugbUoeAYOXPKHiQVVm2XeYEE
9/03BkLXFYI0qlEszOLw0ULdtXG7EBmgClxPd7m7NpXtpHcH41D5NiAT4uF40go2
irk5kB+kghJPUCk/GX0WprMje7h7hWAEITmEHZ6B5SAsilHzUvc8T+bypYjcLpkK
s2UevzNfvtxTHKZpGMTHdb8g488prwIDAQABo2swaTAfBgNVHSMEGDAWgBR0SB68
8syKm4CUQ27LGB9ftHRZyTAMBgNVHRMBAf8EAjAAMA8GA1UdDwEB/wQFAwMHuAAw
JwYDVR0lBCAwHgYIKwYBBQUHAwQGCCsGAQUFBwMCBggrBgEFBQcDATALBgkqhkiG
9w0BAQUDggEBAJe1Dlh623uD9mBjfB3YDKO3agm3vbdMd2vcdKI8TA5dsxMhmHvm
8E+gVsVOrNVbupLoc6OYeJLPvWQ54j9wZnKavBbma067C1QJJ2jEhOhjzoiEDIqT
l/qBhvqabhTG3vIMFSIwOu0zmQD/2iFu9cykKiru8A8djfZWjjfZiHO4dkkiCInP
/dor+Cm5RokGZ+OXhZ/5hxTuGeSAWJIhObVnrnPLZ2c2uYGh6LYip+2GU6L/rp8z
tmLYfldjtTMGYeP4Ivo1s7KHJqqDlATOBwe2XVR9808SrHI7toSpAbdIqP+f77zv
pb5xvOSfmqLuV6eUvJW8d/Wj2mvgw1qLvqY=
-----END CERTIFICATE-----
```

It asks you to confirm that you want to store the certificate, and when you confirm, it stores it.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 8 (0x8)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CA, ST=British Columbia, L=Victoria, O=QA_test_vic, OU=Victori
a_QA, CN=Victoria_QA_CA
        Validity
            Not Before: Nov  1 21:09:38 2010 GMT
            Not After : Nov  1 21:09:38 2015 GMT
        Subject: C=CA, ST=BC, L=Newbury, O=QA_Sample1, OU=Sample_QA, CN=sample1_
qa.victoria
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:e9:5e:a2:81:53:dc:e9:b5:f7:54:33:17:6f:15:
                    9c:00:5c:ff:b2:64:c6:e5:48:be:36:a7:a4:55:f4:
                    b1:df:c9:81:a4:41:fe:29:80:d6:fd:d4:c4:b5:97:
                    b7:c1:3d:42:6c:c0:f8:09:cd:ea:36:f6:3b:b9:d9:
                    ce:15:87:2d:2f:b3:f2:5f:f9:42:06:e2:a0:62:56:
                    06:6d:cc:65:69:62:db:36:34:09:95:5b:c3:d0:e6:
                    85:ee:64:76:3e:ed:d6:47:bb:49:f2:08:81:14:c2:
                    e3:93:db:20:ba:86:e7:60:24:80:01:7f:3d:b7:60:
                    16:ba:06:d4:a1:e0:18:39:73:ca:1e:24:15:56:6d:
                    97:79:81:04:f7:fd:37:06:42:d7:15:82:34:aa:51:
                    2c:cc:e2:f0:d1:42:dd:b5:71:bb:10:19:a0:0a:5c:
                    4f:77:b9:bb:36:95:ed:a4:77:07:e3:50:f9:36:20:
                    13:e2:e1:78:d2:0a:36:8a:b9:39:90:1f:a4:82:12:
                    4f:50:29:3f:19:7d:16:a6:b3:23:7b:b8:7b:85:60:
                    04:21:39:84:1d:9e:81:e5:20:2c:8a:51:f3:52:f7:
                    3c:4f:e6:f2:a5:88:dc:2e:99:0a:b3:65:1e:bf:33:
                    5f:be:dc:53:1c:a6:69:18:c4:c7:75:bf:20:e3:cf:
                    29:af
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:74:48:1E:BC:F2:CC:8A:9B:80:94:43:6E:CB:18:1F:5F:B4:74:59:C
9

            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment, Data Encipherment, Key Agre
ement
            X509v3 Extended Key Usage:
                E-mail Protection, TLS Web Client Authentication, TLS Web Server
 Authentication
    Signature Algorithm: sha1WithRSAEncryption
        97:b5:0e:58:7a:db:7b:83:f6:60:63:7c:1d:d8:0c:a3:b7:6a:
        09:b7:bd:b7:4c:77:6b:dc:74:a2:3c:4c:0e:5d:b3:13:21:98:
        7b:e6:f0:4f:a0:56:c5:4e:ac:d5:5b:ba:92:e8:73:a3:98:78:
        92:cf:bd:64:39:e2:3f:70:66:72:9a:bc:16:e6:6b:4e:bb:0b:
        54:09:27:68:c4:84:e8:63:ce:88:84:0c:8a:93:97:fa:81:86:
        fa:9a:6e:14:c6:de:f2:0c:15:22:30:3a:ed:33:99:00:ff:da:
        21:6e:f5:cc:a4:2a:2a:ee:f0:0f:1d:8d:f6:56:8e:37:d9:88:
        73:b8:76:49:22:08:89:cf:fd:da:2b:f8:29:b9:46:89:06:67:
        e3:97:85:9f:f9:87:14:ee:19:e4:80:58:92:21:39:b5:67:ae:
        73:cb:67:67:36:b9:81:a1:e8:b6:22:a7:ed:86:53:a2:ff:ae:
        9f:33:b6:62:d8:7e:57:63:b5:33:06:61:e3:f8:22:fa:35:b3:
        b2:87:26:aa:83:94:04:ce:07:07:b6:5d:54:7d:f0:ef:12:ac:
        72:3b:b6:84:a9:01:b7:48:a8:ff:9f:ef:bc:ef:a5:be:71:bc:
        e4:9f:9a:a2:ee:57:a7:94:bc:95:bc:77:f5:a3:da:6b:e0:c3:
        5a:8b:be:a6

Do you want to store this certificate? (y/n)
```

7. Restart the inspection-core for the new certificate to take effect.

Parent topic: Windows: Set up S-TAP authentication with SSL certificates

Windows: Installing an SSL certificate generated outside of the Guardium system

Use this procedure to install the SSL certificate that was created by the CA.

About this task

If the CA is sending you a whole certificate to install, you need two files, the private key in PKCS#8 (password protected) format, and the public key in PEM format. The certificate generated needs to be a 2048 bit RSA key.

The CA sends you two files, and the public cert for your CA.

The public-cert of your CA looks like:

```
enance@enance1 Latest $ cat Victoria_QA_CA.pem
-----BEGIN CERTIFICATE-----
MIID2zCCAsWgAwIBAgIBATALBgkqhkiG9w0BAQUwgYAxCzAJBgNVBAYTAkNBMRkw
FwYDVQQIExBCcml0aXNoIENvbHVtYmlhMREwDwYDVQQHEwhWaWN0b3JpYTEUMBIG
A1UEChMLUUFfdGVzdF92aWMxFDASBgNVBAsTC1ZpY3RvcmlhX1FBMRcwFQYDVQQD
Ew5WaWN0b3JpYV9RQV9DQTAeFw0xMDA4MTIxODMzMDJaFw0zMDA4MTIxODMzMDJa
MIGAMQswCQYDVQQGEwJDQTEZMBcGA1UECBMQQnJpdGlzaCBDb2x1bWJpYTERMA8G
A1UEBxMIVmljdG9yaWExFDASBgNVBAoTC1FBX3Rlc3RfdmljMRQwEgYDVQQLEwtW
aWN0b3JpYV9RQTEXMBUGA1UEAxMOVmljdG9yaWFfUUFfQ0EwggEgMAsGCSqGSIb3
DQEBAQOCAQ8AMIIBCgKCAQEA0x3iAXs1KGNoJThXk0+jcNyMBlfwKWRMTOq9PkF4
piznXCRwPz2nQWk5/fpslchmuVYXJtfZi7umDxp2FEMvMmhJfFZiqbCn1Rb5yH+1
V3RsIerB0DFpoWkdt+wD6BufndO5P9eOlvl4bmTl+F0dUM0TxAwtX73CMQOX/n+i
/WrzpWU4lU71KkyWUfJl2Pm8TLEMr5awpzt2rEJ/Q1qItHcksQDbGY0MNLaNojEU
XBzUpu9ezbv+zVH+5iorFYkrH0NQI0NK+YoR1b3Tto0HLDh6istsMfHdNEEQb9BB
vMjqUz4tGB2HDguYTaNbQJj9Yw8uv7/tfwW/cesrqm8DiQIDAQABo2QwYjAPBgNV
HRMBAf8EBTADAQH/MA8GA1UdDwEB/wQFAwMHBgAwHQYDVR0OBBYEFHRIHrzyzIqb
gJRDbssYH1+0dFnJMB8GA1UdIwQYMBaAFHRIHrzyzIqbgJRDbssYH1+0dFnJMAsG
CSqGSIb3DQEBBQOCAQEAbrImEbRyBka0wO/ZuPd0Hw9jpbxIuaYEskakv7aM4TUQ
awf1CiqwwAymmKb2REItLajhjmBFbXBun7d137vBU2KX104I7WGw0xgI5rmlELa+
2fizugY+Bc6mh+5c0haizkyudKzo8mLz2p/IS7SPh2lJ9rnuBleSt9zfiYanPxX1
Q6z1+WRKIRSUmK+ho4bmtgr5F0+ejmZb9nfzeOBj23H9i0mWoaQ/SO+O2iDIvDY0
KYwqCeS2UNEdTcnfuczbBkqnAsf5/GBPIhnWX3onuLkOsHdY0HHPjoqgHauoxPK8
p0sEvlCK8EFOD6wkp0vtNhFQCykxRimHR6Pz9jEVjw==
-----END CERTIFICATE-----
```

The public-cert specific to you/this Guardium system looks like:

```
enance@enance1 Latest $ cat Sample_givenCert.victoria.qa_pub.pem
-----BEGIN CERTIFICATE-----
MIID5jCCAtCgAwIBAgIBCTALBgkqhkiG9w0BAQUwgYAxCzAJBgNVBAYTAkNBMRkw
FwYDVQQIExBCcml0aXNoIENvbHVtYmlhMREwDwYDVQQHEwhWaWN0b3JpYTEUMBIG
A1UEChMLUUFfdGVzdF92aWMxFDASBgNVBAsTC1ZpY3RvcmlhX1FBMRcwFQYDVQQD
Ew5WaWN0b3JpYV9RQV9DQTAeFw0xMDExMTUyMDUwNThaFw0xNTExMTUyMDUwNTha
MIGEMQswCQYDVQQGEwJDQTEZMBcGA1UECBMQQnJpdGlzaCBDb2xvbWJpYTESMBAG
A1UEBxMJVmFuY291dmVyMQswCQYDVQQKEwJRQTESMBAGA1UECxMJUUFfU0FNUExF
MSUwIwYDVQQDExxTYW1wbGVfZ2l2ZW5DZXJ0LnZpY3RvcmlhLnFhMIIBIDALBgkq
hkiG9w0BAQEDggEPADCCAQoCggEBALdt2XhJEJIAognblgFNoiomVvcGIe9PHs0t
3fP5DxAL5PVm+UCRS0xnnCoKe3pdJNagepDwBa2K5UsHbK4vkHJEgWWEd4bx2Ks7
kRoHr83TXK+W8al1HGKRwUSwN0hfm/KV4v8ZX3AFWs2c/BJ2iA77a0mhU0JuWa1/
/scXitJB5ykPjFb2EuReA6ELphaQ/itjZIQTTeVxbamyx42ia9J5B07lFTp3qGdU
yXUwlEFX0HFPmknAAaQrSnpMdQjkOKgzxU0NTV4ILA66hCVkX+ezQeJA90s/AHA5
hAY2fyurKZsOowoE0xlEpFWCGf87zxfkmTaWthqCS0NzEcJ6efECAwEAAaNrMGkw
HwYDVR0jBBgwFoAUdEgevPLMipuAlENuyxgfX7R0WckwDAYDVR0TAQH/BAIwADAP
BgNVHQ8BAf8EBQMDB7gAMCcGA1UdJQQgMB4GCCsGAQUFBwMEBggrBgEFBQcDAgYI
KwYBBQUHAwEwCwYJKoZIhvcNAQEFA4IBAQB+P1m22B72eRESk9rgNdOB+l48k5xw
QHf64TJcoI/Vcz0vtGBC1jDfZzVDIHJaX6ZMtd023QO6rtjQSnhjhb0t/EiimaNO
tysJ0E999E+HQ7UpKYKvdoznwpYEthyoQJ9quKqQc1YW/l8pQMYDEdK8c7yMbJpv
mrxO8h+G3YYQMT6A9KAk/GPA+yKl0fCuogBhPyWM28q35EAIw6H9ahQigWhNkzrL
DCYO8VCLi3BX+OohLvurkyzJm2lnbm7BSb5QB4jISlRBGPoIWhK6VPypboyABfVs
yWHFVs10EUb0Maa/XNZILTAoYAbYK5sX7Ri5hr5KhxnmDd9AJMQsLfik
-----END CERTIFICATE-----
```

The private key (encrypted with pkx#8) looks like:

```
enance@enance1 Latest $ cat Sample_givenCert.victoria.qa_pri.pem
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIE4jAcBgoqhkiG9w0BDAEDMA4ECAKuMvSla9T4AgIBYgSCBMB/RzDgm4xpRDnA
Cd//wgD9c8junXmVpyJWXWgXhlj3Sgv3toKt2yBQY7Rv0peP1y68nuHKZcp/QZDj
QksDvIJHacpz886KQ2p9xxOCrIO3RTVNULPzrucUNuJ2a5W4IGPGwnrNLKsriRH6
CXQjRu19+kbczmPtrlHu7gj6MuCp58sIyXbsOPCnsZBaAOcf72qeKfVa4tKlpobI
e5YDg+UiJXYv1Kfj9t9tftSfaCym0jK+uE3++y5+ah/k+u/VcEb9b6DrlfG8KaJI
/OYVVmRWVIHEY2QjVOsVEXAARjpugf6cXIn8epw/CMaC0yVg4O9OGDrIz/41DVgk
/b3jlr1oWMRVASSqgOQxE2LrNNAF/XiFwpiLUCBHR0fXX9iKJM7nK6AXlf4hrd31
sMm1hICJvQwuRP+1xCHHs3qKk7oFAdyEdMiYthcOoAaynGmP4vPEMB6Zd0Sxd/yN
7IfBT1U7nCtgo4FpAn4FTnkXRd1DqPpvKLqe0kkQCKo9ZWRnnIS1hAs9VJXS6zou
1IohZewrS/TWnPU+ArE/QJ4WkX2dBAe0Q2HMvuXs6J6Rfn+H2eZC+zThOkvqA0ic
UiQAgJB0ohXWEah9BJbIYNULLpbssUySDLPrxYdZRPn5MFKqCXmWw5tAEV8mIcg4
obB6DxVGHz93iPD0XJyBGWpCdcwItzdngnMR316tX4R3jMy2U0hrzk5o01GoZQQ/
eGYsuPzm4zqVJ8S9gUMFR8ocoPWqwhU+Sq4QPCIQEGf5gwxxt9j7L2TtRbD7kxnD
23aPL/wuk45EFJKTQCeZ3kjUqCCuSbqBJXGEjiiUsahus+yJULJ8boFWu1T8zW7m
/CBK1TzY9Fh+gbdOtN4b+zWUrpk5E7ZctFhEwojVFBwgPzUIZEkap4gH+/F5d3rI
uWFBcN7QER35wO8au/k5kLKHDh+5U15ltkJ38P1pJYFE0p5/K81YWnfvUaJmynJY
DfnK0X6Au69/F6+QR4S+bchbrqk73plIiXbkwqapQ26QH5ztIK3T6/nY6RKa7u6N
WvnskpAE1uxf+soM+BpEzpTl2gQQmEaZnh9Ci3ZnpTZE5tkAL0oTqXL9sToyeynz
Z91m+uKxYRjFvc1KPh+I8dUR0E5qXhBdRR7heIlm7/Dg+UqCUkXoyW89G14u/mJT
jB50CHxLAFOSeXnKn8G/9rOHA565r8L/z8D12sli5T1zHicZJ80211zCSezdF+GG
mI12jfOZmNIBgCVUtpOBNX5IDbr7L+0bM6vuDmXRhnhX4f34+5HGfj3ntLAV7bmn
IOEGIhyoGFnoxyWaT0xxa6MVQJazcKSyyyhO8UixFEoKI3drpFXB0tXVb0CLFq+y
QVp9dHgO3Otzw/yCmCpbQQe8UFRYyC74wBf9yPWDtN6MW/IeEZCBoYaeMR+WyonM
mdq5xbriETXD4zha3NGAv2qnzkfkKMBcVeUULulyixMsHmNNJkINNEsj5deVYtOt
4j5EK/aZsTqTgrVq3oGlwgXM1YptvlVR+HPWZfpjwbL+7/NhmK7AhEPo+qQCVD7t
ZGRbdbB7FEN23m88IMSd8xkhS2M1pop1Cj71P/dA+DD/dgcjP2bw7K923d4r3CcS
1yxPhLKM
-----END ENCRYPTED PRIVATE KEY-----
```

Have these files handy to either import (via scp/ftp/etc) to the Guardium system or to copy-paste into the cli interface on the Guardium system.

Procedure

1. Log in to the Guardium system via CLI.
2. Store the private key by entering: cli> store certificate keystore [import | console] The import takes the saved file, and then copies and pastes the contents of the file into your console interface. It asks for the password that the file was saved with. Either you provided this to the CA for creation of the certificate, or more likely, they provided you with a password when they sent your files. Here's what it looks like on the Guardium system:

```
temp4> store system key console
Please paste your new system key, in PEM format.
Include the BEGIN and END lines, then press CTRL-D.

-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIE4jAcBgoqhkiG9w0BDAEDMA4ECAKuMvSla9T4AgIBYgSCBMB/RzDgm4xpRDnA
Cd//wgD9c8junXmVpyJWXWgXhlj3Sgv3toKt2yBQY7Rv0peP1y68nuHKZcp/QZDj
QksDvIJHacpz886KQ2p9xxOCrIO3RTVNULPzrucUNuJ2a5W4IGPGwnrNLKsriRH6
CXQjRu19+kbczmPtrlHu7gj6MuCp58sIyXbsOPCnsZBaAOcf72qeKfVa4tKlpobI
e5YDg+UiJXYv1Kfj9t9tftSfaCym0jK+uE3++y5+ah/k+u/VcEb9b6DrlfG8KaJI
/0YVVmRWVIHEY2QjVOsVEXAARjpugf6cXIn8epw/CMaC0yVg4O9OGDrIz/41DVgk
/b3jlr1oWMRVASSqgOQxE2LrNNAF/XiFwpiLUCBHR0fXX9iKJM7nK6AXlf4hrd31
sMm1hICJvQwuRP+1xCHHs3qKk7oFAdyEdMiYthcOoAaynGmP4vPEMB6ZdOSxd/yN
7IfBT1U7nCtgo4FpAn4FTnkXRdlDqPpvKLqe0kkQCKo9ZWRnnIS1hAs9VJXS6zou
1IohZewrS/TWnPU+ArE/QJ4WkX2dBAe0Q2HMvuXs6J6Rfn+H2eZC+zThOkvqA0ic
UiQAgJB0ohXWEah9BJbIYNULLpbssUySDLPrxYdZRPn5MFKqCXmWw5tAEV8mIcg4
obB6DxVGHz93iPD0XJyBGWpCdcwItzdngnMR316tX4R3jMy2U0hrzk5o01GoZQQ/
eGYsuPzm4zqVJ8S9gUMFR8ocoPWqwhU+Sq4QPCIQEGf5gwxxt9j7L2TtRbD7kxnD
23aPL/wuk45EFJKTQCeZ3kjUqCCuSbqBJXGEjiiUsahus+yJULJ8boFWu1T8zW7m
/CBK1TzY9Fh+gbdOtN4b+zWUrpk5E7ZctFhEwojVFBwgPzUIZEkap4gH+/F5d3rI
uWFBcN7QER35wO8au/k5kLKHDh+5Ul5ltkJ38P1pJYFE0p5/K81YWnfvUaJmynJY
DfnK0X6Au69/F6+QR4S+bchbrqk73plIiXbkwqapQ26QH5ztIK3T6/nY6RKa7u6N
WvnskpAE1uxf+soM+BpEzpTl2gQQmEaZnh9Ci3ZnpTZE5tkAL0oTqXL9sToyeynz
Z91m+uKxYRjFvc1KPh+I8dUR0E5qXhBdRR7heIlm7/Dg+UqCUkXoyW89G14u/mJT
jB50CHxLAFOSeXnKn8G/9r0HA565r8L/z8D12sli5T1zHicZJ8O211zCSezdF+GG
mI12jfOZmNIBgCVUtpOBNX5IDbr7L+0bM6vuDmXRhnhX4f34+5HGfj3ntLAV7bmn
IOEGIhyoGFnoxyWaT0xxa6MVQJazcKSyyyhO8UixFEoKI3drpFXB0tXVb0CLFq+y
QVp9dHgO3Otzw/yCmCpbQQe8UFRYyC74wBf9yPWDtN6MW/IeEZCBoYaeMR+WyonM
mdq5xbriETXD4zha3NGAv2qnzkfkKMBcVeUULulyixMsHmNNJkINNEsj5deVYtOt
4j5EK/aZsTqTgrVq3oGlwgXM1YptvlVR+HPWZfpjwbL+7/NhmK7AhEPo+qQCVD7t
ZGRbdbB7FEN23m88IMSd8xkhS2M1pop1Cj71P/dA+DD/dgcjP2bw7K923d4r3CcS
1yxPhLKM
-----END ENCRYPTED PRIVATE KEY-----
Enter pass phrase for /var/tmp/key.pem:
writing RSA key

ok
temp4>
```

3. Import the signed certificate with: cli> store certificate sniffer [import | console] It displays the information on the cert and then asks you to confirm storing the cert. It looks like:

```
temp4> store system certificate console
Please paste your new system certificate, in PEM format.
Include the BEGIN and END lines, then press CTRL-D.

-----BEGIN CERTIFICATE-----
MIID5jCCAtCgAwIBAgIBCTALBgkqhkiG9w0BAQUwgYAxCzAJBgNVBAYTAkNBMRkw
FwYDVQQIExBCcml0aXNoIENvbHVtYmlhMREwDwYDVQQHEwhWaWN0b3JpYTEUMBIG
A1UEChMLUUFfdGVzdF92aWMxFDASBgNVBAsTC1ZpY3RvcmlhX1FBMRcwFQYDVQQD
Ew5WaWN0b3JpYV9RQV9DQTAeFw0xMDExMTUyMDUwNThaFw0xNTExMTUyMDUwNTha
MIGEMQswCQYDVQQGEwJDQTEZMBcGA1UECBMQQnJpdGlzaCBDb2xvbWJpYTESMBAG
A1UEBxMJVmFuY291dmVyMQswCQYDVQQKEwJRQTESMBAGA1UECxMJUUFfU0FNUExF
MSUwIwYDVQQDExxTYW1wbGVfZ2l2ZW5DZXJ0LnZpY3RvcmlhLnFhMIIBIDALBgkq
hkiG9w0BAQEDggEPADCCAQoCggEBALdt2XhJEJIAognblgFNoiomVvcGIe9PHsOt
3fP5DxAL5PVm+UCRS0xnnCoKe3pdJNagepDwBa2K5UsHbK4vkHJEgWWEd4bx2Ks7
kRoHr83TXK+W8al1HGKRwUSwN0hfm/KV4v8ZX3AFWs2c/BJ2iA77a0mhU0JuWa1/
/scXitJB5ykPjFb2EuReA6ELphaQ/itjZIQTTeVxbamyx42ia9J5B07lFTp3qGdU
yXUwlEFX0HFPmknAAaQrSnpMdQjkOKgzxU0NTV4ILA66hCVkX+ezQeJA90s/AHA5
hAY2fyurKZsOowoE0xlEpFWCGf87zxfkmTaWthqCS0NzEcJ6efECAwEAAaNrMGkw
HwYDVR0jBBgwFoAUdEgevPLMipuAlENuyxgfX7R0WckwDAYDVR0TAQH/BAIwADAP
BgNVHQ8BAf8EBQMDB7gAMCcGA1UdJQQgMB4GCCsGAQUFBwMEBggrBgEFBQcDAgYI
KwYBBQUHAwEwCwYJKoZIhvcNAQEFA4IBAQB+Plm22B72eRESk9rgNdOB+l48k5xw
QHf64TJcoI/Vcz0vtGBC1jDfZzVDIHJaX6ZMtdO23QO6rtjQSnhjhbOt/EiimaNO
tysJOE999E+HQ7UpKYKvdoznwpYEthyoQJ9quKqQc1YW/l8pQMYDEdK8c7yMbJpv
mrxO8h+G3YYQMT6A9KAk/GPA+yKl0fCuogBhPyWM28q35EAIw6H9ahQigWhNkzrL
DCYO8VCLi3BX+OohLvurkyzJm2lnbm7BSb5QB4jISlRBGPoIWhK6VPypboyABfVs
yWHFVs10EUb0Maa/XNZILTAoYAbYK5sX7Ri5hr5KhxnmDd9AJMQsLfik
-----END CERTIFICATE-----
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 9 (0x9)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CA, ST=British Columbia, L=Victoria, O=QA_test_vic, OU=Victoria_QA, CN=Victoria_QA_CA
        Validity
            Not Before: Nov 15 20:50:58 2010 GMT
            Not After : Nov 15 20:50:58 2015 GMT
        Subject: C=CA, ST=British Colombia, L=Vancouver, O=QA, OU=QA_SAMPLE, CN=Sample_givenCert.victoria.qa
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:b7:6d:d9:78:49:10:92:00:a2:09:db:96:01:4d:
                    a2:2a:26:56:f7:06:21:ef:4f:1e:c3:ad:dd:f3:f9:
                    0f:10:0b:e4:f5:66:f9:40:91:4b:4c:67:9c:2a:0a:
                    7b:7a:5d:24:d6:a0:7a:90:f0:05:ad:8a:e5:4b:07:
                    6c:ae:2f:90:72:44:81:65:84:77:86:f1:d8:ab:3b:
                    01:1a:07:af:cd:d3:5c:af:96:f1:a9:75:1c:62:91:
                    c1:44:b0:37:48:5f:9b:f2:95:e2:ff:19:5f:70:05:
                    5a:cd:9c:fc:12:76:88:0e:fb:6b:49:a1:53:42:6e:
                    59:ad:7f:fe:c7:17:8a:d2:41:e7:29:0f:8c:56:f6:
                    12:e4:5e:03:a1:0b:a6:16:90:fe:2b:63:64:84:13:
                    4d:e5:71:6d:a9:b2:c7:8d:a2:6b:d2:79:07:4e:e5:
                    15:3a:77:a8:67:54:c9:75:30:94:41:57:d0:71:4f:
                    9a:49:c0:01:a4:2b:4a:7a:4c:75:08:e4:38:a8:33:
                    c5:4d:0d:4d:5e:08:2c:0e:ba:84:25:64:5f:e7:b3:
                    41:e2:40:f7:4b:3f:00:70:39:84:06:36:7f:2b:ab:
                    29:9b:0e:a3:0a:04:d3:19:44:a4:55:82:19:ff:3b:
                    cf:17:e4:99:36:96:b6:1a:82:4b:43:73:11:c2:7a:
                    79:f1
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:74:48:1E:BC:F2:CC:8A:9B:80:94:43:6E:CB:18:1F:5F:B4:74:59:C9

            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
            X509v3 Extended Key Usage:
                E-mail Protection, TLS Web Client Authentication, TLS Web Server Authentication
    Signature Algorithm: sha1WithRSAEncryption
        7e:3e:59:b6:d8:1e:f6:79:11:12:93:da:e0:35:d3:81:fa:5e:
        3c:93:9c:70:40:77:fa:e1:32:5c:a0:8f:d5:73:3d:2f:b4:60:
        42:d6:30:df:67:35:43:20:72:5a:5f:a6:4c:b5:d3:b6:dd:03:
        ba:ae:d8:d0:4a:78:63:85:b3:ad:fc:48:a2:99:a3:4e:b7:2b:
        09:38:4f:7d:f4:4f:87:43:b5:29:29:82:af:76:8c:e7:c2:96:
        04:b6:1c:a8:40:9f:6a:b8:aa:90:73:56:16:fe:5f:29:40:c6:
        03:11:d2:bc:73:bc:8c:6c:9a:6f:9a:bc:4e:f2:1f:86:dd:86:
        10:31:3e:80:f4:a0:24:fc:63:c0:fb:22:a5:d1:f0:ae:a2:00:
        61:3f:25:8c:db:ca:b7:e4:40:08:c3:a1:fd:6a:14:22:81:68:
        4d:93:3a:cb:0c:26:0e:f1:50:8b:8b:70:57:f8:ea:21:2e:fb:
        ab:93:2c:c9:9b:69:67:6e:6e:c1:49:be:50:07:88:c8:4a:54:
        41:18:fa:08:5a:12:ba:54:fc:a9:6e:8c:80:05:f5:6c:c9:61:
        c5:56:cd:74:11:46:f4:31:a6:bf:5c:d6:48:2d:30:28:60:06:
        d8:2b:9b:17:ed:18:b9:86:be:4a:87:19:e6:0d:df:40:24:c4:
        2c:2d:f8:a4

Do you want to store this certificate? (y/n)
y
ok
temp4>
```

4. Restart the inspection-core for the new certificate to take effect.

Parent topic: Windows: Set up S-TAP authentication with SSL certificates

Windows: Configuring the S-TAP to use x.509 certificate authentication

About this task

First, take note of what you have assigned as the CA and the CN of the certificate. If you don't remember, use the CLI command show system certificate to display the values.

```
temp4 > show system certificate
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 8 (0x8)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CA, ST=British Columbia, L=Victoria, O=QA_test_vic, OU=Victoria_QA, CN=Victoria_QA_CA
        Validity
            Not Before: Nov  1 21:09:38 2010 GMT
            Not After : Nov  1 21:09:38 2015 GMT
        Subject: C=CA, ST=BC, L=Newbury, O=QA_Sample1, OU=Sample_QA, CN=sample1_qa.victoria
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
```

You need the CN of the cert installed on the Guardium system and the public-key for the CA that signed the certificate on the Guardium system. You also might want a Certificate Revocation list signed by the same CA that signed the Guardium system cert, but it's not necessary.

The relevant parameters in the guard_tap.ini are:

```
; Where is the CA certificate
guardium_ca_path=NULL
; What's the CN to expect from the SqlGuard certificate?
sqlguard_cert_cn=NULL
; Path to crls file or dir
guardium_crl_path=NULL
```

If you do not choose to use a value for a parameter, do not include it in the guard_tap.ini. This is pertinent to the CRL path in particular, or if you want to shut off certificate authentication and go back to TLS.

Procedure

1. Copy the public key [and the CRL if wanted] for the CA that the CA sent you to a directory on the S-TAP host. Take note of this directory.
2. Set `guardium_ca_path=[path-to-CA.pem]`
3. Set `sqlguard_cert_cn=[the full CN or partial CN (using * as a wildcard) of the Guardium system]`
4. If you want to use a certificate revocation list at this time, set `guardium_crl_path=[path-to-crl.crl]` It should look like:

```
guardium_ca_path=/var/tmp/pki/Victoria_QA_CA.pem
sqlguard_cert_cn=sample1_qa.victoria
guardium_crl_path=/var/tmp/pki/Victoria_QA_CA.crl
```

5. Change tls=1.
6. Restart the S-TAP You are now connected using Openssl.

Parent topic: Windows: Set up S-TAP authentication with SSL certificates

Windows: Using DB2 exit library

The DB2 exit mechanism enables Guardium to pick up all DB2 traffic, whether encrypted or not and whether local or remote. This solution simplifies the S-TAP configuration, and provides native DB2 support.

About this task

DB2 exit embeds a Guardium library into DB2 via the DB2_Exit mechanism. The DB2_Exit communicates directly with the Guardium S-TAP to forward all DB2 traffic, whether encrypted or not, and both local and remote. DB2 exit captures TCP as well as SHM traffic.

DB2 exit supports terminate, and UID chain.

Limitations:

- DB2 Exit does not support Guardium data masking (scrub/redact).
- The Guardium firewall (V10.1.2 and later) requires DB2 version 10.1 or later.
- Stored Procedures: DB2-Exit monitors stored procedures. Since Guardium does not know what is in the stored procedure, SQL from inside the procedure is not captured.

Procedure

1. Create a new folder within the DB2 SQLLIB folder, for each instance$DB2PATH\security\plugin\commexit\instance_name For example: C:\Program Files\IBM\SQLLIB\security\plugin\commexit\DB2_01
2. Copy the corresponding DLLs from the S-TAP installation directory into the created directories:
   - For 32-bit DB2:
     - db2fexitx86.dll
     - db2exitx86.dll
   - For 64-bit DB2:
     - db2exitx64.dll
     - db2fexitx64.dll
3. Stop the DB2 instance(s), and issue the following command:
   - for 32 bit: UPDATE DBM CFG USING COMM_EXIT_LIST db2fexitx86
   - for 64 bit: UPDATE DBM CFG USING COMM_EXIT_LIST db2fexitx
4. Start the DB2 instances.
5. Add an inspection engine for DB2 Exit with protocol DB2 Exit. Navigate to Manage > Activity Monitoring > S-TAP Control. See parameter descriptions in Windows: Inspection engine parameters. You can also modify the guard_tap.ini, but it's much easier to use the GUI since it fills in some of the information automatically and does some validation. If modifying the guard_tap.ini
   - [DB_DB2_EXIT1]
   - DB_TYPE=DB2_EXIT
   - INSTANCE_NAME=Service_name

   In the TAP section, set the parameter DB2_EXIT_DRIVER_INSTALLED=1

   The service name is not the instance name. You can determine the service name by using the db2tap utility in the S-TAP installation folder, or from the control panel. Set the instance name to the portion of the service name that follows the second dash (-) delimiter. For example, if the service name in the control panel is `DB2 - DB2COPY1 - DB2-01-0`, set INSTANCE_NAME to `DB2-01-0`.
6. To stop using the feature and stop DB2, issue the following command and then restart the DB2: db2 UPDATE DBM CFG USING COMM_EXIT_LIST NULL

Parent topic: Windows: Configuring S-TAP

Windows: Editing the S-TAP configuration parameters

You can modify the S-TAP configuration after it is installed using GIM, the UI, or for advanced users, the configuration file on the database.

Note: Parameters in the GUI may be safely changed. Parameters that are not in the GUI are advanced, and rarely need changing. They are normally be left unmodified; they are for use by Guardium support or advanced users.
CAUTION:
Do not modify advanced parameters unless you are an expert user or you have consulted with IBM Technical Support.

You can some modify parameters in the GUI. See Windows: Configure S-TAP from the GUI.

GIM is an easy method for modifying parameters, if the S-TAP bundle was installed with GIM. See the instructions for v10.1.4 and higher: Set up by Client; and for v10.1-10.1.3: GIM user interfaces.

You can input any parameter in the Setup by Client page, in the Choose parameters ribbon, using the command WINSTAP_CMD_LINE with the syntax parameter=value for [TAP] parameters, and it is added or updated in the guard_tap.ini.

CAUTION:
There is no validation of the input when using the command WINSTAP_CMD_LINE. Use this command carefully. Do not modify advanced parameters unless you are an expert user or you have consulted with IBM Technical Support.

If it is necessary to modify the configuration file from the database server, follow the procedure described in this section.

The S-TAP needs restarting after you modify the guard_tap.ini. If you're using GIM, it restarts the S-TAP automatically.

CAUTION:
Parameters must be added to their relevant section: [Version], [TAP], [SQLGuard], [DB_<name>].

1. Log on to the database server system using the root account.
2. Stop the S-TAP.
3. Make a backup copy of the configuration file: guard_tap.ini. The default file locations is \Program Files\IBM\Windows S-TAP\Bin\
4. Open the configuration file in a text editor.
5. Edit the file as necessary.
6. Save the file.
7. Restart the S-TAP and verify that your change has been incorporated.

- Windows: Guardium Hosts (SQLGuard) parameters
  These parameters describe a Guardium system to which this S-TAP can connect. All parameters in this section are basic, and appear in the [SQL_GUARD] section.
- Windows: General parameters
  These parameters define basic properties of the S-TAP running on a Windows server and the server on which it is installed, and do not fall into any of the other categories.
- Windows: Inspection engine parameters
  These parameters affect the behavior of the inspection engine that the S-TAP uses to monitor a data repository on a Windows server.
- Windows: Firewall parameters
  These parameters affect the behavior of the S-TAP with respect to the firewall.
- Windows: Query rewrite parameters
  The query rewrite parameters affect the behavior of the S-TAP with respect to discovery.
- Windows: Discovery parameters
  The discovery parameters define the behavior of the auto-discovery feature, for discovering database instances and sending the results to the current active S-TAP.
- Windows: Debug parameters
  These parameters affect the behavior of S-TAP debugging.
- Windows: Configuration Auditing System (CAS) parameters
  These parameters affect the behavior of CAS.
- Windows: Driver parameters
  These parameters affect the behavior of several drivers with which the S-TAP interacts.

Parent topic: Windows: Configuring S-TAP

Windows: Guardium Hosts (SQLGuard) parameters

These parameters describe a Guardium system to which this S-TAP can connect. All parameters in this section are basic, and appear in the [SQL_GUARD] section.

GUI	GIM	guard_tap.ini	Default value	Description
✔ (checkmark indicates the primary host)		PRIMARY		Indicates the primary Guardium system for this S-TAP. In guard_tap.ini: 0=secondary, 1=primary
		TAP_GUARD_TCP_PORT	9500	Read only. Port used for S-TAP to connect to Guardium system.
Guardium Host	WINSTAP_SQLGUARD_IP	SQLGUARD_IP	NULL	IP address or hostname of the Guardium system that acts as the host for the S-TAP. You can define multiple hosts by adding [SQLGuard_1], [SQLGuard_2], and so on.

Parent topic: Windows: Editing the S-TAP configuration parameters

Windows: General parameters

These parameters define basic properties of the S-TAP running on a Windows server and the server on which it is installed, and do not fall into any of the other categories.

These parameters are stored in the [VERSION] section of the S-TAP properties file.

Table 1. S-TAP configuration parameters in the [VERSION] section

GUI	guard_tap.ini	Description

GUI	guard_tap.ini	Description
	STAP_CLIENT_BUILD	Read only. The build version of the installed S-TAP.
Version	PROTOCOL_VERSION	Read only. The version of the Guardium system.

These parameters are stored in the [TAP] section of the S-TAP properties file.

Table 2. S-TAP configuration parameters in the [TAP] section

GUI	GIM	guard_tap.ini	Default value	Description
		TAP_TYPE	wstap	Read only. The type of installed S-TAP agent:
Version		TAP_VERSION		Read only. The version of S-TAP installed on the server.
S-TAP Host		TAP_IP		Read only. Used by the file system monitoring service, instead of the SOFTWARE_TAP_HOST parameter. Both parameters should have the same value.
All can control	WSTAP_ALL_CAN_CONTROL	ALL_CAN_CONTROL	0	0=S-TAP can be controlled only from the primary Guardium system. 1=S-TAP can be controlled from any Guardium system.
Load balancing	WINSTAP_PARTICIPATE_IN_LOAD_BALANCING	PARTICIPATE_IN_LOAD_BALANCING	0	Controls S-TAP load balancing (not enterprise load balancing) to Guardium systems: • 0: No load balancing. • 1: Load balancing. Traffic is balanced between the primary and secondary servers, defined in the SQLGuard section. • 2: Redundancy. Fully mirrored S-TAP sends all traffic to all primary and secondary servers, defined in the SQLGuard section. • 3: Hardware load balancing. Guardium uses a load balancer such as F5 or Cisco. S-TAP sends the traffic to the load balancer, which forwards it to one of the collectors in the pool. Use the primary parameter in the SQLGUARD section to specify primary, secondary, etc. servers. If this parameter is set to 0, and you have more than one Guardium system monitoring traffic, then the non-primary Guardium systems are available for failover.
TLS Use		USE_TLS	0	1=use SSL to encrypt traffic between the agent and the Guardium system. 0=do not encrypt. Warning - the traffic between the agent and Guardium system is in clear text. Guardium recommends encrypting network traffic between the S-TAP and the collector whenever possible, only in cases where the performance is a higher priority than security should this be disabled.
TLS Failover		FAILOVER_TLS	1	1= If ssl connection is not possible for any reason, fail over to using non-secure connection. 0=use only secure connections.
		NUMBER_OF_PROCESSORS	4	Read only. Number of processors on the machine
		ALTERNATE_IPS		Comma-separated list of alternate or virtual IP addresses used to connect to this database server. This is used only when your server has multiple network cards with multiple IPs, or virtual IPs. S-TAP only monitors traffic when the destination IP matches either the S-TAP Host IP defined for this S-TAP, or one of the alternate IPs listed here, so it's recommend that you list all virtual IPs here.
		DB2_TAP_INSTALLED	0	Set to 1 for sniffing DB2 shared memory traffic. Starts the DB2 TAP Service when set to 1.
		DB2_EXIT_DRIVER_INSTALLED		DB2 Integration with S-TAP: set to 1 to enable DB2 Exit library integration 1) Let S-TAP capture all DB2 traffic directly from the DB2 engine - Note, that it is only for specifc DB2 releases - 10.1 and onwards 2) When using this method, Firewall and Scrub/Redact functionality are not supported. Also, stored procedures will not be captured. 3) It lets us pick up all DB2 traffic , regardless of encryption/network protocol. 4) This solution simplifies the S-TAP configuration for customers that will deploy this version of DB2, and gives them native DB2 support.
		DB2_SHMEM_DRIVER_INSTALLED		Deprecated, and replaced by db2_tap_installed.
		DB2_SHMEM_DRIVER_LEVEL		Deprecated
		DC_COLLECT_FREQ	24	Specifies the frequency of collection in hours. Minimum is 1, maximum is 24. GuardiumDC is a service that collects updates of user accounts (SIDs and usernames) from the primary domain controller and then signals the changes to Guardium_S-TAP to update S-TAP internal SID/UserName? map. If S-TAP cannot find resolved SID in the map, it tries to get it from the primary Domain Controller, in which case S-TAP logs a message into debug log (level 7) `The account name *** has been retrieved for SID ***`.
		DC_COLLECT_MAXUSERS	200,000	The maximum number of users to collect. Minimum is 10,000.
		DOMAIN_CONTROLLER		The name of the specific controller from which the SID/usernames map should be read.
		HIGH_RESOLUTION_TIMER	0	0: send time stamps in milliseconds. 1: send time stamps in microseconds, but use milliseconds system timer (to reduce system performance hit - multiply milliseconds by 1000). 2: send time stamps in microseconds, use high resolution windows timer (most accurate). For cases 1 and 2, the S-TAP will indicate to the Guardium system that micro seconds are sent, by setting the reserved byte in PacketData to 1.
		BUFFER_FILE_SIZE	50	Advanced. The initial size of the buffer. The range is 5 to 1000 in MB.

GUI	GIM	guard_tap.ini	Default value	Description
		BUFFER_FILE_NAME		The full path of the memory mapped file if BUFFER_MMAP_FILE=1. Default is WSTAP working folder/StapBuffer/STAP_buffer.dtx
		BUFFER_MMAP_FILE	0	1=memory mapped file option. 0=virtual memory allocation
		SOFTWARE_TAP_HOST		The database server host on which S-TAP is installed. It can be an IP address or a name recognized by the DNSserver. There is no default. An invalidly configured SOFTWARE_TAP_HOST is automatically replaced with a valid local IP.
		TCP_ALIVE_MESSAGE	1	This parameter is deprecated since Guardium v10.x. Guardium collectors no longer send UDP alive messages.
Compr es. level		COMPRESSION_LEVEL	0	Compression level, from 1 to 9. 0=no compression.
		DISABLE_SHARED_MEMORY_IF_ TURNED_ON	0	
		FILE_SNIFFER_FREQUENCY	45	Frequency, in seconds, of: • registration attempts with a Guardium system if a previous attempt was not successful • S-TAP checks for new logs available from Program Files\IBM\Windows S-TAP\Logs for uploading onto collector
		MAXIMUM_PACKET_NUM	300,000	Deprecated
		MIN_BYTES_TO_COMPRESS	500	Advanced. Minimum size of message to compress.
		NOT_SEND_TO_SQLGUARD	0	Advanced. Send nothing to the Guardium system.
		RECV_LEVEL	0	Advanced.
Messag es: remote		REMOTE_MESSAGES	1	1=Send messages to the active Guardium system. 0=Do not send messages
		SEND_LEVEL	0	Advanced. Used for thread prioritization.
		SNIFFED_UDP_PORTS	88	Deprecated.
		SYNCH_FLAG	1	Read only. Deprecated in v10.0. Indicates whether parameters are synchronized with the UI.
		TAP_DBSERVER_NAMES		
		TAP_MIN_HEARTBEAT_INTERVA L	30	Maximum time the S-TAP attempts to write to the primary Guardium system buffer before attempting to write to the secondary Guardium buffer. Default is 30 sec, meaning it tries to write at least 5*60/30 times before failover, by default (using also TAP_MIN_TIME_BEFOREFAILOVER).
		TAP_MIN_TIME_BEFOREFAILOV ER	5	The time interval, in minutes, after which the S-TAP switches to secondary Guardium system if: it cannot connect to its primary Guardium system; it can connect to its primary Guardium system but cannot write to its buffer.
		TCP_BUFFER_SIZE	60000	Advanced. Minimum number of bytes to collect before sending a message to the Guardium system
		TIME_NETWORK	0	Advanced. Used for debug only.
		WEB_SERVER_CONNECTIONS	1	Maximum number of DB connections by .net app.
		WEB_SERVER_INSTALLED	0	Deprecated. Formerly used to enable IIS tap.
		WEB_SERVER_PORT	9000	Port for web-server
		GUARDIUM_CA_PATH	NULL	Location of the Certificate Authority certificate.
		SQLGUARD_CERT_CN	NULL	The common name to expect from the Sqlguard certificate.
		GUARDIUM_CRL_PATH	NULL	The path to the Certificate Revocation list file or directory.
		TAP_FAILOVER_SESSION_QUIES CE	240	The number of seconds after failover, when unused sessions in the failover list from the previous active servers can be removed from the current active server,
		TAP_FAILOVER_SESSION_SIZE	8192	Size, in MB, of the failover session list. 0=no failover sessions should be saved
		DB_IGNORE_RESPONSE		Ignore response at inspection level. Use this function to ignore all database responses at the S-TAP level, without sending anything to the Guardium system. In certain environments, where only interested in client transactions, this function saves bandwidth and processing time for the S-TAP and the Guardium system. Use this function for an easier configuration for ignoring unwanted responses from the database, without loading the network. Database types can be listed as comma separated or ALL can be specified to ignore responses from all types of databases, for example, DB_IGNORE_RESPONSE=ALL or DB_IGNORE_RESPONSE=MSSQL,DB2. Supported DB types: ALL, MSSQL_NP, MSSQL, MYSQL, TRD, PGRS, MSSYB, ORACLE, DB2, DB2_EXIT, INFORMIX, KERBEROS, FTP, CIFS.
		DB_IGNORE_RESPONSE_FILTE R	0.0.0.0/0.0.0.0	Comma separated list of IP/MASKs to be response-ignored. Any DB responses of the type specified by DB_IGNORE_RESPONSE to the specified IP/MASKs are ignored NULL: no filtering of responses 0.0.0.0/0.0.0.0: all IPs are filtered

GUI	GIM	guard_tap.ini	Default value	Description
		DB_IGNORE_RESPONSE_LOCAL	1	filtering of local db responses 0:no, 1:yes Note: TCP traffic is not considered Local traffic for db_ignore_response_local parameter.
		DB_IGNORE_RESPONSE_BYPASS_BYTES	65535	DB_IGNORE_RESPONSE starts when bypass bytes are reached.
		DB_IGNORE_RESPONSE_RESETS_PER_REQUEST	1	Reset DB_IGNORE_RESPONSE_BYPASS_BYTES on each request.
		UPLOAD_FEATURE	1	Controls uploading of all log files from Program Files\IBM\Windows S-TAP\Logs onto the collector.

Parent topic: Windows: Editing the S-TAP configuration parameters

Windows: Inspection engine parameters

These parameters affect the behavior of the inspection engine that the S-TAP uses to monitor a data repository on a Windows server.

These parameters are stored in the individual [DB_<name>] inspection engine section of the S-TAP properties file, with the name of a data repository. There can be multiple sections in a properties file, each describing one inspection engine used by this S-TAP.

GUI	guard_tap.ini	Default value	Description
Protocol	DB_TYPE		The type of data repository being monitored.
Instance Name	INSTANCE_NAME		The name of the database instance on this server. Required for MS SQL Server is using encryption; MS SQL Server using Kerberos Authentication; DB2 Exit traffic collection; DB2 SHM traffic. (Default is MSSQLSERVER.)
Port range	PORT_RANGE_START		Starting port range specific to the database instance. Together with TAP_DB_PORT_MAX defines the range of ports monitored for this database instance. There is usually only a single port in the range. For a Kerberos inspection engine, set the start and end values to 88-88. If a range is used, do not include extra ports in the range, as this could result in excessive resource consumption while the S-TAP attempts to analyze unwanted traffic.
Port range	PORT_RANGE_END		Ending port range specific to the database instance.
Named Pipe	NAMED_PIPE	sql\query,sqllocal,\MSSQLSERVER	Specifies the named pipe used by MS SQL Server for local access. If a named pipe is used, but nothing is specified in this parameter, S-TAP attempts to retrieve the named pipe name from the registry.
Client Ip/Mask	NETWORKS		Identifies the clients to be monitored, using a list of addresses in IP address/mask format: n.n.n.n/m.m.m.m. If an improper IP address/mask is entered, the S-TAP does not start. Valid values: • null=select all clients • 127.0.0.1/255.255.255.255=local traffic only Client Ip/Mask (networks) and Exclude Client Ip/Mask (exclude networks) cannot be specified simultaneously. If the IP address is the same as the IP address for the database server, and a mask of **255.255.255.255** is used, only **local** traffic will be monitored. An address/mask value of **1.1.1.1/0.0.0.0** monitors all clients.
Exclude Client Ip/Mask	EXCLUDE_NETWORKS		A list of client IP addresses and corresponding masks that are excluded from monitoring. This option allows you to configure the S-TAP to monitor all clients, except for a certain client or subnet (or a collection of these). Client Ip/Mask (networks) and Exclude Client Ip/Mask (exclude networks) cannot be specified simultaneously.
Process Name	TAP_DB_PROCESS_NAMES		Database service executables that are to be monitored. For example, a DB2 IE would be TAP_DB_PROCESS_NAMES=DB2SYSCS.EXE. For Oracle or MS SQL Server only, when named pipes are used. For Oracle, the list has two entries: oracle.exe,tnslsnr.exe. For MS SQL Server, the list is just one entry: sqlservr.exe.
Identifier	TAP_IDENTIFIER	NULL	Optional. Used to distinguish inspection engines from one another. If you do not provide a value for this field, Guardium auto-populates the field with a unique name using the database type and GUI display sequence number.

These additional parameters are used with IBM DB2 databases.

Table 1. Additional S-TAP configuration parameters for a DB2 inspection engine

GUI	guard_tap.ini	Default value	Description
DB2 Shared Mem. Adjust.	DB2_FIX_PACK_ADJUSTMENT	80	Required when DB2 is selected as the database type, and shared memory connections are monitored. The offset to the server's portion of the shared memory area. Offset to the beginning of the DB2 shared memory packet, depends on the DB2 version: 32 in pre-8.2.1, and 80 in 8.2.1 and higher.
	DB2_LOG_SIZE		Advanced. The maximum file size, in MB, that the functional DLL can keep buffered before it starts throwing away log entries.

GUI	guard_tap.ini	Default value	Description
DB2 Sh. Mem. Client Pos.	DB2_CLIENT_OFFSET	61440	The offset to the client's portion of the shared memory area. Required when DB2 is selected as the database type, and shared memory connections are monitored. The client offset can be calculated by taking the value of the DB2 parameter ASLHEAPSZ and multiplying by 4096 to get the appropriate offset. The default for this parameter is 61440 decimal. This parameter is calculated by taking the DB2 database configuration value of ASLHEAPSZ and multiplying by 4096. To get the value for ASLHEAPSZ, execute the following DB2 command: `db2 get dbm cfg` and look for the value of ASLHEAPSZ. This value is typically 15 which yields the 61440 default. If it's not 15, take the value and multiply by 4096 to get the appropriate client offset.
DB2 Shared Mem. Size	DB2_SHMEM_SIZE	131072	DB2 shared memory segment size. Required when DB2 is selected as the database type, and shared memory connections are monitored.

Parent topic: Windows: Editing the S-TAP configuration parameters

Windows: Firewall parameters

These parameters affect the behavior of the S-TAP with respect to the firewall.

These parameters are stored in the [TAP] section of the S-TAP properties file.

CAUTION:
These are advanced parameters and are usually modified by IBM Technical Support only.

GIM	guard_tap.ini	Default value	Description
WSTAP_FIREWALL_INSTALLED	FIREWALL_INSTALLED	0	Firewall feature enabled. 1=yes, 0=no.
WSTAP_FIREWALL_TIMEOUT	FIREWALL_TIMEOUT	10	Time, in seconds to, wait for a verdict from the Guardium system if the firewall timed out. Look at firewall_fail_close value to know whether to block or allow the connection. The value can be any integer value.

GIM	guard_tap.ini	Default value	Description
WSTAP_FAIL_CLOSE	FIREWALL_FAIL_CLOSE	0	If the verdict does not come back from the Guardium system and the firewall_timeout expires: if firewall_close = 0 the connection goes through; if firewall_close=1 the connection is blocked.
WSTAP_DEFAULT_STATE	FIREWALL_DEFAULT_STATE	0	0: An event triggers traffic in a session to be watched and checked for firewall policy violations. 1: All traffic is watched by default for firewall policy violations
WSTAP_FORCE_WATCH	FIREWALL_FORCE_WATCH	NULL	When the firewall feature is enabled and firewall_default_state is 0, the session is watched automatically when its client IP matches one of this list of IP/MASK values. The list itself is separated with commas, for example, 1.1.1.1/1.1.1.1,2.2.2.2/2.2.2.2
WSTAP_FORCE_UNWATCH	FIREWALL_FORCE_UNWATCH	NULL	When the firewall feature is enabled and firewall_default_state is 1, the session is unwatched automatically when its client IP matches one of this list of IP/MASK values. The list itself is separated with commas, for example, 1.1.1.1/1.1.1.1,2.2.2.2/2.2.2.2,

Parent topic: Windows: Editing the S-TAP configuration parameters

Windows: Query rewrite parameters

The query rewrite parameters affect the behavior of the S-TAP with respect to discovery.

These parameters are stored in the [TAP] section of the S-TAP properties file.

CAUTION:
These are advanced parameters and are usually modified by IBM Technical Support only.

GIM	guard_tap.ini	Default Value	Description
WINSTAP_QRW_INSTALLED	QUERY_REWRITE_INSTALLED	0	Enable / disable the Dynamic Data Masking for Databases feature. When set to 0, all other parameters in this group are ignored. • 0=No • 1=Yes
WINSTAP_QRW_DEFAULT_STATE	QUERY_REWRITE_DEFAULT_STATE	0	Sets the query rewrite activation trigger. Must be 0 if firewall_default_state=1. • 0=QRW activated per session when triggered by a rule in the installed policy • 1=QRW activated for every session regardless of the installed policy
WINSTAP_QRW_FORCE_WATCH	QUERY_REWRITE_FORCE_WATCH	NULL	Comma separated list of client IP/MASKs (for example, 1.1.1.1/1.1.1.1,2.2.2.2/2.2.2.2) to watch automatically. Valid when qrw_default_state is 0. Cannot be configured to the same range as firewall_force_watch.
WINSTAP_QRW_FORCE_UNWATCH	QUERY_REWRITE_FORCE_UNWATCH	NULL	Comma separated list of client IP/MASKs (for example, 1.1.1.1/1.1.1.1,2.2.2.2/2.2.2.2) to exclude from watching. Valid when firewall_default_state is 1. Cannot be configured to the same range as firewall_force_unwatch.
WINSTAP_QUERY_REWRITE_FAIL_CLOSE	QUERY_REWRITE_FAIL_CLOSE	8	If the verdict does not come back from the Guardium system and the QUERY_REWRITE_TIMEOUT expires: if QUERY_REWRITE_CLOSE=0 the query rewrite operation proceeds; if QUERY_REWRITE_CLOSE=1 the connection is terminated.
WINSTAP_QUERY_REWRITE_TIMEOUT	QUERY_REWRITE_TIMEOUT	10	If the verdict does not come back from the Guardium system and the QUERY_REWRITE_TIMEOUT expires: if QUERY_REWRITE_CLOSE=0 the query rewrite operation proceeds; if QUERY_REWRITE_CLOSE=1 the connection is terminated.

Parent topic: Windows: Editing the S-TAP configuration parameters

Windows: Discovery parameters

The discovery parameters define the behavior of the auto-discovery feature, for discovering database instances and sending the results to the current active S-TAP.

These parameters are stored in the [TAP] section of the S-TAP properties file.

CAUTION:
These are advanced parameters and are usually modified by IBM Technical Support only.

GIM	guard_tap.ini	Default value	Description
WINSTAP_DISCOVERY_INTERVAL	DISCOVERY_INTERVAL	24	The time interval, in hours, at which auto-discovery runs. Set to 0 to disable.

Parent topic: Windows: Editing the S-TAP configuration parameters

Windows: Debug parameters

These parameters affect the behavior of S-TAP debugging.

CAUTION:
These are advanced parameters and are usually modified by IBM Technical Support only.
These parameters are stored in the [DEBUG_OPTIONS] section of the S-TAP properties file:

guard_tap.ini	Default value	Description
DEBUG_BUFFER	1	1=log the contents of local packets
DEBUG_FIREWALL	1	1=log firewall events

These parameters are stored in the [TAP] section of the S-TAP properties file:

Table 1. More S-TAP configuration parameters for debugging

guard_tap.ini	Default value	Description
DEBUG_MAX_FILE_SIZE	200	

guard_tap.ini	Default value	Description
DEBUGLEVEL	0	Level of debug messages to store. Leave at 0 unless directed by IBM Technical Support. 0 Only critical error information From v10.1.4: Two "startup" debug logs saved in bin\..\logs. Filename syntax: startup_hostname_timestamp.new and startup_hostname_timestamp.old. Files from bin\..\logs get uploaded automatically if upload_feature is on. 1 All previous messages plus repeatable critical error information From v10.1.4: Two "normal" debug logs saved in bin\StapBuffer. Filename syntax: stap_hostname_timestamp.new and stap_hostname_timestamp.old. Files from bin\StapBuffer are not uploaded. 2 Not used 3 All messages from level 1, plus brief information about packets sent to a Guardium system 4 All messages from level 3, plus local sniffing log 5 All messages from level 4, plus network sniffing log 6 All messages from level 5, plus heartbeat receiving log 7 All messages from level 6, plus miscellaneous debugging information
DUMP_FILE_MODE	0	Enables capture of dump files if S-TAP crashes. When the parameter is not zero, a new dump file is opened every time the S-TAP starts; it is empty if there is no crash. • 0: no crash dumps generated • 1: crash dumps generated, written to the file stap.diag which is created in the S-TAP working directory. S-TAP copies any existing stap.diag file to a backup file before overwriting the stap.diag file. • 2: time-stamped crash dumps generated, written to a file stap-TIMESTAMP.diag which is created in the S-TAP working directory, where TIMESTAMP identifies when the crash dump was generated. If you have issues with crashes, use this option to capture all dumps, not just the most recent one. The timestamp will also help with debugging. This option uses more diskspace, however.
DEBUG_FILE_MODE	<install folder>/StapBuffer/stap.txt	Deprecated in V10.1.4. Location of the S-TAP debug file. Default until 10.1.4 is <install folder>/StapBuffer/stap.txt. v10.1.4 and higher: If the debuglevel > 0, then the log from the previous S-TAP session (if it exists) is saved as: %STAP_DIR%\Bin\StapBuffer\stap_%HOSTNAME%%YY-MM-DD%%HHMMDD%.old and the new log is created as: %STAP_DIR%\Bin\StapBuffer\stap_%HOSTNAME%%YY-MM-DD%%HHMMDD%.new. In addition to this, start-up logs containing just messages related to S-TAP start-up are always generated in %STAP_DIR%\Logs: startup_%HOSTNAME%%YY-MM-DD%%HHMMDD%.old and startup_%HOSTNAME%%YY-MM-DD%%HHMMDD%.new.
STACK_TRACE_FILE_MODE		Deprecated in V10.1.3. Similar to dump_file_mode
KERNEL_DEBUG_LEVEL	0	
SYSLOG_MESSAGES	1	1= send messages to EventViewer. 0=do not send messages.
WER_DUMP	1	
WER_DUMP_FOLDER	None	If the parameter is not set, the following value is used. If the STAP installation folder is rooted anywhere but C:\Program Files (x86)\... then the WER dump folder is set to the full path ending in ...\Windows S-TAP\Bin\..\Logs. If the STAP installation folder contains the text "(x86)" in it, the dump folder is set to C:\Guardium\Dumps and that path will be created by the STAP process. For example, if Windows S-TAP is installed to C:\PROGRAM FILES\IBM\WINDOWS S-TAP and uses default values for WER_DUMP_FOLDER, WER_DUMP_COUNT, Windows S-TAP uses the following registry settings, then Windows S-TAP crash dump is generated via Windows Error Reporting (WER) facility when it's crashed. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\LocalDumps\guardium_stapr.exe DumpCount REG_DWORD 0x1 DumpFolder REG_EXPAND_SZ C:\PROGRAM FILES\IBM\WINDOWS S-TAP\Bin\..\LOGS\ DumpType REG_DWORD 0x2
WER_DUMP_COUNT	1	Max value is 5.

Parent topic: Windows: Editing the S-TAP configuration parameters

Windows: Configuration Auditing System (CAS) parameters

These parameters affect the behavior of CAS.

GUI	guard_tap.ini	Default value	Description

GUI	guard_tap.ini	Default value	Description
	CAS_SERVER_PORT	16017	The port for communication with the CAS agent. 16017 for unencrypted; 16019 for encrypted.

Parent topic: Windows: Editing the S-TAP configuration parameters

Windows: Driver parameters

These parameters affect the behavior of several drivers with which the S-TAP interacts.

CAUTION:
These are advanced parameters and are usually modified by IBM Technical Support only.

guard_tap.ini	Default value	Description
WFP_DRIVER_INSTALLED	1	WFP driver is used instead of LHMON. This option can be supported on Windows 2008 SP2 or newer because Windows supports WFP API since this version. This parameter is ignored when tcp_driver_installed=1
TCP_DRIVER_INSTALLED	1	Use TCP driver.
ORA_DRIVER_INSTALLED	1	Set to 1 for sniffing Oracle ASO and SSL traffic.
ORA_DRIVER_LEVEL	0	Advanced. Used for thread prioritization.
NAMED_PIPES_DRIVER_INSTALLED	1	Set to 1 for local named pipes sniffing
NAMED_PIPES_DRIVER_LEVEL	0	Advanced. Used for thread prioritization.
SHARED_MEMORY_DRIVER_LEVEL	0	Advanced. Used for thread prioritization.
KRB_MSSQL_DRIVER_INSTALLED	2	Deprecated from v10.1.4. It appears in the guard_tap.ini file but it does not affect the configuration. This parameter is used to decrypt MSSQL SSL and Kerberos encrypted traffic. Set to 1 or 2 to collect MSSQL encrypted traffic and Kerberos tickets. If set to 1, when STAP starts, it pre-collects usernames correlated with SIDs, collecting them for the number of seconds defined in krb_mssql_driver_user_collect_time. When set to 2, the pre-collection isn't done and the usernames are correlated at run time. In V10.1, this parameter is used to enable/disable Correlation. If it is set to non-zero value, use Correlation. If zero, don't use Correlation. The default is non zero value.
KRB_MSSQL_DRIVER_LEVEL	0	This parameter is deprecated from v10.1.4. Controls thread priorities of different sniffers.
KRB_MSSQL_DRIVER_NONBLOCKING	0	This parameter is deprecated from v10.1.4. It appears in the guard_tap.ini file but it does not affect the configuration.1=get domain user names from the domain controller in a separate thread. In this case the first packet with the new user does not resolve the user SID into domain user name.
KRB_MSSQL_DRIVER_USER_COLLECT_TIME	30	This parameter is deprecated from v10.1.4. Use the Correlation driver introduced in 10.1.Time limit for collecting SIDs at STAP startup.
CORRELATION_TIMEOUT	5	The number of seconds the WFP and NMP sniffers wait for correlation to occur before giving up and resuming the flow of traffic to the appliance. The default is 5 seconds.
KRB_MSSQL_DRIVER_ONDEMAND	0	Deprecated in v9.0 GPU patch 50. Set to 1 if you want to save time by resolving user SIDs into domain user names only for Kerberos tickets from new users for the running STAP instance.

Parent topic: Windows: Editing the S-TAP configuration parameters

Windows: S-TAP operation and performance

- Windows: Starting S-TAP using GIM
  With GIM, you can start S-TAP without logging into the database server.
- Windows: Stopping S-TAP using GIM
  With GIM, you can stop S-TAP without logging into the database server.
- Windows: Starting S-TAP without GIM
  Learn to start S-TAP from the database server.
- Windows: Stopping S-TAP without GIM
  Learn to stop S-TAP from the database server.
- Windows: Monitoring S-TAP in the GUI
  Use these standard reports and views to monitor your STAP status in the GUI.
- Windows: S-TAP statistics
  The S-TAP statistics are stored in the database table STAP_Statistic on the collector. This table stores the statistics sent by the S-TAP to the sniffer. There is no pre-defined report for this table.
- Windows: Monitoring with the Guardium Agent Monitor
  The Guardium Agent Monitor (GAM) process monitors Guardium agent performance and responsiveness. It is good for detailed analysis during troubleshooting.
- Windows: Troubleshooting S-TAP problems
  You can use the S-TAP Status monitor tab of the System View to begin investigating any problems. Sometimes you might need to use other tools, particularly if you are monitoring databases for which the inspection engines cannot be verified.

Parent topic: Windows: S-TAP user's guide

Windows: Starting S-TAP using GIM

With GIM, you can start S-TAP without logging into the database server.

About this task

Use the following steps to change the WINSTAP_ENABLED parameter and schedule the S-TAP startup on the database server.

Procedure

1. Click Manage > Module Installation > Set up by Client to open the Client Search Criteria.
2. Click Search to perform a filtered search.
3. Select the Clients that will be the target for the action (starting S-TAP)
4. Click Next to open the Common Modules panel.
5. Select the Module for WINSTAP.
6. Click Next to open the Module Parameters panel.
7. Select the clients that will be the target for the action (starting S-TAP®).
8. Change the WINSTAP_ENABLED parameter to 1 (one).
9. Click Apply to Clients to apply to the targeted clients.
10. Click Install/Update to schedule the update to the targeted clients. This update can be scheduled for NOW or some time in the future. When the schedule is run for this update the S-TAP service on the targeted clients starts at the specified time.

Parent topic: Windows: S-TAP operation and performance

Windows: Stopping S-TAP using GIM

With GIM, you can stop S-TAP without logging into the database server.

About this task

Use the following steps to change the WINSTAP_ENABLED parameter and schedule the S-TAP stop on the database server.

Procedure

1. Click Manage > Module Installation > Set up by Client to open the Client Search Criteria.
2. Enter Client Search Criteria if you want to perform a filtered search of registered clients.
3. Click Search to perform filtered search and display the Clients panel.
4. Select the clients that will be the target for the action (stopping S-TAP).
5. Click Next to open the Common Modules panel.
6. Select the Module for WINSTAP.
7. Click Next to open the Module Parameters panel.
8. Select the client that will be the target for the action (stopping S-TAP).
9. Change the WINSTAP_ENABLED parameter to 0.
10. Click Apply to Clients to apply to the targeted clients
11. Click Install/Update to schedule the update to the targeted clients. This update can be scheduled for NOW or some time in the future. When the schedule is run for this update the S-TAP service on the targeted clients is stopped at the specified time.

Parent topic: Windows: S-TAP operation and performance

Windows: Starting S-TAP without GIM

Learn to start S-TAP from the database server.

About this task

Note: When Windows S-TAP encounters a fatal error during start up that is due to configuration problems (unknown local IP address, more than 1 primary SQL-Guard defined, etc.) it logs the reason to the Windows event log. In some cases an exit after a failure may cause a crash and another logged event. This crash should not cause any concern if it is preceded by the event explaining the reason for the failure.

Procedure

1. Log on to the database server system using a system administrator account.
2. From the Services control panel, start the IBM Security Guardium S-TAP.
3. Log in to the Guardium system to which this S-TAP reports. Verify that the Status light in the S-TAP control panel is green.

Parent topic: Windows: S-TAP operation and performance

Windows: Stopping S-TAP without GIM

Learn to stop S-TAP from the database server.

Procedure

1. Log on to the database server system using a system administrator account.
2. From the Services control panel, stop the IBM Security Guardium S-TAP.
3. Log in to the UI of the Guardium system to which this S-TAP was reporting, verify that the Status light in the S-TAP control panel is now red.

Parent topic: Windows: S-TAP operation and performance

Windows: Monitoring S-TAP in the GUI

Use these standard reports and views to monitor your STAP status in the GUI.

You can create alerts that are based on exceptions that are created by S-TAPs, but other domains that are used by S-TAP reports are system-private and cannot be accessed by users.

System View

S-TAP Status Monitor in the System Monitor window: For each S-TAP reporting to this Guardium system, this report identifies the S-TAP Host, S-TAP Version, DB Server Type, Status (active or inactive), Last Response Received (date and time), Instance Name, Primary Host Name, and true/false indicators for: MS SQL Server Shared Memory, DB2® Shared Memory, Win TCP, Local TCP monitoring, Named Pipes Usage, Encryption, Firewall, DB install Dir, DB port Min and DB Port Max.

Note: The DB2 shared memory driver has been superseded by the DB2 Tap feature.

S-TAP Status Monitor: For each S-TAP reporting to this Guardium system, this report identifies the S-TAP Host, DB Server Type, S-TAP Version, Status (active or inactive), Inspection Engine status, Last Response Received (date and time), Primary Host Name, and true/false indicators for: Firewall and Encrypted. Click the S-TAP Status and the Inspection Engine status to see the Verification status on all Inspection Engines.

S-TAP Events: For each S-TAP reporting to this Guardium system, this report identifies the S-TAP Host, Timestamp, Event type (Success, Error Type, and so on), and Tap Message.

If no messages display in the S-TAP Events panel, the production of event messages may have been disabled in the configuration file for that S-TAP®. If this is the case, you may be able to locate S-TAP event messages on the host system in the Event Log.

Tap Monitor

Primary Guardium® Host Change Log: Log of primary host changes for S-TAPs. The primary host is the Guardium system to which the S-TAP sends data. Each line of the report lists the S-TAP Host, Guardium Host Name, Period Start, and Period End.

S-TAP Status: Displays status information about each inspection engine that is defined on each S-TAP Host. This report does not have From and To date parameters, since it is reporting current status. Each row of the report lists the S-TAP Host, DB Server Type, Status, Last Response, Primary Host Name, Yes/No indicators for the following attributes: Shared Memory Driver Installed, DB2 Shared Memory Driver Installed, Named Pipes Driver Installed, and App Server Installed. In addition, it lists the Hunter DBS.

Inactive S-TAPs Since: Lists all inactive S-TAPs that are defined on the system. It has a single runtime parameter: QUERY_FROM_DATE, which is set to now -1 hour by default. Use this parameter to control how you want to define *inactive*. This report contains the same columns of data as the S-TAP Status report, with the addition of a count for each row of the report.

Parent topic: Windows: S-TAP operation and performance

Windows: S-TAP statistics

The S-TAP statistics are stored in the database table STAP_Statistic on the collector. This table stores the statistics sent by the S-TAP to the sniffer. There is no pre-defined report for this table.

To access, use the GUI. You can create alerts based on results.

The time interval is in hours (example, 5 is every 5 hours). Use - (minus) for a time interval less than 1 hour.

Fields in Table

- TIMESTAMP
- SOFTWARE_TAP_HOST
- TOTAL_BYTES_SO_FAR
- TOTAL_BYTES_DROPPED_SO_FAR
- TOTAL_BYTES_IGNORED
- TOTAL_BUFFER_INIT
- IOCTL_REQUESTS
- TOTAL_RESPONSE_BYTES_IGNORED
- System CPU%
- System Idle%
- STAP CPU%
- Buffer recycled

Parent topic: Windows: S-TAP operation and performance

Windows: Monitoring with the Guardium Agent Monitor

The Guardium Agent Monitor (GAM) process monitors Guardium agent performance and responsiveness. It is good for detailed analysis during troubleshooting.

Note: The GAM service should be off by default as it requires configuration specific to the environment in which it is installed. Improper configuration can cause very serious operational issues. This is a tool to aid in troubleshooting and otherwise is not required.

Monitoring covers:

- CPU usage
- Memory
- Handles
- Number of threads
- Alive - responsiveness (supported agents only, currently S-TAP is the only supported agent) (See Responsiveness)

If a monitored agent exceeds a configured threshold, or if it does not respond to the console request, the following actions can be taken, in any combination:

- Automatically run diag.bat
- Automatically stop/restart the service
- Automatically perform a core dump

Guardium Agent Monitor is installed when S-TAP is installed but is not enabled by default. When S-TAP is uninstalled, GAM is uninstalled.

Note: Just like S-TAP, GAM requires administrative privileges. When installing, run with "Run as Administrator" as an administrative user.

The default install location for GAM is the parent folder of S-TAP (C:\Program Files\IBM\Guardium Agent Monitor\).

The default location for GAM output is the \Bin\ subfolder.

After enabling GAM, make sure the process is running on the database server (resmon.exe).

GAM Configuration

The Guardium Agent Monitor runs with its configuration file, resmon.ini, as its argument. The monitor is controlled by using the resmon.ini file. See sample resmon. Note that the default values for all of the parameters are at the bottom in the sample ini.

Global Configuration

NUMBER_OF_SERVICES: Number of services being monitored

UPDATE_INTERVAL: The length of the interval between polling metrics, in seconds

DEBUG: 1 enables the GAM debug log, 0 disables the log

NUMBER_BYTES_IN_LOG: Maximum number of KB for the GAM log

CPU Threshold Configuration

CPU_LOAD_LIMIT: Percentage CPU threshold at which either action is taken, or UPDATE_INTERVAL starts counting occurrences of reaching threshold

CPU_INTERVALS_ALLOWED: Number of intervals the CPU can be above the threshold before triggering an action (used in conjunction with UPDATE_INTERVAL to set a time limit)

UPDATE_INTERVAL: 0 = action is taken when CPU reaches its load limit. 1 = action is taken when CPU has reached its load limit the number of times specified by CPU_INTERVALS_ALLOWED

CPUAVE: Defines the type of CPU average. 1 = usage averaged across all CPU cores (system average), 0 = percentage of the core used by the process.

Memory Usage, Handle Count and Thread Count Thresholds Configuration

For these metrics there are two thresholds, limit and peak limit. An action is triggered when a limit threshold is passed for more intervals than allowed, or when a peak limit threshold is passed. Metrics refers to CPU, memory, and so on.

[METRIC]_LIMIT: Lower level threshold. An action is triggered if this limit is exceeded for more intervals than [METRIC]_INTERVALS_ALLOWED

[METRIC]_INTERVALS_ALLOWED: Number of intervals allowed for the lower limit threshold before an action is triggered (used with UPDATE_INTERVAL for time limit)

[METRIC]_PEAK_LIMIT: Upper level threshold. An action is triggered if this threshold is exceeded once

Note: [METRIC]_INTERVALS_ALLOWED is used in conjunction with UPDATE_INTERVAL to set a time limit for the threshold. (for example, UPDATE_INTERVAL=1, CPU_INTERVALS_ALLOWED=10, CPU_LOAD_LIMIT=10 means an action is triggered if the CPU load is over 10% for over 10 seconds).

Responsiveness

NAMEDPIPE_INTERVAL: The interval, in seconds, at which the S-TAP agent is pinged to verify responsiveness. Set to "0" to disable

Action Configuration

The actions that can be triggered are described under Core Dump Configuration and Diagnostic Configuration. The second and third actions are only initiated if they are triggered within the ACTION_RESET_INTERVAL of the previous action. If the ACTION_RESET_INTERVAL time has elapsed with no new triggers, then the next trigger starts a new cycle starts with the FIRST_ACTION.

FIRST_ACTION: 0 = no action. 1 = stop then restart the service. 2 = stop the service.

SECOND_ACTION: The action initiated the second time there is a trigger during the ACTION_RESET_INTERVAL. 0 = no action. 1 = stop then restart the service. 2 = stop the service.

THIRD_ACTION: The action initiated the third time there is a trigger during the ACTION_RESET_INTERVAL. 0 = no action. 1 = stop then restart the service. 2 = stop the service.

ACTION_RESET_INTERVALS: Number of seconds before resetting the actions.

Core Dump Configuration

A core dump can be taken every time an action is triggered.

ACTION: 1 = take a core dump whenever an action is triggered; 0 = no core dump is taken.

MAX_NUM_DUMP: The maximum number of core dumps to be stored in the dump directory (keeping the latest).

MDTIMEOUT: Core dump timeout time (in milliseconds)

Diagnostic Configuration

A diagnostic file can be run whenever an action is triggered. The diag.bet diagnostic script, found in the same folder as the service's executable path, runs with the DIAG_PARAMETER parameters.

DIAGACTION: 1 = run the diagnostic script whenever an action is triggered; 0 = no diagnostic script is run.

DIAGNAME: Name of the diagnostic file to be run (must be in the same folder as the service executable)

DIAG_PARAMETER: Parameters to be used when running the diagnostic file

Example of resmon.ini

```
;Semi-colon at the beginning of the line indicates a comment
;
[Global]
NUMBER_OF_SERVICES=1
;
;Interval for checking thresholds (seconds)
UPDATE_INTERVAL=1
;
;Enables monitor log
DEBUG=1
;
;"0" means it won't take minidump for action. "1", it will take minidump
ACTION=1
;
;The maximum number of dump stores in dump directory
MAX_NUM_DUMP=3
;
;The average CPU time, "0" is percentage of one core, "1" is average percentage of all cores in system
CPUAVE=1
;
;miniDump timeout in milliseconds
MDTIMEOUT=1000
;Maximum number of BYTES for monitor log (in KB)
NUMBER_BYTES_IN_LOG=200
;
;Configuration for the service
[Service1]
Name=GUARDIUM_STAP
;
;Interval to check aliveness (supported agents only), set to "0" to disable
NAMEDPIPE_INTERVAL=30
;
;Run diagnostic on action, set to "1" to enable
DIAGACTION=0
;
;Diagnostic file name
DIAGNAME=diag.bat
;
;Diagnostic parameters. If the parameter has spaces it needs to be enclosed with quotes
DIAG_PARAMETER=
;
;Percentage of cpu limit
CPU_LOAD_LIMIT=10
;
;Maximum sequential intervals over CPU_LOAD_LIMIT allowed
CPU_INTERVALS_ALLOWED=10
;
;Memory limit (KB)
MEM_USAGE_LIMIT=150000
MEM_USAGE_PEAK_LIMIT=200000
MEM_USAGE_INTERVALS_ALLOWED=30
;
;Handle limit
HANDLE_COUNT_LIMIT=500
HANDLE_COUNT_PEAK_LIMIT=1000
HANDLE_COUNT_INTERVALS_ALLOWED=20
;
;Thread limit
THREAD_COUNT_LIMIT=200
THREAD_COUNT_PEAK_LIMIT=300
THREAD_COUNT_INTERVALS_ALLOWED=20
;
;'1' take action, then restart the service
;'2' take action, then stop the service without start
FIRST_ACTION=1
SECOND_ACTION=1
THIRD_ACTION=2
;
;Reset interval in seconds
ACTION_RESET_INTERVALS=60
```

Parent topic: Windows: S-TAP operation and performance

Windows: Troubleshooting S-TAP problems

You can use the S-TAP Status monitor tab of the System View to begin investigating any problems. Sometimes you might need to use other tools, particularly if you are monitoring databases for which the inspection engines cannot be verified.

If an S-TAP is not connected to your Guardium system

Check whether the IBM Security Guardium S-TAP service is running on the database server:
Check the IBM Security Guardium S-TAP service and see that it's running.

How can I find the S-TAP version?

- From the GUI, the S-TAP® version number is displayed in Manage > System View > S-TAP Status Monitor
- Alternatively, you can display the S-TAP version number from the command line of the database server.

Run debug from the command line to quickly identify configuration issues

Turn on debug from the GIM GUI or the command line. See debug levels in Windows: Debug parameters.

Verify the connection between the database server and the Guardium system

- Verify that you can ping the Guardium system at *sqlguard_ip* from the database server.
- If the ping is successful, verify that you can telnet to the following ports on the Guardium system: 16016/16018

If there is a firewall between the database server and the Guardium system

Verify that the following ports are open for traffic between these two systems: TCP Port 16016 or TLS Port 16018 for encrypted connections.

Note: Use the following command to check the port availability: `nmap -p port guardium_hostname_or_ip`

Verify that the sqlguard_ip parameter is set to the correct *guardium_hostname_or_ip* for the Guardium system that you are connecting to.

1. Click Manage > Activity Monitoring > S-TAP Control to open S-TAP Control.
2. Locate the S-TAP Host for the IP address that corresponds to your database server.
3. Expand the Guardium Hosts subsection, and verify that the active Guardium Host is correctly configured.
4. If necessary, click Modify to update the Guardium Hosts.

Verify that the S-TAP process is not repeatedly restarting

On the database server, run the command `ps -eaf | grep stap` to verify that the process for S-TAP is not changing.

Verify that S-TAP Approval is not turned on

If S-TAP Approval is turned on, any new S-TAP that connects to the Guardium system is refused.

1. Click Manage > Activity Monitoring > S-TAP Certification to open S-TAP Certification.
2. Look at the S-TAP Approval Needed check box. If this box is checked, new S-TAPs can connect to this Guardium system only after they have been added to the list of approved S-TAPs.
3. If S-TAP Approval is turned on, select Daily Monitor > Approved Tap Clients to view a list of approved S-TAPs. If the S-TAP that you are investigating is not on this list, return to the S-TAP Certification pane, enter the IP address of the S-TAP in the Client Host field, and click Add.

S-TAP verification issues

The verification process attempts to log in to your database's STAP client with an erroneous user ID and password, to verify that this attempt is recognized and communicated to the Guardium system. Your S-TAP could be configured in a way that prevents the inspection engine message from reaching the Guardium system from which the request was made.

These configuration details include:

- Load balancing: if the S-TAP is configured to return responses to more than one Guardium system, the error message could be sent to a different Guardium system.
- Failover: If secondary Guardium systems are configured for the S-TAP, the error message could be sent to a secondary Guardium system if the primary Guardium system is too busy.
- Db_ignore_response: if the S-TAP is configured to ignore all responses from the database, it does not send error messages to the Guardium system.
- Client IP/mask: if any mask is defined that is not 0.0.0.0, it could prevent the error message from being sent.
- Exclude IP/mask: if any mask is defined that is not 0.0.0.0, it could prevent the error message from being sent.

Related topics:

- Windows: Monitoring S-TAP in the GUI
- Windows: Monitoring with the Guardium Agent Monitor
- Windows: Inspection engine verification

Parent topic: Windows: S-TAP operation and performance

Linux and UNIX systems: S-TAP user's guide

Guardium S-TAP is a lightweight software agent installed on database servers and file servers. The information collected by the S-TAPs is the basis of all Guardium traffic reports, alerts, visualizations, etc. This sections covers the S-TAP in Linux, Solaris, AIX and HP-UX servers.

For data activity monitoring, the S-TAP monitors activity between the client and the database and forwards that information to the Guardium collector. The database traffic is logged into the collector based on criteria specified in the security policy. It is also possible to reduce the amount of traffic that is originally sent to the collector by ignoring trusted connections or ignoring traffic from specific IPs.

For file activity monitoring, unlike data activity, the policy rules are pushed down to the file server and thus only data that is specified in the security policy is forwarded to the collector.

S-TAP takes care of upgrading S-TAP kernel components at boot time --adjusting to kernel upgrades in Linux environments.

- Linux and UNIX systems: S-TAP functionality
  Familiarize yourself with these concepts before starting an S-TAP installation on a UNIX system.
- Linux and UNIX systems: Installing S-TAP agents
  Verify prerequisites, then install an S-TAP on Linux, Solaris, AIX and HP-UX servers using the Deploy Monitoring Agents tool, Guardium Installation Manager (GIM), the RPM, or the shell installer.
- Linux and UNIX systems: Uninstalling an S-TAP
  Perform this procedure before installing a new version of S-TAP® if you want to save the old configuration file.
- Linux and UNIX systems: Upgrading S-TAP and K-TAP
  Upgrade S-TAP to continue capturing data from pre-existing sessions, and maintain its configuration, without reboot. You can also upgrade K-TAP as part of the S-TAP upgrade.
- Linux and UNIX systems: Configuring S-TAP
- Linux and UNIX systems: S-TAP operation and performance

Linux and UNIX systems: S-TAP functionality

Familiarize yourself with these concepts before starting an S-TAP installation on a UNIX system.

- Linux and UNIX systems: S-TAP support matrix
  Select your S-TAP setup depending on the data you want to monitor or block. Use this table to identify the monitoring mechanisms (Exit libraries, K-TAP, A-TAP) that can perform the operations you require, per operating system and database.
- Linux and UNIX systems: Linux, Solaris, AIX, and HP-UX S-TAP monitoring mechanisms
  The Guardium UNIX S-TAP uses several different monitoring mechanisms to collect database traffic. During configuration, you can choose the method that best meets your requirements. All mechanisms filter the traffic to reduce network overhead and increase performance.
- Linux and UNIX systems: S-TAP to collector encryption
  S-TAP agents can be configured to communicate with collectors over the network in an encrypted (TLS) manner.
- Linux and UNIX systems: UID chains
  UID chain is a mechanism that allows S-TAP (by way of K-TAP) to track the chain of users that occurred before a database connection. It is supported for Solaris Zones, AIX WPAR, Solaris 8/9, Solaris 11 SPARC.
- Linux and UNIX systems: Proxy firewall
  Learn how to monitor traffic that originates from a proxy server.

Parent topic: Linux and UNIX systems: S-TAP user's guide

Linux and UNIX systems: S-TAP support matrix

Select your S-TAP setup depending on the data you want to monitor or block. Use this table to identify the monitoring mechanisms (Exit libraries, K-TAP, A-TAP) that can perform the operations you require, per operating system and database.

For example, you may want to track or perform one or more of the following:

- local traffic only
- local and network traffic
- shared memory
- encrypted data
- monitor and block
- monitor only

This table covers the most common platforms, database types, and protocols, supported by Guardium's monitoring mechanisms. The table presents general guidelines. There may be other combinations that are not presented here that are supported. Some of the supported setups presented here may be dependent on specific configurations. Contact Customer Support to verify the best setup for your specific needs. Empty cells indicate that the combination is not supported.

The exit libraries are preferred over all other monitoring mechanisms. If you cannot use an exit library, K-TAP is the next choice, then A-TAP, and finally PCAP.

OS	Database	Network traffic	Local traffic	Encrypted traffic	Shared Memory	Kerberos	Blocking	Redaction	UID Chain
AIX	Oracle	K-TAP	K-TAP	A-TAP (ASO, SSL)		K-TAP	K-TAP, A-TAP	K-TAP	K-TAP
AIX	Sybase ASE	K-TAP	K-TAP	A-TAP (SSL)		K-TAP	K-TAP, A-TAP	K-TAP	K-TAP, A-TAP (A-TAP only when configured for real IPs)
AIX	Sybase IQ	K-TAP	K-TAP	A-TAP (decrypts login packets only, no TLS support)	A-TAP (Sybase 16.1 does not support DB username)		K-TAP, A-TAP	K-TAP	K-TAP
AIX	DB2	DB2 Exit, K-TAP	DB2 Exit, K-TAP	DB2 Exit	DB2 Exit, K-TAP	K-TAP	DB2 Exit, K-TAP	K-TAP	DB2 Exit, K-TAP
AIX	Informix	Informix Exit, K-TAP	Informix Exit, K-TAP	Informix Exit	Informix Exit, K-TAP		Informix Exit, K-TAP	Informix Exit, K-TAP	Informix Exit, K-TAP
HP-UX	Oracle	K-TAP	K-TAP	A-TAP (ASO, SSL)		K-TAP	K-TAP, A-TAP	K-TAP	K-TAP
HP-UX	Sybase ASE	K-TAP	K-TAP	A-TAP (Sybase 15 only)			K-TAP, A-TAP	K-TAP	K-TAP, A-TAP (A-TAP only when configured for real IPs)
HP-UX	Sybase IQ	K-TAP	K-TAP				K-TAP	K-TAP	K-TAP
HP-UX	DB2	DB2 Exit, K-TAP	DB2 Exit, K-TAP	DB2 Exit	DB2 Exit, K-TAP	K-TAP	DB2 Exit, K-TAP	K-TAP	DB2 Exit, K-TAP
HP-UX	Informix	Informix Exit, K-TAP	Informix Exit, K-TAP	Informix Exit	Informix Exit, K-TAP		Informix Exit, K-TAP	Informix Exit, K-TAP	Informix Exit, K-TAP

OS	Database	Network traffic	Local traffic	Encrypted traffic	Shared Memory	Kerberos	Blocking	Redaction	UID Chain
Linux	DB2	DB2 Exit, K-TAP		DB2 Exit	DB2 Exit, A-TAP	K-TAP	DB2 Exit, K-TAP, A-TAP (A-TAP with Linux 2.6.36 and higher only)	K-TAP	DB2 Exit, K-TAP
Linux	Informix	Informix Exit, K-TAP	Informix Exit, K-TAP	Informix Exit	Informix Exit, A-TAP		Informix Exit, K-TAP, A-TAP (A-TAP with Linux 2.6.36 and higher only)	Informix Exit, K-TAP	Informix Exit, K-TAP
Linux	Oracle	K-TAP	K-TAP	A-TAP (ASO, SSL)		K-TAP	K-TAP, A-TAP (A-TAP with Linux 2.6.36 and higher only)	K-TAP	K-TAP
Linux	Postgres	K-TAP	K-TAP	A-TAP			K-TAP, A-TAP (A-TAP with Linux 2.6.36 and higher only)	K-TAP	K-TAP, A-TAP (A-TAP only when configured for real IPs)
Linux	Sybase IQ	K-TAP		A-TAP (x86_64 only)	A-TAP (Sybase 16.1 does not support DB username)		K-TAP, A-TAP (A-TAP with Linux 2.6.36 and higher only)	K-TAP	K-TAP, A-TAP (A-TAP only when configured for real IPs)
Linux	Sybase ASE	K-TAP	K-TAP	A-TAP			K-TAP, A-TAP (A-TAP with Linux 2.6.36 and higher only)	K-TAP	K-TAP, A-TAP (A-TAP only when configured for real IPs)
Linux	MongoDB	K-TAP	K-TAP	A-TAP			K-TAP, A-TAP (A-TAP with Linux 2.6.36 and higher only)	K-TAP	K-TAP, A-TAP (A-TAP only when configured for real IPs)
Linux	Teradata	Teradata Exit, K-TAP		Teradata Exit, A-TAP			Teradata Exit, K-TAP, A-TAP (ATAP with Linux 2.6.36 and higher only)	K-TAP	K-TAP, A-TAP (A-TAP only when configured for real IPs)
Linux	Netezza	K-TAP					K-TAP	K-TAP	K-TAP
Linux	Cassandra	K-TAP					K-TAP	K-TAP	K-TAP
Linux	SAP HANA	K-TAP					K-TAP	K-TAP	K-TAP
Linux	MySQL	K-TAP	K-TAP				K-TAP	K-TAP	K-TAP
Linux	MemSQL	K-TAP	K-TAP	K-TAP			K-TAP	K-TAP	K-TAP
Linux	Vertica	K-TAP	K-TAP				K-TAP	K-TAP	K-TAP
Linux	Hadoop (Cloudera / Hortonworks)	K-TAP, Cloudera Navigator, Hortonworks and Apache Ranger		Cloudera Navigator, Hortonworks and Apache Ranger			Hortonworks and Apache Ranger		K-TAP
Linux	Greenplum	K-TAP	K-TAP	A-TAP			K-TAP, A-TAP (Linux 2.6.36 and higher only)	K-TAP	K-TAP
Linux	MariaDB	K-TAP	K-TAP				K-TAP	K-TAP	K-TAP
Linux	Aster	K-TAP	K-TAP				K-TAP	K-TAP	K-TAP
Linux	Couch	K-TAP					K-TAP	K-TAP	K-TAP
Linux	Hive	K-TAP					K-TAP	K-TAP	K-TAP
Linux	Accumulo	K-TAP					K-TAP	K-TAP	K-TAP
Linux	Impala	K-TAP					K-TAP	K-TAP	K-TAP
Linux	Hue	K-TAP	K-TAP				K-TAP	K-TAP	K-TAP

OS	Database	Network traffic	Local traffic	Encrypted traffic	Shared Memory	Kerberos	Blocking	Redaction	UID Chain
Linux	WebHDFS	K-TAP					K-TAP	K-TAP	K-TAP
Linux	Solar	K-TAP					K-TAP	K-TAP	K-TAP
Solaris	Oracle	K-TAP	K-TAP	A-TAP (ASO, SSL)		K-TAP	K-TAP, A-TAP	K-TAP	K-TAP
Solaris	Sybase ASE	K-TAP	K-TAP	A-TAP (Sparc only)		K-TAP	K-TAP, A-TAP	K-TAP	K-TAP, A-TAP (A-TAP only when configured for real IPs)
Solaris	Postgres	K-TAP	K-TAP	A-TAP (9.3 and higher)			K-TAP, A-TAP	K-TAP	K-TAP, A-TAP (A-TAP only when configured for real IPs)
Solaris	Sybase IQ	K-TAP	K-TAP				K-TAP	K-TAP	K-TAP
Solaris	DB2	DB2 Exit, K-TAP	DB2 Exit, K-TAP	DB2 Exit	DB2 Exit, K-TAP	K-TAP	DB2 Exit, K-TAP	K-TAP	DB2 Exit, K-TAP
Solaris	Informix	Informix Exit, K-TAP	Informix Exit, K-TAP	Informix Exit	Informix Exit, K-TAP		Informix Exit, K-TAP	Informix Exit, K-TAP	Informix Exit, K-TAP

Parent topic: Linux and UNIX systems: S-TAP functionality

Linux and UNIX systems: Linux, Solaris, AIX, and HP-UX S-TAP monitoring mechanisms

The Guardium UNIX S-TAP uses several different monitoring mechanisms to collect database traffic. During configuration, you can choose the method that best meets your requirements. All mechanisms filter the traffic to reduce network overhead and increase performance.

You choose the mechanism during installation. All mechanisms filter the traffic so that only database-related traffic for specific sets of client and server IP addresses is collected. The mechanisms are presented here in order of preference: exit libraries, K-TAP, A-TAP, PCAP. See Linux and UNIX systems: S-TAP support matrix and choose the mechanism that meets your needs.

Exit libraries
: The exit libraries are the preferred monitoring mechanism. They give the best performance, and can handle both local and network traffic, whether encrypted or not. They always capture DB_USER. The only disadvantage is that exit libraries are only available on some databases.
They require configuration on the database, and if you upgrade the S-TAP version, then the exit library also requires an update.
Exit libraries are supported only for DB2, Informix, and Teradata.

K-TAP
: K-TAP is a kernel module that is installed into the operating system. It supports all protocols and connection methods (for example, TCP, TLI, SHM, Named Pipes). When enabled, it observes access to a database server by hooking into the mechanisms that are used to communicate between the database client and server.

  Use DB2 and Informix exit libraries with K-TAP to capture shared memory traffic on DB2 and Informix servers. This method is preferable to using A-TAP.

  With Linux, the kernel frequently updates, and there are many kernel versions. The K-TAP version depends on the Linux version. See Linux and UNIX systems: Building a K-TAP.

  K-TAP is installed during S-TAP installation. If K-TAP fails to install, PCAP is installed instead. After it is installed, it can be enabled or disabled with a configuration file setting. If you do not load K-TAP during the S-TAP installation, and decide later that you want to use it, you need to reconfigure and restart the S-TAP.

A-TAP

: The A-TAP (application-level tap) sits in the application layer to support monitoring of encrypted database traffic, which cannot be done in the kernel by K-TAP. A-TAP monitors communication between internal components of the database server. It picks up unencrypted data in the application layer, and sends it to the K-TAP. K-TAP is a proxy to pass data to S-TAP, which then sends it to the Guardium collector.

  With A-TAP, instead of capturing data from the kernel, where the data is still encrypted, Guardium captures data by loading a TAP library before executing the original database binary. The A-TAP libraries are a no-op (no interface). The libraries tap the database in application-mode, after the data is decrypted or before it is encrypted by the database. Hence there are no changes made to how the database would normally operate other than the encrypted traffic is now being captured by Guardium. This means that you do not need to update scripts and tools to call the Guardium code before executing the Oracle code.

  A-TAP is included in every S-TAP but must be configured separately for each database instance to be monitored. See Linux and UNIX systems: A-TAP management.

  Restrictions:

  - A-TAP is not supported in an environment where a 32-bit database is located on a 64-bit server.
  - Monitoring: When using A-TAP, redaction is not supported. Blocking is supported for Linux kernels at 2.6.36 or later releases.

  When to use A-TAP?

  A-TAP is required when DBMS encryption in motion is used, but there may be other internal database implementation details such as shared memory that require it.

  Informix and DB2 on Linux integrate with Guardium more closely using an exit and thus are the recommended method for shared memory support when applicable.

PCAP
: PCAP is a packet-capturing mechanism that listens to network traffic from and to a database server. In a UNIX environment, since the K-TAP captures all network traffic, PCAP is rarely used. PCAP is used to capture local TCP/IP traffic on the device.
Restriction:

- PCAP only works on ports (no shared memory, and so on).

Tip: The PCAP uses the client IP/mask values for all local inspection engines to determine what to monitor and report. A PCAP that is installed with an S-TAP with multiple inspection engines that have different client IP/mask values, captures traffic from all clients that are defined in all inspection engines. The PCAP might be processing and sending more information to the Guardium system than you intend.

Parent topic: Linux and UNIX systems: S-TAP functionality

Linux and UNIX systems: S-TAP to collector encryption

S-TAP agents can be configured to communicate with collectors over the network in an encrypted (TLS) manner.

Guardium recommends encrypting network traffic between the S-TAP and the collector whenever possible, only in cases where the performance is a higher priority than security should this be disabled. There is a small impact on performance when enabling encryption. The default S-TAP configuration is no encryption, to avoid any performance impact.

Before you determine the best choice for your environment, consider the following factors:

- Configuring the S-TAP with TLS requires extra time for encryption that might affect performance on the database server where the S-TAP agent is installed. The appliance (collector) also requires time to decrypt this traffic.
- If applications and database users are communicating with the database in an unencrypted manner, configuring the S-TAP agent to communicate over the network with encryption may not make your network safer.

In general, it makes sense to encrypt S-TAP traffic if the data that is sent to an appliance on a different network is encrypted, or if the database traffic that is monitored is network encrypted.

Encryption is enabled during the inspection engine configuration, and can be modified at any time.

Parent topic: Linux and UNIX systems: S-TAP functionality

Linux and UNIX systems: UID chains

UID chain is a mechanism that allows S-TAP (by way of K-TAP) to track the chain of users that occurred before a database connection. It is supported for Solaris Zones, AIX WPAR, Solaris 8/9, Solaris 11 SPARC.

A user can change user names several times before connecting to the database; for example, by running ssh informix@barbet, su - db2inst1, su -, su - oracle9, and then running sqlplus scott/tiger@onora1. With UID Chains, Guardium can trace this process back to the process that called it, and back to the original (offending) user.

- For Solaris Zones, user IDs may be reported instead of user names.
- The SSH client's IP address and port are added to the UID chain.
- Postgres on Solaris 11 with zones is not supported, due to zone configuration not allowing access from master to slave zones in some directories.
- Solaris Zones and AIX® WPAR: set the db2bp_path in the guard_tap.ini file to the full path of the db2bp executable file, the full path of the relevant db2bp as seen from the global zone/wpar.
- No UID Chains for Inter-process Communication (IPC) on Solaris 8/9.
- UID chains are not detected for Hadoop databases.
- The hunter_trace parameter is required for TCP/IP connections on UNIX S-TAP®. Set hunter_trace = 1 during installation to enable uid_chain for local TCP/IP connections.
- If the process that starts the session exits before STAP can examine it, UID chain does not work
- UID chain does not support local TCP on Linux for DB2. In addition, DB2 exit requires a specific version of the database to support UID chains.
- When running as a non-root user, UID chain does not work for DB2 Shared Memory (SHM) with S-TAP.
- Guardium does not log UID chain for network traffic.
- Guardium might not log UID chain for very short sessions since Guardium relies on the process ID of the application to determine the UID chain. If the process that starts the session exits before STAP can examine it, UID chain does not work.

Restriction: UID chain is not supported in any scenario that requires A-TAP for intercepting the traffic, including:

- ATAP intercepting Oracle ASO encrypted traffic
- ATAP intercepting Sybase encrypted traffic
- ATAP intercepting Teradata encrypted traffic
- DB2 or Informix Shared memory traffic on Linux (requires ATAP)

Purging of UID Chain Records

UID Chain Records older than 2 hours are purged when the regular inference process runs. Records older than 1 day are purged on a nightly basis.

Parent topic: Linux and UNIX systems: S-TAP functionality

Linux and UNIX systems: Proxy firewall

Learn how to monitor traffic that originates from a proxy server.

While S-TAP is normally deployed on a database server, a K-TAP based firewall can be deployed to a proxy server. By utilizing S-GATE, you can monitor traffic that originates from the proxy server. See Linux and UNIX systems: Application server parameters and S-GATE Actions (Blocking Actions) in the Policies help topic for more information on setting appserver parameters and using S-GATE within Policies.

Parent topic: Linux and UNIX systems: S-TAP functionality

Linux and UNIX systems: Installing S-TAP agents

Verify prerequisites, then install an S-TAP on Linux, Solaris, AIX and HP-UX servers using the Deploy Monitoring Agents tool, Guardium Installation Manager (GIM), the RPM, or the shell installer.

Depending on your license key, you can use the same S-TAP agent for both file server and database activity monitoring. FAM does not require any specific S-TAP configuration.

S-TAP Linux, Solaris, AIX and HP-UX installation flow

This flow describes installing S-TAP on a single database reporting to one collector. See the related topics for additional information on S-TAP in clusters and zones.

1. Plan the installation, review these topics:
   - Linux and UNIX systems: S-TAP support matrix
   - Linux and UNIX systems: Linux, Solaris, AIX, and HP-UX S-TAP monitoring mechanisms
   - Linux and UNIX systems: S-TAP to collector encryption
   - Enterprise Load Balancing
2. Verify prerequisites.
   - Linux and UNIX systems: Database version and directory requirements
   - The database has sufficient disk space available (Linux and UNIX systems: Disk space requirements for S-TAP).
   - The ports that are required for communication between the collector and the S-TAP are open (Linux and UNIX systems: Port requirements for S-TAP).
   - Identify required IP addresses and check database connectivity (Linux and UNIX systems: System details and checks).
   - If you are installing with GIM, the GIM client must be installed on the target database server. See Installing the GIM client on a UNIX server.
3. Install S-TAP by one of
   - Linux and UNIX systems: Installing S-TAP agent with GIM (v10.1-10.1.3)
   - Quick start for deploying monitoring agents
   - Linux and UNIX systems: Installing the S-TAP client with GIM (v10.1.4)
   - Linux and UNIX systems: Installing and updating S-TAP using RPM
   - Linux and UNIX systems: Installing the S-TAP client using the shell installer

   During S-TAP installation, if auto-discovery is enabled, it auto-discovers databases and creates inspection engines for the discovered databases. The auto-discovery process runs once at the time of S-TAP installation and does not automatically repeat. You can modify the configuration after the installation is complete.
4. Configure any of the optional components if required by your system.
   -
   - Linux and UNIX systems: Kerberos-authenticated database traffic
   - Linux and UNIX systems: Solaris Zones S-TAP configuration
   - Linux and UNIX systems: Oracle RAC S-TAP configuration
5. Reboot or restart if required (Linux and UNIX systems: When to restart or reboot after S-TAP install or upgrade).
6. Complete the S-TAP configuration.
   - Linux and UNIX systems: Configure S-TAP from the GUI
   - Advanced users only: Linux and UNIX systems: Editing the S-TAP configuration parameters
7. If required, configure Enterprise Load Balancing.

- Linux and UNIX systems: S-TAP installation prerequisites
- Linux and UNIX systems: Install the S-TAP agent
  Install an S-TAP client on a Linux, Solaris, AIX, and HP-UX server by using one of: Guardium Installation Manager (GIM), the GIM Deploy Monitoring Agents tool, the RPM, the shell installer, or a native installer, as best suits your needs.
- Linux and UNIX systems: Special environments configuration
  Use these procedures for as relevant for systems with Zones, RAC, WPAR, clusters.

Parent topic: Linux and UNIX systems: S-TAP user's guide

Linux and UNIX systems: S-TAP installation prerequisites

- Linux and UNIX systems: Database version and directory requirements
  Review these database releases, patch level components, and directories, before you install an S-TAP or any associated agent.
- Linux and UNIX systems: Disk space requirements for S-TAP
  Review these disk space requirements before you install an S-TAP or any associated agent.
- Linux and UNIX systems: Port requirements for S-TAP
  If a firewall is located between the Guardium system and an S-TAP agent, verify that the ports that are used for connections between those components are open.
- Linux and UNIX systems: System details and checks
  Verify you have these system details, and that your database is communicating with the Guardium System.

Parent topic: Linux and UNIX systems: Installing S-TAP agents

Linux and UNIX systems: Database version and directory requirements

Review these database releases, patch level components, and directories, before you install an S-TAP or any associated agent.

Table 1. Linux, Solaris, AIX and HP-UX database versions requirements

DB Type	Version
Linux	make version 3.81 or later. To view your version of the make utility, run the command: `make -v`
Oracle ASO, HP-UX 11.11	LD_PRELOAD must be installed. It is installed by patch PHSS_28436 or later.
TLS	For S-TAP® on a server, either /dev/random or /dev/urandom must be present on the server. See the TLS port requirements in Linux and UNIX systems: Port requirements for S-TAP.

Note: A root user that installs GIM or S-TAP needs permissions to create and delete users and groups.

Table 2. Required directories per platform

Requirement Type	Linux	Solaris	AIX	HP-UX
Installation folder does not exist or is empty	/usr/local/guardium/guard_stap	/usr/local/guardium/guard_stap	/usr/local/guardium/guard_stap	/usr/local/guardium/guard_stap
File exists	/bin/sh	/bin/sh	/bin/sh	/bin/sh

Requirement Type	Linux	Solaris	AIX	HP-UX
File exists	/bin/sed or /usr/bin/sed	/bin/sed or /usr/bin/sed	/bin/sed or /usr/bin/sed	/bin/sed or /usr/bin/sed
File exists	tar, awk, grep, tr	tar, awk, grep, tr	tar, awk, grep, tr	tar, awk, grep, tr
File exists	dd and /dev/zero	dd and /dev/zero	dd and /dev/zero	prealloc
File exists	uudecode in /usr/bin or /tmp or perl exists	uudecode in /usr/bin or /tmp or perl exists	uudecode in /usr/bin or /tmp or perl exists	uudecode in /usr/bin or /tmp or perl exists

Parent topic: Linux and UNIX systems: S-TAP installation prerequisites

Linux and UNIX systems: Disk space requirements for S-TAP

Review these disk space requirements before you install an S-TAP or any associated agent.

Table 1. Linux, Solaris, AIX and HP-UX: S-TAP Disk Space Requirements

Disk Space	Description
S-TAP® Program files	GIM Install: AIX: 400 MB; HP-UX: 500 MB; Linux: 450 MB; Solaris: 400 MB non-GIM Install: AIX: 300 MB; HP-UX: 400 MB; Linux: 350 MB; Solaris: 300 MB FAM program files: 600 MB minimum
Buffer file	By default, the S-TAP uses anonymous memory to stage data for transmission to the Guardium system. If you configure the S-TAP to use a buffer file, the size defaults to 50 MB. The size is controlled by the buffer_file_size parameter in the guard_tap.ini file.

Parent topic: Linux and UNIX systems: S-TAP installation prerequisites

Linux and UNIX systems: Port requirements for S-TAP

If a firewall is located between the Guardium system and an S-TAP agent, verify that the ports that are used for connections between those components are open.

Use your firewall management utility to check, and open as relevant, the ports listed.

Table 1. Port Requirements for Linux, Solaris, AIX and HP-UX servers

Port	Protocol	Guardium system connection to ...
16016	TCP	Clear S-TAP
16018	TLS	Encrypted S-TAP
16020	TCP	Regular pooled connections
16021	TLS	TLS pooled connections
16022	TCP	Feed protocol
16023	TLS	Encrypted S-TAP TLS

Parent topic: Linux and UNIX systems: S-TAP installation prerequisites

Linux and UNIX systems: System details and checks

Verify you have these system details, and that your database is communicating with the Guardium System.

- Obtain the IP address of the database server on which you are installing S-TAP. If virtual IPs are used, note those as well (you will need to configure those later, when completing the configuration).
- If installing on the central manager, identify the IP address of the collector that will control this S-TAP, and to which this S-TAP will report.
- Verify connectivity between the database server and the collector. On the database, enter nmap -p <port> <ip_address>. For example, to check that port 16018 (the port Guardium® uses for TLS) is reachable at IP address 192.168.3.104, enter the command
  nmap -p 16018 192.168.3.104
  Typical output looks like:
  ```
  Starting nmap V. 3.00 Interesting ports on g4.guardium.com (192.168.3.104): Port State Service 16018/tcp open unknown
  ```

Parent topic: Linux and UNIX systems: S-TAP installation prerequisites

Linux and UNIX systems: Install the S-TAP agent

Install an S-TAP client on a Linux, Solaris, AIX, and HP-UX server by using one of: Guardium Installation Manager (GIM), the GIM Deploy Monitoring Agents tool, the RPM, the shell installer, or a native installer, as best suits your needs.

In v10.1.4 and higher, use the GIM deploy monitoring agents tool to automatically activate GIM clients, install S-TAP, and begin monitoring database traffic. See Quick start for deploying monitoring agents.

When you install an S-TAP client, the installation program checks whether the guardium group exists. If the group does not exist, the installation program creates it. If you use certain components or features, such as A-TAP or DB2 Exit, you must add users to this group to ensure proper functioning. These requirements are described in the

relevant sections.

The installation process creates log files for the whole STAP package (S-TAP, K-TAP, A-TAP, Tee, P-CAP, Discovery). The log files are good for troubleshooting failed installations. Locations include /var/tmp, /tmp, and /var/log.

The installation process updates inittab, upstart, and rc scripts.

S-TAP installs into /usr/local/guardium

In rare cases you will need to run the S-TAP as guardium (and not root). This can cause other issues and should only be used when necessary. Running S-TAP as the Guardium user can cause some database or protocol to stop working because of permission levels. Verify that the database path or exec file has permission that allows the user Guardium to read. Depending on your environment, typical limitations are:

- Discovery has limited functionality
- wait_for_db_exec might not work. So for cluster, check the database path or exec file for permission that allow for Guardium user to read.
- Database on AIX® WPAR and Solaris Zones may not work, check the permission to access the install path or exec file
- For Oracle BEQ, restart S-TAP after starting or restarting the database.
- For Informix® shared memory, restart S-TAP after starting or restarting the database.
- For DB2 shared memory,
  - When ktap_fast_shmem is set to 0, if shmctl failed because of permission issue, then in most cases S-TAP should be changed to run as root.
  - When ktap_fast_shmem is set to 1, if shared memory segment has read permission by group, then make sure the DB2 instance has been added to user (Guardium) group. But still on each server, only one set of configuration of DB2® can be supported
  - If shared memory segment has read permission by DB2 user only, then S-TAP has to run as root. (Open a DB2 shared memory session, run the command ipcs -ma, check MODE on the output.)

- Linux and UNIX systems: Installing the S-TAP client with GIM (v10.1.4)
  Use the Guardium Installation Manager to install the S-TAP agent either from a stand-alone Guardium appliance, or from the Central manager to schedule installation on one or more databases.
- Linux and UNIX systems: Installing S-TAP agent with GIM (v10.1-10.1.3)
  The Guardium Installation Manager (GIM) is the recommended method for installing S-TAPs on your database servers. GIM enables you to install, upgrade, and manage agents on individual servers or groups of servers. This includes monitoring processes that were installed under its control, modifying agent parameters, and performing other management tasks.
- Linux and UNIX systems: S-TAP GIM installation parameters
  Understand the parameters (each with a short description) that are typically used in your GIM installation.
- Linux and UNIX systems: Installing and updating S-TAP using RPM
  You can install, uninstall, and update S-TAP on a Linux server using the RPM. The advantage of installing by RPM is that you install and maintain STAP using the same method that you manage all other software on the database server.
- Linux and UNIX systems: Installing the S-TAP client using the shell installer
  Use the shell installer, either in interactive mode or non-interactive mode, to install the S-TAP client on Linux, Solaris, HPUX, and AIX database servers.
- Linux and UNIX systems: S-TAP install script parameters
  Understand the script parameters for installing S-TAPs.
- Linux and UNIX systems: Install and uninstall S-TAP with native installers
  The native installer provides a shell for the shell installer. The only advantage is that it ensures that S-TAP is registered in the operating system asset repository. This registration is not required by Guardium for the installation of the S-TAP, but it might be a requirement at your company. Use the native installer only when necessary.
- Linux and UNIX systems: When to restart or reboot after S-TAP install or upgrade
  This topic details the situations, after S-TAP installation, of when to restart and when to reboot the database server or database instance. Restart/reboot requirements are the same for GIM and non-GIM implementations.
- Linux and UNIX systems: Work with K-TAP
  Learn about K-TAP.

Parent topic: Linux and UNIX systems: Installing S-TAP agents

Linux and UNIX systems: Installing the S-TAP client with GIM (v10.1.4)

Use the Guardium Installation Manager to install the S-TAP agent either from a stand-alone Guardium appliance, or from the Central manager to schedule installation on one or more databases.

Before you begin

- Verify all Linux and UNIX systems: S-TAP installation prerequisites.
- Obtain the correct S-TAP installer script, from either Fix Central, or your Guardium representative. The script name identifies the database server operating system.

About this task

After the installation, you can manage all parameters and monitor processes that were installed under its control. If you install by using one of the other installation methods, fewer agent parameters can be modified using GIM.

Procedure

1. Verify that the GIM client is installed on the database server. See Installing the GIM client on a UNIX server.
2. Upload the relevant S-TAP module to the Guardium Installation Manager appliance.
   a. Go to Manage > Module Installation > Upload Modules.
   b. Click Choose File and select the S-TAP module that you want to install.
   c. Click Upload to upload the module to the appliance. The module appears in the Import Uploaded Modules table.
   d. In the Import Uploaded Modules table, click the check box next to the S-TAP module you want to install. The module imports and becomes available for installation. The Upload Modules page resets and the Import Uploaded Modules table is now empty.
3. Follow the GIM instructions in Set up by Client and Linux and UNIX systems: S-TAP GIM installation parameters. These parameters are mandatory:
   - STAP_TAP_IP: the IP address or FQDN of the database server or node on which the STAP is being installed (equivalent to the -taphost command line parameter). If not specified, the GIM_CLIENT_IP value is used.

- STAP_SQLGUARD_IP: the IP address or FQDN of the primary collector with which this STAP communicates (equivalent to the -appliance command line parameter). If not specified, then, the GIM_URL value is used.

Attention: See the enterprise load balancing parameters in Linux and UNIX systems: S-TAP GIM installation parameters.

What to do next

Verify S-TAP status:

- Monitor installation of the Guardium clients by navigating to Manage > Module Installation > Set up by Client (v10.1.4: Legacy). Click Search, then click the next to the S-TAP.
- View the module status in the report at Manage > Reports > Install Management > GIM Clients Status
- Verify that the row of the S-TAP has a green status (first column) in Monitor > Maintenance > S-TAP Logs > S-TAP Staus

Parent topic: Linux and UNIX systems: Install the S-TAP agent
Related concepts:
Guardium Installation Manager

Linux and UNIX systems: Installing S-TAP agent with GIM (v10.1-10.1.3)

The Guardium Installation Manager (GIM) is the recommended method for installing S-TAPs on your database servers. GIM enables you to install, upgrade, and manage agents on individual servers or groups of servers. This includes monitoring processes that were installed under its control, modifying agent parameters, and performing other management tasks.

Before you begin

- Verify all Linux and UNIX systems: S-TAP installation prerequisites.
- Obtain the correct S-TAP installer script, from either Fix Central, or your Guardium representative. The script name identifies the database server operating system.

About this task

After the installation, you can manage all parameters and monitor processes that were installed under its control. If you install by using one of the other installation methods, fewer agent parameters can be modified using GIM.

Procedure

1. Verify that the GIM client is installed on the database server. See Installing the GIM client on a UNIX server.
2. Upload the relevant S-TAP module to the Guardium Installation Manager appliance.
   a. On the Guardium system, navigate to Manage > Module Installation > Upload Modules.
   b. Click Choose File and select the S-TAP module you want to install.
   c. Click Upload to upload the module to the Guardium system. After uploading, the module will be listed in the Import Uploaded Modules table.
   d. In the Import Uploaded Modules table, click the check box next to the S-TAP module you want to install. The module will be imported and made available for installation. After the module is imported, the Upload Modules page will be reset and the Import Uploaded Modules table will be empty.
3. Select client systems where you want to install an S-TAP.
   a. Navigate to Manage > Module Installation > Setup by Client.
   b. On the Client Search Criteria screen, specify search criteria for the clients where you want to install the S-TAP, then click Search to continue. Search for clients using any combination of the following search criteria:
      - Select a client group.
      - Search by client hostname, IP address, or operating system.
      - Leave all search criteria fields empty to return a list of all available clients.
   c. On the Clients screen, click the check box next to the clients where you want to install the S-TAP, then click Next to continue.
4. Select and configure the S-TAP module before installing to client systems.
   a. From the Modules table on the Common Modules screen, select the S-TAP module for installation, then click Next to continue.
      - Use the Display Latest Versions and Display Bundles Only check boxes to filter the list of available modules.
      - Use the Module Status table to review information about the selected module on the target clients.
   b. From the Client Module Parameters screen, specify installation parameters for the S-TAP. These parameters are mandatory:
      - STAP_TAP_IP: the IP address or FQDN of the database server or node on which the STAP is being installed (equivalent to the -taphost command line parameter). If not specified, the GIM_CLIENT_IP value is used.
      - STAP_SQLGUARD_IP: the IP address or FQDN of the primary collector with which this STAP communicates (equivalent to the -appliance command line parameter). If not specified, then, the GIM_URL value is used.

      Attention: See the enterprise load balancing parameters in Linux and UNIX systems: S-TAP GIM installation parameters.
      - To apply the same parameters to multiple clients, specify installation parameters in the Common Module Parameters fields, click the check box next to clients listed in the Client Module Parameters tables, and then click Apply to Selected.
      - To apply unique parameters to individual clients, specify installation parameters directly in the Client Module Parameters table.
   c. Once you have specified installation parameters for the S-TAP, apply those parameters to the selected clients by clicking Apply to Client.
5. Install the S-TAP to the selected clients.
   a. From the Client Module Parameters screen, click Install/Update.
   b. On the Schedule Date dialog, provide a date or time to begin the installation, then click Apply. To begin the installation immediately, use a value of `now` in the Schedule Date field.

What to do next

Verify S-TAP status:

- Monitor installation of the Guardium clients by navigating to Manage > Module Installation > Set up by Client . Click Search, then click the next to the S-TAP.
- View the module status in the report at Manage > Reports > Install Management > GIM Clients Status
- Verify that the row of the S-TAP has a green status (first column) in Monitor > Maintenance > S-TAP Logs > S-TAP Staus

Parent topic: Linux and UNIX systems: Install the S-TAP agent
Related concepts:

Linux and UNIX systems: S-TAP GIM installation parameters

Understand the parameters (each with a short description) that are typically used in your GIM installation.

All parameters are listed in Linux and UNIX systems: Editing the S-TAP configuration parameters.
CAUTION:
Do not modify advanced parameters unless you are an expert user or you have consulted with IBM Technical Support.

Table 1. Other S-TAP Parameters

GIM parameter	Description
STAP_TAP_IP	The IP address or FQDN of the database server or node on which the STAP is being installed (equivalent to the -taphost command line parameter). If not specified, the GIM_CLIENT_IP value is used.
STAP_SQLGUARD_IP	The IP address or FQDN of the primary collector with which this STAP communicates (equivalent to the -appliance command line parameter). If not specified, then, the GIM_URL value is used.
STAP_ADDITIONAL_SQLGUARD_IPS	List of space delimited additional SQLGUARD IP addresses.
STAP_ENABLED	Enables STAP when installation is complete. Default=1 (yes)
KTAP_ENABLED	Controls the Kernel TAP module. Default=1 (yes)
KTAP_ALLOW_MODULE_COMBOS	For Linux only. If the bundle does not have an exact kernel match, it installs the best match. If the K-TAP cannot be installed or does not start, a query is presented to the user whether to continue installation. Default=N
KTAP_LIVE_UPDATE	Enables the KTAP update without requiring a server reboot. Default=Y

Table 2. Enterprise Load Balancing parameters

GIM parameter	Description
STAP_LOAD_BALANCER_IP	Required if you are configuring load balancing. If blank, enterprise load balancing is disabled. This option specifies the IP address of the central manager or managed unit this S-TAP should use for load balancing. • If configuring the enterprise load balancer to run on a managed unit, the S-TAP must be at V10.1 or higher.
STAP_INITIAL_BALANCER_TAP_GROUP	Optional. The application group name that this S-TAP belongs to for enterprise load balancing. Attention: Group names with spaces or special characters are not supported.
STAP_INITIAL_BALANCER_MU_GROUP	Optional. The MU group name the app-group will be associated with. Requires a defined LB-APP-GROUP. An MU group must already exist on the Central Manager before it can be used during installation of S-TAP Attention: Group names with spaces or special characters are not supported.
STAP_LOAD_BALANCER_NUM_MUS	The number of managed units the enterprise load balancer allocates for this S-TAP.

Parent topic: Linux and UNIX systems: Install the S-TAP agent

Linux and UNIX systems: Installing and updating S-TAP using RPM

You can install, uninstall, and update S-TAP on a Linux server using the RPM. The advantage of installing by RPM is that you install and maintain STAP using the same method that you manage all other software on the database server.

Before you begin

- Verify all Linux and UNIX systems: S-TAP installation prerequisites.
- Obtain the correct S-TAP installer script, from either Fix Central, or your Guardium representative. The script name identifies the database server operating system.

About this task

RPM names have the format: `guard-stap-10.1.0.89165-1-rhel-6-linux-x86_64.x86_64.rpm`, where the first three numbers are the release number of STAP (10.0.0, 10.1.2, etc) and the fourth number is the code revision (89165). The number immediately following is the package iteration which would increment in the case of adding KTAP modules to the RPM.

There is a single RPM for the 32-bit S-TAPs and two RPMs for the 64-bit S-TAPs so that the 64-bit S-TAP does not have a dependency on 32-bit libraries if 32-bit exit libraries are not required. The extra RPM looks like guard-stap-32bit-exit-libs-10.1.0.89165-1-rhel-6-linux-x86_64.x86_64.rpm and has a dependency on the main RPM.

By default, the installation process checks the Linux kernel to determine whether a K-TAP module has been created to work with that kernel. If it exists, it installs (sets ktap_installed = 1). If there is none, K-TAP does not install unless you have enabled Loader Flexibility, which aids in the installation of currently built modules when an exact match does not exist. When Loader Flexibility is enabled, it attempts to build a K-TAP to match your Linux kernel.

v10.12 and higher: RPM installs S-TAP to /opt/guardium; this location cannot be changed. tap_ip is set automatically to the hostname of the system. sqlguard_ip is set to 127.0.0.1 as a placeholder for proper configuration. Complete the configuration after the installation, as described in this procedure.

v10.12 and higher: RPM logs are saved to /opt/guardium/rpm_logs

v10.12 and higher: You can run the guard-config-update script as root user or a non-root user. Use the help command to see your permitted functions.

Procedure

1. Unzip the S-TAP package and copy the RPM to /tmp of the database server.
2. v10.12 and higher: To enable Loader Flexibility, set the Linux environment variable `NI_ALLOW_MODULE_COMBOS="Y"`
3. Install the RPM.

a. To get the RPM name, run: `rpm -qa | grep guard_stap`
b. Run the command: `rpm -i <RPM_NAME>`.
The S-TAP installs.
c. v10.1.2 and higher: Complete the configuration by running the script `guard-config-update` using the parameters described in 4.
d. v10.1: Complete the configuration by updating S-TAP parameters in the UI. See Linux and UNIX systems: Configure S-TAP from the GUI.

The S-TAP shell installer does not install if there is already an RPM installed (preventing double installation).

4. v10.1.2 and higher: To configure or update: log in to the system as `root`, change directory to /opt/guardium and run the script `guard-config-update` using the relevant options and actions from the following list:

[--stap-dir]	S-TAP install directory if not default (default:/usr/local/guardium)
[--set-tap-ip [IP or hostname]]	Set tap_ip in S-TAP config file /usr/local/guardium/guard_stap/guard_tap.ini (default: rh5u9x64t.guard.swg.usma.ibm.com)
[--set-sqlguard-ip [IP or hostname]]	Set sqlguard_ip in SQLGuard_0 section in S-TAP config file /usr/local/guardium/guard_stap/guard_tap.ini (default: 127.0.0.1)
[--add-sqlguard [ID] [IP or hostname]] (V10.1.4 and higher)	Add SQLGuard_ID section to S-TAP config file /usr/local/guardium/guard_stap/guard_tap.ini
[--remove-sqlguard [ID]] (V10.1.4 and higher)	Remove SQLGuard_ID section from S-TAP config file /usr/local/guardium/guard_stap/guard_tap.ini
[--modify-sqlguard [ID] [parameter] [value]] (V10.1.4 and higher)	Set SQLGuard_ID section parameter to value in S-TAP config file /usr/local/guardium/guard_stap/guard_tap.ini. Parameters: sqlguard_ip IP address or hostname of SQLGuard unit sqlguard_port Port used to connect to SQLGuard unit (default: 16016) primary Order of preference (1=primary, 2=secondary, 3=tertiary and so on) num_main_thread Number of main connections to use for this SQLGuard, used with participate_in_load_balancing = { 1, 4 } (default: 1) connection_pool_size Number of data connections per main connection to SQLGuard unit (default: 0)
[--modify-tap [parameter] [value]] (V10.1.4 and higher)	Set TAP section parameter to value in S-TAP config file /usr/local/guardium/guard_stap/guard_tap.ini. Parameters: tap_debug_output_level Set debugging level (must be an integer >= 0, but not 2 or 3) participate_in_load_balancing Set participate in load balancing (values: 1, 2, 3, 4). (See Linux and UNIX systems: S-TAP Load Balancing models and configuration guidelines) use_tls Enable TLS [0, 1] failover_tls TLS connections failover to non-TLS [0, 1] hunter_trace Enable UID chain reporting [0, 1] buffer_file_size Buffer file size in MB alternate_ips Comma-separated list of alternate IPs/hostnames for STAP firewall_installed Enable firewall [0, 1] firewall_fail_close Action to take when there is no verdict (e.g. SQLGuard unreachable or timeout reached) [0 : do nothing, 1 : block connection] firewall_default_state Set default state [0 : not watched, 1 : watched] firewall_timeout Set firewall timeout in seconds firewall_force_watch Comma-separated list of IP/masks to watch even with firewall_default_state=0 firewall_force_unwatch Comma-separated list of IP/masks to unwatch even with firewall_default_state=1
[--help-config [option]]	Show information about an option in the ini, if available (show all available if none specified)

[--set-flexload [0 or 1]]	Enable or disable K-TAP flex loading
[--retry-ktap-load]	Retry KTAP loading (useful after installing dev packages, updating after KTAP request, or changing flexload; automatically restarts S-TAP)
[--discover-ies]	Run discovery and replace all Inspection Engines with those discovered
[--stop [service]]	Stop service (S-TAP, tee, or monitor) temporarily (Solaris services and inittab treat this as permanent disable, does not auto-start on boot until re-enabled)
[--start [service]]	Start service (S-TAP, tee, or monitor) if not already running (implies enable)
[--restart [service]]	Restart service (stap, tee, or monitor) if already running
[--disable [service]]	Prevent service (stap, tee, or monitor) from running again
[--enable [service]]	Configure service (stap, tee, or monitor) for automatic start
[--status]	Show which services are started and if they are configured to start automatically

5. To upgrade, copy the RPM package to /opt/guardium and run the command: `rpm -U <RPM_NAME>`
6. To uninstall:
   a. To get the RPM name, run: `rpm -qa | grep guard_stap`
   b. Run `rpm -e <RPM_NAME>`

After un-install, the directory /opt/guardium still exists, but should only contain /opt/guardium/guard_stap/guard_tap.ini.rpmsave and /opt/guardium/rpm_logs

What to do next

After installation completes, verify S-TAP status:

- Verify that the row of the S-TAP has a green status (first column) in Monitor > Maintenance > S-TAP Logs > S-TAP Staus

Parent topic: Linux and UNIX systems: Install the S-TAP agent

Linux and UNIX systems: Installing the S-TAP client using the shell installer

Use the shell installer, either in interactive mode or non-interactive mode, to install the S-TAP client on Linux, Solaris, HPUX, and AIX database servers.

Before you begin

- Verify all Linux and UNIX systems: S-TAP installation prerequisites.
- Obtain the correct S-TAP installer script, from either Fix Central, or your Guardium representative. The script name identifies the database server operating system.

About this task

Interactive mode is an easy way to install and uninstall, but it must be run individually on each system. It provides validation at each step, which means less chance of errors. It is useful for smaller deployments or whenever a guided, step-by-step installation experience is required. In non-interactive mode, you can install multiple S-TAPs by a script, which is especially useful for managing large deployments.

If any stage of the installation fails, undo all of the steps up to that point. Do not leave the S-TAP partially installed.

The S-TAP package name is in the format: `guard-stap-guard-10.1.0_r79927_1-rhel-5-linux-x86_64.sh`, where the first three numbers are the release number, followed by the revision number, in this example r79927.

Interactive mode is recommended for individual S-TAPs. The system prompts for the basic configuration, and verifies your input immediately, so there are no errors. By default, K-TAP is installed automatically during S-TAP installation. The S-TAP installer checks if the K-TAP is available for the kernel version. If the installation process does not find a matching K-TAP, it attempts to build one to match your Linux kernel. If the K-TAP cannot be installed or does not start, a query is presented to the user whether to continue installation.

Use the non-interactive mode to install on multiple databases multiple systems by running a single command, using the tapfile parameter, --tapfile <path to ini file>, and a guard_tap.ini file that specifies the databases and their details. If you are installing on multiple databases, consider using GIM instead of non-interactive mode.

Procedure

1. Log on to the database server using the `root` account.
2. Designate an installation directory and verify it has sufficient disk space, approximately 400 MB - 500 MB total.
3. Copy the S-TAP .tgz to the local disk on the database server, typically to /tmp.
4. For a typical installation by non-interactive mode, the minimum parameters are:

```
./guard-stap-guard-<release number>_<revision number>_1-rhel-5-linux-x86_64.sh -- --ni --dir
<guardium_installation_directory>   --tapip <tap_ip or host_name>  --sqlguardip < sqlguard_ip or host_name>
```

Note: The S-TAP installer includes all possible modules specific to the different Linux kernels. In rare cases, the S-TAP package does not have the appropriate K-TAP module. In this case, copy the K-TAP module to /tmp and install using these commands. The K-TAP module file is copied into the S-TAP install directory during the install.

```
./guard-stap-guard-10.0.0_r79927_1-rhel-5-linux-x86_64.sh --
--modules /tmp/modules-guard-10.0.0_r79927_1.tgz"
```

5. For interactive mode, run the installed script. In some cases you will need to run the S-TAP as Guardium. This can cause other issues and should only be used when absolutely necessary. The only value you must enter is the IP address of the SQL Guard unit. All others can be left at their defaults. The installer prompts as follows.

```
Enter the path prefix [/usr/local]?
Directory /usr/local/guardium/guard_stap does not exist, would you like to create it? [Y/n]
System library path [/usr/lib]?
Run STAP as root, or as user 'guardium'? [R/u]
Install STAP as root, or as user 'guardium'? [r/U]
```

```
Would you like to run guard_discovery? [Y/n]
Do you want to configure load balancer functionality? [y/N]
IP address of the SQL Guard unit:
Do you want to edit the parameters file? [y/N]

If you later update your kernel to another version, we can
try to load the closest fitting delivered module.  This
feature is not enabled by default, but we recommend enabling
it to reduce delays in support.  Note that if all the
packages require to build natively are installed, a local
build to generate an exact matching module will be attempted
prior to looking for non-exact matches.
Do you wish to enable this feature (y/N/h)?
```

When the script asks "Would you like to run guard_discovery? [Y/n]" if you choose yes, then it runs the guard_discovery once with the --update-tap-flag to initially configure inspection engines. No matter what, it configures guard_discovery --send-to-sqlguard-flag to run once every 24 hours.

What to do next

Verify S-TAP status:

- Verify that the row of the S-TAP has a green status (first column) in Monitor > Maintenance > S-TAP Logs > S-TAP Staus

Parent topic: Linux and UNIX systems: Install the S-TAP agent

Linux and UNIX systems: S-TAP install script parameters

Understand the script parameters for installing S-TAPs.

Install Script Command Line Syntax

usage: guard-stap-setup [options]

--ni	Non-interactive install.
-k | -p	Install with K-TAP or PCAP.
--ignore-compat	Ignore script compatibility check.
-k | -t | -p	Install with K-TAP, Tee, or PCAP.
-u	Update if previous installation found.
--user | --root	Run S-TAP as user or root.
--userinst | --rootinst	Install S-TAP as user or root.
--overwrite-existing	Overwrite existing installation if found.
--tls force | failover | none	S-TAP TLS setting.
--dir <dir>	S-TAP install directory.
--tapfile <file>	The install process reads this guard_tap.ini file and uses its parameters for the STAP you are installing. For example: /var/tmp/guard-stap-10.0.0_r103368_v10_5_1-rhel-5-linux-x86_64.sh --ni --dir /usr/local --tapfile /var/tmp/guard_tap.ini.

--ipfile <file>	Text file that specifies a list of hostnames, IP addresses, and Guardium system addresses separated by a single space. For example:
	`database-01 10.10.10.1 gmachine-01`
	`database-02 10.10.10.2 gmachine-01`
	`database-03 10.10.10.3 gmachine-02`
	The command would look like:/var/tmp/guard-stap-10.0.0_r103368_v10_5_1-rhel-5-linux-x86_64.sh --ni --dir /usr/local --ipfile /var/tmp/ipfile.txtGIM is a much easier way of configuring these parameters.

--tapip <tapip>	The IP of the machine S-TAP is being installed on.
--sqlguardip <sqlguardip>	The IP of the Guardium system this S-TAP should communicate with.
--presets <file> | <preset-options>	Read installation settings or write them to a file.
--no-discovery	Do not use the discovery utility to configure inspection engines.
--modules <module-bundles>	Specify an external K-TAP modules bundle
--ktap_allow_module_combos	Allow inexact kernel match for K-TAP loading
--load-balancer-ip <load_balancer_ip>	The IP address of the central manager or managed unit this S-TAP uses for enterprise load balancing.
--lb-app-group <app_group>	Optional. The application group name that this S-TAP belongs to for enterprise load balancing. Attention: Group names with spaces or special characters are not supported.
--lb-mu-group <mu_group>	Optional. The MU group name the app-group will be associated with. Requires a defined LB-APP-GROUP. This parameter can only be specified once, during initial installation. An MU group must already exist on the Central Manager before it can be used during installation of S-TAP Attention: Group names with spaces or special characters are not supported.
--lb-num-mus <number_of_mus>	The number of managed units the enterprise load balancer allocates for this S-TAP.

Parent topic: Linux and UNIX systems: Install the S-TAP agent

Linux and UNIX systems: Install and uninstall S-TAP with native installers

The native installer provides a shell for the shell installer. The only advantage is that it ensures that S-TAP is registered in the operating system asset repository. This registration is not required by Guardium for the installation of the S-TAP, but it might be a requirement at your company. Use the native installer only when necessary.

A native installer ensures that S-TAP is registered in the operating system asset repository. This registration is not required by Guardium for the installation of the S-TAP, but it might be a requirement at your company. There is a separate native installer for each OS type.

- Linux and UNIX systems: Installing and uninstalling S-TAP with AIX native installer
- Linux and UNIX systems: Installing and uninstalling S-TAP with HP-UX native installer
- Linux and UNIX systems: Installing and uninstalling the S-TAP with Solaris native installer

Parent topic: Linux and UNIX systems: Install the S-TAP agent

Linux and UNIX systems: Installing and uninstalling S-TAP with AIX native installer

Before you begin

Verify all Linux and UNIX systems: S-TAP installation prerequisites.

Procedure

1. Obtain the IP address of the database server on which you are installing S-TAP. If virtual IPs are used, note those as well (you will need to configure those later, when completing the configuration).
2. Identify the IP address of the collector that will control this S-TAP, and to which this S-TAP will report.
3. Verify connectivity between the database server and the collector. On the database, enter nmap -p <port> <ip_address>. For example, to check that port 16018 (the port Guardium® uses for TLS) is reachable at IP address 192.168.3.104, enter the command
   nmap -p 16018 192.168.3.104
   Typical output looks like:
   ```
   Starting nmap V. 3.00 Interesting ports on g4.guardium.com (192.168.3.104): Port State Service 16018/tcp open unknown
   ```
4. Locate the appropriate native installer file (.bff file) from the S-TAP Installation DVD, for your version of AIX®.
5. Enter the following command on a clean server (no previous S-TAP installation) to extract the shell installer for AIX, substituting the appropriate file name with the appropriate .bff file:

   ```
   installp -aX -d/var/tmp<filename> SqlGuardInstaller
   Example:
   installp -aX -d/var/tmp/guard-stap-guard-8.0.00rc1_r20934_1-aix-5.2-aix-powerpc.bff SqlGuardInstaller
   ```

   The shell installer that is extracted, named guardium, is under /usr/local.

6. Continue with running the interactive installer of the installation procedure, running the generated installation script rather than the default installation script for the operating system version.

Parent topic: Linux and UNIX systems: Install and uninstall S-TAP with native installers

Remove AIX S-TAP using Native Installer

Procedure

To remove AIX S-TAP using the native installer:

```
/usr/lib/instl/sm_inst installp_cmd -u -f 'filename'
```

Example

```
/usr/lib/instl/sm_inst installp_cmd -u -f'SqlGuardInstaller'
```

Linux and UNIX systems: Installing and uninstalling S-TAP with HP-UX native installer

Before you begin

Verify all Linux and UNIX systems: S-TAP installation prerequisites.

Procedure

1. Obtain the IP address of the database server on which you are installing S-TAP. If virtual IPs are used, note those as well (you will need to configure those later, when completing the configuration).
2. Identify the IP address of the collector that will control this S-TAP, and to which this S-TAP will report.
3. Verify connectivity between the database server and the collector. On the database, enter nmap -p <port> <ip_address>. For example, to check that port 16018 (the port Guardium® uses for TLS) is reachable at IP address 192.168.3.104, enter the command
   nmap -p 16018 192.168.3.104
   Typical output looks like:
   ```
   Starting nmap V. 3.00 Interesting ports on g4.guardium.com (192.168.3.104): Port State Service 16018/tcp open unknown
   ```
4. Locate the appropriate native installer file (.depot.gz file) on the Guardium S-TAP® Installation DVD, for your version of HPUX.
5. Extract the file with

   ```
   gzip -d <filename>.depot.gz
   ```

6. Enter the swinstall command as follows, supplying the selected file name (the appropriate native installer file) and your database server host name. This command starts an interactive program. Follow the prompts and use the appropriate controls to install the appropriate S-TAP installation program (.sh file), which is located in /var/spool/sw/var/tmp.

   ```
   swinstall -s /var/tmp/<filename>.depot @ ,hostname>:/var/spool/sw
   ```

7. Continue with running the interactive installer in the installation procedure, running the generated installation script rather than the default installation script for the operating system version.

Parent topic: Linux and UNIX systems: Install and uninstall S-TAP with native installers

Remove HPUX S-TAP Using Native Installer

Procedure

To remove HPUX S-TAP using the native installer, use the following command:

```
swremove @<hostname>:/var/spool/sw
```

Linux and UNIX systems: Installing and uninstalling the S-TAP with Solaris native installer

Before you begin

Verify all Linux and UNIX systems: S-TAP installation prerequisites.

Procedure

1. Obtain the IP address of the database server on which you are installing S-TAP. If virtual IPs are used, note those as well (you will need to configure those later, when completing the configuration).
2. Identify the IP address of the collector that will control this S-TAP, and to which this S-TAP will report.
3. Verify connectivity between the database server and the collector. On the database, enter nmap -p <port> <ip_address>. For example, to check that port 16018 (the port Guardium® uses for TLS) is reachable at IP address 192.168.3.104, enter the command
   nmap -p 16018 192.168.3.104
   Typical output looks like:
   ```
   Starting nmap V. 3.00 Interesting ports on g4.guardium.com (192.168.3.104): Port State Service 16018/tcp open unknown
   ```
4. Locate the appropriate native installer file (.pkg file) on the Guardium S-TAP® Installation DVD, for your version of Solaris
5. Enter the pkgadd command to run the installer using the selected file:

   ```
   pkgadd -d <filename>.pkg
   ```

   The shell installer is extracted under /usr/local/guardium

6. Continue with running the interactive installer of the installation procedure, running the extracted shell installer script rather than the default installation script for the operating system version.

Parent topic: Linux and UNIX systems: Install and uninstall S-TAP with native installers

Remove Solaris S-TAP Using Native Installer

Procedure

To remove S-TAP using the native installer:

```
pkgrm GrdTapIns
```

Linux and UNIX systems: When to restart or reboot after S-TAP install or upgrade

This topic details the situations, after S-TAP installation, of when to restart and when to reboot the database server or database instance. Restart/reboot requirements are the same for GIM and non-GIM implementations.

What must be restarted after installation of UNIX/Linux S-TAP when using EXIT
- Teradata: needs database restart
- DB2: needs database restart
- Informix: No restart needed. If ifxserver is running, then restart it. If ifxserver is not running, then no need to restart anything.

What must be restarted after installation of UNIX/Linux S-TAP when using A-TAP
- The database must be restarted when using A-TAP.
- A-TAP should be deactivated and de-instrumented prior to any database software updates.

What must be restarted after installation of UNIX/Linux S-TAP when using K-TAP

OS/Database	**Oracle**		**DB2**		**Sybase**		**MS-SQL**		**Informix**	
	TPC/IPC	SHM	TPC/IPC	SHM	TPC/IPC	SHM	TPC/IPC	SHM	TPC/IPC	SHM
Linux	NR	NR	NR	REQ	NR	NR	NR	NR	NR	REQ
AIX	REQ	NR	REQ	NR	REQ	NR	NA	NR	REQ	NR
Solaris	NR	NR	NR	NR	NR	NR	NR	NR	NR	NR
HP-UX	NR	NR	NR	NR	NR	NR	NR	NR	NR	NR

NR = No restart/reboot required (based on utilizing live update mechanism and referencing live update link if you have one)
REQ = Restart required
NA = not applicable

What must be restarted after a live upgrade of UNIX/Linux S-TAP
- No restarts are necessary at all for live upgrades that do not include A-TAP.
- A-TAP should be deactivated and de-instrumented prior to any S-TAP upgrades.

Reboot guidelines

Rebooting the database server is only required when uninstalling K-TAP (whether or not K-TAP is in use).

Parent topic: Linux and UNIX systems: Install the S-TAP agent

Linux and UNIX systems: Work with K-TAP

Learn about K-TAP.

K-TAP is a kernel module that is installed into the operating system. Is it installed during S-TAP installation. After it is installed, it can be enabled or disabled by using a configuration file setting. When enabled, it observes access to a database server by hooking the mechanisms used to communicate between the database client and server. With K-TAP you do not need to change how database clients connect to the server.

At installation time, you will choose whether or not to load the K-TAP kernel module to the server operating system. This is the only way to load that module. If you do not load K-TAP initially, and decide later that you want to use it, you will need to remove S-TAP®, and then re-install it.
Note: If K-TAP fails to load properly during installation, possibly caused by hardware or software compatibility, P-CAP is installed as the default collection mechanism.
Note: Intra-session traffic is transferred from the old KTAP to the new KTAP by use of a callback. This means that, for most databases, it can take two SQL requests before interception resumes with the new KTAP for pre-existing sessions. In the case of Sybase IOCP, this takes three SQL requests due to the nature of the session.

- Linux and UNIX systems: Understanding K-TAP
  When installing S-TAP, it attempts to load the correct K-TAP version.
- Linux and UNIX systems: Building a K-TAP
  There are hundreds of Linux distributions available, and the list is growing. This means that there might not be a K-TAP already available for your Linux distribution. If the correct K-TAP is not available, the S-TAP installation process can build it for you.
- Linux and UNIX systems: Copying a new K-TAP module to other systems
  When you build a new K-TAP module for a Linux database server, you can copy that module to other database servers that run the same Linux distribution.
- Linux and UNIX systems: Enable K-TAP after installation if Tee was installed by default
  If, during the installation process, K-TAP fails to load properly, possibly caused by hardware or software incompatibility, Tee is installed as the default collection mechanism. To switch back to K-TAP, after compatibility issues are resolved, follow these steps.

Parent topic: Linux and UNIX systems: Install the S-TAP agent

Linux and UNIX systems: Understanding K-TAP

When installing S-TAP, it attempts to load the correct K-TAP version.

KTAP loader mechanism

KTAP loader mechanism uses the following sequence for Linux S-TAP installation (with GIM and non-GIM).

Note: KTAP loader mechanism automatically proceeds to the next step if the previous step was unsuccessful.

1. KTAP Loader looks for exact kernel module match for the Operating system level and if found, loads it.
2. If KTAP Loader did not find a match, it compiles KTAP the module locally and loads it. This can happen only if the system has required packages installed (gcc and kernel-devel for booted kernel).
3. If KTAP Loader has not yet been able to load the correct kernel module, and if FlexLoad mechanism is ON, KTAP Loader finds the closest matching kernel module and loads it.

   To turn on the FlexLoad mechanism, use the following flags:
   - For Shell installation: --ktap_allow_module_combos
   - For GIM installation: KTAP_ALLOW_MODULE_COMBOS=Y
4. If KTAP cannot load the kernel module, it informs you with a "Failed to load" message. It either installs the S-TAP without the KTAP, or fails the S-TAP installation. You can then request a matching module from Guardium support. This takes about two weeks to prepare.

Note: See information on CUSTOM BUNDLES in KTAP parameters topic.
Parent topic: Linux and UNIX systems: Work with K-TAP

Linux and UNIX systems: Building a K-TAP

There are hundreds of Linux distributions available, and the list is growing. This means that there might not be a K-TAP already available for your Linux distribution. If the correct K-TAP is not available, the S-TAP installation process can build it for you.

When you install an S-TAP on a Linux system, the installation process checks the Linux kernel to determine whether a K-TAP has been created to work with that kernel. If a kernel is running that hasn't loaded the KTAP before, it searches for a matching module and loads it. If the installation process does not find a matching K-TAP, it attempts to build one to match your Linux kernel.

Most of the K-TAP code is independent of the kernel. The installer for version 9.1 provides a new layer of code, which enables the kernel-independent code to interact with your kernel. This new layer is delivered as proprietary source code. The installer builds the complete K-TAP by compiling this proprietary source code against your Linux kernel. This produces a K-TAP specific to your Linux distribution.

This process requires that the standard kernel development utilities, provided with Linux distribution, are present on the database server where the K-TAP is to be built. The development package must be an exact match for the kernel. The gcc compiler is also required.

If you have several systems running the same Linux distribution, you can build a K-TAP on one system and copy it to the others. For example, you might build a K-TAP on a test system and then copy it to one or more production database servers after testing. If you use the Guardium Installation Manager (GIM) to install the S-TAP, GIM can automatically copy the bundle containing the new K-TAP to a Guardium system from which you can distribute it to other database servers.

When the installer attempts to build a K-TAP module, you see messages issued by guard-ktap-loader. These messages can include:

- It is attempting to build

- The build has completed
- The K-TAP has been loaded
- The build cannot be attempted, because the kernel development package is not found

Parent topic: Linux and UNIX systems: Work with K-TAP
Linux and UNIX systems: Copying a new K-TAP module to other systems
Copying a K-TAP module by using GIM

Linux and UNIX systems: Copying a new K-TAP module to other systems

When you build a new K-TAP module for a Linux database server, you can copy that module to other database servers that run the same Linux distribution.

Before you begin

Use this procedure after you have built and tested a K-TAP module on a Linux database server.

About this task

If you use the Guardium Installation Manager (GIM) to manage agents on your database servers, use GIM to copy the module. See the link below for the procedure to use.

Procedure

1. Log in to the database server with the tested K-TAP.
2. Change directory to /usr/local/guardium/guard_stap/ktap/current/ and run ./guard_ktap_append_modules to add the locally built modules to modules.tgz.
3. Copy the updated modules.tgz file to the target server.
4. Log in to the target server and change directory to /usr/local/guardium/guard_stap/ktap/current/.
5. Run the K-TAP loader with the retry parameter and the full path to the updated modules.tgz file. For example:

   ```
   guard_ktap_loader retry /tmp/modules-9.0.0_r55927_v90_1.tgz
   ```

6. Restart the S-TAP to connect it to the new K-TAP module.

Results

The custom K-TAP module is ready to use on the target system. Repeat this procedure for each matching Linux system to which you want to deploy the K-TAP module.
Parent topic: Linux and UNIX systems: Work with K-TAP
Copying a K-TAP module by using GIM
Linux and UNIX systems: K-TAP parameters

Linux and UNIX systems: Enable K-TAP after installation if Tee was installed by default

If, during the installation process, K-TAP fails to load properly, possibly caused by hardware or software incompatibility, Tee is installed as the default collection mechanism. To switch back to K-TAP, after compatibility issues are resolved, follow these steps.

Procedure

1. Disable the S-TAP®. See Stop UNIX S-TAP for more information.
2. Edit guard_tap.ini and change *ktap_installed* to 1 and *tee_installed* to 0
3. Run the guard_ktap_loader install command.

   ```
   example: /usr/local/guardium/guard_stap/ktap/current/guard_ktap_loader install
   ```

4. Run the guard_ktap_loader start command.

   ```
   example: /usr/local/guardium/guard_stap/ktap/current/guard_ktap_loader start
   ```

5. Re-enable S-TAP. See Restart UNIX S-TAP for more information.

Parent topic: Linux and UNIX systems: Work with K-TAP

Linux and UNIX systems: Special environments configuration

Use these procedures for as relevant for systems with Zones, RAC, WPAR, clusters.

- Linux and UNIX systems: Solaris Zones S-TAP configuration
  Install and configure S-TAP in the Master zone (global zone). All other zones (local zones) share the resource with Master zone.
- Linux and UNIX systems: Oracle RAC S-TAP configuration
- Linux and UNIX systems: Configure S-TAP for DB2 WPAR
- Linux and UNIX systems: Activate A-TAP on all nodes of a DB2 Cluster
  A-TAP needs to be activated on all nodes where a DB2 server is shared by nodes on a DB2 cluster.
- Linux and UNIX systems: Configure delayed cluster disk mounting
  This topic applies for Oracle, Informix® and DB2® database servers only.

Parent topic: Linux and UNIX systems: Installing S-TAP agents

Linux and UNIX systems: Solaris Zones S-TAP configuration

Install and configure S-TAP in the Master zone (global zone). All other zones (local zones) share the resource with Master zone.

About this task

Procedure

1. Install S-TAP on the master zone (global zone) regardless of the zone in which the database runs, since the local zones share information from the master zone.
2. When configuring the Inspection Engine, use the global zone values for the db_install_dir path and tap_db_process_names. (From the global zone, S-TAP monitors access to databases in all zones.)
3. If you are using PCAP, add the IP addresses of all zones that you want to monitor to the alternate_ips parameter in the guard_tap.ini file on the Solaris database.
4. At the end of the installation:
   - K-TAP is not loaded on the local zone as it is only loaded on the global. It is visible on the local zones.
   - S-TAP does not run on the local zones.

Parent topic: Linux and UNIX systems: Special environments configuration

Linux and UNIX systems: Oracle RAC S-TAP configuration

About this task

Oracle RAC (Real Application: Clusters) allows multiple computers to run Oracle RDBMS software simultaneously while accessing a single database, thus providing clustering.

In a non-RAC Oracle database, a single instance accesses a single database. The database consists of a collection of data files, control files, and redo logs located on disk. The instance comprises the collection of Oracle-related memory and operating system processes that run on a computer system.

In an Oracle RAC environment, two or more computers (each with an Oracle RDBMS instance) concurrently access a single database. This allows an application or user to connect to either computer and have access to a single coordinated set of data.

Procedure

1. Install S-TAP on all nodes. In case GIM is used, install GIM client on all nodes, then install bundle S-TAP on all nodes.
2. Configure the STAP parameters. All of the parameters can be configured through GIM UI.
   - STAP_TAP_IP: public IP configured for the node
   - STAP_ALTERNATE_IPS: comma separated list of VIPs (virtual IPs) configured for the node, and the scan listener
     Tip: Use this command to retrieve value for virtual hostnames to put in alternate_ips: su – grid –c 'cat $ORACLE_HOME/network/admin/*.ora'|grep –i host

     For example:

     ```
     [root@racvm121 ~]# su - grid -c 'cat $ORACLE_HOME/network/admin/*.ora'|grep -i host
     LISTENER_RACVM121=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=racvm121-vip.guard.swg.usma.ibm.com)(PORT=1521)
     ```

   - Configure STAP Inspection engine parameter: unix_domain_socket_marker=<key>, where <key> value can be found in listener.ora in the IPC protocol definition
     Tip: Command to retrieve value for unix_domain_socket: `su - grid -c 'cat $ORACLE_HOME/network/admin/*.ora'|grep -i KEY`
     - Example: If the following is a description in the listener.ora LISTENER=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=ORCL)))) then unix_domain_socket_marker=ORCL
     - Example: If there is more than one IPC line in listener.ora, use a common denominator of all the keys:

       ```
       su - grid -c 'cat $ORACLE_HOME/network/admin/*.ora'|grep -i KEY
       LISTENER=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=LISTENER))))
       LISTENER_SCAN1=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=LISTENER_SCAN1))))
       LISTENER_SCAN2=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=LISTENER_SCAN2))))
       LISTENER_SCAN3=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=LISTENER_SCAN3))))
       ```

       Guardium uses a string search in the path. "LISTENER" works for all four and should be used in this case: unix_domain_socket_marker=LISTENER
     - Example: If there is no common denominator, create additional inspection engines with unix_domain_socket_marker corresponding to the specific IPC key(s). For example the guard_tap.ini may look similar to this example in the end:

       ```
       [DB_0]
       ...
       unix_domain_socket_marker=EXTPROC1522
       ...
       [DB_1]
       ...
       unix_domain_socket_marker=LISTENER
       ```

3. If the Oracle database is encrypted (ASO/SSL), activate ATAP on all nodes (active and standby).
   a. Stop all Oracle services (including clusterware) and verify that ohasd.bin is down.
      i. Run `crsctl stop cluster -all`
      ii. Verify that `ohasd.bin` is down
   b. Authorize user oracle and grid (in case listener belongs to user grid).
   c. Configure A-TAP parameters.
   d. Activate A-TAP.
   e. Start all Oracle services in the cluster.
4. In Oracle RAC environment, verify which user starts the listener. If it is with user grid, authorize the user grid.

Parent topic: Linux and UNIX systems: Special environments configuration
Related reference:
Linux and UNIX systems: guardctl utility commands for A-TAP
Linux and UNIX systems: Database-specific guardctl parameters

Linux and UNIX systems: Configure S-TAP for DB2 WPAR

About this task

When ktap_fast_shmem set to 1, if there are multiple DB2 instances that are configured for a single WPAR in guard_tap.ini file and they have the same db2_shmem_size, then the db2_fix_pack_adjustment and db2_shmem_client_position are taken from the first DB2 section for that WPAR. So in cases where there are multiple DB2 instances running on the WPAR:

- If all DB2 instances have the same db2_shmem_size, db2_fix_pack_adjustment, and db2_shmem_client_position, the packets from all instances are collected even if only one instance is configured.
- If all DB2 instances have the same db2_shmem_size, but different db2_fix_pack_adjustment or db2_shmem_client_position, then only packets from the first configured DB2 instance are collected.

Procedure

1. Compute the client I/O area offsest (db2_shmem_client_position)
   a. Open a new bash shell as the db2 instance user.
   b. Run the ps -x command to verify that the db2bp command processor is not currently running for this shell. You should not see a command called db2bp running. If it does, either kill it or run a new shell.
   c. Run the following two commands:

```
db2 get database manager configuration | awk '/ASLHEAPSZ/{print $9 * 4096}'
```

   The output is the required value for db2_shmem_client_position
2. To find the DB2 shared memory segment size (db2_shmem_size), perform one of:
   - This method gives the most accurate results.
     a. Start a DB2 shared memory connection and keep it open.
     b. Run this command to get the process ID for db2sysc: ps -eaf | grep db2sysc. The output looks like:

```
db2inst1  5309370  5505772   0   Nov 11      - 1232:12 db2sysc 0
```

     In this example, the process ID is 5309370.
     c. Run this command to retrieve information about shared-memory processes: ipcs -ma. The output looks like:

```
IPC status from /dev/mem as of Wed Nov 20 13:21:45 CST 2013
T         ID     KEY        MODE       OWNER    GROUP  CREATOR   CGROUP NATTCH     SEGSZ  CPID
m    2097152 0xffffffff D-rw------- pconsole   system pconsole   system      1 536870912 4522088
m          1 0x78000015 --rw-rw-rw-     root   system     root   system      3  16777216 3605314
m          2 0x78000016 --rw-rw-rw-     root   system     root   system      3 268435456 3605314
m  219152387 0xffffffff D-rw-------     root   system     root   system      1 536870912 5243842
m    1048580 0x61013002 --rw------- pconsole   system pconsole   system      1  10485760 4522088
m   10485765 0xd9fd8a61 --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      5  47644672 5571082
m    9437190 0xd9fd8a74 --rw-rw-rw- db2inst1 db2iadm1 db2inst1 db2iadm1      9 140852104 5571082
m    9437191 0xe1bd8858 --rw-rw----   oracle      dba   oracle      dba     40 53687107584 3801352
m    3145736 0x52594801 --rw-rw----     root informix     root informix     13 223019008 5702650
m    3145737 0xd9fd8b68 --rw-rw---- db2inst1 db2iadm1 db2inst1 db2iadm1      1  58720256 6619354
m    3145738 0xffffffff --rw------- db2fenc1 db2fadm1 db2inst1 db2iadm1      7 268435456 5505772
m         11 0x52594802 --rw-rw----     root informix     root informix     13  33439744 5702650
m         12 0x52594803 --rw-rw-rw-     root informix     root informix     13    573440 5702650
m         13 0xf2033f7e --rw------- sybase15   sybase sybase15   sybase      1 115564544 5178168
m  409993231 0x52594804 --rw-rw---- informix informix informix informix     13   8388608 5702650
m  763363344 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 268435456 5309370
m  125829140 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      2    131072 5309370
m  201326613 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 163905536 5309370
m  103750230 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 134217280 5309370
```

     The output contains several columns beyond those shown here, but they do not affect this procedure. Find the line that contains the process ID that was identified in step 2.b and also has a value of 2 under NATTCH. The DB2 shared-memory segment size is the value in the SEGSZ column. In this example, it is 131072.
     d. Tip: if the list returned in step 2.c is too long, you can filter it by using the process ID. In this case, you would enter ipcs -ma | grep 5309370. The results do not contain the column headers, but you can look at the previous results to see the column headers and identify the correct line and column. In this example, it is the last line.

```
m  131072014 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 1342177280 5309370
m  763363344 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 268435456 5309370
m  227541013 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 163905536 5309370
m  106353238 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      2    131072 5309370
```

   - Alternatively, use this method, which is easier but less accurate:
     ATAP and KTAP rely on the size for identification of the Application/Agent shared memory segments. These segments are then tapped for C2S and S2C packets. The segments are equal to the sum of the ASLHEAPSZ and RQRIOBLK parameters. DB2® allocates much larger segments. In most cases, the size is equal to (ASLHEAPSZ + 1) * 2 pages, or (ASLHEAPSZ + 1) * 8192 bytes. Exact size can be determined by observation of the shared memory segments in the system before and after new DB2 local connection is created. Use this sequence of commands to determine the shared memory segment size. ipcs command parameters and output format differ from platform to platform. The following script is based on the AIX® version.

```
ipcs -ma | sort -n -2 +3 > /tmp/before.txt
db2 connect to <some_existing_database>ipcs -ma | sort -n -2 +3 > /tmp/after.txt
db2 terminate
diff /tmp/before.txt /tmp/after.txt | awk '{if ($10 == 2) print $11}'
```

3. Set these parameters in order to capture the DB2 shared memory traffic.

Table 1. DB2 Parameters

Parameter	STAP Name	ATAP Name
Packet header size	db2_fixed_pack_adjustment	db2_header_offset
Client I/O area offset	db2_shmem_client_position	db2_c2soffset
DB2 shared memory segment size	db2_shmem_size	db2_shmsize

Parent topic: Linux and UNIX systems: Special environments configuration

Linux and UNIX systems: Activate A-TAP on all nodes of a DB2 Cluster

A-TAP needs to be activated on all nodes where a DB2 server is shared by nodes on a DB2 cluster.

Procedure

1. Authorize db2 user on node 1. <guardium_base>/xxx/guardctl authorize-user <user-name>
   For example:

   ```
   # /usr/local/guardium/bin/guardctl authorize-user db2inst1

   # /usr/local/guardium/bin/guardctl is_user_authorized db2inst1
   ```

   User 'db2inst1' is authorized.

2. Activate A-TAP on node 1.
   <guardium_base>/xxx/guardctl db_instance=<instance> activate
   For example:

   ```
   # /usr/local/guardium/guard_stap/guardctl db_instance=db2inst1 activate

   # /usr/local/guardium/guard_stap/guardctl list-active
   db2inst1
   ```

3. Restore the original DB2 server on node 1 after activating ATAP on it, so that other nodes can activate ATAP. (All nodes share the executable.(In the db2 adm directory, copy db2sysc-guard-original over db2sysc (make a copy of each first and set them aside). For example:
   `# > cp db2sysc-guard-original db2sysc`
4. Delete db2sysc-guard-original (or it will fail activation on node 2). For example:
   `# rm -rf db2sysc-guard-original`
5. Move cluster resources to node 2. For example:
   `# pcs resource move resource_id <destination node>`
6. Authorize db2 user and activate on node 2 (steps 1 and 2). This will create the libraries on node 2 and replace the db2sysc-guard-original that has been deleted.
   The current status should be:
   Node01:

   ```
   # /usr/local/guardium/guard_stap/guardctl list-active

   db2inst1
   ```

   Node02:

   ```
   # /usr/local/guardium/guard_stap/guardctl list-active

   db2inst1
   ```

Parent topic: Linux and UNIX systems: Special environments configuration

Linux and UNIX systems: Configure delayed cluster disk mounting

This topic applies for Oracle, Informix® and DB2® database servers only.

For these database types, when the S-TAP starts it must have access to the database home. If your environment uses a clustering scheme in which multiple nodes share a single disk that is mounted on the active node, but not on the passive node, the database home is not available on the passive node until failover occurs.

S-TAP can be configured for delayed loading by setting a configuration file property, WAIT_FOR_DB_EXEC. When starting, if S-TAP finds that there is no access to the database home, it checks the WAIT_FOR_DB_EXEC value, and takes the appropriate action.

- WAIT_FOR_DB_EXEC > 0, S-TAP starts regardless of whether or not it can stat() process name. It tries to stat() process name every 15 minutes
- WAIT_FOR_DB_EXEC < = 0 S-TAP tries to stat() process name in inspection engine immediately after it comes up. If it cannot stat() process name, S-TAP exits.

Before setting this property to a positive value, be sure to set all other necessary configuration properties and test that the S-TAP starts and collects data correctly. This property can be set only by editing the configuration file, and not from the GUI.
Parent topic: Linux and UNIX systems: Special environments configuration

Linux and UNIX systems: Uninstalling an S-TAP

Perform this procedure before installing a new version of S-TAP® if you want to save the old configuration file.

About this task

If S-TAP was previously installed, there is a directory named: /usr/local/guardium/guard_stap.

If you have installed A-TAP, you must deactivate it before attempting any upgrade/install operations; see the description of the A-TAP deactivation command, in Linux and UNIX systems: Deactivating A-TAP.

If you are removing a previous version of S-TAP that used K-TAP, you will need to reboot the database server. If K-TAP has been installed, you will have a device file named: /dev/guard_ktap.

Procedure

1. Log on to the database server system using the root account.
2. Optionally, copy the S-TAP configuration file to a safe location (a non-Guardium directory). By default, the full path name is: /usr/local/guardium/guard_stap/guard_tap.ini You can use this file later if you have to re-install this version of the software, or you can refer to it when configuring an updated version of S-TAP. Do not ever use an older configuration file directly with a newer version of the software - newer properties may be missing, and the defaults taken may result in unexpected behavior when you start S-TAP.
3. Run the uninstall script. For example, if the default directory has been used: `[root@yourserver ~]# /usr/local/guardium/guard_stap/uninstall`
4. If your previous version of S-TAP included K-TAP, reboot the database server now.

a. Run the uninstall script again

5. This step applies to AIX® WPARs and Solaris Zones only (skip for all others). If you are uninstalling a previous version of S-TAP that included K-TAP, issue the following commands from the master node: rm -f /wpars/<server>/dev/ktap* and rm -f /wpars/<server>/dev/guard_ktap*, where /wpars/<server> is the path from the master node to the WPAR.

Parent topic: Linux and UNIX systems: S-TAP user's guide

Linux and UNIX systems: Upgrading S-TAP and K-TAP

Upgrade S-TAP to continue capturing data from pre-existing sessions, and maintain its configuration, without reboot. You can also upgrade K-TAP as part of the S-TAP upgrade.

About this task

- Before upgrading S-TAP, upgrade the Guardium system that serves as the S-TAP host.
- If you are removing a previous version of S-TAP® that used K-TAP, you will need to reboot the database server.
- If K-TAP has been installed, you will have a device file named: /dev/guard_ktap

Procedure

1. Log on to the database server system using the root account.
2. If the system has A-TAP and the encryption box is not used:
   a. Stop the database.
   b. User guardctl to deactivate the A-TAP.
3. If the system has A-TAP and the encryption box is used, stop the DB. (ATAP is active whenever the DB is running. Once the encryption box has been set to activate ATAP automatically, it cannot be disabled by simply unchecking the box. The system needs to be rebooted with the feature disabled in order to clear the setting.)
4. Before running live update, either through GIM or shell installers, make sure no process except the S-TAP is using the K-TAP device. The S-TAP must be running and A-Tap must be deactivated. Run fuser /dev/ktap_xxx or lsof | grep ktap_xxx (where xxx is the old version number) to see if any process is holding the device open. Failure to do so can result in unpredictable behavior.
5. If un-installing version 6.0 or later of S-TAP:
   a. For Red Hat Enterprise Linux 6: Stop S-TAP using the stop utap command.
   b. For Red Hat Enterprise Linux 7: Stop S-TAP using the systemctl stop guard_utap command
   c. All others:
      i. Remove the utap agent entry in the /etc/inittab file (regardless of whether or not it has been commented). In a default installation, this statement should look like this: utap:<nnnn>:respawn:/usr/local/guardium/guard_stap/guard_stap /usr/local/guardium/guard_stap/guard_tap.ini
      ii. Save the /etc/inittab file.
      iii. Run the init q command
   d. Run ps - ef | grep stap to verify that S-TAP is no longer running.
6. Copy the S-TAP configuration file to a safe location (a non-Guardium directory).
7. Run the uninstall script. For example, using the default directory: [root@yourserver ~]# /usr/local/guardium/guard_stap/uninstall
   Note: Do not run the uninstall program with S-TAP running. Be sure that you have stopped S-TAP.
8. If your previous version of S-TAP included K-TAP, reboot the database server now.
9. HP-UX servers only (skip for all others): If you are uninstalling a previous version of S-TAP that included K-TAP, run the uninstall script again after reboot.
10. AIX WPARs only (skip for all others): If you are uninstalling a previous version of S-TAP that included K-TAP, issue the following commands from the master node after uninstall: rm -f /wpars/<server>/dev/ktap* and rm -f /wpars/<server>/dev/guard_ktap*, where /wpars/<server> is the path from the master node to the WPAR.
11. Upgrade the S-TAP, using one of
    - Windows: Installing S-TAP agent with GIM (v10.1-10.1.3), or Linux and UNIX systems: Installing the S-TAP client with GIM (v10.1.4) using the Upgrade option at the end of the procedure.
      - If you are upgrading K-TAP, set KTAP_LIVE_UPDATE to yes. Modify other parameters as relevant. Parameters you leave unchanged are carried over in the upgrade.
    - Linux and UNIX systems: Installing and updating S-TAP using RPM, using the -u flag and other relevant upgrade parameters listed in the Linux and UNIX systems: S-TAP install script parameters. To upgrade K-TAP, specify --live_update Y
    - Linux and UNIX systems: Installing the S-TAP client using the shell installer
12. After a K-TAP live upgrade:
    - The first SQL for an existing session after updating K-TAP is not captured.
    - Existing A-TAP sessions on Solaris local zone are not logged.
    - Some processes may still reference memory in the old K-TAP module. Under this scenario, the module refuses to free the resources to prevent future instability. When this happens, the user should, after those resources are no longer being used, try a manual cleanup by running the guard_ktap_cleanup that is kept in the ktap directory.
    - On HP-UX 11.11, the old K-TAP module is no longer installed, but it still shows up as registered when you execute kmadmin -s | grep tap. Manually unregister this module with kmmodreg -U ktap_<version>.
    - On Solaris and AIX®, the old dev-nodes are not automatically deleted after a reboot and they need to be removed manually.

    Exceptions:
    - If the DB server is installed with a version that was not installed through GIM, and the non-GIM K-TAP version is not the same with installing K-TAP version, the value of the KTAP_LIVE_UPDATE is ignored, since an upgrade from a non-GIM version requires system reboot
    - When upgrading from a non-GIM version to the same GIM version, the system does not need to be rebooted.
    - You can NOT reinstall a previously installed K-TAP version without rebooting the machine.

    Error Handling:
    - In the event of a failure, it is extremely important to check the GIM Events List report, since some failures require system reboot in order to fully recover.

Note: K-TAP for AIX only fails to load during an S-TAP installation or upgrade if the ODMDIR environment is not defined. ODMDIR is Object Data Manager Directory. ODM is a database of system and device configuration information integrated into the OS. It is intended for storing system information, software information, and device information. All ODM commands use the ODMDIR environment variable, that is set in the file /etc/environment. The default value of ODMDIR is /etc/objrepos.

Parent topic: Linux and UNIX systems: S-TAP user's guide
Related reference:
Linux and UNIX systems: guardctl utility commands for A-TAP

Linux and UNIX systems: Configuring S-TAP

- Linux and UNIX systems: Configure S-TAP from the GUI
  View all S-TAPs managed by this Guardium system, manage individual STAPs, and perform a few operations on all STAPs.
- Linux and UNIX systems: Discover database instances
  Enable S-TAP to periodically discover database instances and send the results to the current active S-TAP system.
- Linux and UNIX systems: Configuring an Inspection Engine
  Configure or modify an inspection engine in the S-TAP Control pane.
- Linux and UNIX systems: Inspection engine verification
  S-TAP verification confirms that the STAPs and their inspection engines in your environment are running and actively monitoring database activity. Understand verification, and define a schedule to regularly verify S-TAPs.
- Linux and UNIX systems: S-TAP Load Balancing models and configuration guidelines
  Understand the S-TAP load balancing models, and choose the one appropriate to your setup
- Linux and UNIX systems: Set up S-TAP authentication with SSL certificates
  Set up authentication between an S-TAP server and Guardium system.
- Linux and UNIX systems: Increasing S-TAP throughput
  You can configure an S-TAP that reports to multiple Guardium systems to increase the throughput of data.
- Linux and UNIX systems: Kerberos-authenticated database traffic
  Kerberos is a network authentication protocol that eliminates the transmission of unencrypted passwords across the network. Learn how it functions in Guardium .
- Linux and UNIX systems: A-TAP management
  A-TAP is an application-level tap. A-TAP sits in the application layer to support monitoring of encrypted database traffic, which cannot be done in the kernel by K-TAP.
- Linux and UNIX systems: Using Exit libraries
  Exit libraries embed a Guardium library into the database, using the exit mechanism. The exit library, or module, communicates directly with the Guardium S-TAP to forward database traffic.
- Linux and UNIX systems: Editing the S-TAP configuration parameters
  You can modify the S-TAP configuration after it is installed using GIM, the GUI, or for advanced users, in the configuration file on the database.

Parent topic: Linux and UNIX systems: S-TAP user's guide

Linux and UNIX systems: Configure S-TAP from the GUI

View all S-TAPs managed by this Guardium system, manage individual STAPs, and perform a few operations on all STAPs.

About this task

Prerequisite: You must be logged in to the Guardium system that is the active host for the S-TAP.

Some configuration changes require that the S-TAP agent be restarted manually, as indicated in the parameter descriptions.

Sometimes a user is unable to make a decision during the process of installing an S-TAP or may make the wrong decision and it goes undetected until after the installation process is complete. For instance a user may forget to type in or use the wrong IP address when defining a SQL Guard IP. These types of mistakes can be remedied by modifying the S-TAP configurations.

Parameters in the GUI may be safely changed. Parameters that are not in the GUI rarely need changing and should normally be left unmodified; they are for use by Guardium Technical Support or advanced users.

If you have installed your S-TAP by using the Guardium Installation Manager (GIM), you can update some parameters through the GIM GUI or API.

Procedure

1. Click Manage > Activity Monitoring > S-TAP Control to open S-TAP Control.
2. Perform operations on all S-TAPs in the page.
   - Refresh: refresh display of S-TAPs.
   - Add All to Schedule: add all displayed S-TAPs to the S-TAP verification schedule.
   - Remove All from Schedule: remove all displayed S-TAPs from the S-TAP verification schedule.
   - Comments: add comments. See Comments
3. Identify the S-TAP to be configured by its IP address or the symbolic host name of the database server on which it is installed. View and perform operations on individual S-TAPs.

Option	Description
Delete:	Click Delete to remove an S-TAP. Deleting S-TAPs is useful to clean up your display when you know that an S-TAP has become inactive, or when the Guardium unit is no longer listed as a host in the S-TAP's configuration file. In either of these cases, the S-TAP displays indefinitely with an offline status if you do not delete it. You cannot remove an active S-TAP from the list. Clicking delete does not stop an S-TAP from sending information, nor does it remove the Guardium host from the list of hosts stored in the S-TAP's configuration file.

Option	Description
Refresh:	Click Refresh to fetch a copy of the latest S-TAP configuration from the agent. (There is no auto-refresh of the S-TAP display.)
Send Command:	Opens the S-TAP Commands popup, where you can run various commands on the S-TAP host. ○ Restart: Restarts the S-TAP. Not usually needed, and if yes, it's easier to simply kill it from the database server. ○ S-TAP logging ○ Reinitialize buffer: reset the K-TAP statistics along with deleting the S-TAP buffer ○ KTAP logging: Similar to S-TAP Logging; increases the debug output from KTAP ○ Run Diagnostics: Run the S-TAP diagnostics script (and upload the results to the Guardium system) ○ Upload Linux Modules: Linux only. Uploads the local custom build module of K-TAP. ○ Record Replay Log: Records all data to a file on DB server (RECORD) and sends data to collector (REPLAY) ○ Revoke Ignore: All sessions ignored by a revokable ignore policy will be un-ignored and start capturing the traffic again for those sessions ○ Run Database Instance Discovery: Runs the discovery process, once immediately. (If enabled to run automatically, it runs, by default, every 24 hours.)
Edit S-TAP configuration:	Opens the S-TAP configuration window. Parameters that do not appear in the GUI are advanced parameters. Do not modify them if you are not an advanced user, or have not been instructed to modify them by Guardium Technical Support. See GUI parameters: ○ Linux and UNIX systems: General parameters ○ Linux and UNIX systems: Configuration Auditing System (CAS) parameters ○ Linux and UNIX systems: Application server parameters ○ Linux and UNIX systems: Guardium Hosts (SQLGuard) parameters ○ Linux and UNIX systems: Inspection engine parameters
Show S-TAP Event Log:	Click to open the S-TAP event log, where you can see events such as connect, disconnect, GIM server configuration, and so on. This log is very useful for troubleshooting.
Add to Schedule checkbox	Adds the individual S-TAP to the scheduled verification.
Revoke All Ignored Sessions checkbox	A database could be running many sessions, some of which are currently ignored. Clear this option to stop ignoring traffic from that server.

Parent topic: Linux and UNIX systems: Configuring S-TAP

Linux and UNIX systems: Discover database instances

Enable S-TAP to periodically discover database instances and send the results to the current active S-TAP system.

The Guardium Discovery Agent is a software agent automatically installed with the S-TAP package on a database server. The instance discovery agent reports database instances, listener, and port information to the Guardium system. Discovery does not find and report on every detail of the DB instances on the server.

Auto-discovery is enabled by default. Configure it with the parameter discovery_interval.

Database types supported by S-TAP Discovery
Oracle, DB2, Informix, MySQL, PostgreSGL, Enterprise PostgreSQL, Sybase, Hadoop, Teradata, Netezza, MemSQL.

The discovery bundle is not installed in a slave zone or WPAR; the discovery agent running on the global zone collects information from other zones.
Note: On Solaris zones architecture, when DB2® instances are running on slave zones, Discovery does not discover the DB2 shared memory parameters.

Newly discovered database instances can be seen in the Discovered Instances report. From this report, datasources and inspection engines can quickly be added to Guardium using the Actions menu.

If databases on the database server are not operational (started) or are added later, the Discovery Agent can still discover these instances by running the Run Discovery Agent command from the STAP Control window (Manage > Activity Monitoring > S-TAP Control. Click , and select Run Database Instance Discovery).

S-TAP Discovery can be run manually but this action is not suggested. The main reason to run it manually is for debugging purposes. If a new request comes in from the user interface while a scheduled discovery is running, the new request is ignored.

You can run Discovery from a local command line on the database server (/usr/local/guardium/guard_stap/guard_discovery), in one of three ways:

- with the --update-tap flag: edits the guard_tap.ini to add or update inspection engines
- with the --send-to-sqlguard flag (or with no flag, this is the default): sends the found changes to the Guardium system, where they appear in the Discovered Instances report
- with the --print-output flag: prints the found changes to stdout (for debugging)

If the S-TAP running as "user" (and not guardium), the discovery functionality is limited. The following message displays:

```
WARNING: Discovery is enabled and STAP is running as user guardium.
The discovery function is limited when STAP runs as user guardium.
Discovery is most effective when 'tap_run_as_root=1'
```

Note: S-TAP Discovery is not supported on AIX 5.3 because of static libraries are needed on that platform.
Note: In order to avoid an instance where S-TAP discovery does not open the Informix database, it is recommended to start Informix databases using the full path to the executable.

The S-TAP Discovery application parameters should be left at their default values, except for advanced users. Discovery application are described in Linux and UNIX systems: Discovery parameters.

Discovery also uses these parameters:

- tap_ip: the S-TAP with which the database instance is associated.

- sqlguard_ip: S-TAP discovery results are sent to this IP. (The Guardium system with primary=1 in the SQLguard parameters.)

Parent topic: Linux and UNIX systems: Configuring S-TAP

Linux and UNIX systems: Configuring an Inspection Engine

Configure or modify an inspection engine in the S-TAP Control pane.

Before you begin

You must be logged in to the Guardium system that manages the S-TAP.

About this task

Do not configure an S-TAP inspection engine to monitor network traffic that is also monitored directly by a Guardium system that is hosting the S-TAP, or by another S-TAP reporting to the same Guardium system. That would cause the Guardium system to receive duplicate information: it would not be able to reconstruct sessions, and would ignore that traffic.

Procedure

1. Navigate to Manage > Activity Monitoring > S-TAP Control.
2. In the row of the S-TAP, click . The S-TAP Configuration window opens.
3. Scroll to the bottom of the inspection engines, and click next to Add Inspection Engine....
4. Select the protocol and enter the port range. The window refreshes with the relevant parameters, some with their default values.
5. Configure all required parameters, and click Add. If you are missing parameters, the system informs you what is missing.

Parent topic: Linux and UNIX systems: Configuring S-TAP
Related reference:
Linux and UNIX systems: Inspection engine parameters

Linux and UNIX systems: Inspection engine verification

S-TAP verification confirms that the STAPs and their inspection engines in your environment are running and actively monitoring database activity. Understand verification, and define a schedule to regularly verify S-TAPs.

Verification checks sniffer operation and communication between the Guardium system and the inspection engines. You can enable verification for all S-TAP clients on your system, or individual S-TAP clients, or individual inspection engines.

Verification is supported for these database types:

- DB2 and DB2 Exit
- Greenplum
- Informix
- MSSQL (for cluster configuration supports only advanced verification)
- MySQL
- Netezza
- Oracle
- PostgreSQL
- Teradata (advanced verification only)

There are two types of verification:

Standard verification
: Checks the sniffer operation, and the communication between the S-TAP and the inspection engine. It submits invalid login request and verifies that the appropriate error message is returned.

Advanced verification
: Use advanced verification to avoid failed login requests, and manage individual IEs. For avoiding failed login requests, you must identify or create a datasource definition associated with the target database. The datasource definition includes credentials, which the verification process uses to log in to the database. Then it submits a request to retrieve data from a nonexistent table in order to generate an error message.

For both types of verification requests, the results are displayed in a new dialog that provides information about the tests that were performed and recommended actions for tests that failed.

- Linux and UNIX systems: S-TAP verification
  The S-TAP verification process checks several configuration parameters and attempts to connect to the inspection engines.
- Linux and UNIX systems: Configure standard verification
  Use this task to configure all inspection engines on a specific S-TAP client host.
- Linux and UNIX systems: Configure advanced verification
  Use this task to configure all inspection engines on a specific S-TAP client host, and to configure advanced verification.
- Linux and UNIX systems: Configuring the S-TAP verification schedule
  The default schedule for verifying S-TAPs is once per hour, every day. You can change this schedule.

Parent topic: Linux and UNIX systems: Configuring S-TAP

Linux and UNIX systems: S-TAP verification

The S-TAP verification process checks several configuration parameters and attempts to connect to the inspection engines.

Before connecting to the database, the verification process checks whether the sniffer process is running on the Guardium system. The sniffer is responsible for communicating with each S-TAP and processing the data that is received. If the sniffer is not running, responses from the S-TAP are not recognized.

The verification process attempts to log in to your database's STAP client with an erroneous user ID and password, to verify that this attempt is recognized and communicated to the Guardium system.

Next the verification process checks whether it can connect to the selected inspection engine on the database server. It expects to receive a response that indicates a failed login. If a different response is received, you might have to investigate further.

Some error messages from individual databases do not indicate a specific problem. For example, on several supported databases, the error code returned for a wrong port can also mean that the database itself is not started.

View the verification results in the S-TAP Verification page (Manage > Reports > Activity Monitoring > S-TAP Verification page). Failed checks are shown first, with recommendations for next steps. Checks that succeeded are shown in a collapsed section at the end of the list. In some situations, it might be useful to review the successful checks in order to choose among possible next steps.

Parent topic: Linux and UNIX systems: Inspection engine verification

Linux and UNIX systems: Configure standard verification

Use this task to configure all inspection engines on a specific S-TAP client host.

About this task

As an alternative to this procedure, you can use the GRDAPI command verify_stap_inspection_engine_with_sequence.

Procedure

1. Access Manage > Activity Monitoring > S-TAP Control.
2. Use these options:
   - Add All to Schedule: add all inspection engines for all displayed S-TAPs to verification.
   - Remove All from Schedule: remove all inspection engines for all displayed S-TAPs from verification.
   - Add to Schedule: add all inspection engines of the selected S-TAP client to the schedule.

   If an S-TAP does not have the option All Can Control enabled, you can only change its status if your Guardium system is the primary system for this S-TAP.
3. Click Refresh.
4. To verify now, go to Manage > Activity Monitoring > S-TAP Verification Scheduler and click Run Once Now.

Parent topic: Linux and UNIX systems: Inspection engine verification

Linux and UNIX systems: Configure advanced verification

Use this task to configure all inspection engines on a specific S-TAP client host, and to configure advanced verification.

Before you begin

Use this task to configure verification on individual inspection engines, including advanced verification.

About this task

Procedure

1. Access Manage > System View > S-TAP Status Monitor.
2. Click anywhere in the row of the S-TAP.
   The window refreshes with the individual inspection engines of this host.
3. To verify now, select one or more inspection engines and click Verify.
4. Configure advanced verification.
   a. Click one inspection engine, and click Advanced Verify.
   b. Optionally, under Datasource, select Show only matching S-TAP host or select a name from the Name drop-down list to search for a specific inspection engine.
   c. Click Close.
5. To add to or remove from verification.
   a. Select one or more inspection engines.
   b. Click Add to Schedule or Remove from Schedule

Parent topic: Linux and UNIX systems: Inspection engine verification

Linux and UNIX systems: Configuring the S-TAP verification schedule

The default schedule for verifying S-TAPs is once per hour, every day. You can change this schedule.

About this task

The same schedule is used for all S-TAPs that are scheduled for verification.

Once a schedule is defined, you can click the Pause button to temporarily stop the verification process while keeping it active. Use the Run Once Now button to run the verification once in real-time.

Procedure

1. Click Manage > Activity Monitoring > S-TAP Verification Scheduler to open the S-TAP Verification Scheduler.
2. In the S-TAP Verification Scheduler portion of the page, click Modify Schedule.
3. In the Schedule Definition dialog, use the drop-down lists and check boxes to schedule when verification runs. This schedule is applied to all S-TAPs that are scheduled for verification.
4. Click Save to save your changes.

Parent topic: Linux and UNIX systems: Inspection engine verification

Linux and UNIX systems: S-TAP Load Balancing models and configuration guidelines

Understand the S-TAP load balancing models, and choose the one appropriate to your setup

Each load balancing model is described here, along with its specific parameter requirements.

Failover

S-TAP sends traffic to one collector (primary) and fails over to one or more collectors (secondary, thirdly, and so on) as needed. The S-TAP agents are configured with a primary and at least one secondary collector IP. If the S-TAP agent cannot send the traffic to the primary collector for various reasons, the S-TAP agent automatically fails over to the secondary. It continues to send data to the secondary host until either the secondary host system becomes unavailable, or the primary host becomes available again. In the first case, it fails over to the tertiary if there is one defined. In the second case S-TAP fails over from the secondary Guardium host back to the Primary Guardium host. You can configure as many failover collectors as you want, although there is no reason to define more than 3. You can either define one collector as a standby failover collector only, or a few failover collectors. When using one standby failover, one collector is usually sufficient for 4-5 collectors. When using a few failover collectors, each one should run at a maximum 50% capacity, so that there are always resources for additional load. Choose the setup that works best with your architecture, database, and data center layout.

The S-TAP restarts each time configuration changes are applied from the active host.

In the S-TAP Control window, Details section: set Load Balancing to 0; In the Guardium Hosts section: add at least one secondary sqlguard_ip.

Additional failover configuration should be left at the default values, except by advanced users.

Before designating a Guardium system as a secondary host for an S-TAP, verify these items.

- The Guardium system must be configured to manage S-TAPs. To check this and re-configure if necessary, see Configure Guardium system to Manage Agents.
- The Guardium system must have connectivity to the database server where S-TAP is installed. When multiple Guardium systems are used, they are often attached to disjointed branches of the network.
- The Guardium system must not have a security policy that will ignore session data from the database server where S-TAP is installed. In many cases, a Guardium® security policy is built to focus on a narrow subset of the observable database traffic, ignoring all other sessions. Either make sure that the secondary host will not ignore session data from S-TAP or modify the security policy on the Guardium system as necessary.

Load balancing

This configuration balances traffic from one database onto multiple collectors. This option might be good when you must monitor all traffic (comprehensive monitoring) of an active database. (Note that for outliers detection, the collectors need to be under the same aggregator and central manager in order for the aggregator to process all related data.) When the generated traffic is large and you need to house the data online on a collector for an extended period, this method might be your best choice because it performs session-based load balancing across multiple collectors. An S-TAP can be configured in this manner with up to 10 collectors.

Set participate_in_load_balancing to 1 for load balancing.

Grid

With Grid, the S-TAP communicates to the collector through a load balancer, such as f5 and Cisco. The S-TAP agent is configured to send traffic to the load balancer. The load balancer forwards the S-TAP traffic to one of the collectors in the pool of collectors. You also can configure failover between load balancers for continuous monitoring if the load balancer should fail.

Set participate_in_load_balancing to 3 for the grid model.

Redundancy

In redundancy, the S-TAP communicates its entire payload to multiple collectors. The S-TAP is configured with more than one collector (often only two) and communicates the identical content to both. This option provides full redundancy of the same logged data across multiple collectors. It can also be used for logging data and alert on activity at different levels of granularity.

Set participate_in_load_balancing to 2 for redundancy.

Multiple K-TAP buffers

This mode utilizes extra threads and K-TAP buffers to increase throughput. Set participate_in_load_balancing to 4. See Linux and UNIX systems: Increasing S-TAP throughput

Parent topic: Linux and UNIX systems: Configuring S-TAP

Linux and UNIX systems: Set up S-TAP authentication with SSL certificates

Set up authentication between an S-TAP server and Guardium system.

S-TAPs can be configured to only connect to a certain group of machine(s) that authenticate with a given certificate or set of certificates. These certificates can either be generated locally on the Guardium system and sent off to the Certificate Authority (CA) for signing or can be created at the CA and installed whole on the Guardium system.

- Linux and UNIX systems: Generating certificate signing request (CSR) on Guardium system
  Use this procedure to generate a certificate signing request locally on the Guardium system, for sending to the Certificate Authority (CA) for signing.
- Linux and UNIX systems: Installing an SSL certificate generated outside of the Guardium system
  Use this procedure to install the SSL certificate that was created by the CA.

- Linux and UNIX systems: Configuring the S-TAP to use x.509 certificate authentication

Parent topic: Linux and UNIX systems: Configuring S-TAP

Linux and UNIX systems: Generating certificate signing request (CSR) on Guardium system

Use this procedure to generate a certificate signing request locally on the Guardium system, for sending to the Certificate Authority (CA) for signing.

Procedure

1. Log into your Guardium system with CLI.
2. Enter: cli> create csr sniffer
3. Enter the requested data.

```
temp4> create system csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:CA
State or Province Name (full name) [Berkshire]:BC
Locality Name (eg, city) [Newbury]:
Organization Name (eg, company) [My Company Ltd]:QA_Sample1
Organizational Unit Name (eg, section) []:Sample_QA
Common Name (eg, your name or your server's hostname) []:sample1_qa.victoria
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
```

When you've finished, it looks like:

```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=CA, ST=BC, L=Newbury, O=QA_Sample1, OU=Sample_QA, CN=sample1_
qa.victoria
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:e9:5e:a2:81:53:dc:e9:b5:f7:54:33:17:6f:15:
                    9c:00:5c:ff:b2:64:c6:e5:48:be:36:a7:a4:55:f4:
                    b1:df:c9:81:a4:41:fe:29:80:d6:fd:d4:c4:b5:97:
                    b7:c1:3d:42:6c:c0:f8:09:cd:ea:36:f6:3b:b9:d9:
                    ce:15:87:2d:2f:b3:f2:5f:f9:42:06:e2:a0:62:56:
                    06:6d:cc:65:69:62:db:36:34:09:95:5b:c3:d0:e6:
                    85:ee:64:76:3e:ed:d6:47:bb:49:f2:08:81:14:c2:
                    e3:93:db:20:ba:86:e7:60:24:80:01:7f:3d:b7:60:
                    16:ba:06:d4:a1:e0:18:39:73:ca:1e:24:15:56:6d:
                    97:79:81:04:f7:fd:37:06:42:d7:15:82:34:aa:51:
                    2c:cc:e2:f0:d1:42:dd:b5:71:bb:10:19:a0:0a:5c:
                    4f:77:b9:bb:36:95:ed:a4:77:07:e3:50:f9:36:20:
                    13:e2:e1:78:d2:0a:36:8a:b9:39:90:1f:a4:82:12:
                    4f:50:29:3f:19:7d:16:a6:b3:23:7b:b8:7b:85:60:
                    04:21:39:84:1d:9e:81:e5:20:2c:8a:51:f3:52:f7:
                    3c:4f:e6:f2:a5:88:dc:2e:99:0a:b3:65:1e:bf:33:
                    5f:be:dc:53:1c:a6:69:18:c4:c7:75:bf:20:e3:cf:
                    29:af
                Exponent: 65537 (0x10001)
        Attributes:
            challengePassword        :guardium
    Signature Algorithm: sha1WithRSAEncryption
        06:4a:b9:db:04:a1:8d:4c:f7:3f:8f:24:fa:7c:ec:a6:70:77:
        8b:b9:38:7c:b6:e6:51:aa:ed:96:20:16:37:85:a7:44:26:2b:
        87:4c:a4:db:0c:f3:d3:87:e3:68:4a:8e:de:f6:0a:09:58:8f:
        68:98:4f:f3:8a:e2:37:5c:d6:42:32:8f:d9:01:56:41:88:df:
        1a:ba:63:03:62:08:89:06:13:88:74:6f:cd:eb:26:f0:67:a4:
        26:9b:a3:4c:ff:7b:c9:19:2c:12:58:06:ce:22:3c:e6:cd:52:
        b0:d0:da:6a:c9:02:df:02:e6:25:77:39:cf:50:80:e7:1d:01:
        fc:40:17:a2:98:04:bf:8b:24:f6:55:46:99:7b:17:05:01:d3:
        09:3d:a2:f0:e0:ba:5d:15:b8:28:74:d2:a3:fe:fd:86:7d:e0:
        60:e8:e4:38:6a:17:9c:80:80:e3:50:11:5e:35:f5:02:2b:65:
        60:41:2a:dc:ed:a8:a9:9a:6f:24:b4:7a:9c:39:01:a4:fc:cf:
        e6:94:86:f1:18:3a:f5:99:6b:f8:66:a2:ff:04:08:7e:ca:6b:
        2a:aa:cf:72:26:d0:c9:96:a0:98:fd:91:bb:b1:e4:8d:6d:10:
        08:ea:56:de:07:20:d3:e6:9a:bf:de:cf:c3:a4:e8:43:60:4f:
        b4:53:aa:d5
-----BEGIN CERTIFICATE REQUEST-----
MIIC0TCCAbkCAQAwczELMAkGA1UEBhMCQ0ExCzAJBgNVBAgTAkJDMRAwDgYDVQQH
EwdOZXdidXJ5MRMwEQYDVQQKDApRQV9TYW1wbGUxMRIwEAYDVQQLDAlTYW1wbGVf
UUExHDAaBgNVBAMME3NhbXBsZTFfcWEudmljdG9yaWEwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQDpXqKBU9zptfdUMxdvFZwAXP+yZMblSL42p6RV9LHf
yYGkQf4pgNb91MS117fBPUJswPgJzeo29ju52c4Vhy0vs/Jf+UIG4qBiVgZtzGVp
Yts2NAmVWBPQ5oXuZHY+7dZHu0nyCIEUwu0T2yC6hudgJIABfz23YBa6BtSh4Bg5
c8oeJBVWbZd5gQT3/Tc6QtcVgjSqUSzM4vDRQt21cbsQGaAKXE93ubs21e2kdwfj
UPk2IBPi4XjSCjaKuTmQH6SCEk9QKT8ZfRamsyN7uHuFYAQhOYQdnoHlICyKUfNS
9zxP5vKliNwumQqzZR6/M1++3FMcpmkYxMd1vyDjzymvAgMBAAGgGTAXBgkqhkiG
9w0BCQcxChMIZ3VhcmRpdW0wDQYJKoZIhvcNAQEFBQADggEBAAZKudsEoY1M9z+P
JPp87KZwd4u5OHy251Gq7ZYgFjeFp0QmK4dMpNsM89OH42hKjt72CglYj2iYT/OK
4jdc1kIyj9kBVkGI3xq6YwNiCIkGE4h0b83rJvBnpCabo0z/e8kZLBJYBs4iPObN
UrDQ2mrJAt8C5iV3Oc9QgOcdAfxAF6KYBL+LJPZVRpl7FwUB0wk9ovDgul0VuCh0
0qP+/YZ94GDo5DhqF5yAgONQEV419QIrZWBBKtztqKmabyS0epw5AaT8z+aUhvEY
OvWZa/hmov8ECH7Kayqqz3Im0MmWoJj9kbux5I1tEAjqVt4HINPmmr/ez8Ok6ENg
T7RTqtU=
-----END CERTIFICATE REQUEST-----
ok
temp4>
```

4. Copy from the -----BEGIN CERTIFICATE REQUEST----- to the -----END CERTIFICATE REQUEST----- into a file and send this to your CA for signing.

   The CA will sign the certificate and send you back a public key that looks something like:

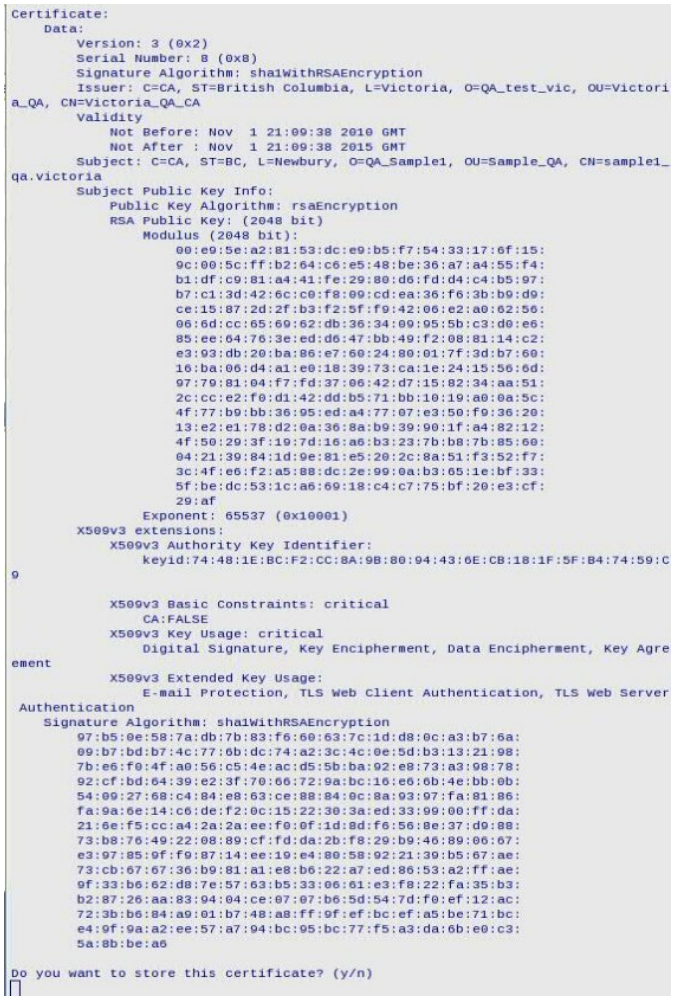
```
enance@enance1 Latest $ cat sample1_qa.victoria.pem
-----BEGIN CERTIFICATE-----
MIID1jCCAsCgAwIBAgIBCDALBgkqhkiG9w0BAQUwgYAxCzAJBgNVBAYTAkNBMRkw
FwYDVQQIExBCcml0aXNoIENvbHVtYmlhMREwDwYDVQQHEwhWaWN0b3JpYTEUMBIG
A1UEChMLUUFfdGVzdF92aWMxFDASBgNVBAsTC1ZpY3Rvcmlhx1FBMRcwFQYDVQQD
Ew5WaWN0b3JpYV9RQV9DQTAeFw0xMDExMDEyMTA5MzhaFw0xNTExMDEyMTA5Mzha
MHMxCzAJBgNVBAYTAkNBMQswCQYDVQQIEwJCQzEQMA4GA1UEBxMHTmV3YnVyeTET
MBEGA1UECgwKUUFfU2FtcGxlMTESMBAGA1UECwwJU2FtcGxlX1FBMRwwGgYDVQQD
DBNzYW1wbGUxX3FhLnZpY3RvcmlhMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA6V6igVPc6bX3VDMXbxWcAFz/smTG5Ui+NqekVfSx38mBpEH+KYDW/dTE
tZe3wT1CbMD4Cc3qNvY7udnOFYctL7PyX/lCBuKgYlYGbcxlaWLbNjQJlVvD0OaF
7mR2Pu3WR7tJ8giBFMLjk9sguobnYCSAAX89t2AWugbUoeAY0XPKHiQVVm2XeYEE
9/03BkLXFYI0qlEszOLw0ULdtXG7EBmgClxPd7m7NpXtpHcH41D5NiAT4uF40go2
irk5kB+kghJPUCk/GX0WprMje7h7hWAEITmEHZ6B5SAsilHzUvc8T+bypYjcLpkK
s2UevzNfvtxTHKZpGMTHdb8g488prwIDAQABo2swaTAfBgNVHSMEGDAWgBR0SB68
8syKm4CUQ27LGB9ftHRZyTAMBgNVHRMBAf8EAjAAMA8GA1UdDwEB/wQFAwMHuAAw
JwYDVR0lBCAwHgYIKwYBBQUHAwQGCCsGAQUFBwMCBggrBgEFBQcDATALBgkqhkiG
9w0BAQUDggEBAJe1Dlh623uD9mBjfB3YDKO3agm3vbdMd2vcdKI8TA5dsxMhmHvm
8E+gVsVOrNVbupLoc6OYeJLPvWQ54j9wZnKavBbma067C1QJJ2jEhOhjzoiEDIqT
l/qBhvqabhTG3vIMFSIwOu0zmQD/2iFu9cykKiru8A8djfZWjjfZiHO4dkkiCInP
/dor+Cm5RokGZ+OXhZ/5hxTuGeSAWJIhObVnrnPLZ2c2uYGh6LYip+2GU6L/rp8z
tmLYfldjtTMGYeP4Ivo1s7KHJqqDlATOBwe2XVR9808SrHI7toSpAbdIqP+f77zv
pb5xvOSfmqLuV6eUvJW8d/Wj2mvgw1qLvqY=
-----END CERTIFICATE-----
```

5. Have this file handy to either copy its contents or import it to the Guardium system. Enter: cli> store certificate sniffer [console | import]
6. If console, copy-paste from **-----BEGIN CERTIFICATE-----** all the way to **-----END CERTIFICATE-----** (including those within the copy) and paste into the CLI when prompted. If choosing import, tell the Guardium system where to import the file from.

```
temp4 > store system certificate console
Please paste your new system certificate, in PEM format.
Include the BEGIN and END lines, then press CTRL-D.

-----BEGIN CERTIFICATE-----
MIID1jCCAsCgAwIBAgIBCDALBgkqhkiG9w0BAQUwgYAxCzAJBgNVBAYTAkNBMRkw
FwYDVQQIExBCcml0aXNoIENvbHVtYmlhMREwDwYDVQQHEwhWaWN0b3JpYTEUMBIG
A1UEChMLUUFfdGVzdF92aWMxFDASBgNVBAsTC1ZpY3Rvcmlhx1FBMRcwFQYDVQQD
Ew5WaWN0b3JpYV9RQV9DQTAeFw0xMDExMDEyMTA5MzhaFw0xNTExMDEyMTA5Mzha
MHMxCzAJBgNVBAYTAkNBMQswCQYDVQQIEwJCQzEQMA4GA1UEBxMHTmV3YnVyeTET
MBEGA1UECgwKUUFfU2FtcGxlMTESMBAGA1UECwwJU2FtcGxlX1FBMRwwGgYDVQQD
DBNzYW1wbGUxX3FhLnZpY3RvcmlhMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA6V6igVPc6bX3VDMXbxWcAFz/smTG5Ui+NqekVfSx38mBpEH+KYDW/dTE
tZe3wT1CbMD4Cc3qNvY7udnOFYctL7PyX/lCBuKgYlYGbcxlaWLbNjQJlVvD0OaF
7mR2Pu3WR7tJ8giBFMLjk9sguobnYCSAAX89t2AWugbUoeAYOXPKHiQVVm2XeYEE
9/03BkLXFYI0qlEszOLw0ULdtXG7EBmgClxPd7m7NpXtpHcH41D5NiAT4uF40go2
irk5kB+kghJPUCk/GX0WprMje7h7hWAEITmEHZ6B5SAsilHzUvc8T+bypYjcLpkK
s2UevzNfvtxTHKZpGMTHdb8g488prwIDAQABo2swaTAfBgNVHSMEGDAWgBR0SB68
8syKm4CUQ27LGB9ftHRZyTAMBgNVHRMBAf8EAjAAMA8GA1UdDwEB/wQFAwMHuAAw
JwYDVR0lBCAwHgYIKwYBBQUHAwQGCCsGAQUFBwMCBggrBgEFBQcDATALBgkqhkiG
9w0BAQUDggEBAJe1Dlh623uD9mBjfB3YDKO3agm3vbdMd2vcdKI8TA5dsxMhmHvm
8E+gVsVOrNVbupLoc6OYeJLPvWQ54j9wZnKavBbma067C1QJJ2jEhOhjzoiEDIqT
l/qBhvqabhTG3vIMFSIwOu0zmQD/2iFu9cykKiru8A8djfZWjjfZiHO4dkkiCInP
/dor+Cm5RokGZ+OXhZ/5hxTuGeSAWJIhObVnrnPLZ2c2uYGh6LYip+2GU6L/rp8z
tmLYfldjtTMGYeP4Ivo1s7KHJqqDlATOBwe2XVR9808SrHI7toSpAbdIqP+f77zv
pb5xvOSfmqLuV6eUvJW8d/Wj2mvgw1qLvqY=
-----END CERTIFICATE-----
```

It asks you to confirm that you want to store the certificate, and when you confirm, it stores it.



7. Restart the inspection-core for the new certificate to take effect.

Parent topic: Linux and UNIX systems: Set up S-TAP authentication with SSL certificates

Linux and UNIX systems: Installing an SSL certificate generated outside of the Guardium system

Use this procedure to install the SSL certificate that was created by the CA.

About this task

If the CA is sending you a whole certificate to install, you need two files, the private key in PKCS#8 (password protected) format, and the public key in PEM format. The certificate generated needs to be a 2048 bit RSA key.

The CA sends you two files, and the public cert for your CA.

The public-cert of your CA looks like:

```
enance@enance1 Latest $ cat Victoria_QA_CA.pem
-----BEGIN CERTIFICATE-----
MIID2zCCAsWgAwIBAgIBATALBgkqhkiG9w0BAQUwgYAxCzAJBgNVBAYTAkNBMRkw
FwYDVQQIExBCcml0aXNoIENvbHVtYmlhMREwDwYDVQQHEwhWaWN0b3JpYTEUMBIG
A1UEChMLUUFfdGVzdF92aWMxFDASBgNVBAsTC1ZpY3RvcmlhX1FBMRcwFQYDVQQD
Ew5WaWN0b3JpYV9RQV9DQTAeFw0xMDA4MTIxODMzMDJaFw0zMDA4MTIxODMzMDJa
MIGAMQswCQYDVQQGEwJDQTEZMBcGA1UECBMQQnJpdGlzaCBDb2x1bWJpYTERMA8G
A1UEBxMIVmljdG9yaWExFDASBgNVBAoTC1FBX3R1c3RfdmljMRQwEgYDVQQLEwtW
aWN0b3JpYV9RQTEXMBUGA1UEAxMOVmljdG9yaWFfUUFfQ0EwggEgMAsGCSqGSIb3
DQEBAQOCAQ8AMIIBCgKCAQEA0x3iAXs1KGNoJThXkO+jcNyMBlfwKWRMTOq9PkF4
piznXCRwPz2nQWk5/fpslchmuVYXJtfZi7umDxp2FEMvMmhJfFZiqbCn1Rb5yH+1
V3RsIerB0DFpoWkdt+wD6BufndO5P9eOlv14bmTl+F0dUM0TxAwtX73CMQOX/n+i
/WrzpWU4lU71KkyWUfJl2Pm8TLEMr5awpzt2rEJ/Q1qItHcksQDbGY0MNLaNojEU
XBzUpu9ezbv+zVH+5iorFYkrH0NQI0NK+YoR1b3Tto0HLDh6istsMfHdNEEQb9BB
vMjqUz4tGB2HDguYTaNbQJj9Yw8uv7/tfwW/cesrqm8DiQIDAQABo2QwYjAPBgNV
HRMBAf8EBTADAQH/MA8GA1UdDwEB/wQFAwMHBgAwHQYDVR0OBBYEFHRIHrzyzIqb
gJRDbssYH1+0dFnJMB8GA1UdIwQYMBaAFHRIHrzyzIqbgJRDbssYH1+0dFnJMAsG
CSqGSIb3DQEBBQOCAQEAbrImEbRyBka0wO/ZuPd0Hw9jpbxIuaYEskakv7aM4TUQ
awf1CiqwwAymmKb2REItLajhjmBFbXBun7d137vBU2KX104I7WGw0xgI5rmlELa+
2fizugY+Bc6mh+5c0haizkyudKzo8mLz2p/IS7SPh2lJ9rnuBleSt9zfiYanPxX1
Q6z1+WRKIRSUmK+ho4bmtgr5F0+ejmZb9nfzeOBj23H9i0mWoaQ/SO+O2iDIvDY0
KYwqCeS2UNEdTcnfuczbBkqnAsf5/GBPIhnWX3onuLkOsHdY0HHPjoqgHauoxPK8
p0sEvlCK8EFOD6wkp0vtNhFQCykxRimHR6Pz9jEVjw==
-----END CERTIFICATE-----
```

The public-cert specific to you/this Guardium system looks like:

```
enance@enance1 Latest $ cat Sample_givenCert.victoria.qa_pub.pem
-----BEGIN CERTIFICATE-----
MIID5jCCAtCgAwIBAgIBCTALBgkqhkiG9w0BAQUwgYAxCzAJBgNVBAYTAkNBMRkw
FwYDVQQIExBCcml0aXNoIENvbHVtYmlhMREwDwYDVQQHEwhWaWN0b3JpYTEUMBIG
A1UEChMLUUFfdGVzdF92aWMxFDASBgNVBAsTC1ZpY3RvcmlhX1FBMRcwFQYDVQQD
Ew5WaWN0b3JpYV9RQV9DQTAeFw0xMDExMTUyMDUwNThaFw0xNTExMTUyMDUwNTha
MIGEMQswCQYDVQQGEwJDQTEZMBcGA1UECBMQQnJpdGlzaCBDb2xvbWJpYTESMBAG
A1UEBxMJVmFuY291dmVyMQswCQYDVQQKEwJRQTESMBAGA1UECxMJUUFfU0FNUExxF
MSUwIwYDVQQDExxTYW1wbGVfZ2l2ZW5DZXJ0LnZpY3RvcmlhLnFhMIIBIDALBgkq
hkiG9w0BAQEDggEPADCCAQoCggEBALdt2XhJEJIAognblgFNoiomVvcGIe9PHs0t
3fP5DxAL5PVm+UCRS0xnnCoKe3pdJNagepDwBa2K5UsHbK4vkHJEgWWEd4bx2Ks7
kRoHr83TXK+W8al1HGKRwUSwN0hfm/KV4v8ZX3AFWs2c/BJ2iA77a0mhU0JuWa1/
/scXitJB5ykPjFb2EuReA6ELphaQ/itjZIQTTeVxbamyx42ia9J5B07lFTp3qGdU
yXUwlEFX0HFPmknAAaQrSnpMdQjkOKgzxU0NTV4ILA66hCVkX+ezQeJA90s/AHA5
hAY2fyurKZsOowoE0xlEpFWCGf87zxfkmTaWthqCS0NzEcJ6efECAwEAAaNrMGkw
HwYDVR0jBBgwFoAUdEgevPLMipuAlENuyxgfX7R0WckwDAYDVR0TAQH/BAIwADAP
BgNVHQ8BAf8EBQMDB7gAMCcGA1UdJQQgMB4GCCsGAQUFBwMEBggrBgEFBQcDAgYI
KwYBBQUHAwEwCwYJKoZIhvcNAQEFA4IBAQB+P1m22B72eRESk9rgNdOB+l48k5xw
QHf64TJcoI/Vcz0vtGBC1jDfZzVDIHJaX6ZMtdO23QO6rtjQSnhjhbOt/EiimaNO
tysJOE999E+HQ7UpKYKvdoznwpYEthyoQJ9quKqQc1YW/l8pQMYDEdK8c7yMbJpv
mrxO8h+G3YYQMT6A9KAk/GPA+yKl0fCuogBhPyWM28q35EAIw6H9ahQigWhNkzrL
DCYO8VCLi3BX+OohLvurkyzJm2lnbm7BSb5QB4jISlRBGPoIWhK6VPypboyABfVs
yWHFVs10EUb0Maa/XNZILTAoYAbYK5sX7Ri5hr5KhxnmDd9AJMQsLfik
-----END CERTIFICATE-----
```

The private key (encrypted with pkx#8) looks like:

```
enance@enance1 Latest $ cat Sample_givenCert.victoria.qa_pri.pem
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIE4jAcBgoqhkiG9w0BDAEDMA4ECAKuMvSla9T4AgIBYgSCBMB/RzDgm4xpRDnA
Cd//wgD9c8junXmVpyJWXWgXhlj3Sgv3toKt2yBQY7Rv0peP1y68nuHKZcp/QZDj
QksDvIJHacpz886KQ2p9xxOCrIO3RTVNULPzrucUNuJ2a5W4IGPGwnrNLKsriRH6
CXQjRu19+kbczmPtrlHu7gj6MuCp58sIyXbsOPCnsZBaAOcf72qeKfVa4tKlpobI
e5YDg+UiJXYv1Kfj9t9tftSfaCym0jK+uE3++y5+ah/k+u/VcEb9b6Drlf68KaJI
/OYVVmRWVIHEY2QjVOsVEXAARjpugf6cXIn8epw/CMaC0yVg4O9OGDrIz/41DVgk
/b3jlr1oWMRVASSqgOQxE2LrNNAF/XiFwpiLUCBHR0fXX9iKJM7nK6AXlf4hrd31
sMm1hICJvQwuRP+1xCHHs3qKk7oFAdyEdMiYthcOoAaynGmP4vPEMB6ZdOSxd/yN
7IfBT1U7nCtgo4FpAn4FTnkXRdlDqPpvKLqe0kkQCKo9ZWRnnIS1hAs9VJXS6zou
1IohZewrS/TWnPU+ArE/QJ4WkX2dBAe0Q2HMvuXs6J6Rfn+H2eZC+zThOkvqA0ic
UiQAgJB0ohXWEah9BJbIYNULLpbssUySDLPrxYdZRPn5MFKqCXmWw5tAEV8mIcg4
obB6DxVGHz93iPD0XJyBGWpCdcwItzdngnMR316tX4R3jMy2U0hrzk5o01GoZQQ/
eGYsuPzm4zqVJ8S9gUMFR8ocoPWqwhU+Sq4QPCIQEGf5gwxxt9j7L2TtRbD7kxnD
23aPL/wuk45EFJKTQCeZ3kjUqCCuSbqBJXGEjiiUsahus+yJULJ8boFWu1T8zW7m
/CBK1TzY9Fh+gbdOtN4b+zWUrpk5E7ZctFhEwojVFBwgPzUIZEkap4gH+/F5d3rI
uWFBcN7QER35wO8au/k5kLKHDh+5U15ltkJ38P1pJYFE0p5/K81YWnfvUaJmynJY
DfnK0X6Au69/F6+QR4S+bchbrqk73plIiXbkwqapQ26QH5ztIK3T6/nY6RKa7u6N
WvnskpAE1uxf+soM+BpEzpTl2gQQmEaZnh9Ci3ZnpTZE5tkAL0oTqXL9sToyeynz
Z91m+uKxYRjFvc1KPh+I8dUR0E5qXhBdRR7heIlm7/Dg+UqCUkXoyW89G14u/mJT
jB50CHxLAFOSeXnKn8G/9rOHA565r8L/z8D12sli5T1zHicZJ8O211zCSezdF+GG
mI12jfOZmNIBgCVUtpOBNX5IDbr7L+0bM6vuDmXRhnhX4f34+5HGfj3ntLAV7bmn
IOEGIhyoGFnoxyWaT0xxa6MVQJazcKSyyyhO8UixFEoKI3drpFXB0tXVb0CLFq+y
QVp9dHgO3Otzw/yCmCpbQQe8UFRYyC74wBf9yPWDtN6MW/IeEZCBoYaeMR+WyonM
mdq5xbriETXD4zha3NGAv2qnzkfkKMBcVeUULulyixMsHmNNJkINNEsj5deVYtOt
4j5EK/aZsTqTgrVq3oGlwgXM1YptvlVR+HPWZfpjwbL+7/NhmK7AhEPo+qQCVD7t
ZGRbdbB7FEN23m88IMSd8xkhS2M1pop1Cj71P/dA+DD/dgcjP2bw7K923d4r3CcS
1yxPhLKM
-----END ENCRYPTED PRIVATE KEY-----
```

Have these files handy to either import (via scp/ftp/etc) to the Guardium system or to copy-paste into the cli interface on the Guardium system.

Procedure

1. Log in to the Guardium system via CLI.
2. Store the private key by entering: cli> store certificate keystore [import | console] The import takes the saved file, and then copies and pastes the contents of the file into your console interface. It asks for the password that the file was saved with. Either you provided this to the CA for creation of the certificate, or more likely, they provided you with a password when they sent your files. Here's what it looks like on the Guardium system:

```
temp4> store system key console
Please paste your new system key, in PEM format.
Include the BEGIN and END lines, then press CTRL-D.

-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIE4jAcBgoqhkiG9w0BDAEDMA4ECAKuMvS1a9T4AgIBYgSCBMB/RzDgm4xpRDnA
Cd//wgD9c8junXmVpyJWXWgXhlj3Sgv3toKt2yBQY7Rv0peP1y68nuHKZcp/QZDj
QksDvIJHacpz886KQ2p9xxOCrIO3RTVNULPzrucUNuJ2a5W4IGPGwnrNLKsriRH6
CXQjRu19+kbczmPtrlHu7gj6MuCp58sIyXbsOPCnsZBaAOcf72qeKfVa4tKlpobI
e5YDg+UiJXYv1Kfj9t9tftSfaCym0jK+uE3++y5+ah/k+u/VcEb9b6DrlfG8KaJI
/0YVVmRWVIHEY2QjVOsVEXAARjpugf6cXIn8epw/CMaC0yVg4O9OGDrIz/41DVgk
/b3jlr1oWMRVASSqgOQxE2LrNNAF/XiFwpiLUCBHR0fXX9iKJM7nK6AXlf4hrd31
sMm1hICJvQwuRP+1xCHHs3qKk7oFAdyEdMiYthcOoAaynGmP4vPEMB6ZdOSxd/yN
7IfBT1U7nCtgo4FpAn4FTnkXRdlDqPpvKLqe0kkQCKo9ZWRnnIS1hAs9VJXS6zou
1IohZewrS/TWnPU+ArE/QJ4WkX2dBAe0Q2HMvuXs6J6Rfn+H2eZC+zThOkvqA0ic
UiQAgJB0ohXWEah9BJbIYNULLpbssUySDLPrxYdZRPn5MFKqCXmWw5tAEV8mIcg4
obB6DxVGHz93iPD0XJyBGWpCdcwItzdngnMR316tX4R3jMy2U0hrzk5o01GoZQQ/
eGYsuPzm4zqVJ8S9gUMFR8ocoPWqwhU+Sq4QPCIQEGf5gwxxt9j7L2TtRbD7kxnD
23aPL/wuk45EFJKTQCeZ3kjUqCCuSbqBJXGEjiiUsahus+yJULJ8boFWu1T8zW7m
/CBK1TzY9Fh+gbdOtN4b+zWUrpk5E7ZctFhEwojVFBwgPzUIZEkap4gH+/F5d3rI
uWFBcN7QER35wO8au/k5kLKHDh+5Ul5ltkJ38P1pJYFE0p5/K81YWnfvUaJmynJY
DfnK0X6Au69/F6+QR4S+bchbrqk73plIiXbkwqapQ26QH5ztIK3T6/nY6RKa7u6N
WvnskpAE1uxf+soM+BpEzpTl2gQQmEaZnh9Ci3ZnpTZE5tkAL0oTqXL9sToyeynz
Z91m+uKxYRjFvc1KPh+I8dUR0E5qXhBdRR7heIlm7/Dg+UqCUkXoyW89G14u/mJT
jB50CHxLAFOSeXnKn8G/9r0HA565r8L/z8D12sli5T1zHicZJ8O211zCSezdF+GG
mI12jfOZmNIBgCVUtpOBNX5IDbr7L+0bM6vuDmXRhnhX4f34+5HGfj3ntLAV7bmn
IOEGIhyoGFnoxyWaT0xxa6MVQJazcKSyyyhO8UixFEoKI3drpFXB0tXVb0CLFq+y
QVp9dHgO3Otzw/yCmCpbQQe8UFRYyC74wBf9yPWDtN6MW/IeEZCBoYaeMR+WyonM
mdq5xbriETXD4zha3NGAv2qnzkfkKMBcVeUULulyixMsHmNNJkINNEsj5deVYtOt
4j5EK/aZsTqTgrVq3oGlwgXM1YptvlVR+HPWZfpjwbL+7/NhmK7AhEPo+qQCVD7t
ZGRbdbB7FEN23m88IMSd8xkhS2M1pop1Cj71P/dA+DD/dgcjP2bw7K923d4r3CcS
1yxPhLKM
-----END ENCRYPTED PRIVATE KEY-----
Enter pass phrase for /var/tmp/key.pem:
writing RSA key

ok
temp4>
```

3. Import the signed certificate with: cli> store certificate sniffer [import | console] It displays the information on the cert and then asks you to confirm storing the cert. It looks like:

```
temp4> store system certificate console
Please paste your new system certificate, in PEM format.
Include the BEGIN and END lines, then press CTRL-D.

-----BEGIN CERTIFICATE-----
MIID5jCCAtCgAwIBAgIBCTALBgkqhkiG9w0BAQUwgYAxCzAJBgNVBAYTAkNBMRkw
FwYDVQQIExBCcml0aXNoIENvbHVtYmlhMREwDwYDVQQHEwhWaWN0b3JpYTEUMBIG
A1UEChMLUUFfdGVzdF92aWMxFDASBgNVBAsTC1ZpY3RvcmlhX1FBMRcwFQYDVQQD
Ew5WaWN0b3JpYV9RQV9DQTAeFw0xMDExMTUyMDUwNThaFw0xNTExMTUyMDUwNTha
MIGEMQswCQYDVQQGEwJDQTEZMBcGA1UECBMQQnJpdGlzaCBDb2xvbWJpYTESMBAG
A1UEBxMJVmFuY291dmVyMQswCQYDVQQKEwJRQTESMBAGA1UECxMJUUFfU0FNUExF
MSUwIwYDVQQDExxTYW1wbGVfZ2l2ZW5DZXJ0LnZpY3RvcmlhLnFhMIIBIDALBgkq
hkiG9w0BAQEDggEPADCCAQoCggEBALdt2XhJEJIAognblgFNoiomVvcGIe9PHsOt
3fP5DxAL5PVm+UCRS0xnnCoKe3pdJNagepDwBa2K5UsHbK4vkHJEgWWEd4bx2Ks7
kRoHr83TXK+W8al1HGKRwUSwN0hfm/KV4v8ZX3AFWs2c/BJ2iA77a0mhU0JuWa1/
/scXitJB5ykPjFb2EuReA6ELphaQ/itjZIQTTeVxbamyx42ia9J5B07lFTp3qGdU
yXUwlEFX0HFPmknAAaQrSnpMdQjkOKgzxU0NTV4ILA66hCVkX+ezQeJA90s/AHA5
hAY2fyurKZsOowoE0xlEpFWCGf87zxfkmTaWthqCS0NzEcJ6efECAwEAAaNrMGkw
HwYDVR0jBBgwFoAUdEgevPLMipuAlENuyxgfX7R0WckwDAYDVR0TAQH/BAIwADAP
BgNVHQ8BAf8EBQMDB7gAMCcGA1UdJQQgMB4GCCsGAQUFBwMEBggrBgEFBQcDAgYI
KwYBBQUHAwEwCwYJKoZIhvcNAQEFA4IBAQB+Plm22B72eRESk9rgNdOB+l48k5xw
QHf64TJcoI/Vcz0vtGBC1jDfZzVDIHJaX6ZMtdO23QO6rtjQSnhjhbOt/EiimaNO
tysJOE999E+HQ7UpKYKvdoznwpYEthyoQJ9quKqQc1YW/l8pQMYDEdK8c7yMbJpv
mrxO8h+G3YYQMT6A9KAk/GPA+yKl0fCuogBhPyWM28q35EAIw6H9ahQigWhNkzrL
DCYO8VCLi3BX+OohLvurkyzJm2lnbm7BSb5QB4jISlRBGPoIWhK6VPypboyABfVs
yWHFVs10EUb0Maa/XNZILTAoYAbYK5sX7Ri5hr5KhxnmDd9AJMQsLfik
-----END CERTIFICATE-----
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 9 (0x9)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CA, ST=British Columbia, L=Victoria, O=QA_test_vic, OU=Victoria_QA, CN=Victoria_QA_CA
        Validity
            Not Before: Nov 15 20:50:58 2010 GMT
            Not After : Nov 15 20:50:58 2015 GMT
        Subject: C=CA, ST=British Colombia, L=Vancouver, O=QA, OU=QA_SAMPLE, CN=Sample_givenCert.victoria.qa
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:b7:6d:d9:78:49:10:92:00:a2:09:db:96:01:4d:
                    a2:2a:26:56:f7:06:21:ef:4f:1e:c3:ad:dd:f3:f9:
                    0f:10:0b:e4:f5:66:f9:40:91:4b:4c:67:9c:2a:0a:
                    7b:7a:5d:24:d6:a0:7a:90:f0:05:ad:8a:e5:4b:07:
                    6c:ae:2f:90:72:44:81:65:84:77:86:f1:d8:ab:3b:
                    01:1a:07:af:cd:d3:5c:af:96:f1:a9:75:1c:62:91:
                    c1:44:b0:37:48:5f:9b:f2:95:e2:ff:19:5f:70:05:
                    5a:cd:9c:fc:12:76:88:0e:fb:6b:49:a1:53:42:6e:
                    59:ad:7f:fe:c7:17:8a:d2:41:e7:29:0f:8c:56:f6:
                    12:e4:5e:03:a1:0b:a6:16:90:fe:2b:63:64:84:13:
                    4d:e5:71:6d:a9:b2:c7:8d:a2:6b:d2:79:07:4e:e5:
                    15:3a:77:a8:67:54:c9:75:30:94:41:57:d0:71:4f:
                    9a:49:c0:01:a4:2b:4a:7a:4c:75:08:e4:38:a8:33:
                    c5:4d:0d:4d:5e:08:2c:0e:ba:84:25:64:5f:e7:b3:
                    41:e2:40:f7:4b:3f:00:70:39:84:06:36:7f:2b:ab:
                    29:9b:0e:a3:0a:04:d3:19:44:a4:55:82:19:ff:3b:
                    cf:17:e4:99:36:96:b6:1a:82:4b:43:73:11:c2:7a:
                    79:f1
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:74:48:1E:BC:F2:CC:8A:9B:80:94:43:6E:CB:18:1F:5F:B4:74:59:C9

            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
            X509v3 Extended Key Usage:
                E-mail Protection, TLS Web Client Authentication, TLS Web Server Authentication
    Signature Algorithm: sha1WithRSAEncryption
        7e:3e:59:b6:d8:1e:f6:79:11:12:93:da:e0:35:d3:81:fa:5e:
        3c:93:9c:70:40:77:fa:e1:32:5c:a0:8f:d5:73:3d:2f:b4:60:
        42:d6:30:df:67:35:43:20:72:5a:5f:a6:4c:b5:d3:b6:dd:03:
        ba:ae:d8:d0:4a:78:63:85:b3:ad:fc:48:a2:99:a3:4e:b7:2b:
        09:38:4f:7d:f4:4f:87:43:b5:29:29:82:af:76:8c:e7:c2:96:
        04:b6:1c:a8:40:9f:6a:b8:aa:90:73:56:16:fe:5f:29:40:c6:
        03:11:d2:bc:73:bc:8c:6c:9a:6f:9a:bc:4e:f2:1f:86:dd:86:
        10:31:3e:80:f4:a0:24:fc:63:c0:fb:22:a5:d1:f0:ae:a2:00:
        61:3f:25:8c:db:ca:b7:e4:40:08:c3:a1:fd:6a:14:22:81:68:
        4d:93:3a:cb:0c:26:0e:f1:50:8b:8b:70:57:f8:ea:21:2e:fb:
        ab:93:2c:c9:9b:69:67:6e:6e:c1:49:be:50:07:88:c8:4a:54:
        41:18:fa:08:5a:12:ba:54:fc:a9:6e:8c:80:05:f5:6c:c9:61:
        c5:56:cd:74:11:46:f4:31:a6:bf:5c:d6:48:2d:30:28:60:06:
        d8:2b:9b:17:ed:18:b9:86:be:4a:87:19:e6:0d:df:40:24:c4:
        2c:2d:f8:a4

Do you want to store this certificate? (y/n)
y
ok
temp4>
```

4. Restart the inspection-core for the new certificate to take effect.

Parent topic: Linux and UNIX systems: Set up S-TAP authentication with SSL certificates

Linux and UNIX systems: Configuring the S-TAP to use x.509 certificate authentication

About this task

First, take note of what you have assigned as the CA and the CN of the certificate. If you don't remember, use the CLI command show system certificate to display the values.

```
temp4 > show system certificate
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 8 (0x8)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CA, ST=British Columbia, L=Victoria, O=QA_test_vic, OU=Victoria_QA, CN=Victoria_QA_CA
        Validity
            Not Before: Nov  1 21:09:38 2010 GMT
            Not After : Nov  1 21:09:38 2015 GMT
        Subject: C=CA, ST=BC, L=Newbury, O=QA_Sample1, OU=Sample_QA, CN=sample1_qa.victoria
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
```

You need the CN of the cert installed on the Guardium system and the public-key for the CA that signed the certificate on the Guardium system. You also might want a Certificate Revocation list signed by the same CA that signed the Guardium system cert, but it's not necessary.

The relevant parameters in the guard_tap.ini are:

```
; Where is the CA certificate
guardium_ca_path=NULL
; What's the CN to expect from the SqlGuard certificate?
sqlguard_cert_cn=NULL
; Path to crls file or dir
guardium_crl_path=NULL
```

If you do not choose to use a value for a parameter, set its value equal to NULL. This is pertinent to the CRL path in particular, or if you want to shut off certificate authentication and go back to TLS.

Procedure

1. Copy the public key [and the CRL if wanted] for the CA that the CA sent you to a directory on the S-TAP host. Take note of this directory.
2. Set `guardium_ca_path=[path-to-CA.pem]`
3. Set `sqlguard_cert_cn=[the full CN or partial CN (using * as a wildcard) of the Guardium system]`
4. If you want to use a certificate revocation list at this time, set `guardium_crl_path=[path-to-crl.crl]` It should look like:

```
guardium_ca_path=/var/tmp/pki/Victoria_QA_CA.pem
sqlguard_cert_cn=sample1_qa.victoria
guardium_crl_path=/var/tmp/pki/Victoria_QA_CA.crl
```

5. Change tls=1.
6. Restart the S-TAP You are now connected using Openssl.

Parent topic: Linux and UNIX systems: Set up S-TAP authentication with SSL certificates

Linux and UNIX systems: Increasing S-TAP® throughput

You can configure an S-TAP that reports to multiple Guardium systems to increase the throughput of data.

You can configure any S-TAP to create multiple threads to increase the throughput of data. If the S-TAP configuration file defines more than one Guardium system, a thread can be created for each Guardium system. S-TAP creates extra threads, matching the number of Guardium systems, in v10.1.4 and higher up to 10 threads. When participate_in_load_balancing parameter is set to 4, the K-TAP creates a similar number of buffers matching the number of Guardium systems up to 5 threads. The K-TAP alternates between the buffers, placing entire packets in each buffer. Each S-TAP thread reads from a different K-TAP buffer, and sends traffic data to a single Guardium system.

In this configuration, no one Guardium receives all the data from the S-TAP. The distribution is similar to that used when participate_in_load_balancing is set to 1.
Attention: Prior to V10 GPU200, when a Guardium system becomes unavailable, no failover is provided. Data that was being sent to a Guardium system is lost until the system becomes available or the configuration is changed.
Attention: Prior to V10 GPU300, if the S-TAP configuration file defines more than one Guardium system, a thread can be created for each Guardium system. This feature is activated only when participate_in_load_balancing parameter is set to 4.

Encrypted and unencrypted A-TAP traffic cannot be sent to the same Guardium system. This is similar to the situation when participate_in_load_balancing is set to 1

Parent topic: Linux and UNIX systems: Configuring S-TAP
Parent topic: Linux and UNIX systems: S-TAP operation and performance

Linux and UNIX systems: Kerberos-authenticated database traffic

Kerberos is a network authentication protocol that eliminates the transmission of unencrypted passwords across the network. Learn how it functions in Guardium .

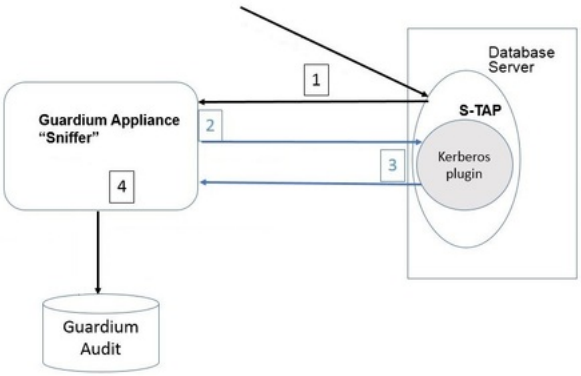
It works in a mutual authentication mode, verifying both the identity of the user that is requesting authentication as well as the server providing the requested authentication. The Kerberos authentication mechanism issues tickets for accessing network services. These tickets contain encrypted data, including an encrypted password, that confirms the user's identity to the requested service.

For auditing and alerting, it's important to know which database user performed an action. When login is done with a Kerberos ticket, determining the database user is not always straightforward.

Guardium S-TAP only sees network traffic and passes it on to the sniffer on the Guardium appliance. When a Kerberos ticket is used for login, S-TAP passes that Kerberos ticket along to the sniffer. For some database server types, the sniffer can determine the database user from the Kerberos login traffic and no additional information is required. For other database server types, the sniffer needs some assistance. That function is performed by the S-TAP Kerberos plugin.

The S-TAP Kerberos plugin is not enabled by default; it requires additional configuration.

If you use Kerberos at all, configure the plugin. There is no performance implication or other downside to configuring the plugin, just in case you need it.



The data flow between the database, the Guardium sniffer and the Guardium audit data is:

1. S-TAP captures the Kerberized database login packet (along with other activity) and sends it to the Guardium appliance.
2. If the sniffer can determine the user name from the Kerberos ticket, it parses it.
3. If the sniffer cannot determine the user name from the Kerberos ticket, it sends the Kerberos ticket, along with a request for the database user, to the S-TAP. S-TAP checks to see if there is a Kerberos plugin configured. If there is a Kerberos plugin configured, S-TAP gives the ticket to the plugin and the plugin attempts to figure

out DB_USER from the ticket. It returns the database user name to S-TAP. (If not, then the database user name is not supplied and you do not see database user names in your reports.)
4. The sniffer can now populate the database user for that ticket, and correlate it with the rest of the database activity for that user in the Audit.

- Linux and UNIX systems: Kerberos authentication supported databases
  View the list of database servers that are supported for Kerberos authentication, and whether they require the Kerberos plugin.
- Linux and UNIX systems: Enabling the Kerberos plugin
- Linux and UNIX systems: Configuring the Kerberos plugin
  To monitor database traffic on a server that uses Kerberos authentication, including identifying the DB_USER, you must configure the guardtap.ini and guardkerbplugin.conf files appropriately.
- Linux and UNIX systems: Finding the Kerberos configuration parameters for Oracle
  For Oracle Kerberos, locate the Kerberos keytab and configuration file locations in sqlnet.ora.
- Linux and UNIX systems: Finding the Kerberos configuration parameters for Sybase
  Use the Sybase environment variables to get the Kerberos information.

Parent topic: Linux and UNIX systems: Configuring S-TAP

Linux and UNIX systems: Kerberos authentication supported databases

View the list of database servers that are supported for Kerberos authentication, and whether they require the Kerberos plugin.

Database	Kerberos plugin required?
DB2	No
Oracle	Yes
Cassandra	Yes
Sybase ASE	Yes
HBase	Yes
MongoDB	No
HDFS	No
Big SQL	No
Hive	Yes
Impala	No

Parent topic: Linux and UNIX systems: Kerberos-authenticated database traffic

Linux and UNIX systems: Enabling the Kerberos plugin

About this task

To enable the plugin, edit the guard_tap.ini configuration file and change the **kerberos_plugin_dir** entry to point to the directory where the plugin itself (libguardkerbplugin.so) and the configuration file (guardkerbplugin.conf) are located.

Procedure

1. For a default shell install: `kerberos_plugin_dir=/usr/local/guardium/guard_stap`
2. For a default GIM install: (exact path varies with software release in use) `kerberos_plugin_dir=/usr/local/IBM/modules/STAP/10.1.3_r101299_1-1495145548`
3. Default (plugin is disabled): `kerberos_plugin_dir=NULL`

Parent topic: Linux and UNIX systems: Kerberos-authenticated database traffic

Linux and UNIX systems: Configuring the Kerberos plugin

To monitor database traffic on a server that uses Kerberos authentication, including identifying the DB_USER, you must configure the guardtap.ini and guardkerbplugin.conf files appropriately.

About this task

All customization settings for the Kerberos plugin are located in the file guardkerbplugin.conf. The default contents of this file are:

```
# Kerberos values
KRB5RCACHETYPE=none
KRB5_KTNAME=/path/to/kerberos/krb5.keytab
KRB5_CONFIG=/path/to/kerberos/krb5.conf
# Plugin values
KRB5_PLUGIN_CCACHE=/path/to/kerberos/krb5cc_*
KRB5_PLUGIN_GSSAPI_LIBRARY=/path/to/lib/libgssapi_krb5.so
#KRB5_PLUGIN_DEBUG=0
```

Lines beginning with a #, as well as blank lines, are treated as comments and ignored. Invalid entries cause errors and prevent the Kerberos plugin from running.

When any configuration entry is changed, the S-TAP must be restarted for the updated values to take effect.

Configuration entries are:

KRB5RCACHETYPE

KRB5RCACHETYPE=none

KRB5_KTNAME
: This is the path to the keytab file; this can either be a keytab file already in use by the system, or one generated by Kerberos utilities specifically for use by the plugin. In general this file will have the name krb5.keytab. for example:
KRB5_KTNAME=/home/oracle11/krb5/keytabKRB5_KTNAME=/home/sybase15/kerberos/keytab

KRB5_CONFIG
: This is the path to the Kerberos configuration file in use by the system. In general this file is named krb5.conf. for example:KRB5_CONFIG=/home/oracle11/krb5/krb5.conf KRB5_CONFIG=/home/sybase15/kerberos/krb5.conf

KRB5_PLUGIN_CCACHE
: This is a wildcard path to where the Kerberos system cache files are located. For example: KRB5_PLUGIN_CCACHE=/tmp/krb5cc*
The value can also be a name if it is on the standard lib path, for example: KRB5_PLUGIN_CCACHE=<library name>.so
V10.1.4 and higher: Multiple paths can be specified, separated by a semicolon (';'), for example:
KRB5_PLUGIN_CCACHE=/home/sybase16/krb5cc*;/tmp/krb5cc*
Note: Specifying more files than needed (for instance, specifying /tmp/*) impacts performance.

KRB5_PLUGIN_GSSAPI_LIBRARY
: This is the location of the Kerberos GSSAPI dynamic library. On most systems this is named libgssapi_krb5.so.

  The location can be specified by a full path, for example:

  KRB5_PLUGIN_GSSAPI_LIBRARY=/usr/lib64/libgssapi_krb5.so KRB5_PLUGIN_GSSAPI_LIBRARY=/opt/freeware/lib64/libgssapi_krb5.so

  Alternately, if the library is located on the standard library search path for the system, you can specify only the file name, for example:

  KRB5_PLUGIN_GSSAPI_LIBRARY=libgssapi_krb5.so
  Note: Any libraries that are needed by the GSSAPI library (typically libkrb5.so, libk5crypto.so, libkrbsupport.so) must also be on the system.
  Important: If the Kerberos libraries are NOT in the standard library paths, you need to use the parameter KRB5_PLUGIN_GSSAPI_LIBRARY. Uncomment it and update its value with full path of libgssapi_krb5.so.

KRB5_PLUGIN_DEBUG
: This parameter is used for debugging the plugin only. For normal operation this line must be commented out, or plugin performance is impacted.

Procedure

1. In the guard_tap.ini file, change the value of kerberos_plugin_dir parameter to the full path to the Guardium S-TAP since that is where the plugin is located.
   - GIM installation: kerberos_plugin_dir=<guardium_base>/modules/STAP/current
   - S-TAP shell installation: kerberos_plugin_dir=<guardium_base>/guard_stap
2. Configure these in the guardkerbplugin.conf file that is also located in S-TAP installation directory:
   - KRB5_KTNAME=<full path to kerberos krb5.keytab file>
   - KRB5_CONFIG=<full path to kerberos krb5.conf file>
   - Optional parameters as described above. This configuration parameter for ticket cache might be required if the Kerberos plugin does not recognize the user. This parameter accepts wild cards as there is usually more than one cache file. V10.1.4 and higher: You can specify multiple paths, separated by colons. KRB5_PLUGIN_CCACHE=<full path to kerberos krb5cc_* files:additional full path to kerberos krb5cc_* files:etc>

   Note: In Guardium releases previous to V. 10.1.2, the parameters allow_weak_crypto = 1 and clockskew = 600 were required. In most cases these parameters are no longer required

Parent topic: Linux and UNIX systems: Kerberos-authenticated database traffic

Linux and UNIX systems: Finding the Kerberos configuration parameters for Oracle

For Oracle Kerberos, locate the Kerberos keytab and configuration file locations in sqlnet.ora.

About this task

Procedure

1. Enter: grep –i KERBEROS $ORACLE_HOME/network/admin/sqlnet.ora
   Output is similar to:

   ```
   SQLNET.AUTHENTICATION_KERBEROS5_SERVICE = oracle
   SQLNET.KERBEROS5_CONF = /home/oracle11/krb5/krb5.conf
   SQLNET.KERBEROS5_REALMS = /home/oracle11/krb5/krb.realms
   SQLNET.AUTHENTICATION_SERVICES= (BEQ,KERBEROS5)
   SQLNET.KERBEROS5_CLOCKSKEW = 600
   SQLNET.KERBEROS5_KEYTAB = /home/oracle11/krb5/keytab
   SQLNET.KERBEROS5_CONF_MIT = TRUE
   ```

2. To find the Kerberos cache parameter, enter: oklist|grep -i cache

   Output is similar to:

   ```
   Ticket cache: /tmp/krb5cc_500
   ```

Parent topic: Linux and UNIX systems: Kerberos-authenticated database traffic

Linux and UNIX systems: Finding the Kerberos configuration parameters for Sybase

Use the Sybase environment variables to get the Kerberos information.

Procedure

1. Enter: klist -k
   Output is similar to:

```
env|grep -i KRB
KRB5_KTNAME=/home/sybase15/kerberos/keytab
KRB5_CONFIG=/home/sybase15/kerberos/krb5.conf
```

2. To find the Kerberos cache parameter, enter: klist -c

   Output is similar to:

   ```
   Ticket cache: FILE:/tmp/krb5cc_533
   ```

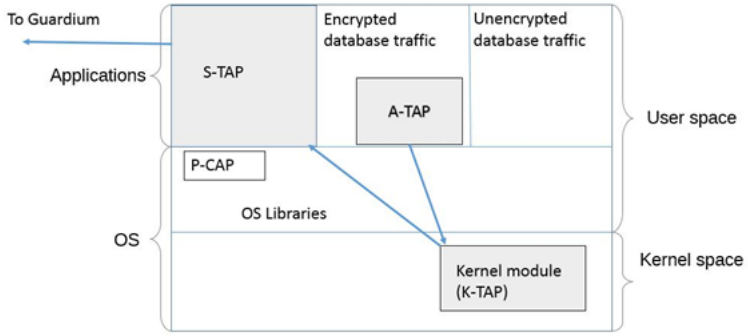
Parent topic: Linux and UNIX systems: Kerberos-authenticated database traffic

Linux and UNIX systems: A-TAP management

A-TAP is an application-level tap. A-TAP sits in the application layer to support monitoring of encrypted database traffic, which cannot be done in the kernel by K-TAP.

The A-TAP mechanism monitors communication between internal components of the database server. The data is unencrypted in the application layer, where A-TAP picks it up and sends to K-TAP. K-TAP is a proxy to pass data to S-TAP, and from there it is then sent to the Guardium collector.

This figure shows where A-TAP fits in with the overall architecture on the database server.



A-TAP is included in every S-TAP but must be specifically configured for each database that requires it.

When to use A-TAP

A-TAP is required when DBMS encryption in motion is used, but there may be other internal database implementation details such as shared memory that require it.

Informix and DB2 on Linux integrate with Guardium more closely using exits, and thus are the recommended method for shared memory support when applicable.

Restrictions: A-TAP is not supported in an environment where a 32-bit database is located on a 64-bit server.

Monitoring restrictions: A-TAP does not support redaction. Blocking is supported for Linux kernels at 2.6.36 or later releases.

- Linux and UNIX systems: Preparing for A-TAP configuration and maintenance
  Configuring and maintaining A-TAP requires coordination with both the database and system administrators.
- Linux and UNIX systems: A-TAP configuration and activation
  Configure and activate each A-TAP.
- Linux and UNIX systems: A-TAP activate, deactivate and DB stop, restart guidelines
  Understand when to activate and deactivate A-TAP, and stop or restart the DB.
- Linux and UNIX systems: guardctl utility commands for A-TAP
  The guardctl utility is the A-TAP management tool. Understand these commands before starting to work with A-TAPs.
- Linux and UNIX systems: guardctl return codes
  The guardctl error codes clarify error conditions that occur, in particular, when you are call the guardctl script to manage ATAP instances via another script.
- Linux and UNIX systems: Database-specific guardctl parameters
  Each database type has specific guardctl requirements.
- Linux and UNIX systems: Deactivating A-TAP
  You must deactivate A-TAP before upgrading the database OS. You also need to deactivate the ATAPs before upgrading or uninstalling STAP (whether or not it's installed via GIM, RPM, or shell installer).
- Linux and UNIX systems: Configuring and Activating A-TAP in Special Environments
  Zones, WPARs, Teradata, and Oracle require additional configuration.
- Linux and UNIX systems: Troubleshooting A-TAP configuration issues
  This section summarizes common mistakes made during A-TAP configurations, their symptoms, and how to avoid them.

Parent topic: Linux and UNIX systems: Configuring S-TAP

Linux and UNIX systems: Preparing for A-TAP configuration and maintenance

Configuring and maintaining A-TAP requires coordination with both the database and system administrators.

To configure and activate A-TAP, the following authorities are needed:

- Root access on the database server
- Authority to stop and restart the database

In addition, you must work with the DBA to get the required parameters to input into the utility. Details of the needed parameters are in Linux and UNIX systems: Database-specific guardctl parameters. For ongoing maintenance, your organization must have documented procedures in place to handle the activation and deactivation of A-TAP during OS and database upgrades. See Linux and UNIX systems: A-TAP activate, deactivate and DB stop, restart guidelines. For clustered environments, you need to configure and activate A-TAP on all nodes.

In most cases, use the Guardium guardctl utililty to activate, upgrade, or deactivate A-TAP. You can also implement a wrapper script to use guardctl as a utility interface to ATAP, which provides its own user experience. See Linux and UNIX systems: guardctl utility commands for A-TAP for details on the syntax and options of the guardctl utility.

Before you begin:

- Make sure that the S-TAP is installed and K-TAP is enabled.
- Ensure that you have the root privileges on the database server.
- Consult Linux and UNIX systems: Database-specific guardctl parameters for your database to ensure you have the parameters you need to run the utility.

Parent topic: Linux and UNIX systems: A-TAP management

Linux and UNIX systems: A-TAP configuration and activation

Configure and activate each A-TAP.

About this task

Prerequisite:

- S-TAP is installed.
- If the software is installed with GIM, verify that GIM_ROOT_DIR is the absolute path to the modules, for example /usr/local/guardium/modules.

Procedure

1. Verify ktap_installed=1 in the guard_tap.ini file.
2. Log off from all active database sessions and stop the database. It is very important that all processes with database admin user are stopped. For example, on oracle, issue ps -ef | grep oracle
3. As root user, authorize the database administrative user to log traffic using the guardctl utility with the authorize-user command as follows:
   `<guardium_base>/xxx/guardctl authorize-user <user-name>`

   shell installer with postgres authorize user
   ```
   /usr/local/guardium/guard_stap/guardctl authorize-user postgres Authorizing user 'postgres' to log traffic
   ```
   shell installer with postgres verify authorization
   ```
   /usr/local/guardium/guard_stap/guardctl is_user_authorized postgres User 'postgres' is authorized.
   ```
   GIM installation with postgres authorize user
   ```
   /usr/local/guardium/modules/ATAP/current/files/bin/guardctl authorize_user postgres Authorizing user 'postgres' to log traffic
   ```
   shell installer example with Greenplum authorize user
   ```
   /usr/local/guardium/guard_stap/guardctl authorize-user <gpadmin> Authorizing user '<gpadmin>' to log traffic
   ```
4. Once S-TAP is installed, add the Oracle OS user to the Guardium group (created by the S-TAP install script). This group is created by the S-TAP installer and users can be added by the system administrator using the usermod utility. Some platforms require the user to be completely logged off in order for this change to take effect. For example, where Oracle is the user ID of the OS user for the Oracle database and db2inst1 is the user ID of the OS user for DB2 database:

   ```
   usermod -a guardium oracle
   usermod -a guardium db2inst1
   ```

   - On Solaris, the user has to be completely logged off from the system.
   - No process should be running in the system under this user id.
   - In order to verify this, use the following command (assuming the user is Oracle):

     ```
     ps -efU oracle
     ```

   - If the output is empty, use the following command to add the user to the group:

     ```
     usermod -G dba,guardium oracle
     ```

   - If the user belongs to groups other than dba, they should be listed as well. The latter can be verified using the following command:

     ```
     id -a oracle
     ```

   - Once the user is added to the Guardium group, the encrypted traffic should be logged for this user.
5. Store the configuration parameters:
   a. See Linux and UNIX systems: Database-specific guardctl parameters to determine the parameters needed for your database type and platform.
   b. Store configuration for the database instance using the store-conf command of the guardctl utility as follows. As root user:
   `<guardium_base>/xxx/guardctl db_instance=<instance> [<name>=<value> ...] store-conf`

   shell installer Oracle on Linux store-conf
   ```
   /usr/local/guardium/guard_stap/guardctl --db-user=oracle11 --db-type=oracle --db-instance=on12rh60 --db-home=/home/oracle11/product/11.1.0/db_1 --db-version=11.2 store-conf
   ```
   GIM installation Oracle on Linux store-conf
   ```
   /usr/local/guardium/modules/ATAP/current/files/bin/guardctl db_instance=$ORACLE_SID db_home=$ORACLE_HOME db_type=oracle db_user=oracle12 db_version=12 store-conf
   ```
   shell installer Greenplum on Linux store-conf
   ```
   /usr/local/guardium/guard_stap/guardctl --db-user=<gpadmin> --db-type=greenplum -db-home=<db_user home directory> --db-instance=<greenplum> --db-base==<db_user home directory> store-conf
   ```

   Note: In Guardium V10.1 and higher, instrumentation is done automatically during activate; there is no explicit instrumentation.
6. Activate A-TAP.
   a. As root user: Enter `<guardium_base>/xxx/guardctl db_instance=<instance> activate`

   shell installer Oracle on Linux activate
   ```
   /usr/local/guardium/guard_stap/guardctl --db-instance=onrh60x activate
   ```
   GIM installation Oracle on Linux activate
   ```
   /usr/local/guardium/modules/ATAP/current/files/bin/guardctl --db-instance=onrh60x activate
   ```

shell installer Greenplum on Linux activate

```
/opt/guardium/guard_stap/guardctl --db-type=greenplum --db-home=/usr/local/greenplum-db-4.3.4.0 --db-user=gpadmin
--db-instance=greenplum --db-base=<db_user home directory> activate
```

Note: Optionally, you can activate A-TAP by using the Encryption checkbox of the inspection engine configuration in the Guardium GUI, though there are no advantages to activating it in the GUI. This option is not available for Linux platforms.

b. Confirm that the instances are activated using the list-active command of the guardctl utility: <guardium_base>/xxx/guardctl list-active

Example: `<guardium_base>/xxx/guardctl list-active oracle`

7. Restart the database server.

Parent topic: Linux and UNIX systems: A-TAP management

Linux and UNIX systems: A-TAP activate, deactivate and DB stop, restart guidelines

Understand when to activate and deactivate A-TAP, and stop or restart the DB.

Restart/load/activated requirements for A-TAP.

Scenario	Instructions
After installation of UNIX A-TAP in Oracle cluster environment	All database instances as well as all inter-cluster processes must be restarted
Before activating A-TAP	Stop database
After activating A-TAP	Restart database
Before deactivating A-TAP	Stop database
Before upgrading database (for example applying Fixpack)	Deactivate A-TAP
Before upgrading S-TAP	Deactivate A-TAP

Parent topic: Linux and UNIX systems: A-TAP management

Linux and UNIX systems: guardctl utility commands for A-TAP

The guardctl utility is the A-TAP management tool. Understand these commands before starting to work with A-TAPs.

guardctl utility

To use the guardctl utility, you must log in as **root**, since it requires superuser privileges. The guardctl utility is installed under <guardium_base>/guard_stap directory where <guardium_base> is the directory where Guardium software is installed. In the case of a GIM installation guardctl it is installed under <guardium_base>/modules/ATAP/current/files/bin.

Syntax

<guardium_base>/xxx/guardctl [<parameter>=value>] [<parameter>=<value> ...] <command> [-q | -v | -qv]

See parameters in Linux and UNIX systems: Database-specific guardctl parameters.

-q, -v, -qv flags

Guardium V10.1.3 and higher: Use these flags to manage the output:

- -q (quiet): suppress all output except name/value pairs
- -v (value pairs): add name/value pairs related to each command
- -qv: outputs name/value pairs only

The output depends on the type of command.

- Commands that take action across all configured instances
  - Print all name/value pairs for each instance except overall_rv and overall_msg
  - Print overall_rv name/value pair at end where value is
    - 0 (success) if and only if all report success
    - 1 (failure) if any report any failure
  - Print overall_msg name/value pair at end
  - Returns the value reported in the “overall_rv” name/value pair
- Commands that take action on a single instance
  - Print all name/value pairs except overall_rv and overall_msg
  - Returns the value reported in the “rv” name/value pair
- Commands that store parameters, print parameters, or check status
  - Does not print name/value pairs

Name/Value pairs output looks like:

```
db_instance: ${db_instance}
db_user: ${db_user}
db_base: ${db_base}
db_home: ${db_base}
db_version: ${db_version}
db_type: ${db_type}
is_active: ${is_active} (“yes” or “no”)
is_instrumented: ${is_db_instrumented} (“yes” or “no”)
msg: some string
rv: ${retval}
```

```
overall_rv: ${retval}
overall_msg: (string)
```

commands

Command	Description
activate	Activates A-TAP for the specified database instance using the stored parameters. v10.1.3 and higher: Outputs Name/Value pairs if -v or -qv specified. v10.1.3, activating an instance that's already active (whether DB is running or not) does not generate an error.
authorize-user	Adds the user to 'guardium' authorization group.
deactivate	Deactivates the A-TAP for the specified, single database instance. v10.1.3 and higher: Outputs Name/Value pairs if -v or -qv specified. From Guardium V10.1.3, deactivating an instance that's already inactive (whether DB is running or not) does not generate an error.
deactivate-all	Deactivates A-TAP for a specified list of database instances. If no database instances are specified, all active A-TAPs are deactivated. v10.1.3 and higher: Outputs Name/Value pairs for each instance, if -v or -qv specified. You can optionally specify the db-type to deactivate a group (e.g. all Oracle). For additional name/value pair, specify “overall_rv={0,1}” at end. Returns success (0) if rv=0 for every instance. Returns failure (1) if at least one instance reports rv != 0.
deinstrument	Removes instrumentation for the specified Oracle DB. Not required from v10.1 and higher. If deinstrumentation is required, it is done automatically during deactivate. V10.1.3 and higher: Outputs Name/Value pairs if -v or -qv specified. v10.1.3 and higher, deinstrumenting an instance that is not instrumented does not generate an error, even if the is DB running, regardless of activation status.
dump-params	Dumps current values of parameters
get-statistics	Get A-TAP statistics. Statistics includes information about which ATAPs are active, which are inactive, and which are in an incorrect in-between state (this shouldn't happen, it usually occurs when someone updates the DB while ATAP is active).
help	Default command, prints the list of supported commands, parameters and their default values.
instrument	Explicitly creates relinked instrumented Oracle. If instrumentation is required, it is usually done automatically during activate. Manual instrumentation is only required for Oracle versions <= 10 on AIX. Instrumenting an already instrumented instance returns an error. v10.1.3 and higher: Outputs Name/Value pairs if -v or -qv specified.
is-active	Returns 1 if there is at least one A-TAP activated instance. Otherwise, returns 0.
is-user-authorized	Checks whether the db-user (running A-TAP) is authorized to the guardium group, and can log database traffic to K-TAP/S-TAP.
list-active	Lists database instance user names of all active A-TAP database instances.v10.1.3 and higher: Outputs Name/Value pairs if -v or -qv specified.
list-configured	Lists database instances with configured but inactive A-TAPs. v10.1.3 and higher: Outputs Name/Value pairs if -v or -qv specified.
oracle-relink	Calls the utility provided by oracle to relink the DB binary.
prepare-libs	Prepares libraries for use in Zone/WPAR installation
repair	Run this command if the DB is (accidentally) upgraded while the A-TAP is active. It renames the -guard-original and -guard-instrumented files. Returns success on successful repair or if repair is not necessary. Does not touch the current DB executable. V10.1.3 and higher: Outputs Name/Value pairs if -v or -qv specified. From v10.1.4, it is called automatically on activate and deactivate.
restore-active-ataps	Restores the active state of the A-TAPs previously saved via save-active-ataps. If an instance fails to activate (due to DB running or some other error), then the remaining instances still attempt to activate. This command can be run multiple times without problem, since activating an already active instance is not an error. Introduced in v10.1.4.
save-active-ataps	Saves the configurations for the currently active A-TAPs in a single file so that they can be restored later to an active state. Useful prior to deactivate-all when preparing to upgrade DBs. Introduced in v10.1.4.
store-conf	Stores the configuration for a particular database instance
store-system-conf	Stores the system configuration parameters

Parent topic: Linux and UNIX systems: A-TAP management

Linux and UNIX systems: guardctl return codes

The guardctl error codes clarify error conditions that occur, in particular, when you are call the guardctl script to manage ATAP instances via another script.

Code	Description	Usage
0	success	Returned by every command. When returned in response to deactivate, all instances are deactivated When returned in response to is-active, there are no active instances
1	bad parameter	Returned by every command when a parameter is invalid or missing
2	is-active called on unrecognized instance	Returned by is-active when a db-instance specified is not known to guardctl and as such cannot be determined to be active or not
20	attempted to activate instance while database was running, but not yet active	Returned by activate to indicate that the DB instance is running, so activation could not take place
21	attempted to deactivate instance while database was running, but not yet inactive	Returned by deactivate to indicate that the DB instance is running, so deactivation could not take place
22	user is not authorized	Returned by instrument and activate to indicate that the db-user specified is not authorized as a member of the 'guardium' group. Run authorize-user to correct.

Code	Description	Usage
23	db-home parameter doesn't match db_install_dir parameter in guard_tap.ini	Returned by store-conf and activate to indicate that the current guard_tap.ini doesn't have an IE configured with a db_home that matches the db_install_dir ATAP parameter. One of those needs to be adjusted to the correct value or STAP may not run.
24	attempt to deactivate an instance where the executable is neither an ATAP executor or the instrumented binary	Returned by deactivate. This instance looks like it should be activated, but the binary isn't what it should be if it is. DB executable could have been updated while ATAP was active. Run the repair command to fix the issue and activate again.
25	attempt to activate atap when encryption=1 set in guard_tap.ini	Returned by activate when the encryption parameter is set to 1 in the IE. Do not activate with guardctl and use the encryption parameter in the ini.
26	db executable file not found	Returned by activate, deactivate, instrument, deinstrument, store-conf, prepare-libs, and repair. The DB executable is missing (e.g. the oracle binary itself is not in the path specified). Check the path parameters used when configuring the instance.
27	instrumentation required but not done	Returned by activate and store-conf when instrumentation is required, but has not already been done. Oracle instrumentation is now automatically done in most cases, but still needs to be manually specified for AIX and Oracle versions <= 10.
28	is-active reports instance is not active	Returned by is-active. Informational only. The db-instance specified is not active or if no instances were specified, no instances are active.
29	deactivate-all not complete success	Returned by deactivate-all when at least one active instance could not be deactivated.
30	is-instrumented reports instance is not instrumented	Not exported via command.
40	internal instrumentation error	Returned by instrument when instrumentation couldn't be completed.
41	internal instrumentation error	Returned by instrument when instrumentation couldn't be completed.
42	internal instrumentation error	Returned by instrument when instrumentation couldn't be completed.
43	instrumentation error, cannot save original binary	Returned by instrument when the -guard-original file already exists. Either A-TAP is currently active with instrumentation, or A-TAP is inactive but the instrumentation is still active. Deactivate and deinstrument before subsequent instrument and activate.
44	attempt to instrument while instance running and not already instrumented	Returned by instrument when DB instance is currently running. Stop DB instance before attempting to instrument again.
45	attempt to instrument while A-TAP is active and not already instrumented	Returned by instrument when A-TAP is already active, but instrumentation is not active. This can happen when switching from an Oracle configuration that doesn't require instrumentation to one that does. Deactivate A-TAP before attempting to instrument again.
46	attempt to instrument and already instrumented instance	Returned by instrument while instance is already instrumented. If instrumentation needs to be redone, deinstrument first.
93	unspecified error due to DB running not when activating, deactivating, or instrumenting (e.g. when running repair command)	
94	no atap library supporting this db	Returned by instrument, deinstrument, prepare-libs, activate, deactivate, repair, list-active, and list-configured. Usually indicates that an unknown error occurred.
95	system error, cannot find group	Returned by activate. The guardium group doesn't appear to be known to this system.
96	system error, cannot create group	Returned by authorize-user. The guardium group did not exist and an attempt to create the group failed.
97	filesystem error, cannot create directory or file, or insufficient space detected	
98	platform unsupported	Returned by instrument, deinstrument, prepare-libs, activate, deactivate, repair, list-active, list-configured, store-conf. The DB you're trying to use with ATAP is not supported on this platform (e.g. DB2, Informix, teradata, or mongo on anything but Linux, etc).
99	other unspecified error	

Parent topic: Linux and UNIX systems: A-TAP management

Linux and UNIX systems: Database-specific guardctl parameters

Each database type has specific guardctl requirements.

- Linux and UNIX systems: Oracle-specific guardctl parameters
  Use these guardctl parameters when configuring A-TAP for a Oracle database.
- Linux and UNIX systems: Sybase-specific guardctl parameters
  Use these guardctl parameters when configuring A-TAP for a Sybase database.
- Linux and UNIX systems: DB2-specific guardctl parameters
  Use these guardctl parameters when configuring A-TAP for a DB2 database, Linux only.
- Linux and UNIX systems: Informix-specific guardctl parameters
  Use these guardctl parameters when configuring A-TAP for a Informix database.
- Linux and UNIX systems: Postgres-specific guardctl parameters
  Use these guardctl parameters when configuring A-TAP for a Postgres database.

Parent topic: Linux and UNIX systems: A-TAP management

Linux and UNIX systems: Oracle-specific guardctl parameters

Use these guardctl parameters when configuring A-TAP for a Oracle database.

Example:

/usr/local/guardium/guard_stap/guardctl --db-user=oracle11 --db-type=oracle --db-instance=on12rh60 --db-home=/home/oracle11/product/11.1.0/db_1 --db-version=11.2 store-conf

Oracle required parameters

Required Parameter	Value	How to determine
db-user	Oracle user name	Use the database instance user name.
db_instance	Oracle instance name	Use the value from $ORACLE_SID
db_type	Oracle	
db_home	Where the database executable is installed .	
db_base	Database instance user home directory	The value for db_base must match the correct path for $ORACLE_BASE or the database instance user home directory. It cannot be ~DB_USER.
db_version	The database version	Run SQL > SELECT * FROM V$VERSION

Oracle optional parameters

Optional Parameter	Value	How to determine	When is it required
db_relink	No/ yes	A-TAP activation method	deprecated
db_use_instrumented	No/ yes	A-TAP activation uses relinked version of Oracle previously created with the instrument command of guardctl.	For S-TAPs at v10.1 and higher, instrumentation is done automatically with the “activate” command or through the Guardium UI. Instrumentation is required for: • Oracle 12 SSL all non-Windows platforms • Oracle 11.2 SSL on AIX • Oracle ASO and SSL on AIX prior to 11.2 For S-TAPs at 10.0, instrumentation is performed manually.
db_bits	32 or 64	DB instance architecture (32 for 32-bit, 64 for 64-bit)	Required only if A-TAP is not able to recognize the architecture.

Parent topic: Linux and UNIX systems: Database-specific guardctl parameters

Linux and UNIX systems: Sybase-specific guardctl parameters

Use these guardctl parameters when configuring A-TAP for a Sybase database.

Sybase required parameters

Example:

/usr/local/guardium/guard_stap/guardctl --db-user=sybase15 --db-type=sybase --db-instance=sn57rh7x --db-version=15 store-conf

Required Parameter	Value	How to determine
db_user	Sybase user name	Use the database instance user name.
db_instance	Sybase instance name	Sybase Server instance name. This parameter is used to name the ATAP instance within guardctl.
db_type	sybase	
db_version	The database version	As Sybase user: > select @@version > go

Sybase optional parameters

Optional Parameter	Value	How to determine	When is it required
db_home	Points to where the database is installed	Same as db_base	The basis for how we look for the DB binary. It can usually use the value of db_base, though it's immediately apparent when activating if it's wrong (guardctl complains about not finding the DB binary)

Optional Parameter	Value	How to determine	When is it required
db_base	Database instance user home directory	DB instance user home directory. this needs to match db_install_dir in some IE in the guard_tap.ini. Do not use the ~DB_USER shortcut, use the full path instead.	If you aren't specifying db_home separately, use the value for db_base as the value for db_home.
db_bits	32 or 64	DB instance architecture (32 for 32-bit, 64 for 64-bit)	Required only if A-TAP is not able to recognize the architecture.
db-tcp-min-port	0 to any integer	Low end of TCP port range to intercept	Specify if you want real IPs reported for encrypted sessions. There are potentially performance impacts in this mode as well as the added complication to the ATAP setup by specifying the port range. Leave blank to use the non-specific IP mode.
db-tcp-max-port	0 to any integer	High end of TCP port range to intercept	Specify if you want real IPs reported for encrypted sessions. There are potentially performance impacts in this mode as well as the added complication to the ATAP setup by specifying the port range. Leave blank to use the non-specific IP mode.

Parent topic: Linux and UNIX systems: Database-specific guardctl parameters

Linux and UNIX systems: DB2-specific guardctl parameters

Use these guardctl parameters when configuring A-TAP for a DB2 database, Linux only.

DB2 (Linux only) required parameters

Example:

/usr/local/guardium/guard_stap/guardctl --db-user=db2inst1 --db-type=db2 --db-instance=dn0rh7x6 --db-version=10.5 store-conf

Required Parameter	Value	How to determine
db_user	DB2 username	Points to the DB instance user name
db_instance	DB2 instance name	$ db2 LIST DATABASE DIRECTORY
db_type	db2	
db_version	The database version	As DB2 user: $ db2level

DB2 (Linux only) optional parameters

Optional Parameter	Value	How to determine	When is it required
db_home	Path where the DB version is installed	Same as db_base	
db_base	Database instance user home directory	Value for db_base must match the correct path DB instance user home directory. It cannot be ~DB_USER.	Where db_base is not same as db_home
db_bits	32 or 64	DB instance architecture (32 for 32-bit, 64 for 64-bit)	Required only if A-TAP is not able to recognize the architecture.
db2-shmsize	131072	DB2 shared memory size	When the value is different than the default
db2-c2soffset	61440	DB2 shared memory client area offset	When the value is different than the default
db2-header-offset	20	DB2 shared memory header offset	When the value is different than the default

Parent topic: Linux and UNIX systems: Database-specific guardctl parameters

Linux and UNIX systems: Informix-specific guardctl parameters

Use these guardctl parameters when configuring A-TAP for a Informix database.

Informix required parameters

Example:

/usr/local/guardium/guard_stap/guardctl --db-user=informix --db-type=informix --db-instance=in17rh7x --db-version=11.70 store-conf

Required Parameter	Value	How to determine
db_user	Informix username	Points to the DB instance user name
db_instance	Informix instance name	Informix Server instance name
db_type	informix	
db_version	The database version	As Informix user: dbaccess -V

Informix optional parameters

Optional Parameter	Value	How to determine	When is it required
db_home	Path where the DB version is installed	Same as db_base	
db_base	Home directory of db_user	DB instance user home directory. Value for db_base must match the correct path DB instance user home directory. It cannot be ~DB_USER.	Where db_base is not same as db_home
db_bits	32 or 64	DB instance architecture (32 for 32-bit, 64 for 64-bit)	

Parent topic: Linux and UNIX systems: Database-specific guardctl parameters

Linux and UNIX systems: Postgres-specific guardctl parameters

Use these guardctl parameters when configuring A-TAP for a Postgres database.

Postgres required parameters

Example:

/usr/local/guardium/guard_stap/guardctl --db-user=postgres --db-type=postgres --db-instance=guardium_qa --db-version=9.4 --db-base=/home/postgres94 store-conf

Required Parameter	Value	How to determine
db-user	Postgres username	Points to the DB instance user name
db_instance	Postgres instance name	Postgres Server instance name
db_type	postgres	
db_version	The database version	As Postgres user: pg_ctl --version

Postgres optional parameters

Optional Parameter	Value	How to determine	When is it required
db_home	Points to where the DB version is installed	Same as db_base	
db_base	Home directory of db_user	DB instance user home directory. Value for db_base must match the correct path DB instance user home directory. It cannot be ~DB_USER.	Where db-base is not same as db-home
db_bits	32 or 64	DB instance architecture (32 for 32-bit, 64 for 64-bit)	
db-tcp-min-port	0 to any integer	Low end of TCP port range to intercept	Using Real IPs
db-tcp-max-port	0 to any integer	High end of TCP port range to intercept	Using Real IPs

Parent topic: Linux and UNIX systems: Database-specific guardctl parameters

Linux and UNIX systems: Deactivating A-TAP

You must deactivate A-TAP before upgrading the database OS. You also need to deactivate the ATAPs before upgrading or uninstalling STAP (whether or not it's installed via GIM, RPM, or shell installer).

Procedure

1. Make sure the database is stopped. Log off from all active database sessions.
2. Deactivate A-TAP for the database:

   general example
   ```
   <guardium_base>/xxx/guardctl –db-instance=<instance-name> deactivate
   ```
   Greenplum example
   ```
   /opt/guardium/guard_stap/guardctl --db-type=greenplum --db-home=/usr/local/greenplum-db-4.3.4.0 --db-user=gpadmin --db-instance=greenplum --db-base=/usr/local/greenplum-db-4.3.4.0 deactivate
   ```
3. Alternately, deactivate all active instances by running:
   ```
   <guardium_base>/xxx/guardctl deactivate-all
   ```

Parent topic: Linux and UNIX systems: A-TAP management

Linux and UNIX systems: Configuring and Activating A-TAP in Special Environments

Zones, WPARs, Teradata, and Oracle require additional configuration.

- Linux and UNIX systems: Installing and activating A-TAP in Zones and WPARs environment
- Linux and UNIX systems: Deactivate and uninstall A-TAP in Zones and WPARs environment

- Linux and UNIX systems: Upgrading A-TAP in Zones and WPARs environment
- Linux and UNIX systems: Configure and activate A-TAP steps for Teradata database
- Linux and UNIX systems: Oracle configuration for A-TAP

Parent topic: Linux and UNIX systems: A-TAP management

Linux and UNIX systems: Installing and activating A-TAP in Zones and WPARs environment

About this task

Procedure

1. Install STAP/KTAP on the master/global Zone/WPAR by the normal method.
2. For Solaris Zones, for each sub-zone where Oracle is installed, make sure the Guardium device is mapped:
   - zoneadm -z <zonename> halt
   - zonecfg -z <zonename>
   - <zonename>> add device
   - <zonename>device> set match=/dev/ktap_xxx (for Solaris 10) (katp_xxx is the filename)
   - <zonename>device> set match=/dev/guard_ktap (for Solaris 11)
   - <zonename>device> end
   - <zonename>> verify
   - <zonename>> exit
   - zoneadm -z <zonename> boot
3. With multiple KTAP devices, repeat the steps for each KTAP device by using the name, ktap_xxxx (Solaris 10) or guard_ktap_x (Solaris 11).
4. Copy the entire A-TAP installation directory to a sub-Zone/sub-WPAR. Assuming Guardium software is installed on the master Zone/WPAR under /usr/local/guardium, and there exists a writable directory /usr/local with enough free space on the sub-Zone/sub-WPAR: On the master/global Zone/WPAR: `cd /usr/local; tar -cvf - guardium | ssh root@subzonehost 'cd /usr/local && tar -xvf -'`
5. Copy the A-TAP libraries to each sub-Zone/sub-WPAR, and activate it.
   - If an A-TAP is to be activated on the master Zone/WPAR, activate it normally using guardctl.
     Note: Activation must be done using guardctl; it cannot be done through enabling encryption box in the inspection engine section in GUI interface or by setting encryption=1 in the guard_tap.ini file.
   - If A-TAP will not be used on the master Zone/WPAR, use guardctl to prepare the libraries for use. On the master Zone/WPAR:
     `/usr/local/guardium/bin/guardctl --db_instance=<instance-name> --db_type=<database-type> --db_version=<database-version> prepare-libs`
     Note: After A-TAP activation, if the database indicates that libguard-xxx.so cannot be found, re-check this step.
6. Install and activate A-TAP for database instances using 1 through 5 on each desired sub-Zone/sub-WPAR.
   Note: A-TAP (guardctl) activation may complain and issue warnings about the following:
   - errors installing libraries under /usr/lib (since that directory belongs to the global/master zone)
   - not being able to change the guard_tap.ini to monitor oracle-guard instead of oracle (since the file is on the global zone)
   - not being able to restart S-TAP (since it is running only on the master zone)
7. Adjust the guard_tap.ini file in the master/global Zone/WPAR by manually editing the guard_tap.ini file..
   - Change the appropriate db_exec_path line:
     - For Oracle on Solaris: set db_exec_path to oracle-guard-original instead of oracle
     - For Oracle on AIX: set db_exec_path to oracle-guard-instrumented instead of oracle
   - Change the files and directories referenced in the IE definitions (db_install_dir and db_exec_file) so they are relative to the root directory of the WPAR and not the global partition. (IE order, tap_identifier string, etc, should be identical in all the guard_tap.ini files.)
8. Restart S-TAP.
9. For Solaris, verify the guard_ktap link and permissions on each sub-Zone. This must be performed as **root** from the global/master Zone.
   a. cd to the sub-zone device directory, for example: `cd /export/home2/zones/iris3/dev`
   b. Verify that the KTAP device exists (if it does not, there was a problem with the installation in 2): `ls -l ktap_*`
   c. Verify that the guard_ktap symbolic link exists: `ls -l guard_ktap`
   d. If it does not exist, create it. (Note: ktap_xxxxx is the device just listed): `ln -fs ktap_xxxx guard_ktap`

      For Example:

      ```
      -bash-3.00# ln -fs ktap_83164_0 guard_ktap
      -bash-3.00# ln -fs ktap_83164_1 guard_ktap1
      -bash-3.00# ln -fs ktap_83164_2 guard_ktap2
      -bash-3.00# ln -fs ktap_83164_3 guard_ktap3
      -bash-3.00# ln -fs ktap_83164_4 guard_ktap4
      -bash-3.00# ln -fs ktap_83164_5 guard_ktap5
      ```

   e. Make sure that guard_ktap and ktap_xxxxx are usable by everyone:

      ```
      chmod 0666 ktap_xxxxx_0
      chmod 0666 ktap_xxxxx_1
      chmod 0666 ktap_xxxxx_2
      chmod 0666 ktap_xxxxx_3
      chmod 0666 ktap_xxxxx_4
      chmod 0666 ktap_xxxxx_5
      chmod 0666 guard_ktap
      chmod 0666 guard_ktap1
      chmod 0666 guard_ktap2
      chmod 0666 guard_ktap3
      chmod 0666 guard_ktap4
      chmod 0666 guard_ktap5
      ```

Note: ATAP, WPAR and encrypted traffic: with a WPAR/Zone, encrypted traffic and decrypted traffic have different IPs when this traffic goes to the analyzer. Thus the db_user in WPAR/Zones is meaningless.

Parent topic: Linux and UNIX systems: Configuring and Activating A-TAP in Special Environments

Linux and UNIX systems: Deactivate and uninstall A-TAP in Zones and WPARs environment

About this task

Procedure

1. On every sub-Zone/sub-WPAR with A-TAP installed/active:
   a. Deactivate (and deinstrument if necessary, for Oracle on AIX) all A-TAPs using guardctl following the steps in Linux and UNIX systems: Deactivating A-TAP.
   b. Manually remove (`rm -rf`) the installation directory
   c. Manually remove the ATAP libraries: `find /usr/lib -type f -name 'libguard-*.so' | xargs rm -f`

   Note: Removing the libraries may give errors; these can be ignored.
2. Uninstall STAP/KTAP using the normal method
   a. Remove the libraries: `find /usr/lib -type f -name 'libguard-*.so' | xargs rm -f o`
   b. On Solaris, remove the ktap device from each zone's configuration:

```
zoneadm -z <zonename> halt
zonecfg -z <zonename>
<zonename>> info
```

   If a ktap device is found, remove it :

```
/<zonename> remove device match=/dev/ktap_xxxx (FOR SOLARIS 10)
/<zonename> remove device match=/dev/guard_ktap (FOR SOLARIS 11)
<zonename>> verify
<zonename>> exit
zoneadm -z <zonename> boot
```

   c. Remove the ktap device file and link from each sub-Zone/sub-WPAR device directory, for example:

```
/export/home2/zones/iris3/dev cd /export/home2/zones/iris3/dev
rm -f ktap_xxxx guard_ktap
```

   d. With multiple KTAP devices, repeat the steps for each KTAP device by using the name ktap_xxxx (Solaris 10) or guard_ktap_x (Solaris 11).

Parent topic: Linux and UNIX systems: Configuring and Activating A-TAP in Special Environments

Linux and UNIX systems: Upgrading A-TAP in Zones and WPARs environment

Procedure

1. For Solaris Zone:
   a. On the master/global-zone, remove the previously installed K-TAP device.

```
zoneadm -z <zonename> halt
zonecfg -z <zonename>
<zonename>> info
```

   b. If a K-TAP device is found, remove it.

```
/<zonename> remove device match=/dev/ktap_xxxx (for Solaris 10)
/<zonename> remove device match=/dev/guard_ktap (for Solaris 11)


<zonename>> verify
<zonename>> exit
zoneadm -z <zonename> boot
```

   c. For Solaris sub-zones, remove the previous K-TAP device file and link from sub-zone device directory. Go to the sub-zone device directory, for example /export/home2/zones/iris3/dev.

```
cd /export/home2/zones/iris3/dev
rm -f ktap_xxxx guard_ktap
```

2. For Solaris Zone:
   a. On the master/global-zone, add the new K-TAP device to the zone configuration:

```
zoneadm -z <zonename> halt
zonecfg -z <zonename>
<zonename>> add device

<zonename>device> set match=/dev/ktap_xxxx (for Solaris 10)
<zonename>device> set match=/dev/ktap_xxxx (for Solaris 11)

<zonename>device> end
<zonename>> verify
<zonename>> exit
zoneadm -z <zonename> boot
```

   b. Add the guard_ktap link and change permission. Go to the sub-zone device directory, for example: sub-zone device directory=/export/home2/zones/iris3/dev

```
cd /export/home2/zones/iris3/dev
ln -fs ktap_xxxx guard_ktap
chmod 0666 ktap_xxxx
chmod 0666 guard_ktap
```

   c. Since there are multiple ktap devices, repeat steps for each K-TAP device by using the name ktap_xxxx_x(solaris 10) or guard_ktap_x (solaris 11)
3. For AIX WPARs: on WPARs, change permission on K-TAP devices. Go to the WPARs device directory, for example: wpars device directory=/wpars/odin3/dev

```
ln -fs ktap_xxxx guard_ktap
chmod 0666 ktap_xxxx
```

```
chmod 0666 guard_ktap
```

Parent topic: Linux and UNIX systems: Configuring and Activating A-TAP in Special Environments

Linux and UNIX systems: Configure and activate A-TAP steps for Teradata database

Step 1: Determine the user running gtwgateway and the path

For Example:

su11u1x64-tera:~ # ps -ef | grep gtwgateway

teradata 5000 4608 0 Jan03 ? 00:00:05 /usr/tgtw/bin/gtwgateway

root 20128 20063 0 12:35 pts/0 00:00:00 grep gtwgateway

gtwgateway runs as user teradata

Set parameter *--db-user=teradata* to guardctl

Path to gtwgateway is /usr/tgtw/bin/gtwgateway. This is the default value for the parameter tdc_gtwgateway and as such does not need to be specified.

Otherwise, the parameter should be *--tdc_gtwgateway=/usr/tgtw/bin/gtwgateway*

Step 2: Determine the path to pdemain

Typically, this will be /usr/pde/bin/pdemain

For Example:

su11u1x64-tera:~ # ps -ef | grep pdemain

root 4608 1 0 Jan03 ? 00:00:25 pdemain –debug

su11u1x64-tera:~ # ls -l /proc/4608/exe

lrwxrwxrwx 1 root tdtrusted 0 2015-01-03 01:20 /proc/4608root 20620 20063

0 12:40 pts/0 00:00:00 grep pdemain/exe ->

/opt/teradata/tdat/pde/15h.00.00.07/bin/pdemain

Checking the inodes for this file and /usr/pde/bin/pdemain, we see that they are the same.

su11u1x64-tera:~ # ls -li /opt/teradata/tdat/pde/15h.00.00.07/bin/pdemain

1638875 -r-xr-xr-x 1 teradata tdtrusted 1294666 2014-01-22 01:40

/opt/teradata/tdat/pde/15h.00.00.07/bin/pdemain

su11u1x64-tera:~ # ls -li /usr/pde/bin/pdemain

1638875 -r-xr-xr-x 1 teradata tdtrusted 1294666 2014-01-22 01:40

/usr/pde/bin/pdemain

Since the inodes are the same and the default value for *--db-home=/usr/pde*, the parameter in this case does not need to be specified. Otherwise, you can specify --db-home=/opt/teradata/tdat/pde/15h.00.00.07 or --db-home=/usr/pde since bin/pdemain in both paths is the same file hardlinked in this case.

Step 3: Stop the Teradata instance

For Example:

su11u1x64-tera:~ # /etc/init.d/tgtw stop

tgtw Shutdown complete

su11u1x64-tera:~ # /etc/init.d/tpa stop

PDE stopped for TPA shutdown

Step 4: Authorize the DB user to the Guardium group

For Example:

/usr/local/guardium/guard_stap/guardctl --db-instance=teradata authorize-user

Step 5: Store the configuration for A-TAP using the parameters determined in steps 1 and 2.

For Example:

/usr/local/guardium/guard_stap/guardctl --db-instance=teradata

--tdc_gtwgateway=/usr/tgtw/bin/gtwgateway --db-type=teradata

--db-home=/opt/teradata/tdat/pde/15h.00.00.07 --db-user=teradata store-conf

Step 6: Activate A-TAP

For Example:

/usr/local/guardium/guard_stap/guardctl --db-instance=teradata activate

Step 7: Restart the Teradata instance

For Example:

su11u1x64-tera:~ # /etc/init.d/tpa start

Teradata Database Initiator service is starting...

Teradata Database Initiator service started successfully.

su11u1x64-tera:~ # /etc/init.d/tgtw start

tgtw Startup complete

Parent topic: Linux and UNIX systems: Configuring and Activating A-TAP in Special Environments

Linux and UNIX systems: Oracle configuration for A-TAP

A-TAP Procedure when working with Oracle Patch Installations

Oracle patches may invoke relink and will replace the Oracle executable, causing the A-TAP to stop functioning.

The correct procedure is:

1. Make sure all A-TAP instances are deactivated
2. Apply Oracle patch(es).
3. Activate A-TAP

However, in case A-TAP was not properly deactivated prior to Oracle patch installation, DO NOT try to deactivate it after patch installation. Instead follow these steps:

1. Check if A-TAP IS OK.

```
grep guardium $ORACLE_HOME/bin/oracle >& /dev/null && echo "ATAP IS OK"
```

   a. If `ATAP IS OK` is displayed, the A-TAP is still active and there is no need to do anything.
   b. If `ATAP IS OK` is NOT displayed, remove $ORACLE_HOME/bin/oracle-guard and activate the A-TAP.

In case everything else fails:

- Remove $ORACLE_HOME/bin/oracle-guard
- Run relink all

A-TAP Problems And Solutions associated with Oracle Permissions

Several problem may occur that have to do with user and group permissions.

- In 'BEQUEATH' access from the user other than the one that installed the database the permissions have to be set manually:
  - add user running sqlplus to group 'guardium'
  - open the read permissions 'chmod a+rx' on the following two directories:

    ```
    /usr/local/guardium/xxx/etc/guard
    /usr/local/guardium/xxx/etc/guard/executor
    ```

  - make sure that the SUID and SGID bits are on ${ORACLE_HOME}/bin/oracle.
    - If not, run the command chmod ug+s ${ORACLE_HOME}/bin/oracle')
- If the UID or EUID are not members of OWNER group GID, the reason for permission denied is that the user matching UID or EUID does not belong to group matching OWNER GID.
- To make it easier, not having to handle different OS syntaxes for adding users and groups, while disabling the automatic addition to group Guardium, two commands are available within guardctl which can be used irrespective of the method you use to activate ATAP (i.e. guardctl or guard_tap.ini):
  - #/path/to/guardium/bin/guardctl is-user-authorized
  - #/path/to/guardium/bin/guardctl authorize-user ...

Note: Group Guardium can be removed on most OS's with groupdel guardium. However, after removal, only the guard_ktap_loader parameter can correctly re-create it and change the K-TAP device permissions.

Parent topic: Linux and UNIX systems: Configuring and Activating A-TAP in Special Environments

Linux and UNIX systems: Troubleshooting A-TAP configuration issues

This section summarizes common mistakes made during A-TAP configurations, their symptoms, and how to avoid them.

Table 1. Oracle Common Mistakes

Symptoms	Mistake	Platform	Error Message(s)	How to Avoid
Activation command fails.	Wrong db_home parameter	All		Always specify the value of $ORACLE_HOME as db_home name.
Activation command fails.	OS user logged in	All		Always make sure the OS user is not logged in. Use w command to see which users are logged in.

Symptoms	Mistake	Platform	Error Message(s)	How to Avoid
Database does not start.	Wrong instance name	All	Failed to execute oracleon1jumbo-guard: No such file or directory: No such file or directory ERROR: ORA-12547: TNS:lost contact	Always specify the value of $ORACLE_SID as db_instance name.
Traffic is not logged.	Wrong or missing db_version	AIX		Always specify numeric version (for example, 10.2 or 9.2). The version number can have only one digit after the decimal point.
Fails to activate.	Missing Oracle-guard-instrumented	AIX	Missing Oracle-guard-instrumented.	Instrument command must be run first to create a re-linked instrumented Oracle executable
Error during ATAP activation	Insufficient disk space, install exits		Matching module found - oracle is supported by /ngs/lpp/guardium/modules/ATAP/current/files/lib/libguard-atap-oraclesta tic-any Testing for disk space... cp : 0653-447 Requested a write of 131072 bytes, but wrote only 126976. Insufficient disk space - please delete some files and try again.	Clean oracle files and retry. Change db_space=8 to db_space=1
guard_stap log shows that guard-atap-ctl failed	GIM_ROOT_DIR not set to absolute path to the modules, for example /usr/local/guardium/modules			When activating A-TAP through the guard_tap.ini file, encryption=1 silently fails. This is especially important when running guard_stap manually - be sure you have defined this environment variable when running guard_stap.

Table 2. DB2 Common Mistakes

Symptoms	Mistake	Platform	Error Message(s)	How to Avoid
Traffic is not logged.	Wrong or missing db2_* parameter	Linux		See how to determine DB2 parameters in Linux and UNIX systems: Inspection engine parameters

Table 3. Informix Common Mistakes

Symptoms	Mistake	Platform	Error Message(s)	How to Avoid
Traffic is not logged properly.	Wrong or missing db_version	Linux		Always specify numeric version (e.g. 7 or 11).

Parent topic: Linux and UNIX systems: A-TAP management

Linux and UNIX systems: Using Exit libraries

Exit libraries embed a Guardium library into the database, using the exit mechanism. The exit library, or module, communicates directly with the Guardium S-TAP to forward database traffic.

- Linux and UNIX systems: DB2 Exit integration with S-TAP
  The DB2 exit mechanism enables Guardium to pick up all DB2 traffic, whether encrypted or not and whether local or remote. It does not require A-TAP or K-TAP.
- Linux and UNIX systems: Informix Exit integration with UNIX S-TAP
  The Informix Exit ifxguard utility (Informix 12.10 and higher) monitors connections to your Informix databases.
- Linux and UNIX systems: Teradata Exit integration
  The Teradata exit module enables Guardium to pick up Teradata traffic, whether encrypted or not and whether local or remote. It does not require A-TAP or K-TAP.

Parent topic: Linux and UNIX systems: Configuring S-TAP

Linux and UNIX systems: DB2 Exit integration with S-TAP

The DB2 exit mechanism enables Guardium to pick up all DB2 traffic, whether encrypted or not and whether local or remote. It does not require A-TAP or K-TAP.

About this task

DB2 exit embeds a Guardium library into DB2 via the DB2_Exit mechanism. The DB2_Exit communicates directly with the Guardium S-TAP to forward all DB2 traffic, whether encrypted or not, and both local and remote. DB2 exit captures TCP as well as SHM traffic. Enabling UID chain with DB2 consumes much less CPU resource than KTAP and UID chain.

The DB2 exit library is a dynamic linked library. The DB2 database loads during database starts.

DB2 exit supports firewall (from STAP 10.1.2, also requires DB2 version 10.1 or later), terminate, and UID chain.

If there is no other Inspection Engine (IE) on the S-TAP that requires K-TAP, then you don't need to load K-TAP: set ktap_installed=0 in guard_tap.ini, or with GIM set ktap_enabled to no, in the GIM dialog for that STAP. You can upgrade the Linux OS and the STAP without being concerned about K-TAP module compatibility. However, if there is another IE in the S-TAP that requires the K-TAP module, you must ensure that a compatible K-TAP module is available when you upgrade your Linux version.

Limitations:

- DB2 Exit does not support Guardium data masking (scrub/redact)
- The Guardium firewall (V10.1.2 and later) requires DB2 version 10.1 or later
- Stored Procedures: DB2 Exit monitors stored procedures. Since Guardium does not know what is in the stored procedure, SQL from inside the procedure is not captured.

When upgrading STAP and DB2

1. Stop the DB2.
2. Upgrade STAP.
3. Copy latest db2 exit lib to DB2 commexit directory.
4. Start the DB2.

When patching STAP

1. Stop the DB2.
2. Patch the DB2 Database
3. In case the DB2 configuration was overwritten you need to re-enable using `db2 UPDATE DBM CFG USING COMM_EXIT_LIST libguard_db2_exit_64`
4. Start the DB2.

The Guardium installer has two versions of the DB2 EXIT library: 32- and 64-bit. Use the one that matches your installed DB2. Both versions are in the Guardium installation directory in the lib sub-directory. On Linux servers, the 64-bit version is in lib64.

DB2 versions V101FP4 and V105FP3 support UID chain.

Library names

- libguard_db2_exit_32.so
- libguard_db2_exit_64.so

Procedure

1. Determine the DB2's bitwise. Log in as `root` and run `db2level`. The output is similar to
   `DB21085I Instance db2inst1 uses 64 bits and DB2 code release SQL09070, with level identifier 08010107`
2. Locate the communication buffer exit library location (DB2PATH)
   a. Log in as DB2 user `trip`
   b. In the DB2 clp, run db2 `get database manager configuration`
   c. In the output, look for default database path: Default database path
   `(DFTDBPATH) = /DB2/trip`
   DFTDBPATH is the value you need for the environment parameter DB2PATH.
3. Set up the DB2 Exit library.
   a. Log in as user `root`
   b. Set the environment parameter: `# export DB2PATH=/DB2/trip`
   c. Create the directory by entering one of these commands. (This is done only the first time the library is installed, as the directory does not exist)
      - mkdir $DB2_PATH/sqllib/security/plugin/commexit
      - mkdir $DB2_PATH/sqllib/security64/plugin/commexit
   d. Change permission: `# chown ${DB2 user}:${DB2 group} $DB2PATH/security64/plugin/commexit`
   e. Copy Guardium's libguard file to commexit by entering one of:

   ```
   # cp /opt/IBM/guardium/module/modules/STAP/libguard_db2_exit_64.so $DB2PATH/security64/plugin/commexit
   # cp /opt/IBM/guardium/module/modules/STAP/libguard_db2_exit_64.so $DB2PATH/security/plugin/commexit
   ```

   where $DB2_PATH is the db2 installation directory.

   If the copy fails with the error `....: Text file busy`, remove the file from the target directory, make a copy and repeat.

   f. Change permission by entering one of:

   ```
   # chown ${DB2 user}:${DB2 group} $DB2PATH/security64/plugin/commexit/libguard_db2_exit_64.so
   # chown ${DB2 user}:${DB2 group} $DB2PATH/security/plugin/commexit/libguard_db2_exit_64.so
   ```

4. Add the DB2 instance to the Guardium group. The Guardium group is created during S-TAP installation. This requirement increases the security of shared memory regions that are created by the S-TAP.
   a. If DB2 user is 'trip', verify if 'trip' has been authorized already. Use guardctl under the ATAP folder.

   ```
   # /opt/IBM/guardium/module/modules/ATAP/10.1.0_r88469_1-1468880597/files/bin/guardctl is-user-authorized trip
   User 'trip' is authorized.
   ```

   b. If the user trip is not authorized, authorize it now:

   ```
   # /opt/IBM/guardium/module/modules/STAP/10.1.0_r88469_1-1468880597/guardctl authorize-user trip
   guardctl authorize-user guardium
   User 'guardium' is already authorized.
   ```

5. Enable db2 exit in DB2 (so it will send the SQL traffic to the S-TAP).
   a. Log in as db2 user and use the db2 clp commands to enable:
   `db2 UPDATE DBM CFG USING COMM_EXIT_LIST libguard_db2_exit_64`
   b. Once enabled, db2 sends SQL traffic to the STAP. Verify if db2 exit is successfully enabled by entering

   ```
   db2 get database manager configuration
   ```

   The output should include

   ```
   Communication buffer exit library list (COMM_EXIT_LIST) = libguard_db2_exit_64
   ```

6. Restart DB2.

a. Login as `db2 user` and enter:

```
# db2stop force; ipclean; db2start
```

b. Verify the response includes:

```
The DB2START command completed successfully
```

c. If the restart was unsuccessful, stop db2 exit to clear any warnings in DB2 by entering:

```
db2 UPDATE DBM CFG USING COMM_EXIT_LIST NULL
```

then restart by entering

```
db2 restart
```

d. If not, check the log file for clues: ~/sqllib/db2dump/db2diag.log

7. If A-TAP is not activated: Configure STAP for DB2_EXIT. (If A-TAP is activated, continue with 8)
   a. Configure the IE for DB2 as usual either in the guard_tap.ini or via GIM. For ease of identification, set db_type=db2.
   b. Unix-type platforms only: Verify that the parameter db_install_dir for DB2_EXIT IE is set to the value of $DB2_HOME or $HOME of DB2 environment variable.
   c. Windows only: Add the instance_name=Service_name. Determine the service name by using the db2tap utility in the S-TAP installation folder, or from the control panel. Set the instance name to the portion of the service name that follows the second dash (-) delimiter. For example, if the service name in the control panel is DB2 - DB2COPY1 - DB2-01-0, set INSTANCE_NAME to DB2-01-0
   d. Restart S-TAP with new configuration.
8. If A-TAP was activated when you started.
   a. Stop the DB2 by entering
   ```
   # db2stop force; ipclean
   ```
   b. Deactivate the A-TAP by entering
   ```
   # /opt/IBM/guardium/module/modules/ATAP/10.1.0_r88469_1-1468880597/files/bin/guardctl db_instance=<db_instance> [--force-action=yes ] deactivate
   ```
   c. Configure the IE for DB2 as usual either in the guard_tap.ini or via GIM . For ease of identification, set db_type=db2.
   d. Unix-type platforms only: Verify that the parameter db_install_dir for DB2_EXIT IE is set to the value of $DB2_HOME or $HOME of DB2 environment variable.
   e. Windows only: Add the instance_name=Service_name. Determine the service name by using the db2tap utility in the S-TAP installation folder, or from the control panel. Set the instance name to the portion of the service name that follows the second dash (-) delimiter. For example, if the service name in the control panel is DB2 - DB2COPY1 - DB2-01-0, set INSTANCE_NAME to DB2-01-0
   f. Restart S-TAP with new configuration.
9. Set up Zones/WPARs.
   a. Copy the S-TAP to the Zones/WPARs.
      i. On the master/global Zone/WPAR: (assuming Guardium software is installed on the master Zone/WPAR under /usr/local/guardium, and there exists a writable directory /usr/local with enough free space on the sub-Zone/sub-WPAR), enter:

      ```
      cd /usr/local
      tar -cvf - guardium | ssh root@subzonehost 'cd /usr/local && tar -xvf -'
      ```

      ii. On Zone/WPARs, add DB2_EXIT IE in the guard_tap.ini with:
      - -- ktap_installed = 0
      - -- tap_run_as_root = 1
      - -- tap_ip = zones/WPAR local IP address
      - No other IEs should be specified in order to start S-TAP on the zone.

   b. Create /var/guard directory.
   c. Start the S-TAP.
      - on WPARs, manually copy/add the utap server entry in inittab file
      - On Solaris zone use the command svcadm -v enable guard_utap
   d. If relevant, configure the tap_debug_output_level.
      Note: **Impact of debug logging on the database server:** The logging is done by the DB2 Exit module. This module is loaded by DB2 and the diagnostics are piped to the log files. Since the database server is performing the actual logging, there is some impact, depending on how much logging is done. Remember that S-TAP logging is meant to be used as part of troubleshooting and not a standard feature, so the impact is only when logging is turned on.
      - When S-TAP log level = 10, debug info is logged into both S-TAP log and db2_exit log (db2diag.log)
      - When S-TAP log level = 11, debug info is only logged into db2_exit log (db2diag.log)

Note: In a WPAR environment when running discovery, if the instance name is the same on both slave zone and master zone, then only one Inspection Engine entry is added that belongs to the master zone.
Note: When changing tap_identifier in the inspection engine, in order for the change to take effect with Informix exit or DB2 exit, the database must be restarted. With ATAP enabled, the database has to be stopped, ATAP deactivated, reactivated, and finally the database started again. For Informix exit, stop ifxguard, then restart the database, then start ifxguard.

Parent topic: Linux and UNIX systems: Using Exit libraries

Linux and UNIX systems: Informix Exit integration with UNIX S-TAP

The Informix Exit ifxguard utility (Informix 12.10 and higher) monitors connections to your Informix databases.

About this task

With Informix Exit, Guardium v.10 and higher can audit all protocols of Informix SQL activities. This includes TCP, Shared Memory and Named Pipe protocols. It supports all Guardium features (S-gate, UID chain, Redaction, query-rewrite, etc). On Linux platforms, you can use Informix Exit instead of ATAP to capture shared memory traffic. Informix exit captures encrypted traffic.

A shared library, Informix Exit, is part of the Guardium Unix S-TAP installation. S-TAP includes 32bit and 64bit.so. They are located under <guardium_installation_directory>/guard_stap, for example:
/usr/local/guardium/guard_stap /usr/local/guardium/guard_stap/libguard_informix_exit_32.so
/usr/local/guardium/guard_stap/libguard_informix_exit_64.so.

Note: When changing tap_identifier in the inspection engine, in order for the change to take effect with Informix exit or DB2 exit, the database must be restarted. With ATAP enabled, the database has to be stopped, ATAP deactivated, reactivated, and finally the database started again. To make tap_identifier work for DB2 exit and Informix exit, make sure db_install_dir is exactly the same with $HOME value in the database. Also, the database needs to restart to pick up the tap_identifier value. For Informix exit, stop ifxguard, then restart the database, then start ifxguard.

Procedure

1. Login as user informix to the database and locate its instance name (INFORMIXSERVER) and its installation directory (INFORMIXDIR) by running these Unix commands:
   ```
   $ echo $INFORMIXSERVER
   INFORMIXSERVER=test117
   $ echo $INFORMIXDIR
   INFORMIXDIR=/home/informix
   ```
2. Install and start up the S-TAP in the db host. See Linux and UNIX systems: Install the S-TAP agent.
3. As user root, make sure the user informix is in the guardium group, for example,
   `/usr/local/guardium/bin/guardctl authorize-user informix`
   or with unix
   `# chgroup users=informix guardium` (AIX only).
4. Login as user informix and enter:
   `$ iduid=501(informix) gid=205(informix) groups=215(guardium)`
5. As user informix, copy the correct informix exit library from the guard_stap directory to the informix user's lib directory, for example,
   `cp /usr/local/guardium/guard_stap/libguard_informix_exit_64.so $INFORMIXDIR/lib/libguard_informix.so`
6. Set up ifxguard. Create a config file under $INFORMIXDIR/etc/ifxguard.$INFORMIXSERVER with these lines:
   ```
   NAME ol_informix1210
   WORKERS 2
   LIBPATH /home/informix/12.10.FC6/lib/libguard_informix.so
   DEBUG 1
   LOGFILE /home/informix/12.10.FC6/etc/ifxguard.msg.txtg.txt
   ```
   Note: INFORMIXDIR=/home/informix/12.10.FC6
7. Bring up ifxguard as user informix
   a. Make sure Informix database server is online (onstat -).

      ```
      $ id
      uid=501(informix) gid=205(informix) groups=215(guardium) $ onstat -
      IBM Informix Dynamic Server Version 12.10.FC6 -- On-Line -- Up 6 days 00:22:25 -- 253104 Kbytes
      ```

   b. If the ifxguard config file is setup as described above, bring up ifxguard with:

      ```
      $ ifxguard
      15:20:17 ifxguard set instance name ol_informix1210
      Starting ifxguard ol_informix1210 ...
      check log file: /home/informix/12.10.FC6/etc/ifxguard.msg.txt
      ```

      You should not see any errors. In case of error, check the file indicated in LOGFILE.

   c. If the ifxguard config file is not under $INFORMIXDIR/etc, specify the file's full path with -c option, - for example

      ```
      $ ifxguard -c /mnt/conf/ifxguard.ol_informix1210
      ```

   d. If ifxguard config file is not set up at all, you can still bring up the agent but must specify the .so library using full-path with -p option and message log file with -l option, for example

      ```
      $ ifxguard -p /home/informix/12.10.FC6/lib/libguard_informix.so -l  home/informix/12.10.FC6/etc/ifxguard.msg.txt
      ```

   e. If there are errors, check the log file indicated in LOGFILE.
8. Make sure ifxguard and S-TAP is up running using ps -ef:
   ```
   $ ps -ef|grep guard
   root 15401210 1 1 15:14:11 - 0:00
   /usr/local/guardium/guard_stap/guard_stap /usr/local/guardium/guard_stap/guard_tap.ini
   informix 22609968 1 0 15:20:17 - 0:00 ifxguard
   ```

   You should see the following msg in /home/informix/12.10.FC6/etc/ifxguard.msg.txt.

   ```
   Wed Feb  3 15:20:17 2016
   15:20:17 INFORMIX-ESQL Version 12.10.FC6
   15:20:17 Build Number:  N253
   15:20:17 Build Host:    cxp01007
   15:20:17 Build OS:      AIX 6.1
   15:20:17 Build Date:    Wed Nov 4 21:55:13 CST 2015
   15:20:17 GLS Version:   glslib-6.00.FC7
   15:20:17
   15:20:17 Starting ifxguard ol_informix1210 ...
   15:20:17 DEBUG[TID1]:Password File /home/informix/12.10.FC6/etc/ passwd_file failed error:No
   such file or directory [2] [onguard_main.c:onguard_pw_init:518]
   15:20:17 DEBUG[TID1]:ifxguard ol_informix1210 connect to trusted host, Password Manager is i
   gnored. [onguard_main.c:onguard_run:2391]
   15:20:17 pcbms = 110023688, spt_fn=fffffffffff300

   15:20:17 CBMS: cbms_initialize()
   15:20:17 Attached /.guard_writer0 shmem[0] 8001000a0000de8
   15:20:17 Attached /.guard_writer1 shmem[1] 8001000a0000eb8
   15:20:17 Attached /.guard_writer2 shmem[2] 8001000a0000f88
   15:20:17 Attached /.guard_writer3 shmem[3] 8001000a0001058
   15:20:17 Attached /.guard_writer4 shmem[4] 8001000a0001128
   15:20:17 Attached /.guard_writer5 shmem[5] 8001000a00011f8
   15:20:17 Attached /.guard_writer6 shmem[6] 8001000a00012c8
   15:20:17 Attached /.guard_writer7 shmem[7] 8001000a0001398
   15:20:17 Attached /.guard_writer8 shmem[8] 8001000a0001468
   15:20:17 Attached /.guard_writer9 shmem[9] 8001000a0001538
   ```

```
15:20:17 Attached to /.guard_reader
15:20:17 guard_conf_message=70000000149b000: my_ip=96eb8b7, intercept_type=1c, debug_level=0
, ignore_response_db_list=NONE
15:20:17 comm exit shm initialization successful
15:20:17 DEBUG[TID1]:new daemon pid is 22609968 [onguard_main.c:onguard_daemonize:2350]
15:20:17 ifxguard ol_informix1210 started
15:20:17 The connection attempt from  ifxguard ol_informix1210 to server ol_informix1210 suc
ceeded. Process id: 22609968:258
15:20:17 Attached to /.guard_reader
15:20:17 The connection attempt from  ifxguard ol_informix1210 to server ol_informix1210 succeeded. Process id: 22609968:515
```

You can ignore the **password file error**. It's a debug message. You can define one password file and run 'onpassword' to encrypt it. Ifxguard reads user informix's password from the encrypted file and connects to Informix Dynamic Server (IDS). If the password file is not defined, then ifxguard connects to IDS as trusted host connection (no password).

9. Add the INFX_EXIT inspection engine either via GRDAPI (create_stap_inspection_engine) or the GUI (Manage > Activity Monitoring > S-TAP Control) with these specific Informix values:

Parameter in GUI	Parameter in GRDAPI	Value
Protocol	protocol	Informix Exit
DB Install Dir	dbInstallDir	/home/informix
Process Name	procName	/INFORMIXTMP/.inf.sqlexec
Intercept Types	interceptTypes	<blank or null>
Identifier	ieIdentifier	<blank or null>
	informixVersion	Informix version

10. Restart the S-TAP.
11. To disable libguard, run: ifxguard -kill $INFORMIXSERVER

Parent topic: Linux and UNIX systems: Using Exit libraries

Linux and UNIX systems: Teradata Exit integration

The Teradata exit module enables Guardium to pick up Teradata traffic, whether encrypted or not and whether local or remote. It does not require A-TAP or K-TAP.

About this task

Introduced in v10.1.3. S-TAP on Teradata 16.10 and higher requires this configuration.

Teradata exit embeds a Guardium library into DB2 via the exit module. The exit module communicates directly with the Guardium S-TAP to forward all Teradata traffic.

Teradata exit supports terminate and firewall. It does not support UID chain or redaction.

The location of libguard_teradata_exit_64.so and other Guardium files varies depending on the installation method and directory chosen.

Procedure

1. Stop the Teradata service:

```
 /etc/init.d/tpa stop
/etc/init.d/tgtw stop
```

2. On your Guardium, configure a Teradata Exit Inspection Engine, similar to:

```
[DB_0]
connect_to_ip=127.0.0.1
db_exec_file=/opt/teradata/tdat/tgtw/16.00.00.05sks/bin/gtwgateway
db_install_dir=/root
db_type=trd_exit
intercept_types=NULL
tap_identifier=NULL
networks=0.0.0.0/0.0.0.0
exclude_networks=
```

3. On the DB, create directory "site" as follows: `mkdir /opt/teradata/tdat/tgtw/site`
4. On the DB, create a symbolic link: `ln -s /usr/local/guardium/modules/STAP/current/files/lib/libguard_teradata_exit_64.so /opt/teradata/tdat/tgtw/site/libtgtwmonitoring.so`
5. On the DB, authorize users to the guardium group to capture traffic. As root, enter:

```
/usr/local/guardium/guard_stap/guardctl --db-user=tdatuser authorize-user
/usr/local/guardium/guard_stap/guardctl --db-user=teradata authorize-user
/usr/local/guardium/guard_stap/guardctl --db-user=root authorize-user
```

6. On the DB, load the Exit library into the Teradata database: `/usr/tgtw/bin/gtwcontrol --monitorlib load=yes`
7. Start the Teradata service:

```
 /etc/init.d/tpa start
/etc/init.d/tgtw start
```

Parent topic: Linux and UNIX systems: Using Exit libraries

Linux and UNIX systems: Editing the S-TAP configuration parameters

You can modify the S-TAP configuration after it is installed using GIM, the GUI, or for advanced users, in the configuration file on the database.

Note: Parameters in the GUI may be safely changed. Parameters that are not in the GUI are advanced, and rarely need changing. They are normally be left unmodified; they are for use by Guardium support or advanced users.
CAUTION:
Do not modify advanced parameters unless you are an expert user or you have consulted with IBM Technical Support.

You can some modify parameters in the GUI. See Linux and UNIX systems: Configure S-TAP from the GUI.

GIM is an easy method for modifying parameters, if the S-TAP bundle was installed with GIM. See the instructions for v10.1.4 and higher: Set up by Client; and for v10.1-10.1.3: GIM user interfaces.

If it is necessary to modify the configuration file from the database server, follow the procedure described in this section. The guard_tap.ini file contains comments that explain many of the parameters.

The S-TAP needs restarting after you modify the guard_tap.ini. If you're using GIM, it restarts the S-TAP automatically.

CAUTION:
Parameters must be added to their relevant section: [TAP], [SQLGuard], [DB_<name>].

1. Log on to the database server system using the root account.
2. Stop the S-TAP.
3. Make a backup copy of the configuration file: guard_tap.ini. The default file locations is /usr/local/guardium/guard_stap/guard_tap.ini
4. Open the configuration file in a text editor.
5. Edit the file as necessary.
6. Save the file.
7. Restart the S-TAP and verify that your change has been incorporated.

- Linux and UNIX systems: Guardium Hosts (SQLGuard) parameters
  These parameters describe a Guardium system to which this S-TAP can connect. All parameters in this section are basic, and appear in the [SQL_GUARD] section.
- Linux and UNIX systems: General parameters
  These parameters define basic properties of the S-TAP running on a DB server and the server on which it is installed, and do not fall into any of the other categories.
- Linux and UNIX systems: Inspection engine parameters
  These parameters affect the behavior of the inspection engine that the S-TAP uses to monitor a data repository on a DB server.
- Linux and UNIX systems: Firewall parameters
  These parameters affect the behavior of the S-TAP with respect to the firewall.
- Linux and UNIX systems: Query rewrite parameters
  The query rewrite parameters affect the behavior of the S-TAP with respect to discovery.
- Linux and UNIX systems: Server-side masking (SSM) parameters
  The server-side masking parameters affect the behavior of the S-TAP with respect to discovery.
- Linux and UNIX systems: Discovery parameters
  The discovery parameters define the behavior of the auto-discovery feature, for discovering database instances and sending the results to the current active S-TAP.
- Linux and UNIX systems: Application server parameters
  These parameters affect the behavior of the S-TAP when an application user name needs to be bounded with database activities.
- Linux and UNIX systems: Hadoop parameters
  Guardium supports integration Hortonworks distributions using Apache Ranger. Understand the S-TAP parameters required for the connection between S-TAPs and Ranger agents.
- Linux and UNIX systems: Configuration Auditing System (CAS) parameters
  These parameters affect the behavior of CAS.
- Linux and UNIX systems: Debug parameters
  These parameters affect the behavior of S-TAP debugging.
- Linux and UNIX systems: K-TAP parameters
  These parameters affect the behavior of the K-TAP.

Parent topic: Linux and UNIX systems: Configuring S-TAP

Linux and UNIX systems: Guardium Hosts (SQLGuard) parameters

These parameters describe a Guardium system to which this S-TAP can connect. All parameters in this section are basic, and appear in the [SQL_GUARD] section.

GUI	GIM	guard_tap.ini	Default value	Description
Pool size		connection_pool_size	0	The number of connections to open between the S-TAP and the sniffer process on a Guardium host. Increasing the value provides additional throughput that may be required when enabling encryption such as TLS. The maximum number of pooled connections is 50. The total is the sum of (connection_pool_size x num_main_threads) in all of the [SQLGuard_n] sections in the guard_tap.ini. Valid values: • 0: disable pooling • 1-10 (for each defined host) Default = 0
Main threads		num_main_threads	1	The number of threads used between the S-TAP and one or more Guardium hosts. Valid values: 1-510 (maximum total of 510 for all defined Guardium hosts) (Until V10.1.3 maximum was 5.) Default = 1 Note: Enterprise load balancing does not support using multiple threads for a single managed unit. When using enterprise load balancing, set this parameter to 1.

GUI	GIM	guard_tap.ini	Default value	Description
✔ (checkmark indicates the primary host)		primary		Indicates the primary Guardium system for this S-TAP. In guard_tap.ini: 1=Primary, 2=Seconday, 3=tertiary, and so on
		sqlguard_port	16016	Read only. Port used for S-TAP to connect to Guardium system.
Guardium Host	STAP_SQLGUARD_IP	sqlguard_ip	NULL	IP address or hostname of the Guardium system that acts as the host for the S-TAP. You can define multiple hosts by adding [SQLGuard_1], [SQLGuard_2], and so on.

Parent topic: Linux and UNIX systems: Editing the S-TAP configuration parameters

Linux and UNIX systems: General parameters

These parameters define basic properties of the S-TAP running on a DB server and the server on which it is installed, and do not fall into any of the other categories.

These parameters are stored in the [TAP] section of the S-TAP properties file.

Table 1. S-TAP configuration parameters in the [TAP] section

GUI	GIM	guard_tap.ini	Default value	Description
		tap_type		The type of installed S-TAP agent: stap=UNIX ztap=Z/OS
Version		tap_version		Read only. The S-TAP version that is installed on the DB server, added to the file during installation or upgrade only.
S-TAP Host	STAP_TAP_IP	tap_ip		Read only. IP address or hostname for the database server system on which S-TAP is installed
Devices	STAP_DEVICES	devices	none	Which interfaces to listen on. Use ifconfig to find the correct interface.
All can control	STAP_ALL_CAN_CONTROL	all_can_control	0	0=S-TAP can be controlled only from the primary Guardium system. 1=S-TAP can be controlled from any Guardium system.
Load balancing	STAP_PARTICIPATE_IN_LOAD_BALANCING	participate_in_load_balancing	0	Controls load balancing to Guardium systems: • 0: No load balancing. • 1: Load balancing. Traffic is balanced between the primary and secondary servers, defined in the SQLGuard section. • 2: Redundancy. Fully mirrored S-TAP sends all traffic to all primary and secondary servers, defined in the SQLGuard section. • 3: Hardware load balancing. Guardium uses a load balancer such as F5 or Cisco. S-TAP sends the traffic to the load balancer, which forwards it to one of the collectors in the pool. • 4: Multiple KTAP buffer and S-TAP threads are used to split the traffic. Use the primary parameter in the SQLGUARD section to specify primary, secondary, etc. servers. If this parameter is set to 0, and you have more than one Guardium system monitoring traffic, then the non-primary Guardium systems are available for failover. Note: Guardium does not support failover with a v10.x S-TAP and a v9.x collector.
		connection_timeout_sec	10	Number of seconds after which the S-TAP considers a Guardium server to be unavailable. It can have any integer value.
TLS Use	STAP_USE_TLS	use_tls	0	1=use SSL to encrypt traffic between the agent and the Guardium system. 0=do not encrypt. Warning: The traffic between the agent and Guardium system is in clear text. Guardium recommends encrypting network traffic between the S-TAP and the collector whenever possible, only in cases where the performance is a higher priority than security should this be disabled. Decrypting login packets isn't supported when TLS is enabled. This means that DB_USER is not populated and failed logins are not associated with an access.

GUI	GIM	guard_tap.ini	Default value	Description
TLS Failover	STAP_FAILOVER_TLS	failover_tls	0	1= If ssl connection is not possible for any reason, fail over to using non-secure connection. 0=use only secure connections.
	STAP_WAIT_FOR_DB_EXEC	wait_for_db_exec	-1	Specifies how the S-TAP starts monitoring its databases after a restart. 1 and greater: When S-TAP restarts, either from a system reboot or user initiated S-TAP stop / start commands, S-TAP polls all databases that have been configured to be monitored and begins monitoring them when available. Any configuration anomalies (either on the database side or the S-TAP side) that limits S-TAP ability to monitor a database does not limit S-TAP from monitoring other databases with valid configurations. Instead, S-TAP starts successfully, monitors all valid configurations, and continues to poll other databases until they become available and then starts monitoring them as well. It is recommended to use existing alerts and reports to monitor and report on any failed S-TAP status. For example, after relinking Oracle, Oracle BEQ traffic is not logged for 15 minutes, this is the time it takes for S-TAP to run periodically and check if an Oracle device node has been changed. 0 and less: S-TAP exits with error message if it cannot access the db_install_dir. If the STAP has multiple IEs, it exits at the first occurrence of not reaching a DB.

	STAP_RUN_AS_ROOT	tap_run_as_root	TAPUSER	To allow S-TAP to run as regular user. 0 = runs as guardium user, 1= runs as root
				
				In some cases you need to run the S-TAP as guardium (and not root). This can cause other issues and should only be used when necessary. Running S-TAP as the guardium user can cause a database or protocol to stop working because of permission levels. Verify that the database path or exec file gives the Guardium user read permission. Depending on your environment, typical limitations are:
				
				• wait_for_db_exec might not work. For cluster, check the database path or exec file for Guardium user read permission.
				• Database on AIX® WPAR and Solaris Zones may not work, check the permission to access the install path or exec file
				• For Oracle BEQ, restart S-TAP after starting or restarting the database.
				• For Informix® shared memory, restart S-TAP after starting or restarting the database.
				• For DB2 shared memory, if shmctl failed because of permission issue, then in most cases S-TAP® should be changed to run as root.
				  ◦ If shared memory segment has read permission by group, then make sure the DB2 instance has been added to user (Guardium) group. But still on each server, only one set of configuration of DB2® can be supported.
				  ◦ If shared memory segment has read permission by db2 user only, then S-TAP has to run as root. (open a DB2 shared memory session, run command ipcs -ma, check MODE on the output)

		tap_buf_dir	NULL	Location of S-TAP buffer file. Default location is $inidir/buffers
		tap_log_dir	NULL	Location of S-TAP log files: guard_stap.stdout.tx, guard_stap.stderr.txt, guard_stap.fam.txt. By default log files are written in /tmp.
Alternate ips	STAP_ALTERNATE_IPS	alternate_ips	NULL	Comma-separated list of alternate or virtual IP addresses used to connect to this database server. This is used only when your server has multiple network cards with multiple IPs, or virtual IPs. S-TAP only monitors traffic when the destination IP matches either the S-TAP Host IP defined for this S-TAP, or one of the alternate IPs listed here, so it's recommend that you list all virtual IPs here.
	TEE_ENABLED	tee_installed	0	1=Tee is in use. 0=Tee is not used.
		tee_msg_buf_len	128	Size of the buffer for Tee in MB. It can take any integer value.
	STAP_BUFFER_FILE_SIZE	buffer_file_size	50	Advanced. Size in MB of the buffer allocated for the packets queue. If the buffer size is set too large, the S-TAP might not be able to start. Files larger than 2560 MB are known to cause this problem.
		buffer_mmap_file	0	1=memory mapped file option. 0=virtual memory allocation
Trace files dir		tracefiles_dir		The Directory in which access tracer files will be stored. The default is INSTALLDIR.

GUI	GIM	guard_tap.ini	Default value	Description
Compres. Level	STAP_COMPRESSION_LEVEL	compression_level	0	Advanced. Compression level. 1-9. 0: no compression 1: best speed 9: best compression 0: no compression -1: default compression
		min_bytes_to_compress	500	Advanced. Minimum size of message to compress.
		tap_min_heartbeat_interval	180	Number of seconds after which the S-TAP should fail over.
		msg_aggregate_timeout	100	time in milliseconds at which K-TAP sends the packets accumulated in its buffer to the S-TAP. Can be any integer value.
		msg_count_watermark	64	Number of packets at which K-TAP sends the packets accumulated in its buffer to S-TAP. Can be any integer value.
		log_program_name	0	To boost performance you may consider disabling getting the sourceprogram name, in doing so you won't be able to tell which program name was using the connection (but all other connection information like user and client address will be available). 0 = don't send source_program name to Guardium system, 1=send source_program name to Guardium system.
		max_server_write_size	16384	The maximum number of bytes that the S-TAP sends to the Guardium system at once. Can be any integer value.
		guardium_ca_path	NULL	Location of the Certificate Authority certificate.
		sqlguard_cert_cn	NULL	The common name to expect from the Sqlguard certificate.
		guardium_crl_path	NULL	The path to the Certificate Revocation list file or directory.
		tap_failover_session_size	1024	The maximum number of failover sessions in the list per Guardium system. 0=failover feature is disabled. Can be any integer value.
		tap_failover_session_quiesce	60	The number of minutes after S-TAP failover, when unused sessions in the failover list from the previous active servers are removed from the current active server. This includes cleaning the session's policy and removing the session from the firewalled and scrubbed lists.
	STAP_KERBEROS_PLUGIN_DIR	kerberos_plugin_dir	NULL	Location of Kerberos files
	STAP_DB_IGNORE_RESPONSE	db_ignore_response	NULL	Comma-separated list of db types to be response-ignored. If it is set to none, no response is ignored; if it is set to all, the responses from all DBs are ignored. Note: If using db_ignore_response=all to set the Oracle database response to be ignored (not captured to reduce traffic load), then be aware that more than just database server responses are involved. Database server responses can also contain important database protocol metadata information used by the application for following database requests interpretation.
	STAP_STATISTIC	stap_statistic	0	Interval at which S-TAP sends statistic information about S-TAP/K-TAP to sniffer ; 0=do not send. Specify a positive integer for hours or a negative integer for minutes.
		stap_statistic_version	1	STAP statistics are version specific to the collector 1: Guardium V10 and higher 0 - Guardium V9
	STAP_UPLOAD_FEATURE	upload_feature	1	If=1, when a new K-TAP is built, upload it automatically to the Guardium system to which this S-TAP reports.
	STAP_UPLOAD_SNAPSHOTS	upload_snapshots	1	Upload snapshots using file upload mechanism
		add_to_verification schedule	0	Add the Inspection Engines defined in guard_tap.ini to S-TAP Verification schedule. STAP Verification will test traffic capture. 0=OFF, 1=ON, default is 0.

GUI	GIM	guard_tap.ini	Default value	Description
	STAP_DB_IGNORE_BYPASS_BYTES	db_ignore_response_bypass_bytes	4096	Integer of bytes size of the result set, that when a result set is greater than the size to ignore the response.
	STAP_DB_IGNORE_RESETS_PER_REQUEST	db_ignore_response_resets_per_request	0	The db_ignore_response_bypass_bytes is reset on each request. 0=no; 1=yes
	STAP_DB_IGNORE_RESPONSE_FILTER	db_ignore_response_filter	0.0.0.0/0.0.0.0	Comma separated list of IP/MASKs to be response-ignored, by default it filters all traffic Any DB responses of the type specified by DB_IGNORE_RESPONSE to the specified IP/MASKs are ignored. 0=no filtering of responses occurs 0.0.0.0/0.0.0.0=all IPs are filtered
	STAP_DB_IGNORE_RESPONSE_LOCAL	db_ignore_response_local	1	Filtering of local db responses. TCP traffic is not considered local traffic for this parameter. 0=no 1=yes
		debug_snapshot	0	Advanced. Collects a debug dump from a STAP. Should be triggered from the GUI (S-TAP Control > S-TAP commands). After triggering a dump from the GUI, the parameter reverts to its default of 0.
		debug_snapshot_level	1	Advanced. The value of tap_debug_output_level that is run for the debug dump: • 1: basic debug • 4: verbose debug
		debug_snapshot_time	60	Advanced. The time interval, in seconds, for which the diagnostic runs. The value can be any integer value.
		force_log_limited	0	Controls sending certain types of information to the collector. Useful when you are concerned about the possibility of storing private data on the Guardium collector. 0=unrestricted. Default 1=restricted logs. Private data is removed.
		hunter_trace	0	Enable UID_CHAIN 0: Disable. 1: Enable. For local TCP/IP connections including Solaris zones and AIX WPARS; or remote TCP/IP connection when appserver_installed = 1
Load Balancer IP	STAP_LOAD_BALANCER_IP	load_balancer_ip		IP address of the load balancer unit. If not defined, S-TAP does not use Enterprise Load Balancing.
Managed Units	STAP_LOAD_BALANCER_NUM_MUS	load_balancer_num_mus	1	Number of managed units to request from load balancer
		merge_with_template	0	Specifies whether or not the configuration from the collector is merged with the template config file when it is pushed to STAP. 0=no 1=yes

GUI	GIM	guard_tap.ini	Default value	Description
		shmid_blacklist	NULL	Comma separated list of shared memory IDs that KTAP filters.
		shmid_blacklist_wait	0	Wait to activate interception until shmid_blacklist items are discovered 0: no, 1: yes (0)
		blacklist_shmem_ops_by_proc	NULL	ktap uses blacklist_shmem_ops_by_proc to filter the shmem interception for the specified processes (comma separated list)
	STAP_FAM_ENABLED	fam_enable	See description for defaults	Global enable/disable for FAM monitor (crawler). 0: disabled 1: enabled In GIM installations from v10.1.4, the default is disabled, and in earlier versions it is enabled by default. In shell installations, the default is enabled in all 10.0 and 10.1 version.
Include client IP in UID chain for SSH daemon	STAP_UID_CHAIN_TRACE	uid_chain_sshd_ip	0	Introduced in v10.1.4. Encode the client IP into the UID chain when ssh is identified as one of the processes in the chain. 0=disabled, 1=enabled

Parent topic: Linux and UNIX systems: Editing the S-TAP configuration parameters

Linux and UNIX systems: Inspection engine parameters

These parameters affect the behavior of the inspection engine that the S-TAP uses to monitor a data repository on a DB server.

These parameters are stored in the individual [DB_<name>] inspection engine section of the S-TAP properties file, with the name of a data repository. There can be multiple sections in a properties file, each describing one inspection engine used by this S-TAP.

GUI	guard_tap.ini	Default value	Description
Protocol	db_type		The type of data repository being monitored.
Port range	port_range_start		Starting port range specific to the database instance. Together with port_range_end defines the range of ports monitored for this database instance. There is usually only a single port in the range. For a Kerberos inspection engine, set the start and end values to 88-88. If a range is used, do not include extra ports in the range, as this could result in excessive resource consumption while the S-TAP attempts to analyze unwanted traffic.
Port range	port_range_end		Ending port range specific to the database instance.
KTAP DB Real Port	real_db_port	4100	Used only when the K-TAP monitoring mechanism is used. Identifies the database port to be monitored by the K-TAP mechanism.
Client Ip/Mask	networks		Identifies the clients to be monitored, using a list of addresses in IP address/mask format: n.n.n.n/m.m.m.m. If an improper IP address/mask is entered, the S-TAP does not start. Valid values: • null=select all clients • 127.0.0.1/255.255.255.255=local traffic only Client Ip/Mask (networks) and Exclude Client Ip/Mask (exclude networks) cannot be specified simultaneously. If the IP address is the same as the IP address for the database server, and a mask of **255.255.255.255** is used, only **local** traffic will be monitored. An address/mask value of **1.1.1.1/0.0.0.0** monitors all clients.
Exclude Client Ip/Mask	exclude_networks		A list of client IP addresses and corresponding masks that are excluded from monitoring. This option allows you to configure the S-TAP to monitor all clients, except for a certain client or subnet (or a collection of these). Client Ip/Mask (networks) and Exclude Client Ip/Mask (exclude networks) cannot be specified simultaneously.
TEE Listen Port-Real Port	tee_listen_port	12344	Deprecated. Replaced by the parameter real_db_port when the K-TAP monitoring mechanism is used. Was required when the TEE monitoring mechanism. The Listen Port is the port on which S-TAP listens for and accepts local database traffic. The Real Port is the port to which S-TAP forwards traffic.
Connect To Ip	connect_to_ip	127.0.0.1	IP address for S-TAP to use to connect to the database. Some databases accept local connection only on the real IP address of the machine, and not on the default (127.0.0.1). When K-TAP is enabled, this parameter is used for Solaris zones and AIX WPARs and it should be the zone IP address in order to capture traffic.

GUI	guard_tap.ini	Default value	Description
DB Install Dir	db_install_dir	NULL	DB2, Informix, or Oracle: Enter the full path name for the database installation directory. For example: /home/oracle10. All other database types enter: NULL. For DB2 exit and Informix exit, db_install_dir must be exactly the same as the $HOME value in the database (or $DB2_HOME for DB2 Exit); otherwise tap_identifier does not function properly.
Process Name	db_exec_file	NULL	For a DB2, Oracle, or Informix database, enter the full path name for the database executable. For example: • Oracle: there is no standard path, it depends on the directory where the database is installed. • Informix: /INFORMIXTMP/.inf.sqlexec. Applies to all Informix platforms but Linux. • Informix with Linux, example: /home/informix11/bin/oninit • MYSQL: mysql • All other database types: NULL
Encryption	encryption	0	Activate ASO or SSL encrypted traffic for Oracle (versions 11 and 12) and Sybase on Solaris, HPUX and AIX. For Oracle, specify db_version in the ini file (e.g. db_version=12) For Oracle12 SSL, instrument on all platforms. For Oracle11 SSL, instrument on AIX. For any Oracle requiring instrumentation, if you are using encryption=1 in the guard_tap.ini (which is not supported on Linux), you must instrument prior to setting that parameter. Some DBs require restart after enabling encryption.
	load_balanced	1	1=database traffic participates in load balancing. 0=database traffic does not participate in load balancing.
Intercept Types	intercept_types	NULL	Protocol types that are intercepted by the IE. Valid values: • NULL: auto intercepts all protocols the Database supports • Comma separated list: IE intercepts these protocol types only.
Identifier	tap_identifier	NULL	Optional. Used to distinguish inspection engines from one another. If you do not provide a value for this field, Guardium auto-populates the field with a unique name using the database type and GUI display sequence number.
DB Version	db_version	9	The database version.
Unix Socket Marker	unix_domain_socket_marker	Null	Specifies UNIX domain sockets marker for Oracle, MySQL and Postgres. Usually the default value is correct, but when the named pipe or UNIX domain socket traffic does not work then you need to make sure this value is set correctly. For example, for Oracle, unix_domain_socket_marker should be set to the KEY of IPC defined in tnsnames.ora. If it is NULL or not set, the S-TAP uses defined default markers identified as: * MySQL - "mysql.sock" * Oracle - "/.oracle/" * Postgres - ".s.PGSQL.5432"

These additional parameters are used with IBM DB2 databases.

Table 1. Additional S-TAP configuration parameters for a DB2 inspection engine

GUI	guard_tap.ini	Default value	Description
DB2 Shared Mem. Adjust.	db2_fix_pack_adjustment	20	Required when DB2 is selected as the database type, and shared memory connections are monitored. The offset to the server's portion of the shared memory area. Offset to the beginning of the DB2 shared memory packet, depends on the DB2 version: 32 in pre-8.2.1, and 80 in 8.2.1 and higher.
DB2 Sh. Mem. Client Pos.	db2_shmem_client_position	61440	The offset to the client's portion of the shared memory area. Required when DB2 is selected as the database type, and shared memory connections are monitored. The client offset can be calculated by taking the value of the DB2 parameter ASLHEAPSZ and multiplying by 4096 to get the appropriate offset. The default for this parameter is 61440 decimal. This parameter is calculated by taking the DB2 database configuration value of ASLHEAPSZ and multiplying by 4096. To get the value for ASLHEAPSZ, execute the following DB2 command: `db2 get dbm cfg` and look for the value of ASLHEAPSZ. This value is typically 15 which yields the 61440 default. If it's not 15, take the value and multiply by 4096 to get the appropriate client offset.
	db2bp_path	Null	Only used when using ATAP on DB2. If the program 'db2bp' (part of DB2) is in the standard location, this does not need to be set. If it is non-standard, then this parameter points to its location. The value of this parameter should be the full path of the relevant db2bp as seen from the global zone/wpar. For example, if the file is /data/db2inst1/sqllib/bin/db2bp and the zone is installed in /data/zones/oracle2nd/root/ then the full path to db2bp that should be set in the db2bp_path parameter is /data/zones/oracle2nd/root/data/db2inst1/sqllib/bin/db2bp
DB2 Shared Mem. Size	db2_shmem_size	131072	DB2 shared memory segment size. Required when DB2 is selected as the database type, and shared memory connections are monitored.

Parent topic: Linux and UNIX systems: Editing the S-TAP configuration parameters

Linux and UNIX systems: Firewall parameters

These parameters affect the behavior of the S-TAP with respect to the firewall.

These parameters are stored in the [TAP] section of the S-TAP properties file.

CAUTION:
These are advanced parameters and are usually modified by IBM Technical Support only.

GIM	guard_tap.ini	Default value	Description
STAP_FIREWALL_INSTALLED	firewall_installed	0	Firewall feature enabled. 1=yes, 0=no.
STAP_FIREWALL_TIMEOUT	firewall_timeout	10	Time, in seconds to, wait for a verdict from the Guardium system if the firewall timed out. Look at firewall_fail_close value to know whether to block or allow the connection. The value can be any integer value.
STAP_FIREWALL_FAIL_CLOSE	firewall_fail_close	0	If the verdict does not come back from the Guardium system and the firewall_timeout expires: if firewall_close = 0 the connection goes through; if firewall_close=1 the connection is blocked.

GIM	guard_tap.ini	Default value	Description
STAP_FIREWALL_DEFAULT_STATE	firewall_default_state	0	0: An event triggers traffic in a session to be watched and checked for firewall policy violations. 1: All traffic is watched by default for firewall policy violations
STAP_FIREWALL_FORCE_WATCH	firewall_force_watch	NULL	When the firewall feature is enabled and firewall_default_state is 0, the session is watched automatically when its client IP matches one of this list of IP/MASK values. The list itself is separated with commas, for example, 1.1.1.1/1.1.1.1,2.2.2.2/2.2.2.2

GIM	guard_tap.ini	Default value	Description
STAP_FIREWALL_FORCE_UNWATCH	firewall_force_unwatch	NULL	When the firewall feature is enabled and firewall_default_state is 1, the session is unwatched automatically when its client IP matches one of this list of IP/MASK values. The list itself is separated with commas, for example, 1.1.1.1/1.1.1.1,2.2.2.2/2.2.2.2,

Parent topic: Linux and UNIX systems: Editing the S-TAP configuration parameters

Linux and UNIX systems: Query rewrite parameters

The query rewrite parameters affect the behavior of the S-TAP with respect to discovery.

These parameters are stored in the [TAP] section of the S-TAP properties file.

CAUTION:
These are advanced parameters and are usually modified by IBM Technical Support only.

GIM	guard_tap.ini	Default Value	Description
STAP_QRW_INSTALLED	qrw_installed	0	Enable / disable the Dynamic Data Masking for Databases feature. When set to 0, all other parameters in this group are ignored. • 0=No • 1=Yes
STAP_QRW_DEFAULT_STATE	qrw_default_state	0	Sets the query rewrite activation trigger. Must be 0 if firewall_default_state=1. • 0=QRW activated per session when triggered by a rule in the installed policy • 1=QRW activated for every session regardless of the installed policy
STAP_QRW_FORCE_WATCH	qrw_force_watch	NULL	Comma separated list of client IP/MASKs (for example, 1.1.1.1/1.1.1.1,2.2.2.2/2.2.2.2) to watch automatically. Valid when qrw_default_state is 0. Cannot be configured to the same range as firewall_force_watch.
STAP_QRW_FORCE_UNWATCH	qrw_force_unwatch	NULL	Comma separated list of client IP/MASKs (for example, 1.1.1.1/1.1.1.1,2.2.2.2/2.2.2.2) to exclude from watching. Valid when firewall_default_state is 1. Cannot be configured to the same range as firewall_force_unwatch.

Parent topic: Linux and UNIX systems: Editing the S-TAP configuration parameters

Linux and UNIX systems: Server-side masking (SSM) parameters

The server-side masking parameters affect the behavior of the S-TAP with respect to discovery.

These parameters are stored in the [TAP] section of the S-TAP properties file.

CAUTION:
These are advanced parameters and are usually modified by IBM Technical Support only.

Parameter	Default value	Description
server_side_masking_installed	0	Enables the server-side masking feature. • 0=No • 1=Yes

Parameter	Default value	Description
server_side_masking_default_state	0	Sets the server-side masking activation trigger. • 0=SSM activated per session when triggered by a rule in the installed policy • 1=SSM activated for every session regardless of the installed policy
server_side_masking_force_watch	NULL	Comma separated list of client IP/MASKs (for example, 1.1.1.1/1.1.1.1,2.2.2.2/2.2.2.2) whose sessions are watched automatically. Valid when server_side_masking_installed=1 and qrw_default_state=0. Cannot be configured to the same range as firewall_force_watch.
server_side_masking_force_unwatch	NULL	Comma separated list of client IP/MASKs (for example, 1.1.1.1/1.1.1.1,2.2.2.2/2.2.2.2) whose sessions are not watched. Valid when server_side_masking_installed is 1 and firewall_default_state is 1. Cannot be configured to the same range as firewall_force_unwatch.

Parent topic: Linux and UNIX systems: Editing the S-TAP configuration parameters

Linux and UNIX systems: Discovery parameters

The discovery parameters define the behavior of the auto-discovery feature, for discovering database instances and sending the results to the current active S-TAP.

CAUTION:
These are advanced parameters and are usually modified by IBM Technical Support only.

GIM	guard_tap.ini	Default value	Description
STAP_DISCOVERY_INTERVAL	discovery_interval	24	The time interval, in hours, at which auto-discovery runs. Set to 0 to disable.
DISCOVERY_DBS	discovery_dbs	oracle:db2:informix:mysql:postgres:sybase:hadoop:teradata:netezza:memsql	Colon (':') separated list of database types to discover.
DISCOVERY_DEBUG	discovery_debug	0	Discovery debug level 0 = errors only 1 = errors and debug statements
DISCOVERY_ORA_ALT_LOCATIONS	discovery_ora_alt_locations		Alternate locations to look for listener.ora files
STAP_DISCOVERY_PORT	discovery_port	8443	The Guardium port the S-TAP Discovery uses to connect to the Guardium system.

Parent topic: Linux and UNIX systems: Editing the S-TAP configuration parameters

Linux and UNIX systems: Application server parameters

These parameters affect the behavior of the S-TAP when an application user name needs to be bounded with database activities.

These parameters are in the [TAP] section on the guard_tap.ini file.

GUI	GIM	guard_tap.ini	Default value	Description
	STAP_APPSERVER_INSTALLED	appserver_installed	0	0 is default, S-TAP acts as normal. 1=S-TAP is set in 'client mode', switches S2C and C2S packets to reflect S-TAP being installed on client, not db server. Also, if 1, checks to see if the other appserver_* parameters are filled in, and if so, examines http packets on the supplied port to grab session information about the end-user of the java-application that resides on the client system.
Ports	STAP_APPSERVER_PORTS	appserver_ports	8080	Comma-separated list of ports, or hyphens for inclusive ranges of ports, on which the Java application is accessed via web browser.

GUI	GIM	guard_tap.ini	Default value	Description
Login pattern	STAP_APPSERVER_LOGIN_PATTERN	appserver_login_pattern		Comma-separated list of strings specifying the login pattern passed to the application. This is the pattern that the Java application is passed to identify a user login.
Username prefix	STAP_APPSERVER_USERNAME_PREFIX	appserver_username_prefix		Comma-separated list of strings specifying the prefix to the username for a given session. This is the pattern the Java application uses to indicate the username of the given session.
Username postfix	STAP_APPSERVER_USERNAME_POSTFIX	appserver_username_postfix		Comma-separated list of strings specifying the postfix to the username for a given session. This is the pattern (or character) used by the Java application to indicate the end of the value for the given variable that indicates the username.
Session pattern	STAP_APPSERVER_SESSION_PATTERN	appserver_session_pattern		Comma-separated list of strings specify the start of an end-user session, using a particular database session. This is the pattern specifying [change of] end-user session for a given database connection.
Session prefix	STAP_APPSERVER_SESSION_PREFIX	appserver_session_prefix		Comma-separated list of strings specifying the session identifier
Session postfix	STAP_APPSERVER_SESSION_POSTFIX	appserver_session_postfix		Comma-separated list of strings specifying where the session id ends.
Session ID pattern	STAP_APPSERVER_USERSESS_PATTERN	appserver_usersess_pattern		Comma-separated list of strings specifying the identifier for marking which end-session a given connection is continuing with.

GUI	GIM	guard_tap.ini	Default value	Description
Session ID prefix	STAP_APPSERVER_USERSESS_PREFIX	appserver_usersess_prefix		Comma-separated list of strings specifying what identifies/precedes the session_id in a given usersess indicator packet.
Session ID postfix	STAP_APPSERVER_USERSESS_POSTFIX	appserver_usersess_postfix		Comma-separated list of strings specifying where the session id ends.

Parent topic: Linux and UNIX systems: Editing the S-TAP configuration parameters

Linux and UNIX systems: Hadoop parameters

Guardium supports integration Hortonworks distributions using Apache Ranger. Understand the S-TAP parameters required for the connection between S-TAPs and Ranger agents.

guard_tap.ini parameters for Hortonworks with Apache Ranger

Note: Some parameters are configurable through the Guardium user interface or through the Guardium Installation Manager. All parameters are configurable using the Guardium API.
CAUTION:
These are advanced parameters and are usually modified by IBM Technical Support only.

Table 1. guard_tap.ini parameters for Hortonworks with Apache Ranger integration

Parameter	Values	Description
log4j_reader_enabled	`0` or `1` `0` is disabled (default). `1` is enabled.	Enable log4j listening mode for Ranger traffic.
log4j_port	Integer. Default = `5555`.	The port where the Guardium S-TAP will listen for Ranger audits.
log4j_listen_address	IP address `0.0.0.0` indicates any IP address of the system (default). `localhost` indicates the loopback address of the system.	Ranger plugins will connect to this address. The default value of `0.0.0.0` is recommended, as this enables the S-TAP to receive traffic from any host. Use `localhost` if configuring the system for high availability. If you choose to restrict access to a specific address, be sure you are not excluding any necessary traffic for monitoring.
log4j_num_connections	Integer Default value is `20`.	The number of concurrent connections to expect from the service or services defined for this S-TAP.
ranger_dynamic_policy_port	integer Default = 5556	Port that Ranger plugins connect to. S-TAP listens here for the Ranger dynamic policy.
ranger_dynamic_policy_listen_address	IP address 0.0.0.0 indicates any IP address of the system (default)	Ranger dynamic policy plugins connect to this address. Use localhost for HA.
ranger_dynamic_policy_num_connections	Integer Default = 20	Maximum number of connections to support from the dynamic policy plugin.
ranger_dynamic_policy_timeout	Integer Default = 10	Number of seconds to wait for a verdict before sending the default verdict result.

Parameter	Values	Description
ranger_dynamic_policy_default_verdict	0 or 1 1 = match, 0 = no match Default = 1	Behavior when Guardium is unreachable or the verdict times out.
ranger_dynamic_policy_reader_enabled	0 or 1 0 is disabled (default). 1 is enabled.	Enable Hortonworks dynamic policy logging.

guard_tap.ini parameters for Cloudera Navigator using Kafka messaging

Guardium supports Cloudera Navigator for collecting audit data using the Kafka messaging system.
Note: Some parameters are configurable through the Guardium user interface or through the Guardium Installation Manager. All parameters are configurable using the Guardium API.
CAUTION:
These are advanced parameters and are usually modified by IBM Technical Support only.

Table 2. guard_tap.ini parameters for Cloudera Navigator using Kafka messaging integration

Parameter	Values	Description
kafka_reader_enabled	`0` or `1` `0` is disabled (default). `1` is enabled.	Enable Cloudera Navigator integration using Kafka publish and consume.
kafka_bootstrap_servers	A comma separated list of `host name:port` pairs. Format: `host:port,host:port` Example: `hostnameofbroker1:9092,hostnameofbroker2:9092`	The `host name:port` list is used for establishing the initial connection to the Kafka cluster. After the initial connection is established, all servers in the cluster are used. You may want to specify more than one bootstrap in case one is down.
kafka_use_tls	`0` or `1` `0` is disabled (default). `1` is enabled.	Indicate whether the Kafka cluster uses TLS.
kafka_topic_name	String Default value is `NavigatorAuditEvents`.	The topic name used by Cloudera Navigator to publish its audit events to Kafka.
kafka_principal	String Default value is `NULL`.	The Kerberos principal name for the S-TAP, which is used when the Kafka cluster requires Kerberos authentication.
kafka_keytab	NULL	The path to the Kerberos keytab file on the S-TAP server.

Parent topic: Linux and UNIX systems: Editing the S-TAP configuration parameters

Linux and UNIX systems: Configuration Auditing System (CAS) parameters

These parameters affect the behavior of CAS.

GUI	guard_tap.ini	Default value	Description
Task checkpoint	cas_task_checkpoint	task_checkpoint	Internal handle program machine state in case of host failure.
Client checkpoint	cas_client_checkpoint	client_checkpoint	File used to restart processing. A series of files is created. Each version of the file ends with a unique number. The default is task_checkpoint and client_checkpoint
Checkpoint period	cas_checkpoint_period	60	Interval time, in seconds, for the check.
Fail over file	cas_fail_over_file	fail_over_file	Name of the outgoing messages buffer. The database writes to this file when the Guardium system cannot be reached. During this time, the file can grow to the maximum size specified. When the limit is reached, a second file is created, using the same name with the digit 2 appended to the end of the name. (This is the point at which CAS begins trying to connect to a secondary server.) If that file also reaches the maximum size, the first file is overwritten. If the first file fills again, the second file is overwritten. Thus, following an extended outage, you may lose data, but you will have an amount of data up to twice the size of the Failover File Size Limit.
Fail over file size limit	cas_fail_over_file_size_limit	50000	Failover file maximum size, in KB. There are two of these files, so the disk space requirement is twice what you specify here. If you specify -1, there is no limit on the file size, but it's recommend that the file size is capped.

GUI	guard_tap.ini	Default value	Description
Max rec. attempts	cas_max_reconnect_attempts	5000	Number of reconnect attempts when connection is lost. After losing a connection to the Guardium system, the maximum number of times CAS attempts to reconnect. Set this value to -1 to remove any maximum (CAS attempts to reconnect indefinitely). The default cas_max_reconnect_attempts and cas_reconnect_interval define an interval of about 3.5 days. After the maximum has been met, CAS continues to run, writing to the failover files, but it does not attempt to reconnect with a Guardium host.
Reconnect interval	cas_reconnect_interval	60	Wait time, in seconds, between reconnect attempts.
Raw data limit	cas_raw_data_limit	1000	Maximum number of kilobytes written for an item when the Keep data checkbox is marked in the item template. If you specify -1, there is no limit.
Md5 data limit	cas_md5_size_limit	1000	Maximum size of a data item, kilobytes, on which the MD5 checksum calculation is performed. If you specify -1, there is no limit.
	cas_command_wait	300	Wait time in seconds before killing a long-running data collection process
	cas_server_failover_delay	60	Wait time in minutes before trying to connect to another Guardium system

Table 1. CAS deprecated parameters

guard_tap.ini
cas_task_baseline
cas_client_baseline

Parent topic: Linux and UNIX systems: Editing the S-TAP configuration parameters

Linux and UNIX systems: Debug parameters

These parameters affect the behavior of S-TAP debugging.

CAUTION:
These are advanced parameters and are usually modified by IBM Technical Support only.
These parameters are in the [TAP] section on the guard_tap.ini file.

Table 1. S-TAP configuration parameters for debugging

GUI	GIM	guard_tap.ini	Default value	Description
Messages Syslog	STAP_SYSLOG_MESSAGES	syslog_messages	1	1= send messages to syslog. 0=do not send messages.
		tap_debug_output_level	0	S-TAP logs level. Logs are stderr.txt, guard_stap.fam.txt, guard_stap.stdout.txt located in the directory specified in tap_log_dir parameter (by default: /tmp/guard_stap). S-TAP Log Levels: • 0: disable • 1: basic debug • 4: verbose debug • 6: Appserver debug • 10: Exit engine debug. Debug info is logged into both S-TAP log and db2_exit log (db2diag.log). • 11: exit engine debug. Debug info is only logged into db2_exit log (db2diag.log).
Messages Remote	STAP_REMOTE_MESSAGES	remote_messages	1	Send messages to the active Guardium host. • 0=Do not send messages • 1=Send messages to the active Guardium system.

Parent topic: Linux and UNIX systems: Editing the S-TAP configuration parameters

Linux and UNIX systems: K-TAP parameters

These parameters affect the behavior of the K-TAP.

These parameters are located in the [TAP] section of the S-TAP properties.

CAUTION:
These are advanced parameters and are usually modified by IBM Technical Support only.

Table 1. K-TAP configuration parameters

guard_tap.ini	Default value	Description
ktap_installed	1	Is Kernel Monitor module installed: 0=NO, 1=YES. ktap_installed and tee_installed are mutually exclusive; only one can be set to on.
ktap_request_timeout	5	The timeout, in seconds, for waiting for K-TAP reply. K-TAP sends ioctl to S-TAP to ask for some information, and waits for the reply from S-TAP. It can have any value.
ktap_dbgev_ev_list	0	It is used to enable K-TAP trace log either through GUI or through guard_tap.ini file: 0=disable, 1=enable ktap trace log located under /var/tmp directory

guard_tap.ini	Default value	Description
ktap_dbgev_func_name	all	List of functions to log in K-TAP trace log. all= all the functions or we can specify specific function such as accept so we log in the log file only the accept functions. If you specify a function that is not relevant to the K-TAP trace log it won't log anything to the log.
ktap_fast_tcp_verdict	1	For TCP connections. 0: "slow" verdict. KTAP sends information about the session to STAP to ask whether or not the traffic should be intercepted. 1: "fast" verdict. KTAP decides on its own. In both cases, the network/exclude network parameters are checked against the incoming IP. From 10.1.4, the value is 1 after upgrade.
ktap_fast_file_verdict	1	For TLI connection, K-TAP sends ioctl to S-TAP to confirm that session is the database connection configured in our IE by checking ports and Ips, when ktap_fast_file_verdict is set to 1, then K-TAP does not send the request to S-TAP as long as session's ports are in the range. it can have either 1 or 0 values (1).
ktap_buffer_size	4194304	Advanced. The size of theK-TAP buffer in Bytes. The range of values is between 1 MB and 16 MB
ktap_buffer_flush	0	Advanced. The way to send messages from K-TAP to S-TAP. If = 1 the S-TAP reads the entire K-TAP buffer and process all the packets in the buffer. If ktap_flush_buffer=0 , the S-TAP reads a fixed amount rather than the entire buffer.
ktap_local_tcp	0	1=only intercept local connections (although previously intercepted connections will still be captured) (this parameter is used for TCP connections)
khash_table_length	24593	Number of sessions that can be stored in the Khash table. It is an integer and can have any value.
khash_max_entries	8192	Length of the table that contains all the information for the specific session. It is an integer and can have any value.
ktap_fast_shmem	1	For db2 shared memory connection • 0=KTAP sends ioctl to the STAP to confirm that the session is the database connection configured in the IE by checking the process ID • 1= K-TAP does not send the request to S-TAP as long as session's db2_shmem_size matches the attached shared memory segment.
ktap_fsmon_buffer_size	4194304	FAM buffer size

Table 2. A-TAP and PCAP configuration parameters

Parameter	Default value	Description
atap_exec_location	/var/guard	Location of the executable that is used when activating A-TAP by enabling the encryption box in the inspection engine section
pcap_read_timeout	0	only PCAP traffic (non-K-TAP): how long should S-TAP wait between PCAP sampling. Do not change this value without consulting with Technical Support, after examining the problem and determining the losses (not capturing all the traffic) are caused due to PCAP/S-TAP related bottleneck.
pcap_dispatch_count	16	Optimization of PCAP capturing; number of packets to bundle (group) before reporting back to S-TAP. Grouping the packets together can reduce the PCAP-to-S-TAP communication, and boost performance. Do not change this value without consulting with Technical Support, after examining the problem and determining the losses (not capturing all the traffic) are caused due to PCAP/S-TAP related bottleneck.
pcap_buffer_size	-1	Size of PCAP socket buffer. This parameter is used for LINUX only. This integer's default value is -1, means to get the maximal buffer possible. Any other case, this is buffer size in kilobytes. 0 is not legal - if it is 0, it means 60 other than that it can be any value up to 65535. Larger buffer mean that it's likely to have losses when there are busts of high volume traffic. The scenario; Burst of high traffic, PCAP captures everything, but the S-TAP (or PCAP-to-S-TAP flow) is not fast enough and cannot keep up with the traffic. To avoid losses, the yet-to-be-processed packets are buffered. The larger the buffer is, the more resilient against higher and longer bursts of high traffic. Do not change this value without consulting with Technical Support, after examining the problem and determining the losses (not capturing all the traffic) are caused due to PCAP/S-TAP related bottleneck.
pcap_backup_ktap	1	When this parameter is enabled, always start PCAP regardless if ktap_installed is enabled or not, as long as there is DB2 defined in IE.

Add parameter to control use of custom KTAP modules distribution via GIM GUI

GIM users - Compile a custom built KTAP into a custom bundle and use it on other database servers.

Non-GIM users - No custom bundles needed, custom KTAP could be compiled and copied between databases server manually.

Parameter Name: GIM_ALLOW_CUSTOM_BUNDLES

Valid values: '1' - allow custom bundles installations . '0' - Reject custom bundle installations

Default value: 1

During GIM scratch installation (DB server) - User can specify a new optional installation parameter, --install_custom_bundles.

If specified, custom bundles installations (for example, custom bundle STAP) will be allowed (GIM_ALLOW_CUSTOMED_BUNDLES will be set to '1') on that DB server. Otherwise won't be allowed (GIM_ALLOW_CUSTOMED_BUNDLES will be set to '0').

During GIM upgrade (via GIM GUI) from a GIM version that did NOT have this parameter - Default value will be '1' (in order not to disable this functionality for customers that might have been using this feature until now).

This parameter can be set to either '1' or '0' when using the configurator utility on the DB server.

This parameter cannot be set to '1' from the GUI if the previous value is '0'.

Note: This functionality will be checked during installation time (on the DB server) and NOT while you are assigning or scheduling a bundle installation or a parameter update (like all the other params are validated).

Affected features: BUNDLE-GIM, configurator.sh, consolidated installer

GuardAPI commands and custom KTAP bundle

In v10

1. STAP_UPLOAD_FEATURE indicator by default is turned on (1) so custom KTAPs when compiled automatically uploaded to appliance
2. In order to compile custom GIM bundle to include new custom KTAP, user need to run grdapi make_bundle_with_uploaded_kernel_module command (need to have exact syntax of the command)
3. In order to use already compiled CUSTOM BUNDLE on any server customer need to turn on GIM_ALLOW_CUSTOM_BUNDLES indicator to 1 (for security reasons this have to be done manually on each DB server). Turning GIM_ALLOW_CUSTOM_BUNDLES indicator back to off could be done from appliance.

Parent topic: Linux and UNIX systems: Editing the S-TAP configuration parameters

Linux and UNIX systems: S-TAP operation and performance

Parent topic: Linux and UNIX systems: S-TAP user's guide

Linux and UNIX systems: Stop S-TAP using GIM

Learn how to stop an S-TAP using GIM.

About this task

On the database host itself, you can stop S-TAP (and all other GIM modules except GIM itself) by stopping GIM's supervisor service with the command: stop gsvr_<release number>. Use initctl list to get the list of services statuses.

You can use GIM to stop S-TAP without ever having to log into the database server. Complete the following steps to change the STAP_ENABLED parameter and schedule the change on the database server.

Procedure

1. Click Manage > Module installation > Set up by Client (v10.1.4: Legacy) to open the Client Search Criteria.
2. Perform a filtered search of registered clients or click Search to view all of the registered clients.
3. Select the clients are the target for the action (stopping S-TAP). If there are more than 20 clients, then the list of clients spreads onto additional pages.
   Note: Clicking Select All selects only the clients on the current page being viewed.
4. Click Next to open the Common Modules panel.
5. Select the Module for S-TAP.
6. Click Next button to open the Module Parameters panel.
7. Select the client that is the target for the action (stopping S-TAP).
8. Change the STAP_ENABLED parameter to 0 (zero).
9. Click Apply to Clients to apply to the targeted clients.
10. Click Install/Update to schedule the update to the targeted clients. This update can be scheduled for NOW or some time in the future.

Parent topic: Linux and UNIX systems: S-TAP operation and performance

Linux and UNIX systems: Restart S-TAP using GIM

Use GIM to restart the S-TAP without ever having to log into the database server.

About this task

Complete the following steps to change the STAP_ENABLED parameter and schedule the change on the database server.

Procedure

1. Click Manage > Module installation > Set up by Client (v10.1.4: Legacy) to open the Client Search Criteria
2. Perform a filtered search of registered clients or click Search to perform an unfiltered search of all registered clients.
3. Select the clients that are the target for the action (starting S-TAP). If there are more than 20 clients, then the list of clients spreads onto additional pages.
   Note: Clicking Select All selects only the clients on the current page being viewed.
4. Click Next to open the Common Modules panel.
5. Select the Module for S-TAP.
6. Click Next to open the Module Parameters panel.
7. Select the client that is the target for the action (starting S-TAP).
8. Change the STAP_ENABLED parameter to 1 (one).
9. Click Apply to Clients to apply to the targeted clients.
10. Click Install/Update to schedule the update to the targeted clients. This update can be scheduled for NOW or some time in the future.

Parent topic: Linux and UNIX systems: S-TAP operation and performance

Linux and UNIX systems: Stop S-TAP without GIM

Use this procedure for an S-TAP that was installed by script or rpm.

Procedure

1. Log on to the database server system by using the root account.
2. For Red Hat
   a. Find the S-TAP process ID by using ps -fe | grep guard_stap | grep -v grep
   b. Kill that process using the command kill
3. For Solaris:

```
-bash-3.00# svcadm -v disable guard_utap
svc:/site/guard_utap:default disabled.
-bash-3.00# ps -eaf | grep stap
    root  2375  1930   0 14:25:36 pts/2       0:00 grep stap
```

4. From the Guardium system to which this S-TAP® reports, verify that the Status light in the S-TAP control panel is red.

Parent topic: Linux and UNIX systems: S-TAP operation and performance

Linux and UNIX systems: Restart S-TAP without GIM

Use this procedure for an S-TAP that was installed by script or rpm.

Procedure

1. Log on to the database server system by using the root account.
2. For all non-Red Hat Enterprise Linux
   a. Open the /etc/inittab file for editing.
   b. Un-comment the following two statements by deleting the comment character (*:* for AIX®, *#* for all others) at the start of each line:

```
#utap:2345:respawn:/usr/local/guardium/guard_stap/guard_stap /usr/local/guardium/guard_stap/guard_tap.ini
```

   c. Optional. If you are using the TEE monitoring mechanism, un-comment the following two statements by deleting the comment character (*:* for AIX, *#* for all others) at the start of each line.
   Note: These processes are not used in the default configuration and must not be started if you are using the K-Tap monitoring mechanism.

```
#utee:2345:respawn:/usr/local/guardium/guard_stap/guard_tee /usr/local/guardium/guard_stap/guard_tap.ini
#hsof:2345:respawn:/usr/local/guardium/guard_stap/guard_hnt
```

   d. Run the init q command to restart the S-TAP® processes.
3. For Red Hat Enterprise Linux
   a. List the currently running agents by using the operating system command initctl list. The output shows the agents that are listed as in the following example:

```
gim_33264 start/running, process 910
gsvr_33264 start/running, process 2552
```

   b. Start each of the agents by using the start <agent> command where agent would be the first entry in the list from a. See the following example.

```
start gim_33264
start gsvr_33264
start guard_utap
```

4. To restart using Solaris services:

```
bash-3.00# svcadm -v enable guard_utap
svc:/site/guard_utap:default enabled.
-bash-3.00# ps -eaf | grep stap
```

```
 root  2379     1   0 14:25:57 ?           0:00
/usr/local/guardium/guard_stap/guard_stap /usr/local/guardium/guard_stap/guard_
    root  2396  1930   0 14:26:00 pts/2       0:00 grep stap
-bash-3.00# svcs guard_utap
STATE          STIME    FMRI
online         14:25:56 svc:/site/guard_utap:default
-bash-3.00#
```

5. Run ps -ef | grep stap to verify that S-TAP is running.
6. From the administrator portal of the Guardium system to which this S-TAP reports, verify that the Status light in the S-TAP control panel is green.

Parent topic: Linux and UNIX systems: S-TAP operation and performance

Linux and UNIX systems: S-TAP logs

The UNIX S-TAP has a few log files.

- guard_stap* logs, located in the filepath specified by tap_log_dir parameter.
  - guard_stap.stderr.txt: is all the output (and the extra debugging output) of STAP
  - guard_stap.fam.txt: Exists only if FAM is enabled; it contains all the output (and extra debug) of FAM monitoring.
  - guard_stap.stdout.txt. Since v10.1.4, it is present in the system, but not used.
- UNIX system log (/var/adm/syslog, /var/log/messages, name and location as relevant on the particular system): contains K-TAP module output messages (along with output messages from all other kernel tasks).

Parent topic: Linux and UNIX systems: S-TAP operation and performance

Linux and UNIX systems: How S-TAP/GIM processes are initialized by different OS types/versions

OS	Version		Initialization method
AIX	6.1	PowerPC	inittab
AIX	7.1	PowerPC	inittab
AIX	7.2	PowerPC	inittab
HP-UX	11.11	pa9000	inittab
HP-UX	11.23	IA-64	inittab
HP-UX	11.23	pa9000	inittab
HP-UX	11.31	IA-64	inittab
HP-UX	11.31	pa9000	inittab
RHEL	4	i686	inittab
RHEL	4	IA-64	inittab
RHEL	4	x86_64	inittab
RHEL	5	i686	inittab
RHEL	5	IA-64	inittab
RHEL	5	ppc64	inittab
RHEL	5	s390x	inittab
RHEL	5	x86_64	inittab
RHEL	6	i686	inittab
RHEL	6	ppc64	inittab
RHEL	6	s390x	inittab
RHEL	6	x86_64	inittab
RHEL	7	ppc64le	systemd
RHEL	7	ppc64	systemd
RHEL	7	s390x	systemd
RHEL	7	x86_64	systemd
SUSE	11	i686	inittab
SUSE	11	ppc64	inittab
SUSE	11	s390x	inittab
SUSE	11	x86_64	inittab
SUSE	12	ppc64le	systemd
SUSE	12	s390x	systemd
SUSE	12	x86_64	systemd
Ubuntu	10.04	x86_64	inittab

OS	Version		Initialization method
Ubuntu	12.04	x86_64	upstart
Ubuntu	14.04	x86_64	upstart
Ubuntu	16.04	x86_64	systemd
Solaris	5.10	i386	service
Solaris	5.10	i386_64	service
Solaris	5.10	SPARC	service
Solaris	5.11	i386_64	service
Solaris	5.11	SPARC	service

Upstart servers

When using Upstart servers, the following are the start and stop commands on the Database server:

To stop S-TAP process:

stop utap

To start S-TAP process:

start utap

To stop GIM and supervisor processes:

stop gim_revision#

stop gsvr_revision#

Example, stop gim_46743

To start GIM and supervisor processes:

start gim_revision#

start gsvr_revision#

Example: start gim_46743

To verify status of Guardium product on the system:

initctl list

status utap

Systemd servers

When using systemd servers, the following are the commands on the Database server:

To stop S-TAP process:

systemctl stop guard_utap.service

To start S-TAP process:

systemctl start guard_utap.service

To stop GIM and supervisor processes:

systemctl stop guard_gim.service

systemctl stop guard_gsvr.service

To start GIM and supervisor processes:

systemctl start guard_gim.service

systemctl start guard_gsvr.service

To verify status of Guardium product on the system:

systemctl -t service -a|grep guard

Services servers

When using services servers, the following are the commands on the Database server:

To stop S-TAP process:

svcadm -v disable guard_utap

To start S-TAP process:

svcadm –v enable guard_utap

To stop GIM and supervisor processes:

svcadm –v disable guard_gim

svcadm –v disable guard_gsvr

To start GIM and supervisor processes:

svcadm –v enable guard_gim

svcadm –v enable guard_gsvr

To verify status of Guardium product on the server:

svcs | grep guard

Parent topic: Linux and UNIX systems: S-TAP operation and performance

Linux and UNIX systems: Determine the S-TAP version

Procedure

1. From the GUI, the S-TAP® version number is displayed in Manage > System View > S-TAP Status Monitor
2. Alternatively, you can display the S-TAP version number from the UNIX command line of the database server, by running the guard_stap binary with the -version or --version argument For example, assuming the S-TAP is installed in the default installation directory, enter one of these commands:

```
-bash-3.2#  <guardium_base>/modules/STAP/current/guard_stap --version

-bash-3.2#  <guardium_base>/guard_stap/guard_stap --version
STAP-doberman_r20511_1-20100728_0514
```

Parent topic: Linux and UNIX systems: S-TAP operation and performance

Linux and UNIX systems: Increasing S-TAP® throughput

You can configure an S-TAP that reports to multiple Guardium systems to increase the throughput of data.

You can configure any S-TAP to create multiple threads to increase the throughput of data. If the S-TAP configuration file defines more than one Guardium system, a thread can be created for each Guardium system. S-TAP creates extra threads, matching the number of Guardium systems, in v10.1.4 and higher up to 10 threads. When participate_in_load_balancing parameter is set to 4, the K-TAP creates a similar number of buffers matching the number of Guardium systems up to 5 threads. The K-TAP alternates between the buffers, placing entire packets in each buffer. Each S-TAP thread reads from a different K-TAP buffer, and sends traffic data to a single Guardium system.

In this configuration, no one Guardium receives all the data from the S-TAP. The distribution is similar to that used when participate_in_load_balancing is set to 1.
Attention: Prior to V10 GPU200, when a Guardium system becomes unavailable, no failover is provided. Data that was being sent to a Guardium system is lost until the system becomes available or the configuration is changed.
Attention: Prior to V10 GPU300, if the S-TAP configuration file defines more than one Guardium system, a thread can be created for each Guardium system. This feature is activated only when participate_in_load_balancing parameter is set to 4.

Encrypted and unencrypted A-TAP traffic cannot be sent to the same Guardium system. This is similar to the situation when participate_in_load_balancing is set to 1

Parent topic: Linux and UNIX systems: Configuring S-TAP
Parent topic: Linux and UNIX systems: S-TAP operation and performance

Linux and UNIX systems: Monitoring S-TAP in the GUI

Use these standard reports and views to monitor your STAP status in the GUI.

You can define new queries or reports on the Rogue Connections domain, and you can create alerts that are based on exceptions that are created by S-TAPs, but other domains that are used by S-TAP reports are system-private and cannot be accessed by users.

System View

S-TAP Status Monitor in the System Monitor window: For each S-TAP reporting to this Guardium system, this report identifies the S-TAP Host, S-TAP Version, DB Server Type, Status (active or inactive), Last Response Received (date and time), Instance Name, Primary Host Name, and true/false indicators for: KTAP, TEE, MS SQL Server Shared Memory, DB2® Shared Memory, Win TCP, Local TCP monitoring, Named Pipes Usage, Encryption, Firewall, DB install Dir, DB port Min and DB Port Max.

Note: The DB2 shared memory driver has been superseded by the DB2 Tap feature.

S-TAP Status Monitor: For each S-TAP reporting to this Guardium system, this report identifies the S-TAP Host, DB Server Type, S-TAP Version, Status (active or inactive), Inspection Engine status, Last Response Received (date and time), Primary Host Name, and true/false indicators for: Firewall and Encrypted. Click the S-TAP Status and the Inspection Engine status to see the Verification status on all Inspection Engines.

S-TAP Events: For each S-TAP reporting to this Guardium system, this report identifies the S-TAP Host, Timestamp, Event type (Success, Error Type, and so on), and Tap Message.

If no messages display in the S-TAP Events panel, the production of event messages may have been disabled in the configuration file for that S-TAP®. If this is the case, you may be able to locate S-TAP event messages on the host system in the syslog file.

Tap Monitor

Rogue Connections: This report is available only when the Hunter option is enabled. The Hunter option is only used when the Tee monitoring method is used. This report lists all local processes that have circumvented S-TAP to connect to the database.

S-TAP Configuration Change History: This report is displayed only when an inspection engine is added or changed. Lists S-TAP configuration changes – each inspection engine change is displayed on a separate row. Each row lists the S-TAP Host, DB Server Type, DB Port From, DB Port To, DB Client IP, DB Client Mask, and Timestamp for the change.

Primary Guardium® Host Change Log: Log of primary host changes for S-TAPs. The primary host is the Guardium system to which the S-TAP sends data. Each line of the report lists the S-TAP Host, Guardium Host Name, Period Start, and Period End.

S-TAP Status: Displays status information about each inspection engine that is defined on each S-TAP Host. This report does not have From and To date parameters, since it is reporting current status. Each row of the report lists the S-TAP Host, DB Server Type, Status, Last Response, Primary Host Name, Yes/No indicators for the following attributes: K-TAP Installed, TEE Installed, Shared Memory Driver Installed, DB2 Shared Memory Driver Installed, Named Pipes Driver Installed, and App Server Installed. In addition, it lists the Hunter DBS.

Inactive S-TAPs Since: Lists all inactive S-TAPs that are defined on the system. It has a single runtime parameter: QUERY_FROM_DATE, which is set to now -1 hour by default. Use this parameter to control how you want to define *inactive*. This report contains the same columns of data as the S-TAP Status report, with the addition of a count for each row of the report.

Parent topic: Linux and UNIX systems: S-TAP operation and performance

Linux and UNIX systems: S-TAP statistics

The S-TAP statistics are stored in the database table STAP_STASTICS on the collector. This table stores the statistics sent by the S-TAP to the sniffer. There is no pre-defined report for this table.

To access, use the GUI. You can create alerts based on results.

The time interval is in hours (example, 5 is every 5 hours). Use - (minus) for a time interval less than 1 hour.

Fields in Table

- TIMESTAMP
- SOFTWARE_TAP_HOST
- TOTAL_BYTES_SO_FAR
- TOTAL_BYTES_DROPPED_SO_FAR
- TOTAL_BYTES_IGNORED
- TOTAL_BUFFER_INIT
- IOCTL_REQUESTS
- TOTAL_RESPONSE_BYTES_IGNORED
- System CPU%
- System Idle%
- STAP CPU%
- Buffer recycled

Parent topic: Linux and UNIX systems: S-TAP operation and performance

Linux and UNIX systems: S-TAP Monitor (guard_monitor)

The S-TAP Watchdog (guard_monitor) monitors S-TAP performance and responsiveness. You can configure specific actions that are triggered when the S-TAP exceeds certain thresholds.

Note: On HP-UX 11.11, the information about the process command is limited to 64-characters. This means that if the full path to the guard_stap binary is longer than 64-characters, the Guardium monitor cannot recognize it.

Monitoring covers:

- CPU utilization: checked with the *ps* command or using cpu time from procfs
- CPU responsiveness to polling: checked by sending the S-TAP process a console request and waiting for a response.

If S-TAP CPU utilization exceeds the configured threshold, or if S-TAP does not respond to the console request, the following actions can be taken:

- Automatically run guard_diag.
- Automatically kill the S-TAP process.
- Automatically core dump and kill the S-TAP process.
- Automatically trace S-TAP process.

Guard Monitor installs automatically at the end of the S-TAP installation. There are no user prompts and no install progress is shown. During S-TAP uninstall, Guard Monitor is automatically uninstalled. The user no longer has the option to reboot in the installer and is instead just notified that a reboot is necessary to complete the uninstall. This reboot is not critical but it is necessary if the user intends to install S-TAP again on the system. If the user uninstalls, does not reboot, and then tries to reinstall there will be an popup blocking the installation notifying the user that S-TAP is partially installed and the server needs to be rebooted.

The guard_monitor runs with its configuration file, guard_monitor.ini as its argument. The monitor is controlled by using the guard_monitor.ini file. For Shell installations, you can make all configuration changes directly on the configuration file. For GIM, use the interface in the GUI to make any changes.

Guard_monitor is not enabled by default. In shell installations, enable it from inittab by uncommenting the “umon” line, or by using the services control facility for the particular Operating Systems (initctl for RedHat 6, systemctl for RedHat 7, SMF for Solaris 10 and up). For GIM installations, guard_monitor is enabled by setting `STAP-UTILS_START_MONITOR=y`.

Note: guard_monitor requires administrative privileges (root).

The default location for the S-TAP Monitor output is /var/tmp/monitor. This location can be configured from guard_monitor.ini (configuration file). See the example of the guard_monitor.ini file at end of this topic.

After enabling guard_monitor, make sure the process is running on the database server.

Examples of settings

Default thresholds are provided for each function. For example, you might want to monitor CPU usage, and set one threshold (75%) for gathering diagnostic information and a higher threshold (85%) at which the S-TAP is killed. You would set auto_diag=1 to enable gathering of diagnostic information, and diag_high_cpu_level=7500 to gather diagnostic information when CPU usage reaches 75%. Then set auto_kill_on_cpu_enable=1 to enable automatic killing of the S-TAP process, and set auto_kill_on_cpu_level=8500 to kill the process when CPU usage reaches 85%.

But you may not want to keep killing the S-TAP process repeatedly, so you can set a limit on that as well. You can limit how many times the process can be killed within one hour by setting kill_num_in_hour=5. Then specify what should happen when the limit is reached: code final_action=1 to disable the S-TAP, or final_action=2 to allow it to continue running.

Guard_monitor CPU polling parameters

guard_monitor.ini	GIM	Description	Default
poll_cpu_interval	STAP-UTILS_MONITOR_POLL_CPU_INTERVAL	Interval, in seconds, at which guard_monitor checks S-TAP CPU utilization. When checking CPU utilization, guard_monitor measures the average CPU utilization over the life of the guard_stap process using *ps*. This means that S-TAP has to run above the CPU threshold for some time before guard_monitor detects a problem.	10
cpu_measurement_timeslice		Interval over which CPU consumption is measured, in seconds. When set to 0, consumption is measured across the life of the process.	5
poll_stap_interval	STAP-UTILS_MONITOR_POLL_STAP_INTERVAL	Interval at which guard_monitor sends a console S-TAP request, in seconds.	10
cpu_measurement_mode Introduced in v10.1.4	NA	Method for calculating CPU consumption: 0: measure CPU consumption relative to one core 1: measure CPU consumption out of total CPU capacity of Guardium system.	0
nonresponsive_action	NULL	Action taken when S-TAP does not respond to polls. • diags • trace • NULL	

Auto-Diag action

If S-TAP CPU utilization exceeds the configured threshold, the most basic action guard_monitor takes is an automatic guard_diag.

By default, the output from the guard_diag is placed in /var/tmp. The file name is derived from the machine name, and the time/date run; it always starts with diag.ustap.

guard_monitor.ini	GIM	Description	Default
auto_diag	STAP-UTILS_MONITOR_AUTO_DIAG	Enables automatic guard_diag. 0=no, 1=yes.	1
diag_high_cpu_level	STAP-UTILS_MONITOR_DIAG_HIGH_CPU_LEVEL	The S-TAP CPU threshold at which guard_monitor initiates a guard_diag. Enter (%CPU threshold*100). v10.1.4 and higher: When cpu_measurement_mode=1, the % can be higher than 100.	7500
diag_num	STAP-UTILS_MONITOR_DIAG_NUM	Enables creation of more than one guard_diag output. Integer.	2

Auto-Kill action

Use these parameters to configure the S-TAP auto-kill.

guard_monitor.ini	GIM	Description	Default
auto_kill_on_cpu_enable	STAP-UTILS_MONITOR_AUTO_KILL_ON_CPU_ENABLE	Enable automatic S-TAP kill. 0=no, 1=yes.	
auto_kill_on_cpu_level	STAP-UTILS_MONITOR_AUTO_KILL_ON_CPU_LEVEL	The S-TAP CPU threshold at which guard_monitor kills S-TAP. Enter (%CPU threshold*100). v10.1.4 and higher: When cpu_measurement_mode=1, the % can be higher than 100.	8500
kill_num_in_hour	STAP-UTILS_MONITOR_KILL_NUM_IN_HOUR	The maximum number of times guard_monitor is killed in an hour. Integer value.	5
final_action	STAP-UTILS_MONITOR_FINAL_ACTION	Action taken when max kills per hour is reached. • 1 = Disable S-TAP. • 2 = Stop killing S-TAP and let it continue.	

Core dump S-TAP before kill

Some S-TAP issues, such as when S-TAP gets stuck in a loop, require more information than provided in the guard_diag output.

The guard_monitor performs automatic core dumping of the S-TAP process. The guard_monitor core dumps S-TAP before killing the process (if S-TAP auto kill is enabled).

Location of core dumps created by guard_monitor: /var/tmp/monitor/coredumps

These parameters configure auto core dumps:

guard_monitor.ini	Description	Default
force_core_before_kill	The type of core dump to generate: sigsegv: This is the most portable of the options, but requires the SA to configure ulimit to enable core dumping. gcore: The most useful, but requires gcore to be installed on the system. Linux platforms only. pstack: Least useful of the options, but may be the only utility available on certain systems. Linux platforms only. NULL: disabled	
force_core_when Introduced in v10.1.4	When to collect a core dump: limitsexceeded: collect core when S-TAP is killed due to exceeding a resource limit nonresponsive: collect core when S-TAP is killed due to it being nonresponsive always: always collect core	always
kill_oldcore_saved	Integer. Specifies whether generated core dumps are saved. When set to non-zero, guard_diag keeps all core dumps generated. Otherwise, it deletes the old core dumps each time a new one is generated.	

Example of guard_monitor.ini

```
The following section header is required for GIM to recognize this .ini file.
; otherwise, it serves no purpose

[TAP]
; output dir for monitor logs, diags, traces, etc.
monitor_output_dir=/var/tmp
; location of guardium installation (need not be where monitor is installed, for example, /usr/local)
stap_dir=/usr/local
; ip to connect to for downloading configuration file and uploading diags and trace output
; this is parsed out of the guard_tap.ini, but backup value here is kept in sync
sqlguard_ip=NULL
; polling interval to verify that server end is still alive (secs)
poll_server_interval=20
; polling interval to check CPU level (secs)
poll_cpu_interval=10
; polling interval to communicate with STAP (secs)
poll_stap_interval=10
; maximum file size of monitor log file (KB)
monitor_log_rotate_size=1024
; number of rotated monitor logs to keep
monitor_log_rotate_num_kept=5
; maximum file size of log files (KB)
log_rotate_size=4096
; number of rotated logs to keep
log_rotate_num_kept=5
; logs to rotate
logs_to_rotate=/tmp/guard_stap.stderr.txt,/tmp/guard_stap.stdout.txt,/usr/local/guardium/guard_stap/ktap/ktap_install.log,/us
r/local/guardium/guard_stap/guard_discovery.stderr.log
; maximum number of STAP kills per hour (doesn't count kills resulting from auto_kill_on_intercept)
kill_num_in_hour=5
; disable STAP when kills per hour limit hit or disable kills and let STAP continue
; disable STAP: 1; disable kill: 2
final_action=2
; automatic kill STAP on CPU level on/off (1/0)
auto_kill_on_cpu_enable=0
; CPU level for kill (% * 100)
auto_kill_on_cpu_level=8500
; snif timeout for kill (secs, 0 disabled)
auto_kill_on_snif_timeout=0
; KTAP timeout for kill (secs, 0 disabled)
auto_kill_on_ktap_timeout=0
; PCAP timeout for kill (secs, 0 disabled)
auto_kill_on_pcap_timeout=0
; TEE timeout for kill (secs, 0 disabled)
auto_kill_on_tee_timeout=0
; SHMEM timeout for kill (secs, 0 disabled)
auto_kill_on_shmem_timeout=0
; automatic diags on/off (1/0)
auto_diag=1
; number of diags runs
diag_num=2
; time between diags runs (mins)
diag_interval=2
```

```
; keep old diag files or not yes/no (1/0)
diag_oldrun_saved=0
; kill STAP process after diags yes/no (1/0)
diag_auto_kill=0
; CPU level to trigger diags (% * 100)
diag_high_cpu_level=7500
; snif timeout to trigger diags (secs, 0 disabled)
diag_snif_timeout=0
; KTAP timeout to trigger diags (secs, 0 disabled)
diag_ktap_timeout=0
; PCAP timeout to trigger diags (secs, 0 disabled)
diag_pcap_timeout=0
; TEE timeout to trigger diags (secs, 0 disabled)
diag_tee_timeout=0
; SHMEM timeout to trigger diags (secs, 0 disabled)
diag_shmem_timeout=0
; automatic trace on/off (1/0)
auto_trace=0
; max time to run trace (secs)
trace_max_time=30
; max log file size for trace (MB)
trace_max_log_size=10
; keep old trace log files yes/no (1/0)
trace_oldlog_saved=0
; kill STAP when trace runs to completion yes/no (1/0)
; (e.g. is not cancelled due to low CPU)
trace_kill_on_complete=0
; CPU level to trigger trace (% * 100)
trace_high_cpu_level=6000
; low CPU level to cancel trace (% * 100)
trace_low_cpu_level=3500
; timeout for snif communication trigger (secs, 0 disabled)
trace_snif_timeout=0
; timeout for KTAP communication trigger (secs, 0 disabled)
trace_ktap_timeout=0
; PCAP timeout to trigger trace (secs, 0 disabled)
trace_pcap_timeout=0
; TEE timeout to trigger trace (secs, 0 disabled)
trace_tee_timeout=0
; SHMEM timeout to trigger trace (secs, 0 disabled)
trace_shmem_timeout=0
; auto-kill STAP when we're not intercepting databases that are configured yes/no(1/0)
; feature is also disabled when guard_tap.ini shows that STAP is running as root
auto_kill_on_intercept=0
; minimum time between STAP requested kills (mins)
intercept_min_time_interval=15
; maximum number of intercept kills per hour
intercept_max_num_in_hour=0
; number of seconds across which CPU consumption is measured    (secs, 0 disabled)
; when disabled, CPU consumption is measured across the life of the process
cpu_measurement_timeslice=0
; method for calculating CPU consumption (0 or 1)
; 0: measure CPU consumption relative to one core
; 1: measure CPU consumption taking number of cores into account
cpu_measurement_mode=0
; when to collect a core dump (always, limitsexceeded, nonresponsive)
; limitsexceeded: collect core when STAP is killed due to exceeding a resource limit
; nonresponsive: collect core when STAP is killed due to it being nonresponsive
; always: always collect core
force_core_when=always

; STAP nonresponsive action
; run diags before killing STAP    : diags
; collect trace before killing STAP: trace
; no collection, just kill STAP    : NULL
nonresponsive_action=diags
```

Parent topic: Linux and UNIX systems: S-TAP operation and performance

Linux and UNIX systems: Troubleshooting S-TAP problems

You can use the S-TAP Status monitor tab of the System View to begin investigating any problems. Sometimes you might need to use other tools, particularly if you are monitoring databases for which the inspection engines cannot be verified.

If an S-TAP is not connected to your Guardium system

Check whether the IBM Security Guardium S-TAP service is running on the database server:
On the database server, from the command line, run the command ps -ef | grep stap to verify that the S-TAP® process is running. In the process list, look for /guardium/guard_stap.

How can I find the S-TAP version?

- From the GUI, the S-TAP version number is displayed in Manage > System View > S-TAP Status Monitor
- Alternatively, you can display the S-TAP version number from the command line of the database server.

Run debug from the command line to quickly identify configuration issues

Use the syntax <stap_program> <parameter_file> <debug_level>, where 4 is the level for normal debug. (Other values do different things, not all of them debug).
For example: /usr/local/guardium/guard_stap/guard_stap /usr/local/guardium/guard_stap/guard_tap.ini 4

Verify the connection between the database server and the Guardium system

- Verify that you can ping the Guardium system at *sqlguard_ip* from the database server.
- If the ping is successful, verify that you can telnet to the following ports on the Guardium system: 16016/16018

If there is a firewall between the database server and the Guardium system

Verify that the following ports are open for traffic between these two systems: TCP Port 16016 or TLS Port 16018 for encrypted connections.

Note: Use the following command to check the port availability: `nmap -p port guardium_hostname_or_ip`

Verify that the sqlguard_ip parameter is set to the correct *guardium_hostname_or_ip* for the Guardium system that you are connecting to.

1. Click Manage > Activity Monitoring > S-TAP Control to open S-TAP Control.
2. Locate the S-TAP Host for the IP address that corresponds to your database server.
3. Expand the Guardium Hosts subsection, and verify that the active Guardium Host is correctly configured.
4. If necessary, click Modify to update the Guardium Hosts.

Verify that the S-TAP process is not repeatedly restarting

On the database server, run the command `ps -eaf | grep stap` to verify that the process for S-TAP is not changing.

Verify that S-TAP Approval is not turned on

If S-TAP Approval is turned on, any new S-TAP that connects to the Guardium system is refused.

1. Click Manage > Activity Monitoring > S-TAP Certification to open S-TAP Certification.
2. Look at the S-TAP Approval Needed check box. If this box is checked, new S-TAPs can connect to this Guardium system only after they have been added to the list of approved S-TAPs.
3. If S-TAP Approval is turned on, select Daily Monitor > Approved Tap Clients to view a list of approved S-TAPs. If the S-TAP that you are investigating is not on this list, return to the S-TAP Certification pane, enter the IP address of the S-TAP in the Client Host field, and click Add.

If the S-TAP shows green status but no data is being processed

Check the status of the A-TAP.

S-TAP verification issues

The verification process attempts to log in to your database's STAP client with an erroneous user ID and password, to verify that this attempt is recognized and communicated to the Guardium system. Your S-TAP could be configured in a way that prevents the inspection engine message from reaching the Guardium system from which the request was made.

These configuration details include:

- Load balancing: if the S-TAP is configured to return responses to more than one Guardium system, the error message could be sent to a different Guardium system.
- Failover: If secondary Guardium systems are configured for the S-TAP, the error message could be sent to a secondary Guardium system if the primary Guardium system is too busy.
- Db_ignore_response: if the S-TAP is configured to ignore all responses from the database, it does not send error messages to the Guardium system.
- Client IP/mask: if any mask is defined that is not 0.0.0.0, it could prevent the error message from being sent.
- Exclude IP/mask: if any mask is defined that is not 0.0.0.0, it could prevent the error message from being sent.

Related topics:

- Linux and UNIX systems: Monitoring S-TAP in the GUI
- Linux and UNIX systems: S-TAP Monitor (guard_monitor)
- Linux and UNIX systems: Inspection engine verification

Parent topic: Linux and UNIX systems: S-TAP operation and performance

DB2 for IBM i S-TAP

You can use the Guardium DB2 for i S-TAP to monitor and report on any database access on IBM i. This includes any programs, such as RPG, that use native database I/O operations or SQL access.

You can use information gathered by the Guardium DB2 for i S-TAP to create activity reports, help you meet auditing requirements, and generate alerts of unauthorized activity. Detailed auditing information includes:

- Session start and end times
- TCP/IP address and port
- Object names (for example, tables or views)
- Users
- SQLSTATEs
- Job and Job numbers
- SQL statements and variables
- Client special register values
- Interface information, such as ODBC, ToolboxJDBC, Native JDBC, .NET, and so on

The S-TAP receives data from two sources:

- SQL Performance Monitor (otherwise known as database monitor) data for SQL applications
- Audit entries from the QSYS/QAUDJRN audit journal for applications using non-SQL interfaces

Data from these sources includes:

- Any SQL access whether it is initiated on the IBM i server or from a client
- Any native access that is captured in the audit journal

The S-TAP sends this data to the Guardium system in real time.

For more information about the DB2 for i S-TAP and related topics, refer to these sources:

- Using IBM Security Guardium for monitoring and auditing IBM DB2 for i database activity: this developerWorks article introduces IBM Guardium, the DB2 for i S-TAP, and key related details.
- IBM i on IBM Knowledge Center: look here for information about IBM i, audit journaling, and other related topics.

i S-TAP for encryption, load balancing, and failover

The IBM i S-TAP supports TLS encryption and S-TAP session load balancing/failover.

Note: i S-TAP TLS support and load balancing is supported only for IBM i 7.1 and 7.2.

Similar to UNIX S-TAPs, i S-TAP configuration parameters are saved in a guard_tap.ini file in the /usr/local/guardium directory on the IBM i server.

Administrators configure the S-TAP is done using the same APIs and UI (S-TAP Control) as other UNIX S-TAPS. When the GUI or API is used to make a change to the S-TAP configuration, the Guardium sniffer sends a message to the S-TAP, which backs up the old .ini file, saves the configuration to the new .ini file and then restarts itself.

Administrators can set up encrypted communication between the S-TAP and the appliance using the S-TAP configuration controls as well as set up various load balancing options.

Using S-TAP failover and load balancing

The failover and load balancing options for the i S-TAP are similar to what exists for UNIX S-TAPs. Use the participate_in_load_balancing parameter to determine whether to use failover or load balancing behavior, and use the SQLGuard sections of your S-TAP to set up primary, secondary, and tertiary Guardium hosts.

One difference is that there is no need for participate_in_load_balancing=3; because of the way the I S-TAP communication is architected, complete session information is available on each message. This means that even before the enhancements delivered in this patch, you could have used hardware balancing (such as F5) with participate_in_load_balancing=1 and a virtual IP address in the primary SQLGuard section of the configuration file.

In a failover configuration, the S-TAP is configured to register with multiple collectors, but only send traffic to one collector at a time (participate_in_load_balancing=0). The S-TAP in this configuration sends all its traffic to one collector unless it encounters connectivity issues to that collector that triggers a failover to a secondary collector.

How to use AppEvent from IMS

The data holding user information of an APP_EVENT DLI call needs to have similar syntax as GuardAppEvent api.

The first two bytes represent ccsid of the encoding of the following bytes. For example, 0x04B8 stands for ccsid 1208. The following bytes need to have the syntax as below:

SELECT

'GuardAppEvent:Start',

'GuardAppEventType:type',

'GuardAppEventUserName:name',

'GuardAppEventStrValue:string',

'GuardAppEventNumValue:number',

'GuardAppEventDateValue:date'

FROM DUAL

For further reference for type, name, string, number, date, check GuardAppEvent API.

Currently, only UTF8 encoding is supported.

Monitoring strategy

Make your monitoring and auditing effective and efficient by developing a strategy that recognizes and fulfills your regulatory and other requirements.

After you know what data you need, develop a strategy for collecting it with as little extraneous data as possible. Monitoring and logging data that you do not need uses up disk space and processing power, and generates extra network traffic. There are several areas where you can implement your strategy:

Database monitoring

The global SQL monitor captures SQL information and puts it into a queue for the S-TAP. You can use the filtering capabilities of the monitor to control which types of users and objects are queued. By default, these types of entries are not forwarded from the S-TAP to the Guardium system:

SQL Abbreviation	Meaning
AD	ALLOCATE DESCRIPTOR
CL	CLOSE
DA	DEALLOCATE DESCRIPTOR
DE	DESCRIBE
EX	EXECUTE (the SQL statement executed is audited)
FE	FETCH
FL	FREE LOCATOR
GD	GET DIAGNOSTICS
GS	GET DESCRIPTOR

HL	HOLD LOCATOR
PR	PREPARE (except authorization errors are captured)
RE	RELEASE
RG	RESIGNAL
SC	SET CONNECTION
SD	SET DESCRIPTOR
SG	SIGNAL

Audit journal

You can configure the system audit journal to capture only those entries that concern objects of interest or users of interest. By default, entries of these types are sent from the S-TAP to the Guardium system:

SQL Abbreviation	Meaning
ZR	Read object
ZC	Change object
CA	Authority change
AD	Auditing change
AF	Authority failure
CO	Create object
DO	Delete object
SV	System Value change
GR	General purpose audit record
OM	Object moved or renamed
PG	Primary group change
PW	Invalid password or user ID
OW	Change owner
OR	Object restored
RA	Restore authority change
RO	Restore owner change
RZ	Restore primary group change

Only those entries that relate to database objects are forwarded:

- *FILE (a table, view, index, logical file, alias, or device file)
- *SQLUDT (an SQL user-defined type)
- *SQLPKG (an SQL package)
- *PGM (a procedure, function, or program)
- *SRVPGM (a procedure, function, global variable, or service program)
- *DTAARA (an SQL sequence)

On the Guardium system

You can define policies that control which information that is received from the S-TAP is ignored, and what actions to take based on other items.

Ignoring data after it has been sent over the network is inefficient. Wherever possible, filter out information that you do not need before it is queued for the S-TAP.

Parent topic: DB2 for IBM i S-TAP

Installing the S-TAP for IBM i

Follow these steps to install or uninstall the S-TAP.

Before you begin

The DB2 for i S-TAP requires Portable Application Solutions Environment (PASE), which is automatically started and stopped as needed when a user starts and stops the DB2 for i S-TAP from the IBM Guardium user interface.

You must know the IP address of the Guardium system to which this S-TAP will connect.

When you download the S-TAP, be sure to filter for the IBM i platform, to ensure that you download the correct package.

About this task

The Guardium Installation Manager (GIM) is not supported on IBM i.

You can use 5250 emulator software to connect to the IBM i system remotely.

Procedure

1. On the IBM i server, enter this command to open the PASE shell: call qp2term.
2. In the PASE shell environment, create a temporary directory to hold the S-TAP installation script, such as /tmp.
3. Use FTP to move the following S-TAP installation shell script to that temporary directory: guard-itap-9.0.0_r*nnnnn*-aix-5.3-aix-powerpc.sh
4. In the same directory, run this command:

```
guard-itap-9.0.0_rnnnnn-aix-5.3-aix-powerpc.sh guardium_host_IP
```

where *guardium_host_IP* is the IP address of the Guardium system.

Results

The S-TAP is installed in /usr/local/guardium. After the installation is complete, the S-TAP attempts to start the processes that enable activity monitoring and to connect to the Guardium system by using the IP address that was specified with the installation command.

What to do next

To validate the successful installation and start of the audit process, log in to the IBM Guardium web console as an administrator, navigate to the System View tab, and check the status of the S-TAP.

Parent topic: DB2 for IBM i S-TAP

Uninstalling the S-TAP

Procedure

To stop and uninstall the S-TAP, issue these commands:

```
RUNSQL SQL('call SYSPROC/SYSAUDIT_End') COMMIT(*NONE)
RMVDIR DIR('/usr/local/guardium') SUBTREE(*ALL)
```

Defining the S-TAP for IBM i

After you install the S-TAP, ensure that it can communicate with the Guardium system.

Before you begin

You must know the log-in credentials for the IBM i system.

About this task

The high-level steps to configure the S-TAP are:

1. Define DB2 for i as a recognized data source to IBM Guardium and test the connection.
2. Populate the Guardium system with information from the configuration file on IBM i that was created when you installed the DB2 for i S-TAP, using the Custom Table Builder process.
3. Create a DB2 for i configuration report. It is from this report interface that you can invoke the Guardium APIs that enable you to start and stop the monitoring process, get status information, and update configuration parameters, including filtering values.

Procedure

1. Click Setup > Tools and Views > Datasource Definitions to open the Datasource Builder. Select Custom Domain from the Application Selection box. Click Next.
2. In the Datasource Finder, click New, which opens the Datasource Builder.
3. Select DB2 for i as the Database Type and then add the appropriate information for the host, service name, and credentials. Click Apply.
4. Click Test Connection to ensure that the configuration succeeded.
5. Click Tools > Report Building.
6. Click Custom Table Builder. Select DB2 for i S-TAP Configuration and then click Upload Data. The Datasource Finder displays a list of DB2 for i S-TAPs.
7. Select your DB2 for i data source from the list/ Click Add.
8. On the Import Data screen, ensure the DB2 for i data source appears. Click Apply and then click Run Once Now. You should see a message that the operation ended successfully with one row inserted.
9. Click Customize in the Guardium title bar. Then click Add Pane.
10. Give the pane a new name, such as My New Reports, and then click Apply.
11. My New Reports appears in the Customize pane. Click the icon next to the name. In the Layout dropdown list, choose Menu Pane. Click Save. Your new pane appears as a tab.
12. Click Report Building in the navigation pane.
13. From the query dropdown list, click DB2 for i S-TAP configuration, then click Search.
14. Select the DB2 for i S-TAP configuration and then click Add to My New Reports (or the name that you specified in step 10).
15. Open the My New Reports tab, which now displays the IBM i report row. Double-click a row in the report and select Invoke. A list of IBM Guardium APIs that you can select is displayed.
16. Select update_istap_config.
17. When you select a Guardium API, the parameters for that API are displayed. You can change any values that you need to. Change the value of the start_monitor parameter to 1. Click Invoke Now.

Results

Using the data that you have entered, the update_istap_config API performs these tasks:

- Creates the message queue that will be used to send entries from the S-TAP to the Guardium system and starts a global database monitor using a view with an INSTEAD OF trigger, which sends the entries to the message queue.
- Starts PASE and the S-TAP.
- Receives journal entries from QAUDJRN and adds them to the message queue.

Parent topic: DB2 for IBM i S-TAP

Guardium Installation Manager

You can use the Guardium® Installation manager (GIM) to install and maintain Guardium components on managed servers.

The GIM component includes a GIM server, which is installed as part of the Guardium system, and a GIM client, which must be installed on servers that host databases or file systems that you want to monitor. The GIM client is a set of Perl scripts that run on each managed server. After you install the GIM client, it works with the GIM server to perform these tasks:

- Check for updates to installed software
- Transfer and install new software
- Uninstall software
- Update software parameters
- Monitor and stop processes that run on the database server

For example, you can use GIM to install your S-TAP modules and keep them up-to-date.

The GIM client uses port 8444 to communicate with the GIM server.

You can use the GIM server through the Guardium user interface or through the command-line interface (CLI).

The software modules that you can deploy by using GIM are packaged as GIM bundles. A *bundle* is a file of type gim that contains software that can be deployed by using GIM.

If your environment includes a Guardium system that is configured as a central manager, you must decide which Guardium systems you want to use as GIM servers. You can either manage all of your GIM clients, up to 4000, from a single Guardium system, such as the central manager, or you can manage them in groups from the different Guardium systems. If you manage all of your GIM clients from a single Guardium system, then you can view the status of all the GIM clients and perform related tasks from that one UI. If you choose to manage your GIM clients in groups from separate Guardium systems, then you can use each UI to work with the GIM clients that it manages; no overall view is available.

If you upgrade to Version 10.0 from V9.0 GPU patch 50 or later, there is no change in how you can view information about GIM clients. If you upgrade from an older version, these restrictions apply: After you upgrade your Central Manager, you can still view information about GIM clients that are assigned to other Guardium systems, but you can no longer do provisioning to those GIM clients from the Central Manager. After you upgrade all your Guardium systems, you can view each GIM client only from the Guardium system that is its GIM server.

To manage large numbers of GIM installations, you can create groups of GIM clients. Then, you can use the groups to install, update, and manage software bundles.

The GIM client monitors the processes that you install by using GIM. It checks the heartbeat of each process once each minute, and passes status changes for the processes to the GIM server. The status of each process is displayed on the Process Monitoring panel. Changes are reflected within three minutes. Changes to the status of the GIM client itself are reflected according to the interval at which the client polls the server and delivers its "alive message".

Note: When performing a system backup and restore from one server, which has GIM defined, to another server, then the user must configure a GIM failover to the restore server. This GIM configuration applies to a Backup Central Manager or a System backup and restore.

- Quick start for deploying monitoring agents
  Use the Deploy Monitoring Agents tool to automatically activate GIM clients, install S-TAPs, and begin monitoring database traffic.
- Managing software with GIM
- GIM Server Allocation
  Remotely connect to a pre-installed and inactive (not connected to any collector) GIM agent and make it connect to some collector without the need to access the database server.
- Installing the GIM client on a Windows server
  Learn how to install the GIM client for Windows using either an interactive installer or a silent installation. Instructions are also provided for uninstalling the GIM client.
- Installing the GIM client on a UNIX server
  Use this command to install the GIM client on each database server.
- Uninstalling GIM and its modules on a UNIX database
  You can uninstall GIM and its modules either from the GUI, or on the database server itself.
- Upgrading the GIM client
  You can use GIM to upgrade the GIM client to a newer version.
- Using groups with GIM
  You can use groups to make some GIM tasks easier.
- Copying a K-TAP module by using GIM
  If you build a custom K-TAP module for a Linux database server, you can use GIM to copy that module to other Linux database servers.
- GIM dynamic updating
  GIM clients check for updates from the GIM server at regular intervals. The GIM server can calculate the best polling interval to use based on system conditions.
- When you upgrade your database server operating system
  When you upgrade the operating system on your database server, you can allow the GIM client to make the required changes in itself and your GIM-installed modules.
- Distributing GIM bundles to managed units
  You can distribute GIM bundles to managed units in order to deploy them on the GIM clients managed by those managed units.
- Removing unused GIM bundles
  You can remove GIM bundles from your GIM server if they are no longer used on any database server.
- Running GIM diagnostics
  You can run diagnostics on GIM clients to verify that the GIM server has accurate data about each client.
- Debugging GIM operations
  You might need to turn on debugging in order to troubleshoot a problem.
- Restarting the supervisor for Solaris with SMF support
  Use a set of CLI commands to restart the supervisor on Solaris servers with SMF support.

Quick start for deploying monitoring agents

Use the Deploy Monitoring Agents tool to automatically activate GIM clients, install S-TAPs, and begin monitoring database traffic.

The deploy monitoring agents tool simplifies the process of establishing a Guardium deployment. Building on existing Guardium installation manager (GIM) infrastructure, the deploy monitoring agents tools helps you quickly find database servers, install monitoring agents (S-TAPs), and configure inspection engines for your databases. In

addition, the tool provides a centralized view for tracking and reviewing deployment status.

- Prerequisites for deploying monitoring agents
  Review prerequisites and restrictions before you being deploying monitoring agents.
- Deploy monitoring agents
  Learn how to quickly deploy S-TAPs and configure inspection engines.

Parent topic: Guardium Installation Manager

Prerequisites for deploying monitoring agents

Review prerequisites and restrictions before you being deploying monitoring agents.

Before using the deploy monitoring agents tool to install S-TAPs and configure inspection engines on your database servers, verify the following prerequisites.

The target S-TAP installation directory must be empty or not exist. You cannot install an S-TAP into a directory that already contains any files.

Install GIM clients in listener mode

Install GIM clients in listener mode on one or more database servers in your environment. To install the GIM client in listener mode on Windows systems, omit the `--host` parameter. To install the GIM client in listener mode on systems such as AIX and Linux, omit the `--sqlguardip` parameter. For more information about GIM listener mode, see GIM Server Allocation.
Important: You may need to open a port between the GIM client on the database server and the Guardium system where you will run the deploy monitoring agents tool. The default port 8445 is used unless you specify a different port when installing the GIM client.

Upload GIM S-TAP modules to the Guardium system

Run the deploy monitoring agents tool as an administrative user from any Guardium system that is not configured as an aggregator. Before you begin, use the following procedure to upload GIM S-TAP modules to the Guardium system.

1. Navigate to Manage > Module Installation > Upload Modules.
2. Click Choose file and select the module you want to install.
3. Click Upload to upload the module to the Guardium system. After uploading, the module will be listed in the Import uploaded modules table.
4. In the Import uploaded modules table, click the check box next to the module you want to install. The module will be imported and made available for installation. After the module is imported, the Upload Modules page will reload and the module will no longer appear in the Import uploaded modules table.

For information about S-TAP offerings and supported platforms, see System requirements and supported platforms for IBM Security Guardium.

Verify that all discoverable database servers are running

Inspection engines can be automatically configured for some databases, including the following:

- DB2 for Linux, UNIX, and Windows
- Informix
- Microsoft SQL Server
- MySQL
- Oracle
- Postgre SQL
- Sybase
- Teradata

To allow the auto-configuration of inspection engines, verify that databases servers are running before deploying monitoring agents.

For more information about automatically discovering database instances, see Discover database instances.

Parent topic: Quick start for deploying monitoring agents

Deploy monitoring agents

Learn how to quickly deploy S-TAPs and configure inspection engines.

Before you begin

Run the deploy monitoring agents tool as an administrative user from any Guardium system that is not configured as an aggregator. Verify the following before you begin:

- GIM clients are installed in listener mode.
- GIM S-TAP modules are imported to the Guardium system.
- Discoverable database servers are running.

For more information, see Prerequisites for deploying monitoring agents.

About this task

The following procedure describes how to use the deploy monitoring agents tool to quickly install S-TAPs and configure inspections engines for monitoring database traffic.

Procedure

1. Open the deploy monitoring agents tool by navigating to Setup > Quick Start > Deploy Monitoring Agents.
2. In the Identify database servers section, use the IP addresses field to specify a range of IP address to search for GIM clients in listener mode. Use the  icon to specify additional IP addresses. Include wildcard (`*`) or range (`-`) characters to expand the search. For example, `10.0.0-5.*`. Use commas to separate complete IP addresses or ranges. For example, `9.70.145.165,9.70.145-148.165,9.70.145.*`.
   Important: Scanning a large number of IP addresses is time intensive and may time-out before the scan completes. Use the IP addresses fields to define a narrow range of IP addresses where you expect to find GIM clients in listener mode.

3. Click Discover to begin scanning for GIM clients in listener mode.
   Tip: By default, the discovery of GIM clients and the deployment of monitoring agents (S-TAPs) is completed in two separate steps: discovery, then deployment. This allows you to manually select the database servers where you want to install S-TAPs, as described in the following steps.

   However, it is possible to streamline the process by automatically installing S-TAPs on all compatible GIM clients that are discovered while scanning IP addresses. To enable the automated mode, click to open the Customize settings dialog and select Automatically deploy agents on discovered database servers. When using the automated mode, after specifying the IP addresses to scan, simply click the Discover and Deploy button.
4. In the Database server status section, select the database servers where you would like to deploy monitoring agents and click Deploy Agents to open the Configure monitoring agents dialog.
5. From the Configure monitoring agents dialog, review and adjust the installation parameters. Click Deploy to begin installing monitoring agents.

   The default parameters should work well for most new deployments. However, you may want to adjust the following settings for your specific environment.

   Windows installation directory

   Specify an installation directory for S-TAPs deployed on Windows database servers. The parameter is ignored and default installation paths are used when deploying on other platforms. For more information about S-TAP installation parameters, see S-TAP command line and GIM installation parameters and S-TAP install script parameters.

   Assign a Guardium collector

   Select Use enterprise load balancing to automatically assign S-TAPs based on the relative load or availability of Guardium collectors in a centrally-managed environment. For more information, see Enterprise load balancing.

   Select Specify collector to assign S-TAPs to a specific Guardium collector.
6. In the Database server status section, use the S-TAP installation status column to monitor the progress of module installation. A status of `Installed` indicates successful and complete installation.

What to do next

If the S-TAP installation status of a database server is marked `Failed`, click the icon to learn more about the problem. If a database server disappears from the Database server status after attempting to deploy monitoring agents, click Error log to learn more about the problem.

Tip: The Error log captures issues related to the Deploy monitoring agents tool. For example, if Deploy monitoring agents cannot find a module required for installation, a message is added to the Error log. Other errors are recorded in component-specific logs and made available for investigation by clicking the icon in the S-TAP installation status column.

After successfully deploying monitoring agents, you are ready to monitor traffic on your database servers and begin meeting security compliance requirements. To configure compliance monitoring, navigate to Setup > Quick Start > Compliance monitoring and see Quick start for compliance monitoring for more information.

Parent topic: Quick start for deploying monitoring agents

Managing software with GIM

- Set up by Client
  Quickly deploy S-TAPs and other software packages using the Guardium Installation Manager (GIM) Set up by Client tool.
- GIM user interfaces
  The purpose of GIM is to provide automatic installation capability for modules, taking advantage of a GIM client and GIM server residing on each database server and Guardium system respectively.
- GIM command line interface
  You can use the CLI in order to install or upgrade modules on the database server.

Parent topic: Guardium Installation Manager

Set up by Client

Quickly deploy S-TAPs and other software packages using the Guardium Installation Manager (GIM) Set up by Client tool.

Before you begin

Before using the Set up by Client tool, verify the following:

- GIM clients are installed on database servers and connected to the Guardium system.
- Compatible GIM bundles are uploaded and imported to the Guardium system.

Procedure

1. Navigate to Manage > Module Installation > Set up by Client.
2. In the Choose clients section, select the database servers where you want to install or update software using GIM. Select individual clients using check boxes in the table, or use the Select client group menu to select a group of clients. Click Next to continue.
   Attention:
   - If you add new clients while using the Set up by Client tool, refresh the browser to see the new clients.
   - When creating or updating a group and editing the Client Name or Client IP address of GIM clients, the name and address must reflect valid values for a GIM client connected to the Guardium system. If an invalid name or address is specified, the edited client will no longer appear as a member of the group.
3. In the Choose bundle section, use the Select a bundle menu to identify the software you want to install or update. Click Next to continue. After selecting a software bundle, the Selected bundle action column indicates the action that will be performed for each client:

   Install
   The selected bundle will be installed on the client. This action indicates a first-time installation of the software on the client.

Upgrade
: The bundle will be upgraded on the client. This action indicates that an earlier version of the software is currently installed on the client.

Update parameters
: The bundle parameters will be updated on the client. This action indicates that the selected software and the currently-installed software are the same version.

Downgrade
: The selected bundle will be installed on the client. This action indicates that the selected software is older than the software currently installed on the client.

None (bundle not found)
: No actions will be performed, indicating that there are no compatible actions on the client for the selected bundle.

Tip:
- Clear the Show only latest versions check box to view and work with earlier versions of a bundle.
- Clear the Show only bundles check box to identify individual modules within a bundle.
- Select the Show only compatible clients check box to hide clients that are not compatible with the selected bundle.

Attention:
- By default, the Select a bundle menu shows only the latest uploaded bundle version regardless of platform or compatibility with selected clients. To install a different bundle version for a specific platform or client, clear the Show only latest versions check box and select the required bundle.
- If you upload and import new bundles while using the Set up by Client tool, refresh the browser to see the new bundles.
- If you already have a bundle scheduled for installation, installing a new bundle removes the existing schedule.

4. In the Choose parameters section, specify values for required and optional parameters. Use the  or  icons to add or remove optional parameters. Use the  icon to search for parameters by name or description. Click Next to continue.
   Important: Unless identified as a client-specific parameter, values provided in the Choose parameters section are applied to all clients where the software will be installed, upgraded, or updated. For client-specific parameters, the value field is disabled and values are defined per-client in the Configure clients section.
5. In the Configure clients section, use the table to review and edit parameter values for each client. Editable parameters show a  icon next to the parameter value. Click the  icon to edit the value.
6. Click Install to begin the software installation. Use the  icon to schedule the installation, then click OK to continue.

What to do next

Use the Choose bundle section to monitor the software installation. Installation status is shown in the Status column. Use the  icon to refresh the installation status.
Parent topic: Managing software with GIM

GIM user interfaces

The purpose of GIM is to provide automatic installation capability for modules, taking advantage of a GIM client and GIM server residing on each database server and Guardium system respectively.

Users may also interact with GIM through the CLI. See GIM command line interface for information on installing and upgrading modules with GIM using CLI.

You can use the GUI of the Guardium Installation Manager (GIM) for these tasks:

- Process Monitoring
- Upload Module Package
- Configure, Install, or Update Modules (by client)
- Configure, Install, or Update Modules (by module)
- Rollback Mechanism

Note: If A-TAP is being used, A-TAP must first be disabled on the database server before performing a GIM-based S-TAP® upgrade or uninstall.
Note: GIM does not support the installation of native S-TAP installers (rpm, dept, bff, etc.)
Note: Installation of modules on a specific client for the FIRST TIME using the GIM utility must be in the form of a BUNDLE. Future upgrades of specific modules which are part of the installed bundle can be either as single modules or bundles.

Process Monitoring

Displays the status for GIM processes on servers.

Supervisor

The GIM Supervisor is a process with the main purpose of supervising and monitoring Guardium® processes. Specifically, it is responsible for starting, stopping, and making sure all of Guardium processes are running at all times and restarting them if they fail.

Note: For Guardium V9.0, on Solaris 5.10/5.11, GIM and SUPERVISOR are now SMF services. They are not inittab entries anymore.

To start/stop gim/supervisor use:

svcadm -v enable guard_gim

svcadm -v enable guard_gsvr

svcadm -v disable guard_gim

svcadm -v disable guard_gsvr

GIM

The GIM process is the GIM client process, which is responsible for such duties as registering to the GIM server, initiate a request to check for software updates, installing the new software, updating module parameters, and uninstalling modules.

Upload Module Package

Loads the modules package file (a .gim file containing module(s) sub-packages) to the database.

1. Click Manage > Install Management > Upload to open Upload.
2. Click Browse to browse where your package (.gim file) is on disk.
3. Click Upload to upload your package.
4. Click the Import icon of the uploaded package located under Import Uploaded modules to load the package.

Configure, Install, or Update Modules (by client)

Tip: For information about the latest GIM software management tool, see Set up by Client.

You can use this option to configure/install a module for any number of clients from packages already loaded.

The simplest, safest, and quickest way to install or uninstall modules is by using bundles. Using bundles guarantees automatic dependency and order resolution.

If you have already created groups of clients, you can use a group to specify the clients to be the target for the specified action. Otherwise use these steps to select a list of clients.

1. Click Manage > Install Management > Set up by Client (Legacy) to open the Client Search Criteria.
2. Click the Search button to perform filtered search and display the Clients panel.
3. Select the clients that will be the target for the specified action.
    - If there are more than 20 clients then the list of clients will be split onto additional pages
      Note: Clicking the Select All button will only select the clients on the current page being viewed
4. From the Clients panel, two actions can be taken:
    - Configure/install common parameters
    - Configure/install module
    - Reset Clients - By clicking Reset Clients, you can disassociate modules from selected clients and remove the client definition from the Guardium system database. Note: Resetting a client does NOT trigger module removal on the database server.
    - View installation state of this client - By clicking on the information icon you can open up the Installation Status panel and view the installation status of a client. This panel displays all modules on the client which are installed or scheduled for update or uninstall. From this panel, you can use the Edit this module icon to configure parameters for each module individually.

Configure, install, or update modules (by module)

Starting from modules, enables users to configure and install a module for any number of clients. Any required packages should have been loaded beforehand.

1. Click Manage > Module Installation > Set up by Module to open the Modules Search Criteria.
2. Click Search to perform filtered search and display the Modules panel showing all the available modules and bundles.
3. Select one or more modules and click Next to open the Clients panel.
4. Select the clients that are the target for the specified action.
   Note: If there are more than 20 clients then the list of clients splits onto additional pages Clicking the Select All button only selects the clients on the current page being viewed
5. From the Clients panel, these actions can be taken:
    - Install/update modules: Select one or more target clients and click Next, then click Install/Update
    - Modify module parameter configuration: Select one or more target clients and click Next, modify parameter values, select the target clients and click Apply to Clients
    - Click Reset Clients to disassociate modules from selected clients and remove the client definition from the Guardium system database. Note: Resetting a client does NOT trigger module removal on the database server.
    - View installation state of this client by clicking the icon to open the Installation Status panel and view the installation status of a client. This panel displays all modules on the client which are installed or scheduled for update. From this panel, the Edit this module icon can be used to configure parameters for each module individually.
    - Click Run Diagnostics: the diagnostic report is run the next time the clients sends an alive message, and is recorded in the GIM Events List.

Configure/install common parameters

1. Click Setup > Tools and Views > Parameter Configuration.
2. Select the clients in the Client Module Parameters section that you would like to modify parameters for
3. Modify any of the listed module parameters within the Client Module Parameters section
   Note: parameters may be entered in the Common Module Parameter section to, by clicking Apply to Selected, populate the selected clients in the Client Module Parameters section.
4. Click Apply to Clients, after entering values for all required parameters on all selected clients, to save the configuration to the database. Before the save, a validation is performed to make sure all required fields have values or their values are in pre-defined range.
5. After Saving configurations, click Install/Update to schedule the module for installation on the selected clients. In addition, from the Module Parameters panel you may uninstall, cancel install/update, cancel uninstall, and revert current changes. Note that the schedule date and time corresponds to the date and time on the selected clients.
   Note: The Generate Grdapi button at the front of the client line under the Client Module Parameter section enables you to view the list of grdapi commands that reflect the changes tat you have made to the module such as assigning, installing, uninstalling, scheduling, and updating of the module. These grdapi commands are provided so you can take the set of commands and apply them to other clients in a script if you would like to reproduce the changes .
   Note: The open Property content button appears in front of every writable properties and opens up a window that simplifies the editing of a long field.
   Note: The View installation state of this client button, also at the front of the client line under the Client Module Parameter section provides a view into the current installation status for the module.
   Note: When installing KTAP as part of BUNDLE-STAP, KTAP status will set to INSTALLED even if the actual KTAP module was missing for this specific platform. However a message will be shown on the GIM-EVENTS report indicating KTAP module was missing.
   Note: You should check the GIM-EVENTS report after installing bundles on the DB servers.
6. Click Back to go back to the Clients panel.

Windows S-TAP Parameters in GIM

During S-TAP installation, or to update the S-TAP configuration, you can use the WINSTAP_CMD_LINE field in the Setup by Client page.

You can input any parameter in the Setup by Client page, in the Choose parameters ribbon, using the command WINSTAP_CMD_LINE with the syntax parameter=value for [TAP] parameters, or CLI parameters (Windows: S-TAP command line installation parameters) with the syntax -param value, and it is added or updated in the guard_tap.ini.

CAUTION:
There is no validation of input to this field.
For example, the following command line options skip the installation of CAS and Named Pipes support.

```
CAS=0 NamedPipes=0
```

If you are installing an S-TAP and you do not want it to automatically discover MSSQL databases, type `START=0` in the WINSTAP_CMD_LINE column to prevent the S-TAP from starting when it is installed. You can also specify this parameter for a single database server by using the GIM API:

```
grdapi gim_update_client_params clientIP=xx.xx.xx.xx paramName=WINSTAP_CMD_LINE paramValue="START=0"
```

Additional guard_tap.ini parameters may also be set at installation. An example is paramValue="START=1 !client_timeout_sec=120&use_tls=1!"

Note: When using GuardAPI commands, the WINSTAP_CMD_LINE paramValue should be quoted and each parameter separated by spaces, such as paramValue="START=1 CAS=0" as in the prior example. A lack of spaces can cause the subsequent installation to not complete as anticipated.

Configure/install module

1. If configuring, installing, or updating:
    a. by client
        i. Click Next to display the Common Modules panel where a list of all available common modules and bundles that can be installed on the selected clients.
        ii. Select a module or bundle to configure/install for the selected clients.
        Note: The status of a module or bundle will be displayed only if its version matches either an installed version or a scheduled version.
        iii. Click Next after selecting a module or bundle from the list.
    b. by module
        i. Click Next after selecting the clients from the list
2. Depending on the module or bundle selected, and possible dependencies, you will then see options based on the selection types:
    - Bundle
      Clicking Next for a bundle will take you to the Module Parameters panel that will display all the parameters for all modules of the bundle. Modify any of the listed module parameters within the Client Module Parameters section.
      Note: A bundle is treated as a regular module.
    - module with no mandatory dependencies

      Clicking Next for modules with no mandatory dependencies will take you to the Module Parameters panel that will display the module's parameters. Modify any of the listed module parameters within the Client Module Parameters section.

    - module with dependencies
      Clicking Next for a module with dependencies displays that module and all dependencies modules in the Dependent Modules screen. Click the Edit icon for any of the modules to configure its parameters for all selected clients; taking you to the Module Parameters panel that will display the module's parameters. Change any parameters there and click the Accept button to come back to the Dependent Modules screen.
      Note: The configuration for module and all of its dependencies can be saved to the database only at once. Also, they can only be installed as a bundle. This means that they cannot be individually saved or scheduled for installation. For example, if, in middle of scheduling installation, the process fails for one of modules on one of the clients, it will roll back all installations before that failure.
      Note: parameters may be entered in the Common Module Parameter section to, by clicking the Apply to Selected, populate the selected clients in the Client Module Parameters section.
3. Click Apply to Clients, after entering values for all required parameters on all selected clients, to save the configuration to the database. Before the save, a validation is performed to make sure all required fields have values or their values are in pre-defined range.
4. After Saving configurations, click Install/Update to schedule the module and its dependencies for installation on the selected clients. In addition, from the Dependent Module Parameters panel you may uninstall, cancel install/update, cancel uninstall, and revert current changes. Note that the schedule date and time corresponds to the date and time on the selected clients.
   Note: The Generate Grdapi button at the front of the client line under the Client Module Parameter section allows the user to view the list of grdapi commands that reflect the changes the user has made to the module such as assigning, installing, uninstalling, scheduling, and updating of the module. These grdapi commands are provided to the user so they can take the set of commands and apply them to other clients in a script if they would like to reproduce.
   Note: The open Property content button appears in front of every writable properties and opens up a window that simplifies the editing of a long field.
   Note: The View installation state of this client button, also at the front of the client line under the Client Module Parameter section provides a view into the current installation status for the module.
   Note: When installing K-TAP as part of BUNDLE-STAP, K-TAP status will set to INSTALLED even if the actual K-TAP module was missing for this specific platform. However a message will be shown on the GIM-EVENTS report indicating K-TAP module was missing.
   Note: Always check the GIM-EVENTS report after installing bundles on the DB servers
   Note: When uninstalling modules, GIM will only uninstall the selected module and not uninstall dependencies

Rollback Mechanism

GIM's rollback mechanism purpose is to handle errors during installation and recover modules to their prior state. The Rollback mechanism supports the following recovery scenarios:

1. Live Upgrade Recovery
   For Bundles
    - When bundles are installed, recovery will rollback the modules that have an install failure within the bundle.
    - Modules that are marked as `NO_ROLLBACK` (in the form of a read-only parameter <MODULE>_NO_ROLLBACK=1) will not be rolled back in the event of a failure. S-TAP/KTAP are two such modules that once successfully installed will not be rolled back in the event of a failure of another module.

   For non-Bundles
    - Rollback entails the removal of the standalone module in the case of a scratch install or reverting back to the previous version in case of an upgrade.
2. Boot Time Installation Recovery
   If installation failure occurs during a system reboot, a second system reboot will be needed in order to complete the recovery. Users will still see the status IP-PR after reboot, and a GIM_EVENT entry that indicates a second reboot is needed to complete the recovery process. The module/bundle state will then indicate a “FAILED” status after the second reboot.

Note: When the status is 'IP-PR' booting the DB-server is different per OS (Any other way of rebooting the system will keep the pending modules in a pending state):

```
Linux   : shutdown -r
SuSe    : reboot
HP      : shutdown -r
Solaris : shutdown -i [6|0]  (Note : '0' can be used only if shutdown is done  from the terminal server)
AIX     : reboot
Tru64   : reboot
```

Note: In addition, prior to reboot, A-TAP instances must be disabled/deactivated.

Changing the GIM server for a GIM client

You can change the GIM server that manages one or more GIM clients. You might want to make this change in order to balance the load among your GIM servers, or to make it easier to distribute GIM packages. To reassign a group of GIM clients to a different GIM server, follow these steps:

1. Click Manage > Install Management > Set up by Module to change the GIM server for a GIM client.
2. Select a GIM bundle that is installed on the clients that you want to reassign. Click Next.
3. Select the clients to be changed. You can click Select All or select clients individually. Click Next.
4. Click Select All.
5. For the GIM_URL parameter, enter the hostname or IP address of the GIM server (Guardium system) to which you want to reassign the selected GIM clients. Click Apply to Selected.
6. On the same panel click Apply to Clients, then click Install/Update and schedule the update.

After the update has been processed, the GIM client will be managed by the new GIM server.
Parent topic: Managing software with GIM

GIM command line interface

You can use the CLI in order to install or upgrade modules on the database server.

The following examples are presented only to cover some of the more common scenarios. For more information and a complete list of all supported CLI commands refer to GuardAPI GIM Functions.

- Loading module packages
- Upgrade or Scratch install using bundles
- Uninstall a module/bundle
- Installation Status
- Querying modules state

Loading module packages

Before modules can be installed on DB server, they must be loaded onto the Central Manager GIM database. If a Central Manager is not part of the architecture, packages must be loaded onto each Guardium system. Use the Load package option in the GIM UI in order to get the packages loaded to the database.

Upgrade or Scratch install using bundles

Note: Scratch install refers also to a case where old (pre-GIM) S-TAP® is installed on the database server.
A bundle is a list of modules grouped together to allow easier installation process. Always use bundles to install or upgrade modules.

1. Get the list of registered clients (i.e. database servers installed with GIM client that have registered with GIM server):

```
grdapi gim_list_registered_clients
ID=0
####### ENTRY 0 #######
CLIENT_ID:          1
IP:                 192.168.2.204
OS:                 HP-UX
OS_RELEASE:         B.11.00
OS_VENDOR:          hp
OS_VENDOR_VERSION:  B.11.00
OS_BITS:            64
PROCESSOR           9000
####### ENTRY 1 #######
CLIENT_ID:          2
IP:                 192.168.2.210
OS:                 Linux
OS_RELEASE:         2.6.16.54-0.2.5-smp
OS_VENDOR:          suse
OS_VENDOR_VERSION:  10.1
OS_BITS:            64
PROCESSOR           x86_64
```

2. Assign (i.e. prepare to install; NOT a request to actually install it on the client) the latest bundle available for a specific client

```
grdapi gim_assign_latest_bundle_or_module_to_client  clientIP=198.168.2.210 moduleName=BUNDLE-STAP
```

Note: In order to assign a specific bundle or module to a client, step 2 should be replaced with the following sequence:

```
gim_get_available_modules clientIP=”client ip”
gim_assign_bundle_or_module_to_client_by_version clientIP=”client ip” modulesName=”Bundle/Module name”
moduleVersion=”Bundle/Module version”
```

3. Schedule the installation.

```
grdapi gim_schedule_install clientIP=192.168.2.210 date=now
```

Note: For multiple client installation repeat steps 2-3.

Note: For flexible GIM scheduling, use now + [1-9][0-9]* minute | hour | day | week | month. Example: now + 1 day, now + 3 minutes

GIM scheduling

All time is relative to Guardium system time. Now means right now as specified by the Guardium system. Now +30 minute is the current Guardium system time + 30 minutes. This can be seen when looking at the installation status by clicking on the small "i" next to a client, for example in Manage > Module Installation > Set up by Client (Legacy). If the time on the database server has passed the time on the Guardium system specified for install, then the install begins.

Example one, set up three clients (a) set for Guardium system time - 1 hour, (b) set for Guardium system time, and (c) set for Guardium system time + 1 hour.

Set up an S-TAP installation via GIM for "now +30 minute".

Guardium system (a), which is already 30 minutes ahead of the time set for installation, will install immediately.

Guardium system (b) will install in 30 minutes.

Guardium system (c) will take another hour after (b) to install.

Example two - Same setup as example one but this time specify "now".

Installation status changes to IP immediately on all clients.

Uninstalling a module/bundle

```
grdapi gim_uninstall_module clientIP=192.168.2.210 module=BUNDLE-STAP date=now
```

You can specify `date=now` or use the format of `YYYY-MM-DD HH:mm`. The uninstallation will take place the next time GIM client checks for updates (GIM_INTERVAL).

Installation Status

Additional information about the latest status the client has sent can be retrieved by running the following command (The status message will appear as an entry in GIM_EVENTS table from which a report can be generated):

The general status message can be obtained by running the following CLI command:

```
grdapi gim_get_client_last_event clientIP="client ip"
grdapi gim_get_client_last_event clientIP=winx64
grdapi gim_get_client_last_event clientIP=9.70.144.73
```

Here is an example of the output from this command:

```
ID=0
OK
BUNDLE-STAP-8.0_r2609_1 INSTALLED
STAP-UTILS-8.0_r2609_1 INSTALLED
COMPONENTS-8.0_r2609_1 INSTALLED
KTAP-8.0_r2609_1 INSTALLED
STAP-8.0_r2609_1 INSTALLED
TEE-8.0_r2609_1 INSTALLED
ATAP-8.0_r2609_1 INSTALLED
```

Querying modules state

In order to query the installed module's state per client the following CLI command needs to be executed.

```
grdapi gim_list_client_modules clientIP=”client ip”
```

The following states are possible:

INSTALLED
: Module is installed.

PENDING-INSTALL
: Module is pending to be scheduled for installation.

PENDING-UNINSTALL
: Module is pending to be scheduled for uninstallation.

PENDING-UPDATE
: Module is pending to be scheduled for update.

IP
: Module installation is in progress.

FAILED
: Module's last operation failed.

IP-PR
: Module requires client reboot in order to complete the installation process. Prior to rebooting, deactivate all A-TAP instances. Rebooting the database server is different per OS (Any other way of rebooting the system will keep the pending modules in a pending state).

  - AIX: reboot
  - Linux : shutdown -r
  - SuSe: reboot
  - HP-UX: shutdown -r
  - Solaris: shutdown -i [6|0] (Note : '0' can be used only if shutdown is done from the terminal server)
  - Tru64: reboot

Output example

```
ID=0
####### ENTRY 0 #######
MODULE_ID:          11
```

```
NAME:                INIT
INSTALLED_VERSION    8.0_r3852_1
SCHEDULED_VERSION    8.0_r3852_1
STATE:               INSTALLED
IS_SCHEDULED:        N
####### ENTRY 1 #######
MODULE_ID:           -1
NAME:                COMMON
INSTALLED_VERSION    8.0_r0_1
SCHEDULED_VERSION    8.0_r0_1
STATE:               INSTALLED
IS_SCHEDULED:        N
####### ENTRY 2 #######
MODULE_ID:           12
NAME:                UTILS
INSTALLED_VERSION    8.0_r3852_1
SCHEDULED_VERSION    8.0_r3852_1
STATE:               INSTALLED
IS_SCHEDULED:        N
####### ENTRY 3 #######
MODULE_ID:           13
NAME:                SUPERVISOR
INSTALLED_VERSION    8.0_r3852_1
SCHEDULED_VERSION    8.0_r3852_1
STATE:               INSTALLED
IS_SCHEDULED:        N
####### ENTRY 4 #######
MODULE_ID:           14
NAME:                GIM
INSTALLED_VERSION    8.0_r3852_1
SCHEDULED_VERSION    8.0_r3852_1
STATE:               INSTALLED
IS_SCHEDULED:        N
####### ENTRY 5 #######
MODULE_ID:           15
NAME:                BUNDLE-GIM
INSTALLED_VERSION    8.0_r3852_1
SCHEDULED_VERSION    8.0_r3852_1
STATE:               INSTALLED
IS_SCHEDULED:        N
```

Parent topic: Managing software with GIM

GIM Server Allocation

Remotely connect to a pre-installed and inactive (not connected to any collector) GIM agent and make it connect to some collector without the need to access the database server.

Overview

The following process (also called GIM Auto-Discovery) allows you to remotely connect to a pre-installed and inactive GIM agent and make it connect to a collector without accessing the database server.

1. An inactive GIM client runs in listener mode and waits for a connection from any collector.
2. From the collector's graphic user interface (GUI) or the GuardAPI, you can send the IP address of any collector to the inactive GIM client.
3. The inactive GIM client accepts the collector's IP address and connects to it.

If GIM is installed without specifying a collector's IP address (--sqlguardip) it will run in server mode. When the GIM agent is running in server mode, it accepts messages only from verified collectors over SSL that have certificate authentication and shared secret verification. If there are 30 or more consecutive authentication failures, the GIM agent stops listening for requests and runs in server mode. This action prevents denial of service (DoS) attacks.

You can define your own certificates, shared secret, and port number. To use other certificates, specify the certificate/key full path name in the installation parameters: --key_file and --cert_file. Load the certificates to the collector key store with the GuardAPI command store certificate gim.

To set a shared secret other than the default one, use the GuardAPI command grdapi gim_set_global_param paramName=gim_listener_default_shared_secret paramValue=<password>. The format should be a string. The shared secret must be identical on the database server and collector.

Note: Do not specify the unencrypted shared secret in the command line.

To use a port other than the default one, specify the port in the installation parameter --listener_port. Set the GIM global parameter gim_listener_default_port with the new port in the GIM Global Parameters.

Note: The default or user defined port must be enabled in the firewall.

Parameters

The following list describes the GIM installation parameters:

- --sqlguardip - Sets the collector IP address/hostname that the GIM client is connecting to. If it is not specified, the GIM client will work in “Listener mode".
- --ca_file - Full file name path to the Certificate Authority PEM file.
- --key_file - Full file name path to the private key PEM file.
- --cert_file - Full file name path to the certificate PEM file.
- --shared_secret - specify a shared secret to verify collectors.
- --listener_port - specify a port number that is different than the default.
- --no_listener - disables GIM from running in "Listener mode" even if --sqlguardip is not specified.

Any attempt to:

- update parameters
- install modules
- uninstall GIM directly on the database server

causes the GIM agent to exit server mode and process the request. If the GIM client cannot connect to the designated collector, it returns to server mode. After the GIM agent is assigned to a valid collector's IP address or host name, you cannot set the GIM server to run in server mode again. All new GIM agent server mode parameters appear as READ-ONLY.
Note: The following parameters must exist in the file system or the installation fails:

- ca_file
- key_file
- cert_file

Additional command line parameter

GIM and Consolidated Installers for GIM have an additional command line parameter:

--allow_ip_hostname_combo <0|1>

param name : GIM_ALLOW_IP_HOST_COMBO

param values : 1 - Enabled, 0 - Disabled

Param default value : 0

param description : If Enabled, and the GIM_CLIENT_IP is different than the db server's hostname, GIM_CLIENTS.GIM_CLIENT_NAME will be set with a value that is the combination of `hostname`_<GIM_CLIENT_IP>.

If GIM_CLIENT_IP is set with an IP address and the GIM_ALLOW_IP_HOST_COMBO is enabled, GIM's hostname will be a combination of the <hostname>_<GIM_CLIENT_IP> This will allow GIM clients uniqueness across database servers with "common" hostname.

LIMITATION: You can NOT set GIM_CLIENT_IP with a "common" hostname. This will be considered as an attempt to register with a duplicate identifier.

Setting GIM in Server Mode Global Parameters

You can set up the server mode GIM parameters by using the following GuardAPI command:

```
grdapi gim_set_global_param
paramName=gim_listener_default_shared_secret
paramValue=<password>
```

This value is encrypted and stored in the database. The value must be identical to the unencrypted value as the shared secret if you install the GIM agent on the database server.

To set up a new default server mode GIM port, use the following GuardAPI command:

```
grdapi gim_set_global_param paramName=gim_listener_default_port paramValue=<port number>
```

This value must be identical to the unencrypted value of the shared secret if you install the GIM agent on the database server.

Note: If you use a different port or shared secret, you must specify the shared secret or port every time you connect the collector IP/hostname to the server mode GIM agent.

GIM Remote Activation

Remotely connect to a pre-installed GIM agent and connect it to a collector without accessing the database server with GIM Remote Activation.

1. Click Manage > Module Installation > GIM Remote Activation.
2. Type in the IP address or host name where GIM is running in listener mode in the IP / hostname field. Otherwise, select a server group from the following list.
3. Type in a numerical value in the GIM Listener Port if it is different from the GIM Global setting. The default value is 8445.
4. Enter the shared secret in the GIM Listener Password field if it is different from the GIM Global setting.
5. Click Submit to process the information or Reset to clear the information.

Note: You must enter an IP address / host name or select a server group, but the GIM listener port and GIM listener password are optional. When you install the GIM client in listener mode, the settings of the shared secret and certificates cannot be changed unless you reinstall the GIM client.
Note: If the "Collector IP" field in GIM Remote Activation is blank, the hostname of the collector is sent to the server. If IP is specified, this is sent instead.

Create a GIM Auto-discovery Process

Create a GIM auto-discovery process to identify and associate GIM clients that have been installed in listener mode. It is also possible to activate GIM clients that have been installed in listener mode using Quick start for deploying monitoring agents.

1. Navigate to Discover > Database Discovery > GIM Auto-discovery Configuration.
2. Create a new GIM auto-discovery process by clicking the  icon.
3. Name the process using the Process name field and then clicking Apply.
4. Define hosts to scan for GIM clients that were installed in listener mode using the Add hosts and ports to process section.
    a. Identify a host or subnet to scan using the Host(s) field. Wildcard characters are enabled. For example, to select all addresses beginning with 192.168.2, use `192.168.2.*`.
    b. Add the host or subnet to the GIM auto-discovery process by clicking Add scan.
    c. Repeat the previous steps to define multiple hosts or subnets to include in the GIM auto-discovery process.

Note:
- If you have a dual stack configuration, define scans for both the IPV4 and the IPV6 addresses.
- Modify existing host or subnet scans by typing over the existing value and clicking Apply to save the changes.
- Remove scans by clicking the  icon. If a task has scan results dependent upon it, the scan cannot be deleted.

5. Run the GIM auto-discovery process by clicking Run Once Now or define a schedule for running the process by clicking Modify Schedule. See Scheduling for information about defining a schedule.
6. After the process has completed, click View Results to see a list of discovered GIM clients and associate those clients with Guardium systems.
    a. Select the GIM clients to associate.
    b. Click Associate to assign the clients to the current Guardium system or click Assign Collector to assign the clients to another Guardium system in your environment.
    c. Use the Results dialog to review the status of client association. After successfully association, GIM clients are no longer in listener mode and are not shown in the GIM auto-discovery results window.
    d. Click Close to close the results window.

GIM Global Parameters

Define your own shared secret or GIM listener port through the user interface.

1. To open the GIM Global Parameters, click Manage > Module Installation > GIM Global Parameters.
2. Select gim_listener_default_shared_secret to set the shared secret or gim_listener_default_port to set the port.
3. Click the  icon to edit the selected parameter.
4. Change the value and click Save to change the parameter or Close to return to the page.

Parent topic: Guardium Installation Manager

Installing the GIM client on a Windows server

Learn how to install the GIM client for Windows using either an interactive installer or a silent installation. Instructions are also provided for uninstalling the GIM client.

About this task

There are currently two types of installers for the GIM client based on your GIM client version. Version 10.1.2 and earlier use build numbers through r89755, while version 10.1.3 and beyond uses build numbers starting from 10.2.30.5. Please pay attention to your GIM client version and build numbers as you go through these instructions.

Parent topic: Guardium Installation Manager

Installing the GIM client using an interactive installer: GIM client version 10.1.2 or older

A wizard is provided to help you install the GIM client on each database server.

Procedure

1. Place the GIM client installer on the database server, in any folder.
2. Run the setup.exe file to start the wizard that installs the GIM client. The setup.exe file is located in the Windows_GimClient folder.
3. Follow and answer the questions in the installation wizard.

What to do next

You can view the results of the installation in the log file at c:\guardiumstaplog.txt.

Installing the GIM client using an interactive installer: GIM client version 10.1.3 and newer

A wizard is provided to help you install the GIM client on each database server.

Procedure

1. Place the GIM client installer on the database server, in any folder.
2. Run the setup.exe file to start the wizard that installs the GIM client. The setup.exe file is located in the GIM-Installer-10.2* folder.
3. Follow and answer the questions in the installation wizard.

What to do next

You can view the results of the installation in the log file at C:\IBM Windows GIM.ctl..

Installing the GIM client using silent installation: GIM client version 10.1.2 or older

If you prefer, you can install the GIM client from the command line instead of using the wizard.

About this task

Procedure

1. Place the GIM client installer on the database server, in any folder.
2. Open a command prompt and navigate to the Windows_GimClient folder under the folder where you placed the installer.
3. Enter this command, with no linebreak. `setup.exe /s /z" --host=g10.guardium.com --path=c:\\program files (x86)\\guardium\\GIM --perl=c:\\perl\\bin --localip=192.168.1.100"` Include all the spaces and quotes exactly as in this example. Removing or adding spaces causes the installer to fail. The --perl= parameter indicates where Perl is installed on this computer. This parameter is optional. If you do not specify it, the installer installs a Perl instance.
   Attention:
   - Omit the --host parameter to install the client in GIM listener mode. Listener mode makes the GIM client available for remote registration from a Guardium system. Example of how to install as listener: setup.exe /s /z"--path=c:\program files (x86)\guardium\GIM --host=GIM_HOST" For more information, see GIM Remote Activation and Create a GIM Auto-discovery Process.

- When cloning database servers and establishing large deployments, use --auto_assign_ip=1 to allocate a random IP address from one of the valid IP addresses of a database server. Do not specify both auto_assign_ip and localip when installing the GIM client. When updating the GIM_AUTO_SET_CLIENT_IP parameter using Manage > Module Installation > Set up by Client or Set up by Module, you must restart the GIM client service for the new setting to take effect.

What to do next

You can view the results of the installation in the log file at c:\guardiumstaplog.txt.

Installing the GIM client using silent installation: GIM client version 10.1.3 or newer

If you prefer, you can install the GIM client from the command line instead of using the wizard.

Procedure

1. Place the GIM client installer on the database server, in any folder.
2. Open a command prompt and navigate to the GIM_Installer* folder under the folder where you placed the installer.
3. Enter this command, with no linebreak. `setup.exe -UNATTENDED -INSTALLPATH "c:\Program Files(x86)\Guardium Installation Manager" -LOCALIP 10.9.876.543`
   Attention:
   -
     - The UNATTENDED and LOCALIP parameters are required. APPLIANCE is optional and if not supplied, will trigger Listener Mode. If using parameter AUTO_ASSIGN_IP, LOCALIP is not required.
     - Omit the -APPLIANCE parameter to install the client in GIM listener mode. Listener mode makes the GIM client available for remote registration from a Guardium system. Example of how to install as listener: setup.exe -UNATTENDED -INSTALLPATH C:\program files (x86)\guardium\GIM -LOCALIP 10.9.876.543. For more information, see GIM Remote Activation and Create a GIM Auto-discovery Process.
     - When cloning database servers and establishing large deployments, use --auto_assign_ip=1 to allocate a random IP address from one of the valid IP addresses of a database server. Do not specify both auto_assign_ip and localip when installing the GIM client. When updating the GIM_AUTO_SET_CLIENT_IP parameter using Manage > Module Installation > Set up by Client or Set up by Module, you must restart the GIM client service for the new setting to take effect.
   - **Windows GIM command line installation reference**

   Parameters applicable to all .NET installers

Parameter	Description
-UNATTENDED	Install silently. A value is not required
-UNINSTALL	Uninstall. A value is not required.
-INSTALLPATH	This is the install directory. Default install path is "C:\Program Files (x86)\Guardium\Guardium Installation Manager"
-CUSTOMER	To change customer name
-COMPANY	To change company name
-SERVICEUSER	To specify a user to run the service under
-SERVICEPASSWORD	The password for the user

   Parameters specific to GIM .NET installers

Parameter	Description
-APPLIANCE	To set the appliance address that GIM connects to. Absence of this parameter will result in GIM installation using Listener Mode.
-LOCALIP	This is the IP of the server where GIM is being installed.
-KEY_FILE	To set the key file to non-default file
-CERT_FILE	To set the certificate file to non-default file
-CA_FILE	To set the CA file to non-default file
-SHARED_SECRET	To set shared secret for registration with appliance if not specified using -APPLIANCE parameter
-LISTENER_PORT	Set listener port for registration with appliance if not using the -APPLIANCE parameter. Default value is 8445.
-AUTO_ASSIGN_IP	When value set to 1, a local IP is automatically assigned and should NOT be specified using -LOCALIP. Default value is 0.

What to do next

You can view the results of the installation in the log file at C:\IBM Windows GIM.ctl.

Uninstalling the GIM client: GIM client version 10.1.2 or older

Procedure

1. Open a command prompt and navigate to the Windows_GimClient* folder under the folder where you installed the client.
2. Enter this command: For Installshield, use

   ```
   setup.exe /s /z"--host=g10.guardium.com --remove=true"
   ```

   The --host= parameter is optional.

Uninstalling the GIM client: GIM client version 10.1.3 and newer

Procedure

1. Open a command prompt and navigate to the GIM_Installer* folder under the folder where you installed the client.
2. Enter this command:

```
setup.exe -UNINSTALL
```

Installing the GIM client on a UNIX server

Use this command to install the GIM client on each database server.

About this task

You can install and use the GIM client in a Solaris slave zone or an AIX workload partition (WPAR). This enables you to use the GIM client to install an S-TAP in a slave zone or WPAR. When you install an S-TAP in a slave zone or WPAR, the K-TAP is disabled, regardless of the setting of the ktap_enabled parameter. You can also use the GIM client to install the Configuration Auditing System (CAS) agent in a slave zone or WPAR. You cannot install the discovery bundle in a slave zone or WPAR; the discovery agent running on the global zone can collect information from other zones. The process for installing the GIM client in a Solaris slave zone or an AIX workload partition is the same as the process for installing in the master zone. The installation can take a few seconds longer than installing in the master zone. If you install the GIM client on a Solaris system with master and slave zones, you must install the client in the same location on the master and slave zones. This location cannot be a shared directory.

On Solaris, the GIM client and supervisor in each slave zone are controlled by the GIM supervisor process that runs in the master zone. If the supervisor process on the master zone is shut down, all GIM processes on the slave zones are shut down as well.

Note: GIM requires 300 MB minimum of disk space, and 700 MB if FAM module is also being installed.

Procedure

1. Place the GIM client installer on the database server in any folder.
2. Run the installer: `./<installer_name> [-- --dir <install_dir> <--sqlguardip> <g-machine ip> --tapip <db server ip address> --perl <perl dir> -q]` The installer name has the syntax: guard-bundle-GIM-<release build>-<DB>-<OS>_<bit>.gim.sh, for example:

   ```
   guard-bundle-GIM-10.5.0_r103224_v10_5_1-rhel-6-linux-x86_64.gim.sh
   ```

   Attention:
   - Omit the --sqlguardip parameter to install the client in GIM listener mode. Listener mode makes the GIM client available for remote registration from a Guardium system. For more information, see GIM Remote Activation and Create a GIM Auto-discovery Process.
   - When cloning database servers and establishing large deployments, use --auto_set_gim_tapip to allocate a random IP address from one of the valid IP addresses of a database server. Do not specify both auto_set_gim_tapip and tapip when installing the GIM client. Update the GIM_AUTO_SET_CLIENT_IP parameter after GIM client installation by using Manage > Module Installation > Set up by Client or Set up by Module.
3. On Red Hat Linux, version 6 or later, run these commands to verify that the files have been added:

   ```
   ls -la /etc/init/gim*
   ls -la /etc/gsvr*
   ```

   On Solaris, version 10 or later, run this command:

   ```
   ls /lib/svc/method/guard_g*
   ```

   On all other platforms, run these commands to verify that the following new entries were added to /etc/inittab:

   ```
   gim:2345:respawn:<perl dir>/perl <modules install dir>/GIM/<ver>/gim_client.pl
   gsvr:2345:respawn:<modules install dir>/perl <modules install dir>/SUPERVISOR/<ver>/guard_supervisor
   ```

   Where modules install dir is the directory where all GIM modules are installed, for example, /usr/local/guardium/modules.
4. Enter this command to verify that the GIM client, SUPERVISOR process, and modules are running:

   ```
   ps -afe | grep modules
   ```

5. Log in to the Guardium system and check the Process Monitoring status.

Parent topic: Guardium Installation Manager

Uninstalling GIM and its modules on a UNIX database

You can uninstall GIM and its modules either from the GUI, or on the database server itself.

Procedure

1. To uninstall using the Guardium GUI.
   a. Schedule an uninstall of the S-TAP bundle (Setup by Client).
   b. Schedule an uninstall of the GIM bundle (Setup by Client).
   c. Reboot the database server to remove K-TAP from the drivers.
2. Alternatively, uninstall on the DB server itself:
   a. Uninstall both the GIM bundle and the S-TAP bundle by executing as root: /full/path/modules/GIM/current/uninstall.pl
   b. Reboot the database server to remove K-TAP from the drivers.

Parent topic: Guardium Installation Manager

Upgrading the GIM client

You can use GIM to upgrade the GIM client to a newer version.

Procedure

1. Upload the latest available BUNDLE-GIM.gim file to the Guardium system.
2. Use the GIM GUI to schedule the installation of the new BUNDLE-GIM.gim file.

3. Monitor the installation process by clicking on the i icon and pressing Refresh. When the installation has successfully completed the INSTALLED status will be displayed.

Parent topic: Guardium Installation Manager

Using groups with GIM

You can use groups to make some GIM tasks easier.

Before you begin

About this task

You can create group of GIM clients and use it to roll out updates to those managed servers.

Procedure

1. Click Setup > Tools and Views > Group Builder. In the Group Builder, create a new group. For the Group Type Description choose Client Hostname. The new group is added to the list of existing groups.
2. Choose the new group in the Modify Existing Groups list and add members to the group. You can add them manually or populate the list from a query. To populate the list from a query, click Populate from Query and note these requirements:
    a. For Query select a report name that begins with GIM.
    b. For Fetch Member from Column, select GIM Client Name.
    c. In each Enter (Like) field, enter a value to be matched, or % if this field is not used to identify clients.
    d. Save the group and run or schedule the query.

Results

You can use the group in the Manage > Module Installation > Set up by Client screen to work with this set of clients as a group rather than individually.
Parent topic: Guardium Installation Manager

Copying a K-TAP module by using GIM

If you build a custom K-TAP module for a Linux database server, you can use GIM to copy that module to other Linux database servers.

Before you begin

The custom K-TAP module is built when you install an S-TAP on a Linux server for which there is no pre-built K-TAPfor the current kernel. The custom K-TAP module is built only if the kernel-devel package is installed. When you install the S-TAP bundle, use the GIM UI to set the value of the GIM parameter STAP_UPLOAD_FEATURE to 1. This tells the GIM client to upload the custom K-TAP module to the Guardium system after it is built and then automatically create a custom S-TAP bundle.

Procedure

1. Use GIM to install the S-TAP on the Linux database server. The installer determines that a custom K-TAP module is required and builds it.
2. The custom K-TAP module, along with its sha256sum value, is uploaded automatically to the Guardium system for which the S-TAP is configured. Note that this might not be the same Guardium system that you use as a GIM server.
3. On the Guardium system to which the K-TAP is uploaded, run this CLI command: grdapi make_bundle_with_uploaded_kernel_module, This adds the newly built K-TAP module to the corresponding S-TAP bundle. There must be at least one S-TAP bundle whose build number and operating system attributes match those of the uploaded K-TAP module. Loaded bundles are stored in /var/gim_dist_packages. The script creates a new S-TAP bundle with _8XX appended to the build number. The new bundle is located in /var/dump. After running the GuardAPI command, grdpi make_bundle_with_uploaded_kernel_module, there is a need to load the new GIM bundle. Otherwise it will not be visible in GIM GUI. If the GuardAPI command, grdpi make_bundle_with_uploaded_kernel_module, is successful, the following example of a message containing the name of the new STAP bundle will be printed: Created guard-bundle-STAP-9.0.0_r71327_v90_800-suse-11-linux-x86_64.gim with kernel ktap-71327-suse-11-linux-x86_64-xCUSTOMxeagle910-3.0.101-303.gefb7031-default-x86_64-SMP. Then run the GuardAPI command, grdapi gim_load_package, and supply the name of the new bundle printed in the previous step.
4. If the new bundle is on a Guardium system that is not your GIM server, copy the new bundle to the GIM server.
5. Use the GIM GUI or CLI to distribute the new bundle to other database servers that are running the same Linux distribution as the server where the custom K-TAP was built. There are hundreds of Linux distributions available, and the list is growing. This means that there might not be a K-TAP already available for your Linux distribution. If the correct K-TAP is not available, the S-TAP installation process can build it for you. When you build a new K-TAP module for a Linux database server, you can copy that module to other database servers that run the same Linux distribution.

Parent topic: Guardium Installation Manager
Copying a new K-TAP module to other systems

GIM dynamic updating

GIM clients check for updates from the GIM server at regular intervals. The GIM server can calculate the best polling interval to use based on system conditions.

Each GIM client sends an "alive" message to its GIM server regularly, to check whether any updates are ready to be processed. This polling interval is calculated and updated based on conditions at the GIM server. The interval is calculated regularly, and the new value is passed to the GIM client in response to its "alive" message. This feature is enabled by default, but you can turn it off if you prefer a fixed interval.

In the event that a GIM client fails to connect to its GIM sever after five consecutive attempts, the GIM client automatically connects to a failover server if one is specified. The GIM client resumes connecting to its original GIM server when that server becomes available. The GIM server and failover server are configured using the GIM_URL and GIM_FAILOVER_URL parameters, respectively.

Dynamic updating is controlled by the Guardium API command gim_set_global_param, with these parameters.

dynamic_alive_enabled

Dynamic alive feature control. 1 – enabled, 0 – disabled. Default =1

dynamic_alive_check_interval

The interval, in minutes, at which the polling interval is recalculated. Default = 5

For example:

```
grdapi gim_set_global_param dynamic_alive_enabled=0
```

When each GIM client sends its alive message to the server, the server responds with the new polling interval as well as any other updates that have been scheduled for that client.

These parameters were valid in 10.0, and removed from 10.1 and higher:

- dynamic_alive_default_load_factor
- dynamic_alive_cpu_level1_threshold
- dynamic_alive_cpu_level2_threshold
- dynamic_alive_db_conn_level1_threshold
- dynamic_alive_db_conn_level2_threshold
- dynamic_alive_cpu_load_sample_time

Parent topic: Guardium Installation Manager

When you upgrade your database server operating system

When you upgrade the operating system on your database server, you can allow the GIM client to make the required changes in itself and your GIM-installed modules.

Before you begin

Review the information at http://www-01.ibm.com/support/docview.wss?uid=swg21679002 to see the options that are available based on the level of your GIM client.

About this task

It is best to update all your GIM-installed modules as soon as possible after the upgrade, whether manually or automatically. By default, the option to update these modules automatically is disabled. If you want to use automatic updating, you must configure the Guardium system that acts as your GIM server to support this option, and you must make the required bundles available on this server.

Procedure

1. For each module that you have installed on your database server, locate the GIM bundle containing the latest version of this module that supports the new operating-system version. The build number of each bundle must be the same or greater than the bundle that is currently installed. Load each bundle onto the GIM server.
2. Use the gim_set_global_param command to set the value of the global parameter auto_install_on_db_server_os_upgrade to 1. This enables the automatic update option on the GIM server.

   ```
   grdapi gim_set_global_param paramName="auto_install_on_db_server_os_upgrade" paramValue="1"
   ```

   By default this parameter is set to 0, which means the option is disabled.
3. After completing all your other preparations, upgrade the operating system on your database server.

Results

At first boot after OS upgrade, the GIM client recognizes that the operating system has been upgraded and because the automatic update option is enabled, the client takes these steps:

1. Changes the configuration files for all GIM-installed modules to support the new operating system attributes.
2. Re-registers all the modules to the GIM server with the updated attributes.
3. Records an alert in the GIM_EVENTS report saying that an OS upgrade has occurred and listing actions that should be taken.

When the modules are re-registered, the GIM server looks first for a bundle that has the same build number as the previously installed bundle, but is compatible with the upgraded OS. If it does not find such a bundle, it looks for the latest bundles that support the new OS attributes. If the server cannot find appropriate bundles, it issues an error message. If the server finds appropriate bundles, it schedules them for upgrade and runs the upgrade process immediately.

What to do next

Review the messages in the GIM_EVENTS report. If the GIM server reports that the modules have been upgraded successfully, verify the proper operation of the modules as you would do after any update.

If error messages have been written to the GIM_EVENTS report, indicating that the upgrade was not successful, review the error messages for guidance.

After completing your planned OS upgrade, disable the automatic update option on the GIM server. This prevents a GIM client from erroneously starting an update process.

```
grdapi gim_set_global_param paramName="auto_install_on_db_server_os_upgrade" paramValue="0"
```

You can re-enable the automatic update option when you perform another OS upgrade.

Parent topic: Guardium Installation Manager

Distributing GIM bundles to managed units

You can distribute GIM bundles to managed units in order to deploy them on the GIM clients managed by those managed units.

Before you begin

About this task

If you manage all your GIM clients from your Central Manager, you can deploy bundles to all your GIM clients directly from the Central Manager. If you manage groups of clients from several managed units, you can distribute GIM bundles from your central manager to those managed units.

The time required for distribution depends on the size of the bundles and network conditions. In a network with substantial latency, transfers can take several hours.

Procedure

1. Copy the bundles that you want to distribute into the /var/gim/dist_packages directory on your Central Manager. All files in this directory will be distributed; you cannot select which bundles you want to distribute.
2. Choose the managed units to which you want to distribute the bundles.
3. Click Distribute GIM bundles. The bundles are copied to the selected managed units.

Results

You can install the bundles from each managed unit to the GIM clients that it manages.
Parent topic: Guardium Installation Manager

Removing unused GIM bundles

You can remove GIM bundles from your GIM server if they are no longer used on any database server.

About this task

This function enables you to maintain your inventory of GIM bundles and prevent it from using disk space unnecessarily.

You can use two new Guardium API commands to identify and remove unused GIM bundles. Perform this procedure on each Guardium system that acts as a GIM server.

Procedure

1. Run the gim_list_unused_bundles command to identify unused bundles for FAM install. Use the includeLatest parameter to indicate whether you want the list that is returned by the command to include the latest version of each GIM bundle. You might have some bundles that you have not yet distributed, or you might want to keep one older version so that you can reinstall it if needed. Set includeLatest to 0 to exclude the latest unused version of each bundle from the command results. Set it to 1 to include all unused versions. This parameter is required and no default value is provided. For example:

   ```
   gim_list_unused_bundles includelatest=0
   ```

   The command returns a list of GIM bundles that are found on the GIM server but are not installed on any database server whose GIM client works with this GIM server.
2. If step 1 identifies some unused bundles, use the gim_remove_bundle command to remove each unwanted bundle. This command takes a single parameter, bundlePackageName, which identifies the bundle to be removed. This parameter is required and no default value is provided. Use names that are returned by the gim_list_unused_bundles command.
   The named bundle is removed only if:
   - The name specified in bundlePackageName matches the name of one and only one specific GIM bundle.
   - There is no GIM bundle whose name matches bundlePackageName installed on any database server whose GIM client works with this GIM server.

   For example:

   ```
   gim_remove_bundle bundlePackageName=name
   ```

   where name is a bundle name that was returned by the gim_list_unused_bundles command.

Results

GIM bundles that are not needed are removed from your GIM server.
Parent topic: Guardium Installation Manager

Running GIM diagnostics

You can run diagnostics on GIM clients to verify that the GIM server has accurate data about each client.

About this task

If you experience trouble with a GIM client, your first step should be to verify that the GIM server has accurate data about that client. Running GIM diagnostics verifies that the modules listed for that client on the GIM server match the modules installed on that client, and that the parameters stored on the GIM client match those stored on the GIM server.

You can run GIM diagnostics either from the Guardium user interface or from the command line. To run from the command line, use this command:

```
grdapi gim_run_diagnostics clientIP=xx.xx.xx.xx
```

The value of clientIP can be either an IP address or a hostname. You must run the command on the Guardium system that is the GIM server for this client.

To run GIM diagnostics from the GUI, use this procedure:

Procedure

1. Use the check boxes next to each client to choose the clients for which you want to run GIM diagnostics.

2. Click Run diagnostics. The next time that each client polls the GIM server for updates, it will receive the diagnostic command and run it immediately.

Results

You can review the results in the GIM_EVENTS report.
Parent topic: Guardium Installation Manager

Debugging GIM operations

You might need to turn on debugging in order to troubleshoot a problem.

About this task

Use these steps to turn on GIM debugging on the GIM server (Guardium system). Modifying gimserver.log4j.properties requires root login on Guardium appliance. Contact Guardium technical Support if required.

Procedure

1. Edit the GIM properties file: /opt/IBM/Guardium/tomcat/gimserver/ROOT/WEB-INF/conf/gimserver.log4j.properties.
2. Change the value ERROR to DEBUG.
3. Save the file.

Results

Debugging will be turned on in a few seconds and debug messages will be written to the daily debug log file in /var/log/guard/debug-logs/.

What to do next

When you have finished debugging, edit the file again and change DEBUG back to ERROR.

Parent topic: Guardium Installation Manager

Enabling GIM client debugging

About this task

To enable debugging on the GIM client, change the parameter module_DEBUG to 1, where module is the name of the installed module whose operation you want to debug. You can modify the parameter by using the CLI or the user interface. Set the value to 0 when you complete your debugging.

Restarting the supervisor for Solaris with SMF support

Use a set of CLI commands to restart the supervisor on Solaris servers with SMF support.

About this task

To restart the supervisor, complete the following procedure. Only use this procedure on Solaris servers with SMF support.

Procedure

1. Stop the supervisor by running the command svcadm -v disable guard_gsvr.
2. Run the command svccfg delete -f guard_gsvr.
3. Restart the supervisor with the command svccfg import <gim install dir>/SUPERVISOR/current/guard_gsvr.xml where <gim install dir> is the file path to the GIM installation directory.

Results

The supervisor is restarted for Solaris with SMF support.
Parent topic: Guardium Installation Manager

Installing your Guardium system

This document details the steps necessary to install and configure your IBM Security Guardium system.

This document also provides information on how to customize the partitioning on the appliance and how to install on a remote drive (SAN).

The steps are:

1. Assemble configuration information and the hardware required before you begin.
2. Set up the physical appliance or the virtual appliance.
3. Install the Guardium® image.
4. Set up initial and basic configurations.
5. Verify successful installation.

The IBM Security Guardium solution is available as:

- Hardware offering – a fully configured software solution delivered on physical appliances provided by IBM®.
- Software offering – the solution delivered as software images to be deployed by the customers on their own hardware either directly or as virtual appliances.

The requirements listed in this document apply to the installation of both the physical appliance and the virtual appliance unless specified otherwise.

- Operating modes
  You can deploy a Guardium system in any of several operating modes.
- License keys
  Establishing a functional Guardium system requires both a base license and one or more append licenses.
- Hardware Requirements
  Detailed hardware requirements and sizing recommendations are available on the IBM Support Portal.
- Guardium port requirements
  Each Guardium system must have ports available for several types of communication. This table lists these connections and the default port numbers that are assigned to them.
- Step 1. Assemble the following before you begin
  To prepare for the deployment of the Guardium system, the network administrator needs to supply the following information.
- Step 2. Set up the physical or virtual appliance
  The setup instructions in this section are different when installing to a physical appliance or a virtual appliance.
- Step 3. Install the Guardium image
  This section explains how to install the image and partition the disk.
- Step 4. Set up initial and basic configuration
  The initial step should be the network configuration, which must be done locally through the Command Line Interface (CLI) accessible through the serial port or the system console.
- Step 5. What to do next
  This section details the steps of verifying the installation, installing license keys, and installing any available maintenance patches.
- Creating the Virtual Image
  Use this section to install the virtual image.
- Custom Partitioning
  If you customize the partitioning of the hard drive, you must make several choices.
- How to partition with an encrypted LVM
  If you want to use an encrypted disk, follow these steps to create an encrypted LVM volume that contains the / and /var logical volumes.
- Example of SAN Configuration
  This appendix details the steps involved in moving to a command prompt in order to pre-partition a hard drive (as is needed for SAN installation).

Operating modes

You can deploy a Guardium system in any of several operating modes.

As you plan your Guardium environment, you might deploy systems in any or all of these operating modes:

Collector
: A collector receives data about database activities or file activities from agents that are deployed on database servers and file servers. The collector processes this data and responds according to policies that are installed on the collector. A collector can export data to an aggregator.

Aggregator
: An aggregator collects data from several collectors, to provide an aggregated view of the data. The aggregator is not connected directly to database servers and file servers. You can allocate collectors to aggregators according to location or function. For example, you might want to connect the collectors that monitor your human resources database servers to a single aggregator, so that you can view data that is related to all those servers in one location. If you want, you can implement a second tier of aggregation by deploying an aggregator that collects data from all your other aggregators, rather than from collectors.
  Note: If you plan to use the appliance as a central manager you MUST select Aggregator option.

Central manager
: There is only one central manager in a Guardium environment, although you can designate another Guardium system as a backup central manager. You can use the central manager to define policies and distribute them to all collectors, to perform other configuration tasks that affect all your Guardium systems, and to perform various other administrative tasks from a single console. Your central manager can also function as an aggregator, collecting data from collectors or from other aggregators. This model provides an enterprise-wide view of activities and enables you to view reports that are based on data that is aggregated from all your Guardium systems.

The number of monitored database servers and file servers that you assign to an collector depends on the amount of data that flows from the servers to the collector. For information about how many collectors and aggregators your environment requires, and how to locate your Guardium systems for best results, refer to the Deployment Guide for IBM Guardium.

If you are using the Guardium Vulnerability Assessment component, you must decide where to run assessment tests. Some customers dedicate a separate Guardium system for this function. You can also run tests from any Guardium system that is deployed as a collector, an aggregator, or a central manager.

Parent topic: Installing your Guardium system

License keys

Establishing a functional Guardium system requires both a base license and one or more append licenses.

Base and append licenses are described as follows:

- Base license keys (also known as reset keys) reflect the machine type of the system. For example, establishing collector system requires a collector base license.
- Append license keys enable specific sets of features. For example, typical data activity monitoring features require a DAM Standard append license. Multiple append licenses can be installed in combination to enable expanded Guardium functionality.

When applying a base license, the machine type is checked to verify compatibility. There are two types of base licenses:

Table 1. Base license types

Base License Type	License Description
Collector	Collector base licenses are valid for establishing a standalone system or a collector.
Aggregator	Aggregator base licenses are valid when establishing an aggegator or a central manager system.

The features available on your Guardium system depend on the append license(s) you have installed. The following append licenses are available and can be used in combination:

Table 2. Append license types

Append License Type	License Description
DAM Express	Predefined functionality for data activity monitoring.
DAM Standard	Core functionality for data activity monitoring.
DAM Advanced	DAM Standard functionality plus fine-grained access control, masking, quarantine, and blocking (activity terminate).
FAM Standard	Core functionality for file activity monitoring.
FAM Advanced	FAM Standard functionality plus blocking.
VA Standard	Vulnerability assessment plus database protection service (DPS), change audit system (CAS), and database entitlement reporting.

For information about installing Guardium licenses, see Install license keys.

Parent topic: Installing your Guardium system
Related tasks:
Install license keys

Hardware Requirements

Detailed hardware requirements and sizing recommendations are available on the IBM Support Portal.

For detailed hardware specifications and sizing recommendations, refer to the following: IBM Guardium V10.1 Software Appliance Technical Requirements.

Parent topic: Installing your Guardium system

Guardium port requirements

Each Guardium system must have ports available for several types of communication. This table lists these connections and the default port numbers that are assigned to them.

Open ports

Ports used in/by the Guardium system.

DB Server – Collector

TCP 8443 - open from DB server to collector

TCP 16016 – Unix STAP, both directions, registration, heartbeat, and data (including IBM i S-TAP running in PASE)

TCP 16017 – Windows/Unix CAS, both directions, templates and data

TCP 16018 – Unix STAP (TLS), both directions, registration, heartbeat, and data

TCP 16019 – Windows/Unix CAS (TLS), both directions, templates and data

TCP 16020 - From STAP agent Clear UNIX STAP connection pooling

TLS 16021 - From STAP agent Encrypted UNIX STAP connection pooling

TCP 8081 – Guardium Installation Manager, both directions, database server to collector/Central Manager

TCP 9500 – Windows STAP, both directions, DB Server to Collector, STAP registration and data

TCP 9501 – Windows STAP (TLS), both directions, DB Server to Collector, STAP registration and data

Collector – Aggregator (Secure Shell – SSL)

TCP 22 – collector to aggregator, SCP data exports, both directions

Central Manager – Managed Devices

TCP 22 – SSH/SCP data transfers, both directions

TCP 8443 – SSL, both directions

TCP 8444 – SSL, STAP to GIM file upload

TCP 3306 – MySQL, opened to specific sources (for instance, the Central Manager is open to all managed units; a managed unit is open to the Central Manager)

TLS 8447 - Used for remote messaging service infrastructure (and profile distribution infrastructure) for communication between Guardium systems in the federated environment / centrally-managed environment. Configuration profiles allow the definition of configuration and scheduling settings from a Central Manager and conveniently distribute those settings to managed unit groups without altering the configuration of the Central Manager itself.

File Activity Monitoring (FAM)

TCP/TLS 16022/16023 - Universal Feed. 16022 (FAM monitoring, unencrypted) and 16023 (FAM monitoring, encrypted) both need to be open bidirectionally. The sniffer needs the block from 16016 to 16023 open bidirectionally.

18087 - Listener port for FAM on IBM Content Classification (ICM) server located on the same machine where FAM is installed. (serverSettings.icmURL=http://localhost:18087) Open bidirectionally.

Guardium Installation Manager (GIM)

8445 - GIM client listener, both directions. The GIM client is doing the listening. Any GIM server on either the Central Manager or the collector can reach out to it (the GIM client).

8446 - GIM authenticated TLS, both directions. Use between the GIM client and the GIM server (on the Central Manager or collector). If GIM_USE_SSL is NOT disabled, then the gim_client will attempt to communicate its certificate via port 8446. IF port 8446 is NOT open, then it defaults to 8444, BUT no certificate is passed (for example, TLS without verification).

8081 - TLS - To use 8081 for the GIM client to connect to the GIM server, there is a need to disable the GIM_USE_SSL parameter - it is ON by default. This parameter is part of the GIM common parameters in the GUI. If GIM_USE_SSL is NOT disabled, then the gim_client will attempt to communicate its certificate via port 8446. IF port 8446 is NOT open, then it defaults to 8444, BUT no certificate is passed (for example, TLS without verification).

Enterprise load balancer

TLS 8443 - S-TAP load balancer - This is needed for UNIX/Linux S-TAPs to communicate instances to the collector. However this port is also used for the Central Manager load balancer. The S-TAP initiates a request to Central Manager (load balancer) on 8443 sending HTTPS message, if installation indicates to use Enterprise load balancer. Between the database server and Central Manager, there will be the capability to use a proxy server, if customer doesn't want an open port directly from database to Central Manager.

Quick Search for Enterprise

TCP 8983 - SOLR - Incoming, SSL

TCP 9983 - SOLR - Incoming, SSL

User Interface – Guardium System (standalone, aggregator, Central Manager)

TCP 22 – user to system, CLI connectivity, both directions

TCP 8443 – user to system, GUI connectivity (configurable), both directions

System – SMTP server

TCP 25 – system to SMTP server, email alerts

System – SNMP server

UDP 161 - SNMP client to system – SNMP Polling

UDP 162 - system to SNMP server, SNMP traps

System – SYSLOG server

UDP/TCP 514 – remote syslog message from/to other systems, typically SIEM**Note:** The local port is 514, but the remote port must be entered into the configuration. If encryption is used, the protocol must be TCP, not UDP.

System – NTP server

TCP/UDP 123 – system to Network Time Protocol Server

System – DNS server

TCP/UDP 53 – system to Domain Name Server

System – EMC Centera (backups)

TCP 3218 – system to EMC Centera

System – Tivoli LDAP

UDP 389 – system to/from Tivoli LDAP

System – Mainframe

TCP 16022 – connects S-TAP to DB2 z/OS, S-TAP IMS, S-TAP VSAM (S-TAP Data Set)

TCP 16023 - TLS connections, specifically IBM‘s Application Transparent Transport Layer Security (AT-TLS)

Ports for connections to Windows database servers

Port	Protocol	Purpose
8075	UDP	Windows S-TAP heartbeat signal (two-way traffic). Note: The UNIX S-TAP agent does not use UDP for heartbeat signals, so there is no corresponding UNIX port for this function.
9500	TCP	Clear Windows S-TAP
9501	TLS	Encrypted Windows S-TAP (optional)
16017	TCP	Clear Windows CAS
16019	TLS	Encrypted Windows CAS (optional)

Default Ports Used for Guardium Application Access

Port	Protocol	Purpose
8443	TCP	Web browser access (https) to the Guardium user interface. Note: This port can be changed by the Guardium administrator, and is also used to register a managed unit to the Central Manager.
22	TCP	SSH access from clients to manage the Guardium appliance
3306	TCP	Communication between central manager and managed units

Ports for connections to z/OS database servers

Port	Protocol	Purpose
16022	TCP	Connects to S-TAP for DB2 z/OS, S-TAP for IMS, S-TAP for Data Sets
16023	TCP	TLS connections, specifically IBM's Application Transport Layer Security (AT-TLS)
41500	TCP	Default starting port for internal message logging communications – LOG_PORT_SCAN_START
39987	TCP	Default agent-specific communications port between the agent and the agent secondary address spaces – ADS_LISTENER_PORT

Default ports used for other features

Port	Protocol	Purpose
20, 21	TCP	FTP Server for backups/archiving (optional)
22	TCP	SCP for backups/archiving, patch distributions, and file-transfers
25	TCP	SMTP (email server) for alerts and other notification
53	TCP	DNS Servers
123	TCP, UDP	NTP (Time Server) for time synchronization
161	TCP, UDP	SNMP Polling (optional)
162	TCP, UDP	SNMP Traps (optional)
389	TCP	LDAP, for example, Active Directory or Sun One Directory
514	TCP	Syslog Server (optional)
636	TCP	LDAP, for example, Active Directory or Sun One Directory over SSL (optional)
1500	TCP	Tivoli Storage Manager backup hosts (optional)
321	T	EMC Centera backup hosts (optional)

8	CP, UDP	
user-defined	TCP	Database Server listener ports, for example, 1521 for Oracle or 1433 for MS-SQL, for Guardium datasource access (optional). Use this port for S-TAP verification and Discovery.
16022/16023	TCP/TLS	Universal Feed - File Activity Monitoring (FAM0
18027		FAM using IBM Content Classification locally (serverSettings.icmURL=http://localhost:18087)
8445		GIM client listener, both directions The GIM client is doing the listening. Any GIM server on either the Central Manager or the collector can reach out to it (the GIM client).
8446	TLS	GIM authenticated TLS, both directions Use between the GIM client and the GIM server (on the Central Manager or collector). If GIM_USE_SSL is NOT disabled, then the gim_client will attempt to communicate its certificate via port 8446. IF port 8446 is NOT open, then it defaults to 8444 BUT no certificate is passed (for example, TLS without verification).
8447	TLS	Used for remote messaging service infrastructure (and profile distribution infrastructure) for communication between Guardium systems in the federated environment / centrally-managed environment. Configuration profiles allow the definition of configuration and scheduling settings from a Central Manager and conveniently distribute those settings to managed unit groups without altering the configuration of the Central Manager itself.
8443	TLS	Enterprise load balancer This is needed for UNIX/Linux S-TAPs to communicate instances to the collector. However this port is also used for the Central Manager load balancer. If the installation wants to use Enterprise load balancer, then the S-TAP initiates a request to the Central Manager on port 8443 by sending an HTTPS message. So between database server and Central Manager, there will be the capability to use a proxy server, if customer doesn't want an open port directly from database to Central Manager.
8081	TLS	To use 8081 for the GIM client to connect to the GIM server - need to disable the GIM_USE_SSL parameter - it is ON by default. This parameter is part of the GIM common parameters in the GUI. If GIM_USE_SSL is NOT disabled, then the gim_client will attempt to communicate its certificate via port 8446. IF port 8446 is NOT open, then it defaults to 8444 BUT no certificate is passed (for example, TLS without verification).
8983	TCP	SOLR, incoming, SSL (Quick Search for Enterprise)
9983	TCP	SOLR, incoming, SSL (Quick Search for Enterprise)

Parent topic: Installing your Guardium system

Step 1. Assemble the following before you begin

To prepare for the deployment of the Guardium system, the network administrator needs to supply the following information.

- IP address for the interface card (eth0)
- Subnet mask for primary IP address
- Default router IP address.
- Hostname and domain name to assign to system
- DNS server IP addresses (up to three addresses), and add the new Guardium system to your DNS domain
- (optional) IP address for secondary management interface
- (optional) Mask for secondary IP management interface
- (optional) Gateway for secondary IP management interface
- (optional) NTP server hostname
- (optional) SMTP configuration information (for email alerts): IP address, port, and if authentication is used, an SMTP user name and password
- (optional) SNMP configuration information (for SNMP alerts) the IP address of the SNMP server and the trap community name to use.

- SAN storage devices
  If the installation is to be deployed on a Storage Area Network (SAN), all configuration information needed by the SAN, must be prepared before deployment. Also, there are additional installation steps required to partition the SAN storage device and install the Guardium OS.

Parent topic: Installing your Guardium system

SAN storage devices

If the installation is to be deployed on a Storage Area Network (SAN), all configuration information needed by the SAN, must be prepared before deployment. Also, there are additional installation steps required to partition the SAN storage device and install the Guardium OS.

Note: Installation on a SAN is supported, installation on a NAS is not supported.
Parent topic: Step 1. Assemble the following before you begin

Step 2. Set up the physical or virtual appliance

The setup instructions in this section are different when installing to a physical appliance or a virtual appliance.

- Physical Appliance
  After the appliance has been loaded into the customer's rack, connect the appliance to the network in the following manner:
- How to identify eth0 and other network ports
  Use the following CLI commands to map the network ports.
- Default passwords for physical appliances
  Default passwords are supplied for predefined users.
- Virtual appliance
  The IBM Security Guardium Virtual Machine (VM) is a software-only solution licensed and installed on a guest virtual machine such as VMware ESX Server.

Parent topic: Installing your Guardium system

Physical Appliance

After the appliance has been loaded into the customer's rack, connect the appliance to the network in the following manner:

1. Find the power connections. Plug the appropriate power cord(s) into these connections.
2. Connect the network cable to the eth0 network port. Connect any optional secondary network cables.
3. Connect a Keyboard, Video and Mouse directly or through a KVM connection (either serial or through the USB port) to the system.
4. Power up the system.

Parent topic: Step 2. Set up the physical or virtual appliance
Related information:
Lenovo System x3550 M5 Installation and Service Guide
Technical Requirements document
Changes in eth0 management port

How to identify eth0 and other network ports

Use the following CLI commands to map the network ports.

show network interface inventory

Use this CLI command to display the port names and MAC addresses of all installed network interfaces.

```
show network interface inventory
eth0 00:13:72:50:CF:40
eth1 00:13:72:50:CF:41
eth2 00:04:23:CB:11:84
eth3 00:04:23:CB:11:85
eth4 00:04:23:CB:11:96
eth5 00:04:23:CB:11:97
```

show network interface port

Use this CLI command to locate a physical connector on the back of the appliance. After using the show network interface inventory command to display all port names, use this command to blink the light on the physical port specified by n (the digit following *eth* - eth0, eth1, eth2, eth3, etc.), 20 times.

```
show network interface port 1
```

The light on port eth1 will now blink 20 times.

Install the software directly on dedicated computer

When installing the Guardium software directly to disk on a dedicated computer, use the Physical appliance instructions.

Parent topic: Step 2. Set up the physical or virtual appliance

Default passwords for physical appliances

Default passwords are supplied for predefined users.

When you receive a physical appliance from IBM, use these passwords for your initial configuration.
Note: Be sure to change all default passwords when you complete the installation.

Table 1. Default passwords for predefined users

User	Default password
accessmgr	guard1accessmgr
admin	guard1admin
cli	guard1cli

Parent topic: Step 2. Set up the physical or virtual appliance

Virtual appliance

The IBM Security Guardium Virtual Machine (VM) is a software-only solution licensed and installed on a guest virtual machine such as VMware ESX Server.

To install the Guardium VM, follow the steps in Creating the Virtual Image. The steps are:

- Verify system compatibility
- Install VMware ESX Server
- Connect network cables
- Configure the VM Management Portal
- Create a new Virtual Machine
- Install the IBM Security Guardium virtual appliance

After installing the VM, return to Step 4, Setup Initial and Basic Configuration, for further instructions on how to configure your Guardium system.

Parent topic: Step 2. Set up the physical or virtual appliance

Step 3. Install the Guardium® image

This section explains how to install the image and partition the disk.

1. Make sure your UEFI/BIOS “boot sequence” settings are set to attempt startup from the removable media (the CD/DVD drive) before using the hard drive.
   Note: Installation can take place from DVD. If needed, get the UEFI/BIOS password from Technical Support.
2. Load the Guardium image from the installation DVD.
3. The following two options appear:

   Standard Installation: this is the default. Use this choice in most cases when partitioning the disk.

   Custom Partition Installation: allows more customization of all partitions (locally or on a SAN disk). See Custom partitioning for further information on how to implement this option.

   Note:
   - The Standard Installation wipes the disk, repartitions and reformats the disk, and installs a new operating system.
   - On the first boot after installation, the user is asked to accept a Licensing Agreement. They can use PgDn to read through the agreement or Q to skip to the end. To accept the terms of the agreement, enter `q` to exit and then type `yes`. The user must enter `yes` to the agreement or the machine will not boot up.
4. The system boots up from DVD. It takes about 12 minutes for this installation.

   (d) The installation process will now ask you to choose a collector or aggregator (will be set to “Collector” automatically after 10 seconds if no input is provided). See the Product Overview for an explanation of Collector and Aggregator. If you wanted to choose aggregator and you did not choose it within 10 seconds, you must reinstall in order to get back to this point where you have a choice of aggregator.

   Note: If you plan to use the appliance as a central manager you MUST select Aggregator option.
5. The system automatically reboots at this point to complete the installation. The first login after a reboot requires a changing of passwords.

Parent topic: Installing your Guardium system

Step 4. Set up initial and basic configuration

The initial step should be the network configuration, which must be done locally through the Command Line Interface (CLI) accessible through the serial port or the system console.

Enter the temporary *cli* password that you supplied previously.

In the following steps, you will supply various network parameters to integrate the Guardium system into your environment, using CLI commands.

In the CLI syntax, variables are indicated by angled brackets, for example: <ip_address>

Replace each variable with the appropriate value for your network and installation. Do not include the brackets.

- Set the primary system IP address
  The primary IP address is for the eth0 connection, and is defined by using the following two commands:
- Set the Default Router IP Address
  Use the following CLI command:
- Set DNS Server IP Address
  Set the IP address of one or more DNS servers to be used by the appliance to resolve host names and IP addresses. The first resolver is required, the others are optional.
- SMTP Server
  An SMTP server is required to send system alerts. Enter the following commands to set your SMTP server IP address, set a return address for messages, and enable SMTP alerts on startup.
- Set Host and Domain Names
  Configure the hostname and domain name of the appliance. This name should match the hostname registered for the appliance in the DNS server.
- Set the Time Zone, Date and Time
  There are options for setting the date and time for the appliance.
- Set the Initial Unit Type
  An appliance can be a standalone unit, a manager or a managed unit; In addition, an appliance can be set to capture database activity via network inspection or S-TAP or both. The standard configuration would be for a standalone appliance (for all appliances), and the most common setting would use S-TAP capturing (only for collectors).
- Reset Root Password
  Reset your root password on the appliance using your own private passkey by executing the following CLI command (requires access key: *"t0Tach"*):
- Validate All Settings
  Before logging out of CLI and progressing to the next configuration step, review and validate the configured settings using the following commands:

- Reboot the System
  If the system is not in its final location, now is a good time to shut down the system, place it in its final network location, and start it up again.

Parent topic: Installing your Guardium system

Set the primary system IP address

The primary IP address is for the eth0 connection, and is defined by using the following two commands:

```
store network interface ip <ip_address>
store network interface mask <subnet_mask>
```

The default network interface mask is 255.255.255.0. If this value is the correct mask for your network, you can skip the second command.

To assign a secondary IP address, use the CLI command, store network interface secondary [on <interface> <ip> <mask> <gw> | off], that can be used to enable/disable the secondary interface.

Next you must restart the network by using the CLI command, restart network. Assigning a secondary IP address cannot be done by using the GUI, only through the CLI.

The remaining network interface cards on the appliance can be used to monitor database traffic, and do not have an assigned IP address.

Parent topic: Step 4. Set up initial and basic configuration

Set the Default Router IP Address

Use the following CLI command:

```
store network routes defaultroute <default_router_ip>
```

Parent topic: Step 4. Set up initial and basic configuration

Set DNS Server IP Address

Set the IP address of one or more DNS servers to be used by the appliance to resolve host names and IP addresses. The first resolver is required, the others are optional.

```
store network resolver 1 <resolver_1_ip>
store network resolver 2 <resolver_2_ip>
store network resolver 3 <resolver_3_ip>
```

Parent topic: Step 4. Set up initial and basic configuration

SMTP Server

An SMTP server is required to send system alerts. Enter the following commands to set your SMTP server IP address, set a return address for messages, and enable SMTP alerts on startup.

```
store alerter smtp relay <smtp_server_ip>
store alerter smtp returnaddr <first.last@company.com>
store alerter state startup on
```

Note: You can also configure the SMTP server by using the user interface. ClickSetup > Alerter.
Parent topic: Step 4. Set up initial and basic configuration

Set Host and Domain Names

Configure the hostname and domain name of the appliance. This name should match the hostname registered for the appliance in the DNS server.

```
store system hostname <host_name>
store system domain <domain_name>
```

Parent topic: Step 4. Set up initial and basic configuration

Set the Time Zone, Date and Time

There are options for setting the date and time for the appliance.

Timezone, date, time and ntp

1. Set timezone
2. Set date and time - Option 1 - set ntp. Option 2 - store system clock datetime

Date/Time Option 1: Network Time Protocol

Provide the details of an accessible NTP server and enable its use.

```
store system ntp server
store system ntp state on
```

Date/Time Option 2: Set the time zone, date and time

Use the following command to display a list of valid time zones:

```
store system clock timezone list
```

Choose the appropriate time zone from the list and use the same command to set it.

```
store system clock timezone <selected time zone>
```

Note: When setting up a new timezone, internal services will restart and data monitoring will be disabled for a few minutes during this restart.

Store the date and time, in the format: YYYY-mm-dd hh:mm:ss

```
store system clock datetime <date_time>
```

Note: Do not change the hostname and the time zone in the same CLI session.

Parent topic: Step 4. Set up initial and basic configuration

Set the Initial Unit Type

An appliance can be a standalone unit, a manager or a managed unit; In addition, an appliance can be set to capture database activity via network inspection or S-TAP or both. The standard configuration would be for a standalone appliance (for all appliances), and the most common setting would use S-TAP capturing (only for collectors).

store unit type standalone - use this command for all appliances.

store unit type stap - use this command for collectors.

Unit type standalone and unit type stap are set by default. Unit type manager (if needed) must be specified.

Note: Unit type settings can be done at a later stage, when the appliance is fully operational.
Parent topic: Step 4. Set up initial and basic configuration

Reset Root Password

Reset your root password on the appliance using your own private passkey by executing the following CLI command (requires access key: *"t0Tach"*):

```
support reset-password root <random>
```

Save the passkey used in your documentation to allow future Technical Support root accessibility. To see the current pass key use the following CLI command:

```
support show passkey root
```

Questions - How secure is the Guardium system root password? Who has access to it?

Guardium appliances are "black box" environments with the end user only having access to limited access Operating System accounts, such as:

cli; guardcli1; guardcli2; guardcli3; guardcli4; and, guardcli5.

The Graphical User Interface user accounts (for example admin and accessmgr) are not defined by the Guardium system's operating system, but are application IDs defined and managed via an application interface (accessmgr).

Being a secured server, root access is not readily available to anyone, but, is often required by Guardium support to gain access to the Guardium apoliances to troubleshoot and resolve issues. Guardium support does not use sudo, or any other userid other than root, to gain access to Guardium appliances.

The root password is secured using a "joint password" mechanism. The customer holds the keys to the appliance in the form of a eight-digit numeric passkey. IBM holds the passkey decoder. Without having both, the passkey and passkey decoder, neither IBM nor the customer can access the appliance as root.

The passkey is managed by the customer via the CLI interface. The customer can change the passkey at any time, without notifying IBM, by using the following CLI command:

```
support reset-password root
```

Anyone with CLI access can retrieve the passkey for root by using the following CLI command:

```
support show passkey root
```

When involving Guardium support, on a remote desktop sharing session, the support analyst will request the root passkey for the Guardium appliance in question. Once the passkey has been decoded, Guardium support will use the root password to gain access to the appliance as root. After the remote desktop sharing session terminates, the customer can change the passkey using the above CLI command, thereby ensuring IBM no longer has the root password for this appliance.

Being an eight-digit numeric key, the passkey has a range of 10000000 to 99999999. This range provides 89,999,999 possible passwords. All encoded passwords are hardened. They do not contain any common passwords, any dictionary words, their length varies and they contain national, special, alphabetic (upper and lower case) and/or numeric characters.

Access to the passkey decoder is restricted to a select few IBM Guardium employees, such as Guardium R&D, Guardium QA and Guardium support staff members. It is not available to IBM staff.

The CLI userids mentioned above (cli, guardcli1, guardcli2, guardcli3, guardcli4, guardcli5) do not use the passkey mechanism and their passwords are 100% governed by the customer with IBM having no access to their passwords. For this reason, IBM recommends keeping the root passkey in a password vault to ensure the appliance is accessible even if the CLI account passwords have been forgotten or misplaced.

Parent topic: Step 4. Set up initial and basic configuration

Validate All Settings

Before logging out of CLI and progressing to the next configuration step, review and validate the configured settings using the following commands:

```
show network interface all
show network routes defaultroute
show network resolver all
show system hostname
```

```
show system domain
show system clock timezone
show system clock datetime
show system ntp all
show unit type
```

Parent topic: Step 4. Set up initial and basic configuration

Reboot the System

If the system is not in its final location, now is a good time to shut down the system, place it in its final network location, and start it up again.

Remove the installation DVD before you reboot the system.

To stop the system, enter the following command in the CLI:

```
stop system
```

The system shuts down. Move the system to its final location, re-cable the system, and power the system back on. After the system is powered on, it is accessible (using the CLI and GUI) through the network, using the provided IP address or host name.

Parent topic: Step 4. Set up initial and basic configuration

Step 5. What to do next

This section details the steps of verifying the installation, installing license keys, and installing any available maintenance patches.

- Verify Successful Installation
  Verify the installation by following the following steps:
- Set Unit Type
  To set up a federated environment, configure one of the appliances as the central manager and set all the other appliances to be managed by the central manager.
- Install license keys
  This topic guides you through the procedure of installing and accepting Guardium license keys.
- Install maintenance patches (if available)
  You can install patches by using the CLI or through the GUI.
- Additional Steps (optional)
  The following sections discuss changing the baseline English to another language, installing S-TAP® agents, defining Inspection Engines and installing CAS agents.

Parent topic: Installing your Guardium system

Verify Successful Installation

Verify the installation by following the following steps:

1. Login to CLI - ssh cli@<ip of appliance>
2. Login to GUI - https://<hostname of appliance>.<full domain>:8443 (use admin userid)

The first login after a reboot will require a changing of passwords.

Login to the Guardium web-based interface and go to the embedded online help for more information on any of the following tasks.

Parent topic: Step 5. What to do next

Set Unit Type

To set up a federated environment, configure one of the appliances as the central manager and set all the other appliances to be managed by the central manager.

Use the CLI command store unit type to set the type of each Guardium system.

Parent topic: Step 5. What to do next

Install license keys

This topic guides you through the procedure of installing and accepting Guardium license keys.

Before you begin

- Download your license keys from Passport Advantage
- Install or upgrade your Guardium system
- Verify that the machine type is correctly set for your system

About this task

Installing a Guardium license key is a two-step process: you need to install the license key and then read and accept the terms of the license agreement. After installing a Guardium license key, the user interface will reload to reflect the functionality enabled by the new license.

Establishing a functional Guardium system requires installing both a base and at least one append licenses. The base license must be installed and accepted before installing and accepting any append licenses.

For more information about Guardium license keys, see License keys.

Attention:

When upgrading a Guardium system, you will not need to apply licenses. License keys will be automatically generated based on your preexisting installation, but you will need to review and accept the license agreements before you can begin using your Guardium system. To review and accept licenses on an upgraded system, navigate to Setup > Tools and Views > License and click the Read and accept license link.

Procedure

1. Log in to your Guardium system as the `admin` user.
2. Verify that the Machine Type displayed in the Guardium banner is correct for the system you are licensing. The machine type will be one of the following:
   - Standalone
   - Central Manager
   - Aggregator

   Attention: If you are setting up a central manager and the Machine Type indicates an aggregator, convert the system from an aggregator to a central manager using the following CLI command: `store unit type manager`.
3. Install a base license.
   a. Navigate to Setup > Tools and Views > License.
   b. On the License page, enter the base key for your system in the License key field and click Apply to continue.
   Attention: Depending on the system you are setting up, you will need to apply either a base collector key or a base aggregator key. A base aggregator key is required when setting up a central manager system.
   c. From the License Agreement dialog, review the license agreement associated with the base key and click Accept when you are ready to accept the terms.
   The Guardium interface will automatically refresh after accepting the agreement, but there will be no change in available functionality after installing a base license key.
4. Install one or more append licenses. Repeat the following steps for each append licence you have purchased and want to install.
   a. Navigate to Setup > Tools and Views > License.
   b. On the License page, enter an append key in the License key field and click Apply to continue.
   c. From the License Agreement dialog, review the license agreement associated with the append key and click Accept when you are ready to accept the terms.
   The Guardium interface will automatically refresh after accepting the agreement, and any new functionality associated with the append license will become available.
   d. Repeat the steps in this section for each append license you want to install.

What to do next

In an environment with a central manager, you can distribute the new licenses by navigating to the Manage > Central Management > Central Management page and clicking the  icon to distribute licenses from the central manager to managed units.

In an environment with a central manager, the central manager and its managed units must use the same shared secret. Set the shared secret from the Setup > Tools and Views > System page or by using the CLI command store system shared secret.

Parent topic: Step 5. What to do next
Related concepts:
License keys

Install maintenance patches (if available)

You can install patches by using the CLI or through the GUI.

Note: In federated environments, maintenance patches can be applied to all of the appliances from the Central Manager.

There may not be any maintenance patches included with the installation materials. If any are included, follow these steps to apply them:

1. Log in to the Guardium® console, as the cli user, using the temporary cli password you defined in the previous installation procedure. You can do this by using an ssh client.
2. Do one of the following:
   - If installing from a network location, enter the following command (selecting either ftp or scp):

     ```
     store system patch install [ftp | scp]
     ```

     And respond to the following prompts (be sure to supply the full path name to the patch file):

     Host to import patch from:

     User on <hostname>

     Full path to patch, including name:

     Password:

   - If installing using the fileserver function, enter the following command:

     ```
     store system install patch sys
     ```

     You will be prompted to select the patch to apply. Use wildcards in the pathname to get multiple patches. Also separate patch names by commas.
3. To install additional patches, repeat step 2.
4. To see if patches have been installed successfully, use the CLI command:

   ```
   show system patch installed
   ```

   Patches are installed by a background process that may take a few minutes to complete.

Parent topic: Step 5. What to do next

Additional Steps (optional)

The following sections discuss changing the baseline English to another language, installing S-TAP® agents, defining Inspection Engines and installing CAS agents.

Change the language

Installation of IBM Guardium is always in English. Use the CLI command store language to change from the baseline English and convert the database to the preferred language. A Guardium system can be changed only to Japanese or Chinese (Traditional or Simplified) after an installation. The store language command is considered a setup of the Guardium system and is intended to be run during the initial setup of the system. Running this CLI command after deployment of the appliance in a specific language can change the information already captured, stored, customized, archived or exported. For example, the psmls (the panes and portlets you have created) will be deleted, since they need to be re-created in the new language.

Note: To avoid the Guardium UI from displaying a mixture of languages, set the Central Manager and managed units to the same language.

Install S-TAP agents

Install S-TAP agents on the database servers and define their inspection engines. S-TAP is a lightweight software agent installed on the database server, which monitors local and network database traffic and sends the relevant information to a Guardium system (the collector) for further analysis, reporting and alerting. To install an S-TAP, refer to the S-TAP section of this information center. To verify that the S-TAP have been installed and are connected to the Guardium system:

1. Log in to the administrator portal.
2. Do one of the following:

Navigate to the Manage > System View, and click S-TAP Status Monitor from the menu. All active S-TAPs display with a green background. A red background indicates that the S-TAP is not active.

Navigate to Manage > Activity Monitoring > S-TAP Control, and confirm that there is a green status light for this S-TAP.

Define Inspection Engines

Define Inspection Engines for network-based activity monitoring.

Install CAS agents

Install Configuration Auditing System (CAS) agents on the database server.

Parent topic: Step 5. What to do next

Creating the Virtual Image

Use this section to install the virtual image.

- VMware Infrastructure Overview
  While you can install a Guardium VM on any VMware product, the VMware ESX server is the recommended platform for a virtual solution and is presented here.
- VM Installation Overview
  To install the IBM Security Guardium VM, follow the steps that are described here. After you install the VM, return to earlier Step 3, Install the IBM Security Guardium image, and earlier Step 4, Initial Setup and Basic Configuration.
- Creating a Hyper-V Virtual Machine

Parent topic: Installing your Guardium system

VMware Infrastructure Overview

While you can install a Guardium VM on any VMware product, the VMware ESX server is the recommended platform for a virtual solution and is presented here.

The VMware ESX Server on which you can install the Guardium VM is one component of the VMware infrastructure. Although not all VMware Infrastructure components are required to support the Guardium VM, you should be familiar with all components that are in use at your installation.

ESX Server: This component is used to configure and control VMware virtual machines on a physical host referred to as the ESX Server host. To install an Guardium VM, you first define a virtual machine on an ESX Server host, and then install and configure the Guardium VM image on that virtual machine. You can create multiple Guardium VMs on a single ESX Server.

VI Client (Virtual Infrastructure Client): This component is used to connect to a standalone ESX Server, or to a VirtualCenter Server. In the latter case, you can administer multiple virtual machines created over multiple ESX Server hosts.

Web Browser: Use a Web browser to download and use the VI Client software from an ESX Server host or the VirtualCenter server.

VirtualCenter Management Server (Optional): This component runs on a remote Windows machine, and can be used to manage multiple virtual machines on multiple ESX Server hosts. It offers a single point of control over all the ESX Server hosts.

Database (Optional): The VirtualCenter Server uses a database to store configuration information for the infrastructure. The database is not needed if the VirtualCenter Server is not used.

License Server (Optional): Stores and manages the licenses needed to maintain a VMware Infrastructure.

For more information, go to www.vmware.com and search for “ESX Quick Start”

Parent topic: Creating the Virtual Image

VM Installation Overview

To install the IBM Security Guardium VM, follow the steps that are described here. After you install the VM, return to earlier Step 3, Install the IBM Security Guardium image, and earlier Step 4, Initial Setup and Basic Configuration.

If you are installing multiple Guardium VM systems in a VMware VirtualCenter Management Server environment, you can create a template system from the first Guardium VM that you create, and then clone that template as necessary. Then, all you need to do is set the IP address on each cloned system. For more information, see the note following Step 7.

Step 1: Verify system compatibility

1. Verify that the host is compatible with VMware's ESX Server (ESX 4.0 Update 4 and higher is the bare minimum to run a Guardium system). See the VMware document entitled Systems Compatibility Guide for ESX Server, which is available online in PDF format.
2. Verify that a virtual machine installed on the host will be able to provide the minimum recommended resources for a Guardium system, whether you plan to use it as a collector, central manager, or aggregator. See the Minimum/Recommended Resources in the Hardware Requirements section of this document.
3. When you create a 64-bit VM for the first time or upgrade a 32-bit VM to 64-bit, ensure that the virtual hardware is correctly configured for 64-bit operation. In some cases, you might need to perform an Upgrade Virtual Hardware operation. For information, refer to your VMware documentation.

Step 2: Install VMware ESX Server

If it is not already installed, install VMware ESX Server. VMware provides installation instructions on their website to help with installing and configuring the VMware Infrastructure and ESX server.

Note: The ESX server is only supported on a specific set of hardware devices. For more information, see the VMware Virtual Infrastructure documentation.

Step 3: Connect network cables

Before you define any virtual switches that will be used for the Guardium VM, you must connect the appropriate NICs to the network. You cannot assign NICs to virtual networks or switches until the NICs are physically connected.

The following table describes how the Guardium VM uses network interfaces. Refer to this table to make the appropriate connections before you configure the virtual switches for use by the Guardium VM.

Table 1. IBM Security Guardium VM Network Interface Use

Interface	Description
Proxy interface (eth0)	This interface is the main gateway to the appliance, and is used for these purposes: • Graphical web-based User Interface (GUI) to manage, configure, and use the solution • Command Line Interface (CLI) for initial setup and basic configuration • Connections with external systems such backup systems, database servers, and LDAP server • Communication with other Guardium components such as other appliances (aggregator, central manager) and agents that are installed on database or file servers such as S-TAP or CAS clients
Application server interface (eth1)	This interface is required if you configure your Guardium system as a transparent proxy. It connects to the application servers whose content your Guardium system is configured to mask.

Step 4: Configure the Guardium VM management portal

The default configuration for a new VMware ESX Server installation creates a single port group for use by the VMware service console and all virtual machines. For the Guardium VM, we strongly recommend that you do not share ports with the VMware console or any other virtual machine. Follow these instructions to create one or more virtual switches to be used by a Guardium VM.

1. Open the VMware VI Client, and log on to either a VirtualCenter Server, or the ESX Server host on which you want to create a new virtual machine.
2. If you are logged in to a VirtualCenter Server, click Inventory in the navigation bar, and expand the inventory as needed to display the managed host or cluster on which you plan to install a Guardium VM.
3. In the inventory display, click the host or cluster on which you plan to install a Guardium VM.
4. Click Configuration tab, click Networking in the Hardware box, and then click Add Networking.

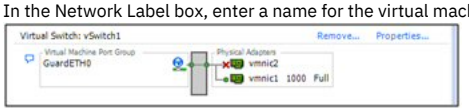
This opens the Add Network Wizard, which is used for various purposes.

Use the Add Network Wizard to define a new virtual switch for the Guardium VM network interface. This is the connection over which you will access the Guardium VM management console, and over which the Guardium VM will communicate with other Guardium components (S-TAPs, for example, which are software agents that you will install later on one or more database servers).

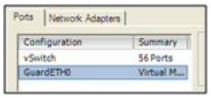
5. In the Connection Types box, click Virtual Machine and click Next.

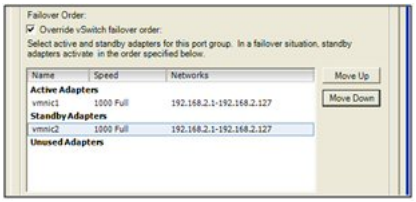
6. In the Network Access panel, click Create a virtual switch, and mark the unclaimed network adapter that you will use for the Guardium VM network interface:

7. Optionally mark a second unclaimed network adapter if want to use the VMware IP teaming capability to provide a secondary (failover) network interface. Later, you will designate this second adapter as a Standby Adapter (and of course, you must cable both NICs appropriately).
8. Click Next to continue to the Connection Settings page of the Add Network Wizard.
9. In the Network Label box, enter a name for the virtual machine port group, for example: GuardETH0, and click Next.



10. In the Summary page, click Finish. The new virtual switch is displayed in the Configuration tab.
11. Optional. If you have defined a second adapter for failover purposes: (a) Click Properties link for the virtual switch just created to open the virtual switch Properties panel. (b) Click Ports tab and select the virtual port group just created (GuardETH0 in the example), and click Edit. (c) In the virtual port group Properties panel, click NIC Teaming tab, mark the Override vSwitch Failover box, and then move the second adapter to the Standby Adapters list. (d) Click OK to close the virtual port group Properties box, and click Close to close the virtual switch Properties box.





Step 5: Create a new virtual machine

If you have not already done so, create a new virtual machine on which to install a Guardium VM.

Perform this task by using the VMware VI Client.

1. Open the VMware VI Client, and log on to either a VirtualCenter Server, or the ESX Server host on which you want to create a new virtual machine.
2. If you are logged in to a VirtualCenter Server, click Inventory in the navigation bar, expand the inventory as needed, and select the managed host or cluster to which you want to add the new virtual machine.
3. From the File menu, click New – Virtual Machine to open the configuration Type panel of the New Virtual Machine wizard.
4. Click Typical as the configuration type, and click Next to continue with the Name and Folder panel.
5. On the Name and Folder panel:

   Enter a name for the new virtual machine in the Virtual Machine Name field. This name appears in the VI Client inventory and is also used as the name of the virtual machines files.

   To set the inventory location for the new virtual machine, select a folder or the root location of a datacenter from the list under Virtual Machine Inventory Location.

   Click Next.

6. If your host or cluster contains resource pools, the Resource Pool panel is displayed, and you must select the resource (host, cluster, or resource pool) in which you want to run the virtual machine. Click Next.
7. On the Datastore panel, optionally select a datastore in which to store the new virtual machine files, and click Next.
8. In the Choose the Guest Operating System panel, choose the operating system that corresponds to the Guardium image that you are installing. Click Linux > RedHat Enterprise Linux 6, 64-bit from the Version box, and click Next. .

   The operating system is not installed now, but the OS type is needed to set appropriate default values for the virtual machine.

   For VM minimum resources, refer to the Hardware Requirements in the Before you begin section.

9. On the Virtual CPUs panel, select the number of CPUs recommended for the type of Guardium VM being installed, and click Next.
10. On the Memory panel, select the amount of memory recommended for the type of Guardium VM being installed, and click Next. Important: the initial value must be at least 16 GB. If customers want to work outside the required range, consult with Technical Support.
11. On the Network panel, click 1 as the number of ports that are required, and click Next.
12. For the selected port, use the Network pull-down menu to choose a port group configured for virtual network use. (You should have defined this port group in the previous procedure.)
13. For the selected port group, mark the Connect at Power On check box (it should be marked by default), and click Next.
14. On the Virtual Disk Capacity panel, enter the amount of disk space to reserve for the new virtual machine in the Disk Size field.
15. On the Ready to Complete panel, verify your settings and click Finish.

This completes the definition of the new virtual machine. The operating system has not yet been installed, so if you attempt to start the virtual machine, that activity will fail.

Step 6: Install the Guardium system

Perform this task using the VMware Virtual Infrastructure Client.

1. Open the VMware VI Client, and log on to either a VirtualCenter Server, or the ESX Server host on which you want to create a new virtual machine.

2. If logged into a VirtualCenter Server, click Inventory in the navigation bar, expand the inventory as needed, and select the virtual machine on which you want to install the Guardium VM.
3. On the Summary tab, click Edit Settings.
4. Click CD/DVD Drive 1.
5. Select one of the following options to determine from where the virtual CD-ROM/DVD device will read the Guardium® Installation program. **We strongly recommend the first option**:

   Datastore ISO File – Connect to the Guardium Installation ISO file on a datastore. If you have not already done so, copy the Guardium ISO files to a datastore accessible from the ESX Server host on which the virtual machine is installed. Click Browse to select the file.

   Caution: For the remaining options, you will place the Guardium Installation CD/DVD in a CD-ROM/DVD drive. If you reboot any system with an Guardium Installation CD/DVD in its CD-ROM/DVD drive, you will install Guardium on that system, wiping out the host operating system and files.

   Client Device – Connect to a CD-ROM/DVD device on the system on which you are running the VI Client. If you select this option, insert the Guardium CD/DVD in the CD-ROM/DVD drive of the system on which the VI Client is running.

   Host Device – Connect to a CD-ROM/DVD device on the ESX Server host machine on which the virtual machine is installed. If you select this option, choose the device from a drop-down menu, and insert the Guardium CD/DVD in the CD-ROM/DVD drive of the ESX Server host machine.

6. Click OK.
7. Click Power On to start the virtual machine.
8. If you selected Client Device as your CD/DVD Drive option, click Virtual CD-ROM (ide0:0) in the toolbar, and select the local CD-ROM device to connect to.
9. Click Console tab to display the virtual machine console. You will need to respond to several prompts during the installation process.
10. Skip this step if you are using theGuardium DVD.

    When prompted for the second CD, depending on option you use in step 5 you need to either put the second CD in its drive or select the second CD ISO image. Continue by pressing Enter. When prompted for the cli password, enter a temporary password for use when logging in to the Guardium CLI, which you will need to do to set the IP configuration parameters for the appliance.

11. When you are prompted for the GUI admin password, enter a temporary password for use when logging in to the Guardium user interface as the admin user.
12. When asked if building a collector or aggregator, choose the appropriate type.
13. Click No to the Master Passkey prompt.

    Caution: If a CD-ROM/DVD drive was used, the CD/DVD ejects when the installation completes. Be sure to remove the installation CD/DVD from that drive. If the ISO file was used, be sure to remove the ISO CD ROM by changing the virtual CD/DVD back to a Client or Host Device. Otherwise, the next time it is rebooted, you will install Guardium on the host machine, wiping out the host machine operating system and all files.

    The machine will reboot automatically, and you will be prompted to log in as the CLI user.

14. At this point, return to Step 4, Set up Initial and Basic Configurations for complete instructions on configuration of the Guardium system.

Step 7: Install Multiple VMs

(Optional) To install multiple GuardiumVMs, you can repeat the procedures for each appliance, or you can minimize your work by cloning the first Guardium VM that you created, and following these steps:

1. Use the VMware virtual infrastructure server product to clone the first Guardium VM that you configured to a template.
2. From the template, create a clone for each additional Guardium VM to be configured.
3. For each clone, log in to the Guardium VM console as the cli user by using the temporary cli password and reset any of the IP configuration parameters that you set in the previous procedure. Mandatory tasks: reset the IP address, reset the GLOBAL_ID (GID), and reset the host name. The UNIQUE_ID (UID) is set automatically and does not require manual configuration. Be sure to review all of the IP configuration settings entered in the previous procedure.

   ```
   store network interface ip <ip_address>
   store network interface mask <subnet_mask>
   store product gid <n>
   store system hostname <host_name>
   ```

   When you are done, enter the restart network command.

   ```
   restart network
   ```

   Note: The unique ID (UID) of the appliance is recalculated every time the hostname changes in order to avoid having multiple appliances with the same unique ID.
   Note: The global ID (GID) can be any number so long as it is unique and less than 9223372036854775808. During the cloning process this unique number is necessary. Please obtain the global IDs from your other appliances and use a number that is unique for this clone.

Parent topic: Creating the Virtual Image

Creating a Hyper-V Virtual Machine

Before you begin

- Hyper-V is a virtualization solution from Microsoft. It is assumed that the Guardium user using Hyper-V has pre-experience with Hyper-V. Most installations of Hyper-V are straight forward. The instructions listed in this Guardium help topic may be more complex than needed.
- Verify system requirements for the version of Guardium being installed.
- Reserve an IP address for the virtual machine.

About this task

Procedure

1. Log into the Hyper-V server as an administrator.
2. Start the Hyper-V manager at Start menu > Administrative Tools > Hyper-V Manager.
3. Right-click on the Hyper-V server and select New > Virtual Machine.

a. Enter the host name in Name field, use the default Store location, then click Next.
b. Enter desired memory in the RAM field, then click Next. Verify that the specified RAM meets the minimum system requirements for your Guardium version.
a. Select connection Trunk > Virtual Network, then click Next.
b. Specify the desired disk size on the Virtual Disk dialog, then click Next. Verify that the specified virtual disk size meets the minimum system requirements for your Guardium version.
c. Accept the default settings under Installation Options, then click Next.
d. Click Finish to create your new virtual machine.
4. Right-click on your new virtual machine in the Virtual Machines list and select Connect to open the console.
5. Power on the virtual machine to reserve a MAC address by clicking the green button or selecting Action > Start.
6. At the boot failure prompt, power off the virtual machine by clicking the gray button or selecting Action > Turn Off.
7. Select File > Settings to continue configuring your virtual machine.
a. Specify the desired number of logical processors under Hardware > Processor > Logical Processors. Verify that the specified number of processors meets the minimum system requirements for your Guardium version.
b. Record the MAC address assigned under Hardware > Network Adapter. You will need this information later in the installation process.
c. Select the network adapter and click Remove.
d. Select Hardware > Add Hardware > Legacy Network Adapter, then click Add. The selection is automatically moved to Legacy Network Adapter.
e. Select Trunk > Virtual Network.
f. Select MAC Address > Static and enter the previously-recorded MAC address.
g. Select the Enable Virtual LAN Identification check box.
h. Enter a VLAN Designation of `3xxx`. For example, `3156`.
i. Select Hardware > BIOS, raise the Legacy Network Adapter, then click OK.
8. Add the virtual machine's MAC address to your IP reservation.
9. Add the virtual machine's IP address, host name, and MAC address to gmachine_list.txt.
10. Start the virtual machine. The Dev-IT managed OS Boot dialog should appear, stop at BOOT: until timeout, and then return to the Boot Failure prompt.
11. Run your PXE command, then use CTRL-ALT-DEL macro button to reboot the virtual machine. Allow the machine to build.
12. Use TOUCH and SU - CLI to assign the proper IP address, route, and DNS settings. The host and domain settings are typically are auto-configured.
13. Use SU - CLI > STOP SYSTEM to shut down the system.
14. Right-cick the virtual machine and select Settings.
a. Replace Legacy Network Adapter with the default network adapter selection.
b. Select Trunk > Virtual Network.
c. Select MAC Address > Static and enter the previously-recorded MAC address.
d. Enter a VLAN Designation of `3xxx`. For example, `3156`.
15. Boot the virtual machine.

What to do next

Verify that the virtual machine is functioning by pinging OTIS from the virtual machine and by logging into the virtual machine over SSH from a remote host.

Some common problems include:

- Not replacing the default network adapter with the legacy adapter will not allow PXE.
- Not replacing the legacy network adapter with the default network adapter leave the Guardium system without network connectivity.
- Starting the machine before changing the MAC address after replacing the legacy network adapter generates a new MAC address and virtual adapter on the virtual machine. This must be remedied for the system to work. Change the MAC address to your previously-recorded MAC address and use the normal method to clean up the ifcfg-eth0 and 70-persistent-nework.rules.

Parent topic: Creating the Virtual Image

Custom Partitioning

If you customize the partitioning of the hard drive, you must make several choices.

1. Choose Custom Partitioning Installation from the boot screen.
Choose Create custom layout and use the recommended partitioning scheme listed here.
Note: The boot loader, a special program that loads the operating system into memory, is part of any custom partitioning installation.
2. Create custom layout. In this case, there are existing partitions on the disk. Do not delete any partitions. Choose the custom layout selection to add whatever partitions you want to what is already on the disk.The following table specifies recommended values for custom layout.

Table 1. Recommended values for custom layout

Partitions	Values
/	25 GB
Swap portion	half of RAM size
/boot	5 GB
/var	All the rest

All the available drives are also displayed on this screen. Choose the drive for the partitioning and then installation.

After the partitioning is finished, the Guardium® system software is installed automatically.

If values are created that exceed the space available on the disk, an error message appears.

Click OK to reboot the system and return to the beginning of Custom Partitioning.

See the Red Hat Enterprise Linux documentation for more information about how the Red Hat distribution handles partitioning.

Note: Non-default partitioned systems - Custom partitioned systems cannot be upgraded using an upgrade patch. Instead, you must use the backup, rebuild, and restore method. If there is uncertainty regarding the partitioning of systems, download and install Health Check p9997. The resulting patch log contains information regarding

system partitioning.
Parent topic: Installing your Guardium system

How to partition with an encrypted LVM

If you want to use an encrypted disk, follow these steps to create an encrypted LVM volume that contains the / and /var logical volumes.

For the encrypted LVM installation, you are asked to enter an encryption key. Then, on EVERY reboot, the user is required to enter this key to unlock the LVM volume (This means that the user must have console access to the appliance, either physical or remote access).

Important – The encryption key must be safeguarded and retained, as it is impossible to replace if lost.

Note: The boot loader, a special program that loads the operating system into memory, is part of a custom partitioning installation. An example of the password entry screen is shown near the end of this topic.

1. Insert the IBM Guardium DVD and boot the machine.
2. Choose Custom Partition Installation from the boot screen.
3. Press Enter.
4. Click Remove all partitions and create default layout from the first RedHat Enterprise Linux screen. Also, select the check boxes Encrypt system and Review and modify partitioning layout.
5. Click Next.
6. A warning notice appears on the following screen, asking if you really want to remove all partitions. Click Yes.
7. Click LogVol00 in the next screen and click Edit to bring up the Edit LVM Volume Group dialog.
8. Click LogVol00 from the list in the previous screen and click Edit.
9. On the next screen, change the size to 10240 and click OK.
10. Click LogVol01 from the list on the next screen and click Edit.
11. Allocate a swap partition that is half as large as the memory that is installed on the system. Specify the size of the swap partition and click OK.
12. Click Add. The Make Logical Volume dialog is displayed.
13. Specify /var as the mount point, and let the system pick the remaining size.
14. Review the sizes of your partitions. Then, click OK.
15. Then click OK from the Edit LVM Volume Group: VolGroup00 dialog.
16. Click Next in the next screen, which will take you to the passphrase dialog.
17. Enter the passphrase of your choice into the Enter passphrase field and enter the identical passphrase into the Confirm passphrase field. Click OK.
    Note: The passphrase must be entered each time that the system is booted. There is no way to recover a lost LVM passphrase.

    The Bootloader configuration dialog is displayed. When a computer with Red Hat Enterprise Linux is turned on, the operating system is loaded into memory by a special program that is called a boot loader. A boot loader usually exists on the system's primary hard disk (or other media device) and has the sole responsibility of loading the Linux kernel with its required files or (in some cases) other operating systems into memory.

    In most cases, the default options are acceptable, but depending on the situation, changing the defaults options may be necessary.
18. At this screen, click Next. This starts the encrypted installation.

    During the installation and further re-boots, you are asked to enter the LUKS (Linux Unified Key Setup) passphrase for the LVM during boot. After you enter the LUKS passphrase, the system completes the boot process.

Parent topic: Installing your Guardium system

Example of SAN Configuration

This appendix details the steps involved in moving to a command prompt in order to pre-partition a hard drive (as is needed for SAN installation).

First partition space on the SAN storage device, and then install the IBM Security Guardium OS. Choose one hard disk for this installation.

Note: Depending on what SAN hardware is used, specific instructions may be different. Installation on a SAN is supported; installation on a NAS is not supported.

Summary of steps

1. Enter system setup (press F1 on IBM® servers during initial boot) and modify the Start Options to select the appropriate PCI slot to boot from (where the QLogic Card is).
2. Modify the BIOS for the QLogic card by pressing Ctrl-Q, when the QLogic BIOS is loading, to enable it to be a boot device. Then select the LUN (logical unit number) of the boot device.
3. Boot from the RedHat 5.8 DVD and enter Rescue mode in order to run fdisk and create partitions on the SAN device using the specifications listed here:

   Table 1. Partitions on SAN device

Partitions	Space
1	500 MB for /boot
2	Amount of system memory + 4 GB
3	25 GB for /
4	All remaining space for /var

   Note: While the RedHat installation process would allow you to create the partitions and load the OS, the system does not boot properly after the installation unless the partitions are pre-created with fdisk.
4. Proceed with the OS installation utilizing the previously defined partitions (use only the /dev/sda device).
5. Reboot and finish the remaining installation steps (hostname, IP configuration, and so on).

Note:

In the SAN environment, the single LUN is presented to RedHat 5.8 as multiple devices due to redundant paths within the network switch(es) on the SAN. (The SDD storage was eight devices.)

This is a function of the SAN storage brand/type and how it is configured at each site.

It is very important to only edit the existing partitions that the IBM Guardium installation sees by adding the mount point and setting the file system (ext4 or swap,) and not changing other settings (such as size) and to unselect all devices other than /dev/sda when selecting which device to load the OS on.

Instructions for running fdisk

Follow these instructions for running fdisk to pre-partition the SAN storage from RedHat rescue mode:

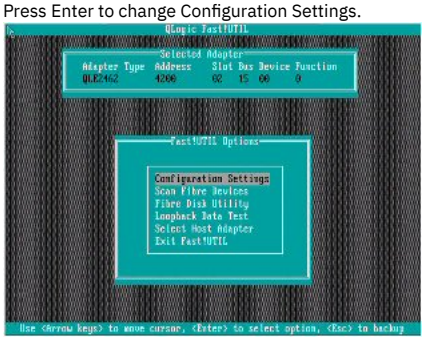
1. Assuming SAN is the only storage attached to the server, type `fdisk /dev/sda`. Type `y` if a warning appears regarding working on the whole device.
2. Type `n` for a new partition.
3. Type `p`for a primary partition.
4. Type `1`for partition #1.
5. Press Enter to accept the default start location.
6. Type `+512M` to make partition 1 500MB in size (this will be the /boot partition).
7. Type `n` for a new partition.
8. Type `p` for a primary partition.
9. Type `2` for partition #2.
10. Press Enter to accept the default start location.
11. Type `+12288M` to make partition 2 12GB in size (this assumes 8GB of physical RAM). The recommended size is physical RAM + 4GB (this will be the swap partition).
12. Type `n` for a new partition.
13. Type `p` for a primary partition.
14. Type `3` for partition #3.
15. Press Enter to accept the default start location.
16. Type `+10240M` to make partition 3 10 GB in size (this will be the / partition).
17. Type `n` for a new partition.
18. Type `p` for a primary partition (will default to partition #4).
19. Press Enter to accept the default start location.
20. Press Enter to fill to maximum size (this will be the /var partition).
21. Type `w` to write the partition table to the SAN.
22. Type `exit` to exit rescue mode and reboot to begin the Custom Partition Installation (Step 3, Install the IBM Security Guardium image).

Examples of screenshots for QLogic setup

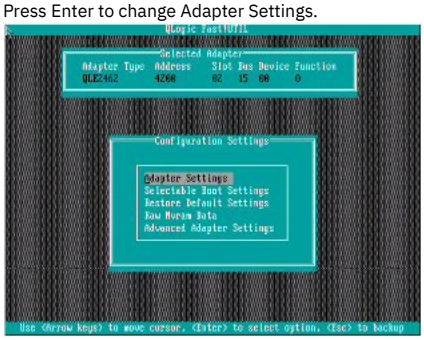
The Q-Logic screens used here are representative of the steps needed. Other Fiber Channel cards can be used.

1. Modify the BIOS for the QLogic card by pressing CTRL-D. This is the first screen presented after pressing Ctrl-Q when prompted to enter the Configuration Setup Utility. This is a two-port card; select the appropriate port and press Enter.

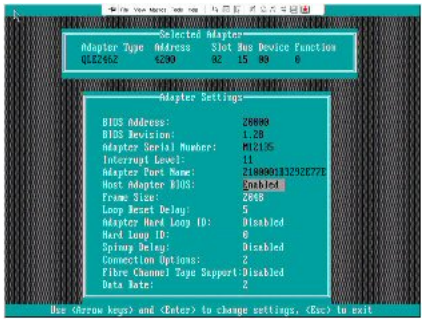
2. Press Enter to change Configuration Settings.



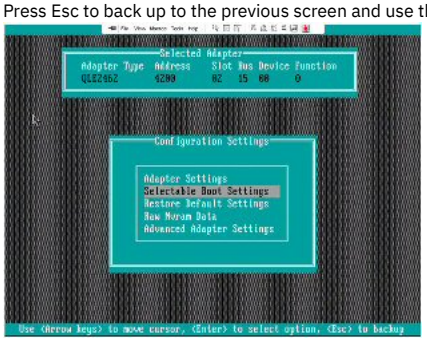
3. Press Enter to change Adapter Settings.



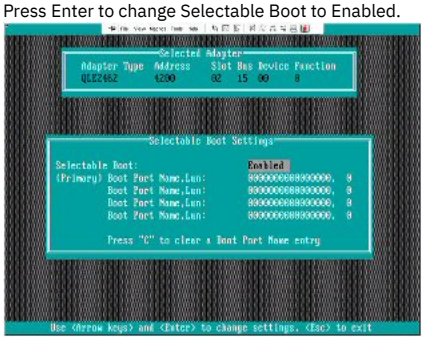
4. Use your arrow keys to select Host Adapter BIOS and press Enter to toggle to Enabled.



5. Press Esc to back up to the previous screen and use the down-arrow to select Selectable Boot Settings and press Enter.



6. Press Enter to change Selectable Boot to Enabled.



7. Select the first Boot Port Name, LUN and press Enter to display a list of LUNs. If you are configuring the proper card/port, the LUN number(s) appear here. Select the first one in the list.

8. Press Esc until you have backed out to the screen that says Reboot and select it to reboot the system. You are now ready to proceed with the IBM Security Guardium installation.

Parent topic: Installing your Guardium system

Upgrading your Guardium System

Use this information to upgrade your IBM Security Guardium system to the latest V10 offering.

Before beginning an upgrade, review the Planning an upgrade, Choosing an upgrade method, and Mixed-version environments during an upgrade sections.

In addition, the following resource are available to support your upgrade experience::

- IBM Security Guardium high-level upgrade roadmap: contains an overview of the supported upgrade paths from various releases of Guardium.
- IBM Guardium V10.1 Software Appliance Technical Requirements: describes the hardware requirements for both physical and virtual machine installations.
- Hints and tips on upgrading to V10: provides videos with information about upgrade planning, execution, and troubleshooting.

- Planning an upgrade
  Learn about different upgrade scenarios and identify the correct approach for upgrading your Guardium systems with minimal downtime.
- Common upgrade tasks
  Tasks such as purging system data, monitoring installations, and cleaning up after an upgrade are common to all Guardium upgrade scenarios.
- Upgrading a 32-bit environment
  Upgrade your 32-bit Guardium environment without using a backup central manager.

- Upgrading a 64-bit environment
  Upgrading your 64-bit Guardium environment without using a backup central manager.
- Upgrading a 32-bit environment with a backup central manager
  Upgrade your 32-bit Guardium environment using a backup central manager.
- Upgrading a 64-bit environment with a backup central manager
  Upgrading your 64-bit Guardium environment using a backup central manager.

Planning an upgrade

Learn about different upgrade scenarios and identify the correct approach for upgrading your Guardium systems with minimal downtime.

- Choosing an upgrade method
  The best approach for upgrading Guardium depends on multiple factors, including the version you are upgrading from, the hardware of your system, and any special partitioning requirements you may have.
- Mixed-version environments during an upgrade
  During an upgrade, your Guardium environment will enter a mixed-version state with restricted functionality.
- Upgrading with central managers and aggregators
  Minimize disruptions to your Guardium environment by following a top-down upgrade approach.

Parent topic: Upgrading your Guardium System

Choosing an upgrade method

The best approach for upgrading Guardium depends on multiple factors, including the version you are upgrading from, the hardware of your system, and any special partitioning requirements you may have.

Determine your current Guardium version and patch level by clicking the icon in the main user interface and selecting About Guardium.

Upgrade to the latest version of Guardium using one of the following methods:

Upgrade patch
: Use an upgrade patch to upgrade all systems in a managed environment. The upgrade patch preserves all data and configurations with the exception of UI customizations due to a new UI architecture. Using an upgrade patch without defining a backup central manager is recommended for 64-bit environments with default partitioning.

Backup, rebuild, restore
: Use a backup, rebuild, and restore method. This requires taking a full system backup, rebuilding the system from the latest ISO, and restoring system data and configuration from the backup. Using the backup, rebuild, and restore method with a backup central manager is recommended for 32-bit environments or systems with custom partitioning.

Important: Custom partitioned systems cannot be upgraded to V10 using an upgrade patch. Instead, you must use the backup, rebuild, and restore method. If there is uncertainty regarding the partitioning of systems, download and install Health Check p9997. The resulting patch log contains information regarding system partitioning.

Use the following tables to identify the best approach for upgrading your systems to the latest version of Guardium.

Table 1. Determine an upgrade method

Guardium system	**Upgrade methods for V10**	
	Backup V9, rebuild system to latest V10, restore from V9 backup	**Apply latest V10 upgrade patch**
V9 patch 600 (64-bit) or later	Yes	Yes
V9 patch 600 (32-bit) or later	Yes	No
V9.0 below patch 600	Yes	No
V8.2 or earlier	No	No

Table 2. Overview of V10 upgrade paths

Guardium level on current system	**Upgrade path to the latest V10**
V8.2	You cannot upgrade V8.2 systems directly to V10 systems. You must rebuild your appliances with the latest V9 (64-bit) ISO and then install the latest V9 to V10 upgrade patch. 1. Create V8.2 system backup. 2. Rebuild appliance with the latest V9 (64-bit) ISO. 3. Install V9 patch 600 or later (64-bit) GPU. 4. Restore the system backup from original V8.2 system. Note: For collectors, upgrade all corresponding S-TAPs to latest V9 before proceeding to the next step. 5. Install Health Check p9997. 6. Create a V9 (64-bit) system backup. 7. Install the latest V9 to V10 upgrade patch.
V9 (32-bit)	1. Create a V9 (32-bit) system backup. 2. Rebuild the appliance with latest V10 (64-bit) ISO. 3. Apply V10 patch 100 or later GPU. 4. Restore the system backup from the original V9 (32-bit) system.

Guardium level on current system	Upgrade path to the latest V10
V9 below patch 600 (64-bit)	1. Create a V9 (64-bit) system backup. 2. Install V9 patch 600 or later (64-bit) GPU. 3. Create a V9 (64-bit) system backup. 4. Install Health Check p9997. 5. Install the latest V9 to V10 upgrade patch.
V9 patch 600 (64-bit) or later	1. Install Health Check p9997. 2. Create V9 (64-bit) system backup. 3. Install the latest V9 to V10 upgrade patch.
V10	1. Apply latest V10 GPU.

Parent topic: Planning an upgrade
Related concepts:
Upgrading a 32-bit environment
Upgrading a 32-bit environment with a backup central manager
Upgrading a 64-bit environment
Upgrading a 64-bit environment with a backup central manager

Mixed-version environments during an upgrade

During an upgrade, your Guardium environment will enter a mixed-version state with restricted functionality.

Since the upgrade process cannot be completed on all systems (central managers, aggregators, and collectors) and all S-TAPs simultaneously, your Guardium environment will enter a mixed-version state during upgrade. For example, after upgrading a central manager to the latest V10, managed units will continue operating at V9 GPU 600. Although mixed-version environments are supported, several limitations must be considered as part of any upgrade plan. For example, data collection, data assessment, and policies (with some restrictions) will continue to work while in a mixed state, but functions with new or enhanced capabilities will not work in a mixed environment.

Important: Upgrade your entire environment to the latest patch level of V10 as soon as possible. Be aware of the following while operating in a mixed-version environment during upgrade:

- Complete Guardium functionality will not be available until the entire environment has been upgraded to the latest V10.
- Do not make configuration changes while operating in a mixed-version environment.
- Guardium V10 does not support mixed environments with managed units below V9 GPU 600.

Distributing configurations and settings
: Configuration distribution is not supported between a V10 central manager and V9 patch 600 or later managed units. This restriction includes the following:

  - Policies cannot be distributed from a V10 central manager to V9 patch 600 managed units. Policies already installed on the managed units prior to the upgrade remain unchanged.
  - Patch backup settings cannot be distributed from a V10 central manager to V9 patch 600 or later managed units. Patch backup settings defined before the upgrade remain unchanged.
  - UI layout customization and distribution is not supported on a V10 central manager with V9 (patch 600 or later) managed units.

Managed units
: You cannot register additional V9 patch 600 or later managed units after upgrading the central manager to V10. Units registered before the upgrade remain registered after the upgrade.

Quick search
: Quick search for enterprise works in a mixed environment that consists of a V10 central manager and V9 patch 530 or later managed units. The user interface must be restarted in order to reinitialize quick search for enterprise. Managed units prior to GPU 500 are unable to take advantage of enterprise search, although local quick search is still available.
  If a central manager is upgraded from V9 to the latest V10 and the managed units remain on V9, quick search is disabled on the V9 managed units until the managed units are upgraded to V10.

Reports
: Some reports will result in SQL errors or may not display data correctly when viewed on V9 patch 600 or later managed units, including the following:

  - Aggregation/Archive Log
  - Connections Quarantined
  - Installed Patches
  - Inactive Inspection Engines
  - S-TAP Verification
  - Connection Profiling List
  - Replay Statistics
  - Replay Summary

  With the exception of *Enterprise Buffer Usage Monitor* data, data from V9 patch 600 or later managed units is not accessible in the following reports on a V10 central manager:

  - Enterprise S-TAP Verification
  - Enterprise Load Balancing Events

Parent topic: Planning an upgrade

Upgrading with central managers and aggregators

Minimize disruptions to your Guardium environment by following a top-down upgrade approach.

This means first upgrading one high-level system and then upgrading the systems or agents that report to it, then upgrading the next high-level system and the systems or agents that report to it, and so on. This approach minimizes the impact of operating a mixed-version Guardium environment.

A top-down approach is necessary because an upgraded aggregator can aggregate data from older releases, but an older aggregator cannot aggregate data from newer releases. Similarly, an upgraded central manager can manage units running older releases, but the managed units will not enjoy full functionality until they are upgraded to match the central manager.

To avoid these issues, upgrade a central manager before upgrading any of its managed units. If you have multiple central managers, first upgrade one central manager and then upgrade its managed units before going on to upgrade the next central manager and its managed units.

Similarly, upgrade an aggregator before upgrading any units that export data to it. If you have several aggregators, first upgrade one aggregator and then upgrade the collectors that report to it before going on to upgrade the next aggregator and its collectors.

Finally, upgrade a collector before upgrading the S-TAPs registered to it. Upgrade one collector and all the S-TAPs registered to it before going on to upgrade the next collector and its S-TAPs.

This approach provides compatible systems--from central managers to aggregators, collectors, and S-TAPs--in each branch of your environment more quickly than upgrading all your central managers or aggregators before upgrading any collectors.

Parent topic: Planning an upgrade

Common upgrade tasks

Tasks such as purging system data, monitoring installations, and cleaning up after an upgrade are common to all Guardium upgrade scenarios.

- Purge system data
  Purging unnecessary data from the Guardium system can significantly speed up the upgrade process.
- Patch installation, distribution, and monitoring
  Before you begin an upgrade, it is helpful to familiarize yourself with how to upload and install patches, monitor patch installations, and verify that installations are successful.
- Track installation progress with diag
  Use the `diag` command to access the upgrade log and track the progress of an upgrade.
- Verify and cleanup after the upgrade
  Verify that the upgrade completed successfully and perform post-upgrade maintenance.

Parent topic: Upgrading your Guardium System

Purge system data

Purging unnecessary data from the Guardium system can significantly speed up the upgrade process.

About this task

For best performance and to minimize risks associated with upgrading large amounts of data, try to achieve less than 20% internal database utilization by purging unnecessary system data.

Procedure

1. Open Manage > Data Management > Data Archive.
2. Click the Purge check box to define a purge operation.
   Important: Changes made to the Data Archive purge configuration will also be applied to the Data Export purge configuration.
3. Define a Purge data older than time period. All data older than the specified period of days, weeks, or months will be purged from the system.
4. Click the Allow purge without archiving or exporting check box.
5. Click Save to save the configuration changes.
6. Click Run Once Now to execute the purge operation and purge old system data.

What to do next

Open Manage > Reports > Activity Monitoring > Scheduled Jobs to monitor the status of the data archive job.
Parent topic: Common upgrade tasks

Patch installation, distribution, and monitoring

Before you begin an upgrade, it is helpful to familiarize yourself with how to upload and install patches, monitor patch installations, and verify that installations are successful.

Install a patch using scp

When upgrading your Guardium environment, there are several ways to upload and install patches on central managers and managed units.

Important: Patches downloaded in ZIP format must be unzipped outside the Guardium system before uploading and installing. Observe the following restrictions for any patch with database structure changes:

- Perform or schedule the patch installation during quiet time on the Guardium system to avoid conflicts with long-running processes such as heavy reports, audit processes, backups, and imports.
- The exact time required for patch installation depends on database utilization, data distribution, and other considerations.
- Install patches in a top-down manner, first patching a central manager before patching aggregators and finally collectors.

To upload and install a patch using `scp`, issue the following CLI command: `store system patch install scp`

When the upload completes, you are automatically prompted to continue with the patch installation.

Install a patch using fileserver

To upload and install a patch using the Guardium fileserver:

1. Initialize the fileserver using the following CLI command: `fileserver [ip_address]` where `[ip_address]` is the system being used to connect to the Guardium system.
2. From a web browser, connect to the Guardium system.
    a. Click Upload Patch.
    b. Browse to select the patch file and then click Upload.
3. Issue the following CLI command to install the patch: `store system patch install system`.

Distribute a patch

To distribute a patch from a central manager to managed units, one of the following must have taken place:

- The patch is installed on the central manager
- The patch has been made available on the central manager by running the following CLI command: `store system patch available`

Distribute the patch to managed units using the Central Management page on the central manager. Navigate to Manage > Central Management > Central Management and click Patch Distribution.

Monitor and verify patch installation

You can monitor and verify the installation of patches in the following ways:

- Issue the following CLI command: `show system patch install`.
- Use the Central Management page on the CM: Manage > Central Management > Central Management > Patch Installation Status.

Important: V9 patches will not available after the Guardium system is upgraded to V10.
Parent topic: Common upgrade tasks

Track installation progress with diag

Use the `diag` command to access the upgrade log and track the progress of an upgrade.

Procedure

1. Log in to the Guardium system CLI.
2. Issue the `diag` command.
3. From the `diag` command menu:
    a. Select 1 Output management and click OK.
    b. Select 3 Export recorded files and click OK.
    c. Choose the log files you need and click OK.
    d. Select 1 FTP or 2 SCP and click OK.
    e. Input the host name that you want to upload to and click OK.
    f. Input the user name and click OK.
    g. Input the password and click OK.
    Note: If 2 SCP is chosen, the destination path is asked for before the password.
    h. Input the destination path and click OK.
    i. Check the information and click OK. The file uploads to the target system.
    j. Select OK to exit.
    k. Select 3 Exit and click OK.
    Note: Return to **3a** if you need to upload another file; otherwise, proceed to the next step.
    l. Select 5 Exit to CLI and click OK.

Parent topic: Common upgrade tasks

Verify and cleanup after the upgrade

Verify that the upgrade completed successfully and perform post-upgrade maintenance.

Procedure

1. If you upgraded using an upgrade patch, log in as the CLI user and issue the following command: `show upgrade-status`. The command will output detailed status information from the upgrade process, and the last line of output should indicate `INFO:Migration Complete`.
2. If you upgraded a central manager, verify that managed units are listed on the Manage > Central Management > Central Management page.
3. Verify that custom reports created in previous versions of Guardium are available at Reports > My Custom Reports.

    My Custom Reports should contain any new reports that you created as well as any predefined reports that you modified in a previous version of Guardium.

4. Refresh all managed units on the Central Management page so you can distribute the licenses down to the upgraded MUs.
5. You may need to update the Guardium DPS file after upgrade or restore procedures. Download the latest DPS file, then use the Harden > Vulnerability Assessment > Customer Uploads tool to upload and import the new DPS file.
6. Company logos uploaded before upgrade or restore procedures may need to be reloaded. To reload a customer logo, follow these steps:
    a. Log in as an admin user.
    b. Navigate to Setup > Tools and Views > Global Profile.
    c. Browse for the company logo file.
    d. Upload the logo file.

7. Verify the status of the Cross-Site Request Forgery (CSRF) and Cross-Site Scripting (XSS) services using the CLI commands show gui csrf_status and show gui xss_status.

Parent topic: Common upgrade tasks

Upgrading a 32-bit environment

Upgrade your 32-bit Guardium environment without using a backup central manager.

Before upgrading your 32-bit Guardium environment via the ISO without using a backup central manager, review the following checklist and complete each item before attempting the upgrade.

Important: Before performing `restore db` on a V10 system, apply the latest maintenance patches after your system has been built to V10. If you are using a 32-bit collector-based central manager, you must rebuild it to a 64-bit collector-based central manager before upgrading to V10.

Upgrade checklist

- Download latest health check patch (p9997) from Fix Central. For more information, see: Guardium health check patch release notes.
- Current systems must be at Guardium V9 and have 32-bit architecture.
- Download the latest Guardium V9 release or get it later from Fix Central [optional].
- Download the latest Guardium V10 ISO from Passport Advantage
- Download all base and append licenses from Passport Advantage
- Download the latest V10 GPU from Fix Central, if one is available
- Record all network configuration parameters returned by the following Guardium CLI commands:

```
show network interface all
show network route defaultroute
show network resolver 1
show system hostname
show system domain
```

1. Upgrading a 32-bit central manager
   When upgrading your 32-bit Guardium environment, follow these steps to run the health check patch and upgrade a central manager using a backup, rebuild, and restore procedure.
2. Upgrade 32-bit managed units
   Upgrade 32-bit managed units using a backup, rebuild, and restore procedure.

Parent topic: Upgrading your Guardium System
Related concepts:
Planning an upgrade

Upgrading a 32-bit central manager

When upgrading your 32-bit Guardium environment, follow these steps to run the health check patch and upgrade a central manager using a backup, rebuild, and restore procedure.

Before you begin

Complete the upgrade checklist in Upgrading a 32-bit environment.

Procedure

1. Upgrade the system to V9 patch 600 or later.
2. Set the time to the local time zone and synchronize time across all Guardium systems using an NTP server.
3. Download and install the latest health check patch (p9997) and verify that the installation was successful. See Patch installation, distribution, and monitoring for instructions.
4. Take a system backup of the central manager and verify that it was successful.
   a. Navigate to Manage > Data Management > System Backup.
   b. Configure the protocol based on your preferences and fill in all fields.
   c. Back up both configuration and data.
   Important: Create at least one valid backup before beginning the upgrade procedure.
5. Mount the latest Guardium V10 ISO.
   a. Select a system type within the first five seconds of entering the Guardium installer. The default selection is Standard Installation (non CM) with a unit type of standalone collector. When upgrading a central manager or an aggregator, select Aggregator.
   b. Allow the installation to complete and the system to reboot.
6. Configure network parameters. Log into the Guardium CLI and issue the following commands:

```
store network interface ip
store network route defaultroute
store network resolver 1
store system hostname
store system domain
```

7. Log into the Guardium user interface and validate the default components.
   Note: If logging in for the first time, the default password is `guardium`.
   a. Verify that only the Welcome and Setup navigation items are visible.
   b. Navigate to Setup > Tools and Views > License or click the  icon to verify that no licenses are installed on the system.
8. Install licenses.
   a. Navigate to the license page by following the notification link or selecting Setup > Tools and Views > License.
   b. Apply all relevant base and append licenses, and accept the license agreements.

c. If necessary, change the system unit type by logging into the CLI and issuing the following CLI command: `store unit type <type>` where `<type>` is `manager`, `standalone`, `netinsp`, `mainframe`, `sink`, or `stap`.

9. Install the latest V10 GPU (if newer than the latest V10 ISO) and the latest maintenance patches on the central manager, and verify that they have installed successfully.
10. Restore data and configurations on the central manager.
    a. Issue the following Guardium CLI command to import the backup files: `import file`.
    b. Import the data and configuration files separately.
    c. Perform the data and configuration restore by issuing the following CLI command: `restore db-from-prev-version`.

    Tip: The restore db log can be accessed by running the `diag` CLI command. See Track installation progress with diag for more information.
11. After restoring data and configurations to the central manager, verify that all relevant managed units information is displayed on the Central Management page.
12. Validate that the managed environment is functioning as expected.
    a. Verify that custom reports were restored
    b. Verify that managed units appear online and are accessible from the Central Management page

    Attention: Be aware of expected limitations when operating in a mixed environment. For more information, see Mixed-version environments during an upgrade.

What to do next

After successfully upgrading your 32-bit Guardium central manager, Upgrade 32-bit managed units.
Parent topic: Upgrading a 32-bit environment
Next topic: Upgrade 32-bit managed units

Upgrade 32-bit managed units

Upgrade 32-bit managed units using a backup, rebuild, and restore procedure.

Before you begin

Before upgrading 32-bit managed units, review and complete the following tasks:

- Upgrading a 32-bit environment
- Upgrading a 32-bit central manager

Important: You must upgrade your environment to V9 patch 600 or later before upgrading to the latest V10.

Procedure

1. Distribute the latest health check patch (p9997) to managed units and verify that it installed successfully. See Patch installation, distribution, and monitoring for more information.
2. Take system backups of all managed units.
3. Rebuild the managed units using the following procedure:
    a. Mount the latest Guardium V10 ISO image.
    b. Select a system type within five seconds of entering the Guardium installer. Use the default selection of Standard Installation (non CM) with a unit type of standalone collector, or allow for an automatic boot.
    c. Allow the installation to complete and the system to reboot.
4. Configure network parameters. Log into the Guardium CLI and issue the following commands:

```
store network interface ip
store network route defaultroute
store network resolver 1
store system hostname
store system domain
```

5. Log into the Guardium user interface and verify that no licenses are installed on the system.
    Tip:
    - If logging in for the first time, the default password is `guardium`.
    - If you are working with a standalone system that will eventually become a managed unit, there is no need to install licenses.

    a. On the main Guardium navigation, verify that only the Welcome and Setup navigation items are available.
    b. Navigate to Setup > Tools and Views > License or click the  icon to verify that no licenses are installed on the system.
6. Restore data and configuration on the managed units.
    Note: When restoring a managed unit from a backup, any custom layouts for that managed unit will be lost if the central manager is down at the time of the restore.
    a. Issue the following Guardium CLI command to import the backup files: `import file`.
    b. Import the data and configuration files separately.
    c. Perform the data and configuration restore by issuing the following CLI command: `restore db-from-prev-version`.
7. Once all managed units have been successfully upgraded, distribute licenses from the central manager to the managed units.
    a. Log into the user interface of the central manager.
    b. Navigate to Central Management > Manage > Central Management and verify that the managed units are listed.
    c. Click the Select all check box to select all managed units.
    d. Click the Refresh button to distribute licenses to the managed units.
    e. Wait until the refresh process completes.
    f. Log into the user interface of the managed units and navigate to Setup > Tools and Views > License to verify that the correct licenses have been installed. When the correct licenses have been installed:
        - The expected navigation menu options will now be available on the managed units.
        - Reports on the managed units will be functional.
        - Reports will be accessible via remote data sources from the central manager.
8. If the latest Guardium V10 GPU (if newer than the latest V10 ISO) and maintenance patches were installed on the central manager, distribute the GPU and maintenance patches to the managed units.
9. If you use VMware Tools, you must reinstall them after completing the upgrade. To reinstall VMware Tools, log into the Guardium CLI, issue the following command, and follow the prompts: `setup vmware_tools install`.

Results

You have successfully completed an upgrade of your 32-bit Guardium environment to the latest V10. Please verify the stability of your Guardium environment.
Parent topic: Upgrading a 32-bit environment
Previous topic: Upgrading a 32-bit central manager

Upgrading a 64-bit environment

Upgrading your 64-bit Guardium environment without using a backup central manager.

Before upgrading your 64-bit Guardium environment via the ISO without using a backup central manager, you review the following checklist below and complete each item before attempting the upgrade.

Important: Before performing `restore db` on a V10 system, apply the latest maintenance patches after your system has been built to V10. If you are using a 64-bit collector-based central manager, the upgrade patch will handle the upgrade and convert the system from a collector-based central manager to an aggregator-based central manager.

Upgrade checklist

- Current systems must be at V9 patch 600 or above and have 64-bit architecture
- Download the latest Guardium V9 release or get it later from Fix Central [optional].
- Download upgrade patch p10000
- Download the latest maintenance patches from Fix Central
- Download latest health check patch (p9997) from Fix Central. For more information, see: Guardium health check patch release notes.

For contingency planning, download the following:

- All required base and append licenses.
- The latest V10 ISO from Passport Advantage.

1. Upgrading a 64-bit central manager
   When upgrading your 64-bit Guardium environment, follow these steps to run the health check patch and upgrade a central manager.
2. Upgrade 64-bit managed units
   Upgrade 64-bit managed units using an upgrade patch.

Parent topic: Upgrading your Guardium System
Related concepts:
Planning an upgrade

Upgrading a 64-bit central manager

When upgrading your 64-bit Guardium environment, follow these steps to run the health check patch and upgrade a central manager.

Before you begin

Complete the upgrade checklist in Upgrading a 64-bit environment.

Procedure

1. Upgrade the system to V9 patch 600 or later.
2. Set the time to the local time zone and synchronize time across all Guardium systems using an NTP server.
3. Download and install the latest health check patch (p9997) and verify that the installation was successful. See Patch installation, distribution, and monitoring for instructions.
4. Take a system backup of the central manager and verify that it was successful.
   a. Navigate to Manage > Data Management > System Backup.
   b. Configure the protocol based on your preferences and fill in all fields.
   c. Back up both configuration and data.
   Important: Create at least one valid backup before beginning the upgrade procedure.
5. Install p10000 on the central manager and monitor its installation.
   Important: After the patch installation completes, the upgrade process automatically begins and the system is rebooted. Do not reboot the system manually.
6. Allow the operating system installation to complete.
   - Installation time depends on the amount of data involved as well as system specifications and configuration
   - Once the operating system installation has completed, the system reboots into the latest Guardium V10 for the first time.
     Attention: After you successfully install the latest V10, the first boot into your system is followed by:
     - Network configuration, database data migration, database start up.
     - License upgrade, PSML upgrade, language setting.
     - Database restart, certificate and key migration, password migration, and file clean-up.
7. Confirm that the central manager has been successfully upgraded:
   a. Log in to the Guardium CLI. If the CLI enters recovery mode, the upgrade is still in progress.
   b. Issue the following CLI command: show upgrade-status The command can also be issued from the CLI recovery mode.
   c. Verify that the last line in the output reads: 5.0:INFO:Migration Complete
   d. If you are still in the CLI recovery mode, exit the CLI and log back in to enter the normal Guardium CLI mode.
   e. Issue the following CLI command:show system patch install
   f. Verify that p10000 status is the following:Phase 5: Migration completed
8. Log into the Guardium user interface and accept license agreements to enable product features.
   a. Navigate to Setup > Tools and Views > License.
   b. Accept the base license agreement.
   c. Accept all applicable append license agreements.
   Note: Skipping this step prevents Guardium features from being enabled.

9. Validate that the managed environment is functioning as expected by verifying that the managed units appear online and are accessible from the Central Management page.
   Attention: Be aware of expected limitations when operating in a mixed environment. For more information, see Mixed-version environments during an upgrade.
10. Install the latest maintenance patches on the central manager and verify that they have installed successfully.

What to do next

After successfully upgrading your 32-bit Guardium central manager, Upgrade 64-bit managed units.
Parent topic: Upgrading a 64-bit environment
Next topic: Upgrade 64-bit managed units

Upgrade 64-bit managed units

Upgrade 64-bit managed units using an upgrade patch.

Before you begin

Before upgrading 64-bit managed units using an upgrade patch, review and complete the following tasks:

- Upgrading a 64-bit environment
- Upgrading a 64-bit central manager

Important: You must upgrade your environment to V9 patch 600 or later before upgrading to the latest V10.

Procedure

1. Distribute the latest health check patch (p9997) to managed units and verify that it installed successfully. See Patch installation, distribution, and monitoring for more information.
2. Take system backups of all managed units.
3. Distribute the p10000 upgrade patch to all managed units and monitor the patch installation. Read Patch installation, distribution, and monitoring for more information.
   Attention: After the patch installation completes, the upgrade process automatically begins and the system is rebooted. Do not reboot the system manually.
   The time required for upgrade depends on the amount of data involved as well as system specifications and configuration. When the upgrade is complete and the system reboots, the first boot of the upgraded system is followed by:
   - Network configuration, database data migration, database start up.
   - License upgrade, PSML upgrade, language setting.
   - Database restart, certificate and key migration, password migration, and file clean-up.

   During this process, you will be unable to log in to upgraded managed units until the database migration completes.
4. Verify that the upgrade process has completed successfully on each managed unit.
   a. Log in to the Guardium CLI of the system being upgraded. If the CLI enters recovery mode, the upgrade is still in process.
   b. Issue the following CLI command: `show upgrade-status`. This command can also be issued from the CLI in recovery mode.
   c. Verify that the last line of output reads: `5.0:INFO:Migration Complete`.
   d. If you are in CLI recovery mode, exit the CLI and log back in to enter the CLI mode.
   e. Issue the following CLI command: `show system patch install`.
      Attention: `show system patch install` will not return results until the upgrade completes after the first reboot.
   f. Verify that the upgrade patch installation status read: `Phase 5: Migration completed`.
5. Once all managed units have been successfully upgraded, distribute licenses from the central manager to the managed units.
   a. Log into the user interface of the central manager.
   b. Navigate to Central Management > Manage > Central Management and verify that the managed units are listed.
   c. Click the Select all check box to select all managed units.
   d. Click the Refresh button to distribute licenses to the managed units.
   e. Wait until the refresh process completes.
   f. Log into the user interface of the managed units and navigate to Setup > Tools and Views > License to verify that the correct licenses have been installed.
      When the correct licenses have been installed:
      - The expected navigation menu options will now be available on the managed units.
      - Reports on the managed units will be functional.
      - Reports will be accessible via remote data sources from the central manager.
6. If the latest V10 GPU and maintenance patches were installed on the central manager, distribute the GPU and maintenance patches to the managed units.
7. If you use VMware Tools, you must reinstall them after completing the upgrade. To reinstall VMware Tools, log into the Guardium CLI, issue the following command, and follow the prompts: `setup vmware_tools install`.

Results

You have successfully completed an upgrade of your 64-bit Guardium environment to the latest V10. Please verify the stability of your Guardium environment.
Parent topic: Upgrading a 64-bit environment
Previous topic: Upgrading a 64-bit central manager

Upgrading a 32-bit environment with a backup central manager

Upgrade your 32-bit Guardium environment using a backup central manager.

Before upgrading your 32-bit Guardium environment using a backup central manager, review the following checklist and complete each item before attempting the upgrade.

Important: Before performing `restore db` on a V10 system, apply the latest maintenance patches after your system has been built to V10. If you are using a 32-bit collector-based central manager, you must rebuild it to a 64-bit collector-based central manager before upgrading to V10.

Upgrade checklist

- Identify and record all managed units defined in the current environment.
- Download latest health check patch (p9997) from Fix Central. For more information, see: Guardium health check patch release notes.
- Current systems must be at Guardium V9 and have 32-bit architecture.
- Download the latest Guardium V9 release or get it later from Fix Central [optional].
- Download the latest Guardium V10 ISO from Passport Advantage
- Download all base and append licenses from Passport Advantage
- Download the latest V10 GPU from Fix Central, if one is available
- Record all network configuration parameters returned by the following Guardium CLI commands:

```
show network interface all
show network route defaultroute
show network resolver 1
show system hostname
show system domain
```

1. Upgrading a 32-bit backup central manager
   When upgrading your 32-bit Guardium environment, follow these steps to run the health check patch and upgrade a backup central manager using a backup, rebuild, and restore procedure.
2. Upgrade old 32-bit primary central manager
   When working with a backup central manager, follow these procedures to upgrade your old 32-bit primary central manager using a backup, rebuild, and restore procedure.
3. Upgrade 32-bit managed units
   Upgrade 32-bit managed units using a backup, rebuild, and restore procedure.

Parent topic: Upgrading your Guardium System
Related concepts:
Planning an upgrade

Upgrading a 32-bit backup central manager

When upgrading your 32-bit Guardium environment, follow these steps to run the health check patch and upgrade a backup central manager using a backup, rebuild, and restore procedure.

Before you begin

Complete the upgrade checklist in Upgrading a 32-bit environment with a backup central manager.

Procedure

1. Upgrade the system to V9 patch 600 or later.
2. Set the time to the local time zone and synchronize time across all Guardium systems using an NTP server.
3. Download and install the latest health check patch (p9997) and verify that the installation was successful. See Patch installation, distribution, and monitoring for instructions.
   Important: You will need to install the latest health check patch (p9997) on both the primary central manager and backup central manager candidate before designating a backup central manager.
4. Define a backup central manager.
   a. Navigate to the Central Management page on the primary central manager.
   b. Select a managed aggregator.
   c. Verify that the primary central manager and the backup central manager candidate have the same patches installed.
   d. Designate the aggregator as a backup central manager.
   e. Verify that the cm_sync_file.tgz file has been created by checking the Aggregation/Archive Log on the primary central manager.
5. Take a system backup of the backup central manager and verify that it was successful.
   a. Navigate to Manage > Data Management > System Backup.
   b. Configure the protocol based on your preferences and fill in all fields.
   c. Be sure to backup both configuration and data.
   Important: Create at least one valid backup before beginning the upgrade procedure.
6. Rebuild the backup central manager using the latest V10 ISO.
   a. Mount the latest V10 ISO.
   b. Select a system type within the first five seconds of entering the Guardium installer. The default selection is Standard Installation (non CM) with a unit type of standalone collector.
7. Allow the installation to complete and the system to reboot.
8. Configure network parameters. Log into the Guardium CLI and issue the following commands:

```
store network interface ip
store network route defaultroute
store network resolver 1
store system hostname
store system domain
```

9. Log into the Guardium user interface and validate the default components.
   Note: If logging in for the first time, the default password is `guardium`.
   a. Verify that only the Welcome and Setup navigation items are visible.
   b. Navigate to Setup > Tools and Views > License or click the  icon to verify that no licenses are installed on the system.
10. Install the license.
    a. Navigate to the license page by either following the link in the notification or selecting Setup > Tools and Views > License.
    b. Apply all relevant base and append licenses, and accept the license agreements.
11. Install the latest V10 GPU (if newer than the latest V10 ISO) and the latest maintenance patches on the central manager, and verify that they have installed successfully.
12. Set the shared secret on the backup central manager by using either the CLI command `store system shared secret` or by navigating to Setup > Tools and Views > System.
13. Restore data and configurations on the central manager.

a. Issue the following Guardium CLI command to import the backup files: `import file`.
b. Import the data and configuration files separately.
c. Perform the data and configuration restore by issuing the following CLI command: `restore db-from-prev-version`.

Tip: The restore db log can be accessed by running the `diag` CLI command. See Track installation progress with diag for more information.

14. From the primary central manager, verify that the V10 backup central manager is available and online. Identify and record the number of managed units reporting to the primary central manager (this information is used after transitioning to the backup central manager).
    Important: The backup central manager (now running the latest Guardium V10) may show a red status light. This happens when the central manager sends a V9 signal to a V10 system and fails, and you can still promote the server as long as the backup central manager sync file is present on your backup central manager. Do not attempt a refresh.
15. Verify that the cm_sync_file.tgz file has completed at least two successful transfers from the primary central manager to the backup central manager by checking the Aggregation/Archive Log on the primary central manager. The transfers should occur at 30-minute intervals.
16. Make the backup central manager the primary central manager. You may encounter the following message after logging into the backup central manager:

    ```
    The central manager version is lower than the version of this managed unit. Functionality is limited until the version mismatch is corrected.
    ```

    a. Navigate to Setup > Central Management.
    b. Click Make Primary CM. If you do not see this option, verify that the cm_sync_file was transferred successfully.
    c. Answer Yes to the message: Are you sure you want to make this unit the primary CM?
    d. Click Close on the pop-up-message: The change will take a few minutes and would require a GUI restart. You will be logged off when the GUI restart is performed. The progress icon is displayed on the user interface page.

    Note: During the conversion process, the Guardium user interface is temporarily unavailable. After the process completes, the login screen returns to normal.
17. Transition the managed units to the new primary central manager. This might take some time to complete. Using an SSH client, connect to the new primary central manager to view the results log.
    a. Initialize the fileserver using the following command: `fileserver [ip_address] [duration]`
    b. From a web browser, connect to the new primary central manager.
    c. View the load_secondary_cm_sync_file.log file to see the progress. The file is located in the gim-snif-guard-logs directory.
    d. When you see the final line Import CM sync info done, the process has finished successfully.
    e. At this point, the user interface refreshes and you will see the login page.
    f. Wait until the top of the hour for the process to complete as the managed units begin transitioning to the new primary central manager.
18. Log into the Guardium user interface and complete the following steps:.
    a. Verify that managed units are now managed by the new primary central manager.
    b. Verify that all managed units have been transitioned except for the old primary central manager.

What to do next

After successfully upgrading your backup central manager and transitioning managed units, Upgrade old 32-bit primary central manager.
Parent topic: Upgrading a 32-bit environment with a backup central manager
Next topic: Upgrade old 32-bit primary central manager

Upgrade old 32-bit primary central manager

When working with a backup central manager, follow these procedures to upgrade your old 32-bit primary central manager using a backup, rebuild, and restore procedure.

Before you begin

Once your backup central manager has become your new primary central manager, you can upgrade your old primary central manager to the latest Guardium V10. Before upgrading your old primary central manager, review and complete the following tasks:

- Upgrading a 32-bit environment with a backup central manager
- Upgrading a 32-bit backup central manager

Procedure

1. Reconfigure the old primary central manager by issuing the following CLI command: `delete unit type manager`. Before continuing, verify that the old primary central manager is now a standalone aggregator.
2. Take a system backup from the old primary central manager. Include both data and configuration in the backup.
3. Rebuild the old primary central manager using the following procedure:
    a. Mount the latest Guardium V10 ISO image.
    b. Select a system type within five seconds of entering the Guardium installer. When working with an old primary central manager, select Aggregator.
    c. Allow the installation to complete and the system to reboot.
4. Configure network parameters. Log into the Guardium CLI and issue the following commands:

    ```
    store network interface ip
    store network route defaultroute
    store network resolver 1
    store system hostname
    store system domain
    ```

5. Log into the Guardium user interface and verify that no licenses are installed on the system.
    Tip:
    - If logging in for the first time, the default password is `guardium`.
    - If you are working with a standalone system that will eventually become a managed unit, there is no need to install licenses.

    a. On the main Guardium navigation, verify that only the Welcome and Setup navigation items are available.
    b. Navigate to Setup > Tools and Views > License or click the  icon to verify that no licenses are installed on the system.
6. If the latest V10 GPU (if newer than the latest V10 ISO) and maintenance patches were installed on the old backup central manager prior to converting it to a primary central manager, install the same GPU and maintenance patches on the old primary central manager.
7. Restore data and configuration on the old primary central manager.
    a. Issue the following Guardium CLI command to import the backup files: `import file`.
    b. Import the data and configuration files separately.

c. Perform the data and configuration restore by issuing the following CLI command: `restore db-from-prev-version`.

8. Set the shared secret on the old primary central manager by navigating to Setup > Tools and Views > System.
9. Register the old primary central manager (the system you have just upgraded) to the new primary central manager.
10. Define a new backup central manager.
    a. Navigate to Manage > Central Management > Central Management on the new primary central manager.
    b. Select the old primary central manager.
    c. Designate the old primary central manager as the new backup central manager.
    d. Wait for at least one backup synchronization to complete. The first backup synchronization should take place within one hour.
    e. Verify that the cm_sync_file.tgz file has been created by checking the Aggregation/Arcive log on the new primary central manager.
11. Optionally revert to the original managed environment configuration by redefining the new backup central manager as the primary central manager.
    a. Answer `Yes` to the message: Are you sure you want to make this unit the primary CM?
    b. Click Close on the Information pop-up message. The progress icon is displayed on the user interface page.
    Attention: The user interface will be temporarily unavailable during the conversion process. When the process completes, the login screen will return to normal.
12. Transition the managed units to the new primary central manager. This process may take some time to complete. Using an SSH client, connect to the new primary central manager to view the results log.
    a. Initialize the fileserver using the following command: `fileserver [ip_address] [duration]`
    b. From a web browser, connect to the new primary central manager.
    c. View the load_secondary_cm_sync_file.log file to see the progress. The file is located in the gim-snif-guard-logs directory.
    d. When you see the final line Import CM sync info done, the process has finished successfully.
    e. At this point, the user interface refreshes and you will see the login page.
    f. Wait five minutes for the process to complete as the managed units begin transitioning to the new primary central manager.
13. Navigate to Manage > Central Management > Central Management and verify that all managed units are green and are now managed by the original primary central manager. The original backup central should not appear in the list of managed units unless it has been reconfigured as a backup central manager.

What to do next

Now that you have upgraded your central manager and backup central manager, Upgrade 32-bit managed units.
Parent topic: Upgrading a 32-bit environment with a backup central manager
Previous topic: Upgrading a 32-bit backup central manager
Next topic: Upgrade 32-bit managed units

Upgrade 32-bit managed units

Upgrade 32-bit managed units using a backup, rebuild, and restore procedure.

Before you begin

Before upgrading 32-bit managed units, review and complete the following tasks:

- Upgrading a 32-bit environment with a backup central manager
- Upgrading a 32-bit backup central manager
- Upgrade old 32-bit primary central manager

Important: You must upgrade your environment to V9 patch 600 or later before upgrading to the latest V10.

Procedure

1. Distribute the latest health check patch (p9997) to managed units and verify that it installed successfully. See Patch installation, distribution, and monitoring for more information.
2. Take system backups of all managed units.
3. Rebuild the managed units using the following procedure:
    a. Mount the latest Guardium V10 ISO image.
    b. Select a system type within five seconds of entering the Guardium installer. Use the default selection of Standard Installation (non CM) with a unit type of standalone collector, or allow for an automatic boot.
    c. Allow the installation to complete and the system to reboot.
4. Configure network parameters. Log into the Guardium CLI and issue the following commands:

```
store network interface ip
store network route defaultroute
store network resolver 1
store system hostname
store system domain
```

5. Log into the Guardium user interface and verify that no licenses are installed on the system.
    Tip:
    - If logging in for the first time, the default password is `guardium`.
    - If you are working with a standalone system that will eventually become a managed unit, there is no need to install licenses.

    a. On the main Guardium navigation, verify that only the Welcome and Setup navigation items are available.
    b. Navigate to Setup > Tools and Views > License or click the  icon to verify that no licenses are installed on the system.
6. Restore data and configuration on the managed units.
    Note: When restoring a managed unit from a backup, any custom layouts for that managed unit will be lost if the central manager is down at the time of the restore.
    a. Issue the following Guardium CLI command to import the backup files: `import file`.
    b. Import the data and configuration files separately.
    c. Perform the data and configuration restore by issuing the following CLI command: `restore db-from-prev-version`.
7. Once all managed units have been successfully upgraded, distribute licenses from the central manager to the managed units.
    a. Log into the user interface of the central manager.
    b. Navigate to Central Management > Manage > Central Management and verify that the managed units are listed.
    c. Click the Select all check box to select all managed units.
    d. Click the Refresh button to distribute licenses to the managed units.

e. Wait until the refresh process completes.
f. Log into the user interface of the managed units and navigate to Setup > Tools and Views > License to verify that the correct licenses have been installed. When the correct licenses have been installed:
   - The expected navigation menu options will now be available on the managed units.
   - Reports on the managed units will be functional.
   - Reports will be accessible via remote data sources from the central manager.

8. If the latest Guardium V10 GPU (if newer than the latest V10 ISO) and maintenance patches were installed on the central manager, distribute the GPU and maintenance patches to the managed units.
9. If you use VMware Tools, you must reinstall them after completing the upgrade. To reinstall VMware Tools, log into the Guardium CLI, issue the following command, and follow the prompts: `setup vmware_tools install`.

Results

You have successfully completed an upgrade of your 32-bit Guardium environment to the latest V10 using a backup central manager. Please verify the stability of your Guardium environment.

Parent topic: Upgrading a 32-bit environment with a backup central manager
Previous topic: Upgrade old 32-bit primary central manager

Upgrading a 64-bit environment with a backup central manager

Upgrading your 64-bit Guardium environment using a backup central manager.

Before upgrading your 64-bit Guardium environment using a backup central manager, review the following checklist and complete each item before attempting the upgrade.

Important: Before performing `restore db` on a V10 system, apply the latest maintenance patches after your system has been built to V10. If you are using a 64-bit collector-based central manager, the upgrade patch will handle the upgrade and convert the system from a collector-based central manager to an aggregator-based central manager.

Upgrade checklist

- Identify and record all managed units defined in the current environment.
- Current systems must be at V9 patch 600 or above and have 64-bit architecture
- Download the latest Guardium V9 release or get it later from Fix Central [optional].
- Download upgrade patch p10000
- Download the latest maintenance patches from Fix Central
- Download latest health check patch (p9997) from Fix Central. For more information, see: Guardium health check patch release notes.

1. Upgrading a 64-bit backup central manager
   When upgrading your 64-bit Guardium environment, follow these steps to run the health check patch and upgrade a backup central manager using a backup, rebuild, and restore procedure.
2. Upgrade old 64-bit primary central manager
   When working with a backup central manager, follow these procedures to upgrade your old 64-bit primary central manager using an upgrade patch.
3. Upgrade 64-bit managed units
   Upgrade 64-bit managed units using an upgrade patch.

Parent topic: Upgrading your Guardium System
Related concepts:
Planning an upgrade

Upgrading a 64-bit backup central manager

When upgrading your 64-bit Guardium environment, follow these steps to run the health check patch and upgrade a backup central manager using a backup, rebuild, and restore procedure.

Before you begin

Complete the upgrade checklist in Upgrading a 64-bit environment with a backup central manager.

Procedure

1. Upgrade the system to V9 patch 600 or later.
2. Set the time to the local time zone and synchronize time across all Guardium systems using an NTP server.
3. Download and install the latest health check patch (p9997) and verify that the installation was successful. See Patch installation, distribution, and monitoring for instructions.
   Important: You will need to install the latest health check patch (p9997) on both the primary central manager and backup central manager candidate before designating a backup central manager.
4. Define a backup central manager.
   a. Navigate to the Central Management page on the primary central manager.
   b. Select a managed aggregator.
   c. Verify that the primary central manager and the backup central manager candidate have the same patches installed.
   d. Designate the aggregator as a backup central manager.
   e. Verify that the cm_sync_file.tgz file has been created by checking the Aggregation/Archive Log on the primary central manager.
5. Take a system backup of the backup central manager and verify that it was successful.
   a. Navigate to Manage > Data Management > System Backup.
   b. Configure the protocol based on your preferences and fill in all fields.
   c. Be sure to backup both configuration and data.
   Important: Create at least one valid backup before beginning the upgrade procedure.
6. Install p10000 on the central manager and monitor its installation.

Important: After the patch installation completes, the upgrade process automatically begins and the system is rebooted. Do not reboot the system manually.

7. Allow the operating system installation to complete.
   - Installation time depends on the amount of data involved as well as system specifications and configuration
   - Once the operating system installation has completed, the system reboots into the latest Guardium V10 for the first time.
     Attention: After you successfully install the latest V10, the first boot into your system is followed by:
     - Network configuration, database data migration, database start up.
     - License upgrade, PSML upgrade, language setting.
     - Database restart, certificate and key migration, password migration, and file clean-up.
8. Confirm that the backup CM upgrade has completed successfully using the following steps
   a. Log in to the CLI.
   b. Issue the following CLI command: show upgrade-status
   c. Verify that the last line in the output reads: 5.0:INFO:Migration Complete
   d. Issue the following CLI command:show system patch install
   e. Verify that p10000 status is the following:Phase 5: Migration completed
9. Install the latest maintenance patches on the central manager and verify that they have installed successfully.
10. Verify that the primary central manager still sees the upgraded backup central manager.
    Important: The backup central manager (now running the latest Guardium V10) may show a red status light. This happens when the central manager sends a V9 signal to a V10 system and fails, and you can still promote the server as long as the backup central manager sync file is present on your backup central manager. Do not attempt a refresh.
11. Verify that the cm_sync_file.tgz file has completed at least two successful transfers from the primary central manager to the backup central manager by checking the Aggregation/Archive Log on the primary central manager. The transfers should occur at 30-minute intervals.
12. Make the backup central manager the primary central manager. You may encounter the following message after logging into the backup central manager:

    ```
    The central manager version is lower than the version of this managed unit. Functionality is limited until the version mismatch is corrected.
    ```

    a. Navigate to Setup > Central Management.
    b. Click Make Primary CM. If you do not see this option, verify that the cm_sync_file was transferred successfully.
    c. Answer Yes to the message: Are you sure you want to make this unit the primary CM?
    d. Click Close on the pop-up-message: The change will take a few minutes and would require a GUI restart. You will be logged off when the GUI restart is performed. The progress icon is displayed on the user interface page.

    Note: During the conversion process, the Guardium user interface is temporarily unavailable. After the process completes, the login screen returns to normal.
13. Transition the managed units to the new primary central manager. This might take some time to complete. Using an SSH client, connect to the new primary central manager to view the results log.
    a. Initialize the fileserver using the following command: `fileserver [ip_address] [duration]`
    b. From a web browser, connect to the new primary central manager.
    c. View the load_secondary_cm_sync_file.log file to see the progress. The file is located in the gim-snif-guard-logs directory.
    d. When you see the final line Import CM sync info done, the process has finished successfully.
    e. At this point, the user interface refreshes and you will see the login page.
    f. Wait until the top of the hour for the process to complete as the managed units begin transitioning to the new primary central manager.
14. Log into the Guardium user interface and accept license agreements to enable product features.
    a. Navigate to Setup > Tools and Views > License.
    b. Accept the base license agreement.
    c. Accept all applicable append license agreements.

    Note: Skipping this step prevents Guardium features from being enabled.
15. Navigate to the Central Management page and ensure that managed units are now managed by the new primary central manager. The old primary central manager should not appear in the list of managed units.

What to do next

After successfully upgrading your backup central manager and transitioning managed units, Upgrade old 64-bit primary central manager.
Parent topic: Upgrading a 64-bit environment with a backup central manager
Next topic: Upgrade old 64-bit primary central manager

Upgrade old 64-bit primary central manager

When working with a backup central manager, follow these procedures to upgrade your old 64-bit primary central manager using an upgrade patch.

Before you begin

Once your backup central manager has become your new primary central manager, you can migrate your old primary central manager to the latest Guardium V10. Before upgrading your old primary central manager, review and complete the following tasks:

- Upgrading a 64-bit environment with a backup central manager
- Upgrading a 64-bit backup central manager

Procedure

1. Reconfigure the old primary central manager by issuing the following CLI command: `delete unit type manager`. Before continuing, verify that the old primary central manager is now a standalone aggregator.
2. Take a system backup from the old primary central manager. Include both data and configuration in the backup.
3. Upgrade the old primary central manager using the p10000 upgrade patch and monitor the patch installation. Read Patch installation, distribution, and monitoring for more information.
   Attention: After the patch installation completes, the upgrade process automatically begins and the system is rebooted. Do not reboot the system manually.
   The time required for upgrade depends on the amount of data involved as well as system specifications and configuration. When the upgrade is complete and the system reboots, the first boot of the upgraded system is followed by:
   - Network configuration, database data migration, database start up.
   - License upgrade, PSML upgrade, language setting.
   - Database restart, certificate and key migration, password migration, and file clean-up.

   During this process, you will be unable to log in to upgraded managed units until the database migration completes.

4. Verify that the upgrade process has completed successfully on the old primary central manager.
    a. Log in to the Guardium CLI of the system being upgraded. If the CLI enters recovery mode, the upgrade is still in process.
    b. Issue the following CLI command: `show upgrade-status`. This command can also be issued from the CLI in recovery mode.
    c. Verify that the last line of output reads: `5.0:INFO:Migration Complete`.
    d. If you are in CLI recovery mode, exit the CLI and log back in to enter the CLI mode.
    e. Issue the following CLI command: `show system patch install`.
    Attention: `show system patch install` will not return results until the upgrade completes after the first reboot.
    f. Verify that the upgrade patch installation status read: `Phase 5: Migration completed`.
5. If the latest V10 GPU (if newer than the latest V10 ISO) and maintenance patches were installed on the old backup central manager prior to converting it to a primary central manager, install the same GPU and maintenance patches on the old primary central manager.
6. Set the shared secret on the old primary central manager by navigating to Setup > Tools and Views > System.
7. Register the old primary central manager (the system you have just upgraded) to the new primary central manager.
8. Define a new backup central manager.
    a. Navigate to Manage > Central Management > Central Management on the new primary central manager.
    b. Select the old primary central manager.
    c. Designate the old primary central manager as the new backup central manager.
    d. Wait for at least one backup synchronization to complete. The first backup synchronization should take place within one hour.
    e. Verify that the cm_sync_file.tgz file has been created by checking the Aggregation/Arcive log on the new primary central manager.
9. Optionally revert to the original managed environment configuration by redefining the new backup central manager as the primary central manager.
    a. Answer `Yes` to the message: Are you sure you want to make this unit the primary CM?
    b. Click Close on the Information pop-up message. The progress icon is displayed on the user interface page.
    Attention: The user interface will be temporarily unavailable during the conversion process. When the process completes, the login screen will return to normal.
10. Transition the managed units to the new primary central manager. This process may take some time to complete. Using an SSH client, connect to the new primary central manager to view the results log.
    a. Initialize the fileserver using the following command: `fileserver [ip_address] [duration]`
    b. From a web browser, connect to the new primary central manager.
    c. View the load_secondary_cm_sync_file.log file to see the progress. The file is located in the gim-snif-guard-logs directory.
    d. When you see the final line Import CM sync info done, the process has finished successfully.
    e. At this point, the user interface refreshes and you will see the login page.
    f. Wait five minutes for the process to complete as the managed units begin transitioning to the new primary central manager.
11. Navigate to Manage > Central Management > Central Management and verify that all managed units are green and are now managed by the original primary central manager. The original backup central should not appear in the list of managed units unless it has been reconfigured as a backup central manager.

What to do next

Now that you have upgraded your central manager and backup central manager, Upgrade 64-bit managed units.
Parent topic: Upgrading a 64-bit environment with a backup central manager
Previous topic: Upgrading a 64-bit backup central manager
Next topic: Upgrade 64-bit managed units

Upgrade 64-bit managed units

Upgrade 64-bit managed units using an upgrade patch.

Before you begin

Before upgrading 64-bit managed units using an upgrade patch, review and complete the following tasks:

- Upgrading a 64-bit environment with a backup central manager
- Upgrading a 64-bit backup central manager
- Upgrade old 64-bit primary central manager

Important: You must upgrade your environment to V9 patch 600 or later before upgrading to the latest V10.

Procedure

1. Distribute the latest health check patch (p9997) to managed units and verify that it installed successfully. See Patch installation, distribution, and monitoring for more information.
2. Take system backups of all managed units.
3. Transfer the p10000 upgrade patch to the central manager and make it available to the managed units.
    a. Transfer the upgrade patch to the central manager. Read Patch installation, distribution, and monitoring for more information.
    b. Make the upgrade patch available to the managed units by issuing the following CLI command from the central manager: `show system patch available`.
4. Distribute the p10000 upgrade patch to all managed units and monitor the patch installation. Read Patch installation, distribution, and monitoring for more information.
    Attention: After the patch installation completes, the upgrade process automatically begins and the system is rebooted. Do not reboot the system manually.
    The time required for upgrade depends on the amount of data involved as well as system specifications and configuration. When the upgrade is complete and the system reboots, the first boot of the upgraded system is followed by:
    - Network configuration, database data migration, database start up.
    - License upgrade, PSML upgrade, language setting.
    - Database restart, certificate and key migration, password migration, and file clean-up.

    During this process, you will be unable to log in to upgraded managed units until the database migration completes.
5. Verify that the upgrade process has completed successfully on each managed unit.
    a. Log in to the Guardium CLI of the system being upgraded. If the CLI enters recovery mode, the upgrade is still in process.
    b. Issue the following CLI command: `show upgrade-status`. This command can also be issued from the CLI in recovery mode.
    c. Verify that the last line of output reads: `5.0:INFO:Migration Complete`.
    d. If you are in CLI recovery mode, exit the CLI and log back in to enter the CLI mode.
    e. Issue the following CLI command: `show system patch install`.
    Attention: `show system patch install` will not return results until the upgrade completes after the first reboot.

f. Verify that the upgrade patch installation status read: `Phase 5: Migration completed`.

6. Once all managed units have been successfully upgraded, distribute licenses from the central manager to the managed units.
   a. Log into the user interface of the central manager.
   b. Navigate to Central Management > Manage > Central Management and verify that the managed units are listed.
   c. Click the Select all check box to select all managed units.
   d. Click the Refresh button to distribute licenses to the managed units.
   e. Wait until the refresh process completes.
   f. Log into the user interface of the managed units and navigate to Setup > Tools and Views > License to verify that the correct licenses have been installed. When the correct licenses have been installed:
      - The expected navigation menu options will now be available on the managed units.
      - Reports on the managed units will be functional.
      - Reports will be accessible via remote data sources from the central manager.
7. If the latest Guardium V10 GPU (if newer than the latest V10 ISO) and maintenance patches were installed on the central manager, distribute the GPU and maintenance patches to the managed units.
8. If you use VMware Tools, you must reinstall them after completing the upgrade. To reinstall VMware Tools, log into the Guardium CLI, issue the following command, and follow the prompts: `setup vmware_tools install`.

Results

You have successfully completed an upgrade of your 64-bit Guardium environment to the latest V10 using a backup central manager. Please verify the stability of your Guardium environment.

Parent topic: Upgrading a 64-bit environment with a backup central manager
Previous topic: Upgrade old 64-bit primary central manager

CLI and API

The Guardium® command line interface (CLI) is an administrative tool that allows for configuration, troubleshooting, and management of the Guardium system. The Guardium application programming interface (API) provides access to many Guardium functions from the command line.

- CLI Overview
  The Guardium command line interface (CLI) is an administrative tool that allows for configuration, troubleshooting, and management of the Guardium system.
- GuardAPI Reference
  GuardAPI provides access to Guardium functionality from the command line.

CLI Overview

The Guardium® command line interface (CLI) is an administrative tool that allows for configuration, troubleshooting, and management of the Guardium system.

Documentation Conventions

All CLI command examples are written in courier text (for example, show system clock).

To illustrate syntax rules, some command descriptions use dependency delimiters. Such delimiters indicate which command arguments are mandatory, and in what context. Each syntax description shows the dependencies between the command arguments by using special characters:

- The < and > symbols denote a required argument.
- The [and] symbols denote an optional argument.
- The | (vertical bar) symbol separates alternative choices when only one can be selected. For example:

```
store full-bypass <ON | OFF>
```

CLI Command Usage

- Commands and keywords can be abbreviated by entering enough characters so the commands are not ambiguous. For example, show can be abbreviated sho.
- Most Guardium CLI commands consist of a command word followed by one or more arguments. The argument may be a keyword or a keyword followed by a variable value (for example an IP address, subnet mask, date, etc.
- Commands and keywords are not case sensitive, but element names are.
- To display command syntax and usage options, enter a question mark (?) as an argument following the command word.
- Use quotation marks around words or phrases to precisely define search terms.

Accessing the CLI

An administrator can access the CLI though:

- A physically connected PC console or serial terminal OR
- A network connection using an SSH client

Physical Console Access

Interactive access to the Guardium appliance is through the serial port or the system console.

PC keyboard and monitor – A PC video monitor can be attached to either the front panel video connector or the video connector on the back of the appliance.

A PC keyboard with a PS/2 style connector can be attached to the PS/2 connector on the back of the appliance. Alternatively, a USB keyboard can be connected to the USB connectors located at the front or back of the appliance.

Serial port access – Using a NULL modem cable, connect a terminal or another computer to the 9-pin serial port at the back of the appliance. The terminal or a terminal emulator on the attached computer should be set to communicate as 19200-N-1 (19200 baud, no parity, 1 stop bit).

A login prompt displays once the terminal is connected to the serial port, or the keyboard and monitor are connected to the console. Enter cli as the user name, and continue with CLI Login.

Network SSH Access

Remote access to the CLI is available on the management IP address or domain name, using an SSH client. SSH clients are freely or commercially available for most desktop and server platforms. A Unix SSH connect command to log in as the cli user might look like this:

```
ssh -l cli 192.168.2.16
```

The SSH client may ask you to accept the cryptographic fingerprint of the Guardium appliance. Accept the fingerprint to proceed to the password prompt.

Note: If, after the first connection, you are asked again for a fingerprint, someone may be trying to induce you to log into the wrong machine.

CLI Login

Access to the CLI is either through the admin CLI account cli or one of the five CLI accounts (guardcli1,...,guardcli5). The five CLI accounts (guardcli1,...,guardcli5) exist to aid in the separation of administrative duties.

Access to the GuardAPI, which is a set of CLI commands to aid in the automation of repetitive tasks, requires the creation of a user (GUI username/guiuser) by access manager and giving those accounts either the admin or cli role. Proper login to the CLI for the purpose of using GuardAPI requires the login with one of the five CLI accounts (guardcli1,...,guardcli5) and an additional login with guiuser by issuing the 'set guiuser' command. See GuardAPI Reference Overview or Set guiuser Authentication for additional information.

Password Hardening

In order to meet various auditing and compliancy requirements the following password enforcements will be in effect for CLI accounts:

- For the account cli either use the cli password supplied or be sure to set a strong password to protect this account. If you have just rebuilt the system from an installation DVD, the Guardium cli user has a default password of guardium. You should change that password immediately.
- Enforcement of an expiration period for the CLI and five CLI accounts where the default is 90 days. When a password expires a required change of password will be invoked during the login process.
- Passwords must be a minimum of eight characters in length.
- Passwords must contain at least one character from three of the following four classes
  - Any upper-case letter
  - Any lower-case letter
  - Any numeric (0,1,2,...)
  - Any non-alphanumeric (special) character
- Once access is granted through the use of a separate GUI username (guiuser) the CLI audit trail will show the CLI_USER+GUI_USER pair used for login.
- CLI users cannot be authenticated through LDAP as these are considered administrative accounts and should be able to login regardless of connectivity to an LDAP server

Limited CLI commands during maintenance of internal database

CLI has three sets of commands - general commands, specialized support commands, and recovery commands. Support commands are to used by Technical Support to analyze the system. Recovery commands are to recover the system when the database is down.

The initial CLI login is:

```
Welcome to CLI - your last login was <date>
```

The welcome message will add further information if the internal database is down due to maintenance or during an upgrade.

If this is the case, the number of CLI commands available will be limited.

```
The internal database on the appliance is currently down and CLI will be working
in "recovery mode";  only a limited set of commands will be available.
```

The CLI commands that available for use during recovery mode are as follows:

```
support reset-password root
restart mysql
restart stopped_services
restart system
restore pre-patch-backup
restore system
```

- Aggregator CLI Commands
  This section list Aggregator CLI commands.
- Alerter CLI Commands
  This section list Alerter CLI commands.
- Certificate CLI Commands
  Use the certificate commands to create a certificate signing request (CSR), and to install server, CA (certificate authority), or trusted path certificates on the Guardium system.
- Configuration and Control CLI Commands
  Use the following CLI commands for configuration and control.
- diag CLI command
  Use these CLI command to access troubleshooting and maintenance utilities through diag.
- File Handling CLI Commands
  Use these commands to backup and restore system information. Many of these tasks can be performed from Guardium user interface.
- Inspection Engine CLI Commands
  Use these CLI commands to configure the inspection engines.
- Investigation Dashboard CLI Commands
  Use these CLI commands to configure the Investigation Dashboard .

- Network Configuration CLI Commands
  Use the network configuration CLI commands to set IP addresses, handle bonding/failover, handle secondary functionality, and reset networking.
- Support CLI Commands
  The following CLI commands are to be used only with the direction of Technical Support.
- System CLI Commands
  Use these CLI commands to configure system settings.
- User Account, Password and Authentication CLI Commands
  Use these CLI commands to configure user accounts, passwords and authentication.

Parent topic: CLI and API
Related information:
Advanced Guardium system management and configuration (video)

Aggregator CLI Commands

This section list Aggregator CLI commands.

aggregator backup keys file

Use this command to back up the shared secret keys file to the specified location.

Syntax

aggregator backup keys file <user@host:/path/filename>

Parameters

user@host:/path/filename For the file transfer operation, specifies a user, host, and full path name for the backup keys file. The user you specify must have the authority to write to the specified directory.

Note: For more information about the shared secret use, see System Shared Secret.

aggregator clean shared-secret

Sets the system shared secret value to null. All files archived or exported from a unit with a null shared secret can be restored or imported only on systems where the shared secret is null.

Syntax

aggregator clean shared-secret

Note: For more information about the shared secret use, see System Shared Secret.

aggregator debug

Starts or stops writing debugging information relating to aggregation activities. Use these commands only when directed to do so by Guardium® Support, and be sure to issue the stop command after you have gathered enough information.

Note: Debug mode will automatically expire after 7 days.

Syntax

aggregator debug <start | stop>

aggregator list failed imports

When an import operation fails because of a shared secret mismatch, the offending file is moved from the /var/importdir directory to the /var/dump directory, and it is renamed using the original file name plus the suffix .decrypt_failed. Use this command to list all such files

Syntax

aggregator list failed imports

aggregator recover failed import

Use this command to move and rename failed import files, prior to re-attempting an import or restore operation. Failed import files are stored in the /var/dump directory, with the suffix .decrypt_failed. Before re-attempting an import or restore operation, those files must be renamed (by removing the .decrypt_failed suffix) and moved to the /var/importdir directory.

Syntax

aggregator recover failed import <all | filename>

Parameters

Use the all option to move all files from the /var/dump directory ending with the suffix .decrypt_failed, or use the filename option to identify a single file to be moved.

Note: After moving the failed files, but before a restore or import operation runs, be sure that the system shared secret matches the shared secret used to encrypt the exported or archived file.

aggregator restore keys file

Use this command to restore the shared secret keys file from the specified location.

Syntax

aggregator restore keys file <user@host:/path/filename>

Parameters

user@host:/path/filename For the file transfer operation, specifies a user, host, and full path name for the backup keys file.

Note: For more information about the shared secret use, see System Shared Secret.

store aggregator drop_ad_hoc_audit_db

Audit Process reports on Aggregator – creates ad-hoc databases for each of its tasks that will include only the relevant days for that task. These ad-hoc databases can be kept for 14 days (for analysis) or deleted immediately after use. The CLI command defines the ad-hoc databases purging policy. Choices are 0 or 1(0 - keep for 14-days or 1 - delete after use).

Syntax

store aggregator drop_ad_hoc_audit_db [1|0]

Drop ad-hoc merge databases? 0

show aggregator drop_ad_hoc_audit_db

store aggregator orphan_cleanup_flag

Use this CLI command to regularly run static orphans cleanup on an aggregator.

Use this CLI command to clean orphans on aggregators that will be scheduled to run on data older then 3 days and will run at the end of a purge.

This process will be started by the user with this CLI command, so in case of large database, the user will be aware of the time length of the process.

It will cover the whole data on the aggregator, but will run it all on a separate temporary database.

Note: On a collector, orphans cleanup is not changed - it runs with the small cleanup tactics and is invoked before export/archive.

show aggregator orphan_cleanup_flag Displays small, large or analyze.

store aggregator orphan_cleanup_flag

store aggregator orphan_cleanup_flag <flag>, where flag is one of the words < small large analyze >

These commands are applicable on aggregator only.

If set to one of small, large or analyze - orphans cleanup script is invoked after each run of merge process.

The orphans cleanup on an aggregator does not remove orphan records of the last 3 days - it does remove all orphans older then 3 days.

If small is specified, the process does not interfere with audit processes that can start after the merge is completed.

If large is specified, the process would run faster where there is a large number of orphans but it's run might interfere with audit processes - if large is specified, audit processes will not start until orphans cleanup is complete.

If analyze is specified, the process first evaluates the number of orphans and uses the large tactics if there are more than 20% orphans - if analyze is specified, audit processes will not start until orphans cleanup is complete.

Syntax

store aggregator orphan_cleanup_flag [small | large | analyze]

Show command

show aggregator orphan_cleanup_flag

store archive_static_table

Use this CLI command to turn off/ turn on the archive static table

USAGE: store archive_static_table <state>,

where state is on/off.

Show command

show archive_static_table

store next_export_static

The aggregation software makes a distinction between two types of tables:

- static tables - grow slowly over time, data in these tables is not time dependent (GDM_OBJECT, GDM_FIELD, GDM_SENTENCE, GDM_CONSTRUCT, etc.).
- dynamic tables- grow quickly with time, data is time dependent (GDM_CONSTRUCT_INSTANCE, GDM_SESSION, GDM_CONSTRUCT_TEXT etc.).

As stated previously, the data of static tables is not time dependant. The data of dynamic tables that is time dependant is linked to static data. As static tables can grow to be very large, the export/archive process does not archive the full static data every day - it archives the full static data the first time it runs, and then at the first day of each month, on any day besides the first of the month, it only archives static data that changed during that day. For this reason when restoring data of any day, it is also required that the first of the month be restored - this ensures that full static data is present and references are not broken.

Use the CLI command, store next_export_static, to set a flag so that the next export contains the full static data.

Syntax

store next_export_static [ON | OFF]

Show command

show next_export_static

store last_used

Use this CLI command during purging and aggregation.

Syntax

store last_used [size | interval | logging]

Show command

show last_used [size | interval | logging]

LAST_USED SIZE - Integer, Default is 50

LAST_USED INTERVAL - Integer, default is 60 (minutes)

LAST_USED LOGGING - Integer

All Tables - 1

Only GDM_Object - 2

None - 0 (Default)

store aggregator static_data

store aggregator static_data [TIMESTAMP | LAST_USED_FOR_OBJECT_ONLY | LAST_USED]

Note: Set the CLI command, last_used logging, prior to using this command.

When the LAST_USED column is updated by the Sniffer in Static tables, this column can be referenced when purging data from these tables or when archiving and exporting data from these tables.

The value of this column can also be updated when importing data to an aggregator.

There are three options:

1. By default, the system behaves like it did in previous versions - the LAST_USED column is not considered in purge, archive and export and is not updated on import, archive and export are done by TIMESTAMP.
2. LAST_USED_FOR_OBJECT_ONLY is considered only for GDM_OBJECT table.
3. LAST_USED is considered for GDM_CONSTRUCT, GDM_SENTENCE, GDM_OBJECT, GDM_FIELD, GDM_JOIN, GDM_JOIN_OBJECT

Note: Options 2 and 3 are only enabled when the sniffer is configured to collect and update this data.
Note: Validations performed only on a collector - If ADMINCONSOLE_PARAMETER.LAST_USED_LOGGING=0, then only TIMESTAMP is allowed. If ADMINCONSOLE_PARAMETER.LAST_USED_LOGGING=1 then all parameters are allowed. If ADMINCONSOLE_PARAMETER.LAST_USED_LOGGING=2, then TIMESTAMP and LAST_USED_FOR_OBJECT_ONLY are allowed. On an aggregator, all parameters are allowed.

Syntax

store aggregator static_data <type>

where <type> is <TIMESTAMP | LAST_USED | LAST_USED_FOR_OBJECT_ONLY>depends on the last_used logging flag.

Use show/store last_used logging commands.

Show command

show aggregator static_data

store archive_table_by_date

Use the CLI command, store archive_table_by_date, only on Aggregators. Use this CLI command to archive all static tables on a daily basis or archive static tables data at the first time of running and every first day of the month. In default, archive data on an aggregator will run with full static tables on a daily basis. If this CLI command is set to ENABLE, static tables will be archived only on the first day of month or the first time archive data is running.

store run_cleanup_orphans_daily

Use this CLI command to clean all the old construct records that are no longer in use. This CLI command is relevant for collectors and aggregators and by default is enabled.

store run_cleanup_orphans_daily

USAGE: store run_cleanup_orphans_daily [on|off]

Show command

show run_cleanup_orphans_daily

store max_number_collector

Set the maximum number of collectors managed by aggregator. Default is 10.

Show command

show max_number_collector

store purge_age_period

Set the period of purge age.

Show command

show purge_age_period

Parent topic: CLI Overview

Alerter CLI Commands

This section list Alerter CLI commands.

The Alerter subsystem transmits messages that have been queued by other components - correlation alerts that have been queued by the Anomaly Detection subsystem, or run-time alerts that have been generated by security policies, for example. The Alerter subsystem can be configured to send messages to both SMTP and SNMP servers. Alerts can also be sent to syslog or custom alerting classes, but no special configuration is required for those two options, beyond starting the Alerter. There are four types of Alerter commands. Use the links in the lists, or browse the commands, which are listed in alphabetical sequence following the lists.

Alerter Start-up and Polling Commands

- stop alerter
- restart alerter
- store alerter state operational
- store alerter state startup
- store alerter poll
- store anomaly-detection poll
- store anomaly-detection state

SMTP Configuration Commands

- store alerter smtp authentication password
- store alerter smtp authentication type
- store alerter smtp authentication username
- store alerter smtp port
- store alerter smtp relay
- store alerter smtp returnaddr

SNMP Configuration Commands

- store alerter snmp community
- store alerter snmp traphost

restart alerter

Restarts the Alerter. You can perform the same function using the store alerter state operational command to stop and then start the alerter:

store alerter state operational off

store alerter state operational on

Syntax

restart alerter

stop alerter

Stops the Alerter.

You can perform the same function using the store alerter state operational command:

store alerter state operational off

Syntax

stop alerter

store alerter poll

Starts (on) or stops (off) the Alerter. The default state at installation time is off. You can also use the restart alerter or stop alerter commands to restart or stop the Alerter subsystem.

Syntax

store alerter state operational <on | off>

Show Command

show alerter state operational

store alerter state operational

Sets the number of seconds, n, that the Alerter waits before checking its outgoing message queue to send SNMP traps or transmit email using SMTP. The default is 30.

Syntax

store alerter poll <n>

Show Command

show alerter poll

store alerter state startup

Enables or disables the automatic start-up of the Alerter on system start-up. The default state at installation time is off.

Syntax

store alerter state startup <on | off>

Show Command

show alerter state startup

store anomaly-detection poll

Sets the Anomaly Detection polling interval, in minutes (n). This controls the frequency with which Guardium® checks log data for anomalies.

Syntax

store anomaly-detection poll <n>

Show Command

show anomaly-detection poll

store anomaly-detection state

Enables or disables the Anomaly Detection subsystem, which executes all active statistical alerts, checks the logs for anomalies, and queues alerts as necessary for the Alerter subsystem.

Syntax

store anomaly-detection state <on | off>

Show Command

show anomaly-detection state

store alerter smtp authentication password

Sets the alerter SMTP authentication password to the specified value. There is no corresponding show command.

Syntax

store alerter smtp authentication <value>

store alerter smtp authentication type

Sets the authentication type required by the SMTP server to the one of the following values:

none: Send without authentication.

auth: Username/password authentication. When used, set the user account and password using the following commands:

store alerter smtp authentication username

store alerter smtp authentication password

Syntax

store alerter smtp authentication type <none | auth>

Show Command

show alerter smtp authentication type

store alerter smtp authentication username

Sets the alerter SMTP email authentication username to the specified name.

Syntax

store alerter smtp authentication username <name>

Show Command

show alerter smtp authentication username

store alerter smtp port

Sets the port number on which the SMTP server listens, to the value specified by n. The default is 25 (the standard SMTP port).

Syntax

store alerter smtp port <n>

Show Command

show alerter smtp port

store alerter smtp relay

Sets the ip address of the SMTP server to be used by the Guardium appliance.

Syntax

store alerter smtp relay <ip address>

Show Command

show alerter smtp relay

store alerter smtp returnaddr

Sets the return email address for email alerts. Any bounced messages or email failures will be returned to this address.

Syntax

store alerter smtp returnaddr <email address>

Show Command

show alerter smtp returnaddr

store alerter snmp community

Sets the SNMP trap community used by the Alerter, to the name specified. There is no corresponding show command.

Syntax

store alerter snmp community <name>

store alerter smtp traphost

Sets the Alerter SNMP trap server to receive alerts, to the specified IP address or DNS host name.

Syntax

store alerter snmp traphost <snmp host>

Show Command

show alerter snmp traphost

store syslog-trap

Usage: store syslog-trap ON | OFF

Parent topic: CLI Overview

Certificate CLI Commands

Use the certificate commands to create a certificate signing request (CSR), and to install server, CA (certificate authority), or trusted path certificates on the Guardium® system.

Note: Guardium does not provide certificate authority (CA) services and does not ship systems with different certificates than the one installed by default. A customer that wants their own certificate must contact a third-party CA (such as VeriSign or Entrust).

Certification Expiration

Expired certificates will result in a loss of function. Run the show certificate warn_expire command periodically to check for expired certificates. The command displays certificates that will expire within six months and certificates that have already expired. The user interface will also inform you of certificates that will expire. To see a summary of all certificates, run the command show certificate summary.

New Certificates

To obtain a new certificate, generate a certificate signed request (CSR) and contact a third-party certificate authority (CA) such as VeriSign or Entrust. Guardium does not provide CA services and will not ship systems with different certificates than the ones that are installed by default. The certificate format must be in PEM and include BEGIN and END delimiters. The certificate can either be pasted from the console or imported through one of the standard import protocols.

Note: Do not perform this action until after the system network configuration parameters have been set.

create csr

Creates a Certificate Signed Request (CSR) for the Guardium system. Do not perform this action until after the system network configuration parameters are set. Within the generated CSR, the common name (CN) is created automatically from the host and domain names assigned.

create csr alias creates a certificate request with an alias.

create csr gim creates a certificate request for gim (GIM Listener).

create csr gui creates a certificate request for the tomcat.

create csr sniffer creates a certificate request for the sniffer.

Syntax

create csr <alias | gimi | gui | sniffer>

restore certificate gim

Restores the certificate gim to the last certificate gim on record or the default certificate gim that was originally provided.

restore certificate gim backup restores the gim certificate to the last saved sniffer gim certificate.

restore certificate gim default restores the gim certificate to the default gim certificate that was supplied with the system.

Syntax

restore certificate gim <backup | default>

restore certificate keystore

Restores the certificate keystore to the last certificate keystore on record or the default certificate keystore that was originally provided.

restore certificate keystore backup restores the certificate keystore to the last saved certificate keystore.

restore certificate keystore default restores the certificate keystore to the default value that was supplied with the system.

Syntax

restore certificate keystore <backup | default>

restore certificate mysql

Restores the client certificate to the last certificate on record.

restore certificate mysql backup restores the last saved mysql certificate.

Syntax

restore certificate mysql <backup>

restore certificate mysql backup client

Restores the client certificate to the last certificate on record.

restore certificate mysql backup client ca restores the last saved client certificate authority (CA) certificate.

restore certificate mysql backup client cert restores the last saved client certificate.

Syntax

restore certificate mysql backup client <ca | cert>

restore certificate mysql backup server

Restores the server certificate to the last certificate on record.

restore certificate mysql backup server ca restores the last saved server certificate authority (CA) certificate.

restore certificate mysql backup server cert restores the last saved server certificate.

Syntax

restore certificate mysql backup server <ca | cert>

restore certificate mysql default client

Restores the mysql client certificate to the default version that was supplied with the system.

restore certificate mysql default client ca restores the mysql client ca certificate to the default version that was supplied with the system.

restore certificate mysql default client cert restores the mysql client certificate to the default version that was supplied with the system.

Syntax

restore certificate mysql default client <ca | cert>

restore certificate mysql default server

Restores the mysql server certificate to the default version that was supplied with the system.

restore certificate mysql default server ca restores the mysql server ca certificate to the default version that was supplied with the system.

restore certificate mysql default server cert restores the mysql server certificate to the default version that was supplied with the system.

Syntax

restore certificate mysql default server <ca | cert>

restore certificate sniffer

Restores the certificate to the last certificate on record.

restore certificate sniffer backup restores the sniffer certificate to the last saved sniffer certificate.

restore certificate sniffer default restores the sniffer certificate to the default sniffer certificate.

Syntax

restore certificate sniffer <backup | default>

restore cert_key mysql backup

Restores the mysql client or server certificate key to the last saved value.

restore cert_key mysql backup client restores the last saved mysql client cert key.

restore cert_key mysql backup server restores the last saved mysql server cert key.

Syntax

restore cert_key mysql backup <client | server>

restore cert_key mysql default

Restores the mysql client or server certificate key to the default version that was supplied with the system.

restore cert_key mysql default client restores the default mysql client cert key that was supplied with the system.

restore cert_key mysql default server restores the default mysql server cert key that was supplied with the system.

Syntax

restore cert_key mysql default <client | server>

show certificate

Displays the summary of all certificates, certificate information, alias list, certificates in the keystore, and expired or soon-to-expire certificates.

This certificate authenticity can be verified by a Guardium CA public key (contained in the CA certificate that is distributed with the client software). This certificate has either a customer company-unique CN (Common Name - for example, acme.com, or a machine-specific CN (for example x4.acme.com). This permits any client to establish that not only does the Guardium system have a valid certification (it is a real Guardium system), but also that it is a specific Guardium system (or a set of Guardium systems) that the client is supposed to connect to.

show certificate all displays a summary of all certificates.

show certificate alias displays an alias list.

show certificate gim displays all GIM certificate information (GIM Listener).

show certificate gui displays all tomcat certificate information.

show certificate keystore displays all certificates in the keystore and an alias list for you to select which certificate to show.

show certificate mysql displays client and server mysql certificate information.

show certificate sniffer displays all sniffer certificate information.

show certificate stap displays all S-TAP certificate information in the keystore.

show certificate summary displays a summary of all certification information.

show certificate trusted displays all trusted certificate information.

show certificate warn_expired displays all expired certificates or certificates that expire in 6 months.

Syntax

show certificate <alias | all | gim | gui | keystore | mysql | sniffer | stap | summary | trusted | warn_expired >

show certificate keystore

Displays certificate information in the keystore.

show certificate keystore all displays all certificates in the keystore.

show certificate keystore alias displays an alias list for you to select which certificate to show.

Syntax

show certificate keystore <all | alias>

show certificate mysql

Displays mysql certificate information.

Parameters

show certificate mysql client shows client mysql information.

show certificate mysql server shows server mysql information.

Syntax

show certificate mysql <client | server>

store certificate

Stores a certificate. Paste your certificate in PEM format and include the BEGIN and END lines.

Parameter

store certificate alias stores a certificate in the keystore after a CSR has been generated. This CLI command supports the CLI command, create csr alias, which allows the user to create an intermediate trusted certificate from scratch. Use both of these commands to create intermediate trusted certificates. These intermediate trusted certificates can then be used to sign other certificates, if required.

store certificate gim will allow the custom gim certificate to be stored in keystore by prompting for certificate, key (optional) and CA certificate (GIM Listener).

store certificate gui stores the tomcat certificate in the keystore after a CSR has been generated.

store certificate keystore asks for a one-word alias to uniquely identify the trusted certificate and store it in the keystore.

store certificate mysql stores mysql client and server certificates.

store certificate sniffer stores sniffer certificates.

store certificate stap stores S-TAP certificates.

Syntax

store certificate <gim | gui | keystore | mysql | sniffer | stap >

store certificate mysql client

Stores a mysql client certificate.

store certificate mysql client ca stores client certificate authority (CA) certificates.

store certificate mysql client cert stores client certificates.

Syntax

store certificate mysql client <ca | cert>

store certificate mysql server

Stores a mysql server certificate.

store certificate mysql server ca stores server certificate authority (CA) certificates.

store certificate mysql server cert stores server certificates.

Syntax

store certificate mysql server <ca | cert>

store cert_key

Stores the system certificate key and the certificate key of a mysql client and server.

store cert_key mysql stores the certificate key of a mysql client and server.

store cert_key sniffer stores the sniffer certificate key.

Syntax

store cert_key <mysql | sniffer>

store cert_key mysql

Stores the certificate key of a mysql client or server.

store cert_key myself client stores the certificate key of a mysql client.

store cert_key myself server stores the certificate key of a mysql server.

Syntax

store cert_key mysql <client | server>

store cert_key sniffer

Stores the system certificate key. This command enables a user to set the system certificate that is used by the Guardium system (in communication with S-TAP®). The certificate can either be pasted from the console or imported via one of the standard import protocols. The certificate format should be PEM and should include the BEGIN and END delimiters. This certificate needs to be signed by a CA whose self-signed certificate is available to S-TAP software through the guardium_ca_path.

store cert_key sniffer console stores the sniffer certificate key by pasting the key into the console.

store cert_key sniffer import stores the sniffer certificate key by importing the key file.

Syntax

store cert_key sniffer <console | import>

Backup and Default Options

You can choose to restore certificates and certificate keys with the backup or default parameter. Use the backup parameter to restore a certificate to the last saved certificate. Use the default parameter to restore a certificate to the original certificate that Guardium supplied.

Certificate Expiration Dates and Summary Commands

Run the show certificate warn_expire command periodically. This command warns you of certificates that will expire in six months and displays a list of expired certificates. For more information, see the show certificate CLI command. To show a summary of all certificates, run the CLI command show certificate summary. Run the commands periodically to review certificate expiration dates.

Parent topic: CLI Overview

Configuration and Control CLI Commands

Use the following CLI commands for configuration and control.

? (question mark)

When entering a command, enter a question mark at any point to display the arguments.

Syntax

<partial_command> ?

Example

CLI> show account strike ?

USAGE: show account strike <arg>, where arg is:

?, count, interval, max

ok

CLI>

delete unit type

Use this command to clear one or more unit type attributes. Note that not all unit type attributes can be cleared using this command. See the table, located after the store unit type command, for more information.

Syntax

delete unit type [manager | standalone] [aggregated] [netinsp] [network routes static] [stap] [mainframe]

commands

Displays an alphabetical listing of all CLI commands.

Syntax

commands

debug

Enable/disable debug mode. Without an argument, it toggles the debug state. Optionally, a state argument can be passed.

Syntax

debug <on | off>

eject

This command dismounts and ejects the CD ROM, which is useful after upgrading or re-installing the system, or installing patches that were distributed via CD ROM.

Syntax

eject

delete scheduled-patch

To delete a patch install request, use the CLI command delete scheduled-patch

See the CLI command, store system patch install for further information on patch installation.

forward support email

When the support-state option is enabled (which it is by default), this command sets the email address to receive system alerts.

Syntax

forward support email to <email address>

Show Command

show support-email

iptraf

IPTraf is a network statistics utility distributed with the underlying operating system. It gathers a variety of information such as TCP connection packet and byte counts, interface statistics and activity indicators, TCP/UDP traffic breakdowns, and LAN station packet and byte counts. The IPTraf User Manual is available on the internet at the following location (it may be available at other locations if this link does not work):

http://iptraf.seul.org/2.7/manual.html

Syntax

iptraf

license check

Indicates if the installed license if valid. Use this command after installing a new product key.

Syntax

license check

ping

Sends ICMP ping packets to a remote host. This command is useful for checking network connectivity. The value of host can be an IP address or host name.

Syntax

ping <host>

quit

Exits the command line interface.

Syntax

quit

recover failed

Command to restore failed CSV/CEF/PDF transfer files, placing the files back into the export folder for another export attempt.

Syntax

recover failed [csv|cef|pdf]

register management

Registers the Guardium system for management by the specified Central Manager. The pre-registration configuration of this Guardium system is saved, and that configuration will be restored later if the unit is unregistered.

Syntax

register management <manager ip> <port>

Parameters

manager ip is the IP address of the Central Manager.

port is the port number used by the Central Manager (usually 8443).

restart gui

Restarts the IBM® Guardium® Web interface. To optionally schedule a restart of the GUI once a day or once a week, use additional parameters. HH is hours 01-24. MM is minutes 01-60. W is the day of the week, 0-6, Sunday is 0. If HHMM is listed twice, only the last entry is used. The parameter clear deletes the scheduled time.

In order to restart the Classifier and Security Assessments processes, run the restart gui command from the CLI (not from the GUI).

Running restart GUI from the GUI only restarts the web services. It is necessary to run the restart GUI command from the CLI to fully restart all processes, including Classifier and Security Assessments processes. It is necessary to run the restart GUI command from the CLI for each managed unit to restart the Classifier listener.

Syntax

restart gui [HHMM|HHMMW|clear]

restart stopped_services

Use this CLI command to restart services previously stopped with the store auto_stop_services_when_full CLI command.

Syntax

restart stopped_services

restart system

Reboots the Guardium system. The system will completely shut down and restart, which means that the cli session will be terminated.

Syntax

restart system

show buffer

This command displays a report of buffer use for the inspection engine process. If you are experiencing load problems, IBM Technical Support may ask you to run this command.

Syntax

show buffer <log | snif>

show buffer log

Use this CLI command to display the buffer usage of the inspection engine process.

show buffer snif

Use this CLI command to display the buffer usage of the sniffer.

show build

Displays build information for the installed software (build, release, snif version).

Syntax

show build

show defrag

Identify fragmented packets and attempt to reconstruct the packets before they get to the network sniffing process. The defrag is relevant only for network sniffing through SPAM or a TAP device.

Syntax

show defrag

Parameters

Packet size- The packet size in bytes, up to a maximum of 217 (131072)

Time interval - The time interval

Trigger level - The trigger level

Release level - The release level specified as a number of seconds, up to a maximum of the 31st power of two (2147483648).

show network routes static

Permit the user to have only one IP address per appliance (through eth0) and direct traffic through different routers using static routing tables. List the current static routes, with IDs.

Syntax

show network routes static

Delete command

delete network routes static

show password

This CLI command displays password functions. Password disable [0|1] removes the use of a password by storing the value 1. Password Expiration [CLI|GUI] [Number of days] displays the number of days between required password changes. Default is 90 days. Password Validation [ON|OFF] determines how strong the password is.

Syntax

show password disable [0|1]

show password expiration [CLI|GUI] 90

show password validation [ON|OFF]

show security policies

Displays the list of security policies.

Syntax

show security policies

show system patch available

Displays the already installed patches and patches scheduled to be installed--showing date/time and the install status.

Syntax

show system patch installed

show system patch installed

Displays the already installed patches and patches scheduled to be installed--showing date/time and the install status.

Syntax

show system patch installed

show system public key

Displays the public key for cli or tomcat. If none exists, this command creates one.

Note: See show system key, store system key in Certificate CLI commands.

Syntax

show system public key <cli | tomcat | grdapi>

stop gui

Stops the Web user interface.

Syntax

stop gui

stop system

Stops and powers down the appliance.

Syntax

stop system

store apply_user_hierarchy

Use this CLI command to apply user hierarchy to audit receiver.

If ON, the non-audit group receiver (the receiver other than the audit group receiver (normal or role) will only see audit results with a group IP beneath the receiver's hierarchy, including the receiver.

Syntax

store apply_user_hierarchy [ON | OFF]

Show command

show apply_user_hierarchy

store allow_simulation

Enables (on) or disables (off) the ability to run the Policy Simulation on the appliance.

In order to run the simulation, the original traffic must be replayed through the rules engine (with the policy needing to be tested). This requires some of the original SQL on the appliance to be saved with their values. The enable/disable of allow_simulation instructs IBM Guardium to save/NOT save any SQL or values whatsoever.

Syntax

store allow_simulation [on|off]

Show command

show allow_simulation

store alp_throttle

Use this CLI to regulate the amount of data that will be logged.

Usage: store alp_throttle <num>

where <num> is the number in range of -2147483647 and 2147483647.

Default is 0.

0 - do not log into GDM_FLAT_LOG and do not create tapks files

>0 - log into GDM_FLAT_LOG and do not create tapks files

<0 - log into GDM_FLAT_LOG and create tapks files

99999 - do not log into GDM_FLAT_LOG, but create tapks files.

Example

10 - log into GDM_FLAT_LOG 10% of statements.

10 - log into GDM_FLAT_LOG 10% of statements and create tapks files

store analyzer

Ignore session: The current request and the remainder of the session will be ignored. This action does log a policy violation, but it stops the logging of constructs and will not test for policy violations of any type for the remainder of the session. This action might be useful if, for example, the database includes a test region, and there is no need to apply policy rules against that region of the database.

This command sets the value of the timeout of the ignore session and sets the duration of the ignore session.

Syntax

store analyzer [ignore_sess_timeout | max_open_sess]

Show command

show analyzer

store auto_stop_services_when_full

When ON, will stop internal services if database exceeds the 90% full threshold.

Inspection Engine, Classification and other Collection-related services will stop. Also, Aggregation import/restore will not process any new files.

To remediate, use the various Support commands (support clean audit_task, support clean log_files, support clean DAM_data, support show large_files) to analyze and manually purge large tables.

Syntax

store auto_stop_services_when_full [ON | OFF]

Show command

show auto_stop_services_when_full

store connect oracle_parser

Use this command to connect and disconnect the Oracle parser from the DB2 parser. The default is OFF (disconnect).

Syntax

store connect oracle_parser [ON | OFF]

Usage: store connect_oracle_parser [state], where state is ON/OFF. ON is connect and OFF is disconnect.

Show command

show connect oracle_parser

store csv_fetch_size

CSV_FETCH_SIZE and CSV_MAX_SIZE are GLOBAL_PROFILE parameters that can only be modified via CLI

Guardium reports can be downloaded in CSV file format.

CSV_MAX_SIZE is used to control the size of the CSV download that are retrieved when clicking Download all records, from the report export menu.

CSV_FETCH_SIZE is used by report REST service to control total number of records.

Note: csv_max_size requires a restart of the GUI for changes to take effect. csv_fetch_size does not requires a restart of the GUI for changes to take effect.

Show command

CLI> show csv_fetch_size

Usage

CLI> store csv_fetch_size

USAGE: store csv_fetch_size <number>

where number is greater than 0

store csv_max_size

CSV_FETCH_SIZE and CSV_MAX_SIZE are GLOBAL_PROFILE parameters that can only be modified via CLI

Guardium reports can be downloaded in CSV file format.

CSV_MAX_SIZE is used to control the size of the CSV download that are retrieved when clicking Download all records, from the report export menu.

CSV_FETCH_SIZE is used by report REST service to control total number of records.

Note: csv_max_size requires a restart of the GUI for changes to take effect. csv_fetch_size does not requires a restart of the GUI for changes to take effect.

Show command

CLI> show csv_max_size

Usage

CLI> store csv_max_size

USAGE: store csv_max_size <number>

where number is greater than 0

store default_queue_size

Use this CLI command to control the configuration parameter ADMINCONSOLE_PARAMETER.DEFAULT_QUEUE_SIZE. The default is 25. The range is 25-300.

The sniffer must be restarted after a change in value.

Syntax

store default_queue_size <N>, where N is the number in range of 25 to 300

Show command

show default_queue_size 25

store defrag

Use this command to restore defragmentation defaults, or to set the defragmentation size. After entering this command, you must issue the restart inspection-core command for the changes to take effect. The defrag is relevant only for network sniffing through SPAM or a TAP device.

Syntax

store defrag [default | size <s> interval <i> trigger <t> release <r>]

Show command

show defrag

Parameters

default - Restore the default size.

s - The packet size in bytes, up to a maximum of 217 (131072)

i - The time interval

t -The trigger level

r - The release level specified as a number of seconds, up to a maximum of the 31st power of two (2147483648).

store delayed_firewall_correlation

Use this CLI command to hold a user connection until the decryption correlation has taken place.

Syntax

store delayed_firewall_collection [on | off]

Show command

show delayed_firewall_correlation

store full-bypass

This command is intended for emergency use only, when traffic is being unexpectedly blocked by the Guardium system. When on, all network traffic passes directly through the system, and is not seen by the Guardium system.

When using this command, you will be prompted for the admin user password.

Syntax

store full-bypass <on | off>

store gdm_analyzer_rule

Analyzer rules - Certain rules can be applied at the analyzer level. Examples of analyzer rules are: user-defined character sets, source program changes, and firewall watch or firewall unwatch modes. In previous releases, policies and rules were applied at the end of request processing on the logging state. In some cases, this meant a delay in decisions based on these rules. Rules applied at the analyzer level means decisions can be made at an earlier stage.

Note: When applying analyzer rules on source program changes, if the source program is not matching the exact pattern, add a .* at the end of the pattern to deal with the possibility that the source program has a trailing space (unseen by user).

Syntax

store gdm_analyzer_rule [active_flag | new]

store gdm_analyzer_rule active_flag

Usage: store gdm_analyzer_rule active_flag <id> <on|off>

where <id> is the rule ID.

Use the CLI command, show gdm_analyzer_rule, to see a list of GDM analyzer rules.

store gdm_analyzer_rule new

Enter rule description (optional):

Enter rule type (required):

Show command

show gdm_analyzer_rule

store gdm_analyzer_rule new

Use the Guardium CLI to add an analyzer rule for a direct regular expression to Mask UID Chain pattern.

CLI> store gdm_analyzer_rule new

Please enter rule description: new rule 4

Rule type:

1. Change source program

2. Set alternate character set

3. Send verdict

4. HADOOP exclude

5. Define protocol and port

6. Ignore session after packets

7. Set empty Oracle DB user when login information is missed

8. Force MS SQL login

9. Transform string

Please select rule type (required): 9

Please enter pattern (required, regex string): (.*)(-ppassword)(.*)

Please enter format (required, regex string): \\\\1-p****\\\\3

Do you want to activate the rule now? (Yes/No)

Y

ok

store gdm_http_session_template

Use this CLI command to set the template for the HTTP session.

Usage

```
store gdm_http_session_template [activate] [add] [deactivate] [remove]
```

Show command

```
show gdm_http_session_template
```

Attempting to retrieve the template information. It may take time. Please wait.

Table 1. store gdm_http_session_template

ID#	Active URL Regex	Session Regex	Username Regex	Login_Session Regex	Comment	Logout_Session_ID	Logout_URL_Regex
1	1	Cookie.*PHPSESSID=([[:a	.*user_name=([[:alnum:]	Set-Cookie:.*PHPSESSID=	example of HTTP session deleted		
2	1	Cookie.*PSJSESSIONID=([	.*SignOnDefault=([[:aln		example of HTTP session	cmd=logout	
3	1	Cookie.*JSESSIONID=([0-	.*username=([[:alnum:]]	Set-Cookie:.*JSESSIONID	example of HTTP session		Logout.jsp

store log external

Use this command to set file size, flush period, gdm error and state of the log external.

This rule will be displayed ONLY if the following CLI command is executed:

store log external state on

Then log external shows up as a policy action

CLI command to check the state:

show log external state

CLI command to enable and disable this action:

store log external state on/off

Usage

```
store log external [file_size] [flush_period] [gdm_error] [state]
```

Usage: store log external gdm_error <state>

where state is on/off. 'on' is to enable and 'off' is to disable.

Usage: store log external file_size <num>

where <num> is the size of the file.

Default is 4096 bytes.

Usage: store log external flush_period <num>

where <num> is the flush period.

Default is 60 seconds.

Usage: store log external state <state>

where state is on/off. 'on' is to enable and 'off' is to disable.

Show command

```
show log external [file_size] [flush_period] [gdm_error] [state]
```

store monitor gdm_statistics

Use this CLI command to get information about the Unit Utilization. Default is 1 (run the script every hour).

Syntax

```
CLI> store monitor gdm_statistics
USAGE: store monitor gdm_statistics <hour>, where hour is value from 0 to 24.
       Default value is 1, means to run the script every hour.
       Value 0, means not to run the script.
```

Show command

CLI> show monitor gdm_statistics

Disable gdm_statistics monitor

store gui

store gui [port | session_timeout | csrf_status]

Sets the TCP/IP port number on which the IBM Guardium appliance management interface accepts connections. The default is 8443. **n** must be a value in the range of 1024 to 65535. Be sure to avoid the use of any port that is required or in use for another purpose.

Set timeout of session - Sets the length of time (in seconds) with no activity before timeout. After the no-activity-timeout has been reached, it is necessary to log on again to IBM Guardium. The default length is 900 seconds (15-minutes).

Set Cross-site Report Forgery (CSRF) (ON | OFF) - See the section **CSRF and 403 Permission Errors** in the Getting Started with GUI help topic. The default value is enabled on an upgraded system. Trying to use certain web browser functions (for example, F5/CTRL-R/Refresh/Reload, Back/Forward) will result in a 403 Permission Error message.

The new session timeout value will take effect only after the next GUI restart.

Syntax

store gui port <n>

store gui session_timeout <n>

store gui csrf_status [on | off]

Show command

Displays the GUI port number, state, session timeout (in seconds) and/or CSRF status.

Syntax

show gui [port | state | all | session_timeout | csrf_status]

store gui cache

Use this CLI command to turn web browser caching ON or OFF (Enable or Disable).

The response is

The parameter has been changed.

Restarting gui

Changing to port 8443

Stopping.....

Safekeeping xregs

ok

The default setting for browser caching is enabled.

The act of changing the cache setting will automatically restart the Guardium web server.

For Firefox, in order for the setting to take affect, the cache on the respective browsers has to be cleared.

Syntax

store gui cache [ON | OFF]

Show command

show gui cache

store gui session_timeout

Sets the length of time (in seconds) with no activity before timeout. After the no activity timeout has been reached, it is necessary to log on again to IBM Guardium. The default length is 900 seconds (15-minutes).

Syntax

store gui session_timeout

Show command

show gui session_timeout

store gui csrf_status

Use this CLI command to enable or disable the Cross-site Request Forgery (CSRF) status.

Syntax

store gui scrf_status [on | off]

Show command

show gui scrf_status

store gui xss_status

Use this CLI command to enable or disable the Cross-Site Scripting (XSS) status. This option is enabled by default on upgraded systems.

Syntax

store gui xss_status [on | off]

Show command

show gui xss_status

store gui hsts_status

Use this CLI command to enable or disable the HSTS (HTTP Strict Transport Security Filter). This option is disabled by default on upgraded systems and is recommended to be turned on after valid certificates are installed. See the topic, How to install an appliance certificate to avoid a browser SSL certificate challenge, for further reference.

Syntax

store gui hsts_status [on | off]

Show command

show gui hsts_status

store installed security policy

Sets the security policy named **policy-name** as the installed security policy.

Syntax

store installed security policy <policy-name>

Show Command

show installed security policy

store keep_psmls

Use this CLI command to retain the current layouts/profiles/portlets created the users of the Guardium application. Set this CLI command to ON before an upgrade, and the psmls from the previous version will be retained.

Syntax

store keep_psmls [ON | OFF]

show keep_psmls

store ldap-mapping

Store LDAP mapping parameters - allow a custom mapping for the LDAP server schema. This command permits customized mapping to the LDAP server schema for email, firstname and lastname attributes. The paging parameter is used to facilitate transfer between any LDAP server type (Active Directory, Novell Directory, Open LDAP, Sun One Directory, Tivoli® Directory). If the paging parameter is set to on, but paging is not supported by the server, the search is performed without paging.

Example for paging. If the CLI command, **ldap-mapping paging** is set to ON, then Microsoft Active Directory will download the maximum number users defined under the limit value on the LDAP Import configuration screen. If CLI command, **ldap-mapping paging** is set to OFF, then Active Directory will download up to only 1000 users not matter what the limit value is set to. All other LDAP server configurations must use the CLI command, **ldap-mapping paging off** in order to download users up to the set limit value.

Note: Each time you change the CLI ldap-mapping attributes you also need to select Override Existing Changes on the LDAP Import configuration screen in IBM Guardium GUI before updating. This action must occur each time you change the CLI ldap-mapping email, firstname or lastname attributes and import LDAP users.

Show commands

show ldap-mapping [email] [firstname][lastname] <name>

show ldap-mapping paging ON|OFF

A GUI restart of the CLI is required for new parameters to take effect.

Examples

Some examples are shown.

store ldap-mapping firstname name

store ldap-mapping lastname sn

store ldap-mapping email mail

store ldap-mapping paging on

If the attributes are written as follows, the mapping process will use the first attribute it finds. If this is not what you want, use one of the examples to map to specific attributes.

Values for firstname attribute: gn,givenName,name

Values for lastname: attribute: sn,surname,name

Values for email attribute: userPrincipalName,mail,email,emailAddress,pkcs9email,rfc822Mailbox

Values for paging: on, off

store license

This command applies a new license key to the appliance.

A license key may be of one of two kinds: override type or append type; an override type replaces the currently installed license while the append type license will be appended to the currently installed license. Append-type licenses can only add functionality; new functions may be enabled and when relevant - expiration dates be updated, remaining number of scans and datasources will be increased, and a certain numeric fields in the license, such as number of managed units will be replaced.

Syntax

store license

Show Command

show license

Example

When using the store license command, you will be prompted to paste the new product key:

CLI> store license

Paste the string received from IBM Guardium and then press Enter.

Copy and paste the new product key at the cursor location, and then press Enter. The product key contains no line breaks or white space characters, and it always ends with (and includes) a trailing equal sign. A series of messages will display, ending with:

We recommend that the machine be rebooted at the earliest opportunity in order to complete the license updating process.

ok

CLI>

Run the restart gui command at this time.

store log classifier level

Sets the debugging level for the classifier, to one of the values shown.

Syntax

store log classifier level DEBUG|INFO|WARN|ERROR|FATAL

Show command

show log classifier level

store log sql parser_errors

Sets the logging of syntactically wrong SQL commands.

Syntax

store log sql parser_errors [on|off]

Note: A restart of the inspection engine is required after the store command is issued to apply change.

Show command

show log sql parser_errors

store log object_join_info

Sets the logging of object_join.

A join table is a way of implementing many-to-many relationships. Use join entity to join tables in a SELECT SQL statement.

Syntax

store log object_join_info [on | off]

Show command

show log object_join_info

store log session_info

Sniffer-related

Syntax

store log session_info [on | off]

Show command

show log session_info

store log exception sql

When **on**, logs the entire SQL command when logging exceptions.

Syntax

store log exception sql <on | off>

Show command

show log exception sql

store logging granularity

Sets the logging granularity to the specified number of minutes. You must use one of the minute values shown in the syntax. The default is 60.

Syntax

store logging granularity <1, 2, 5, 10, 15, 30 or 60>

Show command

show logging granularity

store max_audit_reporting

Displays the audit report threshold. The default is 32. When defining reports in Audit Process, the number of days of the report (defined by the FROM-TO fields) should not exceed a certain threshold (one month by default). See the Workflow Process, Central Management and Aggregation section of the Compliance Workflow Automation help topic for further information on this using this CLI command.

Syntax

store max_audit_reporting

Show command

show max_audit_reporting

store max_result_set_size

Store the max_result_set_size, default value is 100 (size is between 1 and 65535) and aids in tuning the inspection engine when observing returned data. This command sets the limitation for total result set size. This parameter works for any type of database. If the value is beyond the defined threshold, the analyzer will not retrieve data to calculate records affected value.

Syntax

store max_result_set_size <size>

Show command

show max_result_set_size

store max_result_set_packet_size

Store the max_result_set_packet_size, default value is 32 (size is between 1 and 65535) and aids in tuning the inspection engine when observing returned data. This command sets the limitation for packet size in response. This parameter works for any type of database. If the value is beyond the defined threshold, the analyzer will not retrieve data to calculate records affected value.

Syntax

store max_result_set_packet_size <size>

Show command

show max_result_set_packet_size

store max_tds_response_packets

Store the max_tds_response_packets, default value is 5 (size is between 1 and 65535) and aids in tuning the inspection engine when observing returned data. This command sets the limitation for number of packets in response. This parameter works for MS SQL only. If the value is beyond the defined threshold, the analyzer will not retrieve data to calculate records affected value.

Syntax

store max_tds_response_packets <size>

Note: max_tds_response_packets (Tabular Data Stream) is only applicable for MS SQL Server and Sybase.

Show command

show max_tds_response_packets

store maximum query duration

Sets the maximum number of seconds for a query to the value specified by **n**. The default is 180. We recommend that you **do not** set this value greater than the default, because doing so increases the chances of overloading the system with query processing. This value can also be set from the Running Status Monitor panel on the administrator portal.

Syntax

store maximum query duration <n>

Show Command

show maximum query duration

store monitor [buffer | custom_db_usage | gdm_statistics]

Use the CLI command, store monitor buffer to set the interval of how often the script must run that retrieves the information shown in the Buffer Usage Monitor report of the IBM Guardium Monitor tab.

Syntax: store monitor buffer

Use the CLI command, store monitor custom_db_usage to set the state to on and to specify a time to run this job.

Syntax

```
CLI> store monitor custom_db_usage
USAGE: store monitor custom_db_usage <state> <hour>
where state is on/off.
If state is on, specify the hour to run.
Valid value is number from 0 to 23
```

Use the CLI command, store monitor gdm_statistics to get information about the Unit Utilization. Default is 1 (run the script every hour).

Syntax

```
CLI> store monitor gdm_statistics
USAGE: store monitor gdm_statistics <hour>, where hour is value from 0 to 24.
       Default value is 1, means to run the script every hour.
       Value 0, means not to run the script.
```

Show Commands

show monitor buffer

show monitor custom_db_usage

show monitor gdm_statistics

store mysql_utf8mb4

Enable support for 4-byte UTF-8 encoding (utf8mb4).

This command modifies Guardium sniffer processes and internal databases to correctly capture and store 4-byte UTF-8 characters. Enabling utf8mb4 may be useful if datasources in your environment contain 4-byte characters, for example as used for Chinese, Japanese, and Korean ideographs.

Observe the following when using this command:

- The additional processing required to capture and store 4-byte characters will negatively impact the performance of your Guardium system. For this reason, do not enable utf8mb4 unless you require 4-byte character support in your environment.
- If support for 4-byte UTF-8 encoding is required in an aggregated or centrally managed environment, utf8mb4 should be enabled on all Guardium systems in the environment. Enabling utf8mb4 on only some systems in the environment may create problems, such as failed aggregation or incorrectly displayed reports.
- Data collected or aggregated before enabling utf8mb4 will still be available and function correctly after enabling utf8mb4.

CAUTION:
Once 4-byte UTF-8 support has been enabled using the store mysql_utf8mb4 command, the change cannot be undone or reversed. After enabling utf8mb on a Guardium system, the only way to remove support for 4-byte UTF-8 characters is to completely rebuild the system.

Syntax

store mysql_utf8mb4

Show Command

show mysql_utf8mb4

Example

```
> show mysql_utf8mb4
mysql configuration NOT set with UTF8MB4.
ok

> store mysql_utf8mb4
Attempting to change the mysql config file. It may take time. Please wait.
```

```
Start to modify mysql config file
Restarting mysql
Mysql has been restarted. Please exit CLI and log back on.
The parameter IS_UTF8MB4 has been changed to 1.

> show mysql_utf8mb4
mysql configuration set with UTF8MB4.
ok
```

store packet max-size

Limit the maximum size of packets from the sniffer.

Syntax

store packet max-size 1536

Show Command

show packet max-size

store pdf-config

Use this command to change the pdf font size and pdf orientation of the PDF image body content (excluding header/footer).

Size unit ranges from 1 (smallest) to 10 (largest) with default value of 6.

Orientation unit is 1 (for landscape orientation) or 2 (for portrait). The default value is 1.

The change takes effect immediately after typing the CLI command and pressing the Enter key.

Syntax

store pdf-config [orientation | size]

Show Command

show pdf-config [orientation | size]

store pdf-config multilanguage_support

There are different static pdf generator config files for English (Used on English version) and language C/J (Used on Chinese/Japanese). Use this CLI command to define the fonts in the PDF generator. Default is English. Multi-language is language C/J.

Syntax

```
CLI> store pdf-config multilanguage_support
Current setting is Default

1  Default
2  Multi-language
Please select the option (1,2, or q to quit)
```

Show command

show pdf-config multilanguage_support

store populate_from_query_maxrecs

Sets the maximum number of records that can be used to populate groups and aliases from a query.

Use caution when setting a maximum records value via this CLI command. Setting it too high may result in incomplete populate group from query processes. The maximum threshold is dynamic and dependent on the system load and memory utilization. This CLI command is limited to a high value of 200000.

Syntax

store populate_from_query_maxrecs 100000

Show command

show populate_from_query_maxrecs

store product gid

Sets the stored unique product <n> GID value.

Syntax

store product gid <n>

Show Command

show product gid

store purge object

Sets the age (in days) at which non-essential objects will be purged. Use the show purge objects age command to display a table showing the index, object name, and age for each object type for which a purge age is maintained. Then use the appropriate index from that table in the command to set the purge age.

Note: The value of number of days will be set to the default (90 days) when the unit type changes between managed unit/Manager/standalone unit.

Syntax

store purge object age <index> <days>

Show Command

show purge object age

Example

Assume you want to keep an Event Log for 30 days. First issue the show purge objects age command to determine the index (do not use the table; your list may be different). Then enter the store purge object command.

CLI>show purge objects age

Index Name, Age

1. Central Management Persistent Operations, 7
2. S-TAP Event Log, 14
4. Assessment Tests, 7
5. Central Management Temporary Policies, 7
6. S-TAP Change History, 14
7. Kerberos Authentication Information, 1
8. Comment History, 60
9. Comment Local History. 60
10. Call Graph History, 90

. . .

ok

CLI> **store purge object age 2 30**

ok

store quartz_thread_run

This CLI command is for use by Technical Support.

The Java™ Virtual Machine allows the application to have multiple threads. Thread is a piece of the program execution.

Use the store quartz_thread_num CLI command to set the number of threads that can run at the same time.

Use this command to ease conflict between too many threads running at the same time.

The show quartz_thread_num CLI command displays the number of Quartz scheduler threads that run at the same time.

Syntax

store quartz_thread_run <number>

USAGE: store quartz_thread_num <number>, where number is in range 3 to 15 with default value = 5.

Show command

show quartz_thread_num

org.quartz.threadPoll.threadCount= 5

store remotelog

Controls the use of remote logging. In addition to system messages, statistical alerts and policy rule violation messages can be written to syslog (optionally). For each **facility.priority** combination, messages can be directed to a specific host. This command can also control the use of remote logging through an optional port number and can designate a mandatory protocol (UDP or TCP). This command works with any syslog implementation that supports TCP.

If you enable remote logging, be sure that the receiving host has enabled this capability (see the note).

Syntax

store remotelog [help|add|clear] facility.priority host [optional port number:mandatory protocol (UDP or TCP)]

Table 2. Store remotelog parameters

Parameters	Description
help	Displays supported facilities and priorities.

Parameters	Description
add	Adds the specified facility.priority combination to the list of messages to be sent to the specified remote host.
clear	Clears the specified facility.priority combination from the list of messages being sent to the specified host.
facility	Use daemon. The majority of messages issued by the IBM Guardium appliance will be from the daemon facility.
priority	May be one of the following: alert, all, crit, debug, emerg, err, info, notice, warning. The standard IBM Guardium severity codes for alerts and violations map as follows: Guardium severity / Syslog priority INFO / info LOW / warning MED / err HIGH / alert
host	Identifies the host to receive this facility.priority combination.
optional port number	
mandatory protocol	UDP or TCP
format	store remotelog format Some SIEM products may process the IETF RFC 5424 style syslog messages better than the default. This command changes the format. If the format is changed 'restart rsyslog' must be run for this to take effect. USAGE: store remotelog format <default|rfc5424> default - rsyslog traditional format rfc5424 - rsyslog RFC 5424 format Note: syslog receiver must be configured to accept RFC5424 format. Otherwise, it would receive in the traditional format.

Note:

To configure the receiving system to accept remote logging, edit /etc/sysconfig/syslog on that system to include the -r option. For example:

```
SYSLOGD_OPTIONS=-r -m 0
```

Then restart the syslog daemon:

```
/etc/init.d/syslog  restart
```

The standard syslog file in Linux is named:

```
/var/log/messages
```

Common criteria requires that all communications from the Guardium system to a remote syslog server be encrypted. Communications to the remote syslog server can not be in clear text.

CLI commands

show remotelog

store remotelog ?

store remotelog add ?

store remotelog add encrypted

USAGE: store remotelog add encrypted <facility.priority> <host[:port]> <tcp|udp>

Possible facilities: all auth authpriv cron daemon ftp kern local0 local1 local2 local3 local4 local5 local6 local7 lpr mail mark news security syslog user uucp

Possible priorities: alert all crit debug emerg err info notice warning

Note:

If you want to send the encrypted remote log message to the server, the rsyslog configuration in the server needs to accept encrypted message.

Encrypted setting on client and server only works in TCP mode.

Switching from one mode to other on the same remote server: it needs to modify the configuration file to sync with the designated mode and the remote service needs to restart.

Example

```
store remotelog add non_encrypted
store remotelog clear
g32.guard.swg.usma.ibm.com> show remotelog
*.*    @9.70.148.175:10514
```

Use the example to store the certificate as ca.pem in /etc/pki/rsyslog/. This will open a new window and asks the user to paste the certificate.

```
store remote add encrypted all.all <IP address>:<port number> tcp
```

Encrypting syslog

Alerts and other messages can be forwarded to a remote syslog receiver, such as a SIEM system. This message traffic can be encrypted from the collector or aggregator to the remote syslog receiver.

Note: Encryption only works in TCP mode. By default, syslog forwarding uses UDP, so if encryption is required, specify TCP for the CLI command, store remotelog.

Before you begin:

The procedure documented here must be repeated on every collector or aggregator that is sending traffic to the encrypted host.

The certificate used by the remote syslog receiver is needed. Store that certificate on the Guardium system.

1. Have available the public certificate from the CA (Certificate Authority) from Verisign, Thwate, Geotrust, GoDaddy, Comodo, in-house, etc.
2. Log into the CLI on the individual Guardium system from which to send the encrypted syslog. Before executing the command, obtain the appropriate certificate (in PEM format) from the CA, and copy the certificate, including the Begin and End lines, to your clipboard.
3. Enter the following CLI command:store remotelog add encrypted daemon.all <IP address of encrypted remote host>:<port number of remote host> tcp
   Note: This example uses daemon because Guardium sends its application events using daemon.
4. The following instructions will be displayed:

   ```
   Please paste your CA certificate, in PEM format. Include the BEGIN and END lines, and then press CTRL-D.
   ```

   Paste the PEM-format certificate to the command line, then press **CRTL-D**. Guardium will take this input and store it as /etc/pki/rsyslog/ca.pem

   There will follow a message informing of the success or failure of the store operation.

   When successful, Guardium can send encrypted traffic to the remote system with the correct key.

5. Repeat the procedure for each collector and aggregator that is sending syslog traffic to the encrypted host.

store s2c

Sets several configurable parameters for ADMINCONSOLE. These parameters are used for throttling server-to-client (S2C) traffic.

Note: Use this CLI command only when directed by IBM Guardium Technical Services.

Minimum and maximum values:

ANALYZER_S2C_IGNORE = {0,1,2,3}

MAX_S2C_VELOCITY (K bytes/sec) - number >=0 and <= 2147483647

MAX_S2C_INTERVAL (sec) - number >=1 and <= 2147483647

See also the CLI command Store Throttle.

Syntax

store s2c

USAGE: store s2c ignore I maxrate M maxinterval T

where 0<=I<=3 (level), 0<=M<=2147483647 (K/sec), and 1<=T<=2147483647 (seconds) OR store throttle default

store s2c ignore 3 maxrate 300 maxinterval 5007

The new configuration will be effective once the CLI command, restart inspection-core, command is executed.

Show command

show s2c

Throttle S2C parameters (defaults):

Ignore: 0

Max rate: 999999

Max interval: 30

ANALYZER_S2C_IGNORE (0,1,2,3) - Switch s2c throttling mechanisms on/off based on scenarios. This flag is based on bits. 0 = the s2c throttling mechanism is OFF. 1 = turns on the function described in scenario 1, 2 = turns on the function described by scenario 2. 3 = turns both on.

MAX_S2C_VELOCITY - maximal rate (K bytes/sec). If this rate is exceeded, then analyzer should send CLI commands, ignore session, or ignore session reply, request to S-TAP® or sniffer.

MAX_S2C_INTERVAL - time interval in seconds (default 30 sec.) between possible CLI commands, ignore session, or ignore session reply, requests.

Scenario 1

The sniffer starts to receive traffic from S-TAP or network in the middle of large query. Since all incoming packets are DB server responses, no new session will be created by the analyzer and therefore no information will be sent to logger and rules engine. This type of traffic is useless for the sniffer. From the other side, this type of traffic can create additional S-TAP and sniffer load. A throttling mechanism helps to decrease S-TAP and network sniffer load by sending a ignore session message from the analyzer, if the S2C velocity is greater than MAX_S2C_VELOCITY. If for some reason S-TAP or network sniffer were not affected, then analyzer will send ignore session request again after MAX_S2C_INTERVAL seconds. In order to switch this throttling mechanism on, set ANALYZER_S2C_IGNORE flag to 1.

Scenario 2

If the incoming traffic has a high S2C rate (>MAX_S2C_VELOCITY), then a throttling mechanism sends a ignore session reply request to S-TAP for local database connections in the case when S2C velocity is greater than MAX_S2C_VELOCITY. If from some reason S-TAP was not affected, then analyzer will send ignore session reply request again after MAX_S2C_INTERVAL seconds. In order to switch this throttling mechanism on, set ANALYZER_S2C_IGNORE flag to 2.

store sender_encoding

Use this CLI command to encode outgoing messages (email and SNMP traps) in different encoding schemes, where previously everything is encoded in UTF8.

For example, a Guardium customer wanted to encode all of the outgoing SNMP messages in SJIS - an alternative Japanese encoding.

Note: If the conversion fails, for either reason (a) the encoding scheme specified is invalid, or (b) the characters to be encoded can not be represented in the requested encoding scheme, then the message will be sent using UTF8, which is the default encoding scheme.

Syntax

store sender_encoding <str>,

where str is the encoding with maximum length 16

Show command

show sender_encoding

store stap approval

Use this function to block unauthorized STAPs from connecting to the Guardium appliance.

If ON, then STAPs can not connect until they are specifically approved.

If an unapproved STAP connects, it is immediately disconnected until the specific authorization of the IP Address of that STAP.

There is a pre-defined report for approved clients, Approved TAP clients, it is available on the Daily Monitor tab.

Note:

A valid IP address is required, not the host name.

The CLI command, store stap approval, does not work within an environment where there is an IP load balancer.

Within a Central Managed environment, after adding the IPs to approved STAPs, there is a wait time associated with synchronization that might take up to an hour. After synchronization is complete the approved STAPs status will appear green in GUI.

Syntax

store stap approval ON | OFF

Show command

show stap approval

GuardAPI command

grdapi store_stap_approval

The new configuration will be effective after running the CLI command, restart inspection-core.

store stap certificate

Stores a certificate from the S-TAP host (usually a database server), on the IBM Guardium appliance. This command functions exactly like the store certificate console command, described later.

Syntax

store stap certificate

You will be prompted as follows:

Please paste your new server certificate, in PEM format.

Include the BEGIN and END lines, then press CTRL-D.

If you have not done so already, copy the server certificate to your clipboard. Paste the PEM-format certificate to the command line, then press CRTL-D. You will be informed of the success or failure of the store operation.

When you are done, use the **restart gui** command to restart the IBM Guardium GUI.

store stap network_latency

S-TAP verification is a feature by which customers can verify if a S-TAP is monitoring database traffic or not. The verification feature is affected by the customer's network traffic/latency. Since latency is different for each customer, there is a need for a way to list and change the default value that the verification feature uses.

Syntax

store stap network_latency

USAGE: store stap network_latency <N>

where N is the number greater than 0 seconds.

The default value is 5 seconds.

If the number goes higher the S-TAP verification process will become slower.

Show command

show stap network_latency

store set_partitions_for_queries

Use this CLI command to enable/disable partition selection on queries.

Usage:

store set_partitions_for_queries <on|off>

store storage-system

store storage-system

Adds or deletes a storage system type for archiving or system backup.

Syntax

store storage-system <Centera | TSM> <backup | archive> <on | off>

Show Command

show storage-system

Example

Assume you are currently using Centera for system backups, but want to switch to a TSM system. You must turn off the Centera backup option (unless you want to leave that as another option), and turn on the TSM backup option. The commands to do this are highlighted in the example. The show commands are not necessary, but are for illustration only.

CLI> show storage-system

NETWORK :

CENTERA : backing-up

TSM :

SCP : archiving and backing-up

FTP : archiving and backing-up

ok

CLI>store storage centera backup off

ok

CLI> store storage tsm backup on

ok

CLI> show storage-system

NETWORK :

CENTERA :

TSM : backing-up

SCP : archiving and backing-up

FTP : archiving and backing-up

ok

CLI>

store support state

Enables (**on**) or disables (**off)** the sending of email alerts to the support email address, which can be configured using the **forward support email** command. By default, the support state is enabled (**on**), and the default support email address is support@guardium.com.

Syntax

store support state <on | off>

Show Command

show support state

store throttle

This CLI command stores the throttle parameters. After entering this command, you must issue the CLI command, restart inspection-core for the changes to take effect.

This command is used to filter out (ignore) large packets. Throttling has two modes: Thresholds, per session - ignore sessions when identifying a long enough burst (duration configurable) of large packets (size configurable) and stop ignoring the session when traffic goes under a certain threshold (also configurable); and, Overall - ignore all packets larger than a certain size (configurable) in all sessions. This throttling mode completely ignores long and excessive non-database packets smaller than a predefined size (useful for VNC clients and other types of white-noise traffic). Use for network traffic through SPAM port or hardware TAP. For S-TAP traffic, only network TCP traffic picked up by PCAP. See also the CLI command, store s2c.

Syntax

store throttle [default | size <s> interval <i> trigger <t> release <r>]

USAGE: store throttle size S interval I trigger T release R

where 0<=S<=2^17 (bytes), 1<=I,T,R,<=2^31 (seconds)

OR store throttle default

Show Command

show throttle

Throttle parameters:

Packet size: 228000

Time interval: 604800

Trigger level: 10000000

Release level: 10000000

Parameters

default - Enter the keyword default to restore the system defaults (no other parameters are used). The default throttling parameters are never throttle.

s - The packet size in bytes, up to a maximum of 217 (131072).

The remaining parameters are in seconds, up to a maximum of 231 (2147483648):

i - The time interval

t - The trigger level

r- The release level

Note: To restore the throttle defaults, use the CLI command, store throttle default.

store timeout

Sets the timeout value of a CLI session and/or fileserver session. The default value is 600 seconds. A timeout will also close the CLI session.

If the fileserver is stopped because of a timeout, a message will appear, `Warning : Fileserver stopped because of timeout. The file upload may not be complete. Stopping the process.`

Use the CLI commands, show timeout db_connection, to show the socketTimeout value in the conf file, and store timeout db_connection <value>, to set the value of the timeout. The value should be greater than 0. The default value is 25000 seconds. These CLI commands are used in managing the communications between the Central Manager and the managed unit when DNS is not configured.

Syntax

store timeout cli_session <n>

store timeout fileserver_session <n>

store timeout db_connection <n>

Show command

show timeout cli_session 600

show timeout fileserver_session 600

show timeout db_connection 25000

store transfer-method

Sets the file transfer method used for CSV/CEF export. For export file, need to use CLI command, store transfer-method csv, to set the method of transfer. For backup/archive, use the CLI command, store transfer-method backup, to set the method of transfer.

Syntax

store transfer-method <FTP | SCP>

Show Command

show transfer-method

Note: Files sent from one IBM Guardium appliance to another (from a collector to an aggregator, for example) are always sent using SCP.

store uid_chain_polling_interval

Set the interval for UID Chain polling with this CLI command. UID chain is a mechanism which allows S-TAP (by way of K-Tap) to track the chain of users that occurred prior to a database connection.

Set the interval to 0 to turn off the UID Chain processing, in order to improve database performance. If the UID Chain processing is turned off, then calculating the UID Chain and updating children sessions are skipped.

Note: When using any database, the UID chain is not logged for all sessions if the session is very short.

Syntax

store uid_chain_polling_interval <N>

where N is time in minutes (>= 1 minute; default is 2 minutes)

set N = 0, to turn off the UID Chain processing

Show command

show uid_chain_polling_interval

store upd_session_end

This CLI command adds an option to skip the update for the session_end time.

Syntax

store upd_session_end [enable | disable]

Show command

show upd_session_end

store unit type

Use this CLI command to set unit type attributes for the Guardium appliance. See the Unit Type Attributes table for a description of all unit type attributes that can be displayed by this command.

Syntax

store unit type [manager | standalone] [netinsp] [stap] [mainframe] [sink]

Use `store unit type sink` to switch collected DRDA traffic timestamp granularity from 1 millisecond to 1 microsecond.

Show Command

show unit type

Note: Some attributes listed are set using the store unit type command, and cleared using the delete unit type command. The aggregator attribute can only be set during installation of the IBM Guardium software, and cannot be modified except by re-installing the IBM Guardium software.

Unit Type Attributes

The Guardium system unit type attributes that can be displayed by the show unit type command are described in the table. Except where noted, these attributes can be set using the store unit type command, and cleared using the delete unit type command.

Table 3. Unit Type Attributes

Attribute	Description
mainframe	The unit is a mainframe (z/OS®) network inspection appliance.
manager	Central manager functions are enabled for this unit.
netinsp	Inspection of network traffic is enabled.
network route static	Removes one line off the static routing table
standalone	Local management (independent of a central manager)
stap	The unit can receive data from and manage S-TAP and CAS agents.

unregister management

The unregister command restores the configuration that was saved when the appliance was registered for central management. If that happened under a previous release of the IBM Guardium software, restoring that configuration without first applying a patch to bring the saved configuration to the current software release level will disable the appliance, potentially causing the loss of all data stored there. Accordingly, do not unregister a unit until you have verified that the pre-registration configuration is at the current software release level. If you are unsure about how to verify this, contact Technical Support before unregistering the unit.

Syntax

unregister management

Notes:

- This command is intended for emergency use only, when the Central Manager is not available.
- After unregistering using this command, you should also unregister from the Central Manager (from the Administration Console), since that is the only way the count of managed units will be reduced. The count of managed units is authorized by the product key.

Parent topic: CLI Overview
Related information:
Guardium troubleshooting and support (video)

diag CLI command

Use these CLI command to access troubleshooting and maintenance utilities through diag.

Use the diag command as directed by Technical Support.

There are no functions that you would perform with this command on a regular basis. Each main menu entry is described in a separate topic (see Main Menu Commands).

Troubleshooting and Maintenance Utilities through DIAG:

- Aggregator Fix Schema – brings all imported tables that have older schema than that of the aggregator to the schema of the latest patch level of the aggregator (runs in the background and may take several hours to complete). Note: There may be scenarios in which (a) the aggregator will not have the latest patch level or (b) some of the imported tables are of the latest patch level—resulting in not all imported tables having the latest patch level.
- Aggregator Maintenance – full analysis and recovery of the Aggregator. This utility will collect AGG related logs and place it in the diag export folder, calls the Aggregator Fix Schema to sync the schema of all databases, clean AGG workspace and restart the merge process to ensure full analysis of all imported tables (runs in the background and may take several hours to complete).
- Clean Static Orphans on an Aggregator – This option should be used only by Technical Support and only in those cases where static tables grow too much and needed to be cleaned. This utility cleans all the old construct records that are no longer in use.

Opening the Diagnostics Main Menu

To use the diag command, follow the procedure outlined:

1. At the command line prompt, log into the Guardium® appliance with CLI.

   The Guardium user attempting to use the diag command must have an assigned CLI or admin role. The only user who has a CLI role by default is admin. The user with a CLI or admin role is permitted to enter the diag command, use the unlock admin and unlock accessmgr CLI commands, and use the export audit-data CLI command without restrictions. The user with a CLI role does not have to enter user name and password required of a GUI login and does not go through any further role check.

   If the Guardium user attempting to use CLI does not have a CLI or admin role, CLI will not start. The accessmgr assigns CLI and admin roles.

2. After starting CLI, enter the diag command (with no arguments) at the command line prompt.
3. The Guardium user attempting to use the diag command must have an assigned diag role on the Guardium system. By default, only admin has this assigned role. Access to diag is allowed or disallowed based on the role assignment of this user (access to diag is permitted only if this user has the diag role). The accessmgr assigns diag roles.
4. You are presented with the main command menu. Do one of the following to move the option selection cursor (which is selecting the first item in the example):
   - Type the desired entry number (the selection cursor moves to the selected entry).
   - Use the Up or Down arrow key to select the desired entry.
5. Press the Spacebar, the Left arrow key, or the Right arrow key to move the command selection cursor in the display (which is selecting the OK command in the example).
6. Perform an action by selecting the appropriate option in the display area and then doing one of the following:
   - Select the appropriate command with the command selection cursor, then press the Enter key
   - Click on the appropriate action command.

About the diag Output

The diag command creates output in two directories:

- .../guard/diag/current
- .../guard/diag/depot

This output is accessed through the fileserver CLI command. See fileserver for further information.

Each directory is described in the following subsections.

.../guard/diag/current Directory

Most output from the diag commands is written in text format to the current directory. For most commands, this directory contains a separate output file. Each time you run the same command, output is appended to the single file for that command. For a smaller number of commands, a separate file is created for each execution, usually incorporating a date and time stamp in the filename.

We recommend that you “clean up” after each session, so in subsequent sessions you are not looking at old information. When you pack files to a single compressed file for exporting (see the following topic), all files in the current directory are deleted. Alternatively, you can use the Delete recordings command of the Output Management menu to delete individual files.

The files in the current directory are easy to identify since the names are created from menu and command names. For example, after you use the File Summary command from the System Interactive Queries menu, a file named interactive_filesummary.txt is created in the current directory.

If you look at the current directory while in the process of using a command, you may see a hidden temporary file with the same name as the one that will contain the output for that command. The temporary file will be removed when the output is appended to the command output file.

.../guard/diag/depot Directory

When you pack the diag output files in the current directory to a compressed file (to send to Guardium Technical Support, for example), it is stored in the depot directory. The filename is in the format diag_session_<dd_mm_hhmm>.tgz, where the variable portion of the name indicates when the file was created. For example, a file created at 12:15 PM on May 20th would be named as follows: diag_session_20_5_1215.tgz.

After exporting files (see the Export recorded files topic), you can remove them from the depot directory using the Delete recordings command of the Output Management menu.

1 Output Management

The Output Management commands control what is done with the output produced by the diag command. Each Output Management command is described separately.

1.1 End and pack current session

Use this command to pack all diagnostic files in the current directory into a single compressed file, and remove those files from the current directory. When you enter this command, there is no feedback to indicate that the command has completed. You can verify that the command has finished by displaying the directory of the depot directory. When the command completes, there is a file named in the following format: diag_session_<mm_dd_hhmm>.tgz, where the variable portion of the name is a date and time stamp, as described previously. Use the Export recorded files command of the Output Management menu to send the file to another system.

1.2 Delete recordings

Use this command to delete files in the depot or current directory. (To delete only the current session files, use the Delete current session files command.) When you enter this command, the depot directory structure displays:

You can navigate the directories using the Up and Down arrow keys and pressing Enter. For example, selecting ../ and pressing Enter moves the selection up one level in the directory structure.

You could then select the current directory and press enter, to navigate down to that folder and delete individual command output files. Note that you can navigate to other directories, but you cannot delete files except from the current and depot directories.

When you have selected the file you want to delete, press Enter.

Caution: You will not be prompted to confirm the delete action

1.3 Export recorded files

Use this command to send a file from the depot directory to another site. To export a file:

1. Select Export recorded files from the Output Management menu. The depot directory displays.
2. Select the file to be sent or use the ../ and ./ entries to navigate up or down in the directory structure. (However, keep in mind that you can only export files from the depot directory.)
3. With the file to be transmitted selected, press Enter.
4. You are prompted to select FTP or exit. Select FTP and press Enter.
5. You are prompted to supply a host name. Enter the host name of the receiving system (or its IP address), and press Enter.
6. You are prompted for a user name. Enter a user account name for the receiving system, and press Enter.
7. You are prompted for a password. Enter the password for the user on the receiving system.
8. You are prompted to identify a directory to receive the sent file on the receiving system. Enter the path relative to the ftp root of the directory to contain the file on the receiving system and press Enter.
9. You are prompted to confirm the details of the transfer (the file to be sent and its destination). Press Enter to perform the transfer, or select Cancel and press Enter to start over.
10. You are informed of the success (or failure) of the operation.

1.4 Delete current session files

Use this command to delete files created during the current session.

1.5 Exit

Use the Exit command to return to the main menu.

2 System Static Reports

Use the System Static Reports command of the Main Menu to produce an extensive set of reports.

1. Select System Static Reports from the Main Menu. You are informed that the process is running.
2. After the report has been created, it displays in the viewing area. Note that his report is lengthy and may be easier to view using a text editor, after exporting it to a desktop computer).

   Use the Up and Down arrow keys to scroll up or down in the report. When you are done viewing the report, press Enter to return to the Main Menu.

System Static Reports Overview

The following subtopics provide an outline of the major components of the System Static Reports output. The fragments of output shown are intended to illustrate the type and level of information contained in the report, rather than provide a detailed description of the actual contents (that is beyond the scope of this document).

System Configuration Information

The System Static Reports output describes the build version, the patches applied, the current system up time, and name server information:

```
Build version: 34e1eb12eb68ba76cb49028251c9a0d6  /opt/IBM/guardium/etc/cvstag
Patches:
2009/02/22 16:16:50: START Installation of 'Update 5.0'
2009/02/22 16:18:04: Installation Done - Successfully Installed

< lines deleted… >

Current uptime:
  09:03:43  up 6 days, 17:34,  1 user,  load average: 0.44, 0.50, 0.41
System nameservers:
192.168.3.20
DB nameservers:
192.168.3.20
Gateway: 192.168.3.1 (system) 192.168.3.1 (def)
```

Next, the file system information displays (shown partially):

```
Filesystem            Size  Used Avail Use% Mounted on
/dev/hdc3             2.0G  1.1G  813M  58% /
/dev/hdc1              97M  9.2M   83M  10% /boot
none                  504M     0  504M   0% /dev/shm
/dev/hdc2              71G  1.2G   66G   2% /var
        total:    used:    free:  shared: buffers:  cached:
Mem:  1055199232 1041711104 13488128        0 63275008 186220544
Swap: 536698880 295432192 241266688
MemTotal:      1030468 kB
MemFree:         13172 kB

< lines deleted… >
```

This is followed by information about the mail and SNMP servers configured:

```
SMTP server: 192.168.1.7 on port 25 : REACHABLE
SMTP user: undef
SMTP password: undef
SMTP auth: NONE
SNMP trapsink: undef UNREACHABLE
SNMP trap community: undef
SNMP read community: undef
```

The final section of the system configuration section describes the network configuration for the unit: IP address, host and domain names, etc:

```
eth0:                192.168.3.101  (system) 192.168.3.101 (def)
hostname:                         (system)  g1 (def)
domain:                             (system)  guardium.com (def)
mac address:      00:04:23:A7:77:F2  (MAC1)  00:04:23:A7:77:F2 (MAC2)
unit type:           548 Standalone STAP
```

Internal Database Information

The next major section of the System Static Reports output contains information about the internal database status and threads (only the first few threads are shown):

```
uptime 77097  seconds.
27  threads.
78545028  queries.
+------+------------+-----------------------------+---------+---------+------+-----------
| Id   | User       | Host                        | db      | Command | Time | State |  +----------------------------------------
-------------------------------------------
| 1137 | enchantedg | localhost                   | TURBINE | Sleep   | 26   |
| 1257 | enchantedg | localhost.localdomain:33587 | TURBINE | Sleep   | 0    |
| 1258 | enchantedg | localhost.localdomain:60409 | TURBINE | Sleep   | 7716 |
| 1259 | enchantedg | localhost.localdomain:48233 | TURBINE | Sleep   | 322  |

< lines deleted… >
```

The list of threads is followed by an analysis of table status.

Web Servlet Container Information

The next several sections of the System Static Reports output contain information about the Web servlet container environment (Tomcat):

```
================================================================================
Currently defined Tomcat port is 8443.
The TOMCAT daemon is running and listening on port(s): 8005 8443.
Currently OPEN ports
java run by tomcat on port *:8443

< lines deleted… >
================================================================================

These are the nanny latest actions:
May 19 14:13:09 guard nanny:[5528]: Also checking tomcat.
May 19 14:13:09 guard nanny:[5528]: Going for my initial nap.
```

```
< lines deleted… >

This is the TOMCAT command line:
  463 sh -c ps -o pid,cmd -e | grep Dcatalina.base
21917 grep Dcatalina.base.
```

Inspection Engine Information

The next major section of the System Static Reports output contains information about the inspection engine:

```
================================================================================
This is the SNIF (pid: 13036) command line:  13036 /opt/IBM/guardium/bin/snif.
This is the SNIF status:
Name:               snif
State:                R (running)
Tgid: 13036

< lines deleted… >
================================================================================

Current timestamp is 2009-05-20 11:56:41
This is the last timestamp at GDM_CONSTRUCT_INSTANCE: 2009-05-20 11:56:41
This is the last timestamp at GDM_EXCEPTION: 2009-05-20 11:56:41
This is the last timestamp at GDM_POLICY_VIOLATIONS_LOG: 2009-05-20 11:56:41

================================================================================

Snif buf usage at Fri May 20 11:56:44 2009:
100 204800 buffers out of 204800
126 connection used, 32642 unused, 0 dropped (sniffer), 9 ignored (analyzer)
0 bytes lost, 60 connections ended, 601752099 bytes sent, 579063 request sent
Dropped Packets: 0 buffer full, 0 too short , 451 ignored
 time now is 1116604603
Analyzer/Parser buffers size: 6 (66533) 0 (62902)
 ms-tsql-logger  0 (11331)
 syb-tsql-logger  0 (70)
 ora-tsql-logger  79 (67803)
 db2-sql-logger  0 (20544)

< lines deleted… >
```

IP Tables Information

The next major section contains information about the IP tables:

```
================================================================================
IPTABLES:
-------------
       tcp  --  192.168.2.0/24       192.168.1.0/24      tcp spts:1521:60000  set 0x23
       tcp  --  192.168.1.0/24       192.168.2.0/24      tcp dpts:1521:60000  set 0x22
< lines deleted… >
```

S-TAP Information

The next major section contains S-TAP® information:

```
================================================================================
STAP:
----
    0     0 ACCEPT     tcp  --  *      *  0.0.0.0/0      0.0.0.0/0          tcp spt:9500
    0     0 ACCEPT     tcp  --  *      *  0.0.0.0/0      0.0.0.0/0          tcp dpt:9500
 2696  148K ACCEPT     tcp  --  *      *  0.0.0.0/0      0.0.0.0/0          tcp spt:16016
 2835  175K ACCEPT     tcp  --  *      *  0.0.0.0/0      0.0.0.0/0          tcp dpt:16016

< lines deleted… >
```

IP Traffic Information

The next major section contains IP traffic information:

```
IP traffic statistics.
OUTPUT OF ETH0
Fri May 20 11:57:04 2012; ******** Detailed interface statistics started ********

*** Detailed statistics for interface eth0, generated Fri May 20 11:58:04 2009

< lines deleted… >

OUTPUT OF ETH1
Fri May 20 11:57:04 2012; ******** Detailed interface statistics started ********

*** Detailed statistics for interface eth1, generated Fri May 20 11:58:04 2009

Total:               82440 packets, 53892382 bytes
        (incoming: 82440 packets, 53892382 bytes; outgoing: 0 packets, 0 bytes)
IP:    82440 packets, 52632747 bytes
        (incoming: 82440 packets, 52632747 bytes; outgoing: 0 packets, 0 bytes)

< lines deleted… >
```

Information Engine STDERR and STDOUT Information

The next section contains the last messages output by the sniffer:

```
Snif  STDERR:

< lines deleted… >

Snif STDOUT:
Fri_20-May-2009_04:04:35 : Guardium Engine Monitor starting
Fri_20-May-2009_04:14:37 : Guardium Engine Monitor starting
Fri_20-May-2009_04:24:38 : Guardium Engine Monitor starting

< lines deleted… >
```

Import Directory Information

The next section lists the import directory contents:

```
These are the contents of the importdir directory:
total 0
```

Aggregator Activity Information

This section lists aggregator activities (there are none in the example):

```
================================================================================
This is the aggregator last activities:
```

Audit Report

This section lists the following summary information (see example):

```
================================================================================
Range of time in logs: 01/14/10 13:12:26.348 - 01/18/10 12:48:01.073
Selected time for report: 01/14/10 13:12:26 - 01/18/10 12:48:01.073
Number of changes in configuration: 4   - changes to the audit configuration
Number of changes to accounts, groups, or roles: 0
Number of logins: 22    - logins into the machine - ssh and console
Number of failed logins: 114
Number of authentications: 22 - "su", etc.
Number of failed authentications: 5
Number of users: 2
Number of terminals: 18
Number of host names: 9
Number of executables: 7
Number of files: 0
Number of AVC's: 0
Number of MAC events: 0
Number of failed syscalls: 0
Number of anomaly events: 3
Number of responses to anomaly events: 0
Number of crypto events: 0
Number of keys: 0
Number of process IDs: 9173
Number of events: 98669
================================================================================
```

Anomaly Report

This section lists the following (see example):

```
================================================================================
# Date Time Type Exe Term Host AUID Event
================================================================================
1. 01/14/10 13:16:02 ANOM_PROMISCUOUS /usr/sbin/brctl (none) ? -1 8 -  this is expected
to appear - it means the bridge is listening to all traffic
```

Authentication Report

This section lists the following (see example):

```
================================================================================
# Date Time Type Exe Term Host AUID Event
================================================================================
1. 01/14/10 13:13:22 tomcat ? console /bin/su yes 4
2. 01/14/10 13:16:44 tomcat ? console /bin/su yes 11
3. 01/14/10 13:16:44 tomcat ? console /bin/su yes 17
4. 01/14/10 13:16:45 tomcat ? console /bin/su yes 23
5. 01/14/10 13:16:48 tomcat ? console /bin/su yes 29
6. 01/14/10 13:22:29 tomcat ? ? /bin/su yes 155
7. 01/14/10 13:28:10 ? ? tty1 /bin/login no 252
8. 01/14/10 13:28:20 ? ? tty1 /bin/login no 254
```

Login Report

This section lists the following (see example):

```
================================================================================
# Date Time Type Exe Term Host AUID Event
================================================================================
1. 01/14/10 13:22:15 root 192.168.2.9 sshd /usr/sbin/sshd no 142
```

```
2. 01/14/10 13:22:15 root 192.168.2.9 sshd /usr/sbin/sshd no 143
3. 01/14/10 13:22:17 root 192.168.2.9 sshd /usr/sbin/sshd no 144
4. 01/14/10 13:22:17 root 192.168.2.9 sshd /usr/sbin/sshd no 145
5. 01/14/10 13:22:20 root 192.168.2.9 sshd /usr/sbin/sshd no 146
```

3 Interactive Queries

Select System Interactive Queries from the main menu to open the Interactive Queries menu. (Use the Down arrow key to scroll past the tenth item to see all items on this menu.)

In addition to displaying the requested information, each interactive query command creates output in a separate text file in the current directory. See the Overview topic for more information about the files created.

Each command is described in the following sections.

3.1 Files Changed

Use the Files Changed command to display a list of files changed either before or after a specified number of days.

1. Select Files Changed from the Interactive Queries menu. You are prompted to enter a number days. Type a number and press Enter.
2. You are asked if you are interested in the files changed before or after that number of days. Select 1 or 2 and press Enter.
3. The full directory path for each changed file is displayed. Note that if not all data fits in the display area, use the Up and Down arrow keys to scroll through the data. The current position in the file is indicated by the number in the display. The white bars in the display area indicate the presence of more data with a plus sign.

3.2 List Folder

Use this command to list the contents of various directories.

1. Select List Folder from the Interactive Queries menu.
2. You are prompted to select a directory. Select a directory and press Enter. The selected directory is displayed. Remember that if multiple commands of the same type are issued, the data for each execution of the command is appended to the single text file maintained for that command.
3. Press Enter or click Exit when you are done.

3.3 Summarize Folder

Use the Summarize Folder command to display the output of the du (Disk Usage) command:

1. Select Summarize Folder from the Interactive Queries menu. There are no prompts. You are presented with a display of disk use for various directories.
2. Use the Up and Down arrow keys to scroll through the directories.
3. Press Enter or click Exit when you are done.

3.4 File Summary and Export

Use this command to list all or some portion of a log file.

1. Select File Summary from the Interactive Queries menu.
2. You are prompted to select a file. Use the Up and Down arrow keys to scroll the selection cursor to the file you want to view.
3. Press Enter or click OK.
4. You are prompted to select the number of lines to display. Make your selection and press Enter.
5. You are prompted to enter an optional search string. Use this box if you are searching for a particular log message (you can enter a regular expression). Otherwise leave the box empty and press Enter.
6. Following the prompt, press Enter to answer yes, meaning that only unique messages will be displayed. Otherwise select No and press Enter (all messages will be displayed).

   Be aware that when the Summary Style is used, variables are replaced by the pound sign character (#). For some log data containing variables such as IP addresses or dates, the replacements can be extensive.

3.5 Test Email

Use this command to send a test email using the configured SMTP server.

1. Select Test Email from the Interactive Queries menu.
2. You are prompted to select a recipient. Select Custom and press Enter.
3. You are prompted to supply an email address. Type an email address and press Enter. You will be informed of the output of the operation. Note that on the Administration Console, the Test Connection link in the SMTP pane of the Alerter configuration panel only tests that an SMTP port is configured, not that mail can actually be delivered via that server. You can use this command to test email delivery without having to configure and trigger a statistical or real-time alert, or an audit process notification.

3.6 Test SNMP

Use this command to send a test SNMP trap to the configured SNMP server.

1. Select Test SNMP from the Interactive Queries menu.
2. You are informed of the activity and the results. Note that on the Alerter Configuration panel, the Test Connection link in the SNMP pane only tests that an SNMP port is configured, not that a trap can actually be delivered via that server. You can use this command to test trap delivery without having to configure (and trigger) a statistical or real-time alert, or an audit process notification.

3.7 Report Query Data

Use this command to display the actual select statement used for a report query. This might be useful if a user-written report is producing unexpected output.

1. Select Report Query Data from the Interactive Queries menu.

2. You are prompted to make a selection from a list of report titles. Use the Up and Down arrow keys to select an entry and press the Enter key. Each entry in this list is a Report entity. All pre-defined reports are listed first. These are numbered in the range 100-225 (for version 3.6.1 – the numbers will most likely grow incrementally with each release, as more pre-defined reports are created).

   User written reports are listed following the pre-defined reports, beginning with number 20001 (for version 3.6.1).

   The selected report select statement will be displayed.

3.8 GDM Queries

Use this command to display a count of observed SQL calls during a 100 second interval.

1. Select GDM Queries from the Interactive Queries menu.
2. A message displays requesting your patience. Select yes to continue. The CMD_CT column on the display lists the number of observed SQL calls from the specified clients to the specified servers.
3. Press Enter when you are done viewing the report.

3.9 Generate TCP Dump

Use this command to create a TCP dump. For this command, output is written to a command file only and not to the screen. Unlike most other commands, a separate file is created in the current directory for each execution of this command. The file name is in the format: tcpdump_<mmyyyy-hhmmss>, where the variable portion is a date and time stamp: mmyyyy is the month and year, and hhmmss is the hours, minutes, and seconds.

1. Select Generate TCP dump from the Interactive Queries menu.
2. You are prompted to select an interface. Select a port and press Enter.
3. You are prompted for an optional filter IP address. If you are interested in traffic from only a specific address, enter that IP address and press Enter. Otherwise, just press Enter.
4. You are prompted for an optional port number. If you are interested in traffic from only a specific port, enter that port number and press Enter. Otherwise, just press Enter.
5. You are prompted to select how many seconds of traffic to capture. Select a number of seconds and press Enter.
6. You are prompted to press Enter to start collecting data. Press Enter. You are returned to the menu after (approximately) the specified number of seconds.
7. To view the TCP dump data, select the Read TCP dumps command or export the file (see Export Reported Files on the Output Management menu, described previously).

3.10 Read TCP Dumps

Use this command to display a TCP dump file created previously.

1. Select Read TCP dumps from the Interactive Queries menu.
2. You are prompted to select file. The TCP dump files are listed from oldest to newest. The file name is in the format: tcpdump_<mmddyy-hhmmss>, where the variable portion is a date and time stamp: mmddyy is the month, day, and year; and hhmmss is the hours, minutes, and seconds. Select the file you want to view and press Enter.
3. The selected file displays. Use the Up and Down arrow keys to scroll through the display and press Enter when you are done.

3.11 Watch Buffer

Use this command to watch activity in the Guardium buffers:

1. Select Watch Buffer from the Interactive Queries menu. The display is updated every second.
2. Press Ctrl-C to close the display.

3.12 SLON Utility

Use this command to run the slon utility, which tracks packets. Typically, you would only run this command as directed by Technical Support. For this command, output is not written to the screen. Output is written to one of two command files in the current directory, for each execution of the command: apks.txt.<day_dd-mmm-yyyy_hh.mm.ss.ttt> OR requests.txt.<day_dd-mmm-yyyy_hh.mm.ss.ttt>

The variable portions or the file names are date and time stamps. For example, apks.txt.Fri_20-May-2011_08.52.00.789.

1. Select Slon Utility from the Interactive Queries menu.
2. Select the action to be performed and click OK. The choices are:

   (a) to dump Analyzer rules info

   (f) to filter Analyzer packets based on IP and/or mask

   (p) to dump packets to apks.txt

   (l) to dump logger requests to requests.txt

   (m) to dump STAP packets (Select how long to run. Wait for completion and then check the msg-dump file under /var/log/guard/diag/current/tap/)

   (r) to record IPQ traffic

   (s) to dump State machine info

   (t) to configure throttle parameters

3. Regardless of your selection, you will be prompted to select the time period for the activity. Select a time period and press Enter.
4. You are notified that the program will run for the specified time and prompted to press Enter. Press Enter and wait.
5. When processing completes, a message will be displayed. You can use the File Summary command to display the output of this command. Because this command can produce a large amount of data, you will probably want to export the file to another system, where you can view the contents using a text editor. (Pack the current session data, and export the recordings as described earlier in this section.)

3.13 Show Indexes

Use this command to show indexes for various internal tables:

1. Select Show Indexes from the Interactive Queries menu.
2. You are prompted to select a table. Select a table and press Enter to display the indexes for that table.
3. Use the Up and Down arrow keys to scroll through the display. Press Enter when you are done.

3.14 S-TAP Check

Use this command to display S-TAP definitions and traffic information:

1. Select S-TAP Check from the Interactive Queries menu.
2. The system's unit type displays in numeric format. Press Enter.
3. You are prompted to select the number of seconds to monitor the S-TAP traffic. Use the Up and Down arrow keys to make a selection and press Enter.
4. You are informed of approximately how long to wait for output, and prompted to press Enter. Press Enter.
5. The S-TAP Definitions and Server Traffic reports display. Press Enter when you are done viewing the report.

3.15 Interface Link Status

Use this command to display interface link status.

1. Select Interface link status from the Interactive Queries menu.
2. The status of all interfaces displays. Use the Up and Down arrows to scroll through the display.
3. Press Enter when you are done. Note that this command displays the link status only. To display interface configuration information, use the show network interface all CLI command.

3.16 Show Throttle Data

Use this command to display throttle data.

1. Select Show Throttle data from the Interactive Queries menu.
2. Press Enter and wait 3 seconds for throttle statistics.
3. Use the Up and Down arrows to scroll through the display, and press Exit when you are done.

3.17 Generate TCP dump and slon

Use this command to create a TCP dump and run the slon utility, which tracks packets. Typically, you would only run this command as directed by Technical Support. See the individual topics, Generate TCP dump, and Slon Utility.

3.18 Generate SSL dump

Use this command to create a SSL dump..

1. Select Generate SSL dump from the Interactive Queries menu.
2. Select an interface and press OK. Enter filter IP address and press OK. Enter filter port number and press OK.
3. Select how long to run and press OK. Press OK and wait the specified time in order to gather TCP dumps.
4. If you wish to view SSL dumps, press OK.
5. Press Exit when you are done.

3.19 View bash history

Use this command to display bash history.

1. Select View Bash History from the Interactive Queries menu.
2. Press OK.
3. Use the Up and Down arrows to scroll through the display, and press Exit when you are done.

3.20 Generate GDM_Error dump

Use this command to create GDM_ERROR dumps.

1. Select Show Generate GDM_ERROR dump from the Interactive Queries menu.
2. Press OK and then enter password. Press Enter.
3. Use the Up and Down arrows to scroll through the display, and press Exit when you are done.

3.21 Prepare Tomcat Memory dump

When Tomcat has a first outOfMemory error, it will do a memory dump to /var/tmp/tomcat/tomcat.dmp. Use this command to compress, encrypt and move this file to /var/log/guard/diag/tomcat/ for fileserv to retrieve.

1. Select Prepare Tomcat Memory dump from the Interactive Queries menu.
2. Press OK.
3. Use the Up and Down arrows to scroll through the display, and press Exit when you are done.

3.22 Extended Network Information

Click on Extended Network Information option under System interactive query to display the network diagnostics information.

Example

SQLGuard Diagnostics

Network Parameters from ADMINCONSOLE_PARAMETER:

SYSTEM_NETMASK1: 255.255.255.0

SYSTEM_DOMAIN:

SYSTEM_DEFAULT_ROUTE:

SYSTEM_DNS1:

SYSTEM_DNS2:

SYSTEM_DNS3:

TOMCAT_IP:

MANAGER_IP:

HOST_MAC_ADDRESS:

SECOND_DEVICE:

3.23 Generate TCP dump in rotation

This selection is different from other diag selections in the section called Generate TCP and Generate TCP and slon.

For Generate TCP dump in rotation, enter Filter IP address (enter blank for all IPs). Enter Filter Port number. For the question, How long to run? if the TCP dump in rotation is already running, choose the option “Rotation OFF” or “Rotation” (ON). If Rotation is selected, add file size.

The TCP dump will be output to /var/log/guard/tcp.bin1 and /var/log/guard.bin2 in rotation.

Select TCP dump in rotation again to stop the process loop_tcpdump.sh.

4 Perform Maintenance Actions

Select the Perform Maintenance Actions option from the Main Menu to open the Maintenance menu. Use these commands only under the direction of Technical Support. These do not need to be run on a regular basis.

4.1 TURBINE analysis (update index cardinality)

Use this command to optimize index cardinality on Guardium’s internal database. A progress bar displays while the operation is running. When the operation completes, you are returned to the Maintenance menu.

4.2 TURBINE optimize (rebuild indexes, takes longer)

Use this command to analyze and re-index Guardium’s internal database.

1. Select TURBINE optimize (index cardinality) from the Maintenance menu. A progress bar displays while the operation is running. When the operation completes, you are returned to the Maintenance menu.

4.3 Clean disk space

Use this command to clean unused disk space. You are returned to the Maintenance menu when the procedure completes.

1. Select Clean disk space from the Maintenance menu. You will be prompted to select a directory.
2. Select the directory from which you want to remove files. The contents of the directory will be listed, and you will be prompted to confirm that you want to remove all files.
3. When the operation completes, you are returned to the Maintenance menu.

4.4 RAID maintenance

Use this command only under the direction of Technical Support. This command provides access to the Management Menu of the RAID controller utility program, which can be used to display the status of the RAID drives. If your system does not have a RAID controller, an error message displays if you select this command. You must be extremely careful when using the RAID controller utility program, since several of the functions provided will erase all information on the disk.

4.5 Application Debugging Utility

Use this command to turn debugging on or off. You are prompted to enable or disable logging, or to reset the system defaults.

4.6 Modify TURBINE watchdog threshold

Use this option to change the timeout limit for long queries.

4.7 Force unrecoverable MySQL to start

Use this option only when directed to do so by Technical Support.

4.8 Transfer backups and system recovery

Use this command to restore a backed up version of the internal database. You will be prompted to confirm the operation.

4.9 Tomcat Logging Level

Use this command to select the component debug level. Choose one of the following options:

Classifier, Data Level Security, Workflow, or Other.

Choose Classifier to select debug level options: ERROR, WARN, INFO, DEBUG, ALL.

Choose DLS (data level security), Workflow, or Other (text input) to select debug level options: ERROR, WARN, INFO, DEBUG, ALL.

If Other is chosen (text input separated by ',') , enter valid components (dls, workflow, audit, customtable, gui, other, job).

4.10 Aggregator Maintenance

Full analysis and recovery of the Aggregator. This utility will collect AGG related logs and place it in the diag export folder, calls the Aggregator Fix Schema to sync the schema of all databases, clean AGG workspace, and restart the merge process to ensure full analysis of all imported tables (runs in the background and may take several hours to complete).

4.11 Aggregator Fix Schema

Brings all imported tables to the schema of the latest patch level (runs in the background and may take several hours to complete).

4.12 Clean Static Orphans

This option should be used only by Technical Support and only in those cases where static tables grow too much and needed to be cleaned. This utility cleans all the old construct records that don't have any Instances associated with them. A progress message will display during the Clean Static Orphans (for use on collector or aggregator).

5 Exit to CLI

Select Exit to CLI on the Main Menu. Press Enter to close the diag command and return to the command line interface.

Parent topic: CLI Overview

File Handling CLI Commands

Use these commands to backup and restore system information. Many of these tasks can be performed from Guardium® user interface.

About Archived Data File Names

When Guardium data is archived (or exported to an aggregator), there is a separate file for each day of data. Depending on how your export/purge or archive/purge operation is configured, you may have multiple copies of data exported for the same day. Archive and export data file names have the same format:

<daysequence>-<hostname.domain>-w<run_datestamp>-d<data_date>.dbdump.enc

daysequence is a number representing the date of the archived data, expressed as the number of days since year 0. The same date appears in yyyy-mm-dd format in the data_date portion of the name.

hostname.domain is the host name of the Guardium appliance on which the archive was created, followed by a dot character and the domain name.

run_datestamp is the date that the data was archived or exported, in yyyymmdd.hhmmss format.

data_date is the date of the archived data, in yyyy-mm-dd format.

For example: 732423-g1.guardium.com-w20050425.040042-d2005-04-22.dbdump.enc

backup config

These commands back up and restore configuration information from the internal administration tables. The backup config command stores data in the /media/backup directory. The backup config command removes license and other machine-specific information. The backup system command provides a more comprehensive backup of the configuration and the entire system.

Syntax

backup config

restore config

backup system

This topic applies to backup and restore operations for the Guardium internal database. You can back up or restore either configuration information only, or the entire system (data plus configuration information, except for the shared secret key files, which are backed up and restored separately, see the aggregator backup keys file and aggregator restore keys file commands). These commands stop all inspection engines and web services and restart them after the operation completes.

Before restoring a file, be sure that the appliance has the system shared secret of the system that created that file (otherwise, it will not be able to decrypt the information). See About the System Shared Secret in the Guardium Administrator Guide.
Note: System restore must be done to the same patch level of the system backup. For example, if a customer backed up the appliance when it was on Version 7.0, Patch 7 and then wishes to restore this backup into a newly-built appliance, then there is a need to first install Version 7.0, Patches 1 to 7 on the appliance and only then to restore the file.
There are two commands involved in the restore process:

- import file, which returns an archived backup file to the system

- restore system, which restores the system from a backup file previously returned by an import file operation.

For all backup, import and restore commands, you will receive a series of prompts to supply some combination of the following items, depending on which storage systems are configured, and the type of restore operation. Respond to each prompt as appropriate for your operation. The following table describes the information for which you may be prompted.

Note:

One copy of the SCP/FTP/TSM/Centera file transfer is saved, regardless if the transfer was successful or failed. As certain files may take hours to regenerate (for example, system backup), having a readily available copy (in particular if the file transfer failed) is of value to the user. Only one copy of each type of file is retained (archive/system backup/configuration backup/etc.)

Backup system will copy the current license, metering and number of datasources, and then backup the data. Restore system will restore the data and then restore the license, metering and number of datasources. This sequence applies to the regular restore system. Restore from a previous system will require re-configuring license, metering and number of datasources.

When configuring backups, value of zero '0' for the port number indicates that the default port is being used for that protocol and no need to change.

Table 1. backup system

Item	Description
SCP, FTP, TSM, Centera, Snapshot	Select the method to use to transfer the file. TSM and Centera will be displayed only if those storage methods that have been enabled (see the store storage-method command)
Data or Configuration	Select Configuration to back up definitions and configuration information only, or select Data to back up data in addition to configuration information.
restore from archive or restore from backup	Select restore from archive to restore archived data, or select restore from backup to restore configuration information.
normal or upgrade	If restoring from the same software version of Guardium, select normal. If restoring configuration information following software upgrade of the Guardium appliance, select upgrade.
host	The remote host for the backup file.
remote directory	The directory for the backup file. For FTP, the directory is relative to the FTP root directory for the FTP user account used. For SSH, the directory path is a full directory path. For Windows SSH servers, use Unix-style path names with forward slashes, rather than Windows-style backslashes.
username	The user account name to use for the operation (for backup operations, this user must have write/execute permission for the directory specified). **Note:** For Windows, a domain user is accepted with the format of domain\user
password	The password for the username.
file name	The file name for the archive or backup file. See Archived Data Names. A user can select multiple files by using the wildcard character * in the file name. Support of the wildcard character * is permitted when using transfer methods FTP, SCP and Snapshot. Support of the wildcard character * is not permitted on transfer methods TSM or Centera.
Centera server	Enter the Centera server name. If using PEA files, use the following format: <Host name/IP>? <full PEA file name>, for example: 128.221.200.56?/var/centera/us_profile_rwqe.pea.txt
Centera clipID	For a Centera restore operation, the Content Address returned from the backup operation. For example: 6M4B15U4JM4LBeDGKCPF9VQO3UA

After you have supplied all of the information required for the backup or restore operation, a series of messages will be displayed informing you of the results of the operation. For example, for a restore system operation the messages should look something like this (depending on the type of restore and storage method used):

```
gpg: Signature made Thu Feb 22 11:38:01 2009 EST using DSA key ID 2348FF9E gpg: Good signature from "Backup Signer
<support@guardium.com>" Proceeding to shutdown services Proceeding to startup services Safekeeping admin.xreg Safekeeping
client.xreg Safekeeping controllers.xreg Safekeeping controls.xreg Safekeeping guardium-portlets.xreg Safekeeping local-
portlets.xreg Safekeeping local-security.xreg Safekeeping local-skins.xreg Safekeeping media.xreg Safekeeping portlets.xreg
Safekeeping security.xreg Safekeeping skins.xreg guard_sniffer.pl -reorder Recovery procedure was successful. ok
```

Prevent backup/archive scripts from filling up /var

The backup process will check for room in /var before running and fail. This process will also warn the user if there is insufficient space for backup.

The archive process will check the size of the static tables and make sure there is room in /var to create the archive.

An error is now logged in the logfile and GUI if the backup is over 50%

Example:

```
ERROR: /var backup space is at 60% used. Insufficient disk space for backup. CLI> backup system     1. DATA     2. CONFIGURATION
Please enter the number of your choice: (q to quit) 1      1. SCP     2. CONFIGURED DESTINATION  Enter the number of your choice:
(q to quit) 2 Make sure destination is configured in the GUI under the System Backup option Please wait, this may take some time.
```

backup profile

Use this command to maintain the backup profile data (patch mechanism).

The backup file will be copied to the destination according to the backup profile. If the parameter indicating whether to keep the backup file is “1” AND there is enough disk space the backup file will be kept within the system, otherwise removed.

All four fields must be filled in - backup destination host, backup destination directory, backup destination user, and backup destination password.

Syntax

show backup profile

Example

```
patch backup flag is 1    patch backup automatic recovery flag is 1    patch backup dest host is    patch backup dest dir is
patch backup dest user is    patch backup dest pass is    ok
```

Syntax

store backup profile

Example

```
Do you want to set up for automatic recovery? (y/n)    Enter the patch backup destination host:    Enter the patch backup
destination directory:    Enter the patch backup destination user:    Enter the patch backup destination password:
```

export audit-data

Exports audit data from the specified date (yyyy-mm-dd) from various internal Guardium tables to a compressed archive file. The data from a specified date will be stored in a compressed archive file, in the /var/dump directory. The file created will be identified in the messages produced by the system. See the example. Use this command only under the direction of Guardium Support.

Note: Only users with admin role may run this command .

Syntax

export audit-data <yyyy-mm-dd>

Example

```
If you enter the audit-data command for the date 2005-09-16, a set of messages similar to the following will be created: CLI>
export audit-data 2005-09-16 2005-09-16 Extracting  GDM_ACCESS  Data ... Extracting  GDM_CONSTRUCT  Data ... Extracting
 GDM_SENTENCE  Data ... Extracting  GDM_OBJECT  Data ... Extracting  GDM_FIELD  Data ... Extracting  GDM_CONSTRUCT_TEXT  Data ...
Extracting  GDM_SESSION  Data ... Extracting  GDM_EXCEPTION  Data ... Extracting  GDM_POLICY_VIOLATIONS_LOG  Data ... Extracting
 GDM_CONSTRUCT_INSTANCE  Data ... Generating tar file ...  /var/csvGenerationTmp ~ GDM_ACCESS.txt GDM_CONSTRUCT.txt
GDM_CONSTRUCT_INSTANCE.txt GDM_CONSTRUCT_TEXT.txt GDM_EXCEPTION.txt GDM_FIELD.txt GDM_OBJECT.txt GDM_POLICY_VIOLATIONS_LOG.txt
GDM_SENTENCE.txt GDM_SESSION.txt ~ Generation completed, CSV Files saved to /var/dump/732570-supp2.guardium.com-w20050919110317-
d2005-09-16.exp.tgz ok
```

The data from each of the named internal database tables is written to a text file, in CSV format. The name of the archive file ends with exp.tgz and the remainder of the name is formed as described in About Archived Data File Names.

You can use the export file command to transfer this file to another system.

delete audit-data

Use this command only under the direction of Guardium Support. This command is used to remove compressed audit data files. You will be prompted to enter an index number to identify the file to be removed. See Archived Data File Names, for information about how archived data file names are formed.

You will be prompted to identify the file to be removed.

Syntax

delete audit-data

show audit-data

Use this command to display any files that were created by executing the CLI command, export audit-data. For more information about audit data files, see export audit-data.

Syntax

show audit-data <yyyy-mm-dd>

export file

This command exports a single file named filename from the /var/IBM/Guardium/data/dump, /var/log or /var/IBM/Guardium/data/importdir directory.

Use this command only under the direction of Guardium Support. To export Guardium data to an aggregator or to archive data, use the appropriate menu commands on the Administration Console panel.

Syntax

export file </local_path/filename> <user@host:/path/filename>

local_path must be one of the following: /var/IBM/Guardium/data/dump, /var/log or /var/IBM/Guardium/data/importdir

fileserver

Use this command to start an HTTPS-based file server running on the Guardium appliance. This facility is intended to ease the task of uploading patches to the unit or downloading debugging information from the unit. Each time this facility starts, it deletes any files in the directory to which it uploads patches.

Note: Any operation that generates a file that the fileserver will access should finish before the fileserver is started (so that the file is available for the fileserver).

Syntax

fileserver [https://ip address:8445] [duration]

ip address is an optional parameter that allows access to the fileserver from the indicated IP address. By default (without the parameter), access is restricted to the IP address of the SSH client that started the fileserver.

duration is an optional parameter that specifies the number of seconds that the fileserver is active. After the specified number of seconds, the fileserver shuts down automatically. The duration can be any number of seconds from 60 to 3600.

In case of a security setup where browser sessions are redirected through a proxy server, the IP address of the fileserver client will not be the same as SSH client that started the fileserver. Instead, the fileserver client will have the IP address of the proxy server, and this address must be passing the optional ip address parameter. To find the proxy IP address, check your browser settings or the client IP addresses shown in the Logins to Guardium report in the Guardium Monitor interface.

Example

To start the file, enter the fileserver command:

CLI> fileserver <ip address> <duration>

Starting the file server. You can find it at https://(name of appliance):8445

Press ENTER to stop the file server.

Open the fileserver in a browser window, and do one of the following:

- To upload a patch, click Upload a patch and follow the directions.
- To download log data, click Sqlguard logs, navigate to the file you want and download as you would any other file.

When you are done, return to the CLI session and press Enter to terminate the session.

How to access the VA and Entitlement scripts using fileserver

Instructions

From the CLI, run "fileserver <your desktop IP> 3600"

Vulnerability Assessment:

Open a browser and go to: https://<appliance ip>/log/debug-logs/gdmmonitor_scripts/

Choose the file matching your database type

Entitlements:

Open a browser and go to: https://<appliance ip>/log/debug-logs/entitlemnts_monitor_role/

Choose the file matching your database type

import file

See backup config and restore config.

In import file CLI command, user can use wildcard * for the file name in method scp, ftp and snapshot.

Syntax

import file

import tsm config

Uploads a TSM client configuration file to the Guardium appliance. You must do this before performing any archiving or backup operations using TSM. You will always need to upload a dsm.sys file, and if that file includes multiple servername sections, you will also need to upload a dsm.opt file. For information about how to create these files, check with your company's TSM administrator.

You will be prompted for a password for the user account on the specified host.

Syntax

import tsm config <user@host:/path/[dsm.sys | dsm.opt]>

Parameters

user@host - User account to access the file on the specified host.

/path/[dsm.sys | dsm.opt] - Full path filename of the file to import.

Note: In setting up TSM on each collector, if the initial configuration fails, a notification error results which says the test file could not be sent. Logging into the collector as root, and then running a dsmc archive command to the TSM server, the TSM file, with the same credentials, now succeeds. Returning to the GUI, and configuring with the same options used before, the configuration now succeeds as well.

If tsm config has passwordaccess=generate, the password stored in a local file, is sought. The root user needs to run the dsmc command once to create this local password file.

After uploading the tsm config file, if tsm config has a passwordaccess generate prompt, passwordaccess is set to be generated.

```
Would you like to run a dsmc command now to ensure password is set locally (y/n)?     If the answer is y, run a "dsmc query
options>>/dev/null" command, which will prompt user for password.
```

import tsm property

Use this CLI command to upload a file to /opt/tivoli/tsm/client/ba/bin/guard_tsm.properties.

The file size should be 1K.

Syntax

import tsm property user@host:file

This command will upload the input file to /opt/tivoli/tsm/client/ba/bin/guard_tsm.properties

restore config

These commands back up and restore configuration information from the internal administration tables. The backup config command stores data in the /media/backup directory. The backup config command removes license and other machine-specific information. The backup system command provides a more comprehensive backup of the configuration and the entire system.

When restoring a configuration, you must restore a backup that is of the same version and patch level as the original appliance where the backup was created.

Syntax

backup config

restore config

restore db-from-prev-version

This command takes a backup from the immediate past system (backup data must be provided, configuration backup is optional) and performs a restore on a newer system. It includes upgrading the data, portlets, etc.

Perform a full system backup prior to upgrading your Guardium system. If for some reason the upgrade fails and leaves the machine in a way that can not be used, instead of trying to fix and re-run the upgrade, rebuild the machine as the latest system, setting up this latest system with only the basic network information (IP, resolver, route, system hostname and domain).

The result will be the latest system with the data and customization (if configuration file is provided) from the previous system.

First, try a regular upgrade from the previous system to the latest system. If this is not successful, then use the backup as an alternative way to upgrade from the previous system to the latest system.

Note: Older data being restored to an aggregator (not to investigation center), and outside the merge period, will not be visible until the merge period is changed and the merge process rerun.

To run this command, back up the current server for both data and configuration. Once the backup is complete, install the latest release onto the same server. Next, import both the data and configuration file from CLI via the import file command. Then after the two backup files are imported, run, again from CLI, the command restore db-from-prev-version. This restores the backup files (data and configuration) from the older version to the newly installed server.
Note: If you are using Guardium in a non-English language, the restore CLI command sets some strings, including report headers, to English. To view these strings in the non-English language, run the store language CLI command after you run the restore CLI command.

The optional parameter "override" is applicable only to a restore of a Central Manager appliance from backup.

By default, when a user executes the "restore db-from-prev-version" command on a Central Manager appliance, we preserve the existing configuration information on this Central Manager that links to the Managed Units that it manages.

When the user adds "override" to the restore command, the existing Central Manager /Managed Units configuration is overridden by the Central Manager /Managed Units configuration from the backup data.

Syntax

restore db-from-prev-version [override]

Examples

restore db-from-prev-version

restore db-from-prev-version override

Note: Managed units and S-TAP associations in "Associate S-TAPs and Managed Units" are not restored when using this CLI command. The user will have to define associations again.
Syntax

```
restore db-from-prev-version

This procedure will restore and upgrade a previous backup on a newly-installed latest system. If the older files are currently
located on a remote system, use the "import file" cli command to transfer them locally prior to running this procedure. The
imported files will be put in the /var/dump/ directory. Continue (y/n)?
```

Note:

Answering Y (yes) to the following questions during the execution of the CLI command, restore db-from-prev-version, will result in all non-canned/customized reports and panes to compress into one pane with the name of v.x.0 Custom Reports.

Answering N (no) to the same questions will result in all panes being restored to what they were in previous version.

```
Update portal layout (panes and menus structure) to the new v8 default (current instances of custom reports will be copied to the
new layout, as well as parameter changes on predefined reports) for the user admin? (y/n) n  Update portal layout (panes and menus
structure) to the new v8 default (current instances of custom reports will be copied to the new layout, as well as parameter
changes on predefined reports) for all other users? (y/n)
```

restore keystore

Use this command only under direction from Technical Support.

Use this command to restore certifications and private keys used by the Web servlet container environment (Tomcat).

Syntax

restore keystore

restore pre-patch-backup

Use this command only under direction from Technical Support.

Use this command to recover the pre-patch-backup when the appliance database is up or down.

Syntax

```
restore pre-patchbackup Please enter the information to retrieve the file: Is the file in the local system? (y/n) n Start to
recover with the backup profile parameters. Please check the recovery status in the log
/var/log/guard/diag/depot/patch_installer.log ok ------------------------------------ If answer 'n', abort the operation. If
answer 'y', need to enter the file name.
```

restore system

This topic applies to backup and restore operations for the Guardium internal database. You can back up or restore either configuration information only, or the entire system (data plus configuration information, except for the shared secret key files, which are backed up and restored separately, see the aggregator backup keys file and aggregator restore keys file commands). These commands stop all inspection engines and web services and restart them after the operation completes.

Before restoring a file, be sure that the appliance has the system shared secret of the system that created that file (otherwise, it will not be able to decrypt the information). See About the System Shared Secret in the Guardium Administrator Guide.

Note: System restore must be done to the same patch level of the system backup.
There are two commands involved in the restore process:

- import file, which returns an archived backup file to the system
- restore system, which restores the system from a backup file previously returned by an import file operation.

For all backup, import and restore commands, you will receive a series of prompts to supply some combination of the following items, depending on which storage systems are configured, and the type of restore operation. Respond to each prompt as appropriate for your operation. The following table describes the information for which you may be prompted.

Note:

One copy of the SCP/FTP/TSM/Centera file transfer is saved, regardless if the transfer was successful or failed. As certain files may take hours to regenerate (for example, system backup), having a readily available copy (in particular if the file transfer failed) is of value to the user. Only one copy of each type of file is retained (archive/system backup/configuration backup/etc.)

Backup system will copy the current license, metering and number of datasources, and then backup the data. Restore system will restore the data and then restore the license, metering and number of datasources. This sequence applies to the regular restore system. Restore from a previous system will require re-configuring license, metering and number of datasources.

Table 2. restore system

Item	Description
SCP, FTP, TSM, Centera, Snapshot	Select the method to use to transfer the file. TSM and Centera will be displayed only if those storage methods that have been enabled (see the store storage-method command)
Data or Configuration	Select Configuration to back up definitions and configuration information only, or select Data to back up data in addition to configuration information.
restore from archive or restore from backup	Select restore from archive to restore archived data, or select restore from backup to restore configuration information.
normal or upgrade	If restoring from the same software version of Guardium, select normal. If restoring configuration information following software upgrade of the Guardium appliance, select upgrade.
host	The remote host for the backup file.
remote directory	The directory for the backup file. For FTP, the directory is relative to the FTP root directory for the FTP user account used. For SSH, the directory path is a full directory path. For Windows SSH servers, use Unix-style path names with forward slashes, rather than Windows-style backslashes.
username	The user account name to use for the operation (for backup operations, this user must have write/execute permission for the directory specified). **Note:** For Windows, a domain user is accepted with the format of domain\user
password	The password for the username.
file name	The file name for the archive or backup file. See Archived Data files names. A user can select multiple files by using the wildcard character * in the file name. Support of the wildcard character * is permitted when using transfer methods FTP, SCP and Snapshot. Support of the wildcard character * is not permitted on transfer methods TSM or Centera.

Item	Description
Centera server	Enter the Centera server name. If using PEA files, use the following format: <Host name/IP>? <full PEA file name>, for example: 128.221.200.56?/var/centera/us_profile_rwqe.pea.txt Note the ? between the server IPs and Pea file name. This IP address and the .PEA file comes from EMC Centera. The question mark is required when configuring the path. The .../var/centera/... path name is important as the backup may fail if the path name is not followed. The .PEA file gives permissions, username and password authentication per Centera backup request.
Centera clipID	For a Centera restore operation, the Content Address returned from the backup operation. For example: 6M4B15U4JM4LBeDGKCPF9VQO3UA

After you have supplied all of the information required for the backup or restore operation, a series of messages will be displayed informing you of the results of the operation. For example, for a restore system operation the messages should look something like this (depending on the type of restore and storage method used):

```
gpg: Signature made Thu Feb 22 11:38:01 2009 EST using DSA key ID 2348FF9E gpg: Good signature from "Backup Signer
<support@guardium.com>" Proceeding to shutdown services Proceeding to startup services Safekeeping admin.xreg Safekeeping
client.xreg Safekeeping controllers.xreg Safekeeping controls.xreg Safekeeping guardium-portlets.xreg Safekeeping local-
portlets.xreg Safekeeping local-security.xreg Safekeeping local-skins.xreg Safekeeping media.xreg Safekeeping portlets.xreg
Safekeeping security.xreg Safekeeping skins.xreg guard_sniffer.pl -reorder Recovery procedure was successful. ok
```

set up help (secondary disk for backup)

Install a secondary disk or for backup on R610 R710 appliances. Place it slot number 2 and proceed with set up snapshotdisk to configure the partition, format the drive, and mount it. The two CLI choices are set up help and set up snapshotdisk.

Syntax

setup [help | snapshotdisk | vmware_tools]

store tsm authorization

When backupinitiationroot is set to ON in TSM servers, then only root and authorized users can perform backup/archive. When backupinitiationroot is set on and password access in DSM.SYS is set to “generate”, Guardium backup and archive to TSM will fail with the error message:

```
ANS1708E Backup operation failed. Only a root user can do this operation
```

Non-root users must be authorized to perform backup and archive.

This authorization is enabled by executing the CLI command

```
Store tsm authorization backupinitiationroot on
```

This authorization is disabled by executing the CLI command:

```
Store tsm authorization backupinitiationroot off
```

Syntax

store tsm authorization backupinitationiroot <on/off>

Show command

show tsm authorization backupinitationiroot <on/off>

This CLI command displays on, if non-root Guardium users are authorized to perform backup and archive when backupinitiationroot is set to ON in TSM servers. Otherwise, it displays off.

store language

Use this CLI command to change from the baseline English and convert the database to the desired language. Installation of Guardium is always in English. A Guardium system can be changed to Japanese, Chinese (Traditional or Simplified), French,, Spanish, German or Portuguese after an installation.

The CLI command, store language, is considered a setup of the appliance and is intended to be run during the initial setup of the appliance.

Running this CLI command, after deployment of the appliance in a specific language, can change the information already captured, stored, customized, archived or exported.

Note: After switching from English to a desired language, it is not possible to revert back to English, using this CLI command. The Guardium system must be reinstalled in English.

Syntax

CLI> store language [English | Japanese | SimplifiedChinese | TraditionalChinese | French | German | Spanish | Portuguese]

Show command

show language

set up vmware tools

Use this CLI command to install VMware that runs on the ESX infrastructure.

Syntax

setup vmware_tools [install | uninstall]

Step 1: Open the VM client/console and select the VM instance that contains the IBM Guardium appliance. Right-click the instance, select (from the popup menu) Guest => Install/upgrade VMware tools. This enables the instance to access the VMware tools via a mount point.

Step 2: Run the CLI command (from within the VM client/console), setup vmware_tools install, to install VM tools.

Vmware kernel panic after a reboot

VMware ESX 4.1 Virtual machine running Guardium might get a kernel panic after a reboot.

To correct this situation, VMware recommends: Install update 2 on ESX4.1 or Set CPU/MMU virtualization to Use software only instruction set and MMU Virtualization. This option is found under Settings/ Options/ CPU/MMU Use software for instruction set and MMU Virtualization.

Parent topic: CLI Overview

Inspection Engine CLI Commands

Use these CLI commands to configure the inspection engines.

An inspection engine monitors the traffic between a set of one or more servers and a set of one or more clients using a specific database protocol (Oracle or Sybase, for example). The inspection engine extracts SQL from network packets; compiles parse trees that identify sentences, requests, commands, objects, and fields; and logs detailed information about that traffic to an internal database.

add inspection-engines

Adds an inspection engine configuration to the end of the inspection engine list. The parameters are described. You can re-order your list of inspection engines after adding a new one by using the reorder inspection-engines command. Adding an inspection engine does not start it running; to start it running, use the start inspection-engines command.

Syntax

add inspection-engines <name> <protocol>

<fromIP/mask> <port> <toIP/mask>

<exclude client list> <active on startup>

Parameters

name - The new inspection engine name; must be unique on the unit.

protocol - The protocol monitored, which must be one of the following: Aster, Cassandra, CouchDB, DB2, DB2 Exit, exclude IE, FTP, GreenPlumDB, Hadoop, HIVE, HTTP, HUE, IBM ISERIES, IMPALA, Informix, iNFORMIX Exit, KERBEROS, Maria,DB, MongoDB, MS SQL, Mysql, Named Pipes, Netezza, Oracle, PostgreSQL, SAP Hana, Sybase, Teradata, WebHDFS or Windows File Share.

fromIP/mask - A list of clients, identified by IP addresses and subnet masks. Separate each IP address from its mask with a slash, and multiple entries by commas. An address and mask of all zeroes is a wild card. If the exclude client list option is Y, the inspection engine monitors traffic from all clients except for those in this list. If the exclude client list option is N, the inspection engine monitors traffic from only the clients in this list.

port - The port or range of ports over which traffic between the specified clients and database servers will be monitored. To specify a range, separate the two numbers with a hyphen.

toIP/mask - The list of database servers, identified by IP addresses and subnet masks, whose traffic will be monitored. Separate each IP address from its mask with a slash, and multiple entries by commas. An address and mask of all zeroes is a wildcard.

exclude client list - A Y/N value; defaults to N. If Y, the inspection engine monitors traffic from all clients except for those identified in the client list. If N, the inspection engine monitors traffic from only the clients listed in the client list.

active on startup - A Y/N value; defaults to N. If Y, the inspection engine is activated on system startup.

delete inspection-engines

Removes the single inspection engine identified by its name. The name can include only letters, numbers and blanks. If the inspection engine name contains any special characters, use the administrator portal GUI to remove it.

Syntax

delete inspection-engines <name>

reorder inspection-engines

Specifies a new order for the inspection engines, using index values from the list produced by the list inspection-engines command.

Syntax

reorder inspection-engines <index>, <index>...

Example

If the displayed indices are 1, 2, 3, and 4, the following command will reverse order of the engines:

reorder inspection-engines 4,3,2,1

restart inspection-core

Restarts the inspection-engine core, but not the inspection engines. The collection of database traffic stops when this command is issued.

Syntax

restart inspection-core

Note: To restart the collection of traffic for one or more specific inspection engines, follow this command with one or more start inspection engine commands. Alternatively, to restart the collection of traffic for all inspection engines, use the restart inspection-engines command.

restart inspection-engines

Restarts the database inspection engine core and all inspection engines. The collection of database traffic stops temporarily while this occurs and restarts only when database connections re-initiate.

Syntax

restart inspection-engines

show inspection-engines

Displays inspection engine configuration information, as follows:

all - All inspection engines.

configuration <index> - Only the inspection engine identified by the specified index, which is from the list inspection-engines command.

type <db_type> -Displays configurations of a specific database type, which must be one of the supported monitored protocol types: Aster, Cassandra, CouchDB, DB2, DB2 Exit, exclude IE, FTP, GreenPlumDB, Hadoop, HIVE, HTTP, HUE, IBM ISERIES, IMPALA, Informix, iNFORMIX Exit, KERBEROS, Maria,DB, MongoDB, MS SQL, Mysql, Named Pipes, Netezza, Oracle, PostgreSQL, SAP Hana, Sybase, Teradata, WebHDFS or Windows File Share.

Syntax

show inspection-engines <all | configuration <index> | log sqlstrings | type <type> >

Note: Use the CLI command, show inspection-engines all, to display non-STAP Inspection Engines like SPAN ports. The CLI command, list_inspection_engines, will display inspection engines created by STAP.

start inspection-core

Starts the inspection-engine core.

Syntax

start inspection-core

start inspection-engines

Starts one or more inspection engines identified using index values from the list produced by the list inspection-engines command.

Syntax

start inspection-engines <all | id>

start inspection-engines all

Starts all the inspection engines.

Syntax

start inspection-engine all

start inspection-engines id

Usage: start inspection-engines id <n>, where n is a numeric sniffer id.

Syntax

start inspection-engines id <n>

stop inspection-engines id

Usage: stop inspection-engines id <n>, where n is a numeric sniffer id.

stop inspection-core

Stops the inspection-engine core.

Syntax

stop inspection-core

stop inspection-engines

Stops one or more inspection engines identified using index values from the list produced by the list inspection-engines command. It can also stop all inspection-engines.

Syntax

stop inspection-engine <all | id>

stop inspection-engines all

Stops all the inspection engines.

Syntax

stop inspection-engines all

stop inspection-engines id

Stops one or more inspection engines identified using index values from the list produced by the list inspection-engines command.

Syntax

stop inspection-engine <n>, where <n> is numeric sniffer id

store ignored port list

Sets the complete set of port numbers to be ignored by all inspection engines. The list you specify completely replaces the existing list. Each number is separated from the next by a comma, and no blanks or other white-space characters are allowed in the list. Use a hyphen to specify an inclusive range of numbers.

Syntax

store ignored port list <n>

Example

store ignored port list 33,60-70

Show Command

show ignored port list

Parent topic: CLI Overview

Investigation Dashboard CLI Commands

Use these CLI commands to configure the Investigation Dashboard .

show solr connection_timeout

Use this command to show the current connection_timeout value.

```
show solr connection_timeout
```

show solr so_timeout

Use this command to show the current so_timeout value.

```
show solr so_timeout
```

show solr time_allowed

Use this command to show the current time_allowed value.

```
show solr time_allowed
```

store solr connection_timeout

Use this command to set the connection timeout. If the Investigation Dashboard cannot connect to the collector within the specified timeout period, no results from that collector will be returned.

```
store solr connection_timeout [value]
```

Parameter	Value	Description
connection_timeout	integer	The timeout is expressed as a value of `0` to `2147483647` milliseconds. The default value is `100000` milliseconds.

store solr so_timeout

Use this command to set the socket timeout.

```
store solr so_timeout [value]
```

Parameter	Value	Description

so_timeout	integer	The timeout is expressed as a value of `0` to `2147483647` milliseconds. The default value is `100000` milliseconds.

store solr time_allowed

Use this command to set the socket timeout.

```
store solr time_allowed [value]
```

Parameter	Value	Description
time_allowed	integer	The timeout is expressed as a value of `0` to `2147483647` milliseconds. The default value is `90000` milliseconds. Note: Deep search uses 10x (ten times) the time_allowed value.

Parent topic: CLI Overview

Network Configuration CLI Commands

Use the network configuration CLI commands to set IP addresses, handle bonding/failover, handle secondary functionality, and reset networking.

Use the network configuration CLI commands to:

- Identify a connector on the back of the machine (show network interface port)
- Reset networking after installing or moving a network card (store network interface inventory)
- Set IP addresses (store network interface ip, store network interface mask, store network resolver, store network routes defaultroute)
- Enable or disable high-availability (store network interface high-availability)
- Configure the network card if the switch it attaches to will not auto-negotiate the settings (store network interface auto-negotiation, store network interface speed, store network interface duplex)

restart network

Restarts just the network configuration. For example, change the IP address, then run this CLI command.

Syntax

restart network

show network interface all

This command shows settings for the network interface used to connect the Guardium® appliance to the desktop LAN. The IP address, mask, state (enabled or disabled) and high availability status will be displayed. If IP high-availability is enabled, the system will display two interfaces (ETH0 and ETH3). Otherwise, only ETH0 will be displayed.

Syntax

show network interface all

show network routes operational

Display the IP routing configuration in use.

Syntax

show network routes operational

Example

CLI> show net rout ope

Kernel IP routing table

Destination Gateway Genmask Flags Metric Ref Use Iface

192.168.3.0 0.0.0.0 255.255.255.0 U 0 0 0 nic1

169.254.0.0 0.0.0.0 255.255.0.0 U 0 0 0 nic2

0.0.0.0 192.168.3.1 0.0.0.0 UG 0 0 0 nic1

ok

CLI>

show network verify

Display the current network configuaration.

Syntax

show network verify

```
CLI> show network verify

Current Network Configuration
-------------------------------------------------------------------------------
Hostname =
-------------------------------------------------------------------------------
Device     | Address          | Netmask          | Gateway          | Member of
-------------------------------------------------------------------------------
eth0       |
-------------------------------------------------------------------------------
Ethtool Options
-------------------------------------------------------------------------------
Device     | Options (speed,autoneg,duplex)
-------------------------------------------------------------------------------
eth0       |
-------------------------------------------------------------------------------
DNS Servers
-------------------------------------------------------------------------------
Index      | DNS Server
-------------------------------------------------------------------------------
1          |
2          |
-------------------------------------------------------------------------------
Static Routes
-------------------------------------------------------------------------------
Device     | Index      | Address          | Netmask          | Gateway
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Basic Network Settings Verified
```

store network interface auto-negotiation

If auto-negotiation is available on the switch to which a Guardium port is connected, auto-negotiation will be used, and only the restart option of this command will have any effect. Use this command to enable, disable, or restart auto-negotiation for the network interface named ethN. Use the show network interface inventory command to display all port names.

Syntax

store network interface auto-negotiation <ethN> <on | off | restart>

Show Command

show network interface auto-negotiation

store network interface duplex

Use this command only when auto-negotiation is not available on the switch to which the Guardium port is connected. This command configures duplex mode for the port named ethn. Use the show network interface inventory command to display all port names.

Syntax

store network interface duplex <ethn> <half | full>

Show Command

show network interface duplex <ethn>

store network interface high-availability

Enables or disables IP Teaming (also known as bonding), which provides a fail-over capability for the Guardium system primary IP address.

The two ports used (ETH0 and a second interface) must be connected to the same network. There is a slight delay, caused by the switch re-learning the port configuration. The default setting is off.

The port used for the primary IP address is always ETH0. When the high-availability option is enabled, the Guardium system automatically fails over, as needed, to the specified second interface, in effect transferring the primary IP address to the second interface.

Note: IP Teaming and Secondary Interface can not done at the same time.
Syntax:

```
store network interface high-availability [on <NIC> | off ]
```

There is no show network interface high-availability command.

store network interface inventory

Resets the network interface MAC addresses stored in the Guardium internal tables. This command should only be used after replacing or moving a network card.

Note: The store network interface inventory command will detect on-board NIC cards within the Guardium appliance and assign these cards as eth0 and eth1. This command should only be run if specifically instructed to by Guardium Support as it can rearrange the NIC cards.

Syntax

```
CLI> > store network interface inventory
WARNING: Running this function will reorder your NICS and may make the machine unreachable.
WARNING: It is suggested to run this from the console or equivalent.
Are you SURE you want to continue? (y/n)
```

Use the show command to display the port names and MAC addresses of all installed network interfaces.

Syntax

show network interface inventory

Example

CLI> show network interface inventory

Current network card configuration:

Device| Mac Address| Member of

eth0| 00:50:56:3b:c3:73|

eth1| 00:50:56:8a:0d:fa|

eth2| 00:50:56:8a:0d:fb|

eth3| 00:50:56:8a:00:c1|

Note: The “Member of” will show which NICs are in the bond pair, if a bonding exists).

store network interface ip

Sets the primary IP address for the Guardium appliance. When changing the network interface IP address, you may also need to change its subnet mask. See store network interface mask. See store network interface secondary to create and manage a secondary IP address. Bonding/failover is managed from the CLI command, store network interface high-availability.

Syntax

store network interface ip <ip address>

Show Command

show network interface ip

store network interface ip6

Sets the primary IP V6 address for the Guardium appliance. When changing the network interface IP address, you may also need to change its subnet mask. See store network interface mask. See store network interface secondary to create and manage a secondary IP address. Bonding/failover is managed from the CLI command, store network interface high-availability.

Syntax

store network interface ip6 <ip address>

Show Command

show network interface ip6

store network interface map

Maps the Ethernet port identified by ethn to the MAC address mac.

Syntax

store network interface map <ethn> <mac>

store network interface mask

Sets the subnet mask for the primary IP address. When changing the network interface mask, you may also need to change its IP address. See store network interface ip. Note that the subnet mask for a secondary IP address can be assigned only from Setup > Tools and Views > System.

Syntax

store network interface mask <ip mask>

store network interface mtu

Use this CLI command to set the MTU (Maximum Transfer Unit).

```
CLI> store network interface mtu
Usage: store network interface mtu <interface> <mtu>]
       where <interface> is the interface name,
       that is one of ( eth0 )
       and <mtu> is number between 1000 and 9000.
```

Show command

show network interface mtu

eth0 1500

show network interface port

Use this command to locate a physical connector on the back of the appliance. After using the *show network interface inventory* command to display all port names, use this command to blink the light on the physical port specified by n (the digit following eth - eth0, eth1, eth2, eth3, etc.) 20 times.

Syntax

show network interface port <n>

Example

CLI> show network interface port 1

The orange light on port eth1 will now blink 20 times.

store network interface remap

Use this CLI command to remap the NIC.

Syntax

store network interface remap

store network interface reset

Use this CLI command to wipe the existing OS network configuration and reapply the stored Guardium network settings.

Syntax

```
CLI> store network interface reset
WARNING: This command will reset the network configuration to the stored Guardium network settings.
Are you SURE you want to continue? (y/n)
```

store network interface secondary

Use this command to configure a port on the Guardium system as a secondary management interface with a different IP address, network mask, and gateway from the primary.

Note: IP Teaming and Secondary Interface can not done at the same time.
Syntax:

```
store network interface secondary [on <NIC> <ip> <mask> <gateway> | off ]
```

Show command

show network interface secondary

store network interface speed

Use this command only when auto-negotiation is not available on the switch to which the Guardium port is connected. This command configures the speed setting for the port named ethn. Use the show network interface inventory command to display all port names.

Syntax

store network interface speed <ethn> <10 | 100 | 1000>

Show Command

show network interface speed <ethn>

show network arp-table

Displays the address resolution protocol (ARP) table, which is an operational system value. This command is provided for support purposes only.

Syntax

show network arp-table

Example

CLI> sho net arp

IP address HW type Flags HW address Mask Device

192.168.3.1 0x1 0x2 00:0E:D7:98:07:7F * nic1

192.168.3.20 0x1 0x2 00:C0:9F:40:33:30 * nic1

ok

CLI>

show network macs

Displays a list of MAC addresses (like the show network interface inventory command).

Syntax

show network macs

Example

Network card configuration:

Device| Mac Address| Member of

eth0| 00:50:56:3b:c3:73|

eth1| 00:50:56:8a:0d:fa|

eth2| 00:50:56:8a:0d:fb|

eth3| 00:50:56:8a:00:c1|

Note: The “Member of” will show which NICs are in the bond pair, if a bonding exists).

ok

store network interface ip6

Usage: store network interface ip <ip>, where IP is a valid IP6 address.

store network resolver

Sets the IP address for the first, second, or third DNS server to be used by the Guardium appliance. Each resolver address must be unique. To remove a DNS server, enter null instead of an IP address.

Syntax

store network resolver <1 | 2 | 3> <ip address | null>

Show Command

show network resolver <1 | 2 | 3>

store network routes defaultroute

Sets the IP address for the default router to the specified value.

Syntax

store network routes defaultroute <ip address>

Show Commands

show network routes defaultroute

store network routes static

Permit the user to have only one IP address per appliance (through eth0) and direct traffic through different routers using static routing tables. Add line to static routing table.

Syntax

store network routes static

Show Command

List the current static routes, with IDs - Device, Index, Address, Netmask, Gateway

show network routes static

Delete command

delete network routes static

store system domain

Sets the system domain name to the specified value.

Syntax

store system domain <value>

Show Command

show system domain

store system hostname

Sets the system's host name to the specified value.

Syntax

store system hostname <value>

Show Command

show system hostname

Parent topic: CLI Overview

Support CLI Commands

The following CLI commands are to be used only with the direction of Technical Support.

These commands are to assist Technical Support in analyzing the status of the machine, troubleshooting common issues and correct some common problems. There are no functions that you would perform with these commands on a regular basis.

support clean audit_results

A way to manually purge audit results, this command should be used only when absolutely necessary to deal with audit tasks that produce a high number of records and take up too much disk space.

It is strongly advised to consult with Technical Support before running this command.

A Warning message is presented and a confirmation step is needed when running this command.

This command will list the audit processes and tasks information.

It will present the number of rows, ordered from the largest result set to the smallest. The number of report results is greater or equal to the input value.

Next, after the report is presented, the user can select a line number to purge the results of the audit process corresponding to that line number. Selection of this line number will delete the audit data for the selected process name.

Syntax

support clean audit_results <rows>

Input parameters

rows - an integer, number of rows to show. Default 10.

Note: On a system with a great many audit tasks, the completion of this command can take some time.

support clean log_files

This CLI command will delete the specified file after user confirms to delete. If it can not find the file, it will list files larger than 10MB in /var/log and the user delete a large file from the list. A warning message is presented and a confirmation step is included.

Syntax

support clean log_file <filename> >> add filename

support clean DAM_data

A way to manually purge database activity monitoring data, this command should be used only when absolutely necessary.

It is strongly advised to consult with Technical Support before running this command.

A Warning message and a confirmation step are included in the command.

Syntax

support clean DAM_data <purge_type> <start_date> <end_date>

Input parameters

purge_type options: agg, exceptions, full_details, msgs, constructs, access, policy_violations, parser_errors, flat_log

start_date: YYYY-mm-dd

end_date: YYYY-mm-dd

support clean centera_files

Guardium archives/backups stored within Centera have a deletion date marker attached to them by Guardium, however there is no subsequent facility to invoke the deletion. Centera does not have a GUI to allow maintenance of its own files, it relies on API invocations from client applications.

Use the CLI command, support clean centera_files, to delete marked files within Centera.

support clean InnoDB-dumps

Use this CLI command to purge InnoDB tables

This is a password protected command (for Technical Support only)

support clean hosts

USAGE: support clean hosts <IP address> <fully qualified domain name>

support clean servlets

Deletes *jsp*.java and *jsp*.class files and restarts GUI.

Use this CLI command to delete generated Java™ servlets and their classes.

support execute

This utility is designed to provide Guardium Advanced Support with the ability to assist with remote diagnostics and support when direct remote access it not available or permitted.

Support Execute is not a replacement for direct remote connections, but will allow Guardium Support at least some level of root access in a secure way without direct access.

The commands provided by Guardium Advanced Support can be SQL statements, O/S Commands, Shell Scripts or SQL scripts. These will then be provided to the customer along with a Secure Key to allow the command to run via CLI. The Secure key is tied to the system that Guardium Support is working with the customer on, and is not valid for any other system. The command can only be run a number of times permitted by Guardium Support and is only valid for seven days from the agreed date.

The feature is disabled by default. Enable via CLI command in both normal and recovery mode:

support execute [enable | disable]

In order to permit the Guardium Advanced Support team to generate a Secure Key, the MAC address of the system in question must be provided for eth0. Here is an example of the interfaces and MAC addresses:

Customer usage / Logged in as CLI

support execute <CMD String> <PMR #> <KEY>

main execute command provided by Guardium Advanced Support

support execute showlog [<Secure Key>|main|files]

Show usage logs

#'<Secure Key>' for full details of single entry

'main' to display the main execute log

'files' to display log directory list

support execute mac

Eth0 MAC address required by support to generate secure key

support execute info

Show eth0 MAC address, root passkey & other system information

support execute version

Display the "Support Execute" internal binary code version

support execute help

Help details and purpose of utility information

Example of command provided by Guardium Advanced Support:

support execute "select * from GDM_ACCESS%5CG" 11111,111,111 6254130c0f0c3c504b33687c57f41363e4c00

support reset-password accessmgr

This command will reset the accessmgr account password.

Syntax

support reset-password accessmgr 10000000-99999999|random

Parameters

8-digit key number used to generate new password. Keep this key number to provide to Technical Support to receive new accessmgr account password. The selection Random will generate a 8-digit random number.

Note: System will attempt to send notification to the accessmgr account email, if it is setup.

support reset-password root

This command will reset root password on the IBM® Guardium® appliance.

Syntax

support reset-password root 10000000-99999999|random

Parameters

8-digit key number used to generate new password. Keep this key number to provide to Technical Support. The choice Random will generate a 8-digit random number.

This command also requires that the user provide a secret keyword in order to change the root password. Contact Technical Support if there is a need to change the root password.

Note: Do not reset root password unless absolutely required by business rules.

support schedule find_crashed_tables

Use this CLI command, support schedule find_crashed_tables [ON/OFF], to enable/disable the daily cron job of find_crashed_tables.sh script.
USAGE: support schedule find_crash_tables on ALL|db
support schedule find_crash_tables off
This command enables or disables daily schedule of find_crashed_tables script.
Note: Pay particular attention to the database entered. Users can enter "ALL" in order to process all five valid databases for crashed tables or just one of the five valid databases "TURBINE", "GDMS", "CUSTOM", "DATAMART or "DIST_INT".

support show db-processlist

This command will list all the db processes sorted by running time.

Syntax

support show db-processlist all

support show db-processlist locked

support show db-processlist running

support show db-process full

Parameters:

support show db-processlist [ ]

Where

running is option to see all running sql statements

all is option to include also sleeping processes

locked is to display all locked and one oldest processes

full [optional] displays sql queries in expended format

support show db-struct-check

This command will display all the structure differences found during aggregation process.

Syntax

support show db-struct-check

support show db-top-tables

This command will list 20 biggest database tables sorted by size and list of tables sorted by used free table space in percents for those tables which use more than 80% free space. It will allow filtering by table name. All table sizes displayed in Mbytes, free space usage in percents.

Syntax

support show db-top-tables all

support show db-top-tables like

Parameters

support show db-top-tables all

will list biggest size tables out of entire DB sorted

support show db-top-tables like

will list biggest tables matching criteria, where could be any portion of the table name

support show db-status

This command will show database usage.

Selections are free, used, megabytes, percentage.

Syntax

support show db-status free %

support show db-status used %

support show db-status free m

support show db-status used m

support show hardware-info

This command uses a script to collect hardware information and place this collected information in a directory for retrieval.

After running this CLI command, the following message will appear:

Collected HW Info as /var/log/guard/Gather_hw_info-2012-06-25-17-43.tgz

Then run the CLI command, fileserver, to retrieve this .tar file from the server.

support show iptables

This command will display the output of system iptables command.

Syntax

support show iptables diff

support show iptables list

Parameters

[diff | list] parameter controlling normal iptables output presentation versus displaying only differences/delta

[accept | full] parameter will filter output by accept row versus not filtered list

support show large_files

This command will list all the files larger than MB and older than days in the /var /tmp /root folders.

Usage

support show large_files

This command will list all the files larger than MB and older than days in the /var /tmp /root folders

Input parameters:

* size - integer > 10 (in MB)

* age - integer >= 0 (in days)

Syntax:

support show large_files <size> <age>

Parameters

support show large_files

where <size> is the minimum size files to display (default 100M)

where <age> is the number of days since the last modification.

support show netstat

This command will display the output of system netstat command. It will allow filtering of the output by content using grep parameter.

Syntax

support show netstat all

support show netstat grep

Parameters

support show netstat grep

where is alphanumeric string to search

support show netstat all

support show port open

This command is similar to using telnet to detect an open TCP port locally or on a remote host.

If we are able to connect successfully you will see a message like: Connection to 127.0.0.1 8443 port [tcp/*] succeeded!

If you are unable to connect you will see a message like: connect to 127.0.0.1 port 1 (tcp) failed: Connection refused

Syntax: support show port open

IP port - IP must be a valid IPv4 address like 127.0.0.1.

Port must be an integer with a value in 1-65535.

support show top

This command will display the output of system top command sorted by cpu, memory or running time. It has configurable number of iterations (default 1) and number of displayed rows (default 10).

Syntax

support show top [cpu | memory | time]

Parameters

support show top cpu

where N is number of iterations in range 1 to 10 and R is number of rows to display - min 10

support show top memory

where N is number of iterations in range 1 to 10 and R is number of rows to display - min 10

support show top time

where N is number of iterations in range 1 to 10 and R is number of rows to display - min 10

support check tables [DB name] [table name}

Invokes mysqlcheck –c command on tables (checks tables for errors).

Without any parameter this command checks all tables in TURBINE database with 3 minutes timeout for each check. Checks are running in parallel, overall time will vary. Command will show progress in percents.If any check runs more than 3 minutes it will be terminated. All tables, whose checks were terminated by timeout, will be listed on the screen after command completion. Any errors occurred during command's operation will be reported to the log file /var/log/guard/<dbname>_check_tables/errors.<date>.log, where <date> is current date and <dbname> is the name of database.

Errors found for each table check operation will be reported in /var/log/guard/<dbname>_check_tables/check_table_child.<tablename>.<date>.log files, where <date> is current date, <dbname> is a name of database and <tablename> is the name of table checked. Files for healthy tables are not created. With dbname specified as the 1st parameter the command will check all tables in the specified DB with the same timeout (3 minutes). With no parameters specified it will check all TURBINE's tables.

With dbname and tablename specified as the parameters the command will check specified table in specified DB without timeout, until the check operation is complete. This is to allow manual checking the tables whose checks didn't finish in 3 minutes. You can use masks in tablename parameter using percent sign (%).

support shrink innodb-size

Use this CLI command to reduce size of ibdata1 file.

It performs the following steps:

- dumps all InnoDB tables
- stops mysql
- deletes ibdata1, ib_logfile0, ib_logfile1 files
- starts mysql
- restores dumped tables

This is a password protected command (for Technical Support only)

support show innodb-status

Use this CLI command to troubleshoot MySQL issues. Use this CLI command to check what is happening at runtime with MySQL tables. Use this CLI command to determine if long check times with MySQL tables are due to record lock or table lock.

```
support show innodb-status
```

0 queries inside InnoDB, 0 queries in queue

0 read views open inside InnoDB

Main thread process no. 7959, id 139923805550336, state: sleeping Number of rows inserted 6894, updated 6934, deleted 93, read 24787 0.33 inserts/s, 0.00 updates/s, 0.00 deletes/s, 0.67 reads/s

---

END OF INNODB MONITOR OUTPUT

support analyze static-table

Use this CLI command to analyze content of static tables by sorting them based on the largest group per value length and value occurrence.

support must_gather commands

There are some simple must_gather commands that can be run by user CLI that generate specific information about the state of any Guardium system. This information can be uploaded from the appliance and sent to Guardium Technical Support whenever a PMR (Problem Management Record) is logged.

In order to run these commands, you will need to have the appropriate must_gather patch installed.

Once the correct patch is installed, the must_gather commands can be run at any time by user CLI as follows.

1. Open a Putty session (or similar) to the Guardium system of concern.
2. Log in as user CLI.
3. Depending on the type of issue you are facing, paste the relevant must_gather commands into the CLI prompt. More than one must_gather command may be needed in order to diagnose the problem.

   support must_gather system_db_info

   support must_gather purge_issues

   support must_gather audit_issues

   support must_gather agg_issues

   support must_gather cm_issues

   support must_gather alert_issues

   support must_gather patch_install_issues

   The following may take a few minutes to run to completion.

   support must_gather miss_dbuser_prog_issues

   support must_gather sniffer_issues

   For the following commands, you will be prompted for a time in minutes for how long you want the debugger running while you reproduce the problem.

   support must_gather backup_issues

   support must_gather scheduler_issues

   Output is written to the must_gather directory with filename(s) along the lines of this example, must_gather/system_logs/.tgz
4. Send the resulting output to IBM Support.

By using fileserver, you can upload the tgz files and send to Support.

Send via email or upload to ECUREP using - for example - the standard data upload specifying the PMR number and file to upload.

Guardium for z/OS traffic diagnostics commands

support store zdiag on [N]

Where optional N is number of minutes to run diagnostics, from 10 to 600, 60 by default

Turns on Guardium for z/OS traffic diagnostics. This includes collection of TCPDUMP and SLON, collections will stop once corresponding files reach 2 GB size. Once completed, results files tcpdump.tar.gz and slon_all.tar.gz can be found via fileserver command. The /var partition must have at least 15GB of free space.

support store zdiag off

Turns off Guardium for z/OS traffic diagnostics. Results files tcpdump.tar.gz and slon_all.tar.gz can be downloaded using the CLI command, fileserver.

support show zdiag

Shows Guardium for z/OS traffic diagnostics status.

SLON Collection Commands

support store slon on [parameter]

Turns on SLON utility that captures packets got by sniffer for debug. Results files slon_packets.tar.gz, slon_messages.tar.gz or slon_all.tar.gz can be found via fileserver. The /var partition must have at least 15GB of free space.

Where optional parameter is:

packets, dump analyzer packets (default)

snifsql, log sniffer SQL activities and dump analyzer packets

secparams, log secure parameters info and dump analyzer packets

sgate, log S-GATE debugging info and dump analyzer packets

messages, tap message data dump

support store slon off [parameter]

Turns off SLON utility. Results files slon_packets.tar.gz, slon_messages.tar.gz or slon_all.tar.gz can be found via fileserver.

Where optional parameter is:

packets, stop dumping packets, logging secure parameters, S-GATE debug info and sniffer SQL activities (default)

messages, stop tapping message data dump

all, stop all activities

support show slon

Shows SLON utility status.

TCPDUMP Collection Command

support store snif_memory_max
Usage: support snif_memory_max <num>, where num is a number of | 33 | 50 | 75 |
This command only applies to 64-bit system.
Show command
support show snif_memory_max

support store tcpdump on <type> <period> <loglimit> [interface] [IP] [port] [protocol]

support store tcpdump on <type> <period> <loglimit> [interface] [IP] [port] [protocol]

Turns on TCPDUMP utility. After period ends, results file tcpdump.tar.gz can be found via fileserver. The /var partition must have at least 15GB of free space.

Where:

<type> - dump type, 'headers' (only headers captured) or 'raw' (whole packets captured)

<period> - dump period, NUMBER[SUFFIX], where optional SUFFIX may be 's' for seconds, 'm' for minutes (default)

<loglimit> - dump logfile limit, from 1 to 6 gigabytes

Optional filter arguments:

[interface] - network interface name (default eth0)

[IP] - IP address

[port] - port

[protocol] - protocol, 'tcp', 'udp', 'ip', 'ip6', 'arp', 'rarp', 'icmp' or

'icmp6'

Example

support store tcpdump on headers 10m 1

This command will run TCPDUMP saving packets headers for 10 minutes and 1GB log file size limit.

support show tcpdump

Shows TCPDUMP utility status.

support store tcpdump off

Turns off TCPDUMP utility. After stop, results file tcpdump.tar.gz can be found via fileserver.

support must_gather datamining_issues

Collects necessary diagnostic information for Outliers, Quick search and Datamart functionality. Information includes dumps of corresponding internal tables, necessary logs, state of corresponding processes and standard must_gather diagnostics (general system and internal DB info).

support must_gather network_issues [--host=<HOST>], where optional parameter <HOST> is hostname or IP address.

The command gathers all network information from the appliance and polls hosts that Guardium interacts with by using ping, traceroute, corresponding port probing and other measures. If the optional parameter is specified, then it polls only the host that was specified (if Guardium is configured to do any activity on this host).

store antlr3_max

Use this CLI command to help control data flow between Parser and Logger The CLI command, store antlr3_max is an advanced parameter geared towards expert users and Customer Support to help control the data flow between Parser and Logger component of the Sniffer for Oracle, DB2, MySql, and MSSql.

This value (default 20,000) will change the number of concurrent parsed SQL statements that the Logger is able to hold in queue.

The issues that this could potentially help remedy are Sniffer running out of memory and restarting, or Sniffer not utilizing enough memory.

If you notice the sniffer is running out of memory and restarting, lowering the context cap may help to alleviate this. Alternatively, if the Sniffer isn't using enough of the available system memory, raising the context cap can allow it to use more.

store active_parser_engine
This CLI command is used to control which parser engine should be used by sniffer. This CLI command is only applicable to database types supported by ANTLR3 parsers (Oracle, DB2, MS SQL, MySQL
USAGE: store active_parser_engine <num>
where <num> is
1: ANTLR3 parser errors reparsed by ANTLR2 (default)

2: ANTLR2 only
3: ANTLR3 only
Show command
show active_parser_engine

Parent topic: CLI Overview

System CLI Commands

Use these CLI commands to configure system settings.

start ecosystem

Use this command to restart the entire set of ecosystem processes. This is necessary after patching, upgrades and some other operations.

Syntax

start ecosystem

stop ecosystem

Use this command to temporarily and gracefully stop the entire set of ecosystem processes. This is necessary for patching, upgrades and some other operations.

Syntax

stop ecosystem

store system apc

Use this command to configure automatic powering down options when a UPS is attached. Note that the UPS must be attached to a USB connector (serial connections for a UPS are not supported).

Sets the minimum charge percent (0-100) before powering down, or the number of seconds to run on battery power before powering down. The defaults are 25 and zero, respectively.

There are also commands to start and stop the apc process. The apc process is disabled by default.

Syntax

store system apc [battery-level <percent> | timeout <seconds>]

store system apc start

store system apc stop

Show Command

show system apc [battery-level | timeout]

store system auditlog-passthrough

Use this command to enable or disable the passing-through of system audit log data from the auditd service to the local syslog. Because the system audit log is verbose, the auditlog-passthrough feature is best used in conjunction with remote logging. See Configuration and Control CLI Commands for more information about remote logging.

The auditlog-passthrough feature is disabled by default.

Syntax: store system auditlog-passthrough [on | off]

Example:

```
> store sys aud on
Restarting auditd service to pick up the change.
Reloading configuration: [ OK ]
Auditd to syslog passthrough is enabled.
ok
```

Show command: show system auditlog-passthrough

store system banner

store system banner [message | clear]

To create a banner (warning about unauthorized access, etc. or a welcome message) at the CLI login, use the CLI command, store system banner [message | clear].

Syntax

store system banner clear - use this CLI command to remove an existing banner message.

store system banner message - use this CLI command to create a banner message. Enter the banner message and then press CTRL-D.

Show command

show system banner - use this CLI command to view an existing banner message.

store system clock datetime

Sets the system clock's date and time to the specified value, where **YYYY** is the year, **mm** is the month, **dd** is the day, **hh** is the hour (in 24-hour format), **mm** is the minutes, and **ss** is the seconds. The seconds portion is required, but will always be set to 00.

Syntax

store system clock datetime <YYYY-mm-dd hh:mm:ss>

Show Command

show system clock <all |datetime |timezone>

Example

store system clock datetime 2008-10-03 12:24:00

store system clock timezone

Lists the allowable time zone value (list option), or sets the time zone for this system to the specified timezone. Use the list option first to display all time zones, and then enter the appropriate timezone from the list.

IBM® Guardium® also logs the local timezone in the standard audit trail, to address cases where data is used in (or aggregated with) data collected in another time zones.

Note: The timezone setting is not updated automatically when Daylight Saving time occurs. In order to update the machine, the user will need to reset the timezone. Reset the timezone means to set a new timezone, different from what currently is, and then resetting to the correct timezone. Just resetting the timezone to the same one will not work and give the message, No change for the timezone.

Syntax

store system clock timezone <list | timezone>

Show Command

show system clock <all | timezone | datetime>

Example

Use the command first with the **list** option to display all time zones. Then enter the command a second time with the appropriate zone.

CLI> store system clock timezone list

Timezone: Description:

--- ---

Africa/Abidjan:

Africa/Accra:

Africa/Addis_Ababa:

...

...output deleted

...

CLI> store system clock timezone America/New_York

store system conntrack

Sets the current status of connection tracking subsystem of the Linux kernel. Status can be ON|OFF.

Syntax

store system conntrack ON|OFF

Show command

show system conntrack

store system cpu profile

Allow configuration of CPU scaling from a CLI command on hardware that supports CPU scaling.

Use this CLI command to set the appropriate CPU scaling policy for your needs:

- conservative = less power usage, conservative scaling
- balanced = medium power usage, fast scale up
- performance = runs the CPU(s) at maximum clock speed

Guardium software sets the scaling policy to Performance upon installation.

Syntax

store system cpu profile [min|perf|max]

Show command

show system cpu profile

store system custom_db_size

Use this CLI command to set the maximum size of the custom database table (in MB). The Default value is 4000 MB.

Syntax

```
CLI> store system custom_db_max_size
USAGE: store system custom_db_max_size <N>
       where N is number larger than 4000.
```

Show command

show system custom_db_size

store system domain

Sets the system domain name to the specified value.

Syntax

store system domain <value>

Show Command

show system domain

store system hostname

Sets the system's host name to the specified value.

Syntax

store system hostname <value>

Show Command

show system hostname

store system issue

store system issue [message | clear]

The CLI command, store system issue message, will receive input from the console until Ctrl-d and write it to /etc/motd after removing from the input any $,\, \followed by single letter, and ` characters. This is a way to enter messages that make this system compliant with the security policies of customers.

The CLI command, store system issue clear, will restore /etc/motd to the default version.

The version comes from /etc/guardium-release. For example, SG70 -> 7.0, SG80 -> 8.0. If the SG is not found in the /etc/guard-release, the default version is an empty string.

store system netfilter-buffer-size

Set the size of the netfilter buffer.

Syntax

store system netfilter-buffer-size

Show command

Displays the S-TAP® netfilter buffer size. 65536 by default.

show system netfilter-buffer-size

show system ntp diagnostics

Use this CLI command to run ntpq -p and ntptime and send the output directly to the screen. The Guardium system queries ntpd from localhost via udp.

Syntax

show system ntp diagnostics

Example

```
CLI> show system ntp diagnostics
Output from ntpq -p :
localhost.localdomain:
-------------------------------------------------------------------
Output from ntptime :
(Note that if you have just started the ntp server, it may report an 'ERROR' until it has synchronized.)
-------------------------------------------------------------------
ntp_gettime() returns code 5 (ERROR)
  time d3443c21.47a46000  Thu, Apr 26 2012 17:26:57.279, (.279852),
```

```
  maximum error 16384000 us, estimated error 16384000 us
ntp_adjtime() returns code 5 (ERROR)
  modes 0x0 (),
  offset 0.000 us, frequency 0.000 ppm, interval 1 s,
  maximum error 16384000 us, estimated error 16384000 us,
  status 0x40 (UNSYNC),
  time constant 2, precision 1.000 us, tolerance 512 ppm,
```

store system ntp [all | server | state]

store system ntp server

Sets the **host name** of up to three NTP (Network Time Protocol) servers. Note that to enable the use of an NTP server, you must use the **store system ntp state on** command. To define a single NTP server, enter its host name or IP address. To define multiple NTP servers, enter the command with no arguments, an you will be prompted to supply the NTP server host names.

Syntax

store system ntp server

USAGE: store system ntp server

For each server enter either ip or hostname

Enter up to 3 NTP servers to store:

Show Command

show system ntp <all |server>

Delete command

delete ntp-server

store system ntp state

Enables or disables use of an NTP (Network Time Protocol) server.

Syntax

store system ntp state <on | off>

Show Command

show system ntp <all |state>

store system patch install

Installs a single patch or multiple patches as a background process. The **ftp** and **scp** options copy a compressed patch file from a network location to the IBM Guardium appliance. Note that a compressed patch file may contain multiple patches, but only one patch can be installed at a time. To install more than one patch, choose all the patches that need to be installed, separated by commas. Internally the CLI will submit requests for each patch on the list (in the order specified by the user) with the first patch taking the request time provided by the user and each subsequent patch three minutes after the previous one. In addition, CLI will check to see if the specified patch(es) are already requested and will not allow duplicate requests.

The last option (sys) is for use when installing a second or subsequent patch from a compressed file that has been copied to the IBM Guardium appliance using this command previously.

To display a complete list of applied patches, see the Installed Patches report on either Manage > Reports > Install Management > Installed Patches, Manage > Maintenance > General > Installed Patches, or Reports > Guardium Operational Reports > Installed Patches.

In **store system patch install** CLI command, user can choose multiple patches from the list.

Syntax

store system patch install <type> <date> <time>

<type> is the installation type, cd | ftp | scp | sys

<date> and <time> are the patch installation request time, date is formatted as YYYY-mm-dd, and time is formatted as hh:mm:ss

If no date and time is entered or if NOW is entered, the installation request time is NOW.

Parameters

Regardless of the option selected, you will be prompted to select a patch to apply:

Please choose one patch to apply (1-n,q to quit):

cd - To install a patch from a CD, insert the CD into the IBM Guardium CD ROM drive before executing this command. A list of patches contained on the CD will be displayed.

tp or **scp -** To install a patch from a compressed patch file located somewhere on the network, use the **ftp** or **scp** option, and respond to the prompts shown. Be sure to supply the full path name for the patch, including the filename:

Host to import patch from:

User on hostname:

Full path to the patch, including name:

Password:

In store system patch install scp CLI command, user can use wildcard * for the patch file name.

The compressed patch file will be copied to the IBM Guardium appliance, and a list of patches contained on file will be displayed.

sys - Use this option to apply a second or subsequent patch from a patch file that has been copied to the IBM Guardium appliance by a previous store system patch execution.

The store system patch install command will not delete the patch file from the IBM Guardium appliance after the install. While there is no real need to remove the patch file, as same patches can be reinstalled over existing patches and keeping patch files around can aid in analyze various problems, a user may remove patch files by hand or use the CLI command diag (Note, the CLI command diag is restricted to certain users and roles.)

To delete a patch install request, use the CLI command delete scheduled-patch

store system public key reset

After generating SSH public keys using CLI commands, show system public key tomcat or show system public key cli, the CLI command, store system public key reset, will delete the SSH keys. If the SSH keys were never generated, this CLI command does nothing. This command asks for confirmation before deletion.

Syntax

store system public key reset

store system remote-root-login

Enable/disable SSH (root access). Secure Shell or SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices.

Syntax

store system remote-root-login ON|OFF

Show command

show system remote-root-login

store system serialtty

In some environments, the serial TTY is not available so it can not ever be started successfully. Potentially this can appear in the system log and be forwarded to SIEM. This is enabled by default to permit connectivity, but can be disabled later if it is determined that serial consoles are unavailable to the system.

Syntax

store system serialtty <on, off>

Show command

show system serialtty

Reports whether or not serial TTYs are enabled on the system.

Reports either:

Serial TTY consoles are enabled on this system.

Serial TTY consoles are disabled on this system.

store system scheduler

Scheduling is managed by a timing mechanism within the IBM Guardium application. If the timing function is disrupted, it will restart after the restart interval designated by this CLI command.

Use store system scheduler restart_interval [5 to 1440 or -1] to restart the timing function after 5 minutes to 1440 minutes. The default is -1 which means the timing restart mechanism is not installed.

Use store system scheduler wait_for_shutdown [ON | OFF] to restart the scheduler after all jobs currently running finish. The parameters are ON or OFF.

Syntax

store system scheduler restart_interval [5 to 1440 or -1]

store system scheduler wait_for_shutdown [ON | OFF]

Show command

show system scheduler

store system shared secret

Sets the system's shared secret value to the specified value. This key must be the same for a Central Manager and all of the appliances it will manage; or an Aggregator, and all of the appliances from which it aggregates data. After an appliance has registered for management by a Central Manager, the shared secret on that unit is no longer used. (You cannot unregister a unit from Central Management by changing this value.)

Dynamic password for aggregator OS user

The aggregator password will be <the current password> concatenated with the shared secret, meaning: password=<current passwd><share secret>

Users will need to make sure the collectors' shared secret and the aggregator's shared secret is exactly the same, otherwise the SCP transfer will fail from the collector to the aggregator (This is a requirement for managed units and aggregators, collectors and aggregators, and export setup screen). The shared secret can be set both from CLI and from the System pane in the Admin Console tab.

Syntax

store system shared secret <key>

store system snif-alerts-facility

This parameter allows the user to configure the facility for snif generated alerts. Previously alerts directly generated by snif would use the user facility while indirect alerts would use the daemon facility (via the guard_sender utility).

Syntax

store system snif-alerts-facility <facility>

USAGE: store snif-alerts-facility <facility>

facility is one of: daemon ftp local0 local1 local2 local3 local4 local5 local6 local7 lpr user

The default facility is daemon.

Show command

show system snif-alerts-facility

store system snif-buffers-reclaim

Use this CLI command only when directed by IBM Guardium Technical Services.

The new configuration will be effective once the CLI command, restart inspection-core, is executed.

Syntax

store system snif-buffers-reclaim [ON | OFF]

Show command

show system snif-buffers-reclaim

store system snif-thread-number

Use this CLI command to specify how many threads are running.

The new configuration will be effective once the CLI command, restart inspection-core, is executed.

Syntax

store system snif-thread-number [new | default]

Show command

show system snif-thread-number

Snif is running with 6 threads on the 32-bit system

store system snmp contact

Stores the email address for the snmp contact (syscontact) for the IBM Guardium appliance. By default it is info@guardium.com.

Syntax

store system snmp contact <email-address>

Show Command

show system snmp contact

store system snmp location

Stores the snmp system location (syslocation) for the IBM Guardium appliance. By default it is Unknown.

Syntax

store system snmp location <string>

Show Command

show system snmp location

store system snmp query community

Stores the snmp system query community for the IBM Guardium appliance. By default it is guardiumsnmp.

Syntax

store system snmp query community <string>

Show Command

show system snmp query community

Parent topic: CLI Overview

User Account, Password and Authentication CLI Commands

Use these CLI commands to configure user accounts, passwords and authentication.

Set guiuser Authentication

When logging on via CLI with one of the default CLI accounts (guardcli1, ...guardcli5), it is required to run the CLI command, set guiuser, before any GuardAPI commands will work. This authentication is required to prevent users with limited roles in the GUI from gaining unauthorized access to GuardAPI commands.

The use of the guardcli1 ... guardcli5 accounts requires the setting of a local password. Use the CLI command, set guisuer, command to reset the guardcli1 ... guardcli5 accounts and then add a local password, as shown in the Syntax.

Certain CLI commands are dependent on the role of the guiuser. For example, the role of the guiuser (marked when creating a new user from accessmgr view) must be accessmgr in order to access grdapi create_user, grdapi set_user_roles, and grdapi update_user

Syntax

set guiuser <gui_user> password <password>

Example

$ ssh guardcli1@a1.corp.com

IBM Security Guardium , Command Line Interface (CLI)

guardcli1@a1.corp.com's password:

Last login: Thu Nov 4 14:56:34 2012 from 123.a1.corp.com

==========

IBM Security Guardium

Unauthorized access is prohibited

==========

a1.corp.com> set guiuser johny_smith password 3wel9s887s

ok

a1.corp.com>

create_user

Examples

>grdapi create_user firstName=john lastName=smith

password=pASSW0rd confirmPassword=pASSW0rd email=jsmith@us.ibm.com

userName=john disabled=0

ID=20000

```
>grdapi set_user_roles userName="john"
roles="dba,diag,cas,user"
```

ID=20000

Added role (dba).

Failed to add role (diag). Diag must have one of these roles: cli or admin.

Added role (cas).

Added role (user).

```
> grdapi set_user_roles userName="john"
roles="dba,diag,cas,user,cli"
```

ID=20000

Added role (dba).

Added role (diag).

Added role (cas).

Added role (user).

Added role (cli).

```
> grdapi update_user userName="john"
email="john.smith@gmail.com"
```

ID=20000

> grdapi list_users

ID=0

####### User 3 #######

Username: accessmgr

First Name: accessmgr

Last Name: accessmgr

Email:

Disabled: false

####### User 1 #######

Username: admin

First Name: admin

Last Name: admin

Email:

Disabled: false

####### User 33 #######

Username: anon

First Name: anon

Last Name: anon

Email:

Disabled: false

####### User 20000 #######

Username: john

First Name: john

Last Name: smith

Email: john.smith@gmail.com

Disabled: false

####### User 2 #######

Username: bill

First Name: bill

Last Name: green

Email:

Disabled: true

set_user_roles

set_user_roles

Each time that you execute a set_user_roles, you reset the roles of a user. You don't append to the roles. You reset.

When you create a user using GrdAPI, it will create the user with user role. Whenyou set the role, you have to specify all of its roles This is done to enable deletion of existing roles and addition of new roles.

Even in GUI, it displays all roles, in which you can either check or uncheck a role and when you save it, it will save everything that you checked.

What GrdAPI does, is to give user kevin only role INV, where any user must have one of these roles: user, cli, admin, or accessmgr

The correct way to call this GrdAPI is:

```
grdapi set_user_roles userName="kevin"  roles="user,inv"
```

Example

> set guiuser accessmgr password ASDFasdf

ok

> grdapi create_user firstName=kevin

lastName=smith password=pASSW0rd confirmPassword=pASSW0rd

email=ksmith@company.com userName=kevin disabled=0

ID=20000

ok

```
> grdapi set_user_roles userName="kevin" roles="inv"
```

set_user_roles:

ERR=3700

User must have one of these roles: user, cli, admin, or accessmgr.

Error executing the command

ok

```
> grdapi set_user_roles userName="kevin"
roles="user,inv"
```

ID=20000

Added role (user).

Failed to add role (inv). Sorry, before assigning the inv role the user's Last Name must be set to the name of one of the three investigation databases -

INV_1, INV_2, or INV_3 (case-sensitive)

ok

```
> grdapi set_user_roles userName="kevin"
roles="dba,diag,cas,user"
```

ID=20000

Added role (dba).

Failed to add role (diag). Diag must have one of these roles: cli or admin.

Added role (cas).

Added role (user).

ok

>

show guiuser

This displays the user (by role) of GUI.

Show command

show guiuser

Password Control Commands

Use the following commands to control user passwords, as follows:

- store password disable - Set the number of days after which an inactive account will be disabled.
- store password expiration - Set the number of days after which a password will expire.
- store password validation - Enable or disable the hardened password validation rules.

Account Lockout Commands

Use the account lockout commands to disable a Guardium® user account after one or more failed login attempts. Use these commands to:

- Enable or disable the feature. See store account lockout.
- Set the maximum number of login failures allowed an account within a given time interval. See store account strike count and store account strike interval.
- Set the maximum number of failures allowed an account for the life of the Guardium appliance. See store account strike max.
- To unlock the admin user account in the event it becomes locked, see the unlock admin command description.

After a Guardium user account has been disabled, it can be enabled from the Guardium portal, and only by users with the accessmgr role, or the admin user.

Example

Enable account lockout, lock an account after 5 login failures within 10 minutes, and set the maximum number of failures allowed to 999.

store account lockout on

store account strike count 5

store account strike interval 10

store account strike max 999

Note:

If the admin user account is locked, use the unlock admin command to unlock it.

If account lockout is enabled, setting the strike count or strike max to zero does NOT disable that type of check. On the contrary, it means that after just one failure the user account will be disabled!

store account lockout

Enables (on) or disables (off) the automatic account lockout feature, which disables a user account after a specified number of login failures.

Syntax

store account lockout <on | off>

Show Command

show account lockout

store account strike count

Sets the number of failed login attempts (n) in the configured strike interval before disabling the account.

Syntax

store account strike count <n>

Show Command

show account strike count

store account strike interval

Sets the number of seconds (n) during which the configured number of failed login attempts must occur in order to disable the account.

Syntax

store account strike interval <n>

Show Command

show account strike interval

store account strike max

Sets the maximum number (n) of failed login attempts to be allowed for an account over the life of the server, before the account is disabled.

Syntax

store account strike max <n>

Show Command

show account strike max

store password disable

Sets the number of days of inactivity, after which user accounts will be disabled. When set to 0 (zero), no accounts will be disabled by inactivity. At installation, the default value is zero. You must restart the GUI after changing this setting (see restart gui).

Syntax

store password disable <days>

Show Command

show password disable

store password expiration

Sets the age (in days) for user password expiration. When set to -1, the password never expires. For GUI users, when set to 0 (zero), the password never expires. For any other value, the account user must reset the password the first time they log in after the current password has expired. The default value is 90. You must restart the GUI after changing this setting.

Syntax

store password expiration cli <days>

store password expiration gui <days>

Show Command

show password expiration

store password validation

Turns password validation on or off. The default value is on. Running this command restarts the GUI to apply this setting.

When password validation is enabled, the password must be eight or more characters in length, and must include at least one uppercase alphabetic character (A-Z), one lowercase alphabetic character (a-z), one digit (0-9), and one special character from the table. When disabled (not recommended), any length or combination of characters is allowed.

Syntax

store password validation <on | off>

Show Command s

show password validation

Table 1. Special Characters for Guardium Passwords

Character	Description
@	Commercial at sign
#	Number sign
$	Dollar sign
%	Percent sign
^	Circumflex accent (carat)
&	Ampersand
.	Full stop (Period)
;	Semicolon
!	Exclamation mark
-	Hyphen (minus)
+	Plus sign
=	Equals sign
_	Low line (underscore)

store user password

Use this command to reset the cli user password. To simplify the support process, we suggest that you keep the cli user password assigned initially by Guardium. There is no way to retrieve the cli user password once it is set. If you lose this password, contact Guardium Support to have it reset.

Syntax

store user password

You will be prompted to enter the current password, and then the new password (twice). None of the password values you enter on the keyboard will display on the screen.

The cli user password requirements differ from the requirements for user passwords. The cli user password must be at least six characters in length, and must contain at least one each of the following types of characters:

- Digits (0-9)
- Lowercase alphabetic characters (a-z)
- Uppercase alphabetic characters (A-Z)

Running this CLI command will also update the change-time record in the password expiration file.

unlock accessmgr

Use this command to enable the Guardium accessmgr user account after it has been disabled. This command does not reset the accessmgr user account password.

Note: Only users with admin role are allowed to run this CLI command.

Syntax

unlock accessmgr

restart gui

unlock admin

Use this command to enable the Guardium admin user account after it has been disabled. This command does not reset the admin user account password.

Note: Only users with admin role are allowed to run this CLI command.

Syntax

unlock admin

restart gui

Authentication commands

The following commands display or control the type of authentication used.

store auth

Use this command to reset the type of authentication used for login to the Guardium appliance, to SQL_GUARD (i.e. Local Guardium authentication, the default).

Optional authentication methods (LDAP or Radius, for example) can be configured and enabled from the administrator portal, but not from the CLI. See Configure Authentication for more information.

Syntax

store auth SQL_GUARD

Show Command

show auth

Parent topic: CLI Overview

GuardAPI Reference

GuardAPI provides access to Guardium® functionality from the command line.

This allows for the automation of repetitive tasks, which is especially valuable in larger implementations. Calling these GuardAPI functions enables a user to quickly perform operations such as create datasources, maintain user hierarchies, or maintain the Guardium features such as S-TAP® just to name a few.

Proper login to the CLI for the purpose of using GuardAPI requires the login with one of the five CLI accounts (guardcli1,...,guardcli5) and an additional login (issuing the 'set guiuser' command) with a user (GUI username/guiuser) that has been created by access manager and given either the admin or cli role. See Set guiuser Authentication for more information.

GuardAPI is a set of CLI commands, all of which begin with the keyword grdapi.

- To list all GuardAPI commands available, enter the grdapi command with no arguments or use the 'grdapi commands' command with no search argument. For example:

```
CLI> grdapi
or
CLI> grdapi commands
```

- To display the parameters for a particular command, enter the command followed by '--help=true'. For example:

```
CLI> grdapi list_entry_location --help=true
ID=0
function parameters :
fileName
hostName - required
path - required
ok
```

- To search for GuardAPI commands given a search string use the CLI command, grdapi commands <search-string>. For example:

```
CLI> grdapi commands user
ID=0
Matching API Function list :
create_db_user_mapping
create_user_hierarchy
delete_allowed_db_by_user
delete_db_user_mapping
delete_user_hierarchy_by_entry_id
delete_user_hierarchy_by_user
execute_appUserTranslation
execute_ldap_user_import
list_allowed_db_by_user
list_db_user_mapping
list_user_hierarchy_by_parent_user
update_user_db
```

- To display a values list for a parameter, enter the command followed by '--get_param_values=<parameter>;'. For example:

```
CLI> grdapi create_group --get_param_values=appid
Value for parameter 'appid' of function 'create_group' must be one of:
Public
Audit Process Builder
Classifier
DB2 zOS Groups
Express Security
IMS zOS Groups
Policy Builder
Security Assessment Builder
```

```
ID=0
ok
```

Table 1. APIs that support the –get_param_values command structure

API Function	Parameter
create_datasource	application, type, severity, shared
create_group	appid, type

Case Sensitivity

Both the keyword and value components of parameters are case sensitive.

Parameter Values with Spaces

If a parameter value contains one or more spaces, it must be enclosed in double quote characters.

For example:

```
grdapi create_datasource type ="MS SQL SERVER" ...
```

NULL Values and Empty Strings

In general, when calling a GuardAPI function and a value for a non-required parameter is not specified or is set to an empty string ("""") GuardAPI will convert that parameter to a NULL value when calling the GuardAPI function. This translates into GuardAPI ignoring the parameter just as if it were not specified.

If, for example, you wanted to clear out a group from a policy rule you instead would set that group to space (" ") and not an empty string (""""). Using an empty string (""""") would signal GuardAPI to ignore that group and not change that group selection.

Example for clearing out a group from a policy value

```
grdapi update_rule fromPolicy=V8 ruleDesc="LogFull Details" dbUserGroup=" " dbUser=" " objectGroup=" " commandsGroup=" "
```

Return Codes

Regardless of the outcome of the GuardAPI command, a return code is always returned in the first line of output, in the following format:

Table 2. Return Codes

Return Code	Description
ID=identifier	Successful. The identifier is the ID of the object operated upon; for example, the ID of a group that has just been defined.
ERR=error_code	Error. The error_code identifies the error, and one or more additional lines provide a text description of the error. There is a table of common errors in the Overview and a complete listing of error codes in GuardAPI Error Codes.

For example, if we use the create_group command to successfully define an objects group named agroup, the ID of that group is returned:

```
CLI> grdapi create_group desc=agroup type=objects appid=Public
ID=20001
ok
CLI>
```

We could use that ID in the list_group_by_id command to display the group definition

```
CLI> grdapi list_group_by_id id=20001
ID=20001
Group GroupId=20001
Group GroupTypeId=3
Group ApplicationId=0
Group GroupDescription=agroup
Group GroupSubtype=null
Group CategoryName=null
Group ClassificationName=null
Group Timestamp=2008-05-10 07:34:11.0
Group type = OBJECTS
Application Type = Public
Touple Group
ok
```

For an unsuccessful execution, an error code is returned. For example, if we enter the list_group_by_id command again with an invalid ID, we receive the following message:

```
a1.corp.com> grdapi list_group_by_id id=20123
ERR=140
Could not retrieve Group - check Id.
ok
```

Common Error Codes

Error codes with a value less than 100 are for common error conditions. Error codes greater than 100 apply to specific functions, and those are described following each function.

To see a complete list of GuardAPI error codes, type grdapi-errors, at the CLI command prompt.

Table 3. Common Error Codes

Error	Description
0	Missing parameters or unknown errors such as unexpected exceptions.
1	An Exception has occurred, please contact Guardium's support
2	Could not retrieve requested function - check function name. To list all functions, type either the CLI command, grdapi, or grdapi commands, with no arguments. To search, by function name, given a search string, use the CLI command, grdapi commands <search-string>
3	Too many arguments. To get the list of parameters for this function call the function --help=true
4	Missing required parameter. To get the list of parameters for this function call the function with --help=true
5	Could not decrypt parameter, check if encrypted with the correct shared secret.
6	Wrong parameter format, specify a function name followed by a list of parameters using <name=value> format.
7	Wrong parameter value for parameter type.
8	Wrong parameter name, please note, parameters are case sensitive.
9	User has insufficient privileges for the requested API function
10	Parameter Encryption not enabled - shared secret not set.
11	Failed sending API call request to targetHost
12	Error Validating Parameter
13	Target host must be the ip address of the central manager
14	Target host is not managed by this manager
15	Target host is not online
16	Target host cannot be specified on a standalone unit
17	User is not allowed to operate on the specified object
18	Target host cannot be specified
19	Missing end quote
20	User is not allowed to run grdapi commands
21	--username and --source-host are grdapi reserved words and cannot be passed on the command line.
22	A parameter name cannot be specified more than once, please check the command line for duplicate parameters.
23	Value not in constant list.
24	Not a valid encrypted value.
25	Not a valid parameter format - parameters should be specified as <name=value>, spaces are not allowed.

GuardAPI Activity Log

The Guardium Activity Log records all grdapi commands that are executed on the system. To view the commands from the administrator portal, navigate to the User Activity Audit Trail report on the Guardium Monitor tab.

All grdapi activity will be attributed to the cli user. Double-click on the cli row in that report, and select the Detailed Guardium User Activity drill-down report. Every command entered will be listed, along with any and all changes made. In addition, the IP address from which the command was issued is listed.

Encrypted Parameter

GuardAPI is intended to be invoked by scripts, which may contain sensitive information, such as passwords for datasources. To ensure that sensitive information is kept encrypted at all times, the grdapi command supports passing of one encrypted parameter to an API Function. This encryption is done using the System Shared Secret which is set by the administrator and can be shared by many systems, and between all units of a central management and/or aggregation cluster; enabling scripts with encrypted parameters to run on machines that have the same shared secret.

Note: Trying to run an API call with encrypted parameter on a system where shared secret was not set results in an error message of

```
Parameter Encryption not enabled - shared secret not set
```

For Guard API scripts generated through the GUI, if encryption is required it is done using the shared secret of the system where script generation is performed.

The optional parameter encryptedParam is available on every grdapi call. This parameter can be used to pass an encrypted value for another parameter.

The procedure for manual encryption is as follows:

1. Use the Parameter Encryption API

   The encrypt_value API accepts a value to encrypt and the target system's shared secret (key) and then prints out the encrypted value. If the key is not the system's shared secret it will print out a warning.

   ```
   a1.corp.com> grdapi encrypt_value --help=true
   ID=0
   function parameters :
   key - required
   valueToEncrypt - required
   api_target_host
   ok
   ```

Table 4. Encrypted Parameter

Parameter	Description
key	The target system's shared secret
valueToEncrypt	The value to be encrypted
api_target_host	In a central management configuration only, allows the user to specify a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
a1.corp.com> grdapi encrypt_value valueToEncrypt="some value" key=guard
ID=0
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.7 (GNU/Linux)
jA0EAgMCTEIUShudn0tgyTB9GL7wR79UL9X9DCAa6RkUQRbegG52olA4gwOzmpHF
0qEhsd6Uz7l8rUsheUyX9v4=
=c1Cq
-----END PGP MESSAGE-----
```

2. Copy the generated content and embed within your cli script.

```
example of cli.gsh  code :
set guiuser johny_smith password 3wel9s887s
 grdapi create_datasource type=oracle name=myOra host=somehost application=AuditTask owner=admin user=sa serviceName=ora
encryptedParam=password
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.7 (GNU/Linux)
jA0EAgMCTEIUShudn0tgyTB9GL7wR79UL9X9DCAa6RkUQRbegG52olA4gwOzmpHF
0qEhsd6Uz7l8rUsheUyX9v4=
=c1Cq
-----END PGP MESSAGE-----
```

3. Run the script to invoke GrdApi:

```
user> ssh cli@a1.corp.comuser> ssh cli@a1.corp.com
```

Central Management Caution

When using GuardAPI in a Central Management environment, be sure that you understand what components are defined on the Central Manager, and what components are defined on managed units. For information on this topic, see Central Management.

Display attributes for certain users in Query Builder

The admin user can see all query attributes in Query Builder and non-admin users can see query attributes in Query Builder, except those that are designed as admin only (IDs, for example).

There are some entities (like FULL SQL) that have large numbers of attributes in them.

By default, all attributes will show up for all users (admin and non-admin).

Two GuardAPI commands have been added to display or not display certain attributes for certain users.

These GuardAPI commands will enable disable/enable ONLY specific groups of attributes in Full SQL: VSAM, ISAM, MApReduce, APEX, Hive and BigInsight.

Two New GuardAPIs named: grdapi enable_special_attributes and grdapi disable_special_attributes

Both receive only one parameter: attributesGroup.

The valid values for this parameter are: VSAM, IMS, MapReduce, APEX, Hive, BI (BigInsights), IMS/VSAM, DB2 i, F5 (Not case sensitive).

Each Grdapi will enable (disable) all the correspondent attributes for the group, for example VSAM will enable (disable) the following attributes:

- VSAM records
- VSAM records delected
- VSAM records inserted
- VSAM records retrieved
- VSAM records updated
- VSAM User Group ID

Hive will enable (disable) the following attributes:

- Hive command
- Hive database
- Hive error
- Hive parsed SQL
- Hive table name
- Hive user

Note: The attributes will still be displayed if the user has the admin role; enabling or disabling these attributes applies ONLY to non-admin users (with no admin role).
Note: The GUI does not have to be restarted for the change to take effect. With this exception: If a report with the attributes of group F5 has been created and added it to My New Reports, even though the attributes have been enabled, the no admin-user does not have the privilege to view the report. The GUI needs to be restarted to see the report fields.

- GuardAPI Archive and Restore Functions
- GuardAPI Assessment Functions
  Use these CLI commands to add, delete and update Assessment Functions.

- GuardAPI Auto-discovery Functions
  Use these CLI commands to create, modify, list and run Auto-discovery Functions.
- GuardAPI Catalog Entry Functions
  Use these GuardAPI commands to create, list, delete, and update Catalog Entry Functions.
- GuardAPI Classification Functions
  Use the following GuardAPI commands for Classification policy configuration, for test automation and, for scripting of prerequisite data preparation.
- GuardAPI Cloud Datasource Functions
  Use this command to define a cloud datasource.
- GuardAPI Database User Functions
  Use these GuardAPI commands to maintain database user mapping, non-credential scan and set debug level.
- GuardAPI Datasource Functions
  Use these GuardAPI commands to create, list, delete, and update Datasource Functions.
- GuardAPI Datasource Reference Functions
  Use these GuardAPI commands to create, list, and delete Datasource Reference Functions.
- GuardAPI Data User Security Functions
  Use these GuardAPI commands to create, list, delete, and update Data User Security Functions.
- GuardAPI Enterprise Load Balancing Functions
  Use these GuardAPI commands to view and set load balancing parameters, view the current load map, and manage S-TAP and managed unit group associations.
- GuardAPI Entitlement Optimization Functions
  Use these GuardAPI commands to enable and configure the Entitlement Optimization datasources and reporting.
- GuardAPI External Feed Functions
  Use these GuardAPI functions to create mappings for external feeds.
- GuardAPI File Activity Monitor Functions
  Use the following GuardAPI commands to enable and disable the file activity monitor, configure the file Investigation Dashboard activity and entitlement extractions schedule, and get information on the file activity monitor.
- GuardAPI GIM Functions
  Use these CLI commands to list, update, assign, remove and cancel GIM Functions.
- GuardAPI Group Functions
  Use these GuardAPI commands to create, list, and delete Datasource Group Functions.
- GuardAPI Input Generation
  GuardAPI Input Generation allows the user to take the output of one Guardium report and feed it as the input for another Guardium entity; allowing users to used prepared calls to quickly call API functionality.
- GuardAPI Investigation Dashboard Functions
  Use these GuardAPI commands to enable, disable, or configure Investigation Dashboard features and parameters.
- GuardAPI Native Audit Functions
  Use these GuardAPI commands to enable, disable, DB Audit (native audit) on a cloud database; add and remove objects from the Object Audit (audit trail); get configuration, collectors and objects.
- GuardAPI Outliers Detection Functions
  Use the following GuardAPI commands to enable, disable, and configure the Outliers Detection function.
- GuardAPI Process Control Functions
  Use these GuardAPI commands to execute, copy, upload, list, and delete Process Control Functions.
- GuardAPI Query Rewrite Functions
  Automate testing or create definitions for certain complex queries that cannot be done from the user interface by using Guardium APIs at the command-line interface.
- GuardAPI Role Functions
  Use these GuardAPI commands to grant, list and revoke Role Functions.
- GuardAPI S-TAP functions
  Use these CLI commands to create, list, delete, restart, and set S-TAP functions.
- GuardAPI Threat Detection Analytics Functions

Parent topic: CLI and API

GuardAPI Archive and Restore Functions

list_expiration_dates_for_restored_days

List the expiration dates for all restored days.

Parameter	Value type	Description
newExpDate	string	Required. The new expiration date for the day restored.
restoredDay	string	Required. Identifies the restore day for data.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

grdapi list_expiration_dates_for_restored_days

get_expiration_date_for_restored_day

Get the expiration date associated with a given restored day.

Parameter	Value type	Description
newExpDate	string	Required. The new expiration date for the day restored.
restoredDay	string	Required. Identifies the restore day for data.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

```
grdapi get_expiration_date_for_restored_day restoredDay=restoredDay
```

where restoredDay can be of the format of a real day `yyyy-mm-dd hh:mi:ss` or relative day such as `NOW -10 day`.

set_expiration_date_for_restored_day

Set the expiration date for a given restored day.

Parameter	Value type	Description
newExpDate	string	Required. The new expiration date for the day restored.
restoredDay	string	Required. Identifies the restore day for data.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

```
grdapi set_expiration_date_for_restored_day newExpDate=newExpDate restoredDay=restoredDay
```

where newExpDate and restoredDay can be of the format of a real day `yyyy-mm-dd hh:mi:ss` or relative day such as `NOW -10 day`.

set_import

Start or stop import of Aggregation data.

Parameter	Value type	Description
state	string	Required. START or STOP
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi set_import [START]
```

configure_export

Configure the export of Aggregation data.

Parameter	Value type	Description
aggHost	String	Required. Host name of Aggregator.
aggSecHost	String	
exportOlderThan	integer	Required. Detail what data to export by time.
exportValues	integer	Required. 0, 1

Parameter	Value type	Description
ignoreOlderThan	integer	Required. Detail what data to ignore by time.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi configure_export [aggHost] [aggSecHost] [exportOlderThan] [exportValues] [ignoreOlderThan]
```

configure_archive

Configure the archive of Aggregation data.

Parameter	Value type	Description
accessKey	string	Shared secret key of Aggregator.
archiveOlderThan	integer	Required. Detail what data to archive by time.
archiveValues	integer	Required. 0 or 1
bucketName	string	

Parameter	Value type	Description
destHost	string	Host name of archive destination.
ignoreOlderThan	integer	Required. Detail what data to ignore by time.
passwd	string	Password
passwdRetype	string	Retype Password
port	integer	Port number
protocol	string	Required. SCP, FTP, or AMAZON
retention	integer	How long to retain.
secretKey	string	
targetDir	string	
userName	string	User name.

Parameter	Value type	Description
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi configure_archive [accessKey] [archiveOlderThan] [archiveValues][bucketName][destHost][ignoreOlderThan][passwd]
[passwdRetype] [port] [protocol] [retention] [secretKey] [targetDir] [userName]
```

Parent topic: GuardAPI Reference

GuardAPI Assessment Functions

Use these CLI commands to add, delete and update Assessment Functions.

Use the following GuardAPI commands to:

- Add, delete, update the Security Assessment definition
- Add, delete a datasource from an existing Security Assessment
- Add, delete tests from an existing Security Assessment

create_assessment

Use this GuardAPI command to add a security assessment.

Table 1. create_assessment

Parameter	Value type	Description
assessmentDescription	string	Required. Free text – unique - must ensure there is no previous assessment with the same description. If there is one, then ERROR.
fromDate		Valid date or relative date. Not mandatory. Default: NOW -1 DAY
toDate		Valid date or relative date. Not mandatory. Default: NOW

Parameter	Value type	Description
FilterClientIP		Valid IP address. Not mandatory. Default null.
FilterServerIP		Valid IP address. Not mandatory. Default null.

Action: If all parameters are validated created a new record in SECURITY_ASSESSMENT table (MODIFIED_FLAG leave default – 0)

Example

```
grdapi create_assessment assessmentDescription=Assess1
```

add_assessment_datasource

Use this GuardAPI command to add a datasource to a security assessment.

Table 2. add_assessment_datasource

Parameter	Value type	Description
assessmentDescription	string	Required. Free text. Unique - must ensure there is no previous assessment with the same description. If there is one, then ERROR.
datasourceName	string	Required. Free Text: Must be the Name of an existing datasource, if such datasource not present, then ERROR

Action: If all parameters are validated then it adds a record to: ASSESSMENT_DATASOURCE using the ASSESSMENT ID and DATASOURCE ID for the assessment and datasource with the names provided.

Example

```
grdapi add_assessment_datasource assessmentDescription=Assess1 datasourceName=DS1
```

add_assessment_test

Use this GuardAPI command to add a test to an existing security assessment.

Parameter	Value type	Description
assessmentDescription	string	Required - Free text – unique - must ensure there is no previous assessment with the same description, if there is one, then ERROR
testDescription	string	Required - Free Text: Must match the TEST_DESC of an existing test in AVAILABLE_TEST , if such test not present, then ERROR

Parameter	Value type	Description
severity	string	Validates against SEVERITY_DESC table (using DESCRIPTION) – Not mandatory. The default value is INFO.
thresholdValue		If Threshold value required from available test = 0, then IGNORE this parameter. Else (THRESHOLD) value required in available_test = 1, then parameter must be an integer If the parameter is not provided, then use DEFAULT_THRESHOLD_VALUE from AVAILABLE_TEST.
exceptionsGroup		Check the value CAN_HAVE_EXCEPTIONS_GROUP in AVAILABLE_TEST. The parameter is NOT mandatory. If 0 then (exceptions group not supported for this test): If the parameter is provided, then ERROR (can not provide exception group for this test); If the parameter is NOT provided, then use -1 to populate. Else (Exception group supported for the test): If the parameter is NOT provided then use -1 to populate; IF the parameter is provided validate the group and use the group ID. To validate the group select from GROUP_DESC where GROUP_DESCRIPTION = the description provided, and check whether the record exist and the GROUP_TYPE_ID If there is not such group ERROR, then exception group does not exists. If there is such group and the GROUP_TYPE_ID != 55, then ERROR: Exception group must be of the type “VA Exceptions” If the group is present and the type = 55, then use the GROUP_ID.

Additional Validation: Check whether there is already a record in ASSESSMENT_TEST for the ASSESSMENT_ID and TEST_ID, if there is such record: ERROR, this test is already present in the assessment can not add it again.

Action: If all parameters validated then add a record to ASSESSMENT_TEST (note SEVERITY must be populated with the DESCRIPTION)

Example

```
grdapi add_assessment_test  assessmentDescription=Assess1 testDescription="The first test"
```

delete_assessment

Use this GuardAPI command to delete a security assessment.

Parameter	Value type	Description
assessmentDescription	string	Required. Free text. Unique. Must ensure there is no previous assessment with the same description, if there is one, then ERROR

Additional Validation: Must ensure there are no results for the assessment to be deleted by:

Select count (*) from ASSESSSMENT_RESULT_HEADER where ASSESSMENT_ID = TheIdToRemve

IF the select returns > 0 then do not remove, ERROR

Action: If the parameter is validated (identifies the security assessment record, and there are no results for the assessment) delete the SECURITY_ASSESSMENT records, THE ASSESSMENT_TEST records and the ASSESSMENT_DATASOURCE records (all three deletes using the ASSESSMENT_ID)

Example

```
grdapi delete_asssessment assessmentDescription=Assess1
```

delete_assessment_datasource

Use this GuardAPI command to delete a datasource from a security assessment.

Parameter	Value type	Description
assessmentDescription	string	Required. Free text – unique - must ensure there is no previous assessment with the same description. If there is one, then ERROR.
datasourceName	string	Required. Free Text: Must be the Name of an existing data-source, if such datasource not present, then ERROR

Action: If all parameters validated, then check whether there is a record in ASSESSMENT_DATASOURCE for the assessment and datasource provided. If no such record Error, otherwise delete the record.

Example

```
grdapi delete_asssessment_datasource assessmentDescription=Assess1 datasourceName=DS1
```

delete_assessment_test

Use this GuardAPI command to delete a test from an existing security assessment

Parameter	Value type	Description
assessmentDescription	string	Required. Free text – unique - must ensure there is no previous assessment with the same description, if there is one then ERROR
testDescription	string	Free Text: Must match the TEST_DESC of an existing test in AVAILABLE_TEST , if such test not present, then ERROR

Additional Validation: Check whether there is a record in ASSESSMENT_TES for the ASSESSMENT_ID and TEST_ID, if there is no such record: ERROR, this test is not present in the assessment

Action: If all parameters validated then delete the record from ASSESSMENT_TEST.

Example

```
grdapi delete_asssessment_test assessmentDescription=Assess1
```

list_assessments

Use this GuardAPI command to list the security assessments.

Parameter	Value type	Description

Parameter	Value type	Description
assessmentDescription	string	Required. Free text – unique - must ensure there is no previous assessment with the same description, if there is one then ERROR

Example

```
grdapi list_assessments
```

list_assessment_tests

Use this GuardAPI command to show the list of tests for the security assessment.

The output of list_available_tests is in the following format: TEST=[<test description>], DS_TYPE=[<datasource type>] (The actual values are encapsulated within the brackets)

The output of list_assessment_tests is in the following format: TEST_DESC=[<available test description>], DS_TYPE=[<datasourcetype>]

The parameters of list_assessment_tests API command are non-mandatory and support filtering.

Parameter	Value type	Validation
assessmentDescription		The API will: • Validate the description is ONE valid assessment description and will retrieve the ID of the assessment. (if there is no assessment, then error) • Show the list of tests for the assessment (and the datasource type). Select AVAILABLE_TEST.TEST_DESC, DATASOURCE_TYPE.NAME from ASSESSMENT_TEST, DATASOURCE_TYPE, AVAILABLE_TEST, SECURITY_ASSESSMENT where AVAILABLE_TEST.DATASOURCE_TYPE_ID = DATASOURCE_TYPE.DATASOURCE_TYPE_ID and ASSESSMENT_TEST.ASSESSMENT_ID = SECURITY_ASSESSMENT.ASSESSMENT_ID and SECURITY_ASSESSMENT.ASSESSMENT_DESC like “Your Param”

Example

```
grdapi list_assessment_tests
```

update_assessment

Use this GuardAPI command to update the record of the security assessment.

Parameter	Value type	Description
assessmentDescription	string	Must match an existing record in SECURITY_ASSESSMENT

Parameter	Value type	Description
newAssessmentDescription	string	Free Text – IF empty, means do not update the description, use the value from the previous parameter, otherwise: unique must ensure there is no previous assessment with the same description, if there is one then ERROR.
fromDate	string	Valid date or relative date
toDate	string	Valid date or relative date
filterContentIP	string	Valid IP address
filterServerIP	string	Valid IP address

Action: If all parameters validated (and there it identified a SECURITY_ASSESSMENT record with the description provided, then update the record with the values provided)

Example

```
grdapi update_assessment assessmentDescription=Assess1 filterClientIP=192.168.1.1.
```

Parent topic: GuardAPI Reference

GuardAPI Auto-discovery Functions

Use these CLI commands to create, modify, list and run Auto-discovery Functions.

add_autodetect_task

This command adds a task to the specified process.

Parameter	Value type	Description
process_name	string	Required. Name of process

Parameter	Value type	Description
hosts_list	string	Required. Lists of hosts. Space separated list of IPs or IP ranges and wild cards such as 192.168.0.1 192.168.1.*
ports_list	string	Required. List of ports. Comma separated list of ports or port ranges such as 22,23,1400-1600
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi add_autodetect_task process_name=myProcess hosts_list="192.168.1.1 192.168.1.3" ports_list="22,23"
```

create_autodetect_process

This command creates an autodetect process.

Parameter	Value type	Description
check_ICMP_echo		Required. PE parameter to nmap (*) . Values are 'true' or 'false'
host_timeout	string	Required. Parameter to nmap (*) . Timeout value.
process_name	string	Required. Name of process
run_probe_after_scan		Required. Values are 'true' or false'.
use_dns		Required. Parameter to nmap[1]. Values are 'R' or 'true' for always, 'n' or 'false' for never.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Note: * nmap options are accessible from API only and not from GUI. For details of nmap parameters and their impact on scan performance see man nmap.

Example

```
grdapi create_autodetect_process process_name=myProcess
```

modify_autodetect_process

This command modifies an autodetect process.

Parameter	Value type	Description
check_ICMP_echo		Required. PE parameter to nmap (*) . Values are 'true' or 'false'
host_timeout	string	Required. Parameter to nmap (*) . Timeout value.
process_name	string	Required. Name of process
run_probe_after_scan		Required. Values are 'true' or false'.
use_dns		Required. Parameter to nmap[1]. Values are 'R' or 'true' for always, 'n' or 'false' for never.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Note: * nmap options are accessible from API only and not from GUI. For details of nmap parameters and their impact on scan performance see man nmap.

Example

```
grdapi modify_autodetect_process process_name=myProcess
```

delete_autodetect_scans_for_process

This command remove all the tasks for a process, but cannot run if a process is running, scheduled or has results.

Parameter	Value type	Description
process_name	string	Required. Name of process

Parameter	Value type	Description
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi delete_autodetect_scans_for_process process_name=myProcess
```

list_autodetect_processes

This command lists all processes.

Parameter	Value type	Description
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi list_autodetect_processes
```

list_autodetect_tasks_for_process

This command lists all tasks of a specified process.

Parameter	Value type	Description
process_name	string	Required. Name of process

Parameter	Value type	Description
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi list_autodetect_tasks_for_process process_name=myProcess
```

execute_autodetect_process

This command runs the specified process, but it cannot run if no tasks are defined for the process or if the process is currently running.

Parameter	Value type	Description
process_name	string	Required. Name of process
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi execute_autodetect_process process_name=myProcess
```

show_autodetect_process_status

This command shows process status and progress summary.

Parameter	Value type	Description
process_name	string	Required. Name of process

Parameter	Value type	Description
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi show_autodetect_process_status process_name=myProcess
```

stop_autodetect_process

This command stops the run of a specific process.

Parameter	Value type	Description
process_name	string	Required. Name of process
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi stop_autodetect_process process_name=myProcess
```

Parent topic: GuardAPI Reference

GuardAPI Catalog Entry Functions

Use these GuardAPI commands to create, list, delete, and update Catalog Entry Functions.

create_entry_location

Adds a new archive entry to the internal catalog location table.

Parameter	Valuetype	Description
entryType	string	Required. Must be one of the following: • CollectorDataArchive • AggDataArchive • AggResultArchive
processDesc	string	Used and required only when the entryType is AggResultArchive.
fileName	string	Required. Identifies the file.
hostName	string	Required. Identifies the host.
path	string	Required. For FTP: specify the directory relative to the FTP account home directory; for SCP: Specify the directory as an absolute path.
user	string	Required. User account to access the host.
password	string	Required. Password for user.
retention	integer	Optional. The number of days this entry is to be kept in the catalog (the default is 365).
storageSystem	string	Required. Must be one of the following: EMC CENTERA, FTP, SCP, TSM.

Parameter	Value type	Description
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi  create_entry_location entryType=CollectorDataArchive  fileName=733392-a1.corp.com-w20071223.133546-d2007-12-27.dbdump.enc
password=somePassword user=someUser path=/var/dump/ hostName=192.168.1.241  storageSystem=scp
```

list_entry_location

Lists one archive location if a fileName is specified, or lists multiple archive locations when the fileName is omitted.

Parameter		Description
fileName	string	Optional. Identifies the single file location to be listed. If omitted, all file locations on the specified hostName and path will be listed.
hostName	string	Required. Identifies the host.
path	string	Required. For FTP: specify the directory relative to the FTP account home directory; for SCP: Specify the directory as an absolute path.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi list_entry_location   path=/mnt/nfs/ogazit/archive_results/ hostName=192.168.1.33
```

delete_entry_location

Updates one archive location if a fileName is specified, or removes multiple archive locations when the fileName is omitted.

Parameter	Value type	Description
fileName	string	Optional. Identifies the single file location to be removed. If omitted, all file locations on the specified hostName and path will be removed.
hostName	string	Required. Identifies the host.
path	string	Required. For FTP: specify the directory relative to the FTP account home directory; for SCP: Specify the directory as an absolute path.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi delete_entry_location  path=/var/dump/mojgan hostName=192.168.1.18
```

update_entry_location

Updates one archive locations if a fileName is specified, or updates multiple archive locations when the fileName is omitted.

Parameter	Value type	Description
fileName	string	Optional. Identifies the single file location to be updated. If omitted, all file locations on the specified hostName and path will be updated.
hostName	string	Required. Identifies the host.
path	string	Required. For FTP: specify the directory relative to the FTP account home directory; for SCP: Specify the directory as an absolute path.

Parameter	Value type	Description
newHostName	string	Optional. When used, specifies the new host name.
newPath	string	Optional. When used, specifies the new path.
user	string	Required. User account to access the host.
password	string	Required. Password for user.
retention	integer	Optional. The number of days this entry is to be kept in the catalog (the default is 365).
storageSystem	string	Optional. Use one of the following: EMC CENTERA, FTP, SCP, TSM.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi update_entry_location  fileName=a1.corp.com-1_4_2008-01-10_10:27:24.res.70.tar.gz.enc path=/mnt/nfs/ogazit/archive_results/
hostName=qaserver    storageSystem=SCP newPath=/var/dump/mojgan  newHostName=192.168.1.18
```

Parent topic: GuardAPI Reference

GuardAPI Classification Functions

Use the following GuardAPI commands for Classification policy configuration, for test automation and, for scripting of prerequisite data preparation.

For instructions on how to use GuardAPI commands, see GuardAPI Reference Overview help topic.

create_classifier_action

Parameter	Value type	Description
actionName	string	Required. String
actualMemberContent	string	Required. String
actionType	string	Required. String For reference, here is the list of action types with the associated required parameters. The required parameters depends on what you choose for the action type. add_to_group_objects actionName - String - required actualMemberContent - String - required objectGroup - String - required policyName - String - required ruleName - String - required add_to_group_object_fields actionName - String - required objectFieldGroup - String - required policyName - String - required ruleName - String - required create_access_rule accessPolicy - String - required accessRuleAction - String - required actionName - String - required ruleName - String - required create_privacy_set actionName - String - required policyName - String - required privacySet - String - required ruleName - String - required log_policy_violation actionName - String - required policyName - String - required ruleName - String - required action_send_alert actionName - String - required policyName - String - required receiver - String - required ruleName - String - required

Parameter	Value type	Description
description	string	
objectGroup	string	Required.
policyName	string	Required.
ruleName	string	Required.
replaceGroupContent	boolean	
objectFieldGroup	string	Required.
accessPolicy	string	Required.
accessPolicy	string	Required.
accessRuleAction	string	Required.
commandsGroup	string	

Parameter	Value type	Description
includeField	boolean	
includeServerIP	boolean	
receiver	string	
privacySet	string	Required.
severity	string	
notificationType	string	
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Examples

```
grdapi create_classifier_action actionType=add_to_group_objects policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc
objectGroup="DW All Objects" replaceGroupContent=1 actualMemberContent=%FULLLIKE

grdapi create_classifier_action actionType=add_to_group_object_fields policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc objectFieldGroup="DW All Object-Field" replaceGroupContent=1

grdapi create_classifier_action actionType=create_access_rule policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc
accessPolicy=pci accessRuleAction="alert daily" commandsGroup="Select command" includeField=1 includeServerIP=0
receiver="syslog,snmp,mail=admin,mail=a b c,custm=-b"

grdapi create_classifier_action actionType=create_privacy_set policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc
privacySet=-b

grdapi create_classifier_action actionType=log_policy_violation policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc
```

```
severity=MED

grdapi create_classifier_action actionType=send_alert policyName=-policy1 ruleName=-rule1 actionName=-action1 description=desc
notificationType=High receiver="syslog,snmp,mail=admin,mail=a b c,custm=-b"
```

GuardAPI command values

See the table for a list of GuardAPI command values for the command, grdapi create_classifer_action that are used in the GUI. Use these values when creating groups.

Table 1. GrdAPI create_classifer_action

GUI values	**GrdAPI values**
%/%.Name	%/NAME
%/Full	%/FULL
Change/%.Name	CHANGE/NAME
Change/Full	CHANGE/FULL
Fully Qualified Name(Schema.Object)	FULLNAME
Like %Full	%FULLLIKE
Like %Full%	%FULLLIKE%
Like %Name	%NAMELIKE
Like %Name%	%NAMELIKE%
Like Full%	FULLLIKE%
Like Name%	NAMELIKE%
Object Name Only	NAMEONLY
Read/%.Name	READ/NAME
Read/Full	READ/FULL

Example

```
grdapi create_classifier_action actionName=classgrpobjectseach1 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent=NAMEONLY description="object type NAMEONLY"
```

Examples of group object types

```
grdapi create_group appid=Classifier type=OBJECTS desc="Classifier Group of Each Objects" owner=admin category=classifier
classification=classifier subtype=classifier

grdapi create_datasource type="Oracle (DataDirect)" user=scott password=tiger host="swan.guard.swg.usma.ibm.com"
name="Swan Oracle Object Each" shared=true owner=admin application=Classifier port=1521 serviceName=on8swan0

grdapi create_classifier_policy policyName="A Group Object Each Type Policy" category="Object Each Process"
classification="Object Each Process"

grdapi create_classifier_rule policyName="A Group Object Each Type Policy" category="Object Each Process"
classification="Object Each Process" ruleName=groupobjects1 ruleType=SEARCH_FOR_DATA dataTypes=TEXT continueOnMatch=1
tableNameLike="EMP_INFORMATION"
columnNameLike="PHONE" tableTypeTable=1

grdapi create_classifier_action actionName=classgrpobjectseach1 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent=NAMEONLY description="object type NAMEONLY"

grdapi create_classifier_action actionName=classgrpobjectseach2 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent=FULLNAME description="object type FULLNAME"

grdapi create_classifier_action actionName=classgrpobjectseach3 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="%NAMELIKE" description="object type %NAMELIKE"

grdapi create_classifier_action actionName=classgrpobjectseach4 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="NAMELIKE%" description="object type NAMELIKE%"

grdapi create_classifier_action actionName=classgrpobjectseach5 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="%NAMELIKE%" description="object type %NAMELIKE%"

grdapi create_classifier_action actionName=classgrpobjectseach6 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="%FULLLIKE" description="object type %FULLLIKE"

grdapi create_classifier_action actionName=classgrpobjectseach7 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="FULLLIKE%" description="object type FULLLIKE%"

grdapi create_classifier_action actionName=classgrpobjectseach8 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="%FULLLIKE%" description="object type %FULLLIKE%"

grdapi create_classifier_action actionName=classgrpobjectseach9 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="Change/Full" description="object type Change/Full"
```

```
grdapi create_classifier_action actionName=classgrpobjectseach10 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="CHANGE/NAME" description="object type Change/%.name"

grdapi create_classifier_action actionName=classgrpobjectseach11 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="Read/Full" description="object type Read/Full"

grdapi create_classifier_action actionName=classgrpobjectseach12 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="READ/NAME" description="object type Read/%.name"

grdapi create_classifier_action actionName=classgrpobjectseach13 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="%/Full" description="object type %/Full"

grdapi create_classifier_action actionName=classgrpobjectseach14 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="%/NAME" description="object type %/%.name"

grdapi create_classifier_process policyName="A Group Object Each Type Policy"
processName="A Group Object Each Type Process" datasourceNames="Swan Oracle Object Each"

grdapi create_classifier_action actionName=classgrpobjectseach10 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="FULLNAME" description="Fully Qualified Name(Schema.Object)
```

create_classifier_policy

Parameter	Value type	Description
category	string	Required.
classification	string	Required.
description	string	
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi create_classifier_policy policyName=-policy1 classification=class1 description=desc1 category=cat1
```

create_classifier_process

create_classifier_process

Note: Create a classification policy and datasource before calling this GuardAPI.

Parameter	Value type	Description
comprehensive	boolean	
datasourceNames	string	Required.
includeInternalTables	boolean	The setting is disabled by default. Enabling includeInternalTables indicates that you want to scan internal system databases and schema used by the database software provider. Internal system databases and schema are unlikely to contain sensitive data and are not scanned by default. When including internal tables, verify that the classifier datasource user has sufficient privileges to scan the internal databases and schema. Insufficient privileges may result in unexpected classification policy errors. To view and edit the databases and schema affected by the includeInternalTables parameter, use the Group Builder to edit one of the predefined Excluded Classification groups.
policyName	string	Required.
processName	string	Required.
sampleSize	integer	
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi create_classifier_process  datasourceNames=sample_cls_0001 policyName=APITEST_Cls_Ply_10001_1
processName=APITEST_Clps_10001_1
```

create_classifier_rule

Parameter	Value type	Description
policyName	string	Required.
ruleName	string	Required.
ruleType	string	Required. For reference, here is the list of valid rule types with the associated required parameters. Depending on what the user selects for the rule type will determine which parameters are required catalog_search_add policyName - String - required ruleName - String - required search_by_permissions_add policyName - String - required ruleName - String - required grantTypes - String - required search_for_data_add policyName - String - required ruleName - String - required search_for_unstructured_data_add policyName - String - required ruleName - String - required
category	string	
classification	string	
continueOnMatch	boolean	
description	string	

Parameter	Value type	Description
columnNameLike	string	
fireOnlyWithMarker	string	
tableNameLike	string	
tableTypeSynonym	boolean	
tableTypeSystemTable	boolean	
tableTypeTable	boolean	
tableTypeView	boolean	
grantTypes	string	
role	string	
roleGroup	string	

Parameter	Value type	Description
user	string	
userGroup	string	
withAdminOption	boolean	
compareToValuesInGroup	string	
compareToValuesInSQL	string	
dataTypes	string	
evaluationName	string	
hitPercentage	integer	
maxLength	integer	
minLength	integer	

Parameter	Value type	Description
searchExpression	string	
searchLike	string	
grantTypes	string	
showUniqueValues	TrueorFalse	
uniqueValueMask	string	
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Examples

```
grdapi create_classifier_rule policyName=-policy1 ruleName=-rule1 category=-cat1 classification=-class1 description=-desc1
ruleType=CATALOG_SEARCH continueOnMatch=1 tableTypeTable=1 tableTypeSynonym=1 tableTypeSystemTable=1 tableTypeView=1
tableNameLike=t1
columnNameLike=c1 fireOnlyWithMarker=m1

grdapi create_classifier_rule policyName=-policy1 ruleName=-rule1 category=-cat1 classification=-class1 description=-desc1
ruleType=SEARCH_BY_PERMISSIONS continueOnMatch=1 tableTypeTable=1 tableTypeSynonym=1 tableTypeSystemTable=1 tableTypeView=1
user=user1
userGroup="suspicious users" role=role1 roleGroup=-role1 withAdminOption=1 grantTypes=CONTROL,DELETE,DROP fireOnlyWithMarker=m1

grdapi create_classifier_rule policyName=-policy1 ruleName=-rule1 category=-cat1 classification=-class1 description=-desc1
ruleType=SEARCH_FOR_DATA continueOnMatch=1 tableTypeSynonym=1 tableNameLike=tl1 dataTypes=DATE,NUMBER,TEXT columnNameLike=cl1
minLength=11 searchLike=sel1 searchExpression=se1 evaluationName=en1 hitPercentage=44 compareToValuesInSQL=cv1sql
compareToValuesInGroup="dw all objects" fireOnlyWithMarker=m1

grdapi create_classifier_rule policyName=-policy1 ruleName=-rule1 category=-cat1 classification=-class1 description=-desc1
ruleType=SEARCH_FOR_UNSTRUCTURED_DATA continueOnMatch=1 searchLike=s1 searchExpression=e1 fireOnlyWithMarker=m1

grdapi create_datasource type="Oracle (DataDirect)" user=scott password=tiger host="swan.guard.swg.usma.ibm.com"
name="Swan Oracle8 all values" shared=true owner=admin application=Classifier port=1521 serviceName=on8swan0

grdapi create_group appid=Classifier type=OBJECTS desc="AA Classifier ALL Values" owner=admin category=classifier
classification=classifier subtype=classifier
```

```
grdapi create_member_to_group_by_desc desc="AA Classifier ALL Values" member=ACCOUNTING

grdapi create_member_to_group_by_desc desc="AA Classifier ALL Values" member=ACCOUNTTING

grdapi create_member_to_group_by_desc desc="AA Classifier ALL Values" member=ACCOUNTTING

grdapi create_member_to_group_by_desc desc="AA Classifier ALL Values" member=AG

grdapi create_classifier_policy policyName="Search ALL DATA SEARCH smoke values" category="ALL" classification="ALL"

grdapi create_classifier_rule policyName="Search ALL DATA SEARCH smoke values" category="ALL" classification=ALL
ruleName=ALL1 ruleType=SEARCH_FOR_DATA dataTypes=TEXT,NUMBER continueOnMatch=1 tableNameLike="DEPT14%" minLength=1 maxLength=100
tableTypeSynonym=1 tableTypeSystemTable=1 tableTypeTable=1 tableTypeView=1 fireOnlyWithMarker=ACCT searchLike="A%"
searchExpression="^AA*" columnNameLike="DNAME" evaluationName="com.guardium.classifier.custom.RichardEvaluation" hitPercentage=10
compareToValuesInGroup="AA Classifier ALL Values" compareToValuesInSQL="select DNAME from SCOTT.DEPT where DNAME like 'A%G'"
showUniqueValues="true" uniqueValueMask="^AA*"

grdapi create_classifier_process policyName="Search ALL DATA SEARCH smoke values"
processName="Search ALL DATA SEARCH smoke values Process" datasourceNames="Swan Oracle8 all values"
```

delete_classifier_action

Parameter	Value type	Description
actionName	string	Required.
policyName	string	Required.

Example

```
grdapi delete_classifier_action policyName=-policy1 ruleName=-rule1 actionName=-action1
```

delete_classifier_policy

Parameter	Value type	Description
policyName	string	Required.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi delete_classifier_policy policyName=-policy1
```

delete_classifier_process

Parameter	Value type	Description
processName	string	
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

example

```
grdapi delete_classifier_process processName=APITEST_Clps_10001_1
```

delete_classifier_rule

Parameter	Value type	Description
policyName	string	Required.
ruleName	string	Required.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi delete_classifier_rule policyName=-policy1 ruleName=-rule1
```

execute_cls_process

Execute (submit) a classification process

Runs a classification process. It is equivalent of executing Run Once Now from Classification Process Builder. It submits the job which places the process on the Guardium® Job Queue, from which the appliance runs a single job at a time. Administrators can view the job status by selecting Guardium Monitor > Guardium Job Queue. Note: Create a classification process before calling this API.

Parameter	Value type	Description
processName	string	Name of the classification process
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi execute_cls_process processName="classPolicy1"
```

Here is a list of the classifier functions and the parameters for each. In the case where the parameter will have a set list of valid entries, the list will be supplied.

list_classifier_policies

Parameter	Value type	Description
policyName	string	Required.
ruleName	string	Required.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi list_classifier_policy policyName=-policy1 ruleName=-rule1 actionName=-action1 recursive=1
```

Note: Executing this function with no arguments will list all policies. Passing an argument for the policy will list all rules and actions for the policy. Passing a policy and rule will list all of the actions for the rule.

list_classifier_process

Parameter	Value type	Description
processName	string	
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

example:

grdapi list_classifier_process processName=APITEST_CLPS_30001

set_classification_concurrency_limit

The set_classification_concurrency_limit command defines the number of classifier processes that can run concurrently.
Syntax: grdapi set_classification_concurrency_limit limit=[value].

Parameter	Value type	Description
limit	Integer: 1-100, depending on the hardw	The limit value defines the number of classifier processes that can run concurrently. The limit value is the lesser of 100 or twice the number of CPU cores installed on the Guardium system. For example, if a system has 8 CPU cores, the maximum limit value is 16. If a system has 64 CPU cores, the maximum limit value is 100. The default limit value is 1.

Parameter	Value type	Description
	a reconfiguration of the Guardium system. The default value is 1.	

Example:

```
grdapi set_classification_concurrency_limit limit=11
```

Show values: grdapi get_classification_concurrency_limit

update_classifier_action

Parameter	Valuetype	Description
actionName	string	Required.
actualMemberContent	string	Required.
description	string	
objectGroup	string	Required.
policyName	string	Required.
ruleName	string	Required. String
replaceGroupContent	boolean	
objectFieldGroup	string	Required.
accessPolicy	string	Required.
accessRuleAction	string	Required.

Parameter	Value type	Description
commandsGroup	string	
includeField	boolean	
includeServerIP	boolean	
receiver	string	
privacySet	string	Required.
severity	string	
notificationType	string	
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi update_classifier_action actionType=add_to_group_objects policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc objectGroup="DW All Objects" replaceGroupContent=1 actualMemberContent=%FULLLIKE

grdapi update_classifier_action actionType=add_to_group_object_fields policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc objectFieldGroup="DW All Object-Field" replaceGroupContent=1

grdapi update_classifier_action actionType=update_access_rule policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc accessPolicy=pci accessRuleAction="alert daily" commandsGroup="Select command" includeField=1 includeServerIP=0
receiver="syslog,snmp,mail=admin,mail=a b c,custm=-b"
```

```
grdapi update_classifier_action actionType=update_privacy_set policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc privacySet=-b

grdapi update_classifier_action actionType=log_policy_violation policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc severity=MED

grdapi update_classifier_action actionType=send_alert policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc notificationType=High receiver="syslog,snmp,mail=admin,mail=a b c,custm=-b"
```

update_classifier_policy

Parameter	Value type	Description
policyName	string	Required
category	string	Required
classification	string	Required
description	string	
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi update_classifier_policy policyName=-policy1 classification=class1 description=desc1 category=cat1
```

update_classifier_process

update_classifier_process

Parameter	Value type	Description

Parameter	Value type	Description
comprehensive	boolean	
datasourceNames	string	Required.
includeInternalTables		The setting is disabled by default. Enabling includeInternalTables indicates that you want to scan internal system databases and schema used by the database software provider. Internal system databases and schema are unlikely to contain sensitive data and are not scanned by default. When including internal tables, verify that the classifier datasource user has sufficient privileges to scan the internal databases and schema. Insufficient privileges may result in unexpected classification policy errors. To view and edit the databases and schema affected by the includeInternalTables parameter, use the Group Builder to edit one of the predefined Excluded Classification groups.
newName	string	
policyName	string	Required
processName	string	Required
sampleSize	integer	
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

grdapi update_classifier_process datasourceNames=sample_cls_0001,sample_cls_0002 policyName=APITEST_Cls_Ply_10001_1 processName=APITEST_Clps_10001_1 comprehensive=0 sampleSize=3000

update_classifier_rule

Parameter	Value type	Description
policyName	string	Required
ruleName	string	Required
ruleType	string	Required. Values: catalog_search search_by_permissions search_for_data search_for_unstructured_data
category	string	
classification	string	
continueOnMatch	boolean	
description	string	
columnNameLike	string	
fireOnlyWithMarker	string	
tableNameLike	string	

Parameter	Value type	Description
tableTypeSynonym	boolean	
tableTypeSystemTable	boolean	
tableTypeTable	boolean	
tableTypeView	boolean	
grantTypes	string	
role	string	
roleGroup	string	
user	string	
userGroup	string	
withAdminOption	boolean	

Parameter	Value type	Description
compareToValuesInGroup	string	
compareToValuesInSQL	string	
dataTypes	string	
evaluationName	string	
hitPercentage	integer	
maxLength	integer	
minLength	integer	
searchExpression	string	
searchLike	string	

Parameter	Value type	Description
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Examples

```
grdapi update_classifier_rule policyName=-policy1 ruleName=-rule1 category=-cat1 classification=-class1 description=-desc1
ruleType=CATALOG_SEARCH continueOnMatch=1 tableTypeTable=1 tableTypeSynonym=1 tableTypeSystemTable=1 tableTypeView=1
tableNameLike=t1
columnNameLike=c1 fireOnlyWithMarker=m1

grdapi update_classifier_rule policyName=-policy1 ruleName=-rule1 category=-cat1 classification=-class1 description=-desc1
ruleType=SEARCH_BY_PERMISSIONS continueOnMatch=1 tableTypeTable=1 tableTypeSynonym=1 tableTypeSystemTable=1 tableTypeView=1
user=user1
userGroup="suspicious users" role=role1 roleGroup=-role1 withAdminOption=1 grantTypes=CONTROL,DELETE,DROP fireOnlyWithMarker=m1

grdapi update_classifier_rule policyName=-policy1 ruleName=-rule1 category=-cat1 classification=-class1 description=-desc1
ruleType=SEARCH_FOR_DATA continueOnMatch=1 tableTypeSynonym=1 tableNameLike=tl1 dataTypes=DATE,NUMBER,TEXT columnNameLike=cl1
minLength=11
maxLength=22 searchLike=sel1 searchExpression=se1 evaluationName=en1 hitPercentage=44 compareToValuesInSQL=cv1sql
compareToValuesInGroup="dw all objects" fireOnlyWithMarker=m1

grdapi update_classifier_rule policyName=-policy1 ruleName=-rule1 category=-cat1 classification=-class1 description=-desc1
ruleType=SEARCH_FOR_UNSTRUCTURED_DATA continueOnMatch=1 searchLike=s1 searchExpression=e1 fireOnlyWithMarker=m1
```

Parent topic: GuardAPI Reference

GuardAPI Cloud Datasource Functions

Use this command to define a cloud datasource.

create_cloud_datasource

Parameter	Value type	Description
application	String. See description	Required. The application for which the datasource is being defined. One of the following: Access Policy Application User Translation Audit Task Change Audit System Classifier Custom Domain Database Analyzer Monitor Values Security Assessment Stap Verification
cloudTitle	string. see Description	Required. Name of cloud account already defined in Guardium
compatibilityMode	String	The mode used when monitoring a table.
conProperty	String	Optional. Use only if additional connection properties must be included on the JDBC URL to establish a JDBC connection with this datasource. The required format is property=value, where each property and value pair is separated from the next by a comma.
customURL	String	Optional. Connection string to the datasource; otherwise connection is made using host, port, instance, properties, etc. of the previously entered fields. This is useful, for example, when creating Oracle Internet Directory (OID) connections.
dbInstanceAccount	String	Optional. Database Account Login Name that is used by CAS
dbInstanceDirectory	String	Optional. Directory where database software was installed is used by CAS
dbName	String	Optional. For a DB2® or Oracle datasource, enter the schema name. For others, enter the database name.
description	String	Optional. Longer description of the datasource.

Parameter	Value type	Description
host	String	Required. The host name or the IP address.
importServerSSLcert	Boolean	
KerberosConfigName	String	Optional. Name of Kerberos configuration already defined in Guardium system
name	String	Required. A unique name for the datasource in the Guardium system
objectLimit	0, positive integer	Required. The maximum number of sensitive objects found in the classification process that are added automatically to the list of audited objects. Default = 20.
password	string	Password for user.
port	Integer	Optional. Port number.
primaryCollector	Integer	The collector that extracts the audit data from the cloud database.
region	value list	Required.
savePassword	Boolean	Saves and encrypts your authentication credentials on the Guardium appliance. Required if you are defining a datasource with an application that runs as a scheduled task (as opposed to on demand). When set to yes, login name and password are required.
serviceName	String	Optional. Required for Oracle, Informix®, DB2, and IBM® ISeries. For a DB2 datasource enter the database name, for others enter the service name.
severity	value list	Optional. Severity Classification (or impact level) for the datasource. One of: LOW NONE MED HIGH
shared	value list	Optional. Set to **True** or **Share** to share with other applications. To share the datasource with other users, you will have to assign roles from the GUI. Values: Share Not Shared True False
type	value list	Required. Identifies the datasource type. Valid values: Oracle (DataDirect - SID) Oracle (DataDirect - Service Name)
useKerberos	Boolean	Optional (boolean). Set to yes to use Kerberos authentication. If yes, KerberosConfigName must be supplied.
useLDAP	Boolean	Optional (boolean). Set to yes to use LDAP
user	String	Optional. User for the datasource. If used, password must also be used.
useSSL	Boolean	Optional (boolean). Set to yes to use SSL authentication.

list_cloud_datasource_by_name

Parameter	Value type	Description
name	string	Required. Cloud datasource defined in Guardium.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM

restart_cloud_instance

Restarts the specified cloud instance.

Parameter	Value type	Description
datasource_name	string	Required. Cloud datasource defined in Guardium.

Parameter	Value type	Description
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM

update_cloud_datasource

Updates the cloud datasource configuration.

Parameter	Value type	Description
cloudTitle	value list	Required. Title define by GRDAPI command
conProperty	String	Optional. Use only if additional connection properties must be included on the JDBC URL to establish a JDBC connection with this datasource. The required format is property=value, where each property and value pair is separated from the next by a comma.
customURL	String	Optional. Connection string to the datasource; otherwise connection is made using host, port, instance, properties, etc. of the previously entered fields. This is useful, for example, when creating Oracle Internet Directory (OID) connections.
dbInstanceAccount	String	Optional. Database Account Login Name that is used by CAS
dbInstanceDirectory	String	Optional. Directory where database software was installed that will be used by CAS
dbName	String	Optional. For a DB2® or Oracle datasource, enter the schema name. For others, enter the database name.
description	String	Optional. Longer description of the datasource.
host	String	Required. The host name or the IP address.
importServerSSLcert	Boolean	
KerberosConfigName	String	Name of Kerberos configuration already defined in Guardium system
name	String	Required. A unique name for the datasource in the Guardium system
newName	String	Optional. Provides a new name, which must be unique for a datasource on the system.
objectLimit	integer: 0 and higher	Required. The maximum number of sensitive objects found in the classification process that are added automatically to the list of audited objects.
password	String	Password for user
port	Integer	Cloud datasource defined in Guardium.
primaryCollector	Integer	Collector that receives data from cloud DB
region	value list	Required.
savePassword	Boolean	Saves and encrypts your authentication credentials on the Guardium appliance. Required if you are defining a datasource with an application that runs as a scheduled task (as opposed to on demand). When set to yes, login name and password are required.
serviceName	String	Optional. Required for Oracle, Informix®, DB2, and IBM® ISeries. For a DB2 datasource enter the database name, for others enter the service name.
severity	value list	Optional. Severity Classification (or impact level) for the datasource. One of: LOW NONE MED HIGH
shared	value list	Optional. Set to **True** or **Share** to share with other applications. To share the datasource with other users, you will have to assign roles from the GUI. Values: Share Not Shared True False
useKerberos	Boolean	Optional (boolean). Set to yes to use Kerberos authentication. If yes, KerberosConfigName must be supplied.
useLDAP	Boolean	Optional (boolean). Set to yes to use LDAP
user	String	Optional. User for the datasource. If used, password must also be used.
useSSL	Boolean	Optional (boolean). Set to yes to use SSL authentication.

Parent topic: GuardAPI Reference

GuardAPI Database User Functions

Use these GuardAPI commands to maintain database user mapping, non-credential scan and set debug level.

non_credential_scan

API that allows for submitting jobs that will scan databases within the serversGroup for enabled default users in the usersGroup. Submitted jobs will run under the Classifier Listener and may be tracked using the Classifier/Assessment Job Queue report. A submitted job may be canceled from the Classifier/Assessment Job Queue report by double-clicking on the job and choosing Stop Job.

Note: If a server within the serversGroup can not be reached, an exception of type Scheduled Job Exception is added and the serveris not scanned.

Parameter	Value type	Description
databaseType	valuelist	Required. Must be one of the following: ORACLE, DB2®, SYBASE, MS SQL SERVER, MYSQL, TERADATA, POSTGRESQL, NETEZZA, IBM ISERIES, INFORMIX
serversGroup	valuelist	Required. Must be a valid group of servers (Server IP/Instance Name/Port) as defined with Group Builder.
usersGroup	valuelist	Required. Must be a valid group of users (DB User/DB Password) as defined with Group Builder. Default groups exist within Group Builder.

Example

```
grdapi non_credential_scan databaseType=ORACLE serversGroup=oracleServers usersGroup="ORACLE Default Users"
```

Maintain Database Mapping

These APIs help maintain the mapping between database users (Invokers of SQL that caused a violation) and email addresses for real time alerts. See Alerting Actions for more information on Invokers.

- create_db_user_mapping
- delete_db_user_mapping
- list_db_user_mapping

create_db_user_mapping

Use of wildcards:

- In the 'delete' and the 'list' commands, all 4 parameters accept wildcards ('%')
- 'create' command:
  - serverIp - wildcard is valid, '%' can be placed instead of the number in the ip_address format
  - 192.168.2.% - valid
  - 192.%.2.% - valid
  - 192.% - invalid
- serviceName - wildcards (%) are allowed
- dbUserName - no wildcards, '%' is valid, but will be considered as the symbol '%'
- emailAddress - no wildcards, '%' is valid, but will be considered as the symbol '%'

Parameter	Value type	Description
serverIp	string (IPAddress)	Required. Format: IP address as A.B.C.D
serviceName	string	Required. Identifies the service name.
dbUserName	string	Required (any string). Identifies the database user name.
emailAddress	string	Required (any string and requires an '@' sign). Identifies the email address.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi create_db_user_mapping serverIp=192.168.1.104 serviceName=ora1 dbUserName=scott emailAddress=scott@oracle.com
```

delete_db_user_mapping

Use of wildcards:

- In the 'delete' and the 'list' commands, all 4 parameters accept wildcards ('%')
- 'create' command:
  - serverIp - wildcard is valid, '%' can be placed instead of the number in the ip_address format
  - 192.168.2.% - valid
  - 192.%.2.% - valid
  - 192.% - invalid
- serviceName - wildcards (%) are allowed
- dbUserName - no wildcards, '%' is valid, but will be considered as the symbol '%'
- emailAddress - no wildcards, '%' is valid, but will be considered as the symbol '%'

Parameter	Value type	Description
serverIp	string (IPAddress)	Required. Format: IP address as A.B.C.D
serviceName	string	Required. Identifies the service name.
dbUserName	string	Required. Identifies the database user name.
emailAddress	string	Required (any string and requires an '@' sign). Identifies the email address.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi create_db_user_mapping serverIp=192.168.1.104 serviceName=ora1 dbUserName=scott emailAddress=scott@oracle.com
```

list_db_user_mapping

Use of wildcards:

- In the 'delete' and the 'list' commands, all 4 parameters accept wildcards ('%')
- 'create' command:
  - serverIp - wildcard is valid, '%' can be placed instead of the number in the ip_address format
  - 192.168.2.% - valid
  - 192.%.2.% - valid
  - 192.% - invalid
- serviceName - wildcards (%) are allowed
- dbUserName - no wildcards, '%' is valid, but will be considered as the symbol '%'
- emailAddress - no wildcards, '%' is valid, but will be considered as the symbol '%'

Parameter	Value type	Description
serverIp	string (IPAddress)	Required. Format: IP address as A.B.C.D
serviceName	string	Required. Identifies the service name.
dbUserName	string	Required (any string). Identifies the database user name.
emailAddress	string	Required (any string and requires an '@' sign). Identifies the email address.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi create_db_user_mapping serverIp=192.168.1.104 serviceName=ora1 dbUserName=scott emailAddress=scott@oracle.com
```

get debug level

Use this GuardAPI command to view the debug level for IMS™ output.

set_debug_level

Use this GuardAPI command to control IMS output.

If the IMS debug_level = 1, IMS debug fields like mvs_is_plex, mvs_ipaddr, mvs_dlta_sign, mvs_dlta_val output to internal database tables, GDM_CONSTRUCT_TEXT.FULL_SQL or GDM_EXCEPTION.FULL_SQL.

If the IMS debug level is 0, then the IMS debug fields are not distributed.

Parent topic: GuardAPI Reference

GuardAPI Datasource Functions

Use these GuardAPI commands to create, list, delete, and update Datasource Functions.

create_datasource

Use this command to define a new datasource.

Note: In a Central Manager environment, datasources are defined on the Central Manager. GuardAPI will allow you to create datasources on a managed unit, but those datasources cannot be seen or used.

To create Cloud datasources, refer to GuardAPI Cloud Datasource Functions.

Parameter	Value type	Description
application	value list	Required. Identifies the application for which the datasource is being defined. It must be one of the following: Access_policy Application User translation AuditDatabase AuditTask ChangeAuditSystem Classifier CustomDomain DatabaseAnalyzer MonitorValues SecurityAssessment Stap_Verification
compatibilityMode		Compatibility Mode: Choices are Default or MSSQL 2000. The processor is told what compatibility mode to use when monitoring a table.
conProperty	comma separated list of property=value	Optional. Use only if additional connection properties must be included on the JDBC URL to establish a JDBC connection with this datasource. For a Sybase database with a default character set of Roman8, enter the following property: charSet=utf8
customURL		Optional. Connection string to the datasource; otherwise connection is made using host, port, instance, properties, etc. of the previously entered fields. As an example this is useful for creating Oracle Internet Directory (OID) connections.

Parameter	Value type	Description
dbInstanceAccount	string	Optional. Database Account Login Name that will be used by CAS
dbInstanceDirectory	string	Optional. Directory where database software was installed that will be used by CAS
dbName	string	Optional. For a DB2® or Oracle datasource, enter the schema name. For others, enter the database name.
description	string	Optional. Longer description of the datasource.
host	string	Required. Can be the host name or the IP address.
KerberosConfigName	string	Optional. Name of Kerberos configuration already defined in Guardium system
name	string	Required. Provides a unique name for the datasource on the system.
password	string	Optional. Password for user.
port	integer	Optional. Port number.
savePassword	boolean	Saves and encrypts your authentication credentials on the Guardium appliance. Required if you are defining a datasource with an application that runs as a scheduled task (as opposed to on demand). When set to yes, login name and password are required.

Parameter	Value type	Description
serviceName	string	Required for Oracle, Informix®, DB2, and IBM® ISeries. For a DB2 datasource enter the database name, for others enter the service name.
severity		Optional. Severity Classification (or impact level) for the datasource.
shared	boolean	Optional. Set to **true** to share with other applications. To share the datasource with other users, you will have to assign roles from the GUI.
type	valuelist	Required. Identifies the datasource type. Valid values: DB2 DB2 for i DB2 for z/OS Informix MS SQL Server MS SQL Server (DataDirect) MySQL NA Netezza Oracle (DataDirect) Oracle (Service Name) Oracle (SID) PostgreSQL Sybase Sybase IQ Teradata The following can be used when the application is CustomDomain or Classifier: TEXT TEXT:FTP TEXT:HTTP TEXT:HTTPS TEXT:SAMBA
useKerberos	boolean	Optional. Set to yes to use Kerberos authentication. If yes, KerberosConfigName must be supplied.
useLDAP	boolean	Optional. Set to yes to use LDAP

Parameter	Value type	Description
user	string	Optional. User for the datasource. If used, password must also be used.
useSSL	boolean	Optional. Set to yes to use SSL authentication.

Example

```
grdapi create_datasource type=DB2 name=chickenDB2  password=guardium user=db2inst1 dbName=dn0chick application=Access_policy
shared=true port=50000 host=chicken.corp.com
```

create_test_exception

Use this command to add records to the Tests Exceptions. This effects the behavior for vulnerability assessments, if a test on a specific datasource fails it will check the last record of the test exceptions table for that test/datasource such that if the execution date is contained within the from and to dates of the last record the test will be set to PASS, the recommendation will be set to the explanation (from the exceptions record) and the result text will be set to:

```
Test passed, based on exception approved by: .... effective from date to date.
```

Note: The API only adds records to remove an exception a new record should be created with new dates according to the needs.

Parameter	Value type	Description
datasourceName	string	Required. Valid name of a defined datasource.
testDescription	string	Required. A valid test name within Security Assessments.
fromDate		Required. Beginning date for when the exception is valid.
toDate		Required. Ending date for when the exception is valid.
explanation	string	Required. A recommendation as to why the test will pass.

Example

```
grdapi create_test_exception datasourceName=ORAPROD5 testDescription="CVE-2009-0997" fromDate="2012-07-01 08:00:00" toDate="2012-
07-31 08:00:00" explanation="Currently in testing stage"
```

list_datasource_by_name

Displays a datasource definition identified by a name.

Parameter	Value type	Description
name	string	Required. The datasource name.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
CLI> grdapi list_datasource_by_name name=chickenDB2
ID=20000
Datasource DatasourceId=20000
Datasource DatasourceTypeId=2
Datasource Name=chickenDB2
Datasource Description=null
Datasource Host=chicken.corp.com
Datasource Port=50000
Datasource ServiceName=
Datasource UserName=db2inst1
Datasource Password=[B@1415de6
Datasource PasswordStored=true
Datasource DbName=dn0chick
Datasource LastConnect=null
Datasource Timestamp=2008-04-18 15:40:58.0
Datasource ApplicationId=2
Datasource Shared=true
Datasource ConProperty=null
Datasource type =DB2
Application Type = Access_policy
ok
```

list_datasource_by_id

Displays a datasource definition identified by an ID key.

Parameter	Value type	Description
id	integer	Required. The ID number of the datasource to be listed.

Parameter	Value type	Description
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi list_datasource_by_id id=2
```

delete_datasource_by_name

Deletes the specified datasource definition, unless that datasource is being used by an application. This function removes the datasource, regardless of who created it.

Parameter	Value type	Description
name	string	Required. The datasource name.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi delete_datasource_by_name name=swanSybase
```

delete_datasource_by_id

Deletes the specified datasource definition, unless that datasource is being used by an application. This function removes the datasource, regardless of who created it.

Parameter	Value type	Description

Parameter	Value type	Description
id	integer	Required. The ID number of the datasource to be listed.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi delete_datasource_by_id id=2
```

update_datasource_by_name

Updates a datasource definition.

Parameter	Value type	Description
name	string	Required. Identifies the datasource to be updated.
newName	string	Optional. Provides a new name, which must be unique for a datasource on the system.
description	string	Optional. Longer description of the datasource.
host	string	Optional. Can be the host name or the IP address.

Parameter	Value type	Description
port	integer	Optional. Port number.
savePassword	boolean	Saves and encrypts your authentication credentials on the Guardium appliance. Required if you are defining a datasource with an application that runs as a scheduled task (as opposed to on demand). When set to yes, login name and password are required.
serviceName	string	Optional. For an Oracle datasource, enter the service name.
user	string	Optional. User for the datasource. If used, password must also be used.
password	string	Optional. Password for user. If used, user must also be used.
dbName	string	Optional. For DB2 datasources, enter the database name.

Parameter	Value type	Description
conProperty	Comma separated list of: property=value	Optional. Use only if additional connection properties must be included on the JDBC URL to establish a JDBC connection with this datasource. For a Sybase database with a default character set of Roman8, enter the following property: CHARSET=utf8
dbInstanceAccount	string	Optional. Database Account Login Name that will be used by CAS
dbInstanceDirectory	string	Optional. Directory where database software was installed that will be used by CAS
shared	boolean	Optional. Set to **true** to share with other applications. To share the datasource with other users, you will have to assign roles from the GUI.
customURL	string	Optional. Connection string to the datasource; otherwise connection is made using host, port, instance, properties, etc. of the previously entered fields. As an example this is useful for creating Oracle Internet Directory (OID) connections.
severity		Optional. Severity Classification (or impact level) for the datasource.

Parameter	Value type	Description
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.
useKerberos	boolean	Optional. Set to yes to use Kerberos authentication. If yes, KerberosConfigName must be supplied.
useLDAP	boolean	Optional). Set to yes to use LDAP
useSSL	boolean	Optional. Set to yes to use SSL authentication.

Example

```
grdapi update_datasource_by_name name=chickenDB2  newName="chicken DB2" user=" " password=" "
```

update_datasource_by_id

Updates a datasource definition.

Parameter	Value type	Description
id	integer	Required. Identifies the datasource.
newName	string	Optional. Provides a new name, which must be unique for a datasource on the system.

Parameter	Value type	Description
description	string	Optional. Longer description of the datasource.
host	string	Optional. Can be the host name or the IP address.
port	integer	Optional. Port number.
savePassword	boolean	Saves and encrypts your authentication credentials on the Guardium appliance. Required if you are defining a datasource with an application that runs as a scheduled task (as opposed to on demand). When set to yes, login name and password are required.
serviceName	string	Optional. For an Oracle datasource, enter the service name.
user	string	Optional. User for the datasource. If used, password must also be used.
password	string	Optional. Password for user. If used, user must also be used.
dbName	string	Optional. For DB2 datasources, enter the database name.

Parameter	Value type	Description
conProperty	Comma separated list of property=value	Optional. Use only if additional connection properties must be included on the JDBC URL to establish a JDBC connection with this datasource. For a Sybase database with a default character set of Roman8, enter the following property: CHARSET=utf8
dbInstanceAccount	string	Optional. Database Account Login Name that will be used by CAS
dbInstanceDirectory	string	Optional. Directory where database software was installed that will be used by CAS
shared	boolean	Optional. Set to **true** to share with other applications. To share the datasource with other users, you will have to assign roles from the GUI.
customURL	string	Optional. Connection string to the datasource; otherwise connection is made using host, port, instance, properties, etc. of the previously entered fields. As an example this is useful for creating Oracle Internet Directory (OID) connections.
severity		Optional. Severity Classification (or impact level) for the datasource.

Parameter	Value type	Description
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.
useKerberos	boolean	Optional. Set to yes to use Kerberos authentication. If yes, KerberosConfigName must be supplied.
useLDAP	boolean	Optional. Set to yes to use LDAP
useSSL	boolean	Optional. Set to yes to use SSL authentication.

Example

```
grdapi update_datasource_by_id id=20000 user=" " password=" " newName="chickenDB2hooo"
```

list_db_drivers

List only the name of database drivers Oracle (DataDirect) and MS SQL SERVER (DataDirect) are now supported as datasource types.

list_db_drivers_by_details

Lists each database driver in more details (name, class, driver class, URL, and datasource type ID)

Parent topic: GuardAPI Reference

GuardAPI Datasource Reference Functions

Use these GuardAPI commands to create, list, and delete Datasource Reference Functions.

create_datasourceRef_by_id

For a specific object of a specific application type (for example, a specific Classification process), creates a reference to a datasource.

Parameter	Value type	Description
appId	integer	Required. Identifies the application. Must be from this list: • 8 = SecurityAssessment • 47 = CustomTables • 51 = Classifier
datasourceId	integer	Required. Identifies the datasource (from the datasource definition).
objId	integer	Required. Identifies an instance of the appID type specified. For example, if apID=51, this would be the ID of a classification process.

Example

```
grdapi create_datasourceRef_by_id appId=51 datasourceId=20000 objId=2
```

create_datasourceRef_by_name

For a specific object of a specific application type (for example, a specific Classification process), creates a reference to a datasource.

Table 1. create_datasourceRef_by_name

Parameter	Value type	Description
application	string	Required. Identifies the application. Must be from this list: SecurityAssessment CustomTables Classifier
datasourceName	string	Required. Identifies the datasource (from the datasource definition).
objName	string	Required. Identifies an instance of the application type specified. For example, if the application is Classifier, this would be the name of a specific classification process.

Example

```
grdapi  create_datasourceRef_by_name   application=Classifier   datasourceName=swanSybase  objName="class process1"
```

list_datasourceRef_by_id

For a specific object of a specific application type (for example, a specific Classification process), lists all datasources referenced.

Parameter	Value type	Description
appID	integer	Required. Identifies the application. Must be from this list: 8 = SecurityAssessment 47 = CustomTables 51 = Classifier
objID	string	Required. Identifies an instance of the application type specified. For example, if the application is Classifier, this would be the ID of a specific classification process.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi list_datasourceRef_by_id appId=13 objId=1
```

list_datasourceRef_by_name

For a specific object of a specific application type (for example, a specific Classification process), lists all datasources referenced.

Parameter	Value type	Description
application		Required. Identifies the application. Must be from this list: SecurityAssessment CustomTables Classifier
objName	string	Required. Identifies an instance of the application type specified. For example, if the application is Classifier, this would be the name of a specific classification process.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdap list_datasourceRef_by_name application=Classifier  objName="class process1"
```

delete_datasourceRef_by_id

For a specific object of a specific application type (for example, a specific Classification process), removes a datasource reference.

Parameter	Value type	Description
appId		Required (integer). Identifies the application. Must be from this list: 8 = SecurityAssessment 47 = CustomTables 51 = Classifier
datasourceId	integer	Required. Identifies the datasource (from the datasource definition).
objId	integer	Required. Identifies an instance of the appID type specified. For example, if apID=51, this would be the ID of a classification process.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi delete_datasourceRef_by_id appId=51 datasourceId=2 objId=1
```

delete_datasourceRef_by_name

For a specific object of a specific application type (for example, a specific Classification process), removes a datasource reference.

Parameter	Value type	Description
application		Required. Identifies the application. Must be from this list: SecurityAssessment CustomTables Classifier

Parameter	Value type	Description
datasourceName	string	Required. Identifies the datasource (from the datasource definition).
objName	string	Required. Identifies an instance of the application type specified. For example, if the application is Classifier, this would be the name of a specific classification process.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi delete_datasourceRef_by_name application=Classifier datasourceName=swanSybase objName=”class process1”
```

Parent topic: GuardAPI Reference

GuardAPI Data User Security Functions

Use these GuardAPI commands to create, list, delete, and update Data User Security Functions.

create_user_hierarchy

Add a relationship between a user and parent in the user data security hierarchy

Parameter	Value type	Description
userName	string	Required. The name of the user
parentUserName	string	Required. the name of the parent user.

Parameter	Value type	Description
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

grdapi create_user_hierarchy userName=admin parentUserName=accessmgr

Note: An error will occur if the insert is cyclic (a parent reports to a child)

list_user_hierarchy_by_parent_user

List relationships in the user data security hierarchy

Parameter	Value type	Description
userName	string	Required. The name of the user
create	boolean	If set (true or false) will or will not generate create statements for create_user_hierarchy API calls. Use this parameter to get all the commands necessary to generate a batch file. This batch file can be used to move each parent and child pairing to another Guardium system.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

grdapi list_user_hierarchy_by_parent_user userName=admin create=true

Note: Only lists immediate parent-child relationship - will not display "grandchildren"

delete_user_hierarchy_by_entry_id

Deletes a relationship in the user data security hierarchy by entry id

Parameter	Value type	Description
id	integer	Required. Identifies the entry
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

grdapi delete_user_hierarchy_by_entry_id id=1

Note: There is no failure condition if the entry doesn't exist

delete_user_hierarchy_by_user

Deletes a relationship in the user data security hierarchy by user

Parameter	Value type	Description
userName	string	Required. The name of the user
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

grdapi delete_user_hierarchy_by_user userName=admin

Note:

There is no failure condition if the user doesn't exist.

Multiple deletes occurs if the user has multiple parents.

create_allowed_db

Create a User-DB association

Parameter	Value type	Description
userName	string	Required. The name of the user
serverIp		Required. The server IP
instanceName	string	Required. The instance name
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

grdapi create_allowed_db userName=admin serverIp=192.168.1.1 instanceName=abcd

list_allowed_db_by_user

List User-DB associations by user

Parameter	Value type	Description
userName	string	Required. The name of the user
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

grdapi list_allowed_db_by_user userName=admin

delete_allowed_db_by_entry_id

Delete a User-DB association by entry id

Parameter	Value type	Description
id	integer	Required. Identifies the entry.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

grdapi delete_allowed_db_by_entry_id id=1

delete_allowed_db_by_user

Delete a User-DB association by user

Parameter	Value type	Description
userName	string	Required. The name of the user
serverIp		The server IP.
instanceName	string	The instance name. Note: For "blank" instance names, enter instanceName=[blank] (not instanceName=blank)

Parameter	Value type	Description
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

grdapi delete_allowed_db_by_user userName=scott

update_user_db

Fully apply all recent changes to the active User-DB association map

Parameter	Value type	Description
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

grdapi update_user_db

Note: In a Central Management configuration, this command should be run on a Central Manager.
Parent topic: GuardAPI Reference

GuardAPI Enterprise Load Balancing Functions

Use these GuardAPI commands to view and set load balancing parameters, view the current load map, and manage S-TAP and managed unit group associations.

get_load_balancer_load_map

View the current load map.

```
grdapi get_load_balancer_load_map
```

get_load_balancer_params

View the current load balancer configuration parameters.

```
grdapi get_load_balancer_params
```

set_load_balancer_param

Set load balancer configuration parameters.

```
grdapi set_load_balancer_param [paramName=value][paramValue=value][paramType=STAP]
```

See Enterprise load balancing configuration parameters for a list of available parameters and allowed values.

For example, `grdapi set_load_balancer_params paramName=LOAD_BALANCER_ENABLED paramValue=0 paramType=STAP`

Use this format for correct input

grdapi set_load_balancer_param --help=true

ID=0

function parameters : paramName - String - required

paramType - String - required

paramValue - String - required

To get a Constant values list for a parameter, call the function with --get_param_values

assign_load_balancer_groups

Assign a managed unit group to an application or S-TAP group.

`grdapi assign_load_balancer_groups muGroupName=[value] appGroupName=[value]`

Parameter	Value type	Description
muGroupName	`managed unit group name`	For example, `muGroupName=mu_group_NA`.
appGroupName	`application or S-TAP group name`	For example, `appGroupName=app_group_NA`.
ifFailoverGroup	`1 or 0`	For Example, `isFailoverGroup=0`

unassign_load_balancer_groups

Unassign a managed unit group from an application or S-TAP group.

`grdapi unassign_load_balancer_groups muGroupName=[value] appGroupName=[value]`

Parameter	Value type	Description
muGroupName	`managed unit group name`	For example, `muGroupName=mu_group_NA`.
appGroupName	`application or S-TAP group name`	For example, `appGroupName=app_group_NA`.

Parent topic: GuardAPI Reference

GuardAPI Entitlement Optimization Functions

Use these GuardAPI commands to enable and configure the Entitlement Optimization datasources and reporting.

enable_entitlement_optimization

Enables the entitlement optimization feature on this Collector.

`grdapi enable_entitlement_optimization`

disable_entitlement_optimization

Disables the entitlement optimization feature on this Collector.

`grdapi disable_entitlement_optimization`

add_datasource_to_entitlement_optimization

Adds the data from this source to the entitlement optimization data collection, and to individual tabs as specified.

`grdapi add_datasource_to_entitlement_optimization`

Parameter	Value type	Description
datasourceName	`datasourceName`	Name of datasource
isEnabled	one of: `true, false`	Datasource is enabled, or disabled, for entitlement optimization Default = false
userScope	One or more comma separated Guardium user group IDs (groups must contain only users)	Optional. Entitlement recommendations results are filtered by this group of users. Browse Entitlements results: indicates whether users are included in this scope or not; does not present user activity count of users outside the scope. default = NULL
objectScope	One or more comma separated Guardium object group IDs (groups must contain only objects)	Optional. Entitlement recommendations results are filtered by this group of objects. default = NULL
extractActivity	one of: `true, false`	Enables, disables extraction of datasource activity.

		Must be true for Browse Entitlements and What If. Default = false
extractEntitlement	one of: `true, false`	Enables, disables extraction of entitlement data. Must be true for What's New, Users and Roles, Recommendations, and Browse Entitlements Default = false
generateRoleClusters	one of: `true, false`	Enables, disables extraction of behavioral role clustering from the data source, used in the **What If** tab. Must be true for What If. Default = false
generateNews	one of: `true, false`	Activity from this datasource is included in the **What's New?** tab. Default = false
generateRecommendations	one of: `true, false`	Activity from this datasource is included in the **Recommendations**. Default = false
filterTempObjects	one of: `true, false`	For future use. Temporary objects are filtered from the data source's collected data. Default = true
filterIgnoreVerbs	one of: `true, false`	For future use. Ignore verbs are filtered from the data source's collected data. Default = true

remove_datasource_from_entitlement_optimization

Removes all data from this source from the entitlement optimization data collection.

```
remove_datasource_from_entitlement_optimization
```

set_entitlement_datasource_parameter

Modifies parameters for data source that is already enabled for entitlement optimization. Uses the same parameters as add_datasource_to_entitlement_optimization.

```
grdapi set_entitlement_datasource_parameter
```

get_entitlement_datasource_parameter

Displays the parameter settings for each data source on this Collector.

```
grdapi get_entitlement_datasource_parameter
```

Example:

```
Entitlement Optimization is enabled
===================================
Datasource: SCALE-DB16
===================================
isEnabled: true
userScope:
objectScope:
extractActivity: true
extractEntitlement: true
generateRoleClusters: true
generateNews: true
generateRecommendations: true
filterTempObjects: true
filterIgnoreVerbs: true
===================================
Datasource: on12scal
===================================
isEnabled: true
userScope:
objectScope:
extractActivity: true
extractEntitlement: true
generateRoleClusters: true
generateNews: true
generateRecommendations: true
filterTempObjects: true
filterIgnoreVerbs: true
```

Parent topic: GuardAPI Reference

GuardAPI External Feed Functions

Use these GuardAPI functions to create mappings for external feeds.

create_ef_mapping

This function creates a mapping and populates tables based on the name of the report specified by the *reportName* parameter. Each mapping has a name stored in EF_MAP_TYPE_HDR.EF_TYPE_DESC, and that name will be identical to the value of *reportName*. The target table name will also be based on the *reportName* parameter, with underscores added between the words. For example, "My Report" becomes MY_REPORT.

Parameter	Value type	Description
reportName	string	Name of the report to use for external feed mapping. This parameter also determines the name of the mapping and the target table name.

modify_ef_mapping

Sometimes the names generated by create_ef_mapping are not suitable for particular database, and modify_ef_mapping can be used to adjust the names to fit database requirements. Only mappings with ID >= 20000 may be modified in order to protect predefined Guardium mappings.

Parameter	Value type	Description
reportName	string	Name of the mapping to modify.
modifyObj		Specifies the database object to modify, either *table* or *column*. Existing values can be retrieved using the list_ef_mapping function.
oldName		Specifies the old table name to remove.
newName	string	Specifies the new table name to use.

delete_ef_mapping

This function allows you to delete existing mappings. Only mappings with ID >= 20000 may be deleted in order to protect predefined Guardium mappings.

Parameter	Value type	Description
reportName	string	Name of the mapping to delete.

list_ef_mapping

If run without any parameters, this function returns a list of all customer-created mappings. If run with the *reportName* parameter, this function returns details of the specified mapping (such as the table and column names used by the external feed).

Table 1.

Parameter	Value type	Description
reportName	string	Optional. Name of the mapping for which to return details.

Parent topic: GuardAPI Reference

GuardAPI File Activity Monitor Functions

Use the following GuardAPI commands to enable and disable the file activity monitor, configure the file Investigation Dashboard activity and entitlement extractions schedule, and get information on the file activity monitor.

Use the GuardAPI command, grdapi create_policy, to create a FAM policy. After the policy is created, use FAM-specific GuardAPI commands.

For example:

grdapi create_policy ruleSetDesc='TEST'

grdapi create_fam_rule policyName='TEST' ruleName=r-test-sles11 actionName="Log As Violation and Audit" serverHost="9.70.144.98:FAM" filePath="/famtest/*"

For instructions on how to use GuardAPI commands, see GuardAPI Reference.

enable_fam_crawler

Sets the Guardium system to process crawler results and file activity data. The results will be added automatically to quick search index files. Use the parameters to schedule file quick search activity, entitlement extractions, and remote group population.

Note: The Investigation Dashboard must also be enabled with the command grdapi enable_quick_search schedule_interval=1.

Parameter	Value type	Description
extraction_start		Initial date/time from which data is extracted to file quick search. It is limited to 2 days in the past. The default is current time. If the unit is set to HOUR, then it is rounded to an hour. If it is set to DAY, then it is rounded to a day.
schedule_start		The default is current time.
activity_schedule_interval	integer	Required. This parameter sets activity schedule interval. The recommended interval is 2 with the unit set to MINUTE.
activity_schedule_units	valuelist	Required. This parameter sets the unit of the activity unit. The values are either MINUTE or HOUR. The recommended unit is MINUTE.
entitlement_schedule_interval	integer	Required. This parameter sets the entitlement schedule interval. The recommended interval is 1 with the unit set to DAY.

Parameter	Valuetype	Description
entitlement_schedule_units	valuelist	Required. This parameter sets the unit of the entitlement schedule. The possible values are MINUTE, HOUR, and DAY. The recommended unit is DAY.

Example

```
grdapi enable_fam_crawler extraction_start=< > schedule_start=< >
 activity_schedule_interval=2 activity_schedule_units=MINUTE
entitlement_schedule_interval=10 entitlement_schedule_units=MINUTE
```

disable_fam_crawler

Disables the file activity monitor. The file quick search activity and entitlement extractions scheduler are removed. This function also disables remote group population.

Example

```
grdapi disable_fam_crawler
```

get_fam_crawler_info

Shows the status of the file activity monitor. If it is enabled, the command shows the settings for the entitlement extraction and file quick search activity schedule.

```
FAM Crawler (server side) is disabled.
```

```
FAM Crawler (server side) is enabled. Entitlement(1 DAY) Activity(2 MINUTE)
```

Example

```
grdapi get_fam_crawler_info
```

list_policy_fam_rule

Lists all the rules in a FAM policy.

Parameter	Valuetype	Description
policyName	string	Required. Policy name
ruleName	string	Optional. If no ruleName is provided, all policy rules with details will be shown. If a ruleName is provided, details will be listed for that rule.

create_fam_rule

Creates a new FAM rule.

Parameter	Valuet	Description

	type	
policyName	string	Required. Policy name.
ruleName	string	Required. Rule name.
filePath	string	File path to be monitored. Either filePath or filePathGroup must be specified.
notfilePath	boolean	Must be yes or no. Yes means apply this rule to all files except those in the specified path.
filePathGroup	string	Group of file paths. Either filePath or filePathGroup must be specified.
includeSubDirectory	boolean	Must be yes or no. Yes means include files in all subdirectories.
removableMedia	string	Must be yes or no.
osUser	string	OS user name.
osUserGroup	string	Group of OS users.
notOSUser	string	Must be yes or no. Yes means use all users except the specified osUser,
serverHost	string	Host name.
serverHostGroup	str	Group of hostnames.

	ing	
command	string	The command name to be included in the rule, one of • DELETE • EXECUTE • FILEOP • READ • WRITE
commandGroup	string	Group of commands.
notCommand	string	Must be yes or no. Yes means use all commands except the specified command.
actionName	string	Required, The name of the FAM action.
messageTemplate	string	Message template name.
notificationType	string	Notification type, one of • MAIL • SNMP • CUSTOM • SYSLOG
userLoginName	string	User login name.
classDestination	string	Name of custom class to be invoked.

policy_fam_rule_delete

Deletes a rule from a FAM policy.

Parameter	Valuetype	Description
policyName	string	Required. Policy name
ruleName	st	Required. Name of the rule to be deleted.

	string	

add_action_to_fam_rule

Adds an action to an existing FAM rule.

Parameter	Value type	Description
actionName	string	Required. The name of the FAM action.
alertReceiver	string	AlertReceiver is any user of the appliance like admin, etc.
command	string	The command name to be included in the rule. One of: • DELETE • EXECUTE • FILEOP • READ • WRITE
messageTemplate	string	String. Message template name.
notificationType	string	Notification type, one of: • MAIL • SNMP • CUSTOM • SYSLOG
policyName	string	Required. Valid policy name.
ruleName	string	Required. Name of the rule to be updated.

Parent topic: GuardAPI Reference

GuardAPI GIM Functions

Use these CLI commands to list, update, assign, remove and cancel GIM Functions.

gim_list_registered_clients

Lists all the registered clients.

Parameter	Value type	Description
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi gim_list_registered_clients
```

gim_list_client_params

Lists all the (module) parameters assigned to a specific client.

Parameter	Value type	Description
clientIP	string	Required - Client IP Address
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi gim_list_client_params clientIP=192.168.12.210
```

gim_update_client_params

Updates a single module parameters in a specific client.

Parameter	Value type	Description
clientIP	string	Required. IP of target client

Parameter	Value type	Description
paramName	string	Required. Parameter Name
paramValue	string	Required. Parameter Value
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi gim_update_client_params clientIP=192.168.1.100 paramName=STAP_TAP_IP paramValue=192.168.1.100
```

gim_list_client_modules

Lists all the modules assigned to a specific client and their state

Parameter	Value type	Description
clientIP	string	Required - Client IP Address
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi gim_list_client_modules clientIP=192.168.2.210
```

gim_load_package

Loads all the modules within 'filename'.

Note: This command will load a file which resides on local file system, therefore the procedure (cmd='fileserver') of loading a file to the CM/Guardium appliance must precede this command.

Parameter	Value type	Description
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi gim_load_package  filename=*.gim
```

Note: The wildcard "*" can be used within filename.

gim_assign_bundle_or_module_to_client_by_version

Assigns a bundle/module to a client.

Parameter	Value type	Description
clientIP	string	Required - Client IP Address
module	string	Required - Module
moduleVersion	string	Required - Module Version
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi gim_assign_bundle_or_module_to_client_by_version clientIP=192.168.1.100  module=BUNDLE-STAP moduleVersion=”8.0_r1234_1”
```

gim_schedule_install

Schedules for installation all the modules/bundles that were assigned to a client and haven't been installed yet (for example, PENDING). If the parameter module is specific, only the requested module will be scheduled.

Parameter	Value type	Description
clientIP	string	Required - Client IP Address
module	string	Optional - Module. If module is not specified in the command, all the modules for the specified clientIP will be scheduled for install.
date		Required - Date; Format: 'now' or 'yyyy-MM-dd HH:mm'
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi gim_schedule_install clientIP=192.168.1.100 module=BUNDLE-STAP  date="2008-07-02 14:50"
```

```
grdapi gim_schedule_install clientIP=192.168.1.100 date="2008-07-02 14:50"
```

Note: Date in the past may be used to run something immediately.

gim_list_client_status

Displays the status of the latest operation executed for a specific client.

Parameter	Value type	Description
clientIP	string	Required - Client IP Address
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi gim_list_client_status clientIP=192.168.1.100
```

gim_uninstall_module

Uninstalls a module/bundle on a specific client.

Parameter	Value type	Description
clientIP	string	Required - Client IP Address
module	string	Required - Module.
date		Required - Date; Format: 'now' or 'yyyy-MM-dd HH:mm'
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi gim_uninstall_module clientIP=192.168.1.100 module=BUNDLE-STAP
```

gim_cancel_install

Cancels installation of a bundle/module on a specific client. Canceling installation is possible only if a module/bundle is not already in the process of being installed by a client (STATE=IP or IP-PR)

Parameter	Value type	Description
clientIP	string	Required - Client IP Address
module	string	Required- Module.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi gim_cancel_install clientIP=192.168.1.100 module=BUNDLE-STAP
```

gim_list_bundles

Lists all the available bundles. A bundle is a group of modules that can be installed on a client.

Parameter	Value type	Description
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi gim_list_bundles
```

gim_list_mandatory_params

Lists the mandatory parameters for a single module.

Parameter	Value type	Description
module	string	The name of the GIM module for which to display the mandatory parameters
version	string	The version of the GIM module for which to display the mandatory parameters

Example

```
grdapi gim_list_mandatory_params module=name version=number
```

gim_assign_latest_bundle_or module_to_client

Assigns the latest (i.e. the highest version) available bundle or module for a specific client.

Parameter	Value type	Description

Parameter	Value type	Description
clientIP	string	Required - Client IP Address
module	string	Required- Module.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi gim_assign_latest_bundle_or_module_to_client clientIP=192.168.1.100  module=BUNDLE_STAP
```

gim_schedule_uninstall

Schedules uninstallation of all the modules/bundles that were assigned to a client and haven't been uninstalled yet (i.e. “PENDING”). If the parameter 'module' is specific, only the requested module will be scheduled.

Parameter	Value type	Description
clientIP	string	Required - Client IP Address
module	string	Optional - Module. If module is not specified in the command, all the modules for the specified clientIP will be scheduled for install.
date		Required - Date; Format: 'now' or 'yyyy-MM-dd HH:mm'
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi gim_schedule_uninstall clientIP=192.168.1.100 module=BUNDLE-STAP  date="2008-07-02 14:50"   grdapi gim_schedule_uninstall
clientIP=192.168.1.100 date="2008-07-02 14:50"
```

gim_cancel_uninstall

Cancels uninstallation of a bundle/module on a specific client. Canceling uninstallation is possible only if a module/bundle is not already in the process of being installed by a client (STATE=IP or IP-PR)

Parameter	Valuetype	Description
clientIP	string	Required - Client IP Address
module	string	Required- Module.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi gim_cancel_uninstall clientIP=192.168.1.100 module=BUNDLE-STAP
```

gim_remove_bundle

The command will delete bundlePackageName from the database as well as from the file system (from /var/log/guard/gim_packages , and also from/var/gim_dist_packages if the Guardium system is a central manager).

parameters (required):

bundlePackageName

Parameter value take bundle package name as specified in the output of the gim_list_unused_bundles. The command will be successful only if:

2.1 The value of bundlePackageName refers to a BUNDLE

2.2 The value of bundlePackageName is not assigned to any client

2.3 The value of bundlePackageName exists

2.4 There is one and only one bundle that refers to the value of bundlePackageName

ALL the conditions (2.1 to 2.4) must be true in order to delete a bundle from the database/file system. Otherwise an error will be generated.

Example

```
grdapi gim_remove_bundle  bundlePackageName= bundlePackageName
```

gim_unassign_client_module

Unassigns a module from a client. Unlike 'gim_remove_module', this command will untie the connection between a module and a specific client on the CM/Guardium appliance. This command is will NOT uninstall or remove the module on the actual DB-server machine. It is to be used only in cases on synchronization problems between the DB-server (i.e client) information and the CM/Guardium appliance information regarding the current state of the modules.

Parameter	Value type	Description
clientIP	string	Required - Client IP Address
module	string	Optional. Module. If module is not specified in the command, all the modules for the specified clientIP will be scheduled for install.
date		Required. Date; Format: 'now' or 'yyyy-MM-dd HH:mm'
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi gim_unassign_client_module clientIP=192.168.1.100  module=STAP
```

gim_get_purge_list

List old software packages (GIM files) that have previously been uploaded to the Guardium® appliance or CM.

Parameter	Value type	Description
olderThan	string	Required - Number of days. Files older than the number of days specified will be purged. Valid value is any number greater or equal to 0.
excludeLatest	boolean	Optional - true or false (default value is true). true: Avoid purging the latest version per OS per module. false: Purge the latest version per OS per module.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi gim_get_purge_list olderThan=30 excludeLatest=true
```

gim_purge

Remove old software packages (GIM files) that have previously been uploaded to the Guardium appliance or CM.

Parameter	Value type	Description
olderThan	string	Required - Number of days. Files older than the number of days specified will be purged. Valid value is any number greater or equal to 0.
excludeLatest	boolean	Optional - true or false (default value is true). true: Avoid purging the latest version per OS per module. false: Purge the latest version per OS per module.
filename	string	Optional - A specific file that is to be removed. If the file specified is a bundle (for example, starts with 'guard-bundle'), the content of this bundle will be removed.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi gim_purge olderThan=30
```

Note:

Either the 'filename' parameter or (olderThan and/or excludeLatest) can be specified in the command.

GIM purge will not purge files that are currently scheduled for installation.

GIM purge will not allow the removal of any file (for example, parameter filename) that includes '/' character.

gim_get_available_modules

List the available modules / bundles available to install on a specific server.

Parameter	Value type	Description
clientIP	string	Required - Client IP Address

Example

```
grdapi gim_get_available_modules clientIP=192.168.1.100
```

gim_get_client_last_event

List the latest operation executed for a specific client.

gim_get_client_last_event is a GrdAPI command with limited functionality. All it does is show the last event occurred during the latest installation attempt. For example, if during the latest installation of S-TAP there were some errors, it will show up by running that grdapi command. However, if you manually fix the installation problem directly on the database server, this grdapi command will still show the same original error message (even though S-TAP is now running). This command should not be used to evaluate S-TAP status after manual fixes on the database server.

Parameter	Value type	Description
clientIP	string	Required - Client IP Address

Example

grdapi gim_get_client_last_event clientIP=192.168.1.100

grdapi gim_get_client_last_event clientIP=winx64

grdapi gim_get_client_last_event clientIP=9.70.144.73

gim_get_modules_running_status

List the modules / bundles currently running on a specific server.

Parameter	Value type	Description
clientIP	string	Required - Client IP Address
process	string	name of process
status	ON or OFF	
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi gim_get_modules_running_status clientIP=192.168.1.100 process= status=
```

gim_list_unused_bundles

The command returns a list of unused (not installed on any database server) bundles and individual Windows modules that can be uploaded (for example, Windows CAS, Windows FAM).

parameters (required):

includeLatest (valid values 0/1)

If set to value 1, the returned list of unused bundles will include the latest unused bundle.

Example

```
grdapi gim_list_unused_bundles includeLatest=1
```

gim_reset_client

Disassociate modules from selected client.

Parameter	Value type	Description
clientIP	string	Required - Client IP Address
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi gim_reset_client clientIP=192.168.1.100
```

gim_set_diagnostics

Set diagnostics collection within GIM.

Parameter	Value type	Description
clientIP	string	Required - Client IP Address

Parameter	Value type	Description
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi gim_set diagnostics clientIP=192.168.1.100
```

gim_set_global_param

Set global parameters within GIM.

Parameter	Value type	Description
clientIP	string	Required - Client IP Address
paramName	string	Required - Name of the parameter within the API function to be mapped
paramValue	string	Required - Value of the parameter within the API function to be mapped
sqlguardip	string	Optional - IP address /host name of the collector this GIM agent will connect to.
ca_file	string	Optional - Full file name path to the certificate authority PEM file.
key_file	string	Optional - Full file name path to the private key PEM file.

Parameter	Value type	Description
cert_file	string	Optional - Full file name path to the certificate PEM file.
gim_listener_default_port	string	Optional - Set a different port for the GIM agent server mode.
gim_listener_default_shared_secret	string	Optional - Set a shared secret to verify collectors that are sending requests to the new server mode GIM agent.
no_listener	string	Optional - Disable the GIM agent in server mode.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi gim_set_global_param clientIP=192.168.1.100 paramName=gim_listener_default_port paramValue=8445
```

gim_remote_activation

Connects the collector's IP address to a server mode GIM agent or group of GIM agents.

Parameter	Value type	Description
targetGroup	string	Optional - The group name of all the database servers that the collector connects to. It cannot be specified with the targetHost parameter.
sharedSecret	string	Optional - The shared secret that was configured during installation.

Parameter	Value type	Description
targetPort	string	Optional - The port server mode of the GIM agent.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi gim_remote_activation targetGroup=<someGroup> sharedSecret=<password> targetPort=8445
```

Parent topic: GuardAPI Reference

GuardAPI Group Functions

Use these GuardAPI commands to create, list, and delete Datasource Group Functions.

Note: In a Central Management environment, all groups are defined on the Central Manager and sent to the managed units on a scheduled basis.

Group Functions

create_group

list_group_by_id

list_group_by_desc

delete_group_by_id

delete_group_by_desc

update_group_by_id

update_group_by_desc

flatten_hierarchical_groups

Member Functions

create_member_to_group_by_id

create_member_to_group_by_desc

list_group_members_by_id

list_group_members_by_desc

delete_member_from_group_by_id

delete_member_from_group_by_desc

create_group

create_group

Create a group definition.

Parameter	Value type	Description
desc	string	Required. Enter a unique description for the new group.
type	value list	Required. Must be one of the following: Application Event Value Number Application Event Value String Application Event Value Type Application Item Name Application Module Application System ID Application Transaction Code APPLICATION USER Audit Task Type Client Hostname Client IP Client IP/DB User Client IP/Src App./DB User Clietn IP/Src App./DB User/Server IP/Svc. Name Client MAC Address Client OS COMMANDS CVE Pre-defind Tests Database Name DB Error Codes DB PROTOCOL DB PROTOCOL VERSION DB Role DB User/Object/Privilege DB Ver./Patches EXCEPTION TYPE FIELDS Files Permissions Global ID Guardium® Audit Categories Guardium Role Guardium Users Login Succeded Code NET PROTOCOL Object/Command Object/Field

Parameter	Value type	Description
		OBJECTS Operation Type OS User PORT Qualified Objects Records Affected SCHEMA SENTENCE DEPTH Server Description Server Hostname Server IP Server IP/DB User Server IP/Server Port Server IP/Svc. Name/DB User Server OS SERVER TYPE Service Name SOURCE PROGRAM SQL Based pre-defined Tests TeraData Profile/DB User TTL USERS VA Tests Exception WEEKDAY YEAR
appid	value list	Required. Identifies the application for the group. It must be one of the following values: Public Audit Process Builder Baseline Builder Attention: The Baseline Builder and related functionality is deprecated starting with Guardium V10.1.4. Classifier DB2_zOS groups Express Security IMS zOS groups Policy Builder Security Assessment Builder
subtype	string	Optional. A sub type is used to collect multiple groups of the same group type, where the membership of each group is exclusive. For example, assume that you have database servers located in three datacenters, and that you want to group the servers by location. You would define a separate group of database servers for each location, and define all three groups with the same sub type (datacenter, for example).

Parameter	Value type	Description
category	string	Optional. A category is an optional label that is used to group policy violations and groups for reporting.
classification	string	Optional. A classification is another optional label that is used to group policy violations and groups for reporting.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Examples (follow exactly, upper-case and lower-case letters where indicated)

```
grdapi create_group desc=agroup type=OBJECTS  appid=Public owner=admin
```

```
grdapi create_group appid=Access_policy owner=admin  type="OBJECTS"  desc=groupName1
```

list_group_by_id

Display the properties of a specific group.

Parameter	Value type	Description
id	integer	Required. Identifies the group.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi list_group_by_id id=100003
```

list_group_by_desc

Display the properties of a specific group.

Parameter	Value type	Description
desc		Required. The name of the group to be displayed.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi list_group_by_desc desc=agroup
```

delete_group_by_id

Parameter	Value type	Description
id	integer	Required. Identifies the group.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi delete_group_by_id id=100005
```

delete_group_by_desc

Parameter	Value type	Description
desc	string	Required. The name of the group to be removed.

Parameter	Value type	Description
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi delete_group_by_desc desc=agroup
```

update_group_by_id

Update properties of the specified group.

Parameter	Value type	Description
id	integer	Required. Identifies the group to be updated.
newDesc	string	Optional. Enter a unique description for the new group.
subtype	string	Optional. A sub type is used to collect multiple groups of the same group type, where the membership of each group is exclusive. For example, assume that you have database servers located in three datacenters, and that you want to group the servers by location. You would define a separate group of database servers for each location, and define all three groups with the same sub type (datacenter, for example).
category	string	Optional. A category is an optional label that is used to group policy violations and groups for reporting.
classification	string	Optional. A classification is another optional label that is used to group policy violations and groups for reporting.

Parameter	Value type	Description
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi update_group_by_id id=100002 newDesc=beegroup subtype=bee category=be classification=bea
```

update_group_by_desc

Update properties of the specified group.

Parameter	Value type	Description
desc	string	Required. The name of the group to be updated.
newDesc	string	Optional. Enter a unique description for the group.
subtype	string	Optional. A sub type is used to collect multiple groups of the same group type, where the membership of each group is exclusive. For example, assume that you have database servers located in three datacenters, and that you want to group the servers by location. You would define a separate group of database servers for each location, and define all three groups with the same sub type (datacenter, for example).
category	string	Optional. A category is an optional label that is used to group policy violations and groups for reporting.

Parameter	Value type	Description
classification	string	Optional. A classification is another optional label that is used to group policy violations and groups for reporting.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi update_group_by_desc desc=beegroup newDesc=beegroupee category=bebebe classification=bebebebe
```

flatten_hierarchical_groups

Update ALL hierarchical groups that exist in Group Builder.

Parameter	Value type	Description
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi flatten_hierarchical_groups
```

create_member_to_group_by_id

Add a member to a group specified by the group ID.

Parameter	Value type	Description

Parameter	Value type	Description
id	integer	Required. Identifies the group to which the member is to be added.
member	string	Required. The new member name, which must be unique within the group.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi create_member_to_group_by_id  id=100005 member=turkey
```

create_member_to_group_by_desc

Add a member to the named group.

Parameter	Value type	Description
desc	string	Required. The name of the group to which the member is to be added.
member	string	Required. The new member name, which must be unique within the group.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi create_member_to_group_by_desc  desc=bgroup  member=turkey
```

Use these commands to add members to the group

```
grdapi create_member_to_group_by_desc desc=groupName1 member=member_1
grdapi create_member_to_group_by_desc desc=groupName1 member=member_2
grdapi create_member_to_group_by_desc desc=groupName1 member=member_3
grdapi create_member_to_group_by_desc desc=groupName1 member=member_4
grdapi create_member_to_group_by_desc desc=groupName1 member=member_5
```

Additional group GuardAPI commands

create_hierarchical_member_to_group_by_desc

delete_hierarchical_member_from_group_by_desc

function parameters :

desc - String - required

member - String - required

list_group members_by_id

List the members of the specified group.

Parameter	Value type	Description
id	integer	Required. Identifies the group whose members are to be listed.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi list_group_members_by_id  id=100001
```

list_group_members_by_desc

List the members of the specified group.

Parameter	Value type	Description
desc	string	Required. The name of the group whose members are to be listed.

Parameter	Value type	Description
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi list_group_members_by_desc  desc=bgroup
```

delete_member_from_group_by_id

Remove a member from a specified group.

Parameter	Value type	Description
id	integer	Required. Identifies the group from which the member is to be removed.
member	string	Required. The name of the member to be removed.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi delete_member_to_group_by_id  id=100005 member=turkey
```

delete_member_from_group_by_desc

Remove a member from a specified group.

Parameter	Value type	Description
desc	string	Required. The name of the group from which the member is to be removed.
member	string	Required. The name of the member to be removed.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi delete_member_from_group_by_desc desc=bgroup member=boston
```

Parent topic: GuardAPI Reference

GuardAPI Input Generation

GuardAPI Input Generation allows the user to take the output of one Guardium® report and feed it as the input for another Guardium entity; allowing users to used prepared calls to quickly call API functionality.

Generate Input for Guard API Calls

The generation of Guard API calls from reports can be invoked in one of two ways, either from a single row within a report or multi-rows that is based on a whole report (what is seen on the screen). See the how-to topic, Generate API Call From Reports, for an example.

When a report is displayed:

For Single Row:

1. Double-clicking on a row for drill-down displays an option to Invoke... Click the Invoke... option to display a list of APIs that are mapped to this report.

For Multi Row

1. Click the Invoke... icon (within the report status line) to display a list of APIs that are mapped to this report.

   Continue the steps for both Single and Multi Row

2. Click the API you would like to invoke; bringing up the API Call Form for the Report and Invoked API Function. Invoking an API call from a report for multiple rows produces an API Call Form that displays and enables the editing of all records that are displayed on the screen (dependent on the fetch size) to a maximum of 20 records.
3. Fill in the Required Parameters and any non-Required Parameters for the selected API call. Many of the parameters are pre-filled from the report but might be changed to build a unique API call. For specific help in filling out required or non-required parameters, see the individual API function calls within the GuardAPI Reference guide.
   For multi row, use the set of parameters for the API (those with a button for each parameter) to enter a value for a parameter and then click the down arrow button populate that parameter for all records. Also, use the check boxes for each row to select or deselect a row from being included in the API call.
   Note: Parameters with the name of 'password' are masked.
4. Use the drop-down list to select the Log level, where Log level represents the following (0 - returns ID=identifier and ERR=error_code as defined in Return Codes, 1 - displays additional information to screen, 2 - puts information into the Guardium application debug logs, 3 - will do both 1 & 2)
5. Use the drop-down list to select a Parameter to encrypt.
   Note: Parameter Encryption is enabled by setting the Shared Secret and is relevant only for invoking the API function through script generation.
6. Choose to Invoke Now or Generate Script.
   a. If Invoke Now is selected, the API call runs immediately and display an API Call Output screen showing the status of the API call.
   b. If Generate Script is selected
      i. Open the generated script with your favorite editor or optionally save to disk to edit and execute later.

         Example Script

A template script for invoking Sqlguard API function delete_datasource_by_name seven times:

Usage: ssh cli@a1.corp.com<delete_datasource_by_name_api_call.txt

replace any < > with the required value

#

set guiuser <username> password <password>

grdapi delete_datasource_by_name name=192.168.2.91

grdapi delete_datasource_by_name name=egret-oracle

grdapi delete_datasource_by_name name=egret-oracle3

ii. Modify the script; replacing any of the empty parameter values (denoted by '< >')
Note: Empty parameters might remain in the script as the API call ignores them

Example Modified Script

A template script for invoking Sqlguard API function delete_datasource_by_name seven times:

Usage: ssh cli@a1.corp.com<delete_datasource_by_name_api_call.txt

replace any < > with the required value

#

set guiuser <username> password <password>

grdapi delete_datasource_by_name name=egret-oracle3

iii. Execute the CLI function call

Example Call

$ ssh

cli@a1.corp.com<c:/download/delete_datasource_by_name_api_call.txt

Mapping GuardAPI to Report Results

Guardium comes with a battery of predefined reports and many of them have already been mapped to GuardAPI functions to ease configuration. In addition, Guardium offers users the capability to define additional reports, even their own custom made reports, and map them to GuardAPI functions per report.

1. Go to any predefined report in the Daily Monitor tab, Guardium Monitor tab, or Tap Monitor tab.
2. Click the Invoke ... button.
3. Choose the Add API mapping selection.
4. At the new window, Add API mapping shows the name of the report, for example, Guardium Logins; a search/filter mechanism to find the appropriate GuardAPI command; and, selection choices for API functions available under the Predefined Report. Choose the API function, and then click Map Report Attributes.
5. At the new window, API-Report Parameter Mapping, map the parameter name to the Report field. Sometimes there might be data that is not supplied with a Guardium report. For these instances, a constant can be created, added to the report and used within the API parameter mappings.
Note: Save overrides the current mapping.
Note: If the Guardium report, with a constant added, is exported, the constant will not be exported.

To simplify the mapping between the GuardAPI parameters and Guardium attributes, Guardium created the predefined report Query Entities & Attributes that list all the Guardium attributes; giving users a GUI interface and allowing them to easily drill down from that report and create the linkages quickly.

Existing Guardium attributes or user-defined constants may be mapped to the GuardAPI parameters of Existing Attributes or Constants.

Note: When GuardAPI parameters are mapped to report attributes, if a report has more than one attribute that is mapped to the same GuardAPI parameter, the value picked for the API call is the first of these attributes according to the order of display in the report.

Existing Attributes

1. Go to the Query Entities & Attributes report to add the API parameter mappings. (Guardium Monitor -> Query Entities & Attributes)
2. The Query Entities & Attributes report is long because it lists all the Guardium attributes. Narrow down the records you are interested in by using the Customize button.
3. To create the mapping, double-click the attribute row you would like to assign to a parameter name
4. Click the Invoke... option
5. Select the create_api_parameter_mapping API function
6. Fill in the functionName and parameterName in the API Call Form
7. Click the Invoke now button to create the API to Report Parameter Mapping

See how-to topic, Using API Calls From Custom Reports, for a full scenario that maps GuardAPI parameters through the GUI.

Constants

Sometimes there may be data that is not supplied within a Guardium report. For these instances, a constant can be created, added to the report, and then used within the API parameter mappings.

1. Go to the Query Entities & Attributes report to add the API parameter mappings. (Guardium Monitor -> Query Entities & Attributes)
2. The Query Entities & Attributes report is long because it lists all the Guardium attributes. Narrow down the records you are interested in by using the Customize button.
3. To create a constant attribute, double-click any row for the entity you would like to create a constant attribute for
4. Click the Invoke... option
5. Select the create_constant_attribute API function

6. Fill in the constant value to use and an attributeLabel you like to name it
7. Click the Invoke now button to create the constant
8. To create the mapping, double-click the newly created attribute row
9. Click the Invoke... option
10. Select the create_api_parameter_mapping API function
11. Fill in the functionName and parameterName in the API Call Form
12. Click the Invoke now button to create the API to Report Parameter Mapping
13. The newly created attribute must be added to the report. Modify the Query through Query Builder and add the field.

See how-to topic, Using Constants within API Calls, for a full scenario that creates and maps a constant attribute through the GUI.

Note: If the Guardium report, with a constant added, is exported, the constant will not be exported.
Note: When using API mapping, table columns in a report appears in the report field as long as the table column is an attribute of an entity. Some of the columns such as count column will not be displayed in the report field because it cannot be mapped.

Object Security for Certain GuardAPI commands

Role validation implements controls on selected GuardAPI commands to consider the roles of the specific components (and not only the application) and disallow actions if the roles do not match.

This means a user that has the appropriate roles for Policy Builder is able to execute the GuardAPI command, delete_rule, on any policy, regardless of the roles of this specific policy.

Role validation exists for the following Policy rules GuardAPI commands: change_rule_order; copy_rule; copy_rules, delete_rule; update_rule.

Role validation exists for the following Group Description GuardAPI commands: create_member_to_group_by_desc; create_member_to_group_by_id; delete_group_by_desc; delete_group_by_id; delete_member_from_group_by_desc; delete_member_from_group_by_id; update_group_by_id; update_group_by_desc.

Role validation exists for the following Datasource GuardAPI commands: delete_datasource_by_id; delete_datasource_by_name; update_datasource_by_id; update_datasource_by_name.

Role validation exists for the following Audit Process GuardAPI commands: stop_audit_process.

API to run an audit process from tabular and graphical reports

An GuardAPI can be invoked automatically from any report portlet. When the GuardAPI is invoked, it creates a new audit process report.

If such process for the user exists, then the parameters are updated and the same process is used.

The behavior of the GuardAPI is as follows:

1 - If new process, it creates one receiver per email in the list (if any) with <p>a content type as indicated in the emailContentType parameter. It will also create a user receiver for the user that is logged in (invoking the API) if the includeUserReceiver parameter is true.

2 - If existing process, all email receivers are removed and replaced with the emails from the new list (if any) with the content type as defined in the emailContentType parameter. If the list is empty, it removes all email address receivers. If there is already a receiver for the user it will NOT be removed even if the includeUserreceiver is false, however if the parameter is true and there is no such receiver then it is added.

Once the audit process is generated, it is automatically executed (similar to a Run Once Now) and users should expect an item on their to-do list for that audit process.

create_ad_hoc_audit_and_run_once

Parameters:

1 - reportId - The ID on the report to be used for the only task in the Audit process

2 - isForReportRunOnce boolean indicates whether the process should be run once after it is created.

3 - changeParIfExist boolean indicates whether the task parameters should be updated if the process exists

4 - taskParameter All task parameters and the value for each concatenated with the characters ^^ should be like: PAR1=Val1^^PAR2=Val2^^ etc it is valid to leave a parameter empty, for example if PAR2 should remain empty it looks like: PAR1=VAL1^^PAR2=^^PAR3=VAL3^^...

5 - processNamePar - Name of the process if empty it creates a process with the name.

6 - sendToEmails: A comma-separated list of email addresses

7 - emailContentType 0-PDF or 1-CSV (applies ONLY to email receivers

8 - includeUserReceiver boolean indicates whether to create a receiver for the user that is logged in

An GuardAPI can be invoked automatically from any report portlet. When the GuardAPI is invoked, it creates a new audit process report.

Schedule APIs

modify_schedule parameters jobName jobGroup cronString startTime optional

list schedule

delete_schedule parameters jobName jobGroup deleteJob optional

schedule_job parameters jobType objectName optional cronString startTime optional

Note: Some job types for the grdapi schedule_job function do not require an object name. No validation is performed on the object name parameter and users see the standard 'OK' prompt when the function is run with anything entered as the objectName parameter for the following jobs types:csvExportJob, systemBackupJob, dataArchiveJob, dataExportJob, dataImportJob, resultsArchiveJob, AppUserTranslation, IpHostToAlias

grdapi schedule_job --get_param_values=jobType - Value for parameter 'jobType' of function 'schedule_job' must be one of: CustomTableDataUpload; AutoDetectProbeJob; AppUserTranslation; InstallPolicy: AuditJob; ResultArchive; AutoDetectScanJob; CustomTableDataPurge; CSVExport; DataExport; DataArchive; DataImport; PopulateGrpFromQry; SystemBackup; PopulateAlias; IpHostToAlias; UnitUtilization

grdapi set_purge_batch_size

Set the batch size that is used during purge, aids in performance of purge and has a default setting of 200,000. A trade-off in performance and disk space usage should be noted as setting to a larger batch size increases the speed of the purge but consumes more disk space and setting to a low batch size decreases the speed of the purge but not consume as much disk space.

function parameters: batchSize - required api_target_host Example vx29> grdapi set_purge_batch_size batchSize=200000 ID=0 ok

grdapi get_purge_batch_size

Gets the current setting for the purge batch size

function parameters: api_target_host Example vx29> grdapi get_purge_batch_size ID=0 Purge Batch Size = 200000 ok

grdapi patch_install

function parameters: patch_date patch_number - required

grdapi populate_from_dependencies

function parameters: descOfEndingGroup - required descOfStartingGroup - required flattenNamespace getFunctions getJavaClasses getPackages getProcedures getSynonyms getTables getTriggers getViews isAppend - required isEndingGroupQualified owner - required reverseIt selectedDataSourceName - required api_target_host

create_computed_attribute

Use in Reports.

Parameter	Valuetype	Description
attributeLabel	string	Required.
entityLabel	string	Required. Database user
expression	string	Required. Server IP. The user must specify the tableName.field in the expression.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

grdapi create_computed_attribute attributeLabel="CustomUserName" entityLabel="App User Name" expression="SUBSTRING_INDEX(GDM_CONSTRUCT_INSTANCE.APP_USER_NAME,'',1)"

delete_computed_attribute

Use in Reports.

Parameter	Value type	Description
attributeLabel	string	Required.
entityLabel	string	Required.
expression	string	Required.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

update_computed_attribute

Use in Reports.

Parameter	Value type	Description
attributeLabel	string	Required.
entityLabel	string	Required.
expression	string	Required.

Parameter	Value type	Description
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

create_constant_attribute

Use in Reports.

Parameter	Value type	Description
attributeLabel	string	Required.
entityLabel	string	Required.
constant	string	Required.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

delete_constant_attribute

Use in Reports.

Parameter	Value type	Description

Parameter	Value type	Description
attributeLabel	string	Required.
entityLabel	string	Required.
constant	string	Required.
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

update_constant_attribute

Use in Reports.

Parameter	Value type	Description
attributeLabel	string	Required.
entityLabel	string	Required.
constant	string	Required.

Parameter	Value type	Description
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

create_ad_hoc_audit_and_run_once

Use in Reports.

Parameter	Value type	Description
chnageParlfExist	Boolean	Required.
emailContentType	integer	
includeUserReceiver	boolean	
isForReportRunOnce	boolean	Required.
processNamePar	string	
reportID	integer	Required

Parameter	Value type	Description
sendToEmails	string	
taskParameter	string	
api_target_host	string	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

REST API

JSON (JavaScript Object Notation) output option supports GuardAPI functions. This is part of REST APIs. REST stands for Representational State Transfer. It relies on a stateless, client/server, cacheable communications protocol, and in virtually all cases, the HTTP protocol is used. REST is an architecture style for designing networked applications. The idea is that, rather than using complex mechanisms such as CORBA, RPC, or SOAP to connect between machines, simple HTTP is used to make calls between machines. RESTful applications use HTTP requests to post data (create and/or update), read data (for example, make queries), and delete data. Thus, REST uses HTTP for all four Create/Read/Update/Delete operations. REST is a lightweight alternative to mechanisms like RPC (Remote Procedure Calls) and Web Services (SOAP, WSDL).

Guardium's Implementation of REST

1. Register Application (only once) and get Client Secret.
2. Store Client Secret in secure place.
3. Request Access Token for authorization.
4. Store Access Token so grdAPI command is authenticated properly.
5. Use Access Tokens to submit GuardAPI commands.

Example use cases

- I want the ability to dynamically get a small amount of audit data for a certain IP address without having to login to the Guardium GUI.
- I want to populate an existing group, so I can update my policy to prevent unauthorized access to sensitive information.
- I want to get a list of all users within a certain authorized access group.
- I want my application development team to help identify what sensitive tables to monitor.
- I want to script access to grdAPI's without using "expect" scripting language, which requires me to code response text from the target system.

HTTP has a vocabulary of operations (request methods)

- GET (pass parameters in the URL)
- POST (pass parameters in JSON object)
- PUT (pass parameters to change as JSON object)
- DELETE (pass parameters as JSON object)

Special user for internal REST API requests

For internal REST API requests, there is a special ROLE and USER predefined in the system.

This user cannot be removed or modified through the accessmgr UI and cannot be used to log in the UI.

This user's password will never expire, but is revoked if client ID is revoked.

On OAuth client registration, a new function accepts this user and client ID. It generates a random strong password for the user and store it in the TURBINE_USER table.

It returns a client secret and the generated password.

The internal (S-TAP, maybe others) client must secure the client secret and password.

Permissions for different functions can be assigned to the role through accessmgr UI.

RestAPI vs. GuardAPI

GET = List

POST = Create

PUT = Update

DELETE = Delete

GuardAPIs

```
list_datasourcename_by_name (parameters - ?name="MSSQL_1")
```

```
-X GET https://10.10.9.239:8443/restAPI/datasource/?name="MSSQL_1"
```

create_datasource

```
-X POST https://10.10.9.239:8443/restAPI/datasource
```

```
update_datasource_by_name - JSON Object '{password:guardium}'
```

```
-X PUT -d '{password:guardium, name:"MSSQL_1}'
```

```
delete_datasource_by_id - JSON Object '{"id":20020}'
```

```
-X DELETE -d '{"id":20020}'
```

For further information, go to the Using the IBM Security Guardium REST API article on DeveloperWorks.

http://www.ibm.com/developerworks/data/library/techarticle/dm-1404guardrestapi/index.html

Query and restart internal UnitPinger thread

Use this GuardAPI command to query and restart internal UnitPinger thread.
NOTE: This GuardAPIs command needs to be called with api_target_host=127.0.0.1 parameter.
Example
grdapi get_unit_pinger api_target_host=127.0.0.1

register_oauth_client

Use this GuardAPI command to wrap supported GuardAPI functions in a RESTful API that uses JSON (JavaScript Object Notation) for input and output.

Use the GrdAPI command, grdapi register_oauth_client, to register the client and obtain the necessary access token to call the REST services.

REST stands for Representational State Transfer. It relies on a stateless, client/server, cacheable communications protocol, and in virtually all cases, the HTTP protocol is used.

REST is an architecture style for designing networked applications. The idea is that, rather than using complex mechanisms such as CORBA, RPC, or SOAP to connect between machines, simple HTTP is used to make calls between machines.

RESTful applications use HTTP requests to post data (create and/or update), read data (for example, make queries), and delete data. Thus, REST uses HTTP for all four Create/Read/Update/Delete operations. REST is a lightweight alternative to mechanisms like RPC (Remote Procedure Calls) and Web Services (SOAP, WSDL).

function parameters:

client_id - String - required

grant_types - String - required. The only grant type that is supported is password.

redirect_uris - String - required

scope - String - required.

fetchSize - String- optional (default is 20 recores to retain backward compatibility, maximum value is 30000.

sortColumn - optional - If specified must be the column title of one of the report fields.

sortType - optional - asc or desc

Syntax

grdapi register_oauth_client <client_id> <grant_types> <redirect_uris> <scope>

getOAuthTokenExpirationTime

Use this GuardAPI command to get the expiration time of the REST API token

function parameters:

api_target_host - String

setOAuthTokenExpirationTime

Use this GuardAPI command to set the expiration time of the REST API token.

function parameters:

expirationTime - Integer - required

api_target_host - String

Syntax

grdapi setOAuthTokenExpirationTime ExpirationTime=10000

Parent topic: GuardAPI Reference

GuardAPI Investigation Dashboard Functions

Use these GuardAPI commands to enable, disable, or configure Investigation Dashboard features and parameters.

disable_quick_search

Note that the Investigation Dashboard includes the Quick Search Results Table, in addition to the Activity Chart, and various other pre-defined charts.

Disable Investigation Dashboard functionality.

```
grdapi disable_quick_search
```

Parameter	Value	Description
all	`true` or `false`	In an environment with a Central Manager, use this parameter to disable search on all managed units. For example, `all=true`. This parameter is optional.
api_target_host	hostname or IP address	In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM. Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed units, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM This parameter is optional.

enable_quick_search

Enable Investigation Dashboard functionality.

```
grdapi enable_quick_search schedule_interval=[value] schedule_units=[value]
```

For example, the following command enables the Investigation Dashboard with a 2-minute data extraction interval: `grdapi enable_quick_search schedule_interval=2 schedule_units=MINUTE`.

Parameter	Value	Description
all	`true` or `false`	In an environment with a Central Manager, use this parameter to enable search on all managed units. For example, `all=true`. This parameter is optional.
api_target_host	hostname or IP address	In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM. Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed units, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM This parameter is optional.
extraction_start	date	Define the date by which to start the extraction of audit data for search. If this parameter is omitted, extraction starts immediately. This parameter is optional.
includeViolations	`true` or `false`	Determine whether to include violations in the search indexes. Omitting violations can help reduce the size of search indexes. This parameter is optional.

schedule_interval	integer	Used with the schedule_units parameter to define the interval for extracting audit data. For example, `schedule_interval=2 schedule_units=MINUTE`. This parameter is required.
schedule_start	date	Date on which to begin following the extraction interval defined by the schedule_interval and schedule_units parameters. This parameter is optional.
schedule_units	`HOUR` or `MINUTE`	Used with the schedule_interval parameter to define the interval for extracting audit data. For example, `schedule_interval=2 schedule_units=MINUTE`. This parameter is required.

set_enterprise_search_options

Define the search mode for the Investigation Dashboard .

```
grdapi set_enterprise_search_options distributed_search=[value]
```

For example, the following command configures the Investigation Dashboard in all_machines mode to allow searching of data across the entire Guardium environment from any Guardium machine in that environment: `grdapi set_enterprise_search_options distributed_search=all_machines`.

Parameter	Value	Description
api_target_host	hostname or IP address	In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM. Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed units, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM This parameter is optional.
distributed_search	cm_only, local_only, or all_machines	cm_only Searches submitted from a Central Manager return results from across the Guardium environment, but searches submitted from managed units only return local results from that managed units local_only Searches submitted from individual machines return results from that machine only. There is no ability to search data from across the Guardium environment. all_machines Searches can be submitted from any machine and return results from across the Guardium environment. This parameter is required, and the default value is cm_only.

Parent topic: GuardAPI Reference

GuardAPI Native Audit Functions

Use these GuardAPI commands to enable, disable, DB Audit (native audit) on a cloud database; add and remove objects from the Object Audit (audit trail); get configuration, collectors and objects.

add_ip_to_sg

Adds the specified Guardium IP to the cloud security group.

```
add_objects_native_audit parameter=value
```

Parameter	Value	Description
datasource_name	string.	Required. Cloud datasource defined in Guardium
api_target_host	hostname or IP address	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM

add_objects_native_audit

Adds objects to the Object Audit (audit trail) on the specified datasource.

```
add_objects_native_audit parameter=value
```


Parameter	Value	Description
datasource_name	string	Required. Cloud datasource defined in Guardium
objects	string.	Comma separated list of objects. View objects with the get_native_audit_objects or in the GUI.
api_target_host	hostname or IP address	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM

disable_native_audit

Disables DB Audit (native audit) on the specified cloud datasource.

`disable_native_audit parameter=value`

Parameter	Value	Description
datasource_name	string	Required. Cloud datasource defined in Guardium
api_target_host	hostname or IP address	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM

enable_native_audit

Enable DB Audit (native audit) on the specified datasource.

`enable_native_audit parameter=value`

Parameter	Value	Description
datasource_name	string	Required. Cloud datasource defined in Guardium
api_target_host	hostname or IP address	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM

get_native_audit_collectors

Returns the name of the collector, in your environment, that is receiving data from the specified host, port, and service name.

`get_native_audit_collectors parameter=value`

Parameter	Value	Description
host	string	Required. AWS host name
port	integer	Required.
service_name	string	Required.
api_target_host	hostname or IP address	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM

get_native_audit_configurations

Returns all details on the specified host, port, service name: cloud environment id, cloud environment, provider, datasource id, instance name, database engine, service name, host, port, Guardium security group, objects limit, objects, collector.

`get_native_audit_configurations parameter=value`

Parameter	Value	Description
host	string	Required. AWS host name
port	integer	Required.
service_name	string	Required.
api_target_host	hostname or IP address	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM

get_native_audit_objects

Returns all objects found by the classification process on the specified host, port, service name.

`get_native_audit_objects parameter=value`

Parameter	Value	Description
host	string	Required. AWS host name
port	integer	Required.
service_name	string	Required.
api_target_host	hostname or IP address	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM

remove_objects_native_audit

Disable the object audit (audit trail) on the specified objects in the specified datasource.

`remove_objects_native_audit parameter=value`

Parameter	Value	Description
datasource_name	string	Required. Cloud datasource defined in Guardium
objects	string	Comma separated list of objects. View objects with the get_native_audit_objects or in the GUI.
api_target_host	hostname or IP address	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM

Parent topic: GuardAPI Reference

GuardAPI Outliers Detection Functions

Use the following GuardAPI commands to enable, disable, and configure the Outliers Detection function.

grdapi enable_outliers_detection_agg

grdapi enable_outliers_detection_agg

grdapi disable_outliers_detection_agg

Run on a central manager to enable or disable sending export data from all collectors in the CM environment that send their data to the specified aggregator, except a collector that is running outliers detection locally. Data is collected hourly and sent to the aggregator for outliers detection processing. A distributed report mechanism is used to extract and send data to an aggregator.

Table 1. grdapi enable_outliers_detection_agg

Parameter	Value	Description
schedule_interval	1	Mandatory. Must be set to 1
schedule_units	hour	Mandatory. Must be set to hour
aggregator_host_name		The specific aggregator enabled/disabled for outlier detection.
DAM_FAM	DAMorFAM	Optional. Specifies the type of outliers. The default is DAM.

grdapi enable_outliers_detection

grdapi enable_outliers_detection

grdapi disable_outliers_detection

Run on a collector to enable/disable outliers detection locally on the collector.

Parameter	Value	Description
schedule_interval	1	Mandatory. Must be set to 1
schedule_units	hour	Mandatory. Must be set to hour
DAM_FAM	DAMorFAM	Optional. Specifies the type of outliers. The default is DAM.

grdapi set_outliers_detection_parameter privUsersGroupIds

Add additional user groups to the outlier detection algorithm. Use this command to find a group ID: grdapi list_group_by_desc desc=[group name]

Parameter	Value	Description
privUsersGroupIds	string	One or more admin user group IDs.
sensitiveObjectGroupIds	string	One or more sensitive object group IDs.

Parent topic: GuardAPI Reference

GuardAPI Process Control Functions

Use these GuardAPI commands to execute, copy, upload, list, and delete Process Control Functions.

execute_cls_process

Executes (submits) a classification process. It is equivalent of executing Run Once Now from Classification Process Builder. It submits the job which places the process on the Guardium® Job Queue, from which the appliance runs a single job at a time. Administrators can view the job status by selecting Guardium Monitor > Guardium Job Queue.

Note: Create a classification process before calling this API.

Parameter	Value	Description
processName	string	Name of the classification process
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi execute_cls_process processName="classPolicy1"
```

execute_assessment

Executes (submits) a security assessment. It is equivalent of executing Run Once Now from Security Assessment Finder. It submits the job. This places the process on the Guardium Job Queue, from which the appliance runs a single job at a time. Administrators can view the job status by selecting Guardium Monitor > Guardium Job Queue.

Note: Create a Security Assessment before calling this API.

Parameter	Value	Description
assessmentDesc		Name of the assessment
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi execute_assessment assessmentDesc="assessment1"
```

execute_auditProcess

Executes an Audit process. Runs the specified audit process. It is equivalent of executing Run Once Now from Audit Process Builder.

Note: Create an audit process before calling this API.
Note: If the audit report returns a lot of data, the user should execute the audit process from the GUI, due to CLI command heap size limitation.

Parameter	Value	Description
auditProcess		Name of the audit process
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi execute_auditProcess  auditProcess="Appliance Monitoring"
```

stop_audit_process

The stop_audit_process API can not be used through the GuardAPI command line. This function is only usable as an invocation through a drill down. See the sub-topic, Stop an audit process, in Compliance Workload Automation help topic.

Parameter	Value	Description
process		Name of the audit process
run		The RunID of the audit process
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
stop_audit_process
```

execute_populateGroupFromQuery

Executes a populate group from query. It populates the chosen group by executing a configured query. It is the equivalent of executing Run Once Now from Populate Group From Query Set Up screen. If the group is not configured for import, it displays an error message.

Note: This grdapi can only be used for groups that have already been configured in Populate Group From Query Set Up screen (query should have been chosen and parameters should have been set)

Parameter	Value	Description
groupDesc		Group name
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi execute_populateGroupFromQuery  groupDesc="A test"
```

grdapi execute_appUserTranslation

Execute an application user translation. Imports the user definitions for all configured applications in Application User Translation Configuration screen. It is equivalent of executing Run Once Now from Application User Translation Configuration screen.

Note: To run this grdapi, must define at least one Application User Detection in Application User Translation Configuration screen. If not a message will be displayed.

Parameter	Value	Description
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi execute_appUserTranslation
```

execute_flatLogProcess

Merges the flat log information to the internal database. It is equivalent of executing Run Once Now from Flat Log Process screen.

Note: This grdapi can only be executed if Flat Log Process is configured as Process in Flat Log Process screen. If not, an error message will be displayed.

Parameter	Value	Description

Parameter	Value	Description
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi execute_flatLogProcess
```

execute_incidentGenProcess

Executes a query which is defined for the selected incident generation process, using the processId, against the policy violations log. It generates incidents based on that query. It is equivalent of executing Run Once Now from Edit Incident Generation Process screen.

Note: Create a Incident Generation Process before calling this API.

Parameter	Value	Description
processID		Process ID of the incident
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi execute_incidentGenProcess   processId=20003
```

execute_incidentGenProcess_byDetails

Executes a query which is defined for the selected incident generation process, using the query name, against the policy violations log. It generates incidents based on that query. It is equivalent of executing Run Once Now from Edit Incident Generation Process screen.

Note: Create a Incident Generation Process before calling this API.

Parameter	Value	Description
queryName		Query name

Parameter	Value	Description
categoryName		Category Name
user		User
threshold		Threshold
severity		Severity level
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi  execute_incidentGenProcess_byDetails  queryName="Policy Violation Count" user=admin severity=info
```

upload_custom_data

Executes (submits) a classification process. Uploads data to the custom table specified by tableName. It is the equivalent of executing Upload from Import Data screen of Custom Table Builder. To run this grdapi, must first configure the specified custom table in Import Table Structure of Custom Table Builder. From the UI, go to Tools/Report Builder/Custom Table Builder, select a Custom Table, click upload data, and select datasource.

Parameter	Value	Description
tableName	existingcustomtable	Name of custom table

Parameter	Value	Description
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi upload_custom_data tableName="TEST_TABLE"
```

execute_ldap_user_import

Import LDAP users. It imports Guardium user definitions from an LDAP server configured in LDAP User Import screen. It is equivalent of executing Run Once Now from LDAP User Import screen. (login in as accessmgr /LDAP Import)

Note: LDAP must be configured. Otherwise, the system will give an error message.

Parameter	Value	Description
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi execute_ldap_user_import
```

policy_install

Install a policy or multiple policies. If multiple policies are to be installed then the policies need to be delimited by a pipe character '|' with policies being in the order you want to be installed. This needs to be done even if only one policy might have had changes.

Install multiple policies with grdapi policy_install command. Install by position by specifying the policies in the order that you want to install.

Even in UI, when you install a policy after another installed policy, it will reinstall all of them. which is the same as grdapi policy_install command.

Parameter	Value	Description
policy		Policy name

Parameter	Value	Description
api_target_host		In a central management configuration only, allows the user to specify a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Examples

```
grdapi policy_install policy="Policy 1|Policy 2"
```

```
grdapi policy_install policy="policy 20|policy 30|policy 40"
```

delete_policy

Use the delete_policy command to delete a policy specified by the policyDesc parameter.

Parameter	Value	Description
policyDesc		Policy name.
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi delete_policy policyDesc="Hadoop Policy"
```

list_policy

Use the list_policy command to display a list of available policies or to display details about a single policy.

Parameter	Value	Description
policyDesc		Policy name. If unspecified, the list_policy command returns a list of available policies.
detail		Accepts values of true or false. The default value is true and returns policy details. Specifying a value of false returns only policy names.

Parameter	Value	Description
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Examples

Display details of a specific policy:

```
grdapi list_policy policyDesc="Hadoop Policy"
```

Display a detailed list of available policies:

```
grdapi list_policy
```

Display a list of available policy names (no details):

```
grdapi list_policy detail=false
```

copy_rule

Copy a rule <ruleDesc> of <fromPolicy> to the end of <toPolicy> rule's list.

Note: It Copies a rule of <fromPolicy> to the end of <toPolicy> rule's list. Both <fromPolicy> and <toPolicy> must be created, before running this grdapi.

Parameter	Value	Description
ruleDesc		Rule Description
fromPolicy		Policy name
toPolicy		Policy name
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi copy_rule ruleDesc="Rule Description" fromPolicy="policy1"  toPolicy=" policy2  "
```

clone_policy

Use this GuardAPI command to clone a policy.

Parameter	Value	Description
policyDesc		Policy name
clonedpolicyDesc		Cloned Policy name
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi clone_policy policyDesc="Hadoop Policy" clonedPolicyDesc="Hadoop Policy cloned1"
```

update_rule

Update policy rule. Update a rule <ruleDesc> of <fromPolicy> for a rule parameter.

See Policies for additional information on the following policy rule parameters that can be altered with the update_rule API call.

Parameter	Value	Description
ruleDesc		Rule Description
fromPolicy		Policy name
newDesc		New Rule Description
clientIP		Client IP
clientNetMask		Client Net Mask
serverIP		Server IP
serverNetMask		Server Net Mask
objectName		Object Name
sourceProgram		Source Program
dbName		Database Name
dbUser		Database User
command		Command
appUserName		Application User Name
dateTime		Date and Time
logFlag		Log Flag
exceptionType		Exception Type
minCount		Minimum Count
continueToNext		Continue to Next
resetInterval		Reset Interval
serviceName		Service Name
osUser		O/S User
dbType		Database Type
netProtocol		Net Protocol
clientMac		Client MAC

Parameter	Value	Description
fieldName		Field Name
pattern		Patter
appEventExists		Application Event Exists
eventType		Event Type
appEventStrValue		Application Event String Value
appEventNumValue		Application Event Number Value
appEventDate		Application Event Date
eventUserName		Event User Name
errorCode		Error Code
severity		Severity
category		Category
classification		Classification
dataPattern		Data Pattern
sqlPattern		SQL Pattern
xmlPattern		XML Patter
mvcSystem		MVS™ System
clientIpNotFlag		Client IP Not Flag
serverIpNotFlag		Server IP Not Flag
objectNameNotFlag		Object Name Not Flag
sourceProgramNotFlag		Source Program Not Flag
dbNameNotFlag		Database Name Not Flag
dbUserNotFlag		Database User Not Flag
commandNotFlag		Command Not Flag
appUserNameNotFlag		Application User Name Not Flag
exceptionTypeIdNotFlag		Exception Type ID Not FLag
serviceNameNotFlag		Service Name Not Flag
osUserNotFlag		O/S User Not Flag
clientMacNotFlag		Client MAC Not Flag
fieldNameNotFlag		Field Name Not Flag
errorCodeNotFlag		Error Code Not Flag
replacementChar		Replacement Character
messageTemplate		Message Template
recordsAffectedThreshold		Records Affected Threshold
matchedReturnedTreshold		Matched Returned Treshold
clientIpGroup		Client IP Group
serverIpGroup		Server IP Group
objectGroup		Object Group
objectCommandGroup		Object Command Group
objectFieldGroup		Object Field Group
dbUserGroup		Database User Group
commandsGroup		Commands Group
dbNameGroup		Database Name Group
sourceProgramGroup		Source Program Group
appUserGroup		Application User Group
serviceNameGroup		Service Name Group
osUserGroup		O/S User Group
netProtocolGroup		Net Protocol Group
fieldNameGroup		Field Name Group
errorGroup		Error Group

Parameter	Value	Description
appEventStrGroup		Application Event String Group
clientProgramUserServerInstanceGroup		Client Program User Server Instance Group
quarantineMinutes		Quarantine Minutes
clientInfo		Use for DB2 and DB2_COLLECTION_PROFILE
clientInGroup		Use for DB2_COLLECTION_PROFILE
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi update_rule ruleDesc="Rule Description" fromPolicy="policy1"  serviceName="ANY"
```

change_rule_order

Change policy rule order. Change the ordered position of a rule within a policy.

Parameter	Value	Description
fromPolicy		Policy name
order		New order position for Rule
ruleDesc		Rule Description
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi change_rule_order ruleDesc="Copy of policy1 exception1"  fromPolicy="policy1"  order=10
```

list_policy_rules

List the rules for a policy.

Parameter	Value	Description
policy		Policy name
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi list_policy_rules  policy="policy1"
```

delete_rule

Remove a rule from a policy.

Parameter	Value	Description
fromPolicy		Policy name
toPolicy		Policy name
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi delete_rule ruleDesc="Copy (3) of policy1 exception1"  fromPolicy="policy1"
```

uninstall_policy_rule

Use the uninstall_policy_rule command to uninstall the policy rule(s) specified by the policy and ruleName parameters.

Parameter	Value	Description
policy		Policy name.
ruleName		Rule name(s). Specify multiple policy rules using the pipe character, for example `ruleName="rule1|rule2|rule3`.

Parameter	Value	Description
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Examples

Uninstall a single policy rule:

```
grdapi uninstall_policy_rule policy="Hadoop Policy" ruleName="Low interest Objects: Allow"
```

Uninstall multiple policy rules:

```
grdapi uninstall_policy_rule policy="Hadoop Policy" ruleName="Low interest Objects: Allow|Low Interest Commands: Allow"
```

reinstall_policy_rule

Use the reinstall_policy_rule command to reinstall the policy rule(s) specified by the policy and ruleName parameters.

Parameter	Value	Description
policy		Policy name.
ruleName		Rule name(s). Specify multiple policy rules using the pipe character, for example `ruleName="rule1|rule2|rule3`.
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Examples

Reinstall a single policy rule:

```
grdapi reinstall_policy_rule policy="Hadoop Policy" ruleName="Low interest Objects: Allow"
```

Reinstall multiple policy rules:

```
grdapi reinstall_policy_rule policy="Hadoop Policy" ruleName="Low interest Objects: Allow|Low Interest Commands: Allow"
```

delete_Audit_process_result

Use this command to delete any audit process results.

Parameter	Value	Description
ExecutionDateFrom		When did audit process begin
ExecutionDateTo		When did audit process end
ProcessName		Required. What is name of audit process
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi delete_Audit_process_result ExecutionDateFrom=, ExecutionDateTo=, ProcessName=abab
```

create_api_parameter_mapping

Map API parameters to Domain entities and attributes so the parameters can be populated by report values on API call generation or API automation.

Note: The Mapping GuardAPI Parameters to Domain Entities and Attributes in GuardAPI Input Process Generation shows the domains, entities and attributes of the system and has a GUI interface to invoke this API function.

Parameter	Value	Description
functionName		Name of the API function
parameterName		Name of the parameter within the API function to be mapped
domain		Any of the Guardium reporting domains such as Access, Alert, Discovered Instances, Exceptions, Group Tracking, etc.
entityLabel		Any of the entities for the reporting domain
attributeLabel		Any of the attributes within the entity
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi create_api_parameter_mapping functionName="create_group" parameterName="desc" domain="Group Tracking" entityLabel="Group"
attributeLabel="Group Description"
```

list_param_mapping_for_function

List the parameter mappings for an API function.

Note: The Mapping GuardAPI Parameters to Domain Entities and Attributes in GuardAPI Input Process Generation shows the domains, entities and attributes of the system and has a GUI interface to invoke this API function.

Parameter	Value	Description
functionName		Name of the API function
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi list_param_mapping_for_function functionName="create_group"
```

delete_api_parameter_mapping

Delete API Parameter Mappings for Domain Entities and Attributes. Remove the parameter mappings for an API function.

Note: The Mapping GuardAPI Parameters to Domain Entities and Attributes in GuardAPI Input Process Generation shows the domains, entities and attributes of the system and has a GUI interface to invoke this API function.

Parameter	Value	Description
functionName		Name of the API function
parameterName		Name of the parameter within the API function to be mapped
domain		Any of the Guardium reporting domains such as Access, Alert, Discovered Instances, Exceptions, Group Tracking, etc.
entityLabel		Any of the entities for the reporting domain
attributeLabel		Any of the attributes within the entity
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi delete_api_parameter_mapping functionName="create_group" parameterName="desc" domain="Group Tracking" entityLabel="Group"
attributeLabel="Group Description"
```

close_default_events

Close all the events defined on a specific process/task/execution. Close all the events defined on a specific process/task/execution for tasks of type report. Specially needed if for example there is a task with a default event that returned a large number of records, such task can not be signed unless all the events are closed.

Parameter	Value	Description
eventStatus		Required. Event status. Must be a valid status for the default event defined for the audit task and must be a final status.
execDate		Required. Execution Date and Time
processDesc		Required. Audit process description.
taskDesc		Required. Audit task description.
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi close_default_events eventStatus=Done execDate="2010-03-01 08:00:00" processDesc="Audit Process" taskDesc="Task Description"
```

create_quarantine_allowed_until

Use in Policies.

Parameter	Value	Description
allowedUntil		Required.
dbUser		Required. Database user
serverIP		Required. Server IP
serverName		Required. Server name
Type		Required. Value must be one of: normal, DB2z, or IMS.
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

create_quarantine_until

Use in Policies.

Parameter	Value	Description
quarantineUntil		Required.
dbUser		Required. Database user
serverIP		Required. Server IP
serverName		Required. Server name
Type		Required. Value must be one of: normal, DB2z, or IMS.
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

delete_quarantine_until

Use in Policies.

Parameter	Value	Description
quarantineUntil		Required.
dbUser		Required. Database user
serverIP		Required. Server IP
serverName		Required. Server name
Type		Required. Value must be one of: normal, DB2z, or IMS.
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

must_gather

Use grdapi must_gather command to collect information on the state of the Guardium system that can be used by Guardium Support. See Basic information for IBM Support for further information on this topic.

Parameter	Value	Description
commandsList		String - required
description		String - required
duration		Integer - required
emailDestination		String - required
invokingUser		String - required
maxLength		Integer - required
pmrNumber		String - required
start		Date - required
timestamp		Date - required
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

restart_job_queue_listener

Use the restart_job_queue_listener command to restart the job queue listener if the job queue fails to start, does not run waiting jobs, or if a job appears stuck in running or stopping status for a prolonged period of time. Issuing this command immediately restarts the job queue, and any currently executing jobs will be halted and restarted.

Example:

```
grdapi restart_job_queue_listener
```

The restart_job_queue_listener command does not accept any parameters.

update_quarantine_allowed_until

Use in Policies.

Parameter	Value	Description
allowedUntil		Required.
dbUser		Required. Database user
serverIP		Required. Server IP
serverName		Required. Server name
Type		Required. Value must be one of: normal, DB2z, or IMS.

Parameter	Value	Description
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

update_quarantine_until

Use in Policies.

Parameter	Value	Description
quarantineUntil		Required.
dbUser		Required. Database user
serverIP		Required. Server IP
serverName		Required. Server name
Type		Required. Value must be one of: normal, DB2z, or IMS.
api_target_host	hostnameorIPaddress	Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Parent topic: GuardAPI Reference

GuardAPI Query Rewrite Functions

Automate testing or create definitions for certain complex queries that cannot be done from the user interface by using Guardium APIs at the command-line interface.

Note: If you create query rewrite definitions by using APIs, you can still use the UI to retrieve those definitions for testing with the Query Rewrite Builder.

The GuardAPI functions related to query rewrite include:

assign_qr_condition_to_action

create_qr_action

create_qr_add_where

create_qr_add_where_by_id

create_qr_condition

create_qr_definition

create_qr_replace_element

create_qr_replace_element_byId

list_qr_action

list_qr_add_where

list_qr_add_where_by_id

list_qr_condition

list_qr_condition_to_action

list_qr_definitions

list_qr_replace_element

list_qr_replace_element_byId

remove_all_qr_replace_elements

remove_all_qr_replace_elements_byId

remove_qr_action

remove_qr_add_where_by_id

remove_qr_condition

remove_qr_definition

remove_qr_replace_element_byId

update_qr_action

update_qr_add_where_by_id

update_qr_condition

update_qr_definition

update_qr_replace_element_byId

assign_qr_condition_to_action

Create an association between a query rewrite condition and an associated action.

Parameter	Value	Description
actionName		Required. The name of the query rewrite action.
conditionName		Required. The name of the query rewrite condition to be associated with the specified action.
definitionName		Required. The name of the query rewrite definition that is associated with the specified condition and action.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

```
grdapi assign_qr_condition_to_action definitionName="case 15" actionName="qr action15_2" conditionName="qr cond15_2"
```

create_qr_action

Create a query rewrite action for a specified query rewrite definition.

Parameter	Value	Description
actionName		Required. The unique name of the query rewrite action.
definitionName		Required. The query rewrite definition that is associated with this action.
description		An optional description.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

```
grdapi create_qr_action definitionName="case 15" actionName="qr action15_3"
```

create_qr_add_where

Associate a query rewrite function to add a WHERE condition to the specified query rewrite action.

Parameter	Value	Description
actionName		Required. The unique name of the query rewrite action.
definitionName		Required. The query rewrite definition that is associated with this action.
whereText		Text to add to a WHERE clause.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

grdapi create_qr_add_where definitionName="qrw_def_Oracle_1" actionName="qrw_act__addwhere_id2" whereText="id=2"

create_qr_add_where_by_id

Associate a query rewrite function to add a WHERE condition to the specified query rewrite action.

Parameter	Value	Description
qrActionId		Required (integer). The unique ID of query rewrite action.
whereText		Text to add to a WHERE clause.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

grdapi create_qr_add_where_by_id qrActionId=10002 whereText="id=2"

create_qr_condition

Create a query rewrite condition.

Parameter	Value	Description
conditionName		Required. The unique name of this query rewrite condition.
definitionName		Required. The query rewrite definition that is associated with this condition.
depth		Integer that specifies the depth of the parsed SQL that this condition applies to (1 and higher). The default -1 means that the query rewrite condition applies to any matching SQL at any depth.
isForAllRuleObjects		True or false. Use this parameter to associate this condition with objects in a policy access rule. True indicates that the specified condition applies to all objects in the access rule's Object field or Object group for a fired rule. The default is false, which means the query condition is specified using the objects that are defined in this condition. Neither option impacts any rule triggering behavior.
isForAllRuleVerbs		True or false. Use this parameter to associate this condition with objects in a policy access rule. True, indicates that the specified condition applies to all verbs in the access rule's Verb field or Verb group for a fired rule. The default is false, which means the query condition is specified using the verbs that are defined in this condition. Neither option impacts any rule triggering behavior.
isObjectRegex		True or false. Indicates that the specified object is specified by using a regular expression. Default is false.
isVerbRegex		True or false. Indicates that the specified verb is specified by using a regular expression. Default is false.
object		An object (table, view). The default "*" means all objects. This can also be specified as a regular expression, in which case set the isVerbRegex to True.
order		Used to specify the order in which to assemble multiple related query rewrite conditions for complex SQL. Default is 1.
verb		A verb (select, insert, update, delete). The default "*" means all verbs.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

grdapi create_qr_condition definitionName="case 15" conditionName="qr cond15_3" verb=select isForAllRuleObjects=false object=* depth=2 order=3

create_qr_definition

Create a query rewrite definition.

Parameter	Value	Description
dataBaseType		Required. The type of database this query rewrite definition is associated with. Acceptable values are: ORACLE or DB2.
definitionName		Required. A unique name for this query rewrite definition condition.
description		An optional description.
isNegateQrCond		Indicates whether there is a NOT flag on the set of query rewrite conditions that are associated with this definition.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

grdapi create_qr_definition dataBaseType="ORACLE" definitionName="case 15"

create_qr_replace_element

Create a replacement element, or set of elements, such as an entire SQL sentence or a SELECT list.

Parameter	Value	Description
actionName		Required. The unique name of the query rewrite action this rewrite function is associated with.
definitionName		Required. A unique name for this query rewrite definition condition.
isFromAllRuleElements		True or false. Indicates that this action applies to all FROM elements. Default is false.
isFromRegex		True or false. Indicates that the 'from' element is specified by using a regular expression. Default is false.
isReplaceToFunction		True or false. Indicates that the "replace to" is the name of a function, such as user-defined function.
replaceFrom		The incoming string for a matching rule that is to be replaced. Use replaceType to indicate specifically which element of the incoming query to examine.
replaceTo		The replacement string for the matching element.
replaceType		Required. Indicates what is to be replaced. Must be one of the following: • SELECT • VERB • OBJECT • SENTENCE • SELECTLIST
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

grdapi create_qr_replace_element definitionName="case 15" actionName="qr action15_2" replaceType=VERB replaceFrom="select" replaceTo="select++"

create_qr_replace_element_byId

Create a replacement specification for a specified query rewrite action.

Parameter	Value	Description
isFromAllRuleElements		True or false. Indicates that this action applies to all FROM elements. Default is false.
isFromRegex		True or false. Indicates that the "from" element is specified by using a regular expression. Default is false.
isReplaceToFunction		True or false. Indicates that the "replace to" is the name of a function, such as user-defined function.
qrActionId		Required (integer). The unique ID of query rewrite action.
replaceFrom		The incoming string for a matching rule that is to be replaced. Use replaceType to indicate specifically which element of the incoming query to examine.
replaceTo		The replacement string for the matching element.
replaceType		Required. Indicates what is to be replaced. Must be one of the following: • SELECT • VERB • OBJECT • SENTENCE • SELECTLIST

Parameter	Value	Description
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

grdapi create_qr_replace_element_byId qrActionID="1116" replaceType=OBJECT replaceFrom="employee" replaceTo="employee_2"

list_qr_action

Lists query actions for a specified query definition.

Parameter	Value	Description
actionName		The name of the query rewrite action.
definitionName		Required. The query rewrite definition name.
detail		True or false. The default is true, which lists all the associated attributes of the actions. Only the name is returned for false.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

grdapi list_qr_action definitionName="case 2"

Output:

```
qrwg1.guard.swg.usma.ibm.com> grdapi list_qr_action definitionName="case 2"
########################################################################


         QR actions of definition 'case 2' - (id = 1 )

########################################################################
qr action ID: 1
qr action name: qr action2
qr action description: add where by id

ok
Example:
grdapi list_qr_action definitionName="case 2" detail=false

Output:

qrwg1.guard.swg.usma.ibm.com> grdapi list_qr_action definitionName="case 2" detail=false
################################
         QR actions of definition 'case 2' - (id = 1 )
################################
qr action2
ok
```

list_qr_add_where

Lists "add where" functions for a specified query action and query definition pair.

Parameter	Value	Description
actionName		The name of the query rewrite action.
definitionName		Required. The query rewrite definition name.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

grdapi list_qr_add_where actionName="qrw_act_addwhere_id2" definitionName="qrw_def_Oracle_1"

list_qr_add_where_by_id

Lists "add where" functions for a specified query action.

Parameter	Value	Description
qrActionId		Required (integer). The unique identifier for the query rewrite action.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

grdapi list_qr_add_where_by_id qrActionId=20023

list_qr_condition

Lists the query rewrite conditions that are associated with a particular query rewrite definition.

Parameter	Value	Description
conditionName		The name of a query rewrite condition.
definitionName		Required. A query rewrite definition.
detail		True or false. The default is true, which lists all the associated attributes of the conditions. Only the name is returned for false.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

grdapi list_qr_condition definitionName="case 2" conditionName="qr cond2"

Output:

```
qrwg1.guard.swg.usma.ibm.com> grdapi list_qr_condition definitionName="case 2" conditionName="qr cond2"
########################################################################
         QR Condtions of Definition 'case 2' - (id = 1 )

########################################################################

qr condition id: 1
qr condition name: qr cond2
qr definition ID: 1
qr condition verb: *
qr condition object: *
qr condition dept: -1
is verb regex: false
is object regex: false
is action for all rule verbs: false
is action for all rule objects: false
qr condition order: 1
```

list_qr_condition_to_action

Lists the associations between a query rewrite condition and a query rewrite action for a particular query definition.

Parameter	Value	Description
actionName		Required (integer). The unique identifier for the query rewrite action.
definitionName		Required. A query rewrite definition.
Detail		True or false. The default is true, which lists all the associated attributes of the conditions for the specified action and definition. Only the name is returned for false.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

grdapi list_qr_condition_to_action actionName="qr action15_2" definitionName="case 15"

Output:

```
qrwg1.guard.swg.usma.ibm.com> grdapi list_qr_condition_to_action actionName="qr action2" definitionName="case 2"
########################################################################

         QR Condtions of Action 'qr action2' - (id = 1 )

########################################################################

qr condition id: 1
qr condition name: qr cond2
qr definition ID: 1
qr condition verb: *
qr condition object: *
qr condition dept: -1
is verb regex: false
is object regex: false
is action for all rule verbs: false
is action for all rule objects: false
qr condition order: 1
```

list_qr_definitions

Lists query rewrite definitions.

Parameter	Value	Description
definitionName		Required. A query rewrite definition.

Parameter	Value	Description
Detail		True or false. The default is true, which lists all the associated attributes of the conditions for the specified action and definition. Only the name is returned for false.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

grdapi list_qr_definitions

Output:

```
qrwg1.guard.swg.usma.ibm.com> grdapi list_qr_definitions
######################################################################
         QR  Definitions

######################################################################
qr definition ID: 1
qr definition name: case 2
qr definition description:
is negation set on qr conditions: false
```

list_qr_replace_element

Lists replacements for a specified query rewrite action and query rewrite definition pair.

Parameter	Value	Description
actionName		Required. A query rewrite action.
definitionName		Required. A query rewrite definition.
Detail		True or false. The default is true, which lists all the associated attributes of the replacement elements for the specified action and definition. Only the names are returned for false.
replaceType		If specified, must be one of the following: • SELECT • VERB • OBJECT • SENTENCE • SELECTLIST
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

grdapi list_qr_replace_element actionName="qr action2" definitionName="case 2"

Output:

```
qrwg1.guard.swg.usma.ibm.com> grdapi list_qr_replace_element actionName="qr action2" definitionName="case 2"
######################################################################
         QR replace elements for action 'qr action2' - (qrActionId = 1 )

######################################################################
```

```
qr replace element ID: 1
qr replace type: object
qr replace from: emp
qr replace to: NEW_EMP
qr is from regex: false
qr is from all rule elements: false

**************************************************************************
qr replace element ID: 2
qr replace type: selectList
qr replace from: Whole select list
qr replace to: EMPNO,SAL
qr is from regex: false
qr is from all rule elements: false
```

list_qr_replace_element_byId

Lists replacements for a specified query rewrite action.

Parameter	Value	Description
detail		True or false. The default is true, which lists all the associated attributes of the replacement elements for the specified action and definition. Only the names are returned for false.
qrActionId		Required (integer). The unique identifier for the query rewrite action.
replaceType		If specified, must be one of the following: • SELECT • VERB • OBJECT • SENTENCE • SELECTLIST
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

grdapi list_qr_replace_element_byId detail=true qrActionId="22222" replaceType="OBJECT"

remove_all_qr_replace_elements

Deletes query replacement specifications from the system.

Parameter	Value	Description
actionName		Required. A query rewrite action.
definitionName		Required (integer). The unique identifier for the query rewrite action.
replaceType		If specified, must be one of the following: • SELECT • VERB • OBJECT • SENTENCE • SELECTLIST

Parameter	Value	Description
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

grdapi remove_all_qr_replace_elements definitionName="new case 2" actionName="new qr action2“

remove_all_qr_replace_elements_byId

Deletes query replacement specifications from the system.

Parameter	Value	Description
qrActionId		Required (integer). A query rewrite action identifier.
definitionName		Required. A query rewrite definition.
replaceType		If specified, must be one of the following: • SELECT • VERB • OBJECT • SENTENCE • SELECTLIST If replaceType is not specified, then all replacements for the specified action and definition is deleted.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

grdapi remove_all_qr_replace_elements actionName="qr action15_2" definitionName="case 15" replaceType="OBJECT"

remove_qr_action

Deletes a specified query rewrite action from the system.

Parameter	Value	Description
actionName		Required. A query rewrite action.
definitionName		Required. A query rewrite definition.

Parameter	Value	Description
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

grdapi remove_qr_action actionName="qr action15_2" definitionName="case 15"

remove_qr_add_where_by_id

Deletes a specified "add where" function from the system.

Parameter	Value	Description
qrAddWhereId		Required (integer). An "add where" function.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

grdapi remove_qr_add_where_by_id qrAddWhereId=22666

remove_qr_condition

Deletes a query rewrite condition from the system.

Parameter	Value	Description
conditionName		Required. A query rewrite condition.
definitionName		Required. A query rewrite definition.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

grdapi remove_qr_condition conditionName="qr cond15_1" definitionName="case 15"

remove_qr_definition

Deletes a query rewrite definition from the system.

Parameter	Value	Description
definitionName		Required. A query rewrite definition.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

grdapi remove_qr_definition definitionName="case 15"

remove_qr_replace_element_byId

Deletes a specified query element replacement from the system.

Parameter	Value	Description
qrReplaceElementId		Required (integer). A replacement definition ID.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

grdapi qrReplaceElementId=33333

update_qr_action

Updates an existing query rewrite action with a new name and optional description.

Parameter	Value	Description
actionName		Required. The unique name of the query rewrite action.
definitionName		Required. The query rewrite definition that is associated with this action.
description		An optional description.
newName		The new name for the query rewrite action.

Parameter	Value	Description
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

grdapi update_qr_action definitionName="case 2" actionName="qr action2" newName="new qr action2"

update_qr_add_where_by_id

Allows update of an existing "add where" function with new replacement text.

Parameter	Value	Description
qrAddWhereId		Required (integer). The unique identifier for the query rewrite "add where" function.
whereText		The replacement text for the identified where clause.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

grdapi update_qr_add_where_by_id 22222 whereText="1=2"

update_qr_condition

Update an existing query rewrite condition.

Parameter	Value	Description
conditionName		Required. The unique name of this query rewrite condition.
definitionName		Required. The query rewrite definition that is associated with this condition.
depth		Integer that specifies the depth of the parsed SQL that this condition applies to (1 and higher). The default -1 means that the query rewrite condition applies to any matching SQL at any depth.
isForAllRuleObjects		True or false. Indicates that the specified condition applies to all objects for the fired rule. Default is false.
isForAllRuleVerbs		True or false. Indicates that the specified condition applies to all verbs for the fired rule Default is false.
isObjectRegex		True or false. Indicates that the specified object is specified by using a regular expression. Default is false.
isVerbRegex		True or false. Indicates that the specified verb is specified by using a regular expression. Default is false.
newName		The new name for the query rewrite condition.

Parameter	Value	Description
Object		An object (table or view). The default "*" means all objects. This can also be specified as a regular expression, in which case set the isVerbRegex to True.
Order		Used to specify the order in which to assemble multiple related query rewrite conditions for complex SQL. Default is 1.
Verb		A verb (select, insert, update, delete). The default "*" means all verbs.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

grdapi update_qr_condition definitionName="case 16" conditionName="qr cond15_3" newName="qr cond16_3" verb=select object=* dept=2 order=3

update_qr_definition

Update an existing query rewrite definition.

Parameter	Value	Description
dataBaseType		Required. The type of database this query rewrite definition is associated with. Must be either ORACLE or DB2.
definitionName		Required. A unique name for this query rewrite definition condition.
description		An optional description.
isNegateQrCond		Indicates whether there is whether there is a NOT flag on the set of query rewrite conditions that are associated with this definition.
newName		Optional. Specify a new unique name.
sampleSql		Optional. Specify a sample SQL statement. In most cases, you will not use this unless you want to use the inputted sample SQL later in the UI.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

```
grdapi update_qr_definition dataBaseType="DB2" definitionName="case 15" sampleSql="select EMPNO from EMP where ENAME = (select
ENAME from EMP where SAL = (select SAL from EMP where HIREDATE = to_date('06/09/1981 00:00:00', 'MM/DD/YYYY HH24:MI:SS')))"
newName="DB2_case 15"
```

update_qr_replace_element_byId

Update an existing replacement specification for a specified query rewrite action.

Parameter	Value	Description
isFromAllRuleElements		Required. The type of database this query rewrite definition is associated with. Must be either ORACLE or DB2.
isFromRegex		True or false. Indicates that the "from" element is specified by using a regular expression. Default is false.
isReplaceToFunction		True or false. Indicates that the "replace to" is the name of a function, such as user-defined function.
qrReplaceElementId		Required (integer). The unique ID of query rewrite action.

Parameter	Value	Description
replaceFrom		The incoming string for a matching rule that is to be replaced. Use replaceType to indicate specifically which element of the incoming query to examine.
replaceTo		The replacement string for the matching element.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

```
grdapi update_qr_replace_element_byId qrReplaceElementId=1 isFromAllRuleElements=false isFromRegex=false isReplaceToFunction=false
replaceFrom=emp replaceTo=NEW_EMP_UPDATED
```

Parent topic: GuardAPI Reference

GuardAPI Role Functions

Use these GuardAPI commands to grant, list and revoke Role Functions.

Note: In a Central Management environment, the object to which you want to add a role may reside on the Central Manager or on a managed unit. See the Overview of the Aggregation & Central Management help book, for more information.

grant_role_to_object_by_id

Add a role to the specified object - a Classification process, for example. Dependencies are checked before adding the role. For example, before adding a role to a Classification process, that role must be assigned to all components contained by that Classification process (the classification policy and any datasources referenced).

Parameter	Value	Description
objectTypeId		Required (integer). Identifies the type of object to which the role will be assigned. It must be one of the following integers: 1=Query 2=Report 3=Alert 4=Baseline 5=Policy 6=SecurityAssessment 7=PrivacySet 8=AuditProcess 12=CustomTable 13=Datasource 14=CustomDomain 15=ClassifierPolicy 16=ClassificationProcess
objectId		Required (integer). Identifies the object to which the role will be assigned.
roleId		Required (integer). Identifies the role to assign. This can be any existing role ID, or the special value -1, which allows access by all roles.

Parameter	Value	Description
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

grdapi grant_role_to_object_by_id objectTypeId=13 objectId=2 roleId=3

grant_role_to_object_by_Name

Add a role to the specified object - a Classification process, for example. Dependencies are checked before adding the role. For example, before adding a role to a Classification process, that role must be assigned to all components contained by that Classification process (the classification policy and any datasources referenced).
Parameters

Parameter	Value	Description
objectType		Required. Identifies the type of object to which the role will be assigned. It must be one of the following: Query Report Alert Baseline Policy SecurityAssessment PrivacySet AuditProcess CustomTable Datasource CustomDomain ClassifierPolicy ClassificationProcess
objectName		Required. The name of the object (the query or report, for example) to which the role will be assigned.
role		Required. The name of the role to assign. This can be any existing role, or **all_roles** to allow access by all roles.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

grdapi grant_role_to_object_by_Name objectType=Datasource objectName= “swanSybase” role=admin

list_roles_granted_to_object_by_id

Displays the roles assigned to the specified object - a Classification process, for example.

Parameter	Value	Description
objectTypeId		Required (integer). Identifies the type of object to which the role will be assigned. It must be one of the following integers: 1=Query 2=Report 3=Alert 4=Baseline 5=Policy 6=SecurityAssessment 7=PrivacySet 8=AuditProcess 12=CustomTable 13=Datasource 14=CustomDomain 15=ClassifierPolicy 16=ClassificationProcess
objectId		Required (integer). Identifies the object to which the role will be assigned.
roleId		Required (integer). Identifies the role to assign. This can be any existing role ID, or the special value -1, which allows access by all roles.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

grdapi list_roles_granted_to_object_by_id objectTypeId=7 objectId=1

list_roles_granted_to_object_by_Name

Displays the roles assigned to the specified object - a Classification process, for example.

Parameter	Value	Description

Parameter	Value	Description
objectType		Required. Identifies the type of object to which the role will be assigned. It must be one of the following: Query Report Alert Baseline Policy SecurityAssessment PrivacySet AuditProcess CustomTable Datasource CustomDomain ClassifierPolicy ClassificationProcess
objectName		Required. The name of the object (the query or report, for example) to which the role will be assigned.
role		Required. The name of the role to assign. This can be any existing role, or **all_roles** to allow access by all roles.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

grdapi list_roles_granted_to_object_by_Name objectType=PrivacySet objectName="privaceSet 1"

revoke_role_from_object_by_id

Removes a role from the specified object - a Classification process, for example. Dependencies are handled automatically. For example, if the role foo is removed from a specific query, the role foo will also be removed from any report based on that query.

Parameter	Value	Description

Parameter	Value	Description
objectTypeId		Required (integer). Identifies the type of object to which the role will be assigned. It must be one of the following integers: 1=Query 2=Report 3=Alert 4=Baseline 5=Policy 6=SecurityAssessment 7=PrivacySet 8=AuditProcess 12=CustomTable 13=Datasource 14=CustomDomain 15=ClassifierPolicy 16=ClassificationProcess
objectId		Required (integer). Identifies the object to which the role will be assigned.
roleId		Required (integer). Identifies the role to assign. This can be any existing role ID, or the special value -1, which allows access by all roles.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

grdapi revoke_role_from_object_by_id objectTypeId=13 objectId=5 role=-1

revoke_role_from_object_by_Name

Removes a role from the specified object - a Classification process, for example. Dependencies are handled automatically. For example, if the role foo is removed from a specific query, the role foo will also be removed from any report that uses that query.

Parameter	Value	Description

Parameter	Value	Description
objectType		Required. Identifies the type of object to which the role will be assigned. It must be one of the following: Query Report Alert Baseline Policy SecurityAssessment PrivacySet AuditProcess CustomTable Datasource CustomDomain ClassifierPolicy ClassificationProcess
objectName		Required. The name of the object (the query or report, for example) to which the role will be assigned.
role		Required. The name of the role to assign. This can be any existing role, or **all_roles** to allow access by all roles.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

grdapi revoke_role_from_object_by_Name objectType=Datasource objectName="swanSybase" role=admin

Parent topic: GuardAPI Reference

GuardAPI S-TAP® functions

Use these CLI commands to create, list, delete, restart, and set S-TAP functions.

create_stap_inspection_engine

Add an inspection engine to the specified S-TAP. S-TAP configurations can be modified only from the active Guardium® host for that S-TAP, and only when the S-TAP is online.

Parameter	Value	Description
stapHost		Required. The host name or IP address of the database server on which the S-TAP is installed.

Parameter	Value	Description
protocol		Required. The database protocol, which must be one of the these values: DB2® DB2 Exit (DB2 version 10) FTP Informix® Kerberos Mysql Netezza® Oracle PostgreSQL Sybase Teradata Teradata Exit (v10.1.3 and up) Windows File Share exclude IE Windows S-TAP hosts can also use the following protocols: MSSQL named pipes
portMin		Required (integer). Starting port number of the range of listening ports that are configured for the database. (Do not use large inclusive ranges, as this degrades the performance of the S-TAP.)
portMax		Required (integer). Ending port number of the range of listening ports for the database.
teeListenPort teeRealPort		Optional (integer). Not used for Windows. Under UNIX, replaced by the KTAP DB Real Port when the K-TAP monitoring mechanism is used. Required when the TEE monitoring mechanism is used. The Listen Port is the port on which the S-TAP listens for and accepts local database traffic. The Real Port is the port onto which S-TAP forwards traffic.
connectToIp		Optional (integer). The IP address for the S-TAP to use to connect to the database. Some databases accept local connection only on the “real” IP address of the machine, and not on the default (127.0.0.1).
client		Required. A list of Client IP addresses and corresponding masks to specify which clients to monitor. If the IP address is the same as the IP address for the database server, and a mask of 255.255.255.255 is used, only local traffic is monitored. A client address/mask value of 1.1.1.1/0.0.0.0 monitors all clients. (See the example.)
encryption		Optional. Activate ASO encrypted traffic where encryption=0 (no) or encryption=1 (yes).
excludeClient		Optional. A list of Client IP addresses and corresponding masks to specify which clients to exclude. This option enables you to configure the S-TAP to monitor all clients, except for a certain client or subnet (or a collection of these options).
procNames		For a Windows Server: For Oracle or MS SQL Server only, when named pipes are used. For Oracle, the list usually has two entries: oracle.exe,tnslsnr.exe. For MS SQL Server, the list is usually just one entry: sqlservr.exe.
namedPipe		Windows only. Specifies the name of a named pipe. If a named pipe is used, but nothing is specified here, the S-TAP retrieves the named pipe name from the registry.
ktapDbPort		Optional (integer). Not used for Windows. Under UNIX, used only when the K-TAP monitoring mechanism is used. Identifies the database port to be monitored by the K-TAP mechanism.
dbInstallDir		UNIX only. Enter the full path name for the database installation directory. For example: /home/oracle10
procName		For a UNIX Server: For a DB2, Oracle, or Informix database, enter the full path name for the database executable. For example: /home/oracle10/prod/10.2.0/db_1/bin/oracle
procNames		Optional
db2SharedMemAdjustment db2SharedMemClientPosition db2SharedMemSize		These three parameters are used for a DB2 inspection engine, only under the following conditions: • The DB2 server is running under Linux. • The K-TAP monitoring mechanism is installed. • Clients connect to DB2 using shared memory. When these parameters are used, grdapi verifies only that the protocol is db2; it does not verify that the conditions have been met. See the DB2 Linux S-TAP Configuration Parameters topic for a detailed explanation of how to use these parameters.

Parameter	Value	Description
instanceName		Optional (string). Used only for MSSQL or Oracle encrypted traffic. Either the MSSQL or ORACLE encryption flag must be turned on before this parameter can be used.
informixVersion		Informix Version.
ieIdentifier		Optional (string).
interceptTypes		Optional (string).
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi create_stap_inspection_engine stapHost=192.168.2.118 protocol=Oracle portMin=1521 portMax=1521 dbInstallDir=/data/oracle10
procName=/data/oracle10/oracle/product/10.2.0/db_1/bin/oracle client=192.168.0.0/255.255.0.0 ktapDbPort=1521
```

Note:

Sometimes, when adding an inspection engine, a false message of Configuration rejected by S-TAP- see S-TAP event log for details, is displayed even though the configuration was not rejected and installed correctly.

Client IP/mask is required for UNIX S-TAP, optional for Windows S-TAP.

list_inspection_engines

Display the properties of all S-TAPs on the specified host, optionally for a specific database type only.

Parameter	Value	Description
stapHost		Required. The host name or IP address of a database server on which S-TAPs are installed (and configured to report to this Guardium appliance).
type		Optional. If used, inspection engines for the specified database type only will be listed. Type must be one of the following: db2 informix mssql mssql-np oracle sybase
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

a1.corp.com> grdapi list_inspection_engines stapHost=192.168.2.33 type=oracle

ID=20162

Stap Host: 192.168.2.33 - Not Active

oracle Inspection Engines:

name =ORACLE2

type =ORACLE

connect to IP=127.0.0.1

install dir = /home/oracle10

exec file = /home/oracle10/product/10.2.0/db_1/bin/oracle-guard

instance name = MSSQLSERVER

encrypted = no

port range = 1521 - 1521

tee listen port = null, tee rel port = 1521

client = 127.0.0.1/255.255.255.255

client = 192.168.0.0/255.255.0.0

name =ORACLE3

type =ORACLE

connect to IP=127.0.0.1

install dir = /home/oracle9

exec file = /home/oracle9/bin/oracle

instance name = MSSQLSERVER

encrypted = no

port range = 1521 - 1521

ok

list_staps

Display the database servers from which S-TAPs report to this Guardium system, optionally listing only the servers that have S-TAPs for which this Guardium system is the active host (that is, the one to which the S-TAP is sending data and the one from which the S-TAP configuration can be modified).

Parameter	Value	Description
onlyActive		Optional (Boolean). Enter **true**, or omit this parameter, to list only those hosts having S-TAPs for which this Guardium system is the active host. Enter **false** to list all hosts on which S-TAPs have been configured to use this Guardium system as either a primary or secondary host.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

a1.corp.com> grdapi list_staps onlyActive=false

ID=0

staps:

stap host = FALCON

stap host = 192.168.2.33

stap host = 192.168.2.173

stap host = 192.168.2.248

stap host = jumbo

ok

delete_stap_inspection_engine

Remove an S-TAP inspection engine. This Guardium system must be the active host for the S-TAP from which the inspection engine will be removed.

Parameter	Value	Description
stapHost		Required. The host name or IP address of the database server on which the S-TAP is installed.
type		Required. Identifies the type of inspection to be removed. Type must be one of the following: Cassandra, CouchDB, DB2, DB2 Exit, FTP, GreenPlumDB, Hadoop, HTTP, iSERIES, Informix, KERBEROS, MongoDB, MS SQL, mssql-np, Mysql, Named Pipes, Netezza, Oracle, PostgreSQL, SAP Hana, Sybase, Teradata, Teradata Exit (v10.1.3 and up), or Windows File Share
sequence		Required (integer). The sequence number of the inspection engine to be removed within the set of inspection engines of the specified type. You can use the grdapi list_inspection_engines command with the type option first, to verify the sequence number of the inspection engine to be removed.
waitForResponse		Optional. Specifies whether the API will wait for a response from the S-TAP. Valid values are 0 (do not wait) and 1 (wait for a response). The default is 1 when stapHost is a single host name or IP address and 0 in all other cases.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi delete_stap_inspection_engine stapHost=192.168.2.118 type=Oracle sequence=1
```

Note: Sometimes, when deleting an inspection engine, a false message of Cannot remove Inspection Engine - the specified inspection engine is not found, is displayed even though the removal was successful.

restart_stap

Restart an S-TAP inspection engine.

Parameter	Value	Description
stapHost		Required. The host name or IP address of the database server on which the S-TAP is installed.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi restart_stap stapHost=192.168.2.118
```

set_stap_debug

Filter log content by database, protocol, client information, instead of dumping all traffic to the log.

function parameters :

stapDebugInterval - required

stapDebugLevel - required

stapDebugOn - required

stapHost - required

api_target_host

store_stap_approval

Use this function to block unauthorized S-TAPs from connecting to the Guardium system.

If ON, then S-TAPs can not connect until they are specifically approved.

If an unapproved S-TAP connects, it is immediately disconnected until the specific authorization of the IP address of that S-TAP.

There is a pre-defined report for approved clients, Approved TAP clients. It is available on the Daily Monitor tab.

Note:

A valid IP address is required, not the host name.

The store_stap_approval command does not work within an environment where there is an IP load balancer.

Within a Central Managed environment, after adding the IP addresses to approved S-TAPs, there is a wait time associated with synchronization that might take up to an hour. After synchronization is complete, the status of the approved S-TAP will appear green in the GUI.

Function: store_stap_approval

function parameters :

isNeeded - Boolean - required

api_target_host - String

Syntax

grdapi store_stap_approval ON | OFF

CLI command

store stap approval and show stap approval

add_approved_stap_client

Use this GuardAPI command to add an approved S-TAP client.

Use of this GuardAPI command does not restart the sniffer and does not affect already connected S-TAPs. This command affects only new S-TAP connections.

Function: add_approved_stap_client

function parameters :

stapHost - String - required

api_target_host - String

Syntax

grdapi add_approved_stap_client <stapHost>

list_approved_stap_client

Use this GuardAPI command to list approved S-TAP clients.

Function: add_approved_stap_client

function parameters :

api_target_host - String

Syntax

grdapi list_approved_stap_client

list_stap_verification_results

Use this GuardAPI command to list S-TAP verification results.

function parameters:

stapHost - String. The host name or IP address of the database server on which the S-TAP is installed.

Syntax

grdapi list_stap_verification_results <stapHost>

delete_approved_stap_client

Use this GuardAPI command to remove an approved S-TAP client.

Use of this GuardAPI command does not restart the sniffer and does not affect other already connected S-TAPs. This command affects only the specified S-TAP connections.

Function: add_approved_stap_client

function parameters :

stapHost - String - required

api_target_host - String

Syntax

grdapi delete_approved_stap_client <stapHost - String - required>

set_ktap_debug

ID=0

function parameters :

ktapDebugInterval - required

ktapFunctionNames

stapHost - required

api_target_host

display_stap_config

Display all the properties of all S-TAPs on the specified host.

Parameter	Value	Description
stapHost		Required. The host name or IP address of a database server on which S-TAPs are installed and configured to report to this Guardium system, or a comma-separated list of host names or IP addresses. You can also use these values: all_active All S-TAPs that are configured to report to this Guardium system all_windows_active All S-TAPs that are configured to report to this Guardium system and are running on Windows machines all_unix_active All S-TAPs that are configured to report to this Guardium system and are running on UNIX machines

Examples:

```
grdapi display_stap_config stapHost=myhost1,myhost2
grdapi display_stap_config stapHost=all_active
```

update_stap_config

Update properties of all S-TAPs on the specified host.

Parameter	Value	Description
stapHost		Required. The host name or IP address of a database server on which Guardium system, or a comma-separated list of host names or IP addresses. You can also use these values: all_active All S-TAPs that are configured to report to this Guardium system all_windows_active All S-TAPs that are configured to report to this Guardium system and are running on Windows machines all_unix_active All S-TAPs that are configured to report to this Guardium system and are running on UNIX machines
updateValue		Required. One or more key-value pairs, in this format: *section.parameter_name:new_value*. *section* indicates the section of the guard_tap.ini file in which the parameter is contained, and can be TAP or DB_x, where DB_x is a designation for an inspection engine that appears as a section header in the file. You can specify new values for multiple parameters by separating the entries with an ampersand (&) .
waitForResponse		Optional. Specifies whether the API will wait for a response from the S-TAP. Valid values are 0 (do not wait) and 1 (wait for a response). The default is 1 when stapHost is a single host name or IP address and 0 in all other cases.

Examples:

```
grdapi update_stap_config stapHost=all_windows_active updateValue=TAP.XXXX
```

verify_stap_inspection_engine_with_sequence

Use this command to verify the S-TAP inspection engine.

Parameter	Value	Description
addToSchedule		String. Constant values list; valid values are Yes and No.
datasourceName		String. If this parameter is specified, advanced verification is performed against the specified datasource. If this parameter is omitted, standard verification is performed.
sequence		Required. Integer. The sequence number of the existing inspection engine for verification. You can use the grdapi list_inspection_engines command with the type option first, to verify the sequence number of the inspection engine to be verified.
stapHost		Required. String. The host name or IP address of the database server on which the S-TAP is installed.
protocol		Required. The database protocol, which must be one of the these values: DB2, DB2 Exit (DB2 version 10), FTP, Informix, Kerberos, Mysql, Netezza, Oracle, PostgreSQL, Sybase, Teradata, Teradata Exit (v10.1.3 and up), exclude IE. Windows S-TAP hosts can also use the following protocols: MSSQL, named pipes.

Example:

```
grdapi verify_stap_inspection_engine_with_sequence stapHost=9.70.144.212
sequence=3
```

revoke_ignore_stap

This command revokes existing IGNORE S-TAP SESSION (REVOKABLE) policy rule actions that ignore S-TAP session traffic. This command only revokes soft ignore rules (marked as REVOKABLE) and cannot revoke hard rules (not marked as REVOKABLE).

Parameter	Value	Description
stapHost		Required. The host name or IP address of a database server on which S-TAPs are installed and configured to report to this Guardium system, or a comma-separated list of host names or IP addresses. You can also use these values: all_active All S-TAPs that are configured to report to this Guardium system all_windows_active All S-TAPs that are configured to report to this Guardium system and are running on Windows machines all_unix_active All S-TAPs that are configured to report to this Guardium system and are running on UNIX machines
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example

```
grdapi revoke_ignore_stap stapHost=myhost1
```

set_ztap_logging_config

This command controls the logging parameters described below.

Syntax: grdapi set_stap_logging_config parameter=[parameter] value=[value].

Parameter	Value	Description

Parameter	Value	Description
log_db2z_target	0 to disable 1 to enable Parameter is disabled by default.	When enabled using `log_db2z_target=1`, targets in db2z protobuf message are logged to GDM_OBJECT in addition to objects from the parser.

Parameter	Value	Description
log_zkey_to_full_sql	0 to disable 1 to enable Parameter is disabled by default.	When enabled using `log_zkey_to_full_sql=1`, VSAM or IMS Key values will be logged in the full SQL statement for policies using "Log full details."

Example

```
grdapi set_ztap_logging_config parameter=log_db2z_target value=1
```

Show values: grdapi get_ztap_logging_config.

Parent topic: GuardAPI Reference

GuardAPI Threat Detection Analytics Functions

enable_advanced_threat_scanning

Enables the scanner processes to check for specific database attacks such as SQL injection and malicious stored procedures.

Parameter	Value	Description
all		Optional. In a central management configuration only, enables all threat detection scanners on all managed units. Allowable values: `true`, `false`.
schedule_start		Optional. Specifies the date and time to start running the processes. The accepted format is yyyy-mm-dd hh:mm:ss (24-hour clock).

Parameter	Value	Description
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

```
grdapi enable_advanced_threat_scanning all=true schedule_start="2016-03-24 12:00:05”
```

You will see the following message if threat analytics is enabled when outlier detection is not:

```
Warning - Enabling advance threat scanning (AKA Eagle Eye) when Analytic anomaly detection is disabled.
Advance threat scanning (AKA Eagle Eye) enabled.
ok
```

disable_advanced_threat_scanning

Disables threat detection scanners on the collector.

Parameter	Value	Description
all		In a central management configuration only, disables all threat detection scanners on all managed units.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

get_eagle_eye_info

Displays the current settings for threat detection parameters.

Parameter	Value	Description
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

```
grdapi get_eagle_eye_info
Eagle Eye Parameters Values:
EI_CASES_DISPLAY_LIMIT = 3
EI_CONFIDENCE_PCT_CHANGE_TO_REDISPLAY_CASE = 30
EI_EAGLE_EYE_ENABLED = 1
EI_PROCESSOR_TIMEOUT_SEC = 420
EI_SCANNER_PATCH_DEF = 10
EI_SCANNER_TIMEOUT_SEC = 300ok
```

set_eagle_eye_parameter

Use under the direction of IBM personnel. Changes configuration parameters for threat detection. These parameters must be set explicitly using `parameter_name` and `parameter_value` as follows:

```
set_eagle_eye_scanner_parameter parameter_name=[parameter] parameter_value=[value]
```

Parameter	Value	Description
EI_CASES_DISPLAY LIMIT		The number of cases to be displayed in the to-do list report. Default is 3.
EI_CONFIDENCE_PCT_CHANGE_TO_REDISPLAY CASE		The percent of “confidence” change that will cause this case to be redisplayed in the to-do list report, even if it has already appeared before. This can happen if Guardium detects another symptom or symptoms that raise the confidence by this percentage value. Default is 30.
EI_PROCESSOR_TIMEOUT_SEC		Processors that run longer time than this threshold are turned off. Default is 420 seconds.
EI_SCANNER_PATCH_DEF		To avoid false positives as a result of patch installation, if in a single process run the number of stored procedures created exceeds this parameter then the process assumes a patch is installed and it stops analyzing symptoms. Default is 10 stored procedure creations detected in one run.
EI_SCANNER_TIMEOUT_SEC		Scanners that run longer time than this threshold are turned off. Default is 300 seconds.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

get_eagle_eye_scanners_info

Return scanner settings information.

Parameter	Value	Description
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

The data returned will contain the following information:

Field	Description
ID	The scanner ID.
Name	The scanner name.
Status	The status of the scanner from the last run: I: in progress D: done K: killed E: done with errors
Enabled	Indicates if the scanner is enabled. True: enabled False: disabled

Field	Description
Permanent disabled	If the scanner was disabled 3 times in 24 hours, then it is permanently disabled. True: disabled False: enabled

Example:

```
grdapi get_eagle_eye_scanners_info
ID=0
ID:1, Name:SQLInjectionExceptionsScanner, Status:D, Enabled:true, Permanent disabled:false
ID:2, Name:NumNewConstructScanner, Status:D, Enabled:true, Permanent disabled:false
ID:3, Name:SQLInjectionSuspiciousObjectScanner, Status:D, Enabled:true, Permanent disabled:false
ID:4, Name:SqliQueryScanner, Status:Unknown, Enabled:false, Permanent disabled:true
ID:5, Name:EagleEyeSTPCreateProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:6, Name:EagleEyeSTPCallProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:7, Name:EagleEyeSTPExceptionProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:8, Name:EagleEyePreviousStpUsageProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:9, Name:EagleEyeSTPViolationProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:10, Name:EagleEyeSTPUserOutlierScanner, Status:D, Enabled:true, Permanent disabled:false
ok
```

set_eagle_eye_scanner_parameter

Use under the direction of IBM personnel. Activate or deactivate a scanner. These parameters must be set explicitly using `parameter_name` and `parameter_value` as follows:

```
set_eagle_eye_scanner_parameter parameter_name=[parameter] parameter_value=[value]
```

Parameter	Value	Description
scanner_id		Required. The unique ID of the scanner, which you can get from get_eagle_eye_scanners_info GuardAPI command.
is_active		Defines if the scanner should run. Used to start a scanner that was stopped automatically because it timed out. 0 : the scanner is stopped 1: the scanner is activated
is_permanent_inactive		If the scanner was permanently disabled after it was disabled 3 times in 24 hours then it can only be enabled again using this GuardAPI. 1: the scanner is stopped permanently 0: the scanner is enabled
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

The following example reactivates a permanently deactivated scanner.

```
set_eagle_eye_scanner_parameter scanner_id=2 parameter_name=is_permanent_inactive parameter_value=0
```

get_eagle_eye_symptom_period_hours

Show the value of the symptom period parameter in hours. The symptom period determines how long back the process is looking and analyzing the collected symptoms for one case.

Parameter	Value	Description
case_name		Required. The case type. The following values are allowed: STP: malicious stored procedure case SQL_INJECTION: SQL Injection case

Parameter	Value	Description
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

```
grdapi get_eagle_eye_symptom_period_hours case_name=STP
The symptoms period for case type: STP is: 168 in hours
ok
```

set_eagle_eye_symptom_period_hours

Set a value for the symptom period parameter in hours. The symptom period determine how long back the process is looking and analyzing the collected symptoms for a case.

Parameter	Value	Description
case_name		Required. The case type. The following values are allowed: STP: malicious stored procedure case SQL_INJECTION: SQL Injection case
symptom_period_hours		Required. Integer. The number of hours in the past to analyze symptoms for a case.
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

```
grdapi set_eagle_eye_symptom_period_hours case_name=STP symptom_period_hours=170
The symptoms period for case type: STP was changed. The old value was: 168. The new value is: 170
ok
```

get_eagle_eye_debug_level

For use by IBM Service personnel. Displays current debug level:

- 1: on
- 0: off

Parameter	Value	Description

Parameter	Value	Description
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

```
grdapi get_eagle_eye_debug_level
ID=0
component=EAGLE_EYE level=1
ok
```

set_eagle_eye_debug_level

For use by IBM Service personnel. Displays current debug level.

Parameter	Value	Description
level		Integer. Required. Allowable values: 1: on 0: off
api_target_host		Optional parameter that specifies the target host(s) to execute the API. When not specified, it defaults to the unit on which command is executed. Valid values: • all_managed: for all managed units • all: all managed units and CM • group:<group name>: where group name is a group of managed units • from CM only, the host name or IP of any managed unit, for example, `api_target_host=10.0.1.123` • from managed unit, the host name or IP of the CM Guardium V10.1 and 10.1.2: In a central management configuration only, specifies a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM.

Example:

```
grdapi set_eagle_eye_debug_level level=0
ID=0
ok
```

Parent topic: GuardAPI Reference

S-TAP for z/OS V10.1.3 User's Guide

- **IBM Security Guardium S-TAP for Db2 on z/OS**
  These topics describe how to use IBM® Security Guardium® S-TAP® for DB2® on z/OS® V10.1.3 (also referred to as IBM Guardium S-TAP for Db2). The V10.1.3 S-TAP is optimized for the V10.1 Guardium system. IBM Guardium S-TAP for Db2 collects and correlates data access information from a variety of Db2 resources to produce a comprehensive view of business activity for auditors.
- **IBM Security Guardium S-TAP for IMS on z/OS**
  These topics describe how to use IBM Security Guardium S-TAP for IMS on z/OS V10.1.3 (also referred to as IBM Guardium S-TAP for IMS). The V10.1.3 S-TAP is optimized for the V10.1 Guardium system. IBM Guardium S-TAP for IMS collects and correlates data access information from a variety of IMS resources to produce a comprehensive view of business activity for auditors.
- **IBM Security Guardium S-TAP for Data Sets on z/OS**
  These topics describe how to use IBM Security Guardium S-TAP for Data Sets on z/OS V10.1.3 (also referred to as IBM Guardium S-TAP for Data Sets). The V10.1.3 S-TAP is optimized for the V10.1 Guardium system. IBM Guardium S-TAP for Data Sets collects and correlates data access information from a variety of resources to produce a comprehensive view of business activity for auditors.

IBM Security Guardium S-TAP for Db2 on z/OS

These topics describe how to use IBM Security Guardium S-TAP for Db2 on z/OS V10.1.3 (also referred to as IBM Guardium S-TAP for Db2). The V10.1.3 S-TAP is optimized for the V10.1 Guardium system. IBM Guardium S-TAP for Db2 collects and correlates data access information from a variety of Db2 resources to produce a comprehensive view of business activity for auditors.

About these topics

This information is designed to help database administrators, system programmers, and application programmers perform these tasks:

- Plan for the installation of IBM Guardium S-TAP for Db2
- Install and operate IBM Guardium S-TAP for Db2
- Configure the IBM Guardium S-TAP for Db2 environment
- Diagnose and recover from IBM Guardium S-TAP for Db2 problems

A PDF of this User's Guide is also available here.

- **IBM Security Guardium S-TAP for Db2 on z/OS overview**
  IBM Security Guardium S-TAP for Db2 on z/OS (also referred to as IBM Guardium S-TAP for Db2) collects and correlates data access information from Db2 to produce a comprehensive view of business activity for auditors. IBM Guardium S-TAP for Db2 enables you to determine which users updated or read a particular table, on a specific z/OS Db2 system, within a specific time period.
- **Configuring IBM Security Guardium S-TAP for Db2 on z/OS**
  After you install IBM Guardium S-TAP for Db2, you must customize some files for your system. All configuration steps are required in both stand-alone and data sharing environments.
- **Data collection**
  IBM Guardium S-TAP for Db2 collects data from an audited Db2 subsystem, in accordance with the collection policies that you create through the IBM Guardium system. Use a collection policy to specify filtering criteria that captures relevant data and filters out irrelevant data. The filtering criteria that you specify determines which data is streamed to your IBM Guardium system.
- **Reference information**
  These reference topics are designed to provide you with quick access to information about IBM Guardium S-TAP for Db2 sample library members, parameters, and variables.
- **Messages and codes for IBM Security Guardium S-TAP for DB2 on z/OS**

Parent topic: S-TAP for z/OS V10.1.3 User's Guide

IBM Security Guardium S-TAP for Db2 on z/OS overview

IBM Security Guardium S-TAP for Db2 on z/OS (also referred to as IBM Guardium S-TAP for Db2) collects and correlates data access information from Db2 to produce a comprehensive view of business activity for auditors. IBM Guardium S-TAP for Db2 enables you to determine which users updated or read a particular table, on a specific z/OS Db2 system, within a specific time period.

Use IBM Guardium S-TAP for Db2 to collect and correlate the following types of data to the Guardium system:

- Modifications to an object (SQL UPDATE, INSERT, DELETE)
- Reads of an object (SQL SELECT)
- Explicit GRANT and REVOKE operations to capture events where users might be attempting to modify authorization levels
- Assignment or modification of an authorization ID
- Authorization attempts that are denied because of inadequate authorization
- CREATE, ALTER, and DROP operations against an object (such as a table)
- Utility access to an object (IBM utilities only)
- Db2 commands entered, including which users are issuing specific commands

IBM Guardium S-TAP for Db2 uses Db2 data sharing to obtain audit information from all members of the data sharing group.

- **What's new in IBM Security Guardium S-TAP for Db2 on z/OS V10.1.3?**
  Version 10.1.3 of IBM Guardium S-TAP for Db2 provides speed and monitoring enhancements.
- **The IBM Security Guardium S-TAP for Db2 on z/OS installation environment**
  The IBM Guardium S-TAP for Db2 SQL Collector Agent collects data from an audited Db2 subsystem in accordance with the filtering policies you set with the Guardium system.
- **Installation and operation requirements**
  Verify that you have the hardware and software that is required to install and operate IBM Guardium S-TAP for Db2.

Parent topic: IBM Security Guardium S-TAP for Db2 on z/OS

What's new in IBM Security Guardium S-TAP for Db2 on z/OS V10.1.3?

Version 10.1.3 of IBM Guardium S-TAP for Db2 provides speed and monitoring enhancements.

Enhancements to this version of the product include:

- New Simulation mode enables you to test policies without sending data to the appliance. Data is collected on z/OS.
- Support for the collection of BIND/REBIND events
- Support for the collection of CICS Unit of Work ID
- Improved memory management
- Support for blocking policies pushed-down from the appliance
- Improved filtering of events
- MODIFY command now collects more diagnostic information
- Ability to exclude host variables
- Support for initiating an appliance MUST GATHER command from z/OS
- Support for S-TAP logging
- Support for Internet Protocol version 6 (IPV6) introduced with PH16991

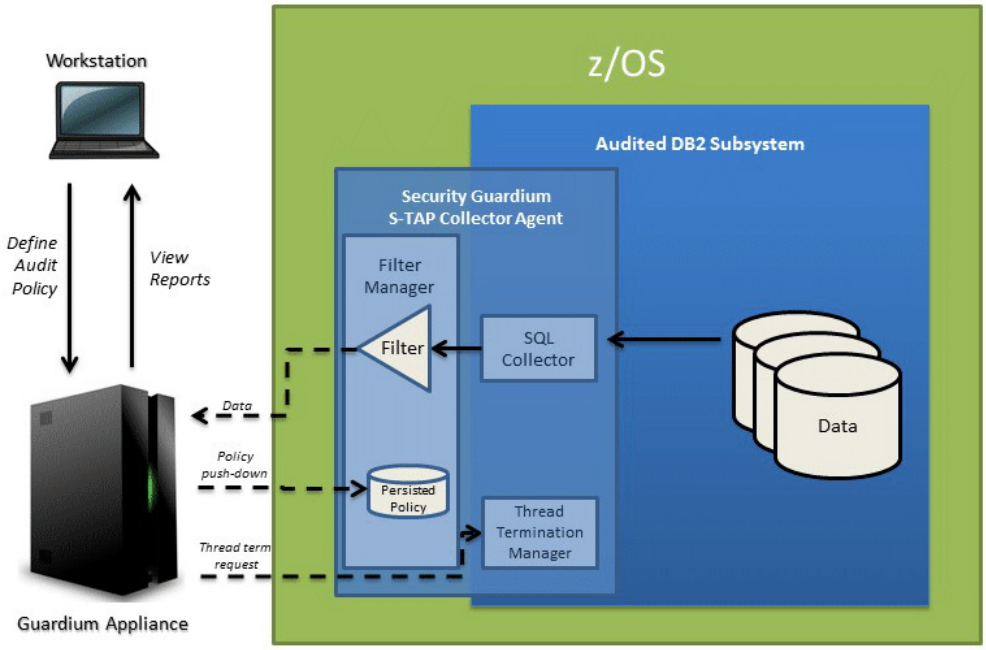
Parent topic: IBM Security Guardium S-TAP for Db2 on z/OS overview

The IBM Security Guardium S-TAP for Db2 on z/OS installation environment

The IBM Guardium S-TAP for Db2 SQL Collector Agent collects data from an audited Db2 subsystem in accordance with the filtering policies you set with the Guardium system.

The IBM Guardium S-TAP for Db2 collector agent runs as a started task and is responsible for the collection of audit data in an IBM Guardium S-TAP for Db2 environment. As shown in the following diagram, SQL collector data is filtered and sent to the Guardium system, enabling you to view reports on your workstation.

Figure 1. An overview of the IBM Guardium S-TAP for Db2 environment



Guardium Appliance System

The Guardium system can gather, and report on, information from multiple agents running on multiple z/OS systems. The Guardium system:

- Provides the user interface, which processes requests and displays the resulting information.
- Enables you to create filtering policies, which specify the types of data to be collected by the agent.
- Stores the collected data.

Guardium Appliance System and S-TAP Collector Agent communication

The Guardium system and the IBM Guardium S-TAP for Db2 agent communicate by using a TCP/IP connection. The filtering policies that you create instruct the agent about the data to collect, such as which jobs and data sets to monitor for data accesses.

The IBM Guardium S-TAP for Db2 agent is responsible for:

- Collecting Db2 audit data based on the policy settings.
- Enabling activities to be blocked.
- Streaming collected event activity to the Guardium system.

For more information about how Guardium system policies are interpreted and enabled by the S-TAP, see Policy pushdown.

With the Guardium system installed, configured, and running in your environment, you can test your connection from the z/OS platform to the Guardium system by configuring and running the IBM Guardium S-TAP for Db2 sample library member, ADHTCPD. Consult your network security team to review the results and confirm that connection from the z/OS platform to the Guardium system is available.

Parent topic: IBM Security Guardium S-TAP for Db2 on z/OS overview

Installation and operation requirements

Verify that you have the hardware and software that is required to install and operate IBM Guardium S-TAP for Db2.

FEC common code FMID H25F132 is required, and must be present on the system for the successful installation of this product.

IBM Db2 Data Access Common Collector for z/OS V1.1 (CQC) common code FMID HCQC110 is required, and must be present on the system for the successful installation of this product.

Hardware requirements

Any hardware that is capable of running Db2 for z/OS (V11 or later, until end of service).

Collector agent requirements

- Db2 Version 11 or later, until end of service.
- z/OS Version 2 Release 2 or later, until end of service.
- The IBM Guardium S-TAP for Db2 collector agent must be run on an operating system version that is equivalent to the operating system version on which the product SMP/E installation is performed.
- Resource Recovery Services (RRS) must be configured and enabled for IBM Guardium S-TAP for Db2 to use the RRSAF attachment facility to connect to Db2.

- **Compatibility with IBM Db2 Query Monitor for z/OS**
  IBM Guardium S-TAP for Db2 does not require Db2 Query Monitor to be installed or activated on a Db2 subsystem that IBM Guardium S-TAP for Db2 audits. If you are running Db2 Query Monitor on your system, be aware that IBM Guardium S-TAP for Db2 can audit a Db2 subsystem that is running Db2 Query Monitor Version 3.2 or later. Certain IBM Guardium S-TAP for Db2 PTFs require Db2 Query Monitor PTFs through SMP/E IFREQ.
- **Required user ID authorizations**
  To operate IBM Guardium S-TAP for Db2, the S-TAP collector agent started task must run under the authority of a Time Sharing Option (TSO) user ID with these authorizations.

Parent topic: IBM Security Guardium S-TAP for Db2 on z/OS overview

Compatibility with IBM Db2 Query Monitor for z/OS

IBM Guardium S-TAP for Db2 does not require Db2 Query Monitor to be installed or activated on a Db2 subsystem that IBM Guardium S-TAP for Db2 audits. If you are running Db2 Query Monitor on your system, be aware that IBM Guardium S-TAP for Db2 can audit a Db2 subsystem that is running Db2 Query Monitor Version 3.2 or later. Certain IBM Guardium S-TAP for Db2 PTFs require Db2 Query Monitor PTFs through SMP/E IFREQ.

To implement Db2 Query Monitor, your site must have the appropriate operating system, environment, hardware, software, and network requirements. For information about installing and operating Db2 Query Monitor, refer to the IBM Db2 Query Monitor for z/OS Knowledge Center.

Compatible releases and maintenance levels

The following product abbreviations are used:

- InfoSphere® Guardium S-TAP for Db2: STP
- IBM Security Guardium S-TAP for Db2 on z/OS: STP
- Db2 Query Monitor: CQM

Table 1. Compatible releases and maintenance levels

	CQM 3.2	**CQM 3.3**	**STP 9.1**	**STP 10.0**	**STP V10.1.3**
CQM 3.2	---	LPAR	Db2	Db2	Db2
CQM 3.3	LPAR	---	Db2	Db2	Db2
STP 9.1	Db2	Db2	---	LPAR	LPAR
STP 10.0	Db2	Db2	LPAR	---	LPAR
STP 10.1.3	Db2	Db2	LPAR	LPAR	---

Where:

LPAR
: The two products releases can coexist on the same LPAR (provided they use a different MASTER name), but cannot be active on the same Db2 subsystem.

Db2
: The two products releases can coexist on the same LPAR and can both be active on the same Db2 subsystem/shared collector.

Parent topic: Installation and operation requirements

Required user ID authorizations

To operate IBM Guardium S-TAP for Db2, the S-TAP collector agent started task must run under the authority of a Time Sharing Option (TSO) user ID with these authorizations.

The collector agent user ID requires Db2 privileges. Grant the collector agent user ID SYSCTRL authority, and the authority to issue the SELECT statements on these tables:

- SYSIBM.SYSTABLES
- SYSIBM.SYSTABLESPACE
- SYSIBM.SYSINDEXES

OMVS segment

The collector agent uses UNIX System Services (USS) callable services as the network interface to the appliance. The USS callable services require that an OMVS segment is defined in the RACF® profile for the user ID under which the collector agent job runs. The OMVS segment that is defined for the user ID must contain the following minimum requirements:

- A numeric user ID that is assigned to the user
- A valid path to an existing home directory
- A program name, for example: /bin/sh or /bin/echo for non-shell
- A numeric group ID that is assigned to the user's DEFAULT group

To verify that the ID has an OMVS segment in its RACF profile, use the following command:

```
LU user ID OMVS
```

To add an OMVS segment to the RACF profile of an ID, refer to this sample command:

```
ALTUSER user ID
OMVS(UID(nnn)HOME('/u/ user ID)
PROGRAM('/bin/sh')
```

Parent topic: Installation and operation requirements

Configuring IBM Security Guardium S-TAP for Db2 on z/OS

After you install IBM Guardium S-TAP for Db2, you must customize some files for your system. All configuration steps are required in both stand-alone and data sharing environments.

Before you begin

Review the collector agent security and system requirements before proceeding with the following steps. A list of sample library members is provided in this User's Guide.

About this task

The following table describes the configuration steps and the corresponding SADHSAMP sample library member that is required for customization.

Table 1. Configuration steps

Step	Description of configuration step	SADHSAMP sample library member to use
1	APF authorizing the LOAD library data set	(Not applicable)
2	Customizing JCL members using the ADHEMAC1 macro	ADHEMAC1
3	Binding DBRMs using the JCL bind job	ADHBIND
4	Granting required authorizations to USERID and ADHPLAN by using the JCL authorization member	ADHGRANT
5	Creating the IBM Guardium S-TAP for Db2 control file	ADHSJ000
6	Configuring the IBM Guardium S-TAP for Db2 control file	ADHSJ001
7	Configuring the collector agent	ADHCFGP and ADHCSSID
8	Authorizing ADHPLCY for policy pushdown	Define ADHPLCY to RACF or an equivalent security system

- **Upgrading from IBM Guardium S-TAP for Db2 V9.0, V9.1, or V10.0**
  You can upgrade to IBM Guardium S-TAP for Db2 V10.1.3 from IBM Guardium S-TAP for Db2 V9.0, V9.1, or V10.0 by completing these steps.
- **Configuring IBM Security Guardium S-TAP for Db2 on z/OS**
  After installation, configure IBM Guardium S-TAP for Db2 by completing the steps that are described in this section.

Parent topic: IBM Security Guardium S-TAP for Db2 on z/OS

Upgrading from IBM Guardium S-TAP for Db2 V9.0, V9.1, or V10.0

You can upgrade to IBM Guardium S-TAP for Db2 V10.1.3 from IBM Guardium S-TAP for Db2 V9.0, V9.1, or V10.0 by completing these steps.

Procedure

1. Complete the SMP/E installation of IBM Guardium S-TAP for Db2 V10.1.3.
2. APF-authorize the V10.1.3 SADHLOAD data set.
3. Customize and run the Db2 bind job in SADHSAMP(ADHBIND).
4. Customize and run the Db2 grant job in SADHSAMP(ADHGRANT).
5. Export and save your collection profiles.
   (V8.1 collection profiles, or policies, were administered either with the InfoSphere® Guardium S-TAP for Db2 administration client, or the IBM Guardium system.)
6. Stop the previous version's collector agent and server address spaces.
7. Update the collector started task JCLs (ADHC*ssid*) to:
   - Remove the previous version of the product SADHLOAD data sets.
   - Include the new V10.1.3 product SADHLOAD data sets in the STEPLIB DD concatenation members.

   Note: ADHS*ssid* and ADHA*ssid* started tasks are not used in IBM Guardium S-TAP for Db2 V10.1.3.
8. Update the V10.1.3 collector configuration member (typically SADHSAMP(ADHCFGP).
9. Install a collection policy on the IBM Guardium system.
   - If policy pushdown was used for V8.1 collection administration, follow the Guardium Policy Builder instructions for migrating policies for V8.1 to V10.1.3.
   - If the InfoSphere Guardium S-TAP for Db2 administration client was used for V8.1 collection administration, use the XML exported in Step 4 as a reference for the Guardium Policy Builder to define collection policies for V10.1.3.
10. Start the collector address space by typing `/S ADHC`*ssid* at the z/OS® command prompt.

What to do next

Now you can install policies on the z/OS host by using the IBM Guardium system interface. No additional configuration steps are required.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Configuring IBM Security Guardium S-TAP for Db2 on z/OS®

After installation, configure IBM Guardium S-TAP for Db2 by completing the steps that are described in this section.

- **APF authorizing the LOAD library data set**
  The system programmer must APF authorize the product LOAD library for data collection to work correctly. The system programmer must modify the IEAAPFxx or PROGxx PARMLIB members to define the IBM Guardium S-TAP for Db2 data set, as specified by ADHEMAC1 macro value #SADHLOAD, as an APF authorized library.
- **Enabling the dynamic LPA facility service CSVDYLPA**
  The user ID that was used to start the Collector Agent PROC must be enabled to use the dynamic LPA facility CSVDYLPA to enable the collector agent to collect data.
- **Service class considerations**
  The collector agent started task must be set at a dispatching priority that is the same as, or higher than, that of Db2.
- **Customizing JCL members**
  Use the edit macro ADHEMAC1 to customize the variables in the JCL to be run. Running ADHEMAC1 allows you to modify members without requiring you to remember plan names, creators, and other variables from one editing session to the next editing session.
- **Creating the IBM Guardium S-TAP for Db2 control file**
  IBM Guardium S-TAP for Db2 configuration information is stored in a VSAM data set, which is the product control file.
- **Configuring the IBM Guardium S-TAP for Db2 control file**
  IBM Guardium S-TAP for Db2 requires information that identifies target Db2 subsystems, product options, and data set attributes. The product configuration is saved in the VSAM product control file data set that you created previously.
- **Configuring the collector agent**
  To configure the collector agent, complete the steps provided in each of the subsequent sections. The address space dispatching priority for IBM Guardium S-TAP for Db2 must be the same as, or higher than, that of Db2.
- **Configuring the collector agent for additional Db2 subsystems**
  The collector agent must be configured for each Db2 subsystem that is to be audited.
- **Support Services Address Space overview**
  IBM Guardium S-TAP for Db2 uses a Support Services Address Space, also referred to as a Master Address Space. Learn about how the Master Address Space works, as well as the implications for using and stopping it.
- **Enabling CICS Login User ID reporting**
  You can capture the CICS® Login User ID for SQL Statements that are run in Db2 for CICS. The capture of CICS transactions is limited to CICS versions TS 4.2 or later, until end of support.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

APF authorizing the LOAD library data set

The system programmer must APF authorize the product LOAD library for data collection to work correctly. The system programmer must modify the IEAAPFxx or PROGxx PARMLIB members to define the IBM Guardium S-TAP for Db2 data set, as specified by ADHEMAC1 macro value #SADHLOAD, as an APF authorized library.

About this task

The IBM Guardium S-TAP for Db2 agent requires that all data sets accessed in the STEPLIB of the collector job be APF authorized, including:

- the LOAD library data set
- adhhlq.SADHLOAD
- the FEC data set fechlq.SFECLOAD (where *adhhlq* and *fechlq* are the data set high level qualifier where S-TAP and FEC products are installed)
- the CQC data set cqchlq.SCQCLOAD (where adhhlq and cqchlq are the data set high level qualifier where S-TAP and CQC products are installed)

Other data sets that require APF authorization are:

- CEE.SCEERUN
- CEE.SCEERUN2
- Db2 EXIT data set (i.e. DSN.VAR1.SDNEXIT)
- Db2 LOAD library data set (i.e. DSN.VAR1.SDSNLOAD)
- SYS1.LINKLIB

Refer to the *z/OS® Knowledge Center* for more information about how to APF authorize libraries.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Enabling the dynamic LPA facility service CSVDYLPA

The user ID that was used to start the Collector Agent PROC must be enabled to use the dynamic LPA facility CSVDYLPA to enable the collector agent to collect data.

About this task

Determine whether the dynamic LPA facility CSVDYLPA is SAF protected. If the dynamic LPA facility CSVDYLPA is not SAF protected, this step is not required.

Procedure

Provide the user ID with ADD/UPDATE/DELETE authority.
For more information about how to enable the CSVDYLPA resource, see section 5.6.3 of the *z/OS® V1R7.0 MVS™ Planning: Operations Guide* (SA22-7601-06), section *Controlling/Adding A Module to LPA after IPL*.
Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Service class considerations

The collector agent started task must be set at a dispatching priority that is the same as, or higher than, that of Db2.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Related tasks

- Configuring the collector agent

Customizing JCL members

Use the edit macro ADHEMAC1 to customize the variables in the JCL to be run. Running ADHEMAC1 allows you to modify members without requiring you to remember plan names, creators, and other variables from one editing session to the next editing session.

Procedure

1. Copy member ADHEMAC1 from the adhhilvl.SADHSAMP to your site's CLIST library, and then edit the ADHEMAC1 macro with the appropriate variables.
2. After you copy the edit macro to your CLIST library, use it to edit each sample library member individually. You might need to update the macro between edits depending on the member being edited and the context of the variable to be modified in the sample library.
3. To run the macro, type the ADHEMAC1 command to automatically update the appropriate variables in the member that you are editing.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Related reference

- ADHEMAC1 edit macro variables

Creating the IBM Guardium S-TAP for Db2 control file

IBM Guardium S-TAP for Db2 configuration information is stored in a VSAM data set, which is the product control file.

About this task

Using the sample JCL that is included with the product, complete these steps to create the IBM Guardium S-TAP for Db2 control file:

Procedure

1. Edit SADHSAMP member ADHSJ000.
2. Add the appropriate job card to ADHSJ000.
3. In the DELETE instruction, change the data set name.
4. In the DEFINE CLUSTER instruction, change the following text within parentheses:
   - Data set NAME
   - VOLUMES
   - DATA NAME
   - INDEX NAME
5. In the REPRO instruction, change the name of the OUTDATASET.
6. Run ADHSJ000 to create the control file. The job steps must end with a return code of zero.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Configuring the IBM Guardium S-TAP for Db2 control file

IBM Guardium S-TAP for Db2 requires information that identifies target Db2 subsystems, product options, and data set attributes. The product configuration is saved in the VSAM product control file data set that you created previously.

About this task

Update the product control file by using the sample JCL that is included with IBM Guardium S-TAP for Db2. Sample library member ADHSJ001 contains the JCL to update the control file. The following steps list the tasks required to configure the product control file data set.
Important: The Db2 plan names that are specified in the product configuration options must match the product plan names assigned to the product's Db2 plans bind plan job.

Procedure

1. Edit SADHSAMP member ADHSJ001.
2. Add the appropriate job card to ADHSJ001.
3. Change ADH.V0A00.CONTROL to the name of the VSAM control data set that you created using member ADHSJ000.
4. Change #SADHLOAD to the name of the product LOADLIB used for IBM Guardium S-TAP for Db2.
5. Modify the SYSIN DD statements as instructed in the sample member. For more information, see Required statements for each subsystem.
   Important: In a data-sharing environment, specify subsystem names (not group names) in ADHSJ001.
6. Run ADHSJ001.
   Ensure that the update job steps of the product control file end with a return code of zero. If a non-zero return code occurs, review the job output for errors, correct the problem, and resubmit the JCL.

- **Required statements for each subsystem**
  The following statements are required for each Db2 subsystem that is added to the control file.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Required statements for each subsystem

The following statements are required for each Db2 subsystem that is added to the control file.

Table 1. Required statements for each subsystem

Statement	Setting
SET DB2 SSID	#SSID
UPDATE DB2 ZPARMS	#SZPARM
UPDATE DB2 BOOTSTRAP 1	#SBSDS01
UPDATE DB2 LOADLIB 1	#SDSNEXIT
UPDATE DB2 LOADLIB 2	#SDSNLOAD
SET PRODUCT CFG	NULL
SET PRODUCT VER	NULL
UPDATE ADH PLAN 1	ADHPLAN1
UPDATE ADH CORR ID 1	ADH ID 1
UPDATE ADH CORR ID 2	ADH ID 2

Parent topic: Configuring the IBM Guardium S-TAP for Db2 control file

Configuring the collector agent

To configure the collector agent, complete the steps provided in each of the subsequent sections. The address space dispatching priority for IBM Guardium S-TAP for Db2 must be the same as, or higher than, that of Db2.

1. Configuring the JCL for ADHBIND
   SADHSAMP(ADHBIND) is a job that binds the packages and plan used by the collector agent.
2. Configuring the JCL for ADHGRANT
   SADHSAMP(ADHGRANT) is a job that grants authorizations to the user ID and plan that are used by the collector agent.
3. Configuring the ADHCFGP data set
   The ADH#MAIN program uses parameters to define the IBM Guardium S-TAP for Db2 subsystem name, the monitored Db2 subsystem, the Guardium system host name or network address TCP/IP port, and other parameters that control how the IBM Guardium S-TAP for Db2 collector agent is implemented.
4. Defining the collector agent started task JCL
   The collector agent runs as a started task. The sample library member ADHC*SSID* contains the sample JCL to set up the IBM Guardium S-TAP for Db2 collector agent started task.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Related reference

- Service class considerations

Configuring the JCL for ADHBIND

SADHSAMP(ADHBIND) is a job that binds the packages and plan used by the collector agent.

Procedure

1. Customize and submit the JCL according to the instructions in the member.
2. Submit the ADHBIND JCL to bind the collector agent packages and plan on each Db2 subsystem on which you want to use IBM Guardium S-TAP for Db2.

Parent topic: Configuring the collector agent
Next topic: Configuring the JCL for ADHGRANT

Configuring the JCL for ADHGRANT

SADHSAMP(ADHGRANT) is a job that grants authorizations to the user ID and plan that are used by the collector agent.

Procedure

1. Customize and submit the JCL according to the instructions in the member.
2. Submit the ADHGRANT JCL to grant authorizations to the user ID and plan that are used by the collector agent for each Db2 subsystem on which you want to use IBM Guardium S-TAP for Db2.
   Note: The ADHGRANT job contains examples of the GRANTs that meet the minimal authorization requirements for the collector agent. Alternative authorizations and, subsequently, GRANTs, can be used to meet the minimal authorization requirements for the collector agent.

Parent topic: Configuring the collector agent
Previous topic: Configuring the JCL for ADHBIND
Next topic: Configuring the ADHCFGP data set

Configuring the ADHCFGP data set

The ADH#MAIN program uses parameters to define the IBM® Guardium® S-TAP® for DB2® subsystem name, the monitored Db2 subsystem, the Guardium system host name or network address TCP/IP port, and other parameters that control how the IBM Guardium S-TAP for Db2 collector agent is implemented.

About this task

These parameters are defined in an 80-byte sequential or partitioned data set that you must allocate to the ADHPARMS DD. A sample is available in the SADHSAMP library member ADHCFGP.

Note: The AUDIT parameter is required. It instructs the collector agent to audit a specific Db2 subsystem. It supports only one Db2 subsystem.

To use the sample ADHCFGP member:

Procedure

1. Copy ADHCFGP to the appropriate location (PARMLIB) on your system.
2. Verify that the parameters are valid for your environment. If necessary, edit the parameter file for your IBM Guardium S-TAP for Db2 objects.
3. Edit the ADHPARMS DD in the started task JCL to point to the ADHCFGP data set that you have customized.

Example

An example of the ADHCFGP member contents is as follows:

```
BROWSE   ADH.SMPE.SAMPLIB(ADHCFGP) - 01 L
Command ===>
SUBSYS(#SSID)
AUDIT(#SSID)
MASTER_PROCNAME(ADHMST31)
APPLIANCE_SERVER(#APPSRVR)
```

Parent topic: Configuring the collector agent
Previous topic: Configuring the JCL for ADHGRANT
Next topic: Defining the collector agent started task JCL

Defining the collector agent started task JCL

The collector agent runs as a started task. The sample library member ADHC*SSID* contains the sample JCL to set up the IBM Guardium S-TAP for Db2 collector agent started task.

Before you begin

To run the collector agent as a started task, the JCL must be in a cataloged procedure library. Modify the sample started task JCL in SADHSAMP library member ADHC*SSID* for your site, according to the instructions in the member.

About this task

The started task requires:

- READ access to the ADHCFGP data set in the RACF® DATASET class
- UPDATE access to the DB2PARMS data set in the RACF DATASET class
- The ability to connect to the Db2 subsystem that is monitored by the collector agent
- The ability to read data from the following Db2 subsystem catalog tables:
  - SYSTABLES
  - SYSINDEXES
  - SYSDBRM
  - SYSPACKAGE
  - SYSPACKSTMT
  - SYSSTMT

Procedure

1. Using the sample library member ADHC*SSID* as a template, customize the member according to the directions contained in the sample JCL. Any valid member name can be used for the started task name, but the suggested started task name is ADHC*SSID*, where *SSID* is the identifier of the Db2 subsystem that is to be monitored.
2. Copy the customized JCL to an appropriate SYSPROC data set. The JCL must include definitions for the following data descriptions:

   ADHPARMS
   : ADHPARMS must name the IBM Guardium S-TAP for Db2 collector agent configuration file.

   DB2PARMS
   : DB2PARMS must name the IBM Guardium S-TAP for Db2 product control file (example: ADH.V0A00.CONTROL).

   ADHPLCY
   : ADHPLCY enables policy persistence. For more information, see the Policy Persistence information provided in Policy pushdown.
   If ADHPLCY is defined, it must point to a data set that is allocated with a record format of fixed blocked (RECFM=FB) and a record length (LRECL) greater than or equal to 256.
   The ADHPLCY data set should be allocated with a minimum of 50 primary tracks and 10 secondary tracks. The ADHPLCY data set can be sequential, PDS, or PDS/E. If you use PDS or PDS/E, the space requirements might need to be increased in relation to the number of members that are contained within the data set.

   ADHLOG
   : ADHLOG is the SYSOUT data set to which IBM Guardium S-TAP for Db2 collector agent log messages will be written.

   STEPLIB
   : STEPLIB must include the IBM Guardium S-TAP for Db2 SADHLOAD data set.
   Note: Every data set allocated to STEPLIB must be APF-authorized.

   SYSPRINT
   : SYSPRINT is the SYSOUT data set to which log messages will be written.

Parent topic: Configuring the collector agent
Previous topic: Configuring the ADHCFGP data set

Related reference

- Sample library members

Configuring the collector agent for additional Db2 subsystems

The collector agent must be configured for each Db2 subsystem that is to be audited.

Before you begin

You must have the following user ID authorities:

- READ access to ADHCFGx parameter data sets, Db2 catalogs, and VSAM control data sets
- Access to the DSNR resource class in Db2
- OMVS segment definition
- GRANT authority for SYSCTRL Db2 to communicate with the agent started task user IDs on all Db2 subsystems to be audited
- READ authority for the Db2 catalog tables
- Authority to use the dynamic LPA facility CSVDYLPA

To define additional Db2 subsystems for auditing, follow these steps:

Procedure

1. For additional stand-alone Db2 subsystems, use the SADHSAMP member ADHBIND to bind IBM Guardium S-TAP for Db2 plans on each Db2 subsystem that is to be audited.
   - For data sharing group members, use ADHBIND to bind one member of the data sharing group. The bind will apply to all additional group members.
   - When configuring the product control file for each member of the data sharing group, the PLAN value that is used in the ADHBIND job can also be used for the ADHPLAN1 value in the SJ001 JCL job.
   - For the first member of the data sharing group, PACKAGES and PLANS that are used in the ADHBIND job will work for all members of the data sharing group.
2. For each data sharing group or additional stand-alone Db2 subsystem, grant EXECUTE permission for the agent started task ID to the ADH PLAN 1, as specified in the PCF file for the Db2 subsystem. Refer to the JCL SADHSAMP member ADHGRANT for additional details on granting EXECUTE permission to the ADH PLAN.
3. Update the control file with the new SSID, or create a new S-TAP control file for each SSID by using the SADHSAMP member ADHSJ001.
4. Configure a new S-TAP agent configuration file.
5. Add the agent started task name to the z/OS® started task table.
6. Start the new S-TAP agent.
   Note:
   - Dispatching priority must be the same as, or higher than, Db2.

   After you start the agent, review the agent log and MVS™ log for any error messages. When an active collection policy is received, the agent starts collecting audit data.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Support Services Address Space overview

IBM Guardium S-TAP for Db2 uses a Support Services Address Space, also referred to as a Master Address Space. Learn about how the Master Address Space works, as well as the implications for using and stopping it.

A Support Services Address Space, also referred to as a Master Address Space, starts for each z/OS® image after the first instance of IBM Guardium S-TAP for Db2, InfoSphere® Optim™ Query Workload Replay for Db2, or IBM Db2 Query Monitor for z/OS starts with a MASTER_PROCNAME value that is not yet in use on that z/OS image.

The Master Address Space is a Service Address Space for all instances of IBM Guardium S-TAP for Db2, InfoSphere Optim Query Workload Replay for Db2, or IBM Db2 Query Monitor for z/OS that specify the same MASTER_PROCNAME parameter value that is running on the z/OS image. The Master Address Space acts as a placeholder for shared collector resources, and is similar to other Master Address Spaces that are used throughout MVS™. For sample, MVS and Db2 both have Master Address Spaces.

The Master Address Space:

- Never shuts down
- Does not run any code except for its initialization routines
- Owns resources that are needed by the shared collector
- Does not require a formal shutdown and should not be canceled or forced to shut down during the operation of IBM Guardium S-TAP for Db2, InfoSphere Optim Query Workload Replay for Db2, or IBM Db2 Query Monitor for z/OS.
- Forcing the Master Address Space to stop causes the abnormal termination of all IBM Guardium S-TAP for Db2, InfoSphere Optim Query Workload Replay for Db2, and IBM Db2 Query Monitor for z/OS subsystems on the LPAR.

Important: During installation, do not stop or start the Master Address Space unless required by product maintenance or instructed to do so by IBM Software Support.

- **Usage considerations for the Master Address Space**
  The following considerations apply to the use of the Support Services Address Space when you are using IBM Guardium S-TAP for Db2 to monitor the same Db2 subsystem, or multiple Db2 subsystems, on the same LPAR.
- **Stopping the Master Address Space**
  Do not stop the Master Address Space unless you are directed to do so by IBM Software Support or by a ++HOLD(ACTION) in a PTF.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Usage considerations for the Master Address Space

The following considerations apply to the use of the Support Services Address Space when you are using IBM Guardium S-TAP for Db2 to monitor the same Db2 subsystem, or multiple Db2 subsystems, on the same LPAR.

Monitoring the same Db2 subsystem
: If you use multiple collector products (such as IBM Guardium S-TAP for Db2, InfoSphere® Optim™ Query Workload Replay for Db2, or IBM Db2 Query Monitor for z/OS®) to monitor the same Db2 subsystem, each product must specify the same value for the MASTER_PROCNAME parameter.

Monitoring multiple Db2 subsystems that reside on the same LPAR
: If you use multiple collector products (such as IBM Guardium S-TAP for Db2, InfoSphere Optim Query Workload Replay for Db2, or IBM Db2 Query Monitor for z/OS) or multiple instances of the same product to monitor different Db2 subsystems that reside on the same LPAR, each product can have a different value for the MASTER_PROCNAME parameter.
  Note: This rule applies to instances when you are running different maintenance levels of the same product on the same LPAR (for example, if you are testing new maintenance levels prior to upgrading your production system).

Parent topic: Support Services Address Space overview

Stopping the Master Address Space

Do not stop the Master Address Space unless you are directed to do so by IBM Software Support or by a ++HOLD(ACTION) in a PTF.

To ensure product stability, the Master Address Space should only be stopped by using the sample job that is provided in SADHSAMP, member ADHMSTR. This job verifies that no IBM Guardium S-TAP for Db2, InfoSphere® Optim™ Query Workload Replay for Db2, or IBM Db2 Query Monitor for z/OS® subsystems are using the Master Address Space before it is stopped.

Parent topic: Support Services Address Space overview

Enabling CICS Login User ID reporting

You can capture the CICS® Login User ID for SQL Statements that are run in Db2 for CICS. The capture of CICS transactions is limited to CICS versions TS 4.2 or later, until end of support.

About this task

Update the CICS Connection definition to capture the CICS Login User ID:

Procedure

1. Set the ATTACHSEC parameter to ATTACHSEC(IDENTIFY) for the user ID to be passed from the Terminal-Owning Region (TOR) to the Application-Owning Region (AOR).
   This makes the user ID available for collection.
2. Ensure that the CICS_USERID collector agent parameter is set to *Y* to enable reporting of the CICS login user ID. For more information, see Collector agent parameters.

Results

The CICS Login User ID is reported in Guardium interface DB2 Client Info field for SQL Statements that are run in Db2 for CICS transactions.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Data collection

IBM Guardium S-TAP for Db2 collects data from an audited Db2 subsystem, in accordance with the collection policies that you create through the IBM Guardium system. Use a collection policy to specify filtering criteria that captures relevant data and filters out irrelevant data. The filtering criteria that you specify determines which data is streamed to your IBM Guardium system.

You can define and manage data collection and filtering in the Guardium Policy Builder of the IBM Guardium system interface.

- **Data collection process**
  During the collection process, IBM Guardium S-TAP for Db2 collects event data and verifies the data against the collection criteria that is defined in the collection policy.
- **Filtering**
  IBM Guardium S-TAP for Db2 V10.1.3 greatly simplifies the filtering process from that which was used in past product versions. All filtering occurs at the point of collection regardless of the field types that are included in the rules for the active collection policy. Filtering occurs at the point of collection with or without the specification of object types, which results in efficient CPU usage.
- **Policy pushdown**
  At startup, the IBM Guardium S-TAP for Db2 collector agent waits for a policy to be streamed (or pushed down) from the Guardium system before activating a collection. When the collector agent receives a policy, it inactivates the active collection (if a collection is active), updates the collection profile with the new policy, and then activates the collection policy.
- **Streaming audit data to multiple systems**
  Multistream mode enables S-TAP audit events to be sent to multiple connected appliances. You can enable multistreaming to up to 6 Guardium appliances (APPLIANCE_SERVER + APPLIANCE_SERVER_*n*, where *n* can be 1 - 5).
- **Starting and stopping the collector agent**
  After you configure the product and review the data collection information, you can start the collector agent. Use the commands provided to start and stop the collector agent started task from a cataloged procedure library.
- **Including or excluding failed accesses and negative SQL code**
  IBM Guardium S-TAP for Db2 enables you to include or exclude failed accesses and negative SQL code on a per-policy basis.
- **Quarantining SQL activity**
  IBM Guardium S-TAP for Db2 enables you to quarantine the SQL activity of specific users for specific periods of time.

- **SQL Blocking**
  You can block the SQL activity of Db2 users' (Auth IDs) access to specific tables and databases. SQL statements that are run against accelerated tables are eligible for blocking if the blocking filtering criteria is met. If a SQL statement matches the blocking criteria, the SQL statement is prevented from running. Use the Guardium appliance interface to define blocking policies.
- **Controlling host variable collection**
  IBM Guardium S-TAP for Db2 enables you to specify, on a per-rule basis, whether host variable information will be sent to the appliance for activity that matches that rule.
- **Collecting Command activity by using the Audit SQL Collector**
  IBM Guardium S-TAP for Db2 enables you to collect Command activity by using the Audit SQL Collector.
- **Collecting SET CURRENT SQLID events by using the Audit SQL Collector**
  IBM Guardium S-TAP for Db2 V10.1.3 enables you to collect SET CURRENT SQLID events by using the Audit SQL Collector.

Parent topic: IBM Security Guardium S-TAP for Db2 on z/OS

Data collection process

During the collection process, IBM Guardium S-TAP for Db2 collects event data and verifies the data against the collection criteria that is defined in the collection policy.

Collection includes the following:

- All reads and all changes (with collector agent based collection)
- Host variables up to a maximum of 256 bytes per variable
- Dynamic SQL text up to 2 million bytes per statement
- Static SQL text up to 4000 bytes

Data collected from Db2 is filtered during the collection process, and non-relevant events are discarded. Specify filtering criteria by defining a collection policy so that only relevant events are captured. This limits the amount of unnecessary data that is collected and stored by IBM Guardium S-TAP for Db2.

- **Collection policy**
  The collection policy is defined by the Guardium policy. It is used to determine which events (SQL, Command, Utilities, etc.) are streamed from the z/OS collector agent to the Guardium appliance. The following methodology determines how the collection policy determines whether to stream events to the Guardium appliance.
- **Collected event types**
  All event types are collected with the SQL Collection mechanism, which is not dependent on other SQL Trace information such as the Db2 Trace (IFI) or SMF data. Filtering criteria is defined and managed through the IBM Guardium system interface. This table lists the types of events that can be collected.

Parent topic: Data collection

Collection policy

The collection policy is defined by the Guardium policy. It is used to determine which events (SQL, Command, Utilities, etc.) are streamed from the z/OS collector agent to the Guardium appliance. The following methodology determines how the collection policy determines whether to stream events to the Guardium appliance.

The collection policy is comprised of one or more rules. Each rule includes a list of filtering criteria (fields), which is used to determine the events that are streamed. An event is streamed to the appliance if the fields within the event match all of the fields defined within any rules of the collection policy. (Evaluation of the rules within the collection policy is *or*.) For example, if a collection policy is composed of three rules (rule 1, rule 2, and rule 3), an event is streamed if it matches rule 1, or rule 2, or rule 3.

Each rule is made up of filter types and values (fields) that are used to determine if an event should be collected. If the fields of the rule are equivalent to the corresponding fields in the event, the rule evaluates the event to be true, or a match, and the event is captured. A rule is considered true if one of each specified filter type and value matches that of the event. (Evaluation of the rule is *and*.) For example:

- If a rule is comprised of the filters DBUser=`User1` and PLAN=`DSNTEP2`, an event is collected by the rule if both DBUser=`User1` and PLAN=`DSNTEP2` are present in the event. If only one of the filtering criterion is present, or neither of the filtering criteria are present, the event does not meet the conditions of the rule and will not be collected by the rule.
- If a rule is comprised of the filters NET_PROTOCOL=`TSO` and OS_USER=`User1`, then only TSO workload events executed by User1 will be collected by the rule (wherein User1 is Original Auth ID). Non-TSO workloads run by User1 will not be collected by the rule, nor will TSO workloads run by User2.

The following sections further describe how to filter the collector agent.

Parent topic: Data collection process

Collected event types

All event types are collected with the SQL Collection mechanism, which is not dependent on other SQL Trace information such as the DB2® Trace (IFI) or SMF data. Filtering criteria is defined and managed through the IBM® Guardium® system interface. This table lists the types of events that can be collected.

Table 1. Collected event types

Collected event types
All reads (SQL SELECT)
All changes (SQL UPDATE, INSERT, DELETE)
Authorization
Audit data for Db2 utilities
Grant/Revoke
Access attempts
Binds/Rebinds
Commit/Rollbacks
Db2 commands

Collected event types
Db2 utilities
Failed logins
Create, Alter, Drop table
Create, Alter, Drop all other object types
Static SQL host variables
Static SQL text
Dynamic SQL host variables
Dynamic SQL text
Negative SQL events
SQL events involving Accelerated/IDAA tables

Information collected for CICS events

For events that are collected with Net Prtcl of a type that originates from CICS, the Internet Protocol (IP) address is reported as Terminal ID and the CICS End User is reported as the DB2 User Name in the IBM Guardium system interface.

- **Audit data for Db2 Utilities**
  You can collect table information for Db2 utility operations that are run against tablespaces. The IBM Guardium S-TAP for Db2 collector agent reports the name of the table associated with the tablespace. Configure audit data for Db2 utilities according to the following rules.

Parent topic: Data collection process

Audit data for Db2 Utilities

You can collect table information for Db2 utility operations that are run against tablespaces. The IBM Guardium S-TAP for Db2 collector agent reports the name of the table associated with the tablespace. Configure audit data for Db2 utilities according to the following rules.

Set the STAP_UTILITY_TS_TO_TABLE parameter to `Y` to collect audit data for Db2 utilities. See Collector agent parameters for more information.
Audit data for Db2 utilities is collected according to the following rules:

- When a single table is contained in the tablespace, the table information is reported.
- When more than one table is contained in the tablespace, the product can be configured to report either:

  No tables
  : The tablespace is reported, but no tables are reported.

  All tables in the tablespace
  : Utility operations are reported against the accessed table.
  This option can result in false positives being reported against tables in the tablespace that were not affected by the running of the utility.

Parent topic: Collected event types

Filtering

IBM Guardium S-TAP for Db2 V10.1.3 greatly simplifies the filtering process from that which was used in past product versions. All filtering occurs at the point of collection regardless of the field types that are included in the rules for the active collection policy. Filtering occurs at the point of collection with or without the specification of object types, which results in efficient CPU usage.

Filtering occurs when you create a filter that uses one or more of the following filter fields:

Net Prtcl
: Specifies the appliance connection type to Db2.

OS User
: Specifies the original operator user ID that is used to connect to Db2.

DB User
: Specifies the primary AUTHID that is used for authorization within Db2. In most situations, this value is the same as OS User.

App. User (PROG=*program*)
: Specifies a valid DB2 program name, such as `DSNTEP2`.

App. User (PLAN=*plan*)
: Specifies a valid DB2 plan name, such as `DSNTEP2`.

Client Info (APPL=*transaction name*)
: Specifies a valid program (or user workstation transaction) name, such as `db2.exe`.

Client Info (WKSTN=*workstation name*)
: Specifies a valid user workstation name, such as `PCsys1`.

Client Info (USER=*user name*)
: Specifies a valid user name, such as `PCuser1`.

Object type (%/SYSIBM.SYSTABLE)
: Specifies a table.

These fields can be fully qualified, or partially qualified by using the percent sign wildcard character. For more information about using wildcard characters, see Filter wildcard support.
The most efficient CPU usage is achieved when you create a filter that eliminates the greatest number of events. To increase filtering efficiency, refine your filtering criteria by indicating the additional filtering types with specific values that are associated with the data that you want to collect.

Improving filtering efficiency

You can improve the CPU efficiency of filtering by including filter types in the filter. Specifying the plan, auth ID, connection type, operator ID, program, workstation user, workstation name, or object filter types that are associated with the performed action improves efficiency, as shown in the following example.

Example

To capture access to a table called *MY.TABLE*, you could create the following filter:

Filter 1
Schema.Table equal to *MY.TABLE*

This filter causes IBM Guardium S-TAP for Db2 to capture only those events that access MY.TABLE.

To increase efficiency in this example, specify a filter field, such as plan, even if you are sure that plan is the only plan that accesses this table. To capture access to the table *MY.TABLE* for an application that runs under a specific plan, such as *MYPLAN*, the following is an example of a more efficient filter:

Filter 2
Plan equal to *MYPLAN*
Schema.Table equal to *MY.TABLE*

Specifying the plan results in only those events with the specified plan and object being streamed to appliance. Fewer events streamed to the appliance results in improved CPU usage.

- **Event types and filtering**
  The following table shows the correlation between the event type and filtering. You can define and manage filtering criteria by setting the Database Type to DB2 Collection Profile in the Guardium Policy Builder of the Guardium appliance interface.
- **Filtering by database name**
  IBM Guardium S-TAP for Db2 enables you to filter by database name. You can specify database name filters, on a per-rule basis, to be included in the SQL activity filters.
- **Filter wildcard support**
  When you are creating a filter, value strings can include the percent sign (%) as a wildcard character. The wildcard character (%) enables the collector to match strings without you having to provide all possible string values for a filter value.

Parent topic: Data collection

Event types and filtering

The following table shows the correlation between the event type and filtering. You can define and manage filtering criteria by setting the Database Type to DB2 Collection Profile in the Guardium Policy Builder of the Guardium® appliance interface.

If you enable collection of SELECT/UPDATE/INSERT/DELETE events, then the event collection is subjected to additional filtering. If you enable collection of event types other than SELECT/UPDATE/INSERT/DELETE, then the events are collected without being subjected to filtering.

Table 1. Event types and filtering

Event type	Subjected to filtering?
SELECT/UPDATE/INSERT/DELETE (SUID)	Yes
CREATE/ALTER/DROP	No
GRANT/REVOKE	No
SET CURRENT SQLID	No
DB2® COMMANDS	No
Db2 UTILITIES	No
FAILED LOGINS	No
NEGATIVE SQLCODEs	No
COMMIT/ROLLBACK	No
BINDS/REBINDS	No

Enabling the collection of specific event types

The active policy determines which event types are enabled for collection. If the event type is enabled within a rule for the active policy, it is enabled for all rules within the active policy.

An event that is enabled in Rule 1 is subjected to subsequent rule filters. The following is an example using ASC event type collection:

- Rule 1 contains an Object field value of `%/%.%`.
- Rule 1 contains AUTHID filtering for User 1.
- Rule 2 contains AUTHID filtering for User 2.
- SELECT/UPDATE/DELETE/INSERT/SET CURRENT USERID/CREATE/ALTER/DROP events are collected for all tables for both User 1 and User 2.

Tip: This example could be simplified by placing both AUTHIDs into a group within a single rule.
The following is an example using event type collection:

- Rule 1 contains the collection of Utility events.
- Rule 1 contains AUTHID filtering for User 1.
- Rule 2 does not contain the collection of Utility events, but it contains AUTHID filtering for User 2.
- All Utility events are collected because they are enabled for Rule 1.

This list describes how you can enable the collection of specific event types:

SELECT/UPDATE/INSERT/DELETE (SUID)
Enable collection by including any filter type or non-blank value in the Object field of the rule.

Two target records are reported for nested INSERT/UPDATE/DELETE events: SELECT, and either INSERT, UPDATE, or DELETE. All nested INSERT/UPDATE/DELETE events are considered Table Change events. If the table filter is set to collect only READ events, then these events are filtered out (not collected).
Wildcarding can be used within the Object field value, for example: `%/SYSIBM.SYSTABLES` or `%/%.%`.

CREATE/ALTER/DROP
: Collection is automatically enabled by including any filter type or non-blank value in the Object field of the rule.
Wildcarding can be used within the Object field value, for example: `%/SYSIBM.SYSTABLES` or `%/%.%`.

GRANT/REVOKE
: Enable collection through the GRANT/REVOKE command setting.

SET CURRENT SQLID
: Collection is automatically enabled by including any filter type or non-blank value in the Object field of the rule.
Wildcarding can be used within the Object field value, for example: `%/SYSIBM.SYSTABLES` or `%/%.%`.

DB2 COMMANDS
: Enable collection through the DB2 Commands command setting.

DB2 UTILITIES
: Enable collection through the UTILITES command setting.

FAILED LOGINS
: Enable collection through the FAILED AUTHID CHANGES command setting.

NEGATIVE SQLCODES
: Enable collection through the presence of a negative SQLCODE list. Only one list is allowed per policy.
SQLCODE collection can be added to an active collection policy. A policy that contains a single rule with only negative SQLCODES results in an inactive policy.

COMMIT/ROLLBACK
: Enable collection by adding COMMIT/ROLLBACK to the Guardium appliance policy.

Parent topic: Filtering

Filtering by database name

IBM Guardium S-TAP for Db2 enables you to filter by database name. You can specify database name filters, on a per-rule basis, to be included in the SQL activity filters.

The following operations are supported:

Included operations
: The event is audited if any of the objects are in any of the DBNAMEs.

Excluded operations
: If all of the objects are not in any of the DBNAMEs, then it is a considered a match.
Example: All of the objects must be in one or more of the DBNAMEs for them to be excluded. If an object is from a DBNAME that is not in the list, then it is considered a match. If any database that is accessed by the query is not in the EXCLUDE DB list, then the query must be captured.

Wildcarding
: Filter values can include the percent sign (%) as a wildcard character.

Parent topic: Filtering

Filter wildcard support

When you are creating a filter, value strings can include the percent sign (%) as a wildcard character. The wildcard character (%) enables the collector to match strings without you having to provide all possible string values for a filter value.

Note: The use of wildcards in filters can potentially result in the collection of significant amounts of captured data.
Filtering fields can be fully qualified, or partially qualified, by using the percent sign wildcard character. You can insert the wildcard character (%) anywhere within the value string. The presence of the wildcard character (%) represents a string of zero of more characters. It can be embedded within a string in the following ways to achieve the following results:

%
: Matches all strings.

%*a*
: Matches all strings that end with the letter *a*, for example: *a*, *ba*, *cba*.

a%
: Matches all strings that start with the letter *a*, for example: *a*, *ab*, *abc*.

a%*a*
: Matches all strings the begin and end with the letter *a*, for example *a*, *aba*, *aca*.

Note: The wildcard character (%) cannot be used explicitly as part of the filter value.
Parent topic: Filtering

Policy pushdown

At startup, the IBM Guardium S-TAP for Db2 collector agent waits for a policy to be streamed (or pushed down) from the Guardium system before activating a collection. When the collector agent receives a policy, it inactivates the active collection (if a collection is active), updates the collection profile with the new policy, and then activates the collection policy.

The following processing occurs in the collector agent when a policy is received:

1. The new policy is compared to the currently active policy if the new policy contains one or more rules.
    a. If the policies are identical, no further processing is required.
    b. If the policies are not identical, the policy is written to DD:ADHPLCY (if defined) and it becomes the active collection policy.
2. If the new policy does not apply to this subsystem, processing continues without any changes. In this case, if there is an active policy, the collection continues to use it. If no policy is active, none is started.
3. If the new policy is inactive (contains no general audit settings, table or target definitions), the active policy is inactivated.

Policy persistence

For a policy to be pushed down, the z/OS collector agent requires connection to the Guardium appliance. If the z/OS collector agent is unable to connect to the appliance, the z/OS collector agent will read the policy from the ADHPLCY DD (if it is defined in the started task JCL). The z/OS collector agent will activate collection based on the policy that is read from the DD until a connection with the appliance is established. When the connection is established, the policy that is pushed down from the appliance replaces the policy that was read from the DD.

The file contents defined by the ADHPLCY DD contains the policy from the last successful policy pushdown from the appliance.

If ADHPLCY is defined, it must point to a data set that is allocated with a record format of fixed blocked (RECFM=FB) and a record length (LRECL) greater than or equal to 80.

Suggested ADHPLCY DD settings are as follows:

- Record format (RECFM): FB
- Record length (LRECL): 80
- Block size (BLCKSIZE): 3120
- Data set name type (DSNTYPE): LIBRARY
- Data set organization (DSORG): PO

The ADHPLCY data set should be allocated with a minimum of 50 primary tracks and 10 secondary tracks. The ADHPLCY data set can be sequential, PDS, or PDS/E. If you use PDS or PDS/E, the space requirements might need to be increased in relation to the number of members that are contained within the data set.

For more information about creating, activating, and inactivating policies from the Guardium system interface, see the how-to topics in the *Security Guardium V10.1.3* documentation in the IBM Knowledge Center.

For more information about using data sets, see the z/OS documentation in the IBM Knowledge Center, https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.1.0/com.ibm.zos.v2r1.idad400/toc.htm.

Parent topic: Data collection

Streaming audit data to multiple systems

Multistream mode enables S-TAP audit events to be sent to multiple connected appliances. You can enable multistreaming to up to 6 Guardium appliances (APPLIANCE_SERVER + APPLIANCE_SERVER_*n*, where *n* can be 1 - 5).

Multistream mode provides a mechanism for distributing a high-volume workload over multiple connected appliances. In multistream mode, a single audit event is only sent to a single appliance. Multistream mode does not enable mirroring of the same set of audit events to multiple appliances.

IBM Guardium S-TAP for Db2 sends events to a single appliance until a ping occurs, or the number of records that is specified by MEGABUFFER_COUNT is reached.

To enable multistreaming, you must specify *MULTI_STREAM* when you configure the APPLIANCE_SERVER_LIST parameter. Parameters APPLIANCE_SERVER and APPLIANCE_SERVER_[1-5] specify the appliances to which you intend to stream events. The appliance that is specified by APPLIANCE_SERVER provides the policy that is used for event matching.

The APPLIANCE_SERVER parameter specifies the first appliance to which audit events are streamed. The collection policy that is pushed down from the first appliance determines which events are collected and streamed to all appliances that are enabled for multistreaming.

The IBM Guardium S-TAP for Db2 agent streams events to the first appliance, then sequentially to each subsequent appliance in the multistreaming set. Each appliance in the multistreaming set then processes (logs and discards) each event in accordance with the locally installed policies.

Parent topic: Data collection

Starting and stopping the collector agent

After you configure the product and review the data collection information, you can start the collector agent. Use the commands provided to start and stop the collector agent started task from a cataloged procedure library.

Procedure

1. To start the collector agent, use the START command.
   Example: /S ADHCSSID
2. To stop the collector agent, use the STOP command, or the MODIFY command with the STOP parameter.
   Example:

   ```
   /P ADHCSSID
   ```

   or

   ```
   /F ADHCSSID,STOP
   ```

Parent topic: Data collection

Including or excluding failed accesses and negative SQL code

IBM® Guardium® S-TAP® for DB2® enables you to include or exclude failed accesses and negative SQL code on a per-policy basis.

In the Guardium appliance interface, create a list of SQL codes to include of exclude during data collection. A policy can contain either all values to be included, or all values to be excluded. In an *include* list, any SQL activity that fails within the SQLCODE list will be collected. In an *exclude* list, any SQL activity that does not fail within the SQLCODE list will be collected.
Note:

- No other filtering criteria will be ANDed with the SQLCODE filter rule when determining the collection status of the event.
- Enabling AUDIT TRACE CLASS 1 (collection of failed accesses) is deprecated because negative SQL codes for these failed accesses will be collected.
- Failed access events are streamed to the appliance if the negative SQL code is:
  - Included in the list of negative SQLCODE to be captured
  - Not based on *ALL FAILED AUTHORIZATIONS* being included in the COMMANDS filter setting for the policy. *ALL FAILED AUTHORIZATIONS* can be removed from the COMMANDS filter setting.

Parent topic: Data collection

Quarantining SQL activity

IBM® Guardium® S-TAP® for DB2® enables you to quarantine the SQL activity of specific users for specific periods of time.

Quarantining a user of a specific Db2 subsystem means that for the period of time that is specified, the quarantined user will not be able to run SQL statement in the targeted Db2 subsystem. If a quarantined user attempts access during a restricted time, access will be denied. Use the Guardium appliance interface to quarantine user activity.

Note: Quarantine does not take effect immediately. The SQL statement that produces the event to trigger the quarantine is completed before the quarantine takes effect. It is possible for additional SQL statements to be run by the quarantined user before the quarantine takes effect.

Parent topic: Data collection

SQL Blocking

You can block the SQL activity of DB2® users' (Auth IDs) access to specific tables and databases. SQL statements that are run against accelerated tables are eligible for blocking if the blocking filtering criteria is met. If a SQL statement matches the blocking criteria, the SQL statement is prevented from running. Use the Guardium® appliance interface to define blocking policies.

Enabling blocking policy

Blocking policy pushdown maps blocking policies to the S-TAP® blocking mechanism within the collector agent. At startup, the collector agent checks if a blocking policy was streamed (or pushed down) from the IBM® Guardium system when a collection policy was pushed. When the collector agent receives a blocking policy, it inactivates any incidence of active blocking, updates the blocking policy, and activates blocking.

When a blocking policy is received, the collector agent completes the following steps:

1. Compares the new blocking policy to the currently active blocking policy, if the new policy contains one or more rules.
   - If the blocking policies are identical, the collector agent determines that no further processing is required.
   - If the blocking policies are different, then the new blocking policy replaces the old one.
2. Evaluates the pushed-down list and filters to determine which events to block.
3. Validates the list of supplied objects.
   - The object must exist at the time of the installation of the blocking policy.
   - If a table that is included in the blocking policy does not exist when the blocking policy is installed, message ADHP190W is generated to identify the table.
   - Blocking is not enabled for tables that are reported by a ADHP190W message.
   - The obid/dbid for the object are checked for performance reasons.
   - If the object is dropped and then recreated, the policy must be reinstalled.

If the field values of the SQL event match corresponding filter values (blocking rule conditions) in the blocking policy, then the SQL statements are blocked and ended with a -807 error code.

For more information about creating, activating, and inactivating blocking policies from the IBM Guardium system interface, refer to the Security Guardium documentation in the IBM Knowledge Center.

Enable or disable blocking on the host

If permitted, you can enable blocking, disable blocking, or report the blocking status (enabled or disabled) by using the following operator commands:

- /F <adhstc>,BLOCKING ENABLE
- /F <adhstc>,BLOCKING DISABLE
- /F <adhstc>,BLOCKING STATUS

These commands override and determine the blocking status whether or not a blocking policy is present. By default, blocking is enabled at startup; but if you use the /F <adhstc>,BLOCKING DISABLE command and push down blocking rules, the blocking rules will be processed and blocking will be established within the z/OS® agent, but blocking will not be enabled. If you use the /F <adhstc>,BLOCKING ENABLE command, blocking is not activated until a blocking policy is pushed down.

The ADHPARMS z/OS collector agent parameter, STAP_BLOCKING, controls whether the blocking operator command is permitted and whether blocking is enabled or disabled. For more information about STAP_BLOCKING, see Collector agent parameters.

Parent topic: Data collection

Controlling host variable collection

IBM® Guardium® S-TAP® for DB2® enables you to specify, on a per-rule basis, whether host variable information will be sent to the appliance for activity that matches that rule.

In the Guardium appliance interface, specify whether host variable information should be sent to the appliance for activity that matches a rule. When host variable collection is enabled, up to 256 bytes per variable of host variable data is sent to the Guardium appliance. For enhanced security of Personally Identifiable Information (PII), host variables are not collected by default in IBM Guardium S-TAP for Db2 V10.0 and later.

In the Guardium appliance interface, specify whether host variable information should be sent to the appliance for activity that matches a rule.

The Guardium appliance interface can be overridden by the FORCE_LOG_LIMITED parameter. This parameter enables you to restrict the collection of personal data by controlling whether the active policy controls the collection of host variables.

- If FORCE_LOG_LIMITED is set to *Y*, the policy setting for the collection of host variables is ignored, and host variables are not collected.
- If FORCE_LOG_LIMITED is set to *N*, the collection of host variables is controlled by the host variable settings in the active policy.

For more information, see Collector agent parameters.
Parent topic: Data collection

Collecting Command activity by using the Audit SQL Collector

IBM Guardium S-TAP for Db2 enables you to collect Command activity by using the Audit SQL Collector.

Command events are not subjected to filtering. All command events are streamed directly to the Guardium appliance for post-collection filtering. All command events are streamed directly to the Guardium appliance for optional post-collection filtering.

Parent topic: Data collection

Collecting SET CURRENT SQLID events by using the Audit SQL Collector

IBM Guardium S-TAP for Db2 V10.1.3 enables you to collect SET CURRENT SQLID events by using the Audit SQL Collector.

In IBM Guardium S-TAP for Db2 V10.1.3, IFI TRACE CLASS 7 is no longer enabled, and SET CURRENT SQLID events are automatically collected by using the Audit SQL Collector. SET CURRENT SQLID events are streamed to the Guardium appliance without being subjected to filtering.

Parent topic: Data collection

Reference information

These reference topics are designed to provide you with quick access to information about IBM Guardium S-TAP for Db2 sample library members, parameters, and variables.

Topics:

Other resources

The following IBM documentation provides more information about configuring and operating this product.

- IBM Ported Tools for z/OS®: Open SSH User's Guide
- z/OS UNIX System Services Planning
- z/OS MVS™ JCL User's Guide
- Db2 Administration Guide
- Monitoring and Tuning Db2 Performance

Parent topic: IBM Security Guardium S-TAP for Db2 on z/OS

Sample library members

Use the following sample library members that are included with IBM Guardium S-TAP for Db2 for installation and configuration.

Table 1. Installation and configuration sample library members

Member	Type	Description
ADHBIND	JCL	Bind job used to bind DBRMs.
ADHBINDB	JCL	Bind job used to bind packages.

Member	Type	Description
ADHCFGP	80-byte sequential or partitioned data set	A listing of required parameters that control how the collector is implemented.
ADHCFGP E	80-byte sequential or partitioned data set	A listing of optional parameters that control how the collector is implemented.
ADHCSSI D	Procedure	IBM Guardium S-TAP for Db2 collector started task procedure. Runs an instance of the IBM Guardium S-TAP for Db2 collector started task.
ADHGRA NT	JCL	Grants required authorizations to USERID and PLAN.
ADHEMA C1	(edit macro)	Customizes the variables that appear in the DDL and JCL to be run.
ADHMST R	JCL	Stops the IBM Guardium S-TAP for Db2 master address space.
ADHSJ00 0	JCL	Allocates VSAM product control file.
ADHSJ00 1	JCL	Sets product configuration options.
ADHSJ00 3	JCL	Generates the product control file content report.
ADHSTAP D	JCL	Produces an IBM Guardium S-TAP for Db2 diagnostic report.
ADHTCPD	JCL	Produces a TCP/IP diagnostic report to use for troubleshooting network connectivity and throughput issues.

Parent topic: Reference information

Related tasks

- Defining the collector agent started task JCL

MODIFY command

The MODIFY command allows you to issue requests against, and dynamically change, characteristics of an active S-TAP task.

The abbreviated version of the MODIFY command is the letter F. The general format of MODIFY is as follows:

```
>>-+-MODIFY-+--procname--,--parameter-------------------------><
   '-F------'
```

wherein:

procname
: The name of the member in a procedure library that was used to start the server or address space.

parameter
: Any of the parameters that are valid for the server.

S-TAP supported MODIFY options with descriptions

The following is a sample syntax diagram:

```
>>-+-MODIFY-+--procname,--+-STAP-+-----------------+
                          |      +-,HELP ----------|
                          |      +-,ALL-----------|
                          |      +-,POLICY--------|
                          |      +-,COUNTS--------|
                          |      +-,CONFIG--------|
                          |      +-,HISTORY_QUEUE--|
                          |      +-,HISTORY_FILTER-|
                          |      +-,HISTORY_IO-----|
                          |      +-,BLOCKING-------|
                          |      +-,QUARANTINE-----|
                          |      +-,GET_STATUS-----|
                          +-BLOCKING--+ ENABLED-----|
                          |           -+ DISABLED----|
                          |           -+ STATUS------|
                          |      +-,MUSTGATHER------|
                          |      +-,TRACE_POLICY,ENABLE----|
                          |      +-,TRACE_POLICY,DISABLE---|
                          |      +-,TRACE_COMPILE,ENABLE---|
                          |      +-,TRACE_COMPILE,DISABLE--|
                          |      +-,TRACE_PROTOBUF,ENABLE--|
                          |      +-,TRACE_PROTOBUF,DISABLE-|
                          |      +-,LOG_EVENTS,ENABLE------|
                          |      +-,LOG_EVENTS,DISABLE-----|
                          |      +-,LOG_LEVEL,F|I|W|E|S----|
                          |      +-,RESET_CONFIG-----------|
```

Note the space (rather than the comma) before BLOCKING ENABLED, DISABLED, and STATUS.
Options are defined as follows:

HELP
: Display all available commands

STAP
: Display the current status of the started task

ALL

View all log information

POLICY
: View log information about the active policy

COUNTS
: View a log of detailed counts

CONFIG
: View a log about the current configuration

HISTORY_QUEUE
: View log details about the internal events queue

HISTORY_FILTER
: View log information about event filter results

HISTORY_IO
: View log details about the streaming of events

BLOCKING
: View log information about the active blocking policy

QUARANTINE
: View log information about the active quarantine policy

GET STATUS
: Request the most recent count of events that were received/processed by the appliance

BLOCKING
: **ENABLED:** Enable the blocking feature. Blocking is activated if a blocking rule is pushed.
DISABLED: Disable the blocking feature.
STATUS: Display blocking status.

MUSTGATHER
: Send a must-gather request to the appliance

TRACE_POLICY,ENABLE
: View information about the policy component

TRACE_POLICY,DISABLE
: Hide information about the policy component

TRACE_COMPILE,ENABLE
: View information about the filter component

TRACE_COMPILE,DISABLE
: Hide information about the filer component

TRACE_PROTOBUF,ENABLE
: View information about the streaming component

TRACE_PROTOBUF,DISABLE
: Hide information about the streaming component

LOG_EVENTS,ENABLE
: Log events that are streamed to the appliance

LOG_EVENTS,DISABLE
: Hide events that are streamed to the appliance

LOG_LEVEL,F|I|W|E|S
: Control the amount of output log information that is generated by the agent: debugging, informational, warning, error, severe

RESET_CONFIG
: Reset agent configurations to the default settings

The following example displays the active S-TAP policy:

```
F ADHPROC,STAP,POLICY

ADHP110I  IBM Security Guardium DB2 S-TAP mode: STREAMING EVENTS
ADHP140I  Event Counts:
ADHP141I  CONNTYPE_OTHER (0) . . . . . . . . . . 1
ADHP141I  CONNTYPE_TSO (1) . . . . . . . . . . . 0
ADHP141I  CONNTYPE_CALL_ATTACH (2) . . . . . . . 0
ADHP141I  CONNTYPE_DLI_BATCH (3)  .  . . . . . . 0
ADHP141I  CONNTYPE_CICS_ATTACH (4) . . . . . . . 0
ADHP141I  CONNTYPE_IMS_ATTACH_BMP (5)  . . . . . 0
ADHP141I  CONNTYPE_IMS_ATTACH_MPP (6)  . . . . . 0
ADHP141I  CONNTYPE_DB2_PRIVATE_PROTOCOL (7)  . . 0
ADHP141I  CONNTYPE_DRDA_PROTOCOL (8) . . . . . . 0
ADHP141I  CONNTYPE_IMS_CONTROL_REGION (9)  . . . 0
ADHP141I  CONNTYPE_IMS_TRANSACTION_BMP (10)  . . 0
ADHP141I  CONNTYPE_DB2_UTILITIES (11)  . . . . . 0
ADHP141I  CONNTYPE_RRSAF (12)  . . . . . . . . . 0
ADHP142I  MISC sent  . . . . . . . . . . . . . . 0
ADHP142I  UTILITY sent . . . . . . . . . . . . . 0
ADHP142I  DB2 COMMAND sent . . . . . . . . . . . 1
ADHP142I  SELECT sent  . . . . . . . . . . . . . 0
ADHP142I  UPDATE sent  . . . . . . . . . . . . . 0
ADHP142I  DELETE sent  . . . . . . . . . . . . . 0
ADHP142I  INSERT sent  . . . . . . . . . . . . . 0
ADHP142I  REVOKE sent  . . . . . . . . . . . . . 0
ADHP142I  GRANT sent   . . . . . . . . . . . . . 0
ADHP142I  COMMIT-ROLLBACK sent   . . . . . . . . 0
ADHP142I  BIND-REBIND sent   . . . . . . . . . . 0
ADHP142I  FAILED_SQLCODE sent   . . . . . . . .  0
ADHP143I  ALTER sent   . . . . . . . . . . . . . 0
ADHP143I  DROP sent  . . . . . . . . . . . . . . 0
ADHP143I  CREATE sent  . . . . . . . . . . . . . 0
ADHP144I  Bytes sent   . . . . . . . . . . . . . 363
ADHP145I  Events Sent  . . . . . . . . . . . . . 1
ADHP146I  Statements processed   . . . . . . . . 0
ADHP140I  Event Counts:
ADHQ3270I STAP INFO: STAGE1 FILTER IS.............. ACTIVE
ADHQ3270I STAP INFO: STAGE2 FILTER IS.............. NOTACTIV
ADHQ3270I STAP INFO: TOTAL EXEC SQL CALLS SEEN..... 0000000000000000
```

```
ADHQ3270I STAP INFO: STMTS PASSED STAGE1 FILTER....  0000000000000000
ADHQ3270I STAP INFO: STMTS FAILED STAGE1 FILTER....  0000000000000000
ADHQ3270I STAP INFO: STMTS PASSED, STAGE1 BYPASSED.  0000000000000000
ADHQ3270I STAP INFO: AUDS BLOCKS QUEUED.............. 0000000000000000
ADHQ3270I STAP INFO: AUDS BLOCKS SENT TO APPLIANCE.. 0000000000000001
ADHQ3270I STAP INFO: AUDS BLOCKS NOT SENT TO APPL... 0000000000000000
ADHQ3270I STAP INFO: AUDS BLOCKS FREED .............. 0000000000000000
ADHQ3270I STAP INFO: AUDS BLOCKS FREED LOST ........ 0000000000000000
ADHQ3270I STAP INFO: BYTES SENT...................... 000000000000016B
ADHQ3270I STAP INFO: UTILITY EVENTS QUEUED.......... 0000000000000000
ADHQ3270I STAP INFO: UTILITY EVENTS FREED............ 0000000000000000
ADHQ3270I STAP INFO: UTILITY REQ COUNT.............. 0000000000000000
```

The following example displays the S-TAP blocking status:

```
F ADHPROC,STAP,POLICY

ADHQ9899I - BLOCKING STATUS
ADHQ2023I - AUTHID BLOCKING IS ENABLED
ADHQ2034I - BLOCK TABLE 181_9901F000 HASH TABLES 181_99101000 SQLHS 1E8B6000

<policy>
    <selectblocking-rule>
        <target>
            <schema>DBTROS</schema>
            <name>TABLE1</name>
        </target>
        <target>
            <schema>DBTROS</schema>
            <name>TABLE2</name>
        </target>
    </selectblocking-rule>
</policy>
```

The following example displays the results of S_TAP GET_STATUS:

```
F ADHPROC,STAP,GET STATUS
ADHP170I - Event count reported by the appliance at time: 112
```

Parent topic: Reference information

Requesting and viewing S-TAP logging information

Use the S-TAP Logging command to issue a request for logging information from the S-TAP agent collector.

About this task

From the S-TAP control panel of the IBM® Guardium® system interface:

Procedure

1. Locate the policy component for your S-TAP (for example, RS22:A91A:POLICY) and select the G icon.
2. Select STAP Logging for Command.
3. Select a logging level and click Apply to request S-TAP logging.
   S-TAP logging levels provide log information as follows:

   Level 0
   : Logs program levels, event queue statistics, agent configuration, policy, and event counts.

   Level 1
   : Logs agent configuration, policy, and event counts.

   Level 2
   : Logs agent configuration.

   Level 3
   : Logs policy.

   Level 4 or higher
   : Logs event counts.

4. To view the S-TAP logging information, locate the policy component of your S-TAP and click the i icon.

Parent topic: Reference information

Collector agent parameters

The collector agent parameters are described in this section.

APPLIANCE_CONNECT_RETRY_COUNT

Required: No

Default: 0

Description: The number of consecutive failed connection attempts before terminating. The value of 0 indicates to never stop attempting connections. A value of 1 indicates a stop immediately after connection attempt fails. Range: 0 - 99999.

Syntax:

APPLIANCE_CONNECT_RETRY_COUNT*(retry_count)*

Example:

APPLIANCE_CONNECT_RETRY_COUNT(1000)

APPLIANCE_NETWORK_REQUEST_TIMEOUT

Default: 0

Range: 0 or 500 - 12000

Description: The value in milliseconds of the period of time to wait for network communication request send or receive to complete. A value of 0 results in no timeout period.

Syntax:

APPLIANCE_NETWORK_REQUEST_TIMEOUT*(timeout)*

Example:

APPLIANCE_NETWORK_REQUEST_TIMEOUT(0)

APPLIANCE_PING_RATE

Required: No

Default: 5

Description: Specifies the time interval between accesses to the Guardium system to prevent timeouts (disconnects) during idle periods. The value is in number of seconds.

Syntax:

APPLIANCE_PING_RATE(*ping_interval*)

Example:

APPLIANCE_PING_RATE(5)

APPLIANCE_PORT

Required: No

Default: 16022

Valid ports: 16022 or 16023

Description: The IP port number of the Guardium system to which the IBM Guardium S-TAP for Db2 audit data collector should connect. This parameter must be properly configured to enable collection of audit data and a connection to the IBM Guardium system. If port 16023 is used, encryption support is required for the connection to the appliance.

Note: Specifying this keyword and parameter designates the port on which the Guardium appliance is listening to the S-TAP. The port is dedicated to the IP address of the appliance. Port 16022 or 16023 can also be in use on z/OS® by another application.
Syntax:

APPLIANCE_PORT*(port_number)*

Example:

APPLIANCE_PORT(16022)

APPLIANCE_RETRY_INTERVAL

Required: No

Default: 3

Description: Specifies the time interval between attempts to establish a connection to the IBM Guardium system. The value is in number of seconds.

Syntax:

APPLIANCE_RETRY_INTERVAL(*retry_interval*)

Example:

APPLIANCE_RETRY_INTERVAL(3)

APPLIANCE_SERVER

Required: Yes

Default: None

Description: The host name or IP address (in dotted-decimal notation, for example: 1.2.3.4) of the IBM Guardium system to which the IBM Guardium S-TAP for Db2 audit data collector should connect.

Note: This parameter must be properly configured to enable collection of audit data, and a connection to the IBM Guardium system. The value can contain up to 128 characters.
Syntax:

APPLIANCE_SERVER*(hostname|ip_address)*

Example:

```
APPLIANCE_SERVER(192.168.2.205)
```

APPLIANCE_SERVER_FAILOVER_[1-5]

Required: No

Default: None

Description: The host name or IP address (in dotted-decimal notation, for example: 1.2.3.4) of the IBM Guardium system to which the IBM Guardium S-TAP for Db2 audit data collector should fail over to if APPLIANCE_SERVER is not available.

Note:

1. This parameter must be properly configured to enable collection of audit data and a connection to the IBM Guardium system. The value can contain up to 128 characters.
2. The collector agent attempts to connect to the fail over systems beginning with APPLIANCE_SERVER_FAILOVER_1, and ending with APPLIANCE_SERVER_FAILOVER_5.
3. Both the APPLIANCE _SERVER_FAILOVER_[1-5] and APPLIANCE_SERVER_[1-5] parameters can be used to designate servers for multistreaming or failover. Use the APPLIANCE_SERVER_LIST(MULTI_STREAM|FAILOVER) parameter to designate how these parameters are used.

Syntax:

```
APPLIANCE_SERVER_FAILOVER_1(hostname|ip_address)
```

Example parameter settings to enable multistream support:

```
APPLIANCE_SERVER_LIST(MULTI_STREAM)
APPLIANCE_SERVER(guardium1.company.com)
APPLIANCE_SERVER_1(guardium2.company.com)
APPLIANCE_SERVER_2(guardium3.company.com
```

APPLIANCE_SERVER_LIST(FAILOVER|MULTI_STREAM|HOT_FAILOVER)

Required: No

Default: FAILOVER

Description: If set to MULTI_STREAM, this parameter specifies that a Guardium appliance connection is to be established for each server that is identified by the APPLIANCE_SERVER_n parameter.

- If a connection is lost, S-TAP audit events continue to transmit over the remaining appliance connection.
- Lost connections are retried at regular intervals that are determined by multiplying the APPLIANCE_CONNECT_RETRY_COUNT by the APPLIANCE_PING_RATE.

If set to FAILOVER, this parameter specifies that one Guardium appliance connection is to be active at a time.

- If the connection to the primary appliance is lost, a failover action occurs, which results in an attempt to connect to the next available server. The next available server is identified by the APPLIANCE_SERVER_FAILOVER_n parameter.
- After a failover action occurs, the connection to the primary server is retried at regular intervals that are determined by multiplying the APPLIANCE_CONNECT_RETRY_COUNT by the APPLIANCE_PING_RATE.

With either setting of APPLIANCE_SERVER_LIST, if all connections fail, and a spill file is specified (parameter OUTAGE_SPILLAREA_SIZE), events are buffered to the spill file until a connection becomes available. If no spill file is specified, and all connections are lost, data loss occurs.

If set to HOT_FAILOVER, this parameter causes all connection types (POLICY and ASC) for each connected Guardium appliance to be kept active by pings. You can specify the primary Guardium appliance by using the APPLIANCE_SERVER parameter. If the primary Guardium appliance becomes unavailable and failover occurs, HOT_FAILOVER maintains the activity of the primary appliance policy.

Syntax:

```
APPLIANCE_SERVER_LIST_FAILOVER
```

Example:

```
APPLIANCE_SERVER_LIST_FAILOVER
```

AUDIT

Required: Yes

Default: None

Description: The Db2 subsystem ID for the Db2 subsystem on which the IBM Guardium S-TAP for Db2 Collector Agent should capture query data.

Note: This parameter must be properly configured to enable collection of capture data. The value can contain up to 4 characters.
Syntax:

```
AUDIT(ssid)
```

Example:

```
AUDIT(DSN1)
```

AUTHID

Required: No

Default: Defaults to the user ID under which the started task will run.

Description: The AUTHID parameter defines the Db2 AUTHID that IBM Guardium S-TAP for Db2 uses when establishing a connection to Db2 during interval processing. If you are using RACF® on your Db2 system, this ID must be defined to RACF. The AUTHID specified needs to be authorized through the resident security package, such as RACF, to perform the functions needed for all processes done by the started task and the Collector Agent monitoring subsystem. Such processes include connecting to each of the monitored Db2 SSIDs and performing file update activities against the IBM Guardium S-TAP for Db2 VSAM control file.

Notes:

1. The ID specified in the startup parameter AUTHID must be a valid TSO user ID and not a RACF group name.
2. If the AUTHID parameter is defined in the RACF Started Procedures Table (ICHRIN03), it should not be used as a startup parameter. The Started Procedures Table (ICHRIN03) associates the names of started procedures with specific RACF user IDs and group names. It can also contain a generic entry that assigns a user ID or group name to any started task that does not have a matching entry in the table. However, it is recommended that you use the STARTED class for most cases rather than the started procedures table.

Syntax:

```
AUTHID(db2authid)
```

Where *db2authid* is the Db2 AUTHID that IBM Guardium S-TAP for Db2 uses when establishing a connection to Db2 during interval processing.
Example:

```
AUTHID(DB2USER)
```

CICS_USERID

Required: No

Default: N

Description: If set to Y, the CICS_USERID parameter enables the capture of CICS Login User ID for SQL statements that are run in Db2 for CICS. For more information see Enabling CICS Login User ID reporting.

Syntax:

```
CICS_USERID(YES|NO)
```

Example:

```
CICS_USERID(Y)
```

COLLECT_COMMIT_ROLLBACK

Required: No

Default: N

Description: If set to Y, the COLLECT_COMMIT_ROLLBACK parameter enables the collection of COMMIT and ROLLBACK events.

Syntax:

```
COLLECT_COMMIT_ROLLBACK(YES|NO)
```

Example:

```
COLLECT_COMMIT_ROLLBACK(Y)
```

DEBUG

Required: No

Default: N

Description: The DEBUG parameter turns on debug mode and produces diagnostic messages for use by IBM Software Support.

Syntax:

```
DEBUG(YES|NO)
```

Example:

```
DEBUG(Y)
```

FORCE

Required: No

Default: N

Description: The FORCE parameter forces installation of a monitoring agent. If you use this parameter, any return codes from any failure reported in message ADHQ2002E are overridden.
Note: This parameter should not be specified without instruction by IBM Software Support.
Syntax:

```
FORCE(YES|NO)
```

Example:

```
FORCE(Y)
```

FORCE_LOG_LIMITED

Required: No

Default: N

Description: This parameter enables you to restrict the collection of sensitive data by controlling whether the active policy controls the collection of host variables.

If this parameter is set to *Y*:

- The policy setting for collection of host variables is ignored and host variables are not collected.
- The APPLIANCE_PORT parameter must be set to 16023. Port 16023 is used for AT-TLS-configured encrypted communications. If APPLIANCE_PORT is not set to 16023, the S-TAP agent will generate a log message indicating the configuration inconsistency, and shut down.

If this parameter is set to *N*, the collection of host variables is controlled by the host variable settings in the active policy.

Syntax:

```
FORCE_LOG_LIMITED(YES|NO)
```

Example:

```
FORCE_LOG_LIMITED(Y)
```

HOSTVAR_LIMIT

Required: No

Default: 1500

Description: This parameter designates the number of storage blocks to be allocated for host variable collection per event. The valid range is 1 -- 9999. If this parameter is not customized, the default value of 1500 is set.

If error message ADHQ1203I is encountered with RC=0008 and RSN=003F, increase the HOSTVAR_LIMIT setting to accommodate the collection of host variables for the monitored workload.

If IBM Guardium S-TAP for Db2 and IBM Db2 Query Monitor for z/OS are simultaneously monitoring the same Db2 subsystem, both products must have matching HOSTVAR_LIMIT settings to avoid receiving a mismatch error.

Syntax:

```
HOSTVAR_LIMIT(n)
```

where *n* is an integer between 1 - 9999.
Example:

```
HOSTVAR_LIMIT(1500)
```

ISM_CONSTRAINT_AGE

Required: No

Default: 300

Description: This parameter controls how much time must have passed since the last storage constraint occurrence for a given ISM storage space before the constraint event is considered to have been relieved.

Syntax:

```
ISM_CONSTRAINT_AGE(n)
```

where *n* is an integer between 1 - 60000 specified in .01 seconds. The default value is 300.
Example:

```
ISM_CONSTRAINT_AGE(16)
```

ISM_ERROR_DETAIL

Required: No

Default: Y

Description: This parameter controls whether messages ADHQ1203I and ADHQ1204I are issued to provide detailed information for ISM Storage Constraint situations. The product recommendation is to leave this parameter set to Y. This setting can be overridden at run time with the /f cqmstc,ISMERROR_DETAIL command.

Syntax:

```
ISM_ERROR_DETAIL(Y|N)
```

Example:

```
ISM_ERROR_DETAIL(Y)
```

ISM_ERROR_BLOCKS

Required: No

Default: 256

Description: This parameter determines the number of ISM Error Blocks that are allocated when IBM Guardium S-TAP for Db2 initializes.

If this value is too low, message ADHQ1219W might be issued. ISM Error Blocks communicate a storage constraint event from somewhere in the product to the task that issues storage constraint messages. If you run out of ISM Error Blocks, the storage constraint message will not be issued. However, an abend table entry will be created to document this event. This is most likely a temporary situation and it does not impact the overall performance of IBM Guardium S-TAP for Db2.

Syntax:

```
ISM_ERROR_BLOCKS(n)
```

where *n* is an integer, 16 - 8192. The default value is 256.
Example:

```
ISM_ERROR_BLOCKS(256)
```

ISM_ERROR_MSG_BLOCKS

Required: No

Default: 256

Description: This parameter determines the number of ISM Error Message Blocks that are allocated when IBM Guardium S-TAP for Db2 initializes. If this value is too low, duplicate ISM error message can be issued for the same space and reason instead of incrementing the occurrence count.

ISM Error Message Blocks are used by the task that issues storage constraint messages to do two things:

1. To consolidate similar storage constraint events to eliminate duplicate messaging for the same condition, and
2. To keep track of storage constraint events so that the Storage Constraint Relieved situation can be detected and messaged.

If you run out of ISM Error Message Blocks, this consolidation will not always occur. This would result in additional, duplicate messages in the log for the similar storage constraint events.

Syntax:

```
ISM_ERROR_MSG_BLOCKS(n)
```

where *n* is an integer between 16 - 8192. The default value is 256.
Example:

```
ISM_ERROR_MSG_BLOCKS(256)
```

MASTER_PROCNAME

Required: Yes

Default: None.

Description: The MASTER_PROCNAME parameter enables users to specify the PROCNAME to be used for the Master Address Space. Specifying this parameter causes IBM Guardium S-TAP for Db2 to use the Master Address Space with the same name.

- The MASTER_PROCNAME for IBM Guardium S-TAP for Db2 and Query Monitor must be the same when each is started at the same time for the same Db2 Subsystem.
- If this Master Address Space is already started, it is shared with other IBM Guardium S-TAP for Db2 subsystems that are already using it.
- If this Master Address Space has not already been started, it will start automatically.

Syntax:

```
MASTER_PROCNAME(procname)
```

where *procname* is the specified Master Address Space PROCNAME (character, 8 bytes).)
Example:

```
MASTER_PROCNAME(CQMMASTR)
```

MAXIMUM_ALLOCATIONS

Required: No

Default: 2048

Description: This parameter determines the maximum amount of global shared memory to be allocated by IBM Guardium S-TAP for Db2 for internal Integrated Storage Manager spaces.

Syntax:

```
MAXIMUM_ALLOCATIONS(n)
```

where *n* is an integer between 512 - 32768 specified in megabytes; must be smaller than SMEM_SIZE.
Example:

```
MAXIMUM_ALLOCATIONS(2048)
```

MESSAGE_LOG_LEVEL

Required: No

Default: I

Description: Controls the amount of output log information that is generated by the agent:

I
: Includes all log messages with an *informational* severity or higher

W
: Includes all log messages with a *warning* severity or higher

E
: Includes all log messages with an *error* severity or higher

S
Includes all log messages with a *severe* severity or higher

The ADHPARMS file is read when the agent is started. Modifying the log-level setting in the ADHPARMS file does not implement the new setting until you restart the collector agent.
Note: During installation, it is recommended that you set the MESSAGE_LOG_LEVEL to I.
Syntax:

```
MESSAGE_LOG_LEVEL(I|W|E|S)
```

Example:

```
MESSAGE_LOG_LEVEL(I)
```

OUTAGE_SPILLAREA_SIZE

Required: No

Default: 0

Description: This parameter determines the maximum amount of memory to be allocated to support the retention of audit data in the event of a Guardium system connection outage.
Note: A value of 0 disables spillfile support. When enabled, OUTAGE_SPILLAREA_SIZE supersedes SEND_FAIL_EVENT_COUNT for temporary data retention.
Syntax:

```
OUTAGE_SPILLAREA_SIZE(n)
```

where *n* is an integer between 0 - 1024 specified in megabytes.
Example:

```
OUTAGE_SPILLAREA_SIZE(2)
```

PREFER_IPV4_STACK

Required: No

Default: N

Description: If set to Y, this parameter causes a request to be issued to the Domain Name Server (DNS) for an IPV4 address for the hostname that is specified in the APPLIANCE_SERVER parameter:

- The DNS lookup request for an IPV4 address is attempted. If an IPV4 address is defined for the hostname, the DNS will respond with the value that will be used to connect to the Guardium appliance.
- If only an IPV6 address is defined at the DNS, then the DNS will respond with the IPV6 address that will be used to connect to the Guardium appliance.
- If both IPV4 and IPV6 addresses are defined at the Guardium appliance, the DNS will respond with both addresses, and the IPV4 address will be used to connect to the appliance.

If this parameter is set to N or omitted from configuration, a request for an IPV6 address is issued to the DNS for the hostname that is specified by the APPLIANCE_SERVER parameter:

- The DNS lookup request for an IPV6 address is attempted. If an IPV6 address is defined for the hostname, the DNS will respond with the value that will be used to connect to the Guardium appliance.
- If only an IPV4 address is defined at the DNS, then the DNS will respond with the IPV4 address that will be used to connect to the Guardium appliance.
- If both IPV4 and IPV6 addresses are defined at the Guardium appliance, the DNS will respond with both addresses, and the IPV4 address will be used to connect to the appliance.

Note: Whether or not this parameter is used, if the address returned from the DNS is not valid for the hostname, it will result in failure to connect to the appliance, and the IBM Guardium S-TAP for Db2 started task will terminate.
Syntax:

```
PREFER_IPV4_STACK(Y|N)
```

Example:

```
PREFER_IVP4_STACK(Y)
```

SEND_FAIL_EVENT_COUNT

Required: No

Default: 100

Description: Specifies the maximum number of events to be buffered during a communication outage with the Guardium system. Events are buffered in internal memory objects and streamed to the appliance at the time of reconnection.
Note: SEND_FAIL_EVENT_COUNT and OUTAGE_SPILLAREA_SIZE are mutually exclusive. When OUTAGE_SPILLAREA_SIZE is specified, spillfile support is enabled, which supersedes SEND_FAIL_EVENT_COUNT for temporary data retention.
Syntax:

```
SEND_FAIL_EVENT_COUNT (event_count)
```

where *event_count* is an integer between 0 – 1024 that represents the number of events to be buffered.
Example:

```
SEND_FAIL_EVENT_COUNT(100)
```

SMEM_SIZE(5|n)

Required: No

Default: 5

Description: This parameter determines the maximum amount global shared memory to be allocated by IBM Guardium S-TAP for Db2 for all purposes.

Syntax:

```
SMEM_SIZE(n)
```

where *n* is an integer between 3 - 32 specified in gigabytes; must be three times larger than MAXIMUM_ALLOCATIONS.
Example:

```
SMEM_SIZE(5)
```

STAP_BLOCKING

Required: No
Default: ENABLED
Description: The STAP_BLOCKING parameter controls whether blocking is enabled or disabled and whether the blocking operator command is permitted to enable, disable, or report status for blocking. This parameter cannot be overwritten by the BLOCKING operator command. STAP_BLOCKING parameter options are as follows:

- STAP_BLOCKING(ENABLED) enables the blocking feature. Blocking is activated if a blocking rule is pushed.
- STAP_BLOCKING(DISABLED) disables the blocking feature.
- STAP_BLOCKING(OPERATOR) enables the blocking feature and enables the BLOCKING operator command. Blocking is activated if a blocking rule is pushed.

Syntax: STAP_BLOCKING(ENABLED|DISABLED|OPERATOR)
Example: STAP_BLOCKING(ENABLED)

STAP_MEGABUFFER

Required: No

Default: Y

Description: When multiple IBM Guardium S-TAP for Db2 audit events are accumulated in a buffer, it is referred to as a megabuffer. A megabuffer reduces the CPU usage that is related to TCP/IP activity. To optimize IBM Guardium S-TAP for Db2 performance, STAP_MEGABUFFER must remain set to `Y`. However, STAP_MEGABUFFER can be set to `N` when buffering is not desired.

Setting the STAP_MEGABUFFER parameter to `N` eliminates buffering, and provides near real-time event streaming to the Guardium appliance. It also increases CPU usage, due to additional TCP/IP calls.

Syntax:

```
STAP_MEGABUFFER(Y|N)
```

Example:

```
STAP_MEGABUFFER(Y)
```

STAP_STREAM_EVENTS

Required: No

Default: Y

Description: This parameter specifies whether events will be streamed to the IBM Guardium system. The default value, *Y*, enables streaming. Specify *N* to disable streaming and enable Simulation mode.

Syntax:

```
STAP_STREAM_EVENTS(Y|N)
```

Example:

```
STAP_STREAM_EVENTS(Y)
```

STAP_TERMINATE_OPTIMIZE

Required: No

Default: N

Description: This parameter can be used to improve the response time for processing STAP_TERMINATE requests from the Guardium appliance. Roundtrip time for STAP_TERMINATE activity is impacted by the STAP_MEGABUFFER parameter. STAP_TERMINATE policies require near real-time event recording to the IBM Guardium system to analyze events against the policy and issue the termination requests to IBM Guardium S-TAP for Db2. To enable near real-time event recording to the Guardium appliance, set the STAP_MEGABUFFER parameter to `N`.

Syntax:

```
STAP_TERMINATE_OPTIMIZE(Y|N)
```

Example:

```
STAP_TERMINATE_OPTIMIZE(N)
```

STAP_UTILITY_MULTITABLE

Required: No

Default: N

Description: The STAP_UTILITY_MULTITABLE parameter works in conjunction with the STAP_UTILITY_TS_TO_TABLE parameter. These parameters control how table information is reported for Db2 Utility access events that involve tablespaces. The STAP_UTILITY_MULTITABLE parameter controls the behavior of the collector when multiple tables are contained in the tablespace. When STAP_UTILITY_MULTITABLE is set to Y:

- The collector will report all tables in the tablespace that are impacted by the utility. This guarantees that tablespace access by a utility execution will result in an audit event against the table name.
- Tables within a tablespace, which were not accessed by the utility, might be reported.

When STAP_UTILITY_MULTITABLE is set to N, no attempt is made to report table information for multi-table tablespaces accessed by a utility. Only the tablespace name is reported.

Syntax:

```
STAP_UTILITY_MULTITABLE(Y|N)
```

Example:

```
STAP_UTILITY_MULTITABLE(N)
```

No table names are reported (default).

```
STAP_UTILITY_MULTITABLE(Y)
```

All table names are reported.

STAP_UTILITY_TS_TO_TABLE

Required: No

Default: Y

Description: The STAP_UTILITY_TS_TO_TABLE parameter controls how table information is reported for Db2 Utility accesses to tablespaces. When the parameter is set to Y, the collector queries the Db2 catalog. The collector then determines and reports on which table exists within the tablespace that has been accessed by the utility execution. If multiple tables are contained in the tablespace, the STAP_UTILITY_MULTITABLE parameter controls whether the collector reports either:

All tables
: All table names in the accessed tablespace

No tables
: Only the tablespace is reported.

This action is controlled by STAP_UTILITY_MULTITABLE parameter setting.

Syntax:

```
STAP_UTILITY_TS_TO_TABLE(Y|N)
```

Example:

```
STAP_UTILITY_TS_TO_TABLE(Y)
```

STARTUP_DIAGNOSTICS

Required: No

Default: N

Description: The STARTUP_DIAGNOSTICS parameter causes IBM Guardium S-TAP for Db2 to produce diagnostic information output during startup of the collector agent. This output might be useful to IBM Support when diagnosing reported problems.

Syntax:

```
STARTUP_DIAGNOSTICS(Y|N)
```

Example:

```
STARTUP_DIAGNOSTICS(Y)
```

SHUTDOWN_DIAGNOSTICS

Required: No

Default: N

Description: The SHUTDOWN_DIAGNOSTICS parameter causes IBM Guardium S-TAP for Db2 to produce diagnostic information output during shutdown (stop) of the collector agent. This output might be useful to IBM Support when diagnosing reported problems.

Syntax:

```
SHUTDOWN_DIAGNOSTICS(Y|N)
```

Example:

```
SHUTDOWN_DIAGNOSTICS(Y)
```

SUBSYS

Required: No

Default: The default value is the Db2 subsystem name.

Description: The SUBSYS parameter defines the SQL Collector subsystem name. The subsystem name does not need to correspond to a Db2 subsystem nor an MVS™ operating system name. The name must be 1-4 characters in length.

Syntax:

`SUBSYS(ssid)`

Where *ssid* is the 1-4 character SQL Collector subsystem name.
Note: The SQL Collector subsystem ID must be unique across the SYSPLEX. A SQL Collector component subsystem must be running on each LPAR that has a Db2 subsystem to be captured. When choosing a collector agent subsystem ID name, be sure it will not conflict with another on the SYSPLEX. If the specified SUBSYS is not unique across the SYSPLEX, message ADHQ1003E will be issued.
Example:

`SUBSYS(ADH1)`

TS_OFFSET(E|W.HH.MM)

Required: No

Default: None (no offset)

Description:

- This parameter enables you to adjust the event timestamps that are steamed to the appliance by specifying the amount of time to adjust (offset) based on timezone.
  - For example, if running with a clock that is set to UTC 0.0 in a timezone that it is UTC + 9, GMT can be considered 9 hours west of the current time. In this situation, the parameter should be set as follows: `TS_OFFSET(W.09.00)`. Event timestamps will be adjusted (offset) by subtracting 9 hours from the original timestamp.
- If TS_OFFSET is not supplied, the timestamps that are streamed to the appliance are not adjusted based on timezone.

Syntax:

E|W
: East or west offset from GMT

HH
: Number of hours

MM
: Number of minutes

Example: TS_OFFSET(W.09.00)

ZIIP_FILTER(Y|N)

Required: No

Default: ZIIP_FILTER(N)

Description:

- ZIIP_FILTER(Y) indicates that the z/OS image running the collector agent started task has an IBM System z® Integrated Information Processor (zIIP). In this case, allow collector agent to perform offload profile filtering to a zIIP.
- If ZIIP_FILTER(Y) is specified and the collector agent started task is running on a z/OS that has no zIIP, message ADHQ1060I is issued, indicating the WLM related service has failed. In this case, collector agent continues to run as if ZIIP_FILTER(N) were set.

Syntax:ZIIP_FILTER(Y)

Example:ZIIP_FILTER(Y)

ZIIP_TCP(Y|N)

Required: No

Default:ZIIP_TCP(N)

Description:

- ZIIP_TCP(Y) indicates that the z/OS image running the collector agent started task has an IBM System z Integrated Information Processor (zIIP). In this case, allow collector agent to offload TCP/IP message processing to a zIIP.
- If ZIIP_TCP(Y) is specified and the collector agent started task is running on a z/OS that has no zIIP, message ADHQ1060I is issued, indicating the WLM related service has failed. In this case, collector agent continues to run as if ZIIP_TCP(N) were set.
  Note: ZIIP_TCP(Y) requires that zIIP filter support be enabled: ZIIP_FILTER(Y). If ZIIP_FILTER(N) and ZIIP_TCP(Y) are specified together, ZIIP_FILTER will be automatically set to Y.

Syntax:ZIIP_TCP(Y)

Example:ZIIP_TCP(Y)

/f cqmstc,ISMERROR_DETAIL(Y|N)

Description: This parameter controls whether ISM constraint message detail is on or off. When the parameter is specified, messages ADHQ1203I and ADHQ1204I are issued for ISM storage constraint situations.

Parent topic: Reference information

Keeping connections active when HOT_FAILOVER is enabled

When the HOT_FAILOVER feature is enabled by the APPLIANCE_SERVER_LIST parameter, all connection types (POLICY and ASC) for each connected Guardium® appliance are kept active by pings.

If the primary appliance becomes unavailable and failover occurs, the appliance policy that was originally pushed from the primary appliance continues to be active. When all Guardium appliances are connected, the status of each appliance connection, listed in the Guardium interface, is green.

Parent topic: Reference information

Collector agent sample parameter file

The following sample parameter file is the minimum set of parameters required in a collector agent parameter file (ADHCFGP). If you want to use this sample file, verify that the values on each parameter are appropriate for your environment.

```
-  5655-STP
-  (C) COPYRIGHT ROCKET SOFTWARE, INC. 1999 - 2015 ALL RIGHTS RESERVED.
-
-  MEMBER: ADHCFGP
-
-  DESCRIPTION: THIS IS A SAMPLE MINIMUM ADHCFGP MEMBER
-               USED FOR IBM SECURITY GUARDIUM S-TAP for DB2 on z/OS
-               COLLECTOR AGENT STARTUP.
-               VERIFY THAT THE VALUES ON EACH PARM ARE APPROPRIATE
-               FOR YOUR ENVIRONMENT.
-
- NOTE:  AFTER USING THE EDIT MACRO, VERIFY THAT NONE OF THE
-        STATEMENTS EXCEED COLUMN 72 IN LENGTH.
-
-
SUBSYS(#SSID)              -
AUDIT(#SSID)              -
MASTER_PROCNAME(ADHMST31)  -
APPLIANCE_SERVER(#APPSRVR)
```

Parent topic: Reference information

ADHEMAC1 edit macro variables

This table shows the ADHEMAC1 edit macro variables, including their default value and instructions for use. An example is also provided.

Table 1. ADHEMAC1 Edit macro variables

Variable	Default	Instructions
#SSID	MYSSID	Change the default to a valid Db2 subsystem ID. Note: The ADHEMAC1 macro sets the SUBSYS parameter using the #SSID variable. Running the macro sets SUBSYS to the Db2 subsystem ID used by the collector agent task. Do not change the #SSID variable in the ADHEMAC1 macro to be anything other than the Db2 subsystem ID used by the collector agent task.
#ADHOWNER	&ZUSER	Change &ZUSER to the value of #ADHQUALIFIER. #ADHOWNER is used to configure the owner of the plans and packages. It is used as the owner value of objects created by statements contained within the package or plan.
#ADHQUALIFIER	SYSTOOLS	Change the default to the schema name being used with this product.
#ADHUSERID	&ZUSER	Use as the authorization ID for the collector agent task.
#SADHLOAD	ADH.IBMTAPE.SADHLOAD	Change the default to the data set containing the IBM Guardium S-TAP for Db2 load modules.
#SADHDBRM	ADH.IBMTAPE.SADHDBRM	Change the default to the data set containing the IBM Guardium S-TAP for Db2 DBRMs.
#SDSNLOAD	DSN.Vxxx.SDSNLOAD	Change the default to the data set containing the Db2 load modules.
#SDSNRUNL	DSN.Vxxx.RUNLIB.LOAD	Change the default to the data set containing the Db2 DSNTEP2 module.
#DSNTEP2	DSNTEP2	Change the default to the DSNTEP2 plan name.
ADHPLAN1	ADHPLAN1	Change the default to a valid plan name. This plan used to collect information about the Db2 System catalog during audit data collection.
#SZPARM	MYSSIDPARM	Change the default to the Db2 ZPARM member that is associated with the Db2 subsystem.
#SBSDS01	MYSSID.BSDS01	Change the default to the DSN of the bootstrap data set 01.
#SBSDS02	MYSSID.BSDS02	Change the default to the DSN of the bootstrap data set 02.
#SDSNEXIT	DSN.Vxxx.SDSNEXIT	Change the default to the data set containing the Db2 ZPARMs.
#SFECLOAD	None	Data set name of the required FEC load library.
#SCQCLOAD	None	Data set name of the required CQC load library.
#ADHCNTRLFILE	ADH.V0A00.CONTROL	Change the default to an appropriate DSN HLQ for the IBM Guardium S-TAP for Db2 VSAM Control file.
#APPSRVR	appliance.company.com	Host name or IP address of the IBM Guardium system.

The following example shows the contents of the ADHEMAC1 member:

```
ISREDIT MACRO (NP)
ISPEXEC VGET (ZUSER)
ISREDIT CHANGE ALL '#SSID'          MYSSID
ISREDIT CHANGE ALL '#ADHOWNER'      &ZUSER
ISREDIT CHANGE ALL '#ADHUSERID'     &ZUSER
ISREDIT CHANGE ALL '#SADHLOAD'      ADH.IBMTAPE.SADHLOAD
ISREDIT CHANGE ALL '#SADHDBRM'      ADH.IBMTAPE.SADHDBRM
ISREDIT CHANGE ALL '#SDSNLOAD'      DSN.Vxxx.SDSNLOAD
ISREDIT CHANGE ALL '#SDSNRUNL'      DSNxxx.RUNLIB.LOAD
ISREDIT CHANGE ALL '#DSNTEP2'       DSNTEP2
ISREDIT CHANGE ALL 'ADHPLAN1'       ADHPLAN1
ISREDIT CHANGE ALL '#SZPARM'        MYSSIDPARM
ISREDIT CHANGE ALL '#SBSDS01'       MYSSID.BSDS01
ISREDIT CHANGE ALL '#SBSDS02'       MYSSID.BSDS02
ISREDIT CHANGE ALL '#SDSNEXIT'      DSN.Vxxx.SDSNEXIT
ISREDIT CHANGE ALL '#SFECLOAD'      FEC.IBMTAPE.SFECLOAD
ISREDIT CHANGE ALL '#SCQCLOAD'      CQC.IBMTAPE.SCQCLOAD
ISREDIT CHANGE ALL '#ADHCNTRLFILE' ADH.V0A00.CONTROL
ISREDIT CHANGE ALL '#APPSRVR'       appliance.company.com
```

Parent topic: Reference information

Related tasks

- Customizing JCL members

Messages and codes for IBM Security Guardium S-TAP for DB2 on z/OS

These topics document the messages and error codes issued by Security Guardium S-TAP for DB2. Messages are presented in ascending alphabetical and numerical order.

Parent topic: IBM Security Guardium S-TAP for Db2 on z/OS

Error messages

Security Guardium S-TAP for DB2 messages adhere to the following format: ADH*nnnx*

Where:

ADH
: Indicates that the message was issued by Security Guardium S-TAP for DB2.

nnn
: Indicates the message identification number.

x
: Indicates the severity of the message:

Table 1. Error message severity codes

Severity Code	Description
E	Indicates that an error occurred, which might or might not require operator intervention.
I	Indicates that the message is informational only.
S	Indicates that operator intervention is required before processing can continue.
W	Indicates that the message is a warning to alert you to a possible error condition.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for DB2 on z/OS

Error messages and codes: ADHAxxx

The following information is about error messages and codes that begin with ADHA.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for DB2 on z/OS

ADHA507E Callable service invocation failed with return code = *rc* and reason code = *rs*

Explanation

A callable service invocation failed with a return code and reason code that are identified in the message.

User response

Refer to the *IBM Db2 for z/OS®* product documentation for an explanation of this reason and return code.

Common causes of this error include:

Insufficient authorization to ADH PLAN specified in the control file
: If either of these issues are indicated by the reason code, verify that SAMPLIB member ADHGRANT was customized and submitted during configuration of the IBM® Guardium® S-TAP® for DB2® agent.

A DB2 Trace is currently running
: Issue the Db2® command -DISPLAY TRACE to view info about any audit traces that might still be running. If audit traces are running, stop them by using the Db2 command -STOP TRACE and then restart the agent. If this does not resolve the problem, check for the existence of additional messages.

If the problem is not resolved after attempting all user responses for existing additional messages, contact IBM Software Support.

Parent topic: Error messages and codes: ADHAxxx

Error messages and codes: ADHGxxx

The following information is about error messages and codes that begin with ADHG.

- **ADHG000I**
  Attempting connection to server *server-address* port=*server-port*
- **ADHG001I**
  Establishing ASC connection to server [*server-address*]
- **ADHG002I**
  Connection established to server [*server-address*]
- **ADHG003I**
  Connection re-established to [*server-address*]
- **ADHG004W**
  Connection was lost from server [*server-address*]
- **ADHG005S**
  Unable to establish a connection to a server [*server-address*]
- **ADHG006E**
  Data loss has occurred as the result of a network send failure
- **ADHG007E**
  Unable to create a communications interface
- **ADHG008S**
  Required parameter was not supplied. Parameter=*parameter-name*
- **ADHG009I**
  TCP/IP streaming disabled due to user setting.
- **ADHG010I**
  Disconnecting from server *server-name*
- **ADHG011E**
  Unable to create an output stream
- **ADHG012E**
  Unable to set socket timeout value. rc=*return-code* reason=*reason-code*
- **ADHG013I**
  Connection attempt timed out. Reattempting connection *reattempt-number* of *total-reattempts*
- **ADHG014I**
  Spillfile support enabled. Spill area size: [*size*] MB
- **ADHG015W**
  Primary server is unavailable
- **ADHG017W**
  Data is being temporarily stored in a spillfile until a connection is re-established
- **ADHG018I**
  Spillfile contents have been successfully be sent to server [*server*]
- **ADHG019S**
  Spillfile storage has been exhausted. Data loss will occur.
- **ADHG020I**
  Registering server [*server*] as eligible for failover.
- **ADHG021E**
  Spillfile is approaching [50% | 85% | 95% |100$] capacity.
- **ADHG022I**
  A connection has been established to failover server [*server*].
- **ADHG026W**
  Invalid port specified for APPLIANCE_PORT. Port 16022 will be used instead.
- **ADHG027I**
  Registering server *server* as eligible for multi-stream.
- **ADHG030I**
  Security Guardium S-TAP for DB2 Collector Agent is terminating
- **ADHG031I**
  Security Guardium S-TAP for DB2 V10.1.3 [*component*] connection established
- **ADHG097E**
  Unexpected error: [*error_description*]. Return code:[*return_code*].
- **ADHG098I**
  This event will be logged due to an unexpected data condition.
- **ADHG099E**
  Unexpected error: *error-condition*

- **ADHG210I**
  A thread termination request was received for thread [*thread-token*]
- **ADHG501E**
  pbSend: Bad host name. code=*error-code*
- **ADHG502E**
  pbSend: Interface not open. code= *error-code*
- **ADHG503E**
  pbSend: Socket I/O problem. code= *error-code*
- **ADHG550E**
  Unable to send message. Connection to server is unavailable.
- **ADHG510E**
  pbWrite: No such message. code= *error-code*
- **ADHG511E**
  pbWrite: Nested too deep. code= *error-code*
- **ADHG512E**
  pbWrite: Stack underflow. code= *error-code*
- **ADHG513E**
  pbWrite: Not in message. code= *error-code*
- **ADHG514E**
  pbWrite: No such field in message. code= *error-code*
- **ADHG515E**
  pbWrite: Not a 32-bit integer field. code= *error-code*
- **ADHG516E**
  pbWrite: Not implemented. code= *error-code*
- **ADHG517E**
  pbWrite: Not a message type. code= *error-code*
- **ADHG520W**
  Encoding exception: Event exceeds protocol message size limit. code=*error-code*
- **ADHG521W**
  Total encoding exceptions encountered due to exceeded message size: *exception-count*
- **ADHG522E**
  Write failed length=*length* rc=*returncode* rsn=*reasoncode*

Parent topic: Messages and codes for IBM Security Guardium S-TAP for DB2 on z/OS

ADHG000I Attempting connection to server *server-address* port=*server-port*

Explanation

The S-TAP® collector will attempt to establish a TCP/IP connection to a Guardium® system at the specified server address and port.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG001I Establishing ASC connection to server [*server-address*]

Explanation

The S-TAP® collector is preparing to establish the TCP/IP connection to the specified Guardium® system.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG002I Connection established to server [*server-address*]

Explanation

The S-TAP® collector was successful in establishing a TCP/IP connection to the Guardium® system.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG003I Connection re-established to [*server-address*]

Explanation

The S-TAP® collector was successful in re-establishing a TCP/IP connection to the Guardium® system following a disconnect.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG004W Connection was lost from server [*server-address*]

Explanation

The TCP/IP connection between the S-TAP® collector and the Guardium® system was lost. The S-TAP collector will automatically attempt to re-establish the connection, however a potential for data loss does exist if the connection is not re-established. A data loss condition is indicated by message ADHG006E.

User response

Determine the cause of the network interruption and correct the problem so that the connection can be re-established.
Parent topic: Error messages and codes: ADHGxxx

ADHG005S Unable to establish a connection to a server [*server-address*]

Explanation

The S-TAP® collector was unable to establish a TCP/IP connection to the Guardium® system.

User response

- Ensure that the Guardium system is listening for a connection at the server and port specified in message ADHG001I.
- Ensure that no firewalls are blocking connections between the collector and Guardium system.
- If port 16023 is used, ensure that AT-TLS has been configured properly between the z/OS® LPAR and the appliance.

Parent topic: Error messages and codes: ADHGxxx

ADHG006E Data loss has occurred as the result of a network send failure

Explanation

During a disconnected state, the S-TAP® collector exceeded the number of events to retain in memory while waiting for the network connection to the Guardium® system to be reestablished.

User response

- Determine the cause of the network interruption and correct the problem so that the connection can be reestablished.
- If deemed necessary, increase the SEND_FAIL_EVENT_COUNT value in the ASC ADHPARMS parameter file to increase the number of events that can be retained in memory during short outages.

Parent topic: Error messages and codes: ADHGxxx

ADHG007E Unable to create a communications interface

Explanation

An attempt to create an internal communications interface failed.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG008S Required parameter was not supplied. Parameter=*parameter-name*

Explanation

A required parameter was not supplied.

User response

Supply a parameter and value for the specified parameter.
Parent topic: Error messages and codes: ADHGxxx

ADHG009I TCP/IP streaming disabled due to user setting.

Explanation

A debug setting was specified that has disabled TCP/IP streaming between the S-TAP® collector and the Guardium® appliance.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG010I Disconnecting from server *server-name*

Explanation

The S-TAP® collector is disconnecting from the Guardium® system.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG011E Unable to create an output stream

Explanation

An attempt to create an internal output stream failed.

User response

Contact IBM® Customer Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG012E Unable to set socket timeout value. rc=*return-code* reason=*reason-code*

Explanation

An attempt to set the timeout threshold in the socket interface failed.

User response

Contact IBM® Customer Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG013I Connection attempt timed out. Reattempting connection *reattempt-number* of *total-reattempts*

Explanation

The S-TAP® collector agent was unable to establish a TCP/IP connection to the Guardium® system within the timeout period. The connection will be reattempted until the *reattempt-number* specified meets the *total-reattempts* number specified.

User response

- Ensure that the Guardium system is listening for a connection at the server and port specified in message ADHG001I.
- Ensure that there no firewalls are blocking connections between the collector and Guardium system.

Parent topic: Error messages and codes: ADHGxxx

ADHG014I Spillfile support enabled. Spill area size: [*size*] MB

Explanation

A spillfile area was successfully allocated at the specified size.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG015W Primary server is unavailable

Explanation

A connection to the primary Guardium® system is not available. Failover systems will be attempted for connection.

User response

Determine the cause of the connection interruption to the primary Guardium system and attempt to restore the connection.
Parent topic: Error messages and codes: ADHGxxx

ADHG017W Data is being temporarily stored in a spillfile until a connection is re-established

Explanation

A Guardium® system connection is unavailable. Collected data is written to the spillfile area until a system connection can be established.

User response

Determine the cause of the system connection outage and attempt to restore the connection.
Parent topic: Error messages and codes: ADHGxxx

ADHG018I Spillfile contents have been successfully be sent to server [*server*]

Explanation

The Guardium® system connection has been restored. The spillfile data that was collected during a connection outage has been sent to the specified system.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG019S Spillfile storage has been exhausted. Data loss will occur.

Explanation

A Guardium® system connection is unavailable and the spillfile is out of space. Data collected after this time will be lost.

User response

Determine the cause of the connection outage to the system and attempt to restore the connection. Notify others of the outage as necessary.
Parent topic: Error messages and codes: ADHGxxx

ADHG020I Registering server [*server*] as eligible for failover.

Explanation

The specified server will be added to the list of failover servers to register for the connection. Registration is attempted after all failover servers have been added. A successful failover registration is indicated by message ADHG012I.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG021E Spillfile is approaching [50% | 85% | 95% |100$] capacity.

Explanation

A Guardium® system connection is unavailable and the spillfile area is at the specified capacity.

User response

Determine the cause of the connection outage to the system and attempt to restore the connection.
Parent topic: Error messages and codes: ADHGxxx

ADHG022I A connection has been established to failover server [*server*].

Explanation

A connection to the primary Guardium® system is not available. A connection has successfully been established to one of the specified failover server.

User response

Determine the cause of the connection interruption to the primary system and attempt to restore the connection.
Parent topic: Error messages and codes: ADHGxxx

ADHG026W Invalid port specified for APPLIANCE_PORT. Port 16022 will be used instead.

Explanation

The APPLIANCE_PORT parameter currently supports a setting of 16022, but the parameter has been retained for future support. If APPLIANCE_PORT is specified with a value other than 16022, message ADHG026W is issued, and port 16022 will be used instead.

User response

Change APPLIANCE_PORT parameter setting to 16022 or remove the parameter entirely.
Parent topic: Error messages and codes: ADHGxxx

ADHG027I Registering server *server* as eligible for multi-stream.

Explanation

The specified server will be added to the list of servers that are eligible for multistream support.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG030I Security Guardium® S-TAP® for DB2® Collector Agent is terminating

Explanation

The collector is terminating.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG031I Security Guardium® S-TAP® for DB2® V10.1.3 [*component*] connection established

Explanation

The specified component successfully established a TCP/IP connection to the Guardium system.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG097E Unexpected error: [*error_description*]. Return code:[*return_code*].

Explanation

An unexpected error was encountered.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG098I This event will be logged due to an unexpected data condition.

Explanation

A collected event contained unexpected or invalid data fields. The event fields are written to DD:ADHLOG for use in diagnosing the problem.

User response

Contact IBM® Software Support with the error log.
Parent topic: Error messages and codes: ADHGxxx

ADHG099E Unexpected error: *error-condition*

Explanation

An unexpected error was encountered.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG210I A thread termination request was received for thread [*thread-token*]

Explanation

A –CANCEL THREAD command was issued by Security Guardium® S-TAP® for DB2® as a result of a request received by the Guardium system. The command ended successfully. *Thread-token* represents the cancelled thread token, as would be reported by a –DISPLAY THREAD DB2 command.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG501E pbSend: Bad host name. code=*error-code*

Explanation

While sending a message, the socket interface encountered a bad host name condition.

User response

- Verify that the host name value provided for APPLIANCE_SERVER in the ASC ADHPARMS parameter file is valid.
- Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHGxxx

ADHG502E pbSend: Interface not open. code= *error-code*

Explanation

While sending a message, a problem was encountered with an internal interface.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG503E pbSend: Socket I/O problem. code= *error-code*

Explanation

While sending a message, the socket interface encountered a socket I/O problem.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG550E Unable to send message. Connection to server is unavailable.

Explanation

An attempt to send a status (non-audit) message to the Guardium® system failed because a connection was unavailable.

User response

Determine the cause of the connection outage to the system and attempt to restore the connection.
Parent topic: Error messages and codes: ADHGxxx

ADHG510E pbWrite: No such message. code= *error-code*

Explanation

While building a message, a problem was encountered with an internal interface

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG511E pbWrite: Nested too deep. code= *error-code*

Explanation

While building a message, a problem was encountered with an internal interface.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG512E pbWrite: Stack underflow. code= *error-code*

Explanation

While building a message, a problem was encountered with an internal interface.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG513E pbWrite: Not in message. code= *error-code*

Explanation

While building a message, a problem was encountered with an internal interface.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG514E pbWrite: No such field in message. code= *error-code*

Explanation

While building a message, a problem was encountered with an internal interface.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG515E pbWrite: Not a 32-bit integer field. code= *error-code*

Explanation

While building a message, a problem was encountered with an internal interface.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG516E pbWrite: Not implemented. code= *error-code*

Explanation

While building a message, a problem was encountered with an internal interface.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG517E pbWrite: Not a message type. code= *error-code*

Explanation

While building a message, a problem was encountered with an internal interface.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG520W Encoding exception: Event exceeds protocol message size limit. code=*error-code*

Explanation

The network protocol used to communicate to the Guardium® system is limited to 64 KB in payload size. If an audited event results in a payload that exceeds this limit, this message is issued, and a truncated message is built and sent to the system. This message is only issued once per collector instance. At termination, message ADHG521W reports the total number of events impacted by this exception. The specified *error-code* value is for use by technical support.

User response

No action is required. If an excessive number of exceptions are observed, or if you are concerned that the exceptions are impacting audit data integrity, use APPLIANCE_PORT(16022), which uses a communications protocol capable of delivering events with larger payloads.
Parent topic: Error messages and codes: ADHGxxx

ADHG521W Total encoding exceptions encountered due to exceeded message size: *exception-count*

Explanation

The network protocol used to communicate to the Guardium® system is limited to 64 KB in payload size. If an audited event results in a payload that exceeds this limit, message ADHG520W is issued. At termination, this message reports the total number of events that have been impacted by this exception, displayed as *exception-count*.

User response

No action is required. If an excessive number of exceptions are observed, or if you are concerned that the exceptions are impacting audit data integrity, use APPLIANCE_PORT(16022), which uses a communications protocol capable of delivering events with larger payloads.
Parent topic: Error messages and codes: ADHGxxx

ADHG522E Write failed length=*length* rc=*returncode* rsn=*reasoncode*

Explanation

During an attempted TCP/IP data send of the length specified, the send failed with the specified return and reason code.

User response

Refer to the IBM manual, *z/OS UNIX System Services Messages and Codes*, for an explanation of the reason code. The last 4 digits of the reason code correspond to the errors of the send API. Also, review the ADHLOG of the S-TAP Collector Agent for other messages that might indicate problems with the connection between the S-TAP Collector Agent and the Guardium appliance.

This send failure might be the result of excessive amounts of data being sent to the appliance. Refer to the appliance reporting to determine whether excessive numbers of events were sent to the appliance prior to the send failure. If you determine the failure to be the result of excessive amounts of data, review and modify the active policy to decrease the amount of data that is sent to the appliance.

Parent topic: Error messages and codes: ADHGxxx

Error messages and codes: ADHIxxxx

The following information is about error messages and codes that begin with ADHI.

- **ADHI026W**
  Invalid port specified for APPLIANCE_PORT. Port 16022 will be used instead.
- **ADHI031I**
  Security Guardium S-TAP for DB2 V10.1.3 [component] connection established
- **ADHI530E**
  DB2 connection failed [*function*] SQLCODE=[*sqlcode*] RSN=[*reason-code*]

- **ADHI531W**
  Option STAP_UTILITY_TS_TO_TABLE(Y) is ignored due to a previous error
- **ADHI612E**
  Termination requested as the result of a previous error
- **ADHI613E**
  SQLCODE -805 encountered for plan name [*plan_name*]
- **ADHI697E**
  Unexpected error: [*error_description*]. Return code:[*return_code*]
- **ADHI699E**
  Unexpected error: [*error-condition*]

Parent topic: Messages and codes for IBM Security Guardium S-TAP for DB2 on z/OS

ADHI026W Invalid port specified for APPLIANCE_PORT. Port 16022 will be used instead.

Explanation

The APPLIANCE_PORT parameter currently supports a setting of 16022, but the parameter has been retained for future support. If APPLIANCE_PORT is specified with a value other than 16022, message ADHG026W is issued, and port 16022 will be used instead.

User response

Change APPLIANCE_PORT parameter setting to 16022 or remove the parameter entirely.
Parent topic: Error messages and codes: ADHIxxxx

ADHI031I Security Guardium® S-TAP® for DB2® V10.1.3 [component] connection established

Explanation

The specified component successfully established a TCP/IP connection to the Guardium system.

User response

None action is required.
Parent topic: Error messages and codes: ADHIxxxx

ADHI530E DB2® connection failed [*function*] SQLCODE=[*sqlcode*] RSN=[*reason-code*]

Explanation

A DB2 attachment facility error occurred.

User response

An error occurred while performing a DB2 attachment function. See the *IBM® DB2 for z/OS® Messages and Codes* manual for more information about the return and reason codes.
Parent topic: Error messages and codes: ADHIxxxx

ADHI531W Option STAP_UTILITY_TS_TO_TABLE(Y) is ignored due to a previous error

Explanation

The option STAP_UTILITY_TS_TO_TABLE was set to enable collection of expanded utility information. However, an error occurred when attempting to establish the DB2® connection, which is required for this feature. The option is disabled.

User response

Review ADHLOG for occurrences of message ADHG503E to determine the cause of the DB2 connection failure.
Parent topic: Error messages and codes: ADHIxxxx

ADHI612E Termination requested as the result of a previous error

Explanation

An unrecoverable error condition was encountered. A shutdown request will sent to the collector agent.

User response

Check the ADHLOG for prior errors and attempt to resolve any previous errors.
Parent topic: Error messages and codes: ADHIxxxx

ADHI613E SQLCODE -805 encountered for plan name [*plan_name*]

Explanation

A DB2® bind error -805 was encountered for the specified plan name.

User response

Run the ADHBIND job located in the SADHSAMP library.
Parent topic: Error messages and codes: ADHIxxxx

ADHI697E Unexpected error: [*error_description*]. Return code:[*return_code*]

Explanation

An unexpected error was encountered.

User response

Contact IBM® Support.
Parent topic: Error messages and codes: ADHIxxxx

ADHI699E Unexpected error: [*error-condition*]

Explanation

An unexpected error was encountered.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHIxxxx

Error messages and codes: ADHKxxxx

The following information is about error messages and codes that begin with ADHK.

- **ADHK001I**
  Scope expression received, len = *length of expression text*
- **ADHK002I**
  Starting Compilation...
- **ADHK004I**
  Constant Pool for routine: (at *memoryLocation*).
- **ADHK005W**
  Level *level* '*compilerMessage*'.
- **ADHK101I**
  Compiling filter. Flags1 *Flags*; Compile Trace *True/False*; Runtime Trace *RuntimeTraceFlag*; RuntimeTrace *RuntimeTraceValue*; Stage 1 Requested *True/False*.
- **ADHK102I**
  Rule Expression.
- **ADHK103I**
  Profile contained no filter information for this agent.
- **ADHK104I**
  Filter Compile Failed.
- **ADHK105I**
  Variable text
- **ADHK106I**
  Compiled filter requires *bytes* bytes of dynamic save area.
- **ADHK110I**
  Rule expression:
- **ADHK111I**
  Compiling filter. flags1 *flags1* trace=*trace* runtimeTraceFlag *runtimeTraceFlag* runtimeTrace *runtimeTrace*
- **ADHK203I**
  Stage one filtering was not enabled.
- **ADHK204I**
  Error while creating stage one filter.
- **ADHK205I**
  No valid stage one filter criteria found.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for DB2 on z/OS

ADHK001I Scope expression received, len = *length of expression text*

Explanation

The filter compiler has received a filter expression of length *length* and expression text of *expression Text*. Only the first line of the expression text is output with this message. Only issued when trace-filter is true.

User response

None required.
Parent topic: Error messages and codes: ADHKxxxx

ADHK002I Starting Compilation...

Explanation

The expression compiler is starting to compile the filter expression. Only issued when trace-filter is true.

User response

No action is required.
Parent topic: Error messages and codes: ADHKxxxx

ADHK004I Constant Pool for routine: (at *memoryLocation*).

Explanation

This is a debugging message that shows the memory location of an important data structure for the compiled filter. This line is followed by a hexadecimal printout of the contents of that memory. Only issued when trace-filter is true.

User response

No action is required.
Parent topic: Error messages and codes: ADHKxxxx

ADHK005W Level *level* '*compilerMessage*'.

Explanation

These are messages generated by the filter compiler if there is anything wrong with the generated filter expression. The compiled filter will not be used. The agent and/or collector will shut down.

User response

Contact IBM® Software Support. Provide the agent and/or collector logs along with the xml file for the active profile at the time the message was generated.
Parent topic: Error messages and codes: ADHKxxxx

ADHK101I Compiling filter. Flags1 *Flags*; Compile Trace *True/False*; Runtime Trace *RuntimeTraceFlag*; RuntimeTrace *RuntimeTraceValue*; Stage 1 Requested *True/False*.

Explanation

An informational message is issued whenever a new profile is about to be compiled into a compiled filter.

User response

No action is required.
Parent topic: Error messages and codes: ADHKxxxx

ADHK102I Rule Expression.

Explanation

The following lines show the filter expression that was generated from the profile.

User response

No response required.
Parent topic: Error messages and codes: ADHKxxxx

ADHK103I Profile contained no filter information for this agent.

Explanation

The currently active filter had nothing specified to be collected in the current context. For example, in the ASC started task, if the filter has no targets, or if none of the targets had any events checked, then there is nothing for the ASC started task to collect.

User response

No response is required, in general. However, if you had intended data to be collected, you may wish to review the active profile. If you believe the message is issued in error, contact IBM® Software Support.
Parent topic: Error messages and codes: ADHKxxxx

ADHK104I Filter Compile Failed.

Explanation

The expression that was generated from the currently active profile could not be compiled into a filter.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHKxxxx

ADHK105I *Variable text*

Explanation

This message has been issued from the filter compiler

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHKxxxx

ADHK106I Compiled filter requires *bytes* bytes of dynamic save area.

Explanation

The compiled filter needs a certain amount of filter working memory to be able to do filtering, and this message only appears if the amount of filter working memory allocated (8192 bytes) is insufficient. This is unusual, and indicates a very large and complicated profile.

User response

You can consider reducing the size of the profile through the use of wildcards. If that is not possible, contact IBM® Software Support.
Parent topic: Error messages and codes: ADHKxxxx

ADHK110I Rule expression:

Explanation

his message will be followed by a full, multi-line, display of the filter expression generated from the profile. This message is only printed if trace-filter is true.

User response

No action is required.
Parent topic: Error messages and codes: ADHKxxxx

ADHK111I Compiling filter. flags1 *flags1* trace=*trace* runtimeTraceFlag *runtimeTraceFlag* runtimeTrace *runtimeTrace*

Explanation

An informational message issued whenever a new profile is about to be compiled into a compiled filter.

User response

No action is required.
Parent topic: Error messages and codes: ADHKxxxx

ADHK203I Stage one filtering was not enabled.

Explanation

Stage 1 filtering must be enabled.

User response

To enable stage 1 filtering, enter `STAGE1_FILTER(Y)` in the ADHCPARMS DD.
Parent topic: Error messages and codes: ADHKxxxx

ADHK204I Error while creating stage one filter.

Explanation

A bug in the filtering code prevented the correct creation of a filter for stage 1. If the stage 2 filter compiled correctly, filtering proceeds successfully at a higher overhead.

User response

Contact IBM® Software Support with XML export of the profile, and the JES output that contained this message.
Parent topic: Error messages and codes: ADHKxxxx

ADHK205I No valid stage one filter criteria found.

Explanation

Stage 1 filtering is based on a subset of the profile fields. If one or more rules in the profiles do not include at least one of the profile fields, then stage 1 filtering might not apply.

User response

Review the filtering stages section of the User's Guide and adjust the profile accordingly.
Parent topic: Error messages and codes: ADHKxxxx

Error messages and codes: ADHPxxxx

The following information is about error messages and codes that begin with ADHP.

- **ADHP000I**
  Attempting connection to server *server-address* port=*server-port*
- **ADHP001I**
  Establishing Policy connection to server [*server-address*]
- **ADHP002I**
  Connection established to server [*server-address*]
- **ADHP003I**
  Connection was re-established to [*server name*]
- **ADHP004W**
  Connection was lost from server [*server-address*]
- **ADHP005S**
  Unable to establish a connection to server [*server-address*]
- **ADHP006E**
  Data loss has occurred as the result of a network send failure
- **ADHP007E**
  Unable to create a communications interface
- **ADHP008S**
  Required parameter was not supplied. Parameter=*parameter-name*
- **ADHP009I**
  TCP/IP streaming disabled due to user setting.
- **ADHP010I**
  Disconnecting from server *server-name*
- **ADHP012I**
  Failover support enabled
- **ADHP013I**
  Connection attempt timed out. Reattempting connection *reattempt-number* of *total-reattempts*.
- **ADHP015W**
  Primary server is unavailable
- **ADHP017W**
  Data is being temporarily stored in a spillfile until a connection is re-established
- **ADHP018I**
  Spillfile contents have been successfully be sent to server [*server*]
- **ADHP019S**
  Spillfile storage has been exhausted. Dataloss will occur
- **ADHP020I**
  Registering server [*server*] as eligible for failover
- **ADHP021E**
  Spillfile is approaching [50% | 85% | 95% |100%] capacity
- **ADHP022I**
  A connection has been established to failover server [server]

- **ADHP023I**
  A persisted policy from DD:ADHPLCY is being used.
- **ADHP026W**
  Invalid port specified for APPLIANCE_PORT. Port 16022 will be used instead.
- **ADHP028E**
  Required policy not available at initialization.
- **ADHP030I**
  Security Guardium S-TAP for DB2 Policy component is terminating
- **ADHP031I**
  Security Guardium S-TAP for DB2 V10.1.3 *component* connection established
- **ADHP093E**
  Policy discarded because all DB2 rules contain errors
- **ADHP094E**
  Policy discarded due to error
- **ADHP095E**
  error: rule discarded due to error
- **ADHP096E**
  rule error: *[error]*
- **ADHP097E**
  Unexpected error: [*error_description*]. Return code:[*return_code*]
- **ADHP099E**
  Unexpected error: *error-condition*
- **ADHP101W**
  Invalid value for filter. Reason: [*reason*]. Value: [*value*]
- **ADHP102E**
  Invalid value for sqlcode: [*_sqlcode_*]
- **ADHP110I**
  Security Guardium S-TAP for DB2 mode: *****
- **ADHP111I**
  STAP command [STAP MODIFY command]
- **ADHP120I**
  Installed Policy:
- **ADHP121I**
  [*policy segment*]
- **ADHP122I**
  Installed Quarantine:
- **ADHP123I**
  [*quarantine segment*]
- **ADHP124I**
  Installed Blocking:
- **ADHP125I**
  [*blocking segment*]
- **ADHP126I**
  STAP BLOCKING mode: [ENABLED|DISABLED|OPERATOR]
- **ADHP130I**
  Agent configuration:
- **ADHP131I**
  [*agent configuration segment*]
- **ADHP140I**
  Event Counts:
- **ADHP141I**
  [*event type*] [*total collected*]
- **ADHP142I**
  [*event type*] [*total collected*]
- **ADHP143I**
  [*event type*] [*total collected*]
- **ADHP144I**
  [*event type*] [*total collected*]
- **ADHP145I**
  [*event type*] [*total collected*]
- **ADHP146I**
  [*event type*] [*total collected*]
- **ADHP150I**
  Program levels:
- **ADHP151I**
  [*program level segment*]
- **ADHP160I**
  S-TAP allocation queue history:
- **ADHP161I**
  TimeStamp-------Queued----------Freed
- **ADHP162I**
  [*allocation queue segment*]
- **ADHP163I**
  S-TAP filter history:
- **ADHP164I**
  TimeStamp----Pass Stage 1-- ---Pass Stage2
- **ADHP165I**
  [*filter queue segment*]
- **ADHP166I**
  S-TAP IO history:

- **ADHP167I**
  TimeStamp--------Sent----------Bytes sent--------Write time
- **ADHP168I**
  [*filter queue segment*]
- **ADHP170I**
  Event count reported by the appliance at time: [*count*]
- **ADHP179E**
  Option [*option*] is invalid for STAP command
- **ADHP180I**
  [*policy* | *quarantine* | *blocking*] policy push detected.
- **ADHP183E**
  FORCE_LOG_LIMITED is enabled but APPLIANCE_PORT is not compatible.
- **ADHP182I**
  SUPPORT_FORCE_LOG_LIMITED is enabled.
- **ADHP183I**
  FORCE_LOG_LIMITED is not supported by the appliance.
- **ADHP184I**
  A pushed down [*policy* | *blocking* | *quarantine*] is in use.
- **ADHP185I**
  A [*policy* | *quarantine* | *blocking*] from DD is in use.
- **ADHP186I**
  A [*policy* | *quarantine* | *blocking*] from DD is in use, ignoring any pushed down policy.
- **ADHP188I**
  Blocking policy removed.
- **ADHP189W**
  There is no table found in database: [*database name*]
- **ADHP190W**
  DB2 object: [*object type*] with name: [*object name*] does not exist.
- **ADHP191W**
  Blocking is NOT ACTIVE because there is no valid target in the policy.
- **ADHP192E**
  SQL statement execution was unsuccessful, SQLCODE is: [*sqlcode value*] SQLSTATE is: [*sqlstate value*]
- **ADHP193I**
  STAP Logging command pushed down from UI to request STAP logging information.
- **ADHP200E**
  Unexpected element in policy definition: *<element>*
- **ADHP201E**
  A policy must contain at least one rule
- **ADHP203E**
  Duplicate schema specification: [*schema-name*]
- **ADHP204E**
  Duplicate table specification: [*table-name*]
- **ADHP205E**
  Duplicate First Read event specification.
- **ADHP206E**
  Duplicate First Change event specification.
- **ADHP207E**
  Expected <*policy*> specification but found <*****>.
- **ADHP208E**
  Policy syntax error
- **ADHP209E**
  Error in opening data set: [*dataset*]
- **ADHP210I**
  A thread termination request was received for thread [*thread ID*]
- **ADHP211W**
  Policy syntax error [*error*]
- **ADHP212W**
  [*policy* | *quarantine* | *blocking*] not enabled for ddname [*ddname*] reason: XML error
- **ADHP213E**
  Blocking policy syntax error: Invalid network [*network*]
- **ADHP214E**
  Blocking policy syntax error: Invalid netmask [*netmask*]
- **ADHP215E**
  Blocking policy syntax error: Invalid IP address [*IP address*]
- **ADHP216W**
  Blocking policy is ignored due to a previous error.
- **ADHP217W**
  Incomplete rule discarded. Rule name: [*_rule-name_*]
- **ADHP218W**
  Only one SQLCODE list is allowed. SQLCODE is discarded: [*sqlcode*]
- **ADHP220I**
  Appliance connect retry count has been reached, appliance ping rate is now increased to [*number*]
- **ADHP250E**
  Unable to send message. Connection to server is unavailable.
- **ADHP550E**
  Unable to send message. Connection to server is unavailable

Parent topic: Messages and codes for IBM Security Guardium S-TAP for DB2 on z/OS

ADHP000I Attempting connection to server *server-address* port=*server-port*

Explanation

The S-TAP® policy component will attempt to establish a TCP/IP connection to a Guardium® system at the specified server address and port.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP001I Establishing Policy connection to server [*server-address*]

Explanation

The Security Guardium® S-TAP® for DB2® policy component is preparing to establish the TCP/IP connection to the specified Guardium system.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP002I Connection established to server [*server-address*]

Explanation

The S-TAP® policy component was successful in establishing a TCP/IP connection to the Guardium® system.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP003I Connection was re-established to [*server name*]

Explanation

The S-TAP® policy component was successful in establishing a TCP/IP connection to the Guardium® system following a disconnect.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP004W Connection was lost from server [*server-address*]

Explanation

The TCP/IP connection between the S-TAP® policy component and the Guardium® system was lost. The S-TAP policy component will automatically attempt to reestablish the connection, however a potential for data loss exists if the connection is not established. A data loss condition is indicated by message ADHP006E.

User response

Determine the cause of the network interruption and correct the problem so that the connection can be established.
Parent topic: Error messages and codes: ADHPxxxx

ADHP005S Unable to establish a connection to server [*server-address*]

Explanation

The S-TAP® Policy component was unable to establish a TCP/IP connection to the Guardium® system.

User response

- Ensure that the Guardium system is listening for a connection at the server and port specified in message ADHP001I. .
- Ensure that there are no firewalls blocking connections between the collector and the Guardium system.

Parent topic: Error messages and codes: ADHPxxxx

ADHP006E Data loss has occurred as the result of a network send failure

Explanation

During a disconnection, the S-TAP® policy component exceeded the number of events that can be retained in memory while waiting for the network connection to the Guardium® system to be reestablished.

User response

- Determine the cause of the network interruption and correct the problem so that the connection can be established.
- If necessary, increase the SEND_FAIL_EVENT_COUNT value in the ASC ADHPARMS parameter file to increase the number of events that can be retained in memory during short outages.

Parent topic: Error messages and codes: ADHPxxxx

ADHP007E Unable to create a communications interface

Explanation

An attempt to create an internal communications interface failed.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHPxxxx

ADHP008S Required parameter was not supplied. Parameter=*parameter-name*

Explanation

A required parameter was not supplied.

User response

Supply a parameter and value for the specified parameter.
Parent topic: Error messages and codes: ADHPxxxx

ADHP009I TCP/IP streaming disabled due to user setting.

Explanation

A debug setting was specified that has disabled TCP/IP streaming between the S-TAP® policy component and the Guardium® system.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP010I Disconnecting from server *server-name*

Explanation

The S-TAP® policy component is disconnecting from the Guardium® system.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP012I Failover support enabled

Explanation

One or more failover servers were successfully registered with the communications interface, enabling failover support.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP013I Connection attempt timed out. Reattempting connection *reattempt-number* of *total-reattempts.*

Explanation

The S-TAP® policy component was unable to establish a TCP/IP connection to the Guardium® system within the timeout period. An attempt to be made to reestablish the connection until the *reattempt-number* reaches the *total-reattempts* number.

User response

- Ensure that the Guardium system is listening for a connection at the server and port specified in message ADHP001I.
- Ensure that no firewalls are blocking connections between the collector and Guardium system.

Parent topic: Error messages and codes: ADHPxxxx

ADHP015W Primary server is unavailable

Explanation

A connection to the primary Guardium® system is not available. Failover appliances will be attempted for connection.

User response

Determine the cause of the connection interruption to the primary system and attempt to restore the connection.
Parent topic: Error messages and codes: ADHPxxxx

ADHP017W Data is being temporarily stored in a spillfile until a connection is re-established

Explanation

A Guardium® system connection is unavailable and collected data is being written to the spillfile area until an system connection can be restored.

User response

Determine the cause of the connection outage to the system and attempt to restore the connection.
Parent topic: Error messages and codes: ADHPxxxx

ADHP018I Spillfile contents have been successfully be sent to server [*server*]

Explanation

The spillfile data that was collected during a connection outage has been sent to the specified Guardium® system upon reconnection.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP019S Spillfile storage has been exhausted. Dataloss will occur

Explanation

A Guardium® system connection is unavailable and the spillfile is out of space. Data collected after this time will be lost.

User response

Determine the cause of the connection outage to the system and attempt to restore the connection. Notify others of the outage as necessary.
Parent topic: Error messages and codes: ADHPxxxx

ADHP020I Registering server [*server*] as eligible for failover

Explanation

The specified server will be added to the list of failover servers to register for the connection. Registration is attempted after all failover servers have been added. A successful failover registration is indicated by message ADHP012I.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP021E Spillfile is approaching [50% | 85% | 95% |100%] capacity

Explanation

A Guardium® system connection is unavailable and the spillfile area has reached the specified percentage of capacity.

User response

Determine the cause of the connection outage to the system and attempt to restore the connection.
Parent topic: Error messages and codes: ADHPxxxx

ADHP022I A connection has been established to failover server [server]

Explanation

A connection to the primary Guardium® system is not available. A connection has successfully been established to one of the specified failover server.

User response

Determine the cause of the connection interruption to the primary system and attempt to restore the connection.
Parent topic: Error messages and codes: ADHPxxxx

ADHP023I A persisted policy from DD:ADHPLCY is being used.

Explanation

The S-TAP® policy component was unable to establish a connection to the Guardium® system. A persisted policy from DD:ADHPLCY is being used.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP026W Invalid port specified for APPLIANCE_PORT. Port 16022 will be used instead.

Explanation

The APPLIANCE_PORT parameter currently supports a setting of 16022, but the parameter has been retained for future support. If APPLIANCE_PORT is specified with a value other than 16022, message ADHG026W is issued, and port 16022 will be used instead.

User response

Change APPLIANCE_PORT parameter setting to 16022 or remove the parameter entirely.
Parent topic: Error messages and codes: ADHPxxxx

ADHP028E Required policy not available at initialization.

Explanation

At startup, the policy manager did not receive a policy from the Guardium appliance or policy DD.

User response

If APPLIANCE_SERVER_LIST is set to *FAILOVER*, this problem can be resolved by verifying that either:

- the primary server is active and a policy is installed, or
- the persistence policy DD is configured and has a valid policy installed from a previous policy.

IF APPLIANCE_SERVER_LIST is set to *MULTI_STREAM*, verify that the primary server is active during startup.
Parent topic: Error messages and codes: ADHPxxxx

ADHP030I Security Guardium® S-TAP® for DB2® Policy component is terminating

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP031I Security Guardium® S-TAP® for DB2® V10.1.3 *component* connection established

Explanation

The S-TAP Policy component successfully established a TCP/IP connection to the Guardium system.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP093E Policy discarded because all DB2® rules contain errors

Explanation

All of the DB2 collection profile interception policies that were pushed down from the Guardium® appliance contain errors. As a result, Security Guardium S-TAP® for DB2 collection is deactivated.

User response

Review the ADHLOG for messages that were issued prior to this message that indicate why the DB2 rules were discarded. Examples of relevant messages include ADHP096E and ADHP101W. Use the reason and value that is reported in the message to correct the incorrect value or error in the collection policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP094E Policy discarded due to error

Explanation

One or more errors were detected while processing an interception policy that was pushed down from the Guardium appliance. As a result, the entire policy, as well as any rules that are contained within the policy, are ignored.

User response

Review the ADHLOG for messages that were issued prior to this message (for example, ADHP101W) that indicate why the policy was discarded. Use the reason and value that is reported in the message to correct the incorrect value or error in the collection policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP095E error: rule discarded due to error

Explanation

One or more errors were detected while processing an interception policy rule that was pushed down from the Guardium appliance. As a result, the rule containing these errors is ignored.

User response

Review the ADHLOG for messages that were issued prior to this message that indicate why the rule was discarded. Examples of relevant messages include ADHP096E and ADHP101W. Use the reason and value that is reported in the message to correct the incorrect value or error in the collection policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP096E rule error: *[error]*

Explanation

An error was detected while processing an interception policy rule that was pushed down from the Guardium appliance.

User response

Use the error text that is provided in this message to correct the value or error in the collection policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP097E Unexpected error: [*error_description*]. Return code:[*return_code*]

Explanation

An unexpected error was encountered.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHPxxxx

ADHP099E Unexpected error: *error-condition*

Explanation

An unexpected error was encountered.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHPxxxx

ADHP101W Invalid value for filter. Reason: [*reason*]. Value: [*value*]

Explanation

An invalid value was detected while processing the collection policy received from the Guardium® system.

User response

Attempt to correct the invalid value or error in the collection policy by referencing the reason and value reported in the message.
Parent topic: Error messages and codes: ADHPxxxx

ADHP102E Invalid value for sqlcode: [*_sqlcode_*]

Explanation

A SQL code that was detected while processing the collection policy from the IBM® Guardium® system is not valid.

User response

Attempt to correct the SQL code in the collection policy by referencing the value that is reported in the message. See *SQL error codes* in the IBM Knowledge Center for more information.
Parent topic: Error messages and codes: ADHPxxxx

ADHP110I Security Guardium® S-TAP® for DB2® mode: *****

Explanation

This message is issued when information about the event streaming mode is requested by issuing the /F STAP command, where ***** is either *STREAMING EVENTS* or *POLICY SIMULATION*.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP111I STAP command [STAP MODIFY command]

Explanation

This message indicates that an S-TAP MODIFY command has been issued.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP120I Installed Policy:

Explanation

The header of the installed policy

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP121I [*policy segment*]

Explanation

A segment of the installed policy

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP122I Installed Quarantine:

Explanation

The header of the installed quarantine policy

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP123I [*quarantine segment*]

Explanation

A segment of the installed quarantine policy

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP124I Installed Blocking:

Explanation

The header of the installed blocking policy

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP125I [*blocking segment*]

Explanation

A segment of the installed blocking policy

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP126I STAP BLOCKING mode: [ENABLED|DISABLED|OPERATOR]

Explanation

This message indicates whether S-TAP blocking is enabled, disabled, or in operator mode.

User response

No action is required. See SQL Blocking for more information.
Parent topic: Error messages and codes: ADHPxxxx

ADHP130I Agent configuration:

Explanation

The header of the agent configuration

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP131I [*agent configuration segment*]

Explanation

A segment of the agent configuration

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP140I Event Counts:

Explanation

The header of the event collection statistics

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP141I [*event type*] [*total collected*]

Explanation

The total count collected for the event

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP142I [*event type*] [*total collected*]

Explanation

The total count collected for the event

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP143I [*event type*] [*total collected*]

Explanation

The total count collected for the event

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP144I [*event type*] [*total collected*]

Explanation

The total count collected for the event

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP145I [*event type*] [*total collected*]

Explanation

The total count collected for the event

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP146I [*event type*] [*total collected*]

Explanation

The total count collected for the event

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP150I Program levels:

Explanation

The header of S-TAP program levels

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP151I [*program level segment*]

Explanation

A segment of S-TAP program levels

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP160I S-TAP allocation queue history:

Explanation

The header of S-TAP allocation queue history

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP161I *TimeStamp-------Queued-----------Freed*

Explanation

The subheader of S-TAP allocation queue history

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP162I [*allocation queue segment*]

Explanation

A segment of the allocation queue history

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP163I S-TAP filter history:

Explanation

The header of S-TAP filter history

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP164I *TimeStamp----Pass Stage 1-- ---Pass Stage2*

Explanation

The subheader of the S-TAP filter history

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP165I [*filter queue segment*]

Explanation

A segment of S-TAP filter history

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP166I S-TAP IO history:

Explanation

The header of S-TAP IO history

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP167I *TimeStamp--------Sent----------Bytes sent--------Write time*

Explanation

The subheader of S-TAP IO history

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP168I [*filter queue segment*]

Explanation

A segment of S-TAP IO history

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP170I Event count reported by the appliance at time: [*count*]

Explanation

Number of collected events reported by the appliance.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP179E Option [*option*] is invalid for STAP command

Explanation

An invalid value was detected while processing the S-TAP command.

User response

Check the command and try again.
Parent topic: Error messages and codes: ADHPxxxx

ADHP180I [*policy* | *quarantine* | *blocking*] policy push detected.

Explanation

A policy pushdown from the Guardium appliance has been detected.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP183E FORCE_LOG_LIMITED is enabled but APPLIANCE_PORT is not compatible.

Explanation

The FORCE_LOG_LIMITED parameter is enabled but APPLIANCE_PORT is not set correctly.

User response

Check the compatible values for FORCE_LOG_LIMITED and APPLIANCE_PORT.
Parent topic: Error messages and codes: ADHPxxxx

ADHP182I SUPPORT_FORCE_LOG_LIMITED is enabled.

Explanation

The S-TAP has been configured not to collect host variables.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP183I FORCE_LOG_LIMITED is not supported by the appliance.

Explanation

The appliance does not support the FORCE_LOG_LIMITED feature.

User response

Check for the compatible appliance with which to use the FORCE_LOG_LIMITED feature.
Parent topic: Error messages and codes: ADHPxxxx

ADHP184I A pushed down [*policy* | *blocking* | *quarantine*] is in use.

Explanation

Policy push down is in use.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP185I A [*policy* | *quarantine* | *blocking*] from DD is in use.

Explanation

A policy supplied by DD is in use rather than one from push down.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP186I A [*policy* | *quarantine* | *blocking*] from DD is in use, ignoring any pushed down policy.

Explanation

A policy supplied by DD is in use. Any pushed down policy will be discarded.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP188I Blocking policy removed.

Explanation

All blocking policies have been uninstalled.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP189W There is no table found in database: [*database name*]

Explanation

The database [*database name*] that was specified in the blocking policy is either empty or not defined.

User response

Rebuild the blocking policy with a valid database for blocking to be active for the database.
Parent topic: Error messages and codes: ADHPxxxx

ADHP190W DB2 object: [*object type*] with name: [*object name*] does not exist.

Explanation

The DB2 object [*object type*] specified in the blocking policy does not exist.

User response

Rebuild the blocking policy with valid blocking targets for blocking to be active for the DB2 object.
Parent topic: Error messages and codes: ADHPxxxx

ADHP191W Blocking is NOT ACTIVE because there is no valid target in the policy.

Explanation

No valid blocking target has been found in the blocking policy. Blocking will not be activated.

User response

Rebuild the blocking policy with valid blocking targets for blocking to be activated.
Parent topic: Error messages and codes: ADHPxxxx

ADHP192E SQL statement execution was unsuccessful, SQLCODE is: [*sqlcode value*] SQLSTATE is: [*sqlstate value*]

Explanation

A SQL statement execution was unsuccessful during policy pushdown process.

User response

Determine the cause of the SQLCODE. Correct the installed policy if necessary.
Parent topic: Error messages and codes: ADHPxxxx

ADHP193I STAP Logging command pushed down from UI to request STAP logging information.

Explanation

S-TAP logging levels provide log information as follows:

Level 0
: Logs program levels, event queue statistics, agent configuration, policy, and event counts.

Level 1
: Logs agent configuration, policy, and event counts.

Level 2
: Logs agent configuration.

Level 3
: Logs policy.

Level 4 or higher
: Logs event counts.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP200E Unexpected element in policy definition: *<element>*

Explanation

An unexpected element has been found while parsing policy.

User response

Correct the unexpected element and update the policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP201E A policy must contain at least one rule

Explanation

No rule was found in the policy.

User response

Update the policy to contains at least one rule.
Parent topic: Error messages and codes: ADHPxxxx

ADHP203E Duplicate schema specification: [*schema-name*]

Explanation

A duplicated schema within one target has been detected.

User response

Update the policy with only one schema per target.
Parent topic: Error messages and codes: ADHPxxxx

ADHP204E Duplicate table specification: [*table-name*]

Explanation

A duplicate table within one target has been detected.

User response

Update the policy with only one table per target.
Parent topic: Error messages and codes: ADHPxxxx

ADHP205E Duplicate First Read event specification.

Explanation

A duplicate First Read event has been detected.

User response

Update the policy with only one First Read event per target.
Parent topic: Error messages and codes: ADHPxxxx

ADHP206E Duplicate First Change event specification.

Explanation

A duplicate First Change event has been detected.

User response

Update the policy with only one First Change event per target.
Parent topic: Error messages and codes: ADHPxxxx

ADHP207E Expected <*policy*> specification but found <***>.

Explanation

The <*policy*> tag was expected but a different tag (<***>) was found.

User response

Correct the policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP208E Policy syntax error

Explanation

A syntax error was found while parsing the policy.

User response

Correct the policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP209E Error in opening data set: [*dataset*]

Explanation

An error occurred while opening a data set for policy parsing.

User response

Make sure the dataset exists and is associated with the appropriate permissions.
Parent topic: Error messages and codes: ADHPxxxx

ADHP210I A thread termination request was received for thread [*thread ID*]

Explanation

A termination request was received for thread [*thread ID*].

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP211W Policy syntax error [*error*]

Explanation

A syntax error was found while parsing the policy.

User response

Correct the policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP212W [*policy* | *quarantine* | *blocking*] not enabled for ddname [*ddname*] reason: XML error

Explanation

The policy from DD is not enabled because a syntax error was found.

User response

Correct the policy in the DD.
Parent topic: Error messages and codes: ADHPxxxx

ADHP213E Blocking policy syntax error: Invalid network [*network*]

Explanation

Network value is not valid in the installed blocking policy.

User response

Correct the network value and reinstall the blocking policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP214E Blocking policy syntax error: Invalid netmask [*netmask*]

Explanation

Netmask value is not valid in the installed blocking policy.

User response

Correct the netmask value and reinstall the blocking policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP215E Blocking policy syntax error: Invalid IP address [*IP address*]

Explanation

IP address value is not valid in the blocking policy.

User response

Correct the IP address value and reinstall the blocking policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP216W Blocking policy is ignored due to a previous error.

Explanation

The installed blocking policy contains a syntax error. The blocking policy is discarded.

User response

Resolve the error and reinstall the blocking policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP217W Incomplete rule discarded. Rule name: [_*rule-name*_]

Explanation

An incomplete policy rule is detected.

System action

The rule is discarded.

User response

Use the Guardium Policy Builder of the Guardium® appliance interface to define and manage data collection and filtering. Correct the specified rule *rule-name* and add the necessary filters to make it a complete rule.
Parent topic: Error messages and codes: ADHPxxxx

ADHP218W Only one SQLCODE list is allowed. SQLCODE is discarded: [*sqlcode*]

Explanation

More than one SQLCODE list is detected.

System action

The first list is accepted. Additional lists are discarded.

User response

Ensure that there is only one SQLCODE list for each installed policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP220I Appliance connect retry count has been reached, appliance ping rate is now increased to [*number*]

Explanation

Ping rate has been increased to a larger value after reaching the specified number of APPLIANCE_CONNECT_RETRY_COUNT attempts.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP250E Unable to send message. Connection to server is unavailable.

Explanation

S-TAP was unable to send messages to the appliance.

User response

Make sure the appliance is online and reachable by the S-TAP.
Parent topic: Error messages and codes: ADHPxxxx

ADHP550E Unable to send message. Connection to server is unavailable

Explanation

An attempt to send a non-audit status message to the Guardium® system failed because no connection to the appliance is available.

User response

Determine the cause of the connection outage to the system and attempt to restore the connection.
Parent topic: Error messages and codes: ADHPxxxx

Error messages and codes: ADHQxxxx

The following information is about error messages and codes that begin with ADHQ. These messages are generated from the collector agent.

- **ADHQ1000E**
  NOT APF AUTHORIZED
- **ADHQ1001I**
  DB2 QUERY COMMON COLLECTOR INITIALIZATION IN PROGRESS FOR SUBSYSTEM
- **ADHQ1002I**
  DB2 AUDIT SQL COLLECTOR INITIALIZATION COMPLETE FOR SUBSYSTEM
- **ADHQ1003E**
  SUBSYSTEM *ssid* ALREADY ACTIVE
- **ADHQ1004I**
  QUERY COMMOON COLLECTOR TERMINATION IN PROGRESS FOR SUBSYSTEM *subsystem*
- **ADHQ1005I**
  QUERY COMMON COLLECTOR TERMINATION COMPLETE FOR SUBSYSTEM *ssid*
- **ADHQ1006E**
  statement DD STATEMENT MISSING
- **ADHQ1007E**
  INVALID USERID SPECIFIED FOR AUTHID
- **ADHQ1010I**
  DEBUG MODE ON
- **ADHQ1011I**
  DEBUG MODE OFF
- **ADHQ1016E**
  INVALID COMMAND SYNTAX
- **ADHQ1017E**
  INVALID COMMAND
- **ADHQ1019I**
  INTERVAL EXTERNALIZATION MODE OFF
- **ADHQ1020E**
  DB2 SUBSYSTEM *ssid* IS NOT DEFINED
- **ADHQ1024E**
  dsn SPECIFICATION INVALID
- **ADHQ1026E**
  SHARED MEMORY FAILURE FOR OBJECT *object request* RC =*rc* RS=*rs*
- **ADHQ1027I**
  CPU=*CPU Type-CPU Model-CPU Manufacturer*. *OS Name OS Version.OS Release.OS Modification*.
- **ADHQ1028E**
  Component requires a 64 bit processor and z/OS® 1.5 or higher.
- **ADHQ1031E**
  Serious error in master address space *address space*.
- **ADHQ1032I**
  Recreating master address space.
- **ADHQ1033E**
  Unable to create master address space *address space*.
- **ADHQ1034I**
  Master address space has started.
- **ADHQ1035E**
  Unable to restart master (RS=rc).
- **ADHQ1055E**
  CQM1055E DB2 ssid IS EXPERIENCING STORAGE CONSTRAINTS, DATA LOSS MAY OCCUR, REASON=code
- **ADHQ1060I**
  ZIIP SUPPORT IS NOT ACTIVE. *nnnnnnnn* RC=*yy* RSN=*zzzzzzzz nnnnnnnn* is the name of the service that failed with a nonzero return code (RC).
- **ADHQ1061E**
  MISSING PARAMETER: *parameter*
- **ADHQ1062E**
  COMMUNICATION INTERFACE DISABLED BY CROSS MEMORY FAILURE
- **ADHQ1062I**
  ZIIP SUPPORT IS INSTALLED
- **ADHQ1065E**
  REQUIRED DATA ACCESS COMMON COLLECTOR MODULE NOT FOUND
- **ADHQ1066E**
  Subsystem terminating due to abend while compiling the collection profile. SVCDUMP collected.
- **ADHQ1070E**
  Terminating due to XML profile processing error RC (xxxxxxxx)
- **ADHQ1071E**
  Terminating due to missing XML profile at start up
- **ADHQ1080I**
  POLICY MANAGER STARTED.
- **ADHQ1081I**
  POLICY MANAGER STOPPED.
- **POLICY PUSH DETECTED.**
- **ADHQ1083I**
  POLICY PUSH SENT.
- **ADHQ1084I**
  QUARANTINE ONLY POLICY DETECTED.
- **ADHQ1085I**
  CURRENT QUARANTINE POLICY IS REMOVED.
- **ADHQ1086I**
  BOTH NEW POLICY AND QUARANTINE POLICY DETECTED.

- **ADHQ1086E**
  ADHQ1086E *statement* DD STATEMENT MISSING
- **ADHQ1153E**
  RETURN CODE *return_code* REASON CODE *reason_code* WAS ENCOUNTERED DURING TRANSLATION SOURCE CCSID *ccsid* TARGET CCSID *ccsid*
- **ADHQ1202I**
  STORAGE CONSTRAINT RELIEVED FOR SPACE – *space* – OCCURRENCES: *count*
- **ADHQ1203I**
  ASID=*asid*,TCB=*tcb*,CPID=*cpid*, MODULE=*module*,ADDR=*addr*, RC=*rc*,RSN=*rsn*
- **ADHQ1204I**
  FUNC=*func*,SP=*subpool*,FLG2=*flag*,FLG3=*flag*
- **ADHQ1205E**
  ISM ERROR OCCURRED, DETAIL FOLLOWS: *note*
- **ADHQ1209I**
  ISM ERROR RC=*rc*,RSN=*rsn*,SPACE – *space*
- **ADHQ1210E**
  ISM SPACE IS DISABLED – space
- **ADHQ1211I**
  AN ABEND OCCURRED DURING ISM PROCESSING FOR SPACE – *space*
- **ADHQ1212E**
  AN ERROR OCCURRED IN THE EXTENT EXIT ROUTINE FOR SPACE – *space*
- **ADHQ1213W**
  SPACE IS FULL AND NO MORE EXTENTS CAN BE OBTAINED FOR SPACE – space
- **ADHQ1214W**
  OWNER LIMIT EXCEEDED FOR SPACE – *space*
- **ADHQ1215W**
  SPACE IS FULL AND NO MORE LARGE EXTENTS CAN BE OBTAINED FOR SPACE – *space*
- **ADHQ1216E**
  EXTENT PROCESSING FAILED (ABEND) FOR SPACE – *space*
- **ADHQ1217W**
  SPACE IS FULL AND NO MORE LARGE EXTENTS CAN BE OBTAINED FOR SPACE – *space*
- **ADHQ1218W**
  MAXIMUM EXTENTS HAS BEEN REACHED FOR SPACE – *space*
- **ADHQ1219W**
  ALL ISMERROR MESSAGE BLOCKS ARE IN USE
- **ADHQ1500E**
  ABNORMAL EOT FOR *subtask* SUBTASK
- **ADHQ2001E**
  DB2 SUBSYSTEM *ssid* ALREADY MONITORED BY SUBSYSTEM *ssid*
- **ADHQ2002E**
  MONITORING AGENT INSTALLATION FAILED FOR SUBSYSTEM *ssid*
- **ADHQ2003I**
  FORCING MONITORING AGENT INSTALLATION FOR *ssid*
- **ADHQ2005I**
  MULTIPLE MONITORING AGENT INSTALLATION FOR SUBSYSTEM *ssid*
- **ADHQ2008E**
  DB2 SYSTEM *ssid* IS BEING MONITORED BY A 2.2 OR BELOW VERSION CQM SUBSYSTEM AND CANNOT BE AUDITED
- **ADHQ2009E**
  DB2 SYSTEM ssid WAS PREVIOUSLY MONITORED BY A 2.2 OR EARLIER CQM SUBSYSTEM qmid WHICH HAS NOT APPLIED APAR PK55535.
- **ADHQ2010I**
  CURRENTLY ACTIVE POLICY RESULTS IN DISABLED COLLECTION
- **ADHQ2013I**
  CURRENTLY ACTIVE POLICY RESULTS IN GRANT/REVOKE COLLECTION
- **ADHQ2014I**
  CURRENTLY ACTIVE POLICY RESULTS NO HOST VARIABLE COLLECTION.
- **ADHQ2015I**
  CURRENTLY ACTIVE POLICY RESULTS NEGATIVE SQL CODES COLLECTION.
- **ADHQ2016I**
  CURRENTLY ACTIVE POLICY RESULTS DB2 COMMANDS COLLECTION.
- **ADHQ2017I**
  CURRENTLY ACTIVE POLICY RESULTS IN DBNAMES OPTIMIZATION.
- **ADHQ2018I**
  CURRENTLY ACTIVE POLICY RESULTS IN A QUARANTINE LIST.
- **ADHQ2019I**
  CURRENTLY ACTIVE POLICY RESULTS IN DB2 UTILITIES COLLECTION
- **ADHQ2020I**
  CURRENTLY ACTIVE POLICY RESULTS IN FAILED LOGIN COLLECTION.
- **ADHQ2100E**
  UNRECOGNIZED PARAMETER
- **ADHQ2101E**
  PARAMETER ERROR DETECTED FOR *parameter*
- **ADHQ2103E**
  DUPLICATE PARAMETER DETECTED FOR *parameter*
- **ADHQ2110E**
  TERMINATING DUE TO ERRORS IN PARAMETER FILE
- **ADHQ2111E**
  ERROR READING PARAMETER DATASET - MEMBER NOT FOUND
- **ADHQ2402I**
  DATASPACE MANAGEMENT IN PROGRESS FOR *dsmgmt*
- **ADHQ2403I**
  n DATASPACE PAGES RELEASED FOR *ssid*

- **ADHQ2408E**
  INVALID REPLY. REPLY "U" TO ACCEPT OR "R" TO REJECT
- **ADHQ2601E**
  ALLOCATION FAILED FOR VSAM DATASET *dsn* RETCD=*rc* REAS=*rs*
- **ADHQ2603E**
  DEALLOCATION FAILED FOR DATASET *data_set* RETCD=*return_code* REAS=*reason_code*
- **ADHQ3001I**
  DB2 STARTUP DETECTED FOR SUBSYSTEM *ssid*
- **ADHQ3002I**
  MONITORING AGENT STARTED FOR SUBSYSTEM *ssid*
- **ADHQ3003I**
  DB2 SHUTDOWN DETECTED FOR SUBSYSTEM *ssid*
- **ADHQ3005I**
  MONITORING AGENT DEACTIVATED FOR *ssid*
- **ADHQ3006I**
  AUDITING AGENT ACTIVATED FOR *ssid*
- **ADHQ3192E**
  LEVEL STATUS DB2(ssid) message
- **ADHQ3192I**
  LEVEL STATUS DB2(ssid) message
- **ADHQ3200I**
  DISPLAY AGENTS
- **ADHQ3201I**
  DB2 SUBYSYSTEM *ssid* AGENT ADDRESS *address*
- **ADHQ3202I**
  ssid AGENT ADDRESS *address*
- **ADHQ3203I**
  ASC DIAGNOSTIC DISPLAY:
- **ADHQ3204I**
  SDA ADDRESS *address*
- **ADHQ3205I**
  ssid ADDRESS *address*
- **ADHQ3206I**
  DIAGNOSTIC DATA FOR ABEND AT PSW *psw*
- **ADHQ3207I**
  SYSTEM COMPLETION CODE *code*
- **ADHQ3208I**
  OCCURRENCES *n* DATE *date* TIME *time*
- **ADHQ3209I**
  GPR 0-3 *info*
- **ADHQ3210I**
  GPR 4-7 *info*
- **ADHQ3211I**
  GPR 8-11 *info*
- **ADHQ3212I**
  GPR 12-15 *info*
- **ADHQ3213I**
  AR 0-3 *info*
- **ADHQ3214I**
  AR 4-7 *info*
- **ADHQ3215I**
  AR 8-11 *info*
- **ADHQ3216I**
  AR 12-15 *info*
- **ADHQ3240I**
  DB2 QM DATASPACE USAGE DISPLAY:
- **ADHQ3241I**
  dataspace DATASPACE
- **ADHQ3242I**
  NODE SIZE *size*
- **ADHQ3243I**
  TOTAL NODES *n*
- **ADHQ3244I**
  AVAILABLE NODES *n*
- **ADHQ3245I**
  PERCENT UTILIZED *n*
- **ADHQ3250I**
  POSTING INTERVAL PROCESSOR
- **ADHQ3251I**
  INTERVAL PROCESSOR NOT POSTED - DB2 UNAVAILABLE
- **ADHQ3252I**
  INTERVAL PROCESSING ALREADY IN PROGRESS
- **ADHQ3308E**
  DB2 SYSTEM ssid IS MONITORED BY DB2 QUERY MONITOR ssid WHICH HAS MISMATCHED OBJ AGENT
- **ADHQ3315E**
  MASTER SUBSYSTEM DOES NOT MATCH
- **ADHQ3402I**
  ISSUING COMMAND *cmd*
- **ADHQ3551E**
  VSAM LOGIC ERROR ENCOUNTERED WHILE ACCESSING CONTROL FILE FOR DB2 *ssid*. VSAMRC='*rc*' VSAMRS=X'*rs*'

- **ADHQ3552E**
  SETUP INFORMATION MISSING FROM CONTROL FILE FOR DB2 *ssid*
- **ADHQ3553E**
  message ERROR *message*
- **ADHQ4001E**
  CONNECT TO DB2 *ssid* FAILED FOR PLAN *plan* RETURN CODE *rc* REASON CODE *rs*
- **ADHQ4003E**
  CONNECT FAILED - DB2 NOT OPERATIONAL
- **ADHQ5010I**
  MONITORING AGENT DEINSTALLATION IN PROGRESS FOR SUBSYSTEM *ssid*
- **ADHQ5011I**
  MONITORING AGENT DEINSTALLATION COMPLETE FOR SUBSYSTEM *ssid*
- **ADHQ5012I**
  REQURESTING MONITORING AGENT ACTIVATION FOR DB2 SUBSYSTEM *ssid*
- **ADHQ5013I**
  REQUESTING MONITORING AGENT DEACTIVATION FOR DB2 SUBSYSTEM *ssid*
- **ADHQ6101E**
  LOCATE FAILED FOR *dataset* R0=*code* RC=*rc*
- **ADHQ6102E**
  SCRATCH FAILED FOR *file* SCRATCH STATUS CODE=*code* RO=*ro*
- **ADHQ7001E**
  table TABLE NOT LOCATED IN DB2 CATALOG
- **ADHQ7008E**
  QUERY COMMON COLLECTOR *ssid* NOT VALID OR HAS NOT BEEN STARTED SINCE IPL
- **ADHQ7009E**
  OUT OF SPACE CONDITION DETECTED WHILE WRITING TO THE *dsn* DATASET
- **ADHQ7010E**
  MISSING "ADD" PARAMETER FOR *parameter* AT LINE *line* COLUMN *column*
- **ADHQ7011E**
  INTERNAL ERROR - UNABLE TO RESOLVE ALTERNATE COLUMN *column*
- **ADHQ7015E**
  NUMBER OF BSDS SPECIFICATIONS INVALID OR MISSING
- **ADHQ7016E**
  DUPLICATE RECORD STORE ATTEMPTED FOR DB2 SUBSYSTEM *ssid*
- **ADHQ8001E**
  ERRORS DETECTED IN *parameters* PARAMETERS:
- **ADHQ8002E**
  UNIDENTIFIED KEYWORD DETECTED AT LINE *line* COLUMN *column*
- **ADHQ8003E**
  INVALID SYNTAX SPECIFIED FOR *parameter* NEAR LINE *line* COLUMN *column*
- **ADHQ8004E**
  PARAMETER LENGTH EXCEEDED FOR *parameter* NEAR LINE *line* COLUMN *column*
- **ADHQ8005E**
  PARAMETER MISSING FOR *parameter* NEAR LINE *line* COLUMN *column*
- **ADHQ8006E**
  NON NUMERIC DATA SPECIFIED FOR *parameter* NEAR LINE *line* COLUMN *column*
- **ADHQ8007E**
  INVALID VALUE SPECIFIED FOR *parameter* NEAR LINE *line* COLUMN *column*
- **ADHQ8008E**
  value MUST BE *value* THAN *value*
- **ADHQ8009E**
  DUPLICATE PARAMETER *parameter* AT LINE *line* COLUMN *column*
- **ADHQ8010E**
  DUPLICATE SUBPARAMETER DETECTED FOR PARAMETER *parameter* AT LINE *line* COLUMN *column*
- **ADHQ8011E**
  DB2 VERSION NOT SUPPORTED
- **ADHQ8012E**
  ERROR OPENING DDNAME *ddname*
- **ADHQ8013E**
  INVALID PARAMETER LENGTH FOR *parameter*
- **ADHQ8014E**
  LOGIC ERROR: *error*
- **ADH8022I**
  adh parameter value
- **ADH9899I**
  adh modify command

Parent topic: Messages and codes for IBM Security Guardium S-TAP for DB2 on z/OS

ADHQ1000E NOT APF AUTHORIZED

Explanation

The collector agent started task or job is not APF authorized.

User response

The collector agent requires that the target load libraries be APF-authorized.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1001I DB2® QUERY COMMON COLLECTOR INITIALIZATION IN PROGRESS FOR SUBSYSTEM

Explanation

This message appears during the normal initialization process of the collector agent.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1002I DB2® AUDIT SQL COLLECTOR INITIALIZATION COMPLETE FOR SUBSYSTEM

Explanation

This message appears during the normal initialization process of the collector agent and confirms the initialization process has completed.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1003E SUBSYSTEM *ssid* ALREADY ACTIVE

Explanation

The collector agent indicated in the message is already active and can therefore cannot process another activate command.

User response

Verify that you are activating the correct system. If you are attempting to activate a subsystem that is already active, do not attempt activation.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1004I QUERY COMMOON COLLECTOR TERMINATION IN PROGRESS FOR SUBSYSTEM *subsystem*

Explanation

This message appears during normal shutdown of the Collector Agent and indicates the collector is undergoing shutdown.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1005I QUERY COMMON COLLECTOR TERMINATION COMPLETE FOR SUBSYSTEM *ssid*

Explanation

The collector agent subsystem has been terminated. This message could appear as part of normal shutdown or as a failure to connect to a subsystem.

User response

Investigate other write-to-operator (WTO) messages preceding this one to determine the reason for the termination.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1006E *statement* DD STATEMENT MISSING

Explanation

The parameter DD statement (for example, ADHCFGP DD statement) is missing from the JCL for the collector agent started task.

User response

Create the necessary DD statement and code the appropriate parameters in the data set.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1007E INVALID USERID SPECIFIED FOR AUTHID

Explanation

The user ID entered in the AUTHID parm in the ADHCFGP data set has not been defined to RACF® or an equivalent security system.

User response

Correct the user ID, or ensure the ID is defined to your security system.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1010I DEBUG MODE ON

Explanation

Debugging mode has been turned on.

User response

None required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1011I DEBUG MODE OFF

Explanation

Debugging mode has been turned off.

User response

None required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1016E INVALID COMMAND SYNTAX

Explanation

The command syntax is invalid.

User response

Correct the command.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1017E INVALID COMMAND

Explanation

An invalid MVS™ Modify command was issued.

User response

Correct the command and execute it again.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1019I INTERVAL EXTERNALIZATION MODE OFF

Explanation

The collector agent subsystem was started with externalization mode set to off.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1020E DB2® SUBSYSTEM *ssid* IS NOT DEFINED

Explanation

The DB2 subsystem indicated in the message is not defined.

User response

Verify that you have specified the correct DB2 subsystem.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1024E *dsn* SPECIFICATION INVALID

Explanation

The data set name listed in this message is not valid.

User response

Verify that you specified the correct data set name in ADHCFGP.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1026E SHARED MEMORY FAILURE FOR OBJECT *object request* RC =*rc* RS=*rs*

Explanation

A shared memory failure has occurred for the indicated object.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1027I CPU=*CPU Type-CPU Model-CPU Manufacturer. OS Name OS Version.OS Release.OS Modification*.

Explanation

This message displays information about the CPU and the operating system.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1028E Component requires a 64 bit processor and z/OS® 1.5 or higher.

Explanation

Your system does not meet the minimum system requirements.

User response

Upgrade to the minimum requirements.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1031E Serious error in master address space *address space*.

Explanation

A serious error has occurred in the master address space specified.

User response

Verify that the master address space is available.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1032I Recreating master address space.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1033E Unable to create master address space *address space*.

Explanation

DB2® Query Monitor is not able to create the master address space specified.

User response

Many issues that cause this error relate to security setup. If you encounter this message, send your console log to IBM® Software Support.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1034I Master address space has started.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1035E Unable to restart master (RS=rc).

Explanation

The master address space could not be restarted.

User response

verify the master address space is available and restart.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1055E CQM1055E DB2® ssid IS EXPERIENCING STORAGE CONSTRAINTS, DATA LOSS MAY OCCUR, REASON=code

Explanation

The DB2 subsystem indicated in the message is experiencing storage constraints.

User response

Verify that your DB2 subsystem has the needed storage allocations.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1060I ZIIP SUPPORT IS NOT ACTIVE. *nnnnnnnn* RC=*yy* RSN=*zzzzzzzz nnnnnnnn* is the name of the service that failed with a nonzero return code (RC).

Explanation

Table 1. Return code explanations

Service	Description
IWM4ECRE (WLM Enclave Create)	The return codes and reason codes are documented in *z/OS V1R10.0 MVS™ Programming Workload Management Services*.
IWM4EoCT (WLM CPU Offload Time Service)	The return codes and reason codes are not documented in any existing WLM manual. However, RC=4 typically means no ZIIP is configured on the instance of z/OS®. If you have a ZIIP processor and it is properly configured, report the RC to the vendor.
MAXWFLOAD (Enclave SRB load service)	An error occurred trying to LOAD ADHMAXWF (the enclave SRB routine that runs on the ZIIP). Make sure you have the correct STEPLIB configured.
IEAVAPE (Z/OS Allocate Pause Element)	These return codes are described in *z/OS V1R10.0 MVS Programming Assembler Services References V2*. If the ADHQ1060I has IEAVAPE has the failing service, contact the vendor for resolution.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1061E MISSING PARAMETER: *parameter*

Explanation

The specified parameter has not been defined in the sample library member ADHCFGP.

User response

Add the missing parameter to the ADHCFGP sample library member.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1062E COMMUNICATION INTERFACE DISABLED BY CROSS MEMORY FAILURE

Explanation

A cross memory failure has occurred and as a result the communication interface has been disabled.

User response

Troubleshoot the memory failure and restart the ASC.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1062I ZIIP SUPPORT IS INSTALLED

Explanation

The collector agent has detected that WLM is configured for zIIP support. This does not necessarily indicate that zIIP processors are installed or are available for zIIP offload of collector agent processing.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1065E REQUIRED DATA ACCESS COMMON COLLECTOR MODULE NOT FOUND

Explanation

The started task did not find the Data Access Common Collector (CQC) initialization module, which prevented successful startup.

User response

Verify that the Data Access Common Collector (CQC) has been installed and that the load library is included in the started task STEPLIB concatenation
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1066E Subsystem terminating due to abend while compiling the collection profile. SVCDUMP collected.

Explanation

An abend was detected when compiling the collection profile. A memory dump was collected to gather the diagnostic information.

User response

If you are unable to take corrective measures to resolve the abend, then the SVCDUMP, the collector joblog, and the details of the collection profile in use should be reported to IBM® Software Support for resolution of this error.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1070E Terminating due to XML profile processing error RC (xxxxxxxx)

Explanation

A policy is sent from the Guardium® system to the Security Guardium S-TAP® for DB2® collector agent during their initial communication. If the policy received by the collector agent is not composed of valid XML syntax, the collector terminates.

User response

Verify that the Guardium system is properly configured, using the APPLIANCE_SERVER parameter. The system should be set up to accept connections from collectors. If the problem persists, contact IBM® Software Support with the return code specified in this message.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1071E Terminating due to missing XML profile at start up

Explanation

A policy is sent from the Guardium® system to the Security Guardium S-TAP® for DB2® collector agent during their initial communication. If the policy is not received by the collector agent during the initial communication set up, then the collector terminates.

User response

Verify that the Guardium system is properly configured, using the APPLIANCE_SERVER parameter. The appliance should be set up to accept connections from collectors. If the problem persists, contact IBM® Software Support.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1080I POLICY MANAGER STARTED.

Explanation

The internal policy manager task has started.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1081I POLICY MANAGER STOPPED.

Explanation

The internal policy manager task has stopped.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

POLICY PUSH DETECTED.

Explanation

A policy was received from the appliance.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1083I POLICY PUSH SENT.

Explanation

The policy was sent to Audit SQL Collector.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1084I QUARANTINE ONLY POLICY DETECTED.

Explanation

A pushed policy was included on a quarantine list. The currently active audit policy is unchanged and is still active.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1085I CURRENT QUARANTINE POLICY IS REMOVED.

Explanation

A new policy push occurred which resulted in the removal of the quarantine list.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1086I BOTH NEW POLICY AND QUARANTINE POLICY DETECTED.

Explanation

A new policy push occurred, which resulted in new policy and quarantine lists to be activated.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1086E ADHQ1086E *statement* DD STATEMENT MISSING

Explanation

The parameter DD statement (for example, ADHPARMS DD statement) is missing from the JCL for the collector agent started task.

User response

Create the necessary DD statement and code the appropriate parameters in the data set.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1153E RETURN CODE *return_code* REASON CODE *reason_code* WAS ENCOUNTERED DURING TRANSLATION SOURCE CCSID *ccsid* TARGET CCSID *ccsid*

Explanation

An error was encountered during the translation of the indicated CCSIDs. This may be the result of not having defined conversion paths between the CCSID of the collected SQL text and CCSID 1208 when performing a DB2® offload.

User response

To offload SQL text, verify that all necessary CCSID paths to 1208 are installed. You must define conversion paths between the CCSID of the collected SQL text and CCSID 1208.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1202I STORAGE CONSTRAINT RELIEVED FOR SPACE – *space* – OCCURRENCES: *count*

Explanation

An Integrated Storage Manager error had previously occurred due to a storage constraint for the space named in the message. The storage constraint has now been relieved. The number of storage constraint occurrences for this incident is displayed in the message.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1203I ASID=*asid*,TCB=*tcb*,CPID=*cpid*, MODULE=*module*,ADDR=*addr*, RC=*rc*,RSN=*rsn*

Explanation

A Security Guardium® S-TAP® for DB2® Integrated Storage Manager error has occurred. This message provides details that can be used by IBM® Software Support to diagnose the situation.

User response

Provide the text of this message to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1204I FUNC=*func*,SP=*subpool*,FLG2=*flag*,FLG3=*flag*

Explanation

A Security Guardium® S-TAP® for DB2® Integrated Storage Manager error has occurred. This message provides details that can be used by IBM® Software Support to diagnose the situation.

User response

Provide the text of this message to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1205E ISM ERROR OCCURRED, DETAIL FOLLOWS: *note*

Explanation

A Security Guardium® S-TAP® for DB2® Integrated Storage Manager error has occurred. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

Provide the text of this message and messages ADHQ1203I and ADHQ1204I along with any memory dumps that have been produced to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1209I ISM ERROR RC=*rc*,RSN=*rsn*,SPACE – *space*

Explanation

A Security Guardium® S-TAP® for DB2® Integrated Storage Manager error has occurred. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

Provide the text of this message and messages ADHQ1203I and ADHQ1204I along with any memory dumps that have been produced to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1210E ISM SPACE IS DISABLED – space

Explanation

A Security Guardium® S-TAP® for DB2® Integrated Storage Manager error has occurred. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

Provide the text of this message and messages ADHQ1203I and ADHQ1204I along with any memory dumps that have been produced to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1211I AN ABEND OCCURRED DURING ISM PROCESSING FOR SPACE – *space*

Explanation

A Query Monitor Integrated Storage Manager error has occurred. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

Provide the text of this message and messages ADHQ1203I and ADHQ1204I along with any dumps that may have been produced to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1212E AN ERROR OCCURRED IN THE EXTENT EXIT ROUTINE FOR SPACE – *space*

Explanation

A Security Guardium® S-TAP® for DB2® Integrated Storage Manager error has occurred. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

Provide the text of this message and messages ADHQ1203I and ADHQ1204I along with any memory dumps that might been produced to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1213W SPACE IS FULL AND NO MORE EXTENTS CAN BE OBTAINED FOR SPACE – space

Explanation

A Security Guardium® S-TAP® for DB2® Integrated Storage Manager operation has failed because no more extents can be obtained for the space named in the message. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

This may be a temporary situation due to the level of DB2 activity currently monitored by Security Guardium S-TAP for DB2. If message ADHQ1202I is also issued to indicate that the Storage Constraint has ended, then processing resumes. If this situation occurs frequently, adjust the amount of data collected by Security Guardium S-TAP for DB2, or increase the amount of available memory by using the MAXIMUM_ALLOCATIONS and SMEM_SIZE parameters.

If you need assistance with modifying these parameters, provide the text of this message and messages ADHQ1203I and ADHQ1204I to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1214W OWNER LIMIT EXCEEDED FOR SPACE – *space*

Explanation

A Security Guardium® S-TAP® for DB2® Monitor Integrated Storage Manager error has occurred. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

Provide the text of this message and messages ADHQ1203I and ADHQ1204I along with any memory dumps that might have been produced to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1215W SPACE IS FULL AND NO MORE LARGE EXTENTS CAN BE OBTAINED FOR SPACE – *space*

Explanation

A Security Guardium® S-TAP® for DB2® Monitor Integrated Storage Manager operation has failed because no more large extents can be obtained for the space named in the message. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Support to diagnose the problem.

User response

This might be a temporary situation due to the level of DB2 activity currently being monitored by Security Guardium S-TAP for DB2. If message ADHQ1202I is also issued to indicate that the Storage Constraint has ended, then processing resumes. If this situation occurs frequently, adjust the amount of data collected by Security Guardium S-TAP for DB2, or increase the amount of available memory by using the MAXIMUM_ALLOCATIONS and SMEM_SIZE parameters.

If you need assistance with modifying these parameters, provide the text of this message and messages ADHQ1203I and ADHQ1204I to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1216E EXTENT PROCESSING FAILED (ABEND) FOR SPACE – *space*

Explanation

A Security Guardium® S-TAP® for DB2® Integrated Storage Manager error has occurred. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

Provide the text of this message and messages ADHQ1203I and ADHQ1204I along with any memory dumps that have been produced to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1217W SPACE IS FULL AND NO MORE LARGE EXTENTS CAN BE OBTAINED FOR SPACE – *space*

Explanation

A Security Guardium® S-TAP® for DB2® Integrated Storage Manager operation has failed because the request would have exceeded the maximum storage allocation specified in the MAXIMUM_ALLOCATIONS parameter in ADHPARMS. At the time of the error, Security Guardium S-TAP for DB2 was attempting to allocate additional storage for the space named in the message. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

This might be a temporary situation due to the level of DB2 activity currently being monitored by Security Guardium S-TAP for DB2. If message ADHQ1202I is also issued to indicate that the Storage Constraint has ended, then processing resumes. If this situation occurs frequently, adjust the amount of data collected by Security Guardium S-TAP for DB2, or increase the amount of available memory by using the MAXIMUM_ALLOCATIONS and SMEM_SIZE parameters.

If you need assistance with modifying these parameters, provide the text of this message and messages ADHQ1203I and ADHQ1204I to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1218W MAXIMUM EXTENTS HAS BEEN REACHED FOR SPACE – *space*

Explanation

An Integrated Storage Manager operation has failed because the request would have exceeded the maximum number of extents allowed for the space named in the message. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

This might be a temporary situation due to the level of DB2® activity currently being monitored. If message ADHQ1202I is issued later to indicate that the Storage Constraint has ended, then processing resumes normally. If this situation rarely occurs, it might not be a problem. If this situation occurs frequently, adjust the amount of data collected by Security Guardium® S-TAP® for DB2, or increase the amount of available memory by using the MAXIMUM_ALLOCATIONS and SMEM_SIZE parameters.

If you need assistance with tuning these parameters, provide the text of this message and messages ADHQ1203I and ADHQ1204I to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1219W ALL ISMERROR MESSAGE BLOCKS ARE IN USE

Explanation

An Integrated Storage Manager error has occurred. However there were no free ISMERROR message blocks available.

User response

Increase the value of the ISM_ERROR_BLOCKS parameter in the ADHPARMS file. If this parameter is already set to the maximum value and the problem persists, contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1500E ABNORMAL EOT FOR *subtask* SUBTASK

Explanation

An abnormal end of task occurred for the subtask indicated in the message.

User response

Verify conditions surrounding the abnormal end of task and reissue the subtask.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2001E DB2® SUBSYSTEM *ssid* ALREADY MONITORED BY SUBSYSTEM *ssid*

Explanation

The indicated DB2 subsystem is already being monitored by the collector agent shown in the message.

User response

A DB2 subsystem can only be monitored by a single collector agent. To monitor the DB2 subsystem with another collector agent, first stop the monitoring of the DB2 subsystem by the collector agent (shown in the message).

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2002E MONITORING AGENT INSTALLATION FAILED FOR SUBSYSTEM *ssid*

Explanation

A monitoring agent was unable to start. Another SQL-type monitoring product might be active within the specified DB2® subsystem.

User response

Check to see if another SQL-type monitoring product is active. If so, shut down the other product and restart the S-TAP® collector. If this does not resolve the problem, contact IBM® Software Support.

If you encounter message ADHQ2002E and receive a memory dump, contact IBM Software Support and provide the memory dump for diagnostic purposes.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2003I FORCING MONITORING AGENT INSTALLATION FOR *ssid*

Explanation

The collector agent has detected that a monitoring agent is already active, but is forcing installation because `FORCE (Y)` was included.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2005I MULTIPLE MONITORING AGENT INSTALLATION FOR SUBSYSTEM *ssid*

Explanation

The collector agent has installed multiple monitoring agents for the subsystem shown in the message.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2008E DB2 SYSTEM *ssid* IS BEING MONITORED BY A 2.2 OR BELOW VERSION CQM SUBSYSTEM AND CANNOT BE AUDITED

Explanation

This message indicates an incompatibility between DB2 Query Monitor and S-TAP. InfoSphere® Guardium S-TAP for DB2 Version 9.1 will not start auditing a DB2 subsystem that is running Query Monitor at Version 3.1 or earlier.

User response

Ensure that you are running compatible versions of S-TAP and Query Monitor, or run only one product at a time.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2009E DB2® SYSTEM ssid WAS PREVIOUSLY MONITORED BY A 2.2 OR EARLIER CQM SUBSYSTEM qmid WHICH HAS NOT APPLIED APAR PK55535.

Explanation

You must apply Query Monitory V2R2 APAR PK55535.

User response

Apply the required maintenance.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2010I CURRENTLY ACTIVE POLICY RESULTS IN DISABLED COLLECTION

Explanation

The currently installed collection policy, as received from the Guardium® system, results in no ASC collection. This can be the result of:

- No policies are installed on the system.
- No DB2® Collection Profile policies are installed on the system.
- No DB2 Collection Profile policies matching the Svc. Name of the collector agent SSID are installed on the system.
- No DB2 Collection Profile policies contain Object entries that would result in ASC collection.

User response

If ASC collection is expected when this message is issued, review installed policy definitions in the Guardium system administration interface for the previously listed conditions. If no ASC collection is expected when this message is issued, no action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2013I CURRENTLY ACTIVE POLICY RESULTS IN GRANT/REVOKE COLLECTION

Explanation

The activated policy enables the collection of GRANT and REVOKE SQL statements. GRANT and REVOKE SQL statements are collected if they match the policy filter criteria.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2014I CURRENTLY ACTIVE POLICY RESULTS NO HOST VARIABLE COLLECTION.

Explanation

Host variables, which are also known as BIND variables, are not collected.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2015I CURRENTLY ACTIVE POLICY RESULTS NEGATIVE SQL CODES COLLECTION.

Explanation

The active policy contains a negative SQL code list that results in the collection of events ending with a negative SQL code.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2016I CURRENTLY ACTIVE POLICY RESULTS DB2 COMMANDS COLLECTION.

Explanation

Collection of COMMAND events is enabled.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2017I CURRENTLY ACTIVE POLICY RESULTS IN DBNAMES OPTIMIZATION.

Explanation

The currently active policy contains rules with DBNAME filters, which enables optimized filtering of audit events.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2018I CURRENTLY ACTIVE POLICY RESULTS IN A QUARANTINE LIST.

Explanation

The active policy contains a quarantine list that might cause DB2 activity to be quarantined.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2019I CURRENTLY ACTIVE POLICY RESULTS IN DB2 UTILITIES COLLECTION

Explanation

The active policy enables the collection of DB2 utilities.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2020I CURRENTLY ACTIVE POLICY RESULTS IN FAILED LOGIN COLLECTION.

Explanation

The active policy enables the collection of Failed Login events.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2100E UNRECOGNIZED PARAMETER

Explanation

The collector agent has encountered an unrecognized parameter.

User response

Check the startup parameters to ensure that the parameters specified are all valid.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2101E PARAMETER ERROR DETECTED FOR *parameter*

Explanation

The collector agent has encountered an error in one of the startup parameters.

Note: Message ADHQ2101E can be issued when the collector agent is started if the ADHCFGP file specifies primary space allocations for back store data sets that are less than the default.

User response

Check the startup parameters to ensure that all are specified properly. Check that primary space allocations for back store data sets are not set for less than their default values.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2103E DUPLICATE PARAMETER DETECTED FOR *parameter*

Explanation

Duplicate parameters were specified in the Query Common Collector startup parameters.

User response

Check the startup parameters to ensure that all are specified properly. Remove any duplicate parameters.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2110E TERMINATING DUE TO ERRORS IN PARAMETER FILE

Explanation

An error in the collector agent parameter file caused the termination of processing.

User response

Verify that the input you specified for your collector agent parameters in ADHCFGP is valid and correct for your objectives.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2111E ERROR READING PARAMETER DATASET - MEMBER NOT FOUND

Explanation

The collector agent encountered an error while attempting to read the ADHCFGP data set. The ADHPARMS DD statement specified a PDS data set and the member name specified did not exist.

User response

Correct the JCL specification for the ADHPARMS DD statement and specify a valid member name.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2402I DATASPACE MANAGEMENT IN PROGRESS FOR *dsmgmt*

Explanation

Indicates dataspace management is in progress for the subsystem shown in the message.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2403I *n* DATASPACE PAGES RELEASED FOR *ssid*

Explanation

Displays the number of dataspace pages that have been released for the subsystem shown in the message.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2408E INVALID REPLY. REPLY "U" TO ACCEPT OR "R" TO REJECT

Explanation

The replay you entered is not valid.

User response

Enter U to accept or R to reject.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2601E ALLOCATION FAILED FOR VSAM DATASET *dsn* RETCD=*rc* REAS=*rs*

Explanation

This message is issued by the started task if there is a problem during the dynamic allocation of a data set. When this message occurs, the collector agent stops and the startup process and terminates.

User response

To further diagnose and resolve the problem using the return code and reason code listed in the message, refer to the *MVS™ Programming Authorized Assembler Services Guide* (SA22-7608-07).

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2603E DEALLOCATION FAILED FOR DATASET *data_set* RETCD=*return_code* REAS=*reason_code*

Explanation

This message reports errors encountered during the execution of a CLOSE macro instruction.

User response

To further diagnose and resolve the problem using the return code and reason code listed in the message, refer to the *z/OS® V1R1.0 DFSMS/DFP Diagnosis Reference* (GY27-7618-01) or the following Web page:

http://publibz.boulder.ibm.com/cgi-bin/bookmgr_OS390/BOOKS/dgt2r101/20.8.1.2
Parent topic: Error messages and codes: ADHQxxxx

ADHQ3001I DB2® STARTUP DETECTED FOR SUBSYSTEM *ssid*

Explanation

The collector agent determined that a DB2 subsystem in its monitor list has started.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3002I MONITORING AGENT STARTED FOR SUBSYSTEM *ssid*

Explanation

Security Guardium® S-TAP® for DB2® has initiated monitoring for the named subsystem.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3003I DB2® SHUTDOWN DETECTED FOR SUBSYSTEM *ssid*

Explanation

The collector agent determined that a DB2 subsystem in its monitor list has shut down.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3005I MONITORING AGENT DEACTIVATED FOR *ssid*

Explanation

The monitoring agent has been deactivated for the indicated Collector Agent.

User response

None required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3006I AUDITING AGENT ACTIVATED FOR *ssid*

Explanation

The collector agent has been instructed to start the monitoring agent for a given DB2® subsystem when it becomes active. Monitoring of SQL for the DB2 subsystem will start when the monitoring agent is started indicated by message ADHQ3002I. Monitoring will continue after message ADHQ3002I is issued until one of the following

events occur:

1. The DB2 subsystem is stopped.
2. A deactivate for the monitoring agent is performed.
3. The collector agent subsystem that is monitoring the DB2 subsystem is stopped.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3192E LEVEL STATUS DB2(ssid) message

Explanation

This message displays if a mismatch in code level exists between Security Guardium® S-TAP® for DB2® and Query Monitor. One message per mismatched code level will occur.

User response

Ensure that all the programs listed have the Query Monitor and corresponding Security Guardium S-TAP for DB2 maintenance applied.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ3192I LEVEL STATUS DB2(ssid) message

Explanation

This message displays if a mismatch in code level exists between Security Guardium® S-TAP® for DB2® and DB2 Query Monitor. This message occurs once per mismatched code level.

User response

Verify that all the programs listed have the Query Monitor and corresponding S-TAP for DB2 maintenance applied.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ3200I DISPLAY AGENTS

Explanation

This message is used in conjunction with other messages to indicate display agents.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3201I DB2® SUBYSYSTEM *ssid* AGENT ADDRESS *address*

Explanation

Indicates the DB2 subsystem and agent address.

User response

None required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3202I *ssid* AGENT ADDRESS *address*

Explanation

Indicates the monitoring agent address.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3203I ASC DIAGNOSTIC DISPLAY:

Explanation

Indicates ASC diagnostic display is in effect.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3204I SDA ADDRESS *address*

Explanation

Indicates the SDA address.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3205I *ssid* ADDRESS *address*

Explanation

This message is used in conjunction with other messages to indicate the address.

User response

None required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3206I DIAGNOSTIC DATA FOR ABEND AT PSW *psw*

Explanation

The message displays diagnostic data for the abend.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3207I SYSTEM COMPLETION CODE *code*

Explanation

The message indicates the system completion code.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3208I OCCURRENCES *n* DATE *date* TIME *time*

Explanation

Indicates the number of occurrences and the date and time at which the took place.

User response

None required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3209I GPR 0-3 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3210I GPR 4-7 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3211I GPR 8-11 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3212I GPR 12-15 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3213I AR 0-3 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3214I AR 4-7 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3215I AR 8-11 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3216I AR 12-15 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3240I DB2® QM DATASPACE USAGE DISPLAY:

Explanation

This message appears in conjunction with other messages as a result of the MVS™ Modify command DISPLAY DATASPACES.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3241I *dataspace* DATASPACE

Explanation

This message appears in conjunction with ADHQ3240I as a result of the MVS™ Modify command `DISPLAY DATASPACES`.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3242I NODE SIZE *size*

Explanation

This message appears in conjunction with ADHQ3240I as a result of the MVS™ Modify command DISPLAY DATASPACES. This message lists the node size for the named data space.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3243I TOTAL NODES *n*

Explanation

This message appears in conjunction with ADHQ3240I as a result of the MVS™ Modify command `DISPLAY DATASPACES`. This message lists the total number of nodes allowed for the named data space.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3244I AVAILABLE NODES *n*

Explanation

This message appears in conjunction with ADHQ3240I as a result of the MVS™ Modify command `DISPLAY DATASPACES`. This message lists the total number of nodes available for use by the named data space.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3245I PERCENT UTILIZED *n*

Explanation

This message appears in conjunction with ADHQ3240I as a result of the MVS™ Modify command `DISPLAY DATASPACES`. This message lists the percentage of nodes used for the named data space.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3250I POSTING INTERVAL PROCESSOR

Explanation

This message appears to inform you that the interval processor has been started through an MVS™ Modify INTERVAL command.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3251I INTERVAL PROCESSOR NOT POSTED - DB2® UNAVAILABLE

Explanation

The interval processor was not started because a DB2 subsystem is not available.

User response

Verify the status of all monitored DB2 subsystems.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3252I INTERVAL PROCESSING ALREADY IN PROGRESS

Explanation

This message appears to inform you that the interval processor was already started through an MVS™ Modify `INTERVAL` command.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3308E DB2® SYSTEM ssid IS MONITORED BY DB2 QUERY MONITOR ssid WHICH HAS MISMATCHED OBJ AGENT

Explanation

This message indicates that the maintenance levels of one or more object modules do not match between the Security Guardium® S-TAP® for DB2 and Query Monitor installations. The maintenance code levels for Security Guardium S-TAP for DB2 and Query Monitor installations must match.

User response

Ensure that the maintenance levels match between the Security Guardium S-TAP for DB2 and Query Monitor installations. Apply maintenance as required to one or both environments to ensure that the maintenance levels match.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3315E MASTER SUBSYSTEM DOES NOT MATCH

Explanation

For monitoring and auditing to be active on the DB2® subsystem, a DB2 subsystem that is monitored by DB2 Query Monitor or Workload Replay for DB2 for z/OS® or audited by Security Guardium® S-TAP® for DB2 must have a matching MASTER_PROCNAME parameter between the Query Monitor subsystem and the Workload Replay DB2 subsystem, or the Security Guardium S-TAP for DB2 ASC started task.

User response

Update the MASTER_PROCNAME parameter for DB2 Query Monitor, Security Guardium S-TAP for DB2, or Workload Replay so that the same MASTER_PROCNAME is in use by all products for the monitored DB2 subsystem. After updating the MASTER_PROCNAME, restart the started task for the task that is affected by the parameter change.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3402I ISSUING COMMAND *cmd*

Explanation

Indicates command execution.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3551E VSAM LOGIC ERROR ENCOUNTERED WHILE ACCESSING CONTROL FILE FOR DB2® *ssid*. VSAMRC='*rc*' VSAMRS=X'*rs*'

Explanation

A VSAM logic error was encountered when accessing the control file for the DB2 subsystem indicated in the message.

User response

Verify that the DB2 control file for the DB2 subsystem listed in the message has been properly allocated and that the appropriate DB2 subsystem and plan names information have been specified correctly.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3552E SETUP INFORMATION MISSING FROM CONTROL FILE FOR DB2® *ssid*

Explanation

There is insufficient information in the control file for the DB2 subsystem indicated in the message.

User response

Modify the control file to include the necessary information.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3553E *message* ERROR *message*

Explanation

An error has occurred. This message is customized to display various messages such as initialization errors.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ4001E CONNECT TO DB2® *ssid* FAILED FOR PLAN *plan* RETURN CODE *rc* REASON CODE *rs*

Explanation

Security Guardium® S-TAP® for DB2 was not able to connect to the DB2 subsystem using the plan shown in the message.

User response

Refer to *DB2 Universal Database for z/OS® V8 Messages* (GC18-9602-01) and *DB2 Universal Database for z/OS V8 Codes* (GC18-9603-01) to further diagnose and resolve the problem.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ4003E CONNECT FAILED - DB2® NOT OPERATIONAL

Explanation

The collector agent was not able to connect to the DB2 subsystem because DB2 is not currently operational.

User response

Verify that DB2 is functioning correctly.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ5010I MONITORING AGENT DEINSTALLATION IN PROGRESS FOR SUBSYSTEM *ssid*

Explanation

The monitoring agent deinstallation is in progress for the DB2® subsystem indicated in the message.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ5011I MONITORING AGENT DEINSTALLATION COMPLETE FOR SUBSYSTEM *ssid*

Explanation

The monitoring agent deinstallation completed for the DB2® subsystem indicated in the message.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ5012I REQURESTING MONITORING AGENT ACTIVATION FOR DB2® SUBSYSTEM *ssid*

Explanation

The monitoring agent for the indicated DB2 subsystem is being requested for activation.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ5013I REQUESTING MONITORING AGENT DEACTIVATION FOR DB2® SUBSYSTEM *ssid*

Explanation

The monitoring agent for the indicated DB2 subsystem is being requested for deactivation.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ6101E LOCATE FAILED FOR *dataset* R0=*code* RC=*rc*

Explanation

A catalog located failed during interval data set expiration processing. r0 contains the contents of the register zero and rc is the LOCATE return code.

User response

See *z/OS® DFSMSdfp Advanced Services* (SC26-7400-02) for a description of the return codes issued by LOCATE.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ6102E SCRATCH FAILED FOR *file* SCRATCH STATUS CODE=*code* RO=*ro*

Explanation

The scratch failed for the indicated file.

User response

See *z/OS® DFSMSdfp Advanced Services* (SC26-7400-02) for a description of the return codes issued by LOCATE.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ7001E *table* TABLE NOT LOCATED IN DB2® CATALOG

Explanation

The table indicated in the message cannot be found in the DB2 catalog.

User response

Verify that the table you specified exists.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ7008E QUERY COMMON COLLECTOR *ssid* NOT VALID OR HAS NOT BEEN STARTED SINCE IPL

Explanation

The collector agent shown in the message is not a valid collector agent.

User response

Verify that you specified the correct Query Common Collector subsystem ID, and that the collector agent is available.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ7009E OUT OF SPACE CONDITION DETECTED WHILE WRITING TO THE *dsn* DATASET

Explanation

An out-of-space condition was encountered when attempting to write to the data set indicated in the message.

User response

Verify that adequate space has been allocated to the data set.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ7010E MISSING "ADD" PARAMETER FOR *parameter* AT LINE *line* COLUMN *column*

Explanation

The ADD parameter is missing for the indicated line and column.

User response

Specify an ADD parameter.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ7011E INTERNAL ERROR - UNABLE TO RESOLVE ALTERNATE COLUMN *column*

Explanation

There has been an internal error.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ7015E NUMBER OF BSDS SPECIFICATIONS INVALID OR MISSING

Explanation

An invalid number of BSDS parameters has been sent as input to the ADH#CTLF utility.

User response

Verify that the two boot strap data sets used for your DB2® subsystem are properly specified.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ7016E DUPLICATE RECORD STORE ATTEMPTED FOR DB2® SUBSYSTEM *ssid*

Explanation

This message describes an error condition when attempting to load records into the control file that already exist without specifying REPLACE(Y) for the DB2 subsystem indicated in the message.

User response

Edit your ADH#CTLF job to include REPLACE(Y). Refer to the instructions in SADHSAMP library member ADH#CTLF for details.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8001E ERRORS DETECTED IN *parameters* PARAMETERS:

Explanation

Errors have been detected in ADHCFGP.

User response

Verify that the parameters you specified in ADHCFGP are correct and modify any syntax errors before proceeding.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8002E UNIDENTIFIED KEYWORD DETECTED AT LINE *line* COLUMN *column*

Explanation

An unknown keyword has been found.

User response

Verify the correct syntax and modify the keyword as needed.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8003E INVALID SYNTAX SPECIFIED FOR *parameter* NEAR LINE *line* COLUMN *column*

Explanation

The syntax specified for the parameter indicated in the message is not valid.

User response

Correct the syntax and resubmit the job.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8004E PARAMETER LENGTH EXCEEDED FOR *parameter* NEAR LINE *line* COLUMN *column*

Explanation

The length of the value specified for the parameter indicated in the message exceeded the valid length for that parameter.

User response

Correct the syntax and resubmit the job.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8005E PARAMETER MISSING FOR *parameter* NEAR LINE *line* COLUMN *column*

Explanation

A required parameter is missing from ADHLOADP.

User response

Correct the syntax and resubmit the job.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8006E NON NUMERIC DATA SPECIFIED FOR *parameter* NEAR LINE *line* COLUMN *column*

Explanation

Non-numeric data was specified in ADHLOADP for the parameter listed in the message.

User response

Specify numeric data for the parameter.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8007E INVALID VALUE SPECIFIED FOR *parameter* NEAR LINE *line* COLUMN *column*

Explanation

An invalid value was specified in ADHLOADP.

User response

Correct the value and resubmit the job.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8008E *value* MUST BE *value* THAN *value*

Explanation

The value of the parameter shown in the message must be within the specified range.

User response

Correct the value of the parameter so it falls within the range indicated in the message text.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8009E DUPLICATE PARAMETER *parameter* AT LINE *line* COLUMN *column*

Explanation

A parameter you specified is a duplicate.

User response

Correct the syntax to eliminate the duplicate parameter.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8010E DUPLICATE SUBPARAMETER DETECTED FOR PARAMETER *parameter* AT LINE *line* COLUMN *column*

Explanation

A sub-parameter you specified is a duplicate.

User response

Correct the syntax to eliminate the duplicate sub-parameter.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8011E DB2® VERSION NOT SUPPORTED

Explanation

The version of DB2 with which you are attempting to use is not supported by unload functionality of the collector agent.

User response

The collector agent unloads data to DB2 Version 8, DB2 Version 9, or DB2 Version 10.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8012E ERROR OPENING DDNAME *ddname*

Explanation

The collector agent encountered an error attempting to open the TEXTDATA data set.

User response

Verify that the TEXTDATA data set is configured properly and has adequate space available.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8013E INVALID PARAMETER LENGTH FOR *parameter*

Explanation

The value you specified for the TBCREATOR parameter is too long and is therefore invalid.

User response

Specify a valid value for TBCREATOR. Valid values are up to eight characters in length.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8014E LOGIC ERROR: *error*

Explanation

The collector agent has encountered a logic error.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADH8022I *adh parameter value*

Explanation

This message is used to display the contents of the ADHPARMS file that was processed when Security Guardium® S-TAP® for DB2® was started.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADH9899I *adh modify command*

Explanation

This message is used to display the text of a modify command that was issued to Security Guardium® S-TAP® for DB2®.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

IBM Security Guardium S-TAP for IMS on z/OS

These topics describe how to use IBM Security Guardium S-TAP for IMS on z/OS V10.1.3 (also referred to as IBM Guardium S-TAP for IMS). The V10.1.3 S-TAP is optimized for the V10.1 Guardium system. IBM Guardium S-TAP for IMS collects and correlates data access information from a variety of IMS resources to produce a comprehensive view of business activity for auditors.

About these topics

This information is designed to help database administrators, appliance programmers, and application programmers perform these tasks:

- Plan for the installation of IBM Guardium S-TAP for IMS
- Install and operate IBM Guardium S-TAP for IMS
- Configure the IBM Guardium S-TAP for IMS environment
- Diagnose and recover from IBM Guardium S-TAP for IMS problems

A PDF of this User's Guide is available here.

- **IBM Security Guardium S-TAP for IMS on z/OS**
  These topics describe how to use IBM Security Guardium S-TAP for IMS on z/OS V10.1.3 (also referred to as IBM Guardium S-TAP for IMS). The V10.1.3 S-TAP is optimized for the V10.1 Guardium system. IBM Guardium S-TAP for IMS collects and correlates data access information from a variety of IMS resources to produce a comprehensive view of business activity for auditors.
- **What does IBM Security Guardium S-TAP for IMS on z/OS V10.1.3 do?**
  IBM Security Guardium S-TAP for IMS on z/OS (also referred to as IBM Guardium S-TAP for IMS) is an auditing tool that collects and correlates data access information from IMS Online regions, IMS batch jobs, IMS archived log data sets, and SMF records to produce a comprehensive view of business activity that occurs within one or more IMS environments.
- **Installing IBM Security Guardium S-TAP for IMS on z/OS**
  The following sections describe hardware, software, and user ID authority prerequisites for product installation.
- **IBM Security Guardium S-TAP for IMS on z/OS security**
  IBM Guardium S-TAP for IMS requires access to various IMS data sets and IBM Guardium system components.
- **Configuration overview**
  These actions are required to configure IBM Guardium S-TAP for IMS.
- **Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent**
  This section describes the information necessary for configuring the agent.
- **Setting up an IMS environment for auditing**
  This section describes how to customize IMS environments to capture DLI calls, including customizing IMS catalogued procedures, coexisting with other DFSFLGX0 and DFSISVI0 exit routines, customizing IMS to use a zIIP, copying common load modules from SAUILOAD to SAUIIMOD, and the security considerations related to IMS processing.
- **Using agent configuration keywords to customize auditing**
  Some agent configuration keywords must be used for the product to function. You can also use agent configuration keywords for optional auditing specifications.
- **IBM Security Guardium S-TAP for IMS on z/OS agent reference information**
  The IBM Guardium S-TAP for IMS agent provides access to database and appliance services, in support of the product's remote clients. The agent also reads audited DLI events placed in the z/OS System Logger log streams by the IMS Online and DLI/DBB batch Data collectors and sends the DLI events to the IBM Guardium system using TCP/IP connections.
- **Data collection**
  The collection process involves the gathering of audit event data at run time. Specify various filtering criteria to capture all relevant events and limit the amount of data that is collected and stored.
- **Creating and modifying IMS definitions**
  An IMS definition establishes a connection from your Guardium system to the IMS environment that you want to audit. To create and modify IMS definitions from the Guardium system interface, the agent address space (AUIA*STC*) must have a preestablished connection to the Guardium system.
- **Reference information**
  This chapter provides IBM Guardium S-TAP for IMS reference information.
- **Troubleshooting**
  Use the following topics to diagnose and correct problems that you experience with IBM Guardium S-TAP for IMS.

Parent topic: S-TAP for z/OS V10.1.3 User's Guide
Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

What does IBM Security Guardium S-TAP for IMS on z/OS V10.1.3 do?

IBM Security Guardium S-TAP for IMS on z/OS (also referred to as IBM Guardium S-TAP for IMS) is an auditing tool that collects and correlates data access information from IMS Online regions, IMS batch jobs, IMS archived log data sets, and SMF records to produce a comprehensive view of business activity that occurs within one or more IMS environments.

IBM Guardium S-TAP for IMS assists auditors in determining who read or updated a particular IMS database and its associated data sets, what mechanism was used to perform that action, and when the access took place.

IBM Guardium S-TAP for IMS can collect and correlate many different types of information, including:

- Accesses to databases and segments from IMS Online regions.
- Accesses to databases and segments from IMS DLI/DBB batch jobs.
- Accesses to databases, image copies, IMS logs, and RECON data sets and security violations to these data sets as recorded by SMF.
- IMS Online region START and STOP, database, and PSB change of state activity and user signon and signoff as recorded in the IMS Archived Log data sets.

Restriction: IBM Guardium S-TAP for IMS supports auditing of Data Entry Databases (DEDBs) and IMS Full Function databases. Auditing of Main Storage Databases (MSDBs) is not supported.

- **What's new in IBM Security Guardium S-TAP for IMS on z/OS V10.1.3?**
  Here's what's new in version 10.1.3 of IBM Guardium S-TAP for IMS.
- **IBM Guardium S-TAP for IMS components**
  IBM Guardium S-TAP for IMS consists of an agent, a Common Storage Management Utility, and the IBM Guardium system.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

What's new in IBM Security Guardium S-TAP for IMS on z/OS V10.1.3?

Here's what's new in version 10.1.3 of IBM Guardium S-TAP for IMS.

Enhancements to this version include:

- Echoing of active policy XML as described in Echoed XML statement definitions.
- Increased security of online and batch log streams as described in z/OS log streams.
- Filtering of DLI called based on IMS LTERM names
- Collection of the accessed HALDB PARTITION name during DLI call processing
- Check agent status without accessing z/OS by using a Guardium interface command
- Ability to enable simulation mode to simulate mainframe activity levels, test deployment, and gauge appliance requirements without sending data to the Guardium appliance
- New parameters to simplify audit record validation, debugging, and agent configuration
- Simplified agent configuration:
  - Complete SMF configuration is no longer required if the SMF_CYCLE_INTERVAL(0) parameter is specified in the AUICONFG file and SMF processing is disabled.
  - Complete IMSL configuration is no longer required if the IMSL_CYCLE_INTERVAL(0) parameter is specified in the AUICONFG file and IMSL processing is disabled.
- Messages AUII050I and AUIJ250I now include the IMSID to help identify which IMS system issued the message.
- Reduced CPU consumption and greater reliability during processing of IMS DLI calls in IMS online environments.
- RECON data sets that are read by the SMF (AUIF*STC* and IMS SLDS (AUIL*STC*) can optionally be copies of the live IMS RECON data sets.
- Option to disable DLI call auditing of IMS online DLI calls that originate from the following IMS region types: AER, BMP, CICS®, DBCTL, IFP, MPP, and ODBA.
- Support for Internet Protocol version 6 (IPV6) introduced with PH16991

Parent topic: What does IBM Security Guardium S-TAP for IMS on z/OS V10.1.3 do?

IBM Guardium S-TAP for IMS components

IBM Guardium S-TAP for IMS consists of an agent, a Common Storage Management Utility, and the IBM Guardium system.

- **IBM Guardium system**
  The IBM Guardium system can gather and report information from multiple agents running on multiple z/OS systems.
- **IBM Guardium S-TAP for IMS agent**
  The IBM Guardium S-TAP for IMS agent coordinates the collection of audited data, and the transmission of audited DLI call data to the IBM Guardium system.

Parent topic: What does IBM Security Guardium S-TAP for IMS on z/OS V10.1.3 do?

IBM Guardium system

The IBM Guardium system can gather and report information from multiple agents running on multiple z/OS systems.

Note: In environments where multiple agents connect to a common IBM Guardium system or appliance, the z/OS agent started task names (AUIAS*TC*, AUILS*TC*, AUIF*STC*) must be unique. Unique started task names enable the IBM Guardium S-TAP for IMS policies that are pushed from the IBM Guardium system to be attributed to, and monitored by, the correct z/OS agent.

IBM Guardium system components

The IBM Guardium system:

- Provides the user interface, which processes requests and displays the resulting information.
- Enables you to create collection policies, which specify the types of data to be collected by the agent.
- Stores the collected data.

IBM Guardium system and S-TAP agent communication

The IBM Guardium system and the IBM Guardium S-TAP for IMS agent communicate using a TCP/IP connection. The policies you create, using the user interface, tell the agent what data to collect. The policy specifies filter information, such as which data sets are to be monitored for data accesses.

Parent topic: IBM Guardium S-TAP for IMS components

IBM Guardium S-TAP for IMS agent

The IBM Guardium S-TAP for IMS agent coordinates the collection of audited data, and the transmission of audited DLI call data to the IBM Guardium system.

The IBM Guardium S-TAP for IMS agent can collect data from one or more of the following sources within a SYSPLEX:

- A single IMS system
- Multiple IMS systems that share a common set of RECON data sets
- Multiple IMS systems using diverse RECON data sets

The agent maintains the communication links that are needed to exchange information with:

- The IBM Guardium system
- IMS Online and Batch data collectors and activity monitors
- The IMS Archive Log data set and SMF activity monitors

The agent also provides data collection schemas, called policies, to the activity monitors on which detail the IMS artifacts are to be audited, and to what level.

The agent runs as a started task on the z/OS host. An example of the JCL to be used is in member AUIASTC of the SAUISAMP installation data set.

The agent collects data from the following sources:

- IMS online activities
- IMS batch activities
- SMF data
- IMS archived log data
- IMS RECON data sets

For more information about how data is collected from these sources, see Data collection monitors.
Parent topic: IBM Guardium S-TAP for IMS components

Installing IBM Security Guardium S-TAP for IMS on z/OS

The following sections describe hardware, software, and user ID authority prerequisites for product installation.

Review the IBM Guardium S-TAP for IMS V10.1.3 Program Directory for a list of product materials and SMP/E installation instructions.

- **Hardware and software prerequisites**
  The following hardware and software are required to operate IBM Guardium S-TAP for IMS V10.1.3.
- **User ID authorities that are required for installation**
  The following z/OS USERID authorities are needed to install IBM Guardium S-TAP for IMS.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

Hardware and software prerequisites

The following hardware and software are required to operate IBM Guardium S-TAP for IMS V10.1.3.

- z/OS Version 2 Release 2 or later, until end of service.
- IMS V13 -- V15, until end of service.
- Any hardware capable of running z/OS Version 2 Release 1 or later, until end of service.

IBM Guardium S-TAP for IMS requires use of the following:

- 64-bit memory
- TCP/IP connectivity
- z/OS System logger log streams
- UNIX System Services
- OMVS segment

Parent topic: Installing IBM Security Guardium S-TAP for IMS on z/OS

User ID authorities that are required for installation

The following z/OS USERID authorities are needed to install IBM Guardium S-TAP for IMS.

If you are installing this product, your z/OS user ID must have the authority to:

- Define z/OS system log streams
- Update the IMS cataloged procedure data set members DLIBATCH and DBBBATCH to include product load libraries

Parent topic: Installing IBM Security Guardium S-TAP for IMS on z/OS

IBM Security Guardium S-TAP for IMS on z/OS security

IBM Guardium S-TAP for IMS requires access to various IMS data sets and IBM Guardium system components.

- **APF authorization**
  IBM Guardium S-TAP for IMS requires certain data sets to be accessible and APF-authorized on all LPARS of the SYSPLEX where IMS batch jobs or monitored IMS online regions might run.
- **OMVS segment**
  TCP/IP connectivity and other UNIX System services on z/OS require that the address space that is using these services use a z/OS user ID or group name that is defined with an OMVS segment.
- **TCP/IP connections**
  IBM Guardium S-TAP for IMS uses Transmission Control Protocol/Internet Protocol (TCP/IP) to connect to the Guardium appliance. To enable this communication, make sure you have the correct permissions assigned.
- **z/OS log streams**
  IBM Guardium S-TAP for IMS monitors the IMS batch jobs and online regions and writes audit data to z/OS log streams.
- **IMS RESLIB data sets**
  READ access to the IMS RESLIB/SDFSRESL data sets is required for each IMS system that requires the IMS SLDS to be processed by IBM Guardium S-TAP for IMS. READ access is required to allow a LOAD/READ of module DFSVC000 to determine the version release level of the audited IMS.
- **SMF and IMS archive log data sets**
  READ access to the SMF data sets and the IMS archived logs data sets (SLDS) is required for the user under whose authority the agent runs. If these data sets are protected by RACF® or another security product, a policy must be defined to grant this access. The z/OS catalogs containing the names of these data sets, as well as the physical data sets themselves, must be accessible from the LPAR on which the IBM Guardium S-TAP for IMS agent runs.
- **DBRC RECON data sets**
  IBM Guardium S-TAP for IMS uses the native VSAM services to read data from the RECON data sets. These RECON data sets must be accessible from all the LPARS where the IBM Guardium S-TAP for IMS agents might run.
- **Operator commands**
  You can use z/OS Operator commands, to start IBM Guardium S-TAP for IMS tasks.
- **Quarantining Database DLI calls**
  IBM Guardium S-TAP for IMS enables you to quarantine the DB DLI calls of specific users for specific periods of time.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

APF authorization

IBM Guardium S-TAP for IMS requires certain data sets to be accessible and APF-authorized on all LPARS of the SYSPLEX where IMS batch jobs or monitored IMS online regions might run.

About this task

Refer to the *z/OS Knowledge Center* for more information about how to APF authorize libraries.

Procedure

1. APF-authorize product data set SAUILOAD on all LPARS of the SYSPLEX.
   SAUILOAD contains the IMS Online and Batch Activity Monitor executable code.
2. APF-authorize product data set SAUIIMOD on all LPARS of the SYSPLEX where IMS batch jobs or IMS online regions to be monitored might run.
   SAUIIMOD contains IMS specific executable load modules.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS security

OMVS segment

TCP/IP connectivity and other UNIX System services on z/OS require that the address space that is using these services use a z/OS user ID or group name that is defined with an OMVS segment.

Defining your z/OS user ID or group name with an OMVS segment might require the use of the IBM RACF command ADDUSER/ALTUSER xxxxxx OMVS(UID(zzz)) or a security product equivalent command. Review your z/OS Security Server documentation for more information.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS security

TCP/IP connections

IBM Guardium S-TAP for IMS uses Transmission Control Protocol/Internet Protocol (TCP/IP) to connect to the Guardium appliance. To enable this communication, make sure you have the correct permissions assigned.

If you are working from a secure communications port, enable the user ID that is associated with the agent started task to have READ/WRITE permissions on the ports that are assigned to the agent.

See Using agent configuration keywords to customize auditing for more information about the ADS_LISTENER_PORT, APPLIANCE_PORT, and LOG_PRT_SCAN_START configuration keywords.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS security

z/OS log streams

IBM Guardium S-TAP for IMS monitors the IMS batch jobs and online regions and writes audit data to z/OS log streams.

The IBM Guardium S-TAP for IMS Online and DLI/DBB batch data collectors audit DLI events that occur in the IMS Online and DLI/DBB Batch regions. Audited DLI events are written to z/OS System Logger log streams, which are then read by the IBM Guardium S-TAP for IMS agent. The IMS agent sends the audit data to the IBM Guardium appliance by using TCP/IP connections.

To permit the IMS Online and DLI/DBB batch collectors to write to the log streams, systems authorization facility (SAF) security access of UPDATE to the z/OS log stream is required for all user IDs associated with the audited IMS Control region and DLI/DBB batch jobs that might cause IMS DLI calls to be audited.

You can now use an additional SAF resource to further secure the online and batch log streams. For example, you can now prevent the log streams from being read by a user program or utility that is initiated by a user who is authorized to update to the log stream. Apply z/OS V2R3 and V2R4 APAR OA56050 to optionally add an additional authority check for a SAF profile that covers resource (WRITE_ONLY_log-stream-name) in class LOGSTRM. This new profile option enables you to limit users to only connecting to (IXGCONN REQUEST=CONNECT), writing to (IXGWRITE), and disconnecting from (IXGCONN REQUEST=DISCONNECT) the log stream. Other IXG calls, such as IXGBRWSE (read), are rejected with return code 8 and reason code '081C'x. For more information, refer to the documentation provided in the HOLD data for APAR OA56050.

Note: User IDs that are associated with the IBM Guardium S-TAP for IMS agent must have authority to read and delete data from the log stream and should not be limited by using resource (WRITE_ONLY_log-stream-name). Log stream UPDATE authority is recommended for the IBM Guardium S-TAP for IMS agents.
Parent topic: IBM Security Guardium S-TAP for IMS on z/OS security

IMS RESLIB data sets

READ access to the IMS RESLIB/SDFSRESL data sets is required for each IMS system that requires the IMS SLDS to be processed by IBM Guardium S-TAP for IMS. READ access is required to allow a LOAD/READ of module DFSVC000 to determine the version release level of the audited IMS.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS security

SMF and IMS archive log data sets

READ access to the SMF data sets and the IMS archived logs data sets (SLDS) is required for the user under whose authority the agent runs. If these data sets are protected by RACF® or another security product, a policy must be defined to grant this access. The z/OS catalogs containing the names of these data sets, as well as the physical data sets themselves, must be accessible from the LPAR on which the IBM Guardium S-TAP for IMS agent runs.

Consult your security administrator to determine what is currently protected and how to grant the required access.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS security

DBRC RECON data sets

IBM Guardium S-TAP for IMS uses the native VSAM services to read data from the RECON data sets. These RECON data sets must be accessible from all the LPARS where the IBM Guardium S-TAP for IMS agents might run.

VSAM access to the RECON data sets is READ-ONLY, allowing the IBM Guardium S-TAP for IMS jobs and started tasks with a security access of READ to process the RECON data sets.

Consult your security administrator to determine how your RECON data sets are protected, and how to grant the required access.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS security

Operator commands

You can use z/OS Operator commands, to start IBM Guardium S-TAP for IMS tasks.

The user ID that is assigned to the IBM Guardium S-TAP for IMS agent started task must be permitted to issue START commands to initiate the AUIF*stc*, AUIL*stc*, and AUIU*stc* tasks. During installation, administrators can configure the z/OS security product to restrict users and programs from issuing z/OS Operator commands.
Parent topic: IBM Security Guardium S-TAP for IMS on z/OS security

Quarantining Database DLI calls

IBM Guardium S-TAP for IMS enables you to quarantine the DB DLI calls of specific users for specific periods of time.

Quarantining a user of a specific IMS subsystem means that for the specified time period, the quarantined user is not able to run DB DLI calls either by using the targeted IMS subsystem, or while running DLI/DBB batch jobs.

If a quarantined user attempts access during a restricted time, the DLI call is not performed, and a status code of `AI` is returned in the DBPCB status code field.

To create quarantine rules, access the Policy Builder from the Tools and Views section of the Guardium appliance interface Setup menu.

Note:

- DLI calls that are made to IMS Fast Path databases by using IMS Fast Path exclusive transactions or BMPs cannot be quarantined.
- Quarantine does not take effect immediately. The audited DLI call that produces the event to trigger the quarantine is completed before the quarantine takes effect. It is possible for DLI calls to be run by the quarantined user before the quarantine takes effect.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS security

Configuration overview

These actions are required to configure IBM Guardium S-TAP for IMS.

Review the following steps, which are described in greater detail in the following sections:

- Verify that you have the resource authorizations that are required to configure the product.

- Review the steps to plan your configuration and customize your environment.
- Set up the z/OS log streams. Review the CFRM and log stream size requirements, and the related security considerations, limitations, and restrictions. Define the log streams for batch and online jobs.
- Determine a naming convention for the agent (AUIA*STC*, AUIF*STC*, AUIL*STC*, and AUIU*STC*) started tasks, where *STC* can be changed to any 1 - 4 character length string.
  Tip: Retain the AUI prefix to simplify task identification.
- Configure the agent by customizing the configuration file, customizing the agent JCL, and starting the agent.
- Set up the IMS environment for auditing by customizing the IMS cataloged procedure, configuring IMS exits, customizing IMS to use an IBM System z® Integrated Information Processor (zIIP), and review the related security considerations.

Note: No WLM (Workload Manager) considerations are necessary. All agent started tasks use the STC WLM class.

- **Upgrading from Guardium S-TAP for IMS V9.0**
  Complete the following steps to upgrade from InfoSphere® Guardium S-TAP for IMS V9.0 to IBM Guardium S-TAP for IMS V10.1.3. These steps enable V9.0 product assets, such as JCLs and configuration and repository contents, to be upgraded to V10.1.3, while allowing the full use and functionality of the V10.1.3 product.
- **Upgrading from Guardium S-TAP for IMS V9.1 or V10.0**
  The agent JCL and configuration file that are used by IBM Guardium S-TAP for IMS V9.1 and V10.0 are compatible with IBM Guardium S-TAP for IMS V10.1.3. No configuration changes are required to upgrade from IBM Guardium S-TAP for IMS V9.1 to IBM Guardium S-TAP for IMS V10.1.3.
- **Planning your configuration and customizing your environment**
  Collect user ID and environment information before you configure IBM Guardium S-TAP for IMS V10.1.3.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

Upgrading from Guardium S-TAP for IMS V9.0

Complete the following steps to upgrade from InfoSphere® Guardium S-TAP for IMS V9.0 to IBM Guardium S-TAP for IMS V10.1.3. These steps enable V9.0 product assets, such as JCLs and configuration and repository contents, to be upgraded to V10.1.3, while allowing the full use and functionality of the V10.1.3 product.

Before you begin

New versions or releases of IBM Guardium S-TAP for IMS should be installed as a new installation base. However, if circumstances prevent you from doing so, follow these instructions to upgrade from the previous version's installation base.

Procedure

1. Deactivate or uninstall all policies that apply to the agent that you are upgrading.
2. Shut down the agent that you are upgrading.
3. Customize the AUIMIG10 SAMPLIB member to convert the configuration file and repository to V10.1.3 format, and submit.
   The comments that are contained in the AUIMIG10 SAMPLIB member describe how to customize the JCL. A V10.1.3 format configuration file, and an IMS definition report will be produced.
4. Use the IMS definition report, which is produced by the AUIMIG10 utility, to add the IMS definitions to your IBM Guardium system.
5. Update the new configuration file, which is produced by the AUIMIG10 utility, with any changes.
6. Update the AGENT (AUIA*STC*) and Memory Management Utility (AUIU*STC*) JCLs as follows:
   a. Remove the //AUICFG DD JCL statement.
   b. Add a //AUICONFG DD JCL statement, and set it to reference the new configuration member produced by the AUIMIG10 utility.
   c. Change the //STEPLIB DD JCL statement to reference the V10.1.3 product load library (SAUILOAD).
   d. Remove the //AUIREPOS DD JCL statement from the AUIU*STC* JCL.
7. Update the SMF (AUIF*STC*) and IMS Archive Log (AUIL*STC*) JCLs as follows:
   a. Remove the //AUICFG DD JCL statement, and any procedure parameters that reference it.
   b. Change the //STEPLIB DD JCL statement to reference the V10.1.3 product load library (SAUILOAD).
8. Update the IMS Control region JCLs that are audited by the agent to use the V10.1.3 product IMS load library (SAUIIMOD).
9. Update the IMS DBBBATCH and DLIBATCH cataloged procedures, and any equivalent JCL members, to use the V10.1.3 product IMS load library (SAUIIMOD).
10. Start the agent.
11. Install or activate the policies that you want to apply.
12. Stop and restart your IMS systems.

What to do next

Now, you can:

- Install additional policies on the z/OS host by using the IBM Guardium system user interface.
- Manage agent and IMS definitions by using the IBM Guardium system user interface.

Note: The format of the data that is written to the z/OS logstreams has changed from V9.0 to V10.1.3. IBM Guardium S-TAP for IMS V10.1.3 converts any existing V9.0 data from existing logstreams to a usable format. If you migrate from a V10.1.3 system back to a V9.0 system, you must reinitialize the z/OS log streams before restarting InfoSphere Guardium S-TAP for IMS V9.0.

Parent topic: Configuration overview

Upgrading from Guardium S-TAP for IMS V9.1 or V10.0

The agent JCL and configuration file that are used by IBM Guardium S-TAP for IMS V9.1 and V10.0 are compatible with IBM Guardium S-TAP for IMS V10.1.3. No configuration changes are required to upgrade from IBM Guardium S-TAP for IMS V9.1 to IBM Guardium S-TAP for IMS V10.1.3.

Before you begin

Do not attempt to run AUIMIG10 to upgrade from Guardium S-TAP for IMS V9.1 or V10.0 to IBM Guardium S-TAP for IMS V10.1.3.

About this task

The format of the data that is written to the z/OS logstreams has changed in V10.1.3. IBM Guardium S-TAP for IMS V10.1.3 converts any existing Guardium S-TAP for IMS V9.1 and V10.0 data from existing logstreams to a usable format. If you migrate from a V10.1.3 system back to a V9.1 or V10.0 system, you must reinitialize the z/OS log streams before restarting the previous product version.
Parent topic: Configuration overview

Planning your configuration and customizing your environment

Collect user ID and environment information before you configure IBM Guardium S-TAP for IMS V10.1.3.

Tip: To upgrade to IBM Guardium S-TAP for IMS from a previous version, refer to the appropriate topic:

- Upgrading from Guardium S-TAP for IMS V9.0
- Upgrading from Guardium S-TAP for IMS V9.1 or V10.0

If you are upgrading from a previous version to V10.1.3, no further configuration steps are required. Upgrading to V10.1.3 requires the use of, and modifications to, the same agent name and JCLs that were used with previous versions. For your reference, see the Sample library members table.
Before you configure a new installation of IBM Guardium S-TAP for IMS V10.1.3, determine the following:

- The user IDs that will be used to run the agent started tasks
- Where the agent started tasks will run

Then, customize the ISPF edit macro, review the job card requirement, and set up the z/OS log streams, as described in the following sections.

- **Customizing the ISPF edit macro**
  The SAUISAMP data set shipped with IBM Guardium S-TAP for IMS includes an ISPF edit macro to help with the editing of the rest of the SAMPLIB members to be used in the subsequent steps.
- **Job cards for the sample JCL in the SAMPLIB**
  Some JCL members included with the product SAMPLIB have a filler card for the job card.
- **Setting up z/OS log streams**
  IBM Guardium S-TAP for IMS uses the z/OS System Logger to funnel events from IMS online regions and DLI/DBB batch jobs to the DLI event processor (AUIA*STC* task). Both XCF based and DASD based log streams are supported.

Parent topic: Configuration overview

Customizing the ISPF edit macro

The SAUISAMP data set shipped with IBM Guardium S-TAP for IMS includes an ISPF edit macro to help with the editing of the rest of the SAMPLIB members to be used in the subsequent steps.

About this task

The edit macro is named AUIEMAC1 and provides a straightforward way to customize the variable values for the variables that appear in the JCL that will run. Use this edit macro as part of a command list (CLIST) to edit the other SAMPLIB members.

Procedure

1. To set up the edit macro, copy AUIEMAC1 from the #HLQ.SAUISAMP to a CLIST library.
2. Edit the macro by providing the appropriate values for each of the variables.
3. To run the macro, type the name of the edit macro in the command line in ISPF.

Results

After you modify the edit macro, you can use it as a command to customize other SAMPLIB members in the following steps, unless otherwise specified.

Example

The contents of the edit macro AUIEMAC1 included in the SAMPLIB are as follows:

```
ISREDIT MACRO (NP)
ISPEXEC VGET (ZUSER)
ISREDIT CHANGE ALL '#AUILOAD'           AUI.IBMTAPE.SAUILOAD
ISREDIT CHANGE ALL '#AUIIMOD'           AUI.IBMTAPE.SAUIIMOD
ISREDIT CHANGE ALL '#AUISAMP'           AUI.IBMTAPE.SAUISAMP
ISREDIT CHANGE ALL '#AUICONFG'          AUICONFG
```

This table describes each variable in the edit macro AUIEMAC1 included in the SAMPLIB:

Table 1. AUIEMAC1 Edit macro variables

Variable	Default	Instructions
#AUILOAD	AUI.IBMTAPE.SAUILOAD	Change the default value to point to the location of the SAUILOAD for IBM Guardium S-TAP for IMS.
#AUIIMOD	AUI.IBMTAPE.SAUIIMOD	Change the default value to point to the location of the SAUIIMOD for IBM Guardium S-TAP for IMS.
#AUISAMP	AUI.IBMTAPE.SAUISAMP	Change the default value to point to the location of the SAUISAMP data set, or copy of that data set where you will be performing the configuration and customization edits.
#AUICONFG	AUICONFG	Change the default value to point to the member name in the configuration file that you want to use.

Parent topic: Planning your configuration and customizing your environment

Job cards for the sample JCL in the SAMPLIB

Some JCL members included with the product SAMPLIB have a filler card for the job card.

A valid job card conforming to your site's JCL standards must be provided before submitting any of the JCL.
Parent topic: Planning your configuration and customizing your environment

Setting up z/OS log streams

IBM Guardium S-TAP for IMS uses the z/OS System Logger to funnel events from IMS online regions and DLI/DBB batch jobs to the DLI event processor (AUIA*STC* task). Both XCF based and DASD based log streams are supported.

Each agent requires two unique log streams:

- one log stream for DLI events generated by IMS Control regions
- one log stream for DLI events generated by DLI/DBB batch jobs

Log streams cannot be shared between agents. Each log stream name must be unique.

It is recommended that XCF based log streams be used whenever possible, because this type of log stream is accessible from any LPAR within a sysplex, and has performance benefits. For more information about log streams, refer to the IBM publication: *System Programmer's Guide to: z/OS System Logger*.

- **Log stream security**
  Verify the following conditions have been met to insure log stream security.
- **XCF-based log streams**
  The advantages of using XCF-based log streams, as opposed to DASD-based log streams, include accessibility from any LPAR within the sysplex, and improved performance.
- **DASD-based log streams**
  This section provides rules and information about DASD-based log streams. Using DASD-based log streams limits auditing by the agent to the LPAR within which the agent is started. IMS Control regions and IMS DLI/DBB batch jobs that run on other LPARS will not be audited.

Parent topic: Planning your configuration and customizing your environment

Log stream security

Verify the following conditions have been met to insure log stream security.

Important:

- The USERID your IMS online control region runs under must have WRITE access to the log stream.
- If DLI/DBB batch jobs runs under a common USERID, that USERID must have WRITE permission to the log stream.
- The USERID under which the DLI Event Collector (AUIA*STC* task) executes must have READ/WRITE access to the log streams.
- If individual users are permitted to run DLI/DBB batch jobs under their own USERID, a universal access of WRITE is recommended for the log stream.

Parent topic: Setting up z/OS log streams

XCF-based log streams

The advantages of using XCF-based log streams, as opposed to DASD-based log streams, include accessibility from any LPAR within the sysplex, and improved performance.

AUILSTR1

Two JCL members in the SAUISAMP product data set are included to assist in the definition of XCF-based log streams.

This JCL is used to define the XCF structures to a CFRM policy needed by the log streams used by the DLI/DBB batch and IMS online control regions. Detailed instructions are in the comments of the JCL.
Note: The addition of structures to a CFRM policy are cumulative, and the execution of this JCL without consideration to previously defined structures within the CFRM policy result in the loss of existing CFRM structure definitions. It is highly recommended that a systems programmer customize and submit this JCL.

There are two DEFINE STRUCTURE sections for this JCL: one for the batch structure, and one for the online structure. The following values must be customized for the batch structure:

The name of the batch structure
    (NAME(batch_struc_name))
The coupling facility used to contain the structure
    (PREFLIST(cfname))

The following values must be customized for the online structure:

The name of the online structure
    (NAME(online_struc_name))
The coupling facility used to contain the structure
    (PREFLIST(cfname))

Do not change any other values, such as SIZE, INITSIZE, and ALLOWAUTOALT without carefully considering the impact that your changes will have on performance and data integrity.

Note:

- AUILSTR1 must run successfully before proceeding.
- When auditing in a large test or production environment, the INITSIZE and SIZE parameters can be increased to a higher value (example: 49200) for improved throughput.

AUILSTR2

This JCL is used to add the XCF based log streams to a LOGR policy used by the IMS Control region and DLI/DBB batch jobs. Detailed instructions are in the comments of the JCL.
Note: The addition of structures to a CFRM policy are cumulative, and the execution of this JCL without consideration to previously defined structures within the CFRM policy result in the loss of existing CFRM structure definitions. It is highly recommended that a systems programmer customize and submit this JCL.

There are two DEFINE STRUCTURE sections for this JCL: one for the batch structure and log stream, and one for the online structure.

Values that must be customized for IMS Batch processing include:
DEFINE STRUCTURE values:

The name of the batch structure (from AUILSTR1)
(NAME(batch_struc_name))

The name of this log stream is used as input to the Batch DLI Log Stream Name field when defining log streams to the agent. Use the LOG_STREAM_DLIB keyword of the configuration member that is specified by the AUICONFG DD statement of the agent (AUIA*STC*) JCL. The LOGSNUM, MAXBUFSIZE and AVGBUFSIZE should not be changed from the default values.

The name of the batch structure (from AUILSTR1)
(STRUCTNAME(batch_struc_name))
The selection of the Staging data set classes
(STG_DATACLAS, STG_MGMTCLAS, and STG_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates a staging data set for the log stream. The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of these parameters.

The selection of offload data set classes
(LS_DATACLAS, LS_MGMTCLAS, and LS_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates an offload data set for the log stream. The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of these parameters.

The size of the Batch Log stream DASD data sets
(STG_SIZE)
Note: This can be removed if the STG_DATACLAS value is specified.

The allocation/size of the offload data sets
(LS_SIZE(13500))

The default value is 13500 (the number of 4K blocks). The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of this size. When auditing in a large test or production environment, a value of 40500 might improve throughput.

The High level qualifier of the offload and staging data sets
(HLQ or EHLQ)

The HLQ and EHLQ are mutually exclusive and only one can be used. Other parameters found in the batch structure and online log stream definition might have a do not change comment. These parameters contain the recommended values and should not be altered without careful consideration of the impact of changes to log stream performance and data integrity. The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations of each potential parameter.

You must customize the following values for online structure and log stream processing:

DEFINE STRUCTURE values:

The name of the online structure (from AUILSTR1)
(NAME(online_struc_name))

The LOGSNUM, MAXBUFSIZE and AVGBUFSIZE should not be changed from the default values.
DEFINE LOGSTREAM values:

The name of the log-stream
(NAME(online_logstream_name))

The name of this log stream is used as input to the Online DLI Log Stream Name field when defining log streams to the agent. Use the LOG_STREAM_DLIO keyword of the configuration member specified by AUICONFG DD statement of the agent (AUIA*STC*) JCL.

The name of the online structure (from AUILSTR1)
(STRUCTNAME(online_struc_name))
The selection of the Staging data set classes
(STG_DATACLAS, STG_MGMTCLAS, and STG_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates a staging data set for the log stream. The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations of each potential parameter.

The size of the ONLINE Log stream DASD data sets
(STG_SIZE)
Note: This can be removed if the STG_DATACLAS value is specified.

The selection of offload data set classes
(LS_DATACLAS, LS_MGMTCLAS, and LS_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates an offload data set for the log stream. The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations of each potential parameter.

The allocation/size of the offload data sets
(LS_SIZE(13500))

The default value is 13500 (the number of 4K blocks). The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of this size. When auditing in a large test or production environment, a value of 40500 might improve throughput.

The High level qualifier of the offload and staging data sets
(HLQ or EHLQ)

The HLQ and EHLQ are mutually exclusive and only one can be used. Other parameters found in the batch structure and online log stream definition might have a do not change comment. These parameters contain the recommended values and should not be altered without careful consideration of the impact of changes to log stream performance and data integrity. The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations of each potential parameter.
Parent topic: Setting up z/OS log streams

DASD-based log streams

This section provides rules and information about DASD-based log streams. Using DASD-based log streams limits auditing by the agent to the LPAR within which the agent is started. IMS Control regions and IMS DLI/DBB batch jobs that run on other LPARS will not be audited.

DASD-based logs streams can only be accessed from one LPAR at a time. Any IMS Online Control regions and DLI/DBB batch jobs to be audited must run on the same LPAR as the agent runs on.

One JCL member in the SAUISAMP product data is included to assist in the definition of DASD-based log streams.

AUILSTR3

This JCL is used to add the DASD based log streams to a LOGR policy used by the IMS Control region and DLI/DBB batch jobs. Detailed instructions can be found within the comments of the JCL.
Note: It is highly recommended that a systems programmer customize and submit this JCL.
There are two DEFINE STRUCTURES sections to this JCL: one for the batch structure, and one for the online structure. Values which must be customized for IMS batch log stream processing are as follows:
DEFINE LOGSTREAM values:

The name of the log-stream
(NAME(batch_logstream_name))

The name of this log stream is used as input to the Batch DLI Log Stream Name field when defining log streams to the agent. Use the LOG_STREAM_DLIO keyword of the configuration member specified by AUICONFG DD statement of the agent (AUIA*STC*) JCL.

The selection of the Staging data set classes
(STG_DATACLAS, STG_MGMTCLAS and STG_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates a staging data set for the log stream. Other parameters found in the batch structure and online log stream definition might have a do not change comment. These parameters contain the recommended values and should not be altered without careful consideration of the impact of changes to log stream performance and data integrity. For more information, the IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of these parameters, and can be found on the IBM Information Center.

The selection of offload data set classes
(LS_DATACLAS, LS_MGMTCLAS and LS_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates an offload data set for the log stream. For more information, the IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of these parameters, and can be found on the IBM Information Center.

The size of the Batch Log stream DASD data sets
(STG_SIZE)
Note: This can be removed if the STG_DATACLAS value is specified.

The allocation/size of the offload data sets
(LS_SIZE(13500))

A value of 13500 (the number of 4K blocks) is the default/supplied value. For more information, the publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of this size, and can be found on the IBM Information Center.

The High level qualifier of the offload and staging data sets
(HLQ or EHLQ)

The HLQ and EHLQ are mutually exclusive and only one can be used. For more information, the IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations of each potential parameter, and can be found on the IBM Information Center.

Values which must be customized for IMS ONLINE processing include the following:

DEFINE LOGSTREAM values:

The name of the log-stream
(NAME(online_logstream_name))

The name of this log stream is used as input to the Online DLI Log Stream Name field when defining log streams to the agent using the Guardium user interface.

The selection of the Staging data set classes

(STG_DATACLAS, STG_MGMTCLAS, and STG_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates a staging data set for the log stream. For more information, the IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of these parameters, and can be found on the IBM Information Center.

The size of the ONLINE Log stream DASD data sets
(STG_SIZE)
Note: This can be removed if the STG_DATACLAS value is specified.

The selection of offload data set classes
(LS_DATACLAS, LS_MGMTCLAS, and LS_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates an offload data set for the log stream. For more information, the publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of these parameters, and can be found on the IBM Information Center.

The allocation/size of the offload data sets
(LS_SIZE(13500))

A value of 13500 (the number of 4K blocks) is the default/supplied value. For more information, the publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of this size, and can be found on the IBM Information Center.

The High level qualifier of the offload and staging data sets
(HLQ or EHLQ)

The HLQ and EHLQ are mutually exclusive and only one can be used. Other parameters found in the batch structure and online log stream definition might have a do not change comment. These parameters contain the recommended values and should not be altered without careful consideration of the impact of changes to log stream performance and data integrity. For more information, the publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations of each potential parameter, and can be found on the IBM Knowledge Center
Parent topic: Setting up z/OS log streams

Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent

This section describes the information necessary for configuring the agent.

The agent has a primary agent address space that runs as a started task (AUIA*STC*) and multiple secondary address spaces (AUIF*STC*, the SMF collector, AUIL*STC*, the IMS log collector, AUIU*STC*, the common storage utility) that are automatically started and stopped by the primary address space.

The agent primary address space reads the configuration file specified by the AUICONFG DD statement in the AUIA*STC* JCL, and passes the appropriate configuration information to the associated AUIF*STC* and AUIL*STC* tasks. The AUIU*STC* JCL requires the same configuration file to be specified as was specified for the AUIA*STC* task. Use the AUICONFG DD statement to specify the configuration file.

The SAUISAMP member AUICONFG provides a sample configuration that can be used by the agent primary address space started task.

Refer to the following instructions about the AUICONFG data set or the instructions in the data sets to complete the next steps.

Note:

- The data set must be edited using the EBCDIC encoding (1047 CCSID).
- It is recommended that you make a copy of the AUICONFG from SAUISAMP and customize it for use by a given agent.

- **Customizing the agent by using agent parameter keywords**
  Use agent parameter keywords to customize the agent. The agent configuration file provides the parameters that can be customized. The parameters that do not have a default value must be specified before you start the agent started task.
- **Agent configuration**
  The IP addresses of the IBM Guardium system appliances are specified using the SAUISAMP data set AUICONFG member using the APPLIANCE_SERVER and APPLIANCE_SERVER_FAILOVER_[1-5] keywords.
- **Customizing the agent JCL**
  The SAUISAMP member AUIA*STC* provides a sample JCL that can be used for the agent started task. This topic describes how to customize the JCL.
- **Starting and stopping the agent**
  Start the agent by issuing the command /S AUIASTC from the SDSF command line. The primary agent address space starts the AUIF*STC* address spaces. One or more instances of AUIL*STC* might also be started, depending on the list of active collections.
- **Agent security considerations**
  The user ID of the agent started tasks (the primary and the secondary started tasks) should have the necessary RACF® profiles for reading the configuration member contents.
- **Modifying the frequency of AUIJ012I messages**
  You can modify how frequently the agent provides a count of DLI calls (from the default of every 10K DLI calls to a value of your choice, 10K – 999K, 1M – 10M.)

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

Customizing the agent by using agent parameter keywords

Use agent parameter keywords to customize the agent. The agent configuration file provides the parameters that can be customized. The parameters that do not have a default value must be specified before you start the agent started task.

How to use the agent parameters

- Use the AUICONFG DD statement to reference these parameters with the agent JCL (AUIA*STC*) and Memory Management secondary address space JCL (AUIU*STC*).
- The AUICONFG DD can be used in other agent secondary address space JCLs (AUIF*STC* and AUIL*STC*).
- Define the data set (DSORG=PS) or data set member (DSORG=PDS|PDS/E) that contains these parameters as RECFM=FB LREL=80.

- Specify only one keyword and parameter per line.
- An asterisk (*) or hyphen (-) in column one indicates that the line is a comment.
- Characters in column 72 and beyond are ignored.

Required parameters

The following parameters must be manually configured:

- APPLIANCE_SERVER
- LOG_STREAM_DLIB
- LOG_STREAM_DLIO
- SMF_DSN_MASK
- SMF_SPILL_FILE

All available agent parameters

ADS_SHM_ID

Required: No
Default: None
Description: This keyword is optional when only one agent exists in a sysplex environment. If more than one agent exists, the configuration file for each agent should have this keyword specified with a unique integer with a value of 100000 - 999999 specified as its parameter. This keyword identifies a shared memory segment that is specific to each agent.
Note:

- This keyword must be used in combination with ADS_LISTENER_PORT.
- If you specify this keyword, you must add an //AUICONFG DD statement to the AUIF*STC* and AUIL*STC* address space JCLs. This DD statement should point to the same data set and member as the agent AUIA*STC* and AUIU*STC* JCLs to enable communication between all participating address spaces.

Syntax: ADS_SHM_ID*(Shared_Memory_label)*
Example: ADS_SHM_ID(100010)

ADS_LISTENER_PORT

Required: No
Default: 39987
Description: This keyword is optional when only one agent exists in a sysplex environment. If more than one agent exists, the configuration file for each agent should have this keyword specified with a unique port number specified. This keyword identifies an agent-specific communications port between the agent (AUIA*STC*) and the agent secondary address spaces (AUIF*STC*, AUIL*STC*). Valid port numbers are 1 - 65535. Check with your network administrator for a list of ports available for this use.
Note:

- This keyword must be used in combination with ADS_SHM_ID.
- If you specify this keyword, you must add an //AUICONFG DD statement to the AUIF*STC* and AUIL*STC* address space JCLs. This DD statement should point to the same data set and member as the agent AUIA*STC* and AUIU*STC* JCLs to enable communication between all participating address spaces.

Syntax: ADS_LISTENER_PORT*(port_number)*
Example: ADS_LISTENER_PORT(16055)

APPLIANCE_SERVER

Required: Yes
Default: None
Description: The host name or IP address (in dotted decimal notation, for example: 1.2.3.4) of the IBM Guardium system to which the agent (AUIA*STC*) should connect.
Note: This parameter must be correctly configured to enable a connection to the IBM Guardium system. This value can contain up to 128 characters.
Syntax: APPLIANCE_SERVER*(hostname|IP_address)*
Example:

```
APPLIANCE_SERVER(wal-vm-guardium20)
APPLIANCE_SERVER(192.168.2.205)
```

APPLIANCE_SERVER_[1-5]

Required: No
Default: None
Description: Enables alternative host names or TCP/IP addresses to be used for multistream Guardium appliance destinations or failover recovery processing. Up to five alternative host names or TCP/IP addresses are supported.
To specify one or more entries, include this parameter with a numeric suffix from 1 - 5. Provide a unique host name or TCP/IP address for each entry.
Valid values are any valid host name or TCP/IP address.
Note:

- The use of this keyword does not eliminate the need for the APPLIANCE_SERVER keyword.
- The APPLIANCE_SERVER_LIST parameter designates how this parameter is used.
- If used in combination, this parameter overrides the APPLIANCE _SERVER_[MULTI_STREAM|FAILOVER|HOT_FAILOVER]_[1-5] parameter.

Syntax:

```
APPLIANCE_SERVER_n(hostname|IP_addr)
```

where *n* can be 1, 2, 3, 4, or 5.
Example:

```
APPLIANCE_SERVER_1(nwt-vm-guardium3)
APPLIANCE_SERVER_1(192.168.2.205)
```

APPLIANCE_SERVER_[MULTI_STREAM|FAILOVER|HOT_FAILOVER]_[1-5]

Required: No

Default: None
Description: The host name or IP address (in dotted decimal notation, for example: 1.2.3.4) of the IBM Guardium system for the IBM Guardium S-TAP for IMS agent to use to stream to multiple Guardium appliance destinations or for failover processing. This value can contain up to 128 characters.
Note:

- The use of this keyword does not eliminate the need for the APPLIANCE_SERVER keyword.
- If this parameter, or the APPLIANCE_SERVER_[1-5] parameter, is not detected at startup, then neither failover nor hot failover processing is activated.
- The APPLIANCE_SERVER_LIST parameter designates how this parameter is used.
- If used in combination, this parameter is overridden by the APPLIANCE_SERVER_[1-5] parameter.

Syntax:

```
APPLIANCE_SERVER_[MULTI_STREAM|FAILOVER|HOT_FAILOVER]_n(hostname|IP_address)
```

where *n* can be 1, 2, 3, 4, or 5.
Example:

```
APPLIANCE_SERVER_MULTI_STREAM_1(wal-vm-guardium20)
APPLIANCE_SERVER_FAILOVER_1(nwt-vm-guardium8)
APPLIANCE_SERVER_HOT_FAILOVER_1(wal-vm-guardium16)
APPLIANCE_SERVER_MULTI_STREAM_1(192.168.2.201)
APPLIANCE_SERVER_FAILOVER_1(192.168.2.202)
APPLIANCE_SERVER_HOT_FAILOVER_1(192.168.2.203)
```

APPLIANCE_SERVER_LIST(MULTI_STREAM|FAILOVER|HOT_FAILOVER)
Required: No
Default: FAILOVER
Description: Set APPLIANCE_SERVER_LIST to *MULTI_STREAM* for a Guardium appliance connection to be established for each server that is identified by the APPLIANCE_SERVER_MULTI_STREAM_n parameter.

- If a connection is lost, S-TAP audit events continue to transmit over the remaining appliance connection.
- Lost connections are retried at regular intervals that are determined by multiplying the APPLIANCE_CONNECT_RETRY_COUNT by the APPLIANCE_PING_RATE.

Set APPLIANCE_SERVER_LIST to *FAILOVER* for one Guardium appliance connection to be active at a time.

- If the connection to the primary appliance is lost, a failover action occurs, which results in an attempt to connect to the next available server. The next available server is identified by the APPLIANCE_SERVER_FAILOVER_n parameter. The agent attempts to connect to subsequent Guardium systems, beginning with APPLIANCE_SERVER_FAILOVER_1 and ending with APPLIANCE_SERVER_FAILOVER_5.
- After a failover action occurs, the connection to the primary server is retried at regular intervals that are determined by multiplying the APPLIANCE_CONNECT_RETRY_COUNT by the APPLIANCE_PING_RATE.

Set APPLIANCE_SERVER_LIST to *HOT_FAILOVER* to cause connection types for each connected Guardium appliance identified by the APPLIANCE_SERVER_HOT_FAILOVER_n parameter to be kept active by pings.

- You must specify the primary Guardium appliance by using the APPLIANCE_SERVER parameter.
- If the primary Guardium appliance becomes unavailable and failover occurs, *HOT_FAILOVER* maintains the activity of the primary appliance policy.

With any setting of APPLIANCE_SERVER_LIST, if all connections fail, and a spill file is specified (parameter OUTAGE_SPILLAREA_SIZE), events are buffered to the spill file until a connection becomes available. If no spill file is specified, and all connections are lost, data loss occurs.
The default is *FAILOVER*.

APPLIANCE_PORT
Required: No
Default: 16022
Valid ports: 16022 or 16023
Description: The IP port number of the IBM Guardium system to which the IBM Guardium S-TAP for IMS agent should connect. This parameter must be correctly configured to enable a connection to the IBM Guardium system. If port 16023 is used, encryption support is required for the connection to the appliance.
Note: Specifying this keyword and parameter designates the port on which the IBM Guardium system is listening to the S-TAP. The port is dedicated to the IP address of the appliance. Port 16022 or 16023 can also be in use on z/OS by another application.
Syntax: APPLIANCE_PORT*(port_number)*
Example: APPLIANCE_PORT(16022)

APPLIANCE_PING_RATE
Required: No
Default: 5
Description: Specifies the interval time between accesses to the IBM Guardium system to prevent timeout disconnections during idle periods. The value is in number of seconds.
Syntax: APPLIANCE_PING_RATE*(ping_interval)*
Example: APPLIANCE_PING_RATE(5)

APPLIANCE_NETWORK_REQUEST_TIMEOUT
Required: No
Default: 500
Description: Specifies a value in milliseconds of time to wait for the completion of a network communication request to send or receive. A value of 0 results in no timeout period. Range: 0 or 500 - 12000.
Syntax: APPLIANCE_NETWORK_REQUEST_TIMEOUT*(milliseconds)*
Example: APPLIANCE_NETWORK_REQUEST_TIMEOUT(500)

AUIU_EXCLUDE_LPAR
Required: No
Default: None
Description: Specifies a list of LPAR names (one to eight characters) in a SYSPLEX environment where the Common Storage Management Utility (AUIU*STC*) should not be scheduled. Multiple AUIU_EXCLUDE_LPAR statements can be specified to allow for LPAR name strings that are longer than 53 bytes.
Note: Use this keyword with caution. DLI calls run on the excluded LPARS are not audited.
With the exception of the LPAR where the agent resides, all LPARS can be excluded by using the option *ALL in place of an LPAR name.
Syntax: AUIU_EXCLUDE_LPAR(*list_of_lpars*)

Example: AUIU_EXCLUDE_LPAR(RS21,MYLPAR,YOURLPAR) or AUIU_EXCLUDE_LPAR(*ALL)

AUIU_PROC_NAME

Required: No

Default: AUIU*STC*

Description: Specifies the PROCLIB member name that contains the Common Storage Management Utility JCL. This JCL is supplied as member name AUIU*STC* in the sample library (AUISAMP). If multiple agents are used within a sysplex, each agent requires a separate JCL for each AUIU*STC* address space.

Syntax: AUIU_PROC_NAME*(auiu_mbr_name)*

Example: AUIU_PROC_NAME(AUIUV1013)

DISPLAY_IMSMSG_DLIB(Y|N)

Required: No

Default: N

Description: Controls the output of informational messages AUIJ255I, AUIJ256I, AUIJ257I, and AUIJ258I in the AUILOG output DD of the AUIA*STC* agent address space. These messages are generated from data that is produced by the IMS DLI/DB batch jobs, and is passed to the agent from the DLIB z/OS log stream.

The default setting, *N*, prevents these messages from being written to the AUILOG DD.

Specify *Y* for these messages to be written to the AUILOG DD.

Syntax: DISPLAY_IMSMSG_DLIB*(Y|N)*

Example: DISPLAY_IMSMSG_DLIB(Y)

DISPLAY_IMSMSG_DLIO(Y|N)

Required: No

Default: N

Description: Controls the output of informational messages AUIJ255I, AUIJ256I, AUIJ257I, and AUIJ258I in the AUILOG output DD of the AUIA*STC* agent address space. These messages are generated from data that is produced by the IMS Control Region and passed to the agent from the DLIO z/OS log stream.

The default setting, *N*, prevents these messages from being written to the AUILOG DD.

Specify *Y* for these messages to be written to the AUILOG DD.

Syntax: DISPLAY_IMSMSG_DLIO*(Y|N)*

Example: DISPLAY_IMSMSG_DLIO(Y)

DLIFREQ

Required: No

Default: 100K

Description: Enables you to customize the number of DLI calls that are sent to the Guardium appliance before message AUIJ012I (providing a count of the number of events sent to appliance) is issued.

The count can be represented in thousands (K) or millions (M). Valid values are 10K – 999K and 1 – 10M.

Syntax: DLIFREQ*(100K)*

Example: DLIFREQ(100K)

FORCE_LOG_LIMITED

Required: No

Default: N

Description: Enables you to force limited audit logging by removing sensitive information (such as IMS segment data and concatenated key values) from data that is sent to the Guardium appliance by the S-TAP.

Specify *Y* to restrict sensitive data from being sent to the Guardium appliance.

Syntax: FORCE_LOG_LIMITED*(Y|N)*

Example: FORCE_LOG_LIMITED(N)

IMSL_AUDIT_LEVELS

Required: No

Default: ALL

Description: Specifies the events to be audited from those that are found using the IMS Archive Log task (AUIL*STC*) for each IMS instance under control of this agent. A specification other than `ALL` limits auditing to the events you specify.

For example, if you specify `USERS`, then all audited IMS instances under the agent report user signons and signoffs. If you specify `ALL`, you can use the Guardium interface to specify further limitations on what is audited for each audited IMS subsystem.

Table 1. IMSL_AUDIT_LEVELS audit parameters and events.

Parameter	Audited event
ALL	All events are audited (default)
CTL_STRT	IMS control region stops and starts
USERS	User signon and signoff
DBOPN	Database opens and closes
DB_PSB	DBDDUMP, DB/PSB START/STOP/LOCK/UNLOCK

Syntax: IMSL_AUDIT_LEVELS*(ALL|CTL_STRT|USERS|DBOPN|DB_PSB)*

Example: IMSL_AUDIT_LEVELS(ALL)

IMSL_CYCLE_INTERVAL

Required: No

Default: 15

Description: Specifies the frequency (in minutes) that the IMS Archive Log task (AUIL*STC*) checks the RECON data sets for new IMS SLDS (System Log Data Sets) to process. This value should correspond to the frequency at which IMS generates SLDS data sets during a normal workload. For example, if IMS SLDS are produced every 20 minutes, the IMSL_CYCLE_INTERVAL should be set to 20. A value of 0 (zero) can be specified to instruct the agent not start the AUIL*STC* task for any IMS subsystem that the agent controls. Valid parameters are 0 – 1440.

Syntax: IMSL_CYCLE_INTERVAL*(time_in_minutes)*

Example: IMSL_CYCLE_INTERVAL(45)

IMSL_ID_PREFIX

Required: No
Default: None
Description: Allows the partial customization of the 8-byte ID that is used when starting the AUILSTC task.
When this keyword is not used, the string *AAAAAAAA* is used for the first AUILSTC task to be started. Subsequent started AUILSTC tasks cause the ALPHA string to be incrementally increased by one character until the value of *ZZZZZZZZ* is reached. When *ZZZZZZZZ* is reached, the string is reset to *AAAAAAAA* when the agent (AUIASTC) is stopped and restarted.
When this keyword is used, the specified prefix (up to 6 bytes) is used, while the remaining two to seven characters are incrementally increased in the manner previously described. This enables a constant value (the specified prefix) to be used, alongside a wildcard character, when you are defining the ID to the TCP/IP security package to permit access to TCP/IP ports.
Note: The first character of the keyword must be an alphabetic character.
Syntax: IMSL_ID_PREFIX*(your_prefix)*
Example: IMSL_ID_PREFIX(MYPFX)
The example IMSL_ID_PREFIX(MYPFX) results in a generated AUILSTC ID of *MYPFXAAA -- MYPFXZZZ*.

IMSL_PROC_NAME
Required: No
Default: AUIL*STC*
Description: Specifies the PROCLIB member name that contains the IMS Archive Log JCL. This JCL is supplied as member name AUIL*STC* in the sample library (AUISAMP). If multiple agents are used within a sysplex, each agent requires a separate JCL for each AUIL*STC* address space.
Syntax: IMSL_PROC_NAME*(auil_mbr_name)*
Example: IMSL_PROC_NAME(AUILV1013)

IMSL_SLDS_SRCH
Required: No
Default: 30
Description: This keyword can be used to limit the number of days within which the IMS log reader (AUILxxxx) will search for IMS system log data sets (SLDS) to process.

- If an IMS checkpoint does not exist for the SLDS reader, AUILxxxx will search for IMS SLDS that were created on the current day and for *x* days prior to the current day (where *x* is the value that you set for this parameter).
- If an IMS checkpoint that is set for the SLDS reader exceeds the number of days between the current day and the value that you set for this parameter, then the IMS checkpoint will be used as the starting point for IMS SLDS to be read and processed.
- If you set a value of *0* (zero) for this parameter, then only the current day's IMS SLDS will be processed. Also, IMS SLDS that were migrated from a hierarchical storage manager product will not be recalled for processing.
  Note: If you set a value of *0* (zero) for this parameter, AUILxxxx processing will omit any IMS SLDS that were created on the previous day. This can cause data to be missed if, for example, the AUILxxxx task is run at 12:05 AM. IMS SLDS that were created prior to midnight will not be recognized as being within the current day, and thus will not be processed.

Syntax: IMSL_SLDS_SRCH*(number_of_days)*
Example: IMSL_SLDS_SRCH(15)

LOG_FILTER(I/E)
Required: No
Default: I (include)
Description: Specifies whether to include or exclude messages that have been specified by the LOG_FILTER_MSG_ID parameter.

- The default value, `I`, allows only the specified message IDs to be included in the AUILOG output stream. Message IDs that are not specified by the LOG_FILTER_MSG_ID(messages) parameter will be suppressed. The default value should be used unless there is a specific business need to suppress messages.
- The optional value, `E`, suppresses the specified message IDs from the AUILOG output stream.
  Tip: The `E` value should only be used if the LOG_FILTER_MSG_ID keyword has been customized to suppress specific messages. Do not use the optional value (E) in conjunction with LOG_FILTER_MSG_ID(*) unless you want to prevent all messages from being written to the AUILOG output stream. Suppressing all messages is not recommended.

Syntax: LOG_FILTER*(include/exclude)*
Example: LOG_FILTER(E)

LOG_FILTER_MSG_ID(messages)
Required: No
Default: * (all messages)
Description: Can be used in conjunction with the LOG_FILTER(I/E) parameter to suppress specific messages from being written to the AUILOG output stream.
Tip: The LOG_FILTER_MSG_ID(*) default value should only be used with the LOG_FILTER(I) default value. Do not specify LOG_FILTER(E) in conjunction with LOG_FILTER_MSG_ID(*) unless you want to prevent all messages from being written to the AUILOG output stream. Suppressing all messages is not recommended.
Syntax: LOG_FILTER_MSG_ID*(id1,id2,id3...)*
Example: LOG_FILTER_MSG_ID(AUIZ014W)

LOG_PORT_SCAN_START
Required: No
Default: 41500
Description: Specifies the first communications port number to be checked for availability to be used for internal message logging communications. Use this keyword if environmental conditions dictate that a sequential scan and test of ports from port numbers 41500 - 65535 should not be performed. You can override the starting port with a port of your choice. This keyword and parameter can be used with the LOG_PORT_SCAN_COUNT keyword to limit the ports that are scanned to a specific range.
Syntax: LOG_PORT_SCAN_START*(port_number)*
Example: LOG_PORT_SCAN_START(41500)

LOG_PORT_SCAN_COUNT
Required: No
Default: 10
Description: This keyword can be used in conjunction with the LOG_PORT_SCAN_START keyword to limit number of the ports that are scanned and tested for availability. The integer specified (1 - 65535) represents the number of ports that should be scanned. If the port number specified by the LOG_PORT_SCAN_START value plus the LOG_PORT_SCAN_COUNT value exceeds 65535, the scan terminates at port 65535.
Syntax: LOG_PORT_SCAN_COUNT*(number_of_ports)*
Example: LOG_PORT_SCAN_COUNT(1000)

LOG_STREAM_DLIB
Required: Yes
Default: None

Description: This required keyword is used to specify the z/OS System Logger log stream to stream audited events from DLI DBB batch jobs. The value should be the BATCH_LOGSTREAM_NAME value specified as the DEFINE LOGSTREAM NAME parameter of the AUILSTR2 or AUILSTR3 JCLs.
Syntax: LOG_STREAM_DLIB*(log_stream_name)*
Example: LOG_STREAM_DLIB(AUI_BATCH_LOG_STREAM)

LOG_STREAM_DLIO

Required: Yes
Default: None
Description: This required keyword is used to specify the z/OS System Logger log stream to be used to stream audited events from IMS Control Regions. The value should be the ONLINE_LOGSTREAM_NAME value specified as the DEFINE_LOGSTREAM_NAME parameter of the AUILSTR2 or AUILSTR3 JCLs.
Syntax: LOG_STREAM_DLIO*(log_stream_name)*
Example: LOG_STREAM_DLIO(AUI_ONLINE_LOG_STREAM)

LOOPBACK_ADDRESS

Required: No
Default: LOCALHOST
Description: Specifies the loopback host or IP address that is used for communications between the agent and the agent secondary address spaces. For most network configurations, the default value of `LOCALHOST` can be used. If `LOCALHOST` cannot be resolved on your system, consult your network specialist for the correct loopback mnemonic or IP address to be used.
Syntax: LOOPBACK_ADDRESS*(hostname|IP_address)*
Example: LOOPBACK_ADDRESS(LOCALHOST)

LPAR_MONITOR_INTERVAL

Required: No
Default: 5
Description: Specifies the frequency (in minutes) for the agent to request a list of LPARs that are active within the SYSPLEX. Schedule the Common Storage Management Utility (AUIU*STC*) tasks on any LPAR coming online to the SYSPLEX. Valid parameters are integers between 1 and 60.
Syntax: LPAR_MONITOR_INTERVAL*(minutes)*
Example: LPAR_MONITOR_INTERVAL(5)

MESSAGE_LOG_LEVEL

Required: No
Default: I
Description: Controls the amount of output log information that is generated by the agent.

Table 2. Message severity codes and descriptions.

Message severity code	Description
I	Includes all log messages
W	Includes all log messages with a warning severity or higher
E	Includes all log messages with an error severity or higher
O	Instructs the agent not to log error messages
S	Includes all log messages with a severe error code

Syntax: MESSAGE_LOG_LEVEL*(I|W|E|O|S)*
Example: MESSAGE_LOG_LEVEL(I)

OUTAGE_SPILL_AREA_SIZE

Required: No
Default: 0
Description: Determines the maximum amount of memory in megabytes to be allocated for the retention of audit data in the event of a IBM Guardium system connection outage. A value of `0`, or the absence of this keyword, disables spill area support. The maximum value permitted as a parameter is 1024.
Syntax: OUTAGE_SPILL_AREA_SIZE*(memory_size)*
Example: OUTAGE_SPILL_AREA_SIZE(15)

POLICY_READ_INTERVAL

Required: No
Default: 5
Description: Determines the frequency in seconds that the connection to the IBM Guardium system checks for changes to the installed policies that are used to determine audited event collection.
Syntax: POLICY_READ_INTERVAL*(time_in_seconds)*
Example: POLICY_READ_INTERVAL(5)

STAP_STREAM_EVENTS

Required: No
Default: Y
Description: Specifies whether events will be streamed to the IBM Guardium system. The default value, *Y*, enables streaming. Specify *N* to disable streaming and enable Simulation mode.
Syntax: STAP_STREAM_EVENTS*(Y|N)*
Example: STAP_STREAM_EVENTS(Y)

PREFER_IPV4_STACK

Required: No

Default: N

Description: If set to Y, this parameter causes a request to be issued to the Domain Name Server (DNS) for an IPV4 address for the hostname that is specified in the APPLIANCE_SERVER parameter:

- The DNS lookup request for an IPV4 address is attempted. If an IPV4 address is defined for the hostname, the DNS will respond with the value that will be used to connect to the Guardium appliance.
- If only an IPV6 address is defined at the DNS, then the DNS will respond with the IPV6 address that will be used to connect to the Guardium appliance.
- If both IPV4 and IPV6 addresses are defined at the Guardium appliance, the DNS will respond with both addresses, and the IPV4 address will be used to connect to the appliance.

If this parameter is set to N or omitted from configuration, a request for an IPV6 address is issued to the DNS for the hostname that is specified by the APPLIANCE_SERVER parameter:

- The DNS lookup request for an IPV6 address is attempted. If an IPV6 address is defined for the hostname, the DNS will respond with the value that will be used to connect to the Guardium appliance.
- If only an IPV4 address is defined at the DNS, then the DNS will respond with the IPV4 address that will be used to connect to the Guardium appliance.
- If both IPV4 and IPV6 addresses are defined at the Guardium appliance, the DNS will respond with both addresses, and the IPV4 address will be used to connect to the appliance.

Note: Whether or not this parameter is used, if the address returned from the DNS is not valid for the hostname, it will result in failure to connect to the appliance, and the IBM Guardium S-TAP for IMS started task will terminate.

Syntax:

```
PREFER_IPV4_STACK(Y|N)
```

Example:

```
PREFER_IVP4_STACK(Y)
```

SMF_AUDIT_LEVELS

Required: No

Default: ALL

Description: Specifies which events to audit of those found using the SMF task (AUIF*STC*). A specification other than `ALL` limits the events to be audited to the events you specify. For example, if `DELETE` is specified, then all audited IMS instances under the agent would only be capable of reporting data set `DELETE` events. If `ALL` is specified, you can further limits what is audited for each audited IMS subsystem, using the user interface.

Table 3. SMF_AUDIT_LEVELS audit parameters and events

Parameter	Audited event
ALL	All events are audited (default)
UPDATE	Data sets opened with UPDATE access
DELETE	Data sets deleted
READ	Data sets opened with READ access
CREATE	Data sets created
ALTER	Data sets opened with ALTER access
RACF®	RACF violations on data sets

Syntax: SMF_AUDIT_LEVELS*(ALL|UPDATE|DELETE|READ|CREATE|ALTER|RACF)*

Example: SMF_AUDIT_LEVELS(ALL)

SMF_CYCLE_INTERVAL

Required: No

Default: 300

Description: Specifies the frequency (in minutes) that the SMF task (AUIFSTC) checks the z/OS catalog for new data sets, which meet the specified data set masks, using the SMF_DSN_MASK keyword. This value should correspond to the frequency at which your z/OS system swaps SMF logging VSAM files (sometimes known as SMF MANX|MANY) during a normal workday. For example, if the SMF logging files are swapped every 8 hours, the SMF_CYCLE_INTERVAL should be set to `480` (8 hours * 60 minutes). A value of zero can be specified to indicate that the agent should not start the AUIF*STC* task and SMF auditing should not be performed. Valid parameters are 0 – 1440.

Syntax: SMF_CYCLE_INTERVAL*(time_in_minutes)*

Example: SMF_CYCLE_INTERVAL(45)

SMF_DSN_MASK_[1-10]

Required: Yes

Default: None

Description: At least one instance of this keyword is required (SMF_DSN_MASK_1). This keyword provides a data set mask used to query the z/OS catalog for sequential format data sets containing SMF data offloaded from the SMF log-files (MANX|MANY) using the IFASMFDP program. These sequential files can be the original files created when offloading the MANX|MANY files, or a copy of these sequential files created by customizing and running AUISMFDF and AUISMFDP jobs located in the product sample data set. In most environments, only one SMF_DSN_MASK would be specified, but up to 10 are allowed.

Table 4. Masking character rules

Character	Rule
%	Indicates that only one alphanumeric or national character can occupy that position
%%%	Indicates that more than one character can be substituted, with the number of substitution characters being equal to the number of percent signs specified.

Example 1: specifying a GDG data set in the mask: If the AUISMFDP job has been customized to produce a GDG data set as the SORTOUT DD output data sets, you can choose to specify the fully qualified GDG base name in the mask for system name field. For example, A.B.C. IBM Guardium S-TAP for IMS uses catalog services to determine the names of all cataloged GDG entries under this name, for example:

- A.B.C.G0001V00
- A.B.C.G0002V00
- A.B.C.G0003V00

Example 2: specifying a data set name explicitly: Provide the generation and version values as a mask. For example, A.B.C.G%%%%V%%. IBM Guardium S-TAP for IMS uses catalog services to determine the names of all cataloged data sets that match this mask, for example:

- A.B.C.G0021V00
- A.B.C.G0022V00
- A.B.C.G0023V00

Example 3: specifying a DSN using a DATE/TIME naming convention: If you have customized the AUISMFDP job to produce a data set name that contains date and time values as qualifiers within the data set name as the SORTOUT DD output data sets, you can specify the data set name using a string of percent signs within the date and time qualifier names. For example: HLQ.D%%%%%%.T%%%%%%.SMFDATA. IBM Guardium S-TAP for IMS uses catalog services to determine the names of all cataloged data sets matching the mask, for example:

- HLQ.D091122.T131000.SMFDATA
- HLQ.D091123.T131100.SMFDATA
- HLQ.D091124.T131200.SMFDATA

Note: The percent (%) wildcard character should only be specified for the numeric characters of the generation and version node of GDG data sets, or as the numeric characters of date or time nodes of the SMF dataset.
Syntax: SMF_DSN_MASK_1*(SMF.DUMP.DSN)*
Example:

```
SMF_DSN_MASK_1(AUI.SMF.DUMP.COPY)
SMF_DSN_MASK_2(AUI.SMF.DUMP.GDG.G%%%%V%%)
SMF_DSN_MASK_3(AUI.SMF.D%%%%%%.T%%%%%%.COPY)
```

SMF_EVENT_EXPIRY
Required: No
Default: 5
Description: Specifies the number of days that incomplete SMF events should be retained in the SMF spill file. Incomplete SMF events are audited events that have not yet received the associated SMF Type 30 record, which indicates that the step/job is complete, and contains information that is needed to complete the reporting of the event. When an event exceeds the expiration date, it is flagged as incomplete, sent to the IBM Guardium system, and removed from the SMF spill file. The valid range is 1 to 180 days.
Syntax: SMF_EVENT_EXPIRY*(days)*
Example: SMF_EVENT_EXPIRY(5)

SMF_PROC_NAME
Required: No
Default: AUIFSTC
Description: Specifies the PROCLIB member name that contains the SMF secondary address space JCL. This JCL is supplied as member name AUIF*STC* in the sample library (AUISAMP). If multiple agents are used within a sysplex, each agent requires a separate JCL for each AUIF*STC* address space.
Syntax: SMF_PROC_NAME*(auif_mbr_name)*\
Example: SMF_PROC_NAME(AUIFV91)

SMF_SELF_AUDIT
Required: No
Default: N
Description: Indicates whether to audit the accesses of IMS data sets that are used by the product to determine the names of IMS artifacts to be audited. Examples of IMS data sets that can be accessed include RECON data sets and IMS archived logs (SLDS). A value of `N` indicates that these accesses should not be audited. A value of `Y` indicates that these data sets should be considered for auditing.
Syntax: SMF_SELF_AUDIT*(N|Y)*
Example: SMF_SELF_AUDIT(N)

SMF_SPILL_FILE
Required: Yes
Default: None
Description: Specifies the DSN of a sequential format fixed block data set with a LRECL of 300. This data set is used to store incomplete audited SMF events. Incomplete audited SMF events are events triggered by SMF records that have yet to encounter an SMF Type 30 record, indicating the step or job has completed. The AUIFUSPL member of the SAUISAMP data set provides an example of the allocation specifications for this data set.
Syntax: SMF_SPILL_FILE*(dsn)*
Example: SMF_SPILL_FILE(AUI.V1013.SPILL)

TCPIP_BUFFER_SIZE
Required: No
Default: 32768
Description: Specifies the size of an internal buffer that is used to hold audited events in preparation of the TCP/IP send to the IBM Guardium system, and specifies the size of the TCP/IP buffer. In most environments, the size of this buffer should not be changed
Syntax: TCPIP_BUFFER_SIZE*(buffer_size)*
Example: TCPIP_BUFFER_SIZE(32768)

TRACE_CONFIG
Required: No
Default: ON
Description: TRACE_CONFIG(ON) enables IBM Guardium S-TAP for IMS configuration values to display by default at agent startup. You can optionally use this keyword to disable the IBM Guardium S-TAP for IMS configuration value display. To prevent the displayed report of agent configuration parameters during agent startup, specify TRACE_CONFIG(OFF).
Syntax: TRACE_CONFIG*(ON|OFF)*
Example: TRACE_CONFIG(OFF)

WTO_MSG
Required: No
Default: None
Description: Allows a user to request that specific informational, warning, or error messages written to the AUILOG DD statement of the agent (AUIA*STC*) or agent secondary address spaces (AUIF*STC*, AUIL*STC* or AUIU*STC*) also be written to the Operator Console (WTO). This enables these messages to be recognized by an automated operations tool, or provides higher operator visibility for these messages and allows appropriate action to be taken. Each message requires a separate keyword, and each keyword must be specified on a separate line.
Syntax: WTO_MSG*(msgnumber)*
Example:

```
WTO_MSG(AUIJ011I)
WTO_MSG(AUIL607W)
WTO_MSG(AUIY006E)
```

XML_ECHO_AUILOG(Y|N)
Required: No
Default: N
Description: Indicates that when an audit policy is installed on a IBM Guardium system appliance, its corresponding XML is to be echoed to the AUILOG DD. If there is more than one policy installed on the agent, the XML of each policy is echoed. If all installed policies are subsequently uninstalled, then the echoed XML reflects that there are no installed policies. For more information about echoed XML statements, see XML statement definitions.
Syntax: XML_ECHO_AUILOG(Y|N)
Example: XML_ECHO_AUILOG(Y)

XML_ECHO_DATASET(Data_Set_Name[,Cylinders])
Required: No
Default: None
Description:

Indicates that when the IBM Guardium system installs an audit policy, its corresponding XML is echoed to a data set (specified by the data set name value in this parameter). If there is more than one policy installed on the agent, the XML of each is echoed. If all installed policies are subsequently uninstalled, then the echoed XML reflects that there are no installed policies. The XML will not be echoed when the installed policy is already active, is being reinstalled, and there have been no changes to the policy.

If *Data_Set_Name* is intended to be a Generation Data Group (GDG), then it must be set as the GDG base name. The agent checks the system catalog to determine whether *Data_Set_Name* exists and whether or not it is a GDG base name.

Data_Set_Name can contain z/OS system symbols such as &SYSNAME. To determine the names of the system symbols that are currently defined to the system, issue the DISPLAY SYMBOLS command to the system console.

If *Data_Set_Name* does not exist, and there is no GDG base defined in this name, the agent allocates the data set as non-GDG. If *Data_Set_Name* is a regular physical sequential data set (non-GDG based) and does exist, the agent allocates space for the *Cylinders* keyword when the agent is restarted.

Cylinders defaults to 1 and can range from 1 – 10.
Syntax: XML_ECHO_DATASET*(&Data_Set_Name[,Cylinders])*
Example: XML_ECHO_DATASET(AUIAGENT.ECHO.XML.GDG.BASE,2)

ZIIP_AGENT_DLI
Required: No
Default: N
Description: Indicates that the following agent processes should be zIIP capable: agent reads of audited events from the z/OS System Logger log streams, formatting of these events into protobuf style messages, and sending of these messages to the IBM Guardium system using TCP/IP.
Note: Use of the zIIP depends on the presence of a zIIP on the LPAR where the agent is running, as well as use of the Workload Management Service Policies. For more information about zIIP, see the topic on Customizing IMS to use a System z® Integrated Information Processor (zIIP).
Syntax: ZIIP_AGENT_DLI*(Y|N)*
Example: ZIIP_AGENT_DLI(Y)

Parent topic: Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent

Related reference

- Customizing IMS to use a System z Integrated Information Processor (zIIP)

Agent configuration

The IP addresses of the IBM Guardium system appliances are specified using the SAUISAMP data set AUICONFG member using the APPLIANCE_SERVER and APPLIANCE_SERVER_FAILOVER_[1-5] keywords.

See Providing Guardium system failover for more information.
Parent topic: Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent

Customizing the agent JCL

The SAUISAMP member AUIA*STC* provides a sample JCL that can be used for the agent started task. This topic describes how to customize the JCL.

Before you begin

In environments where multiple agents connect to a common IBM Guardium system or appliance, the z/OS agent started task names (AUIA*STC*, AUIL*STC*, AUIF*STC*) must be unique. Unique started task names enable the IBM Guardium S-TAP for IMS policies that are pushed from the IBM Guardium system to be attributed to, and monitored by, the correct z/OS agent.

Procedure

1. Edit SAUISAMP members AUIA*STC*, AUIF*STC*, AUIL*STC* and AUIU*STC* by running the ISPF edit macro.
   See Planning your configuration and customizing your environment for more details.
2. Modify the CFG=AUI.V100.AGTCFG(AUICONFG) in AUIA*STC* to specify the location of the customized configuration data set for the agent created in the previous section.
3. Optional: You can rename the AUIA*STC* member to any character name that is valid for started tasks in your environment.
4. Optional: You can rename the AUIF*STC*, AUIL*STC*, and AUIU*STC*. AUIF*STC*, AUIL*STC*, and AUIU*STC* names should match the values of the IMSL_PROC_NAME, SMF_PROC_NAME, and AUIU_PROC_NAME keywords that you supply in the configuration file.
5. Copy the AUIA*STC*, AUIF*STC*, AUIL*STC* and AUIU*STC* members to the PROCLIB for the site.
   Contact the z/OS systems programmer to determine the location of the PROCLIB.
   Note: APF authorization of the AUILOAD file is required for each of these members before they are started.

Parent topic: Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent

Starting and stopping the agent

Start the agent by issuing the command /S AUIASTC from the SDSF command line. The primary agent address space starts the AUIF*STC* address spaces. One or more instances of AUIL*STC* might also be started, depending on the list of active collections.

Stop the agent by issuing the command /STOP AUIASTC, or /MODIFY AUIASTC,STOP, from the SDSF command line. The primary agent address space then stops all the secondary address spaces that are online, and shuts down. Depending on the load, and the activity in the other secondary address spaces, the shut down process can take time. Monitor the AUILOG DD of the primary address space AUIA*STC* for informational messages on the status of the secondary address spaces.

Parent topic: Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent

Agent security considerations

The user ID of the agent started tasks (the primary and the secondary started tasks) should have the necessary RACF® profiles for reading the configuration member contents.

Important: Contact your system administrator to ensure that localhost is resolving to 127.0.0.1 (loopback address). The TCP/IP communication between the agent and the secondary address spaces relies on this resolution. If this is not possible at your site, use the *loop-back-address* element in the AUICONFG sample library member to avoid localhost resolution by specifying the loopback IP address directly, or by specifying an appropriate host name that resolves to the loopback address.
Parent topic: Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent

Modifying the frequency of AUIJ012I messages

You can modify how frequently the agent provides a count of DLI calls (from the default of every 10K DLI calls to a value of your choice, 10K – 999K, 1M – 10M.)

Use the agent parameter keyword DLIFREQ to modify the frequency of AUIJ012I messages, or issue the command /MODIFY AGENT,SET CONFIG DLIFREQ *aaaK* | *bbM*, from the SDSF command line.

Parent topic: Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent

Setting up an IMS environment for auditing

This section describes how to customize IMS environments to capture DLI calls, including customizing IMS catalogued procedures, coexisting with other DFSFLGX0 and DFSISVI0 exit routines, customizing IMS to use a zIIP, copying common load modules from SAUILOAD to SAUIIMOD, and the security considerations related to IMS processing.

- **Security considerations for IMS processing**
  IBM Guardium S-TAP for IMS does not impose any additional RACF® or other security restrictions on IMS assets during IMS processing. However, the IMS control region and any DLI/DBB batch jobs being executed, must have UPDATE authority to the z/OS system log streams you have defined for use by IBM Guardium S-TAP for IMS.
- **Customizing IMS environments to capture DLI calls**
  For IBM Guardium S-TAP for IMS to report on IMS database accesses, it needs to be sensitive to IMS DL/I calls. Use the following sections to establish proper set-up of the relationship between your IMS online and batch environments and IBM Guardium S-TAP for IMS.
- **Customizing IMS cataloged procedures**
  For IBM Guardium S-TAP for IMS to monitor DL/I calls from IMS online Transactions, BMPs and DLI/DBB batch jobs, the IMS Control region and DLI/DBB batch jobs require access to these IBM Guardium S-TAP for IMS programs.
- **Coexisting with other DFSFLGX0 and DFSISVI0 exit routines**
  IBM Guardium S-TAP for IMS provides product-specific DFSFLGX0 (IMS Logger) and DFSISVI0 (IMS Batch) exits to enable the product to report on IMS DL/I call activity. In some IMS environments, user requirements or third-party vendor products also require the use of these exits. IBM Guardium S-TAP for IMS can accommodate the use of multiple DFSFLGX0 and DFSISVI0 exit routines.
- **Defining LOGWRT exits**
  Use the EXITDEF parameter in the USER_EXITS section of the DFSDFxxx IMS PROCLIB member to define LOGWRT exits to be used by your IMS subsystem.
- **Customizing IMS to use a System z Integrated Information Processor (zIIP)**
  IBM Guardium S-TAP for IMS allows you to configure an IMS control region to prepare specific auditing functions for execution on a System z® Integrated Information Processor (zIIP). Execution on a zIIP is governed by the Workload Management software on your appliance, as well as the workload already assigned to the zIIP.
- **Copying common load modules from SAUILOAD to SAUIIMOD**
  After the initial SMP/E installation of IBM Guardium S-TAP for IMS, copy common load modules from the SAUILOAD to SAUIIMOD data set using the modules described in this topic.
- **Configuring APP_EVENT support**
  IBM Guardium S-TAP for IMS allows IMS DLI application programs to store user information on the IBM Guardium system. This enables your user data to be linked with DLI DB calls that are made from within the same application checkpoint, unit-of-work, or commit. APP_EVENT calls are linked to audited DLI calls by subsystem ID, application sequence number, and number of commits within a schedule. Follow these steps to install and configure a new IMS database, named AUIAPPEV, to be used for this purpose.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

Security considerations for IMS processing

IBM Guardium S-TAP for IMS does not impose any additional RACF® or other security restrictions on IMS assets during IMS processing. However, the IMS control region and any DLI/DBB batch jobs being executed, must have UPDATE authority to the z/OS system log streams you have defined for use by IBM Guardium S-TAP for IMS.

Parent topic: Setting up an IMS environment for auditing

Customizing IMS environments to capture DLI calls

For IBM Guardium S-TAP for IMS to report on IMS database accesses, it needs to be sensitive to IMS DL/I calls. Use the following sections to establish proper set-up of the relationship between your IMS online and batch environments and IBM Guardium S-TAP for IMS.

Note: The IBM Guardium S-TAP for IMS programs that are used to communicate with your IMS environments are found in the SAUIIMOD data set, and are created during product installation.
Parent topic: Setting up an IMS environment for auditing

Customizing IMS cataloged procedures

For IBM Guardium S-TAP for IMS to monitor DL/I calls from IMS online Transactions, BMPs and DLI/DBB batch jobs, the IMS Control region and DLI/DBB batch jobs require access to these IBM Guardium S-TAP for IMS programs.

The IBM Guardium S-TAP for IMS programs that must be accessed reside in the SAUIIMOD installation data set. The preferred method of installing IBM Guardium S-TAP for IMS into your IMS environment is to copy the entire contents of the SAUIIMOD data set into your IMS RESLIB (IMS.SDFSRESL) data set.

If copying IBM Guardium S-TAP for IMS programs into your IMS RESLIB is not possible, then the SAUIIMOD data set must be included in your IMS control region JCL as the first data set of the STEPLIB DD concatenation. The SAUIIMOD data set must also be included as the first data set of the STEPLIB DD concatenation of the DLI batch cataloged procedure (DLIBATCH member of the IMS PROCLIB data set) and the DBB batch cataloged procedure (DBBBATCH member of the IMS PROCLIB data set).

Note:

- If the SAUIIMOD data set is included in any JCL, you must ensure that it is APF-authorized.
- IBM Guardium S-TAP for IMS provides and uses the DFSFLGX0 and DFSISIV0 IMS exits to establish communication with IMS services, however no customization of these exits is required.

Parent topic: Setting up an IMS environment for auditing

Coexisting with other DFSFLGX0 and DFSISVI0 exit routines

IBM Guardium S-TAP for IMS provides product-specific DFSFLGX0 (IMS Logger) and DFSISVI0 (IMS Batch) exits to enable the product to report on IMS DL/I call activity. In some IMS environments, user requirements or third-party vendor products also require the use of these exits. IBM Guardium S-TAP for IMS can accommodate the use of multiple DFSFLGX0 and DFSISVI0 exit routines.

Using IMS Tools Generic Exits

IMS Tools Generic Exits are a collection of components that provide common command and exit routine interfaces to support the operation of IMS tools in an IMS environment.

IBM Guardium S-TAP for IMS supports the protocols used by the IMS Tools Generic Exit product. You can define the IBM Guardium S-TAP for IMS copy of the DFSFLGX0 exit by either supplying IMS with a PROCLIB member using a BPE-style control statement, or by building a load module that contains the required information.

An example of the PROCLIB control statement follows:

```
EXITDEF(TYPE(LOGR) EXITNAME(AUIFLGX0) LOADLIB(AUI.SAUIIMOD))
```

See the IBM IMS Tools Generic Exit Reference Manual for Generic Logger Exit setup and usage.
Important: The IBM IMS Tools Generic Exit product does not support exit DFSISVI0.

Using IBM Guardium S-TAP for IMS exit cascading

For situations where the IBM IMS Tools Generic Exit is not available for use, IBM Guardium S-TAP for IMS provides a method of supporting two instances of the DFSFLGX0 and DFSISVI0 exits.

When loaded and run, the IBM Guardium S-TAP for IMS supplied program AUIFLGX0 (DFSFLGX0) and AUIISVI0 (DFSISIV0) determines from which DSN within the JOBLIB/STEPLIB concatenation it was loaded from. It then searches all subsequent DSNs within the JOBLIB/STEPLIB DD concatenation, looking for the next occurrence of the exit with the same name.

- If none are found, or it is determined that the IMS Tools Generic Exit product is involved in executing the exit, no cascading is done.
- If an exit is found, and it is determined that the exit found is in fact another instance of the IBM Guardium S-TAP for IMS exit (as could happen if the SAUIIMOD data set was specified multiple times in the JOBLIB/STEPLIB concatenation), the search will continue with the remainder of the DSNs in the concatenation.
- If a non-IBM Guardium S-TAP for IMS Exit is found, this new exit is loaded, and called with R13 pointing to the save area supplied by IMS. A new 512 byte user work area, obtained specifically for this exit instance, is then pointed to by the SXPLAWRK field of the IMS Standard User Exit Parameter List (DFSSXPL). This 512 byte work area is obtained when the first (or INIT) call is done; the work area address (in the SXLPAWRK field) and work area content are maintained for all subsequent calls.

Exit cascading restrictions

Note: These restrictions only apply when using the exit cascading feature, and not when using the IBM IMS Tools Generic Exit product.
The IBM Guardium S-TAP for IMS Exit (AUIFLGX0 or AUIISVI0) must be first in the JOBLIB/STEPLIB concatenation, unless the exit that exists in a prior DSN also has a method of cascading calls to other exits, and is capable of providing an IMS formatted area in R13 and the address of a unique, persistent 512 byte work area in the SXPLAWRK parameter list field to the AUIFLGX0 or AUIISVI0 program.

In a non-APF-authorized environment, such as when executing program DFSULTR0 or an IMS DLI/DBB batch program, the exit load module to be cascaded to must have an ALIAS, and the ALIAS must be appropriately either DFSFLGX0 or DFSISVI0, if the target exit module has the RENT or REUS attribute on.

Parent topic: Setting up an IMS environment for auditing

Defining LOGWRT exits

Use the EXITDEF parameter in the USER_EXITS section of the DFSDFxxx IMS PROCLIB member to define LOGWRT exits to be used by your IMS subsystem.

You must specify the exit name AUIFLGX0 in the list of LOGWRT exits to be used. This disables the cascading feature, which prevents other LOGWRT exits in the STEPLIB from being unintentionally invoked. You must include the SAUIIMOD load library in the IMS Control Region STEPLIB concatenation.

Example:

```
<SECTION=USER_EXITS>
EXITDEF=(TYPE=LOGWRT,EXITS=(AUIFLGX0))
```

Parent topic: Setting up an IMS environment for auditing

Customizing IMS to use a System z Integrated Information Processor (zIIP)

IBM Guardium S-TAP for IMS allows you to configure an IMS control region to prepare specific auditing functions for execution on a System z® Integrated Information Processor (zIIP). Execution on a zIIP is governed by the Workload Management software on your appliance, as well as the workload already assigned to the zIIP.

To use this feature, the LPAR on which the IMS Control region executes must have a zIIP installed. The IMS Control Region should also make use of the z/OS Workload Manager product. For more information on using z/OS Workload Manager with the IMS Control Region, see the *Workload Manager and IMS* section of the *IBM IMS System Administration* manual.

The following processes can be scheduled on a zIIP:

- Calling of the compiled filter to determine if the DLI event is to be audited, and if the segment concatenated key or segment data should be sent to the Guardium appliance.
- Movement of the audited DLI calls to a storage buffer used to hold audited data until a write to the z/OS System Logger log-stream can be executed
- Calling of the z/OS System Logger IXGWRITE, which moves the audited data from the buffer to the log-stream when the buffer fills, or a flush of the buffer is scheduled

To indicate that the IMS Control region should attempt to schedule these processes on the zIIP, a //AUIZIIP DD DUMMY DD statement should be added to the IMS Control Region JCL. When detected, the audit code produces the informational message AUII055I, indicating that zIIP processing will be attempted.

Warning messages AUII042W and AUII043W are issued if zIIP processing is requested when a zIIP is not available, and when IMS is not using Workload Manager. Error message AUII044E indicates that the request was rejected. In all instances where the attempt to use the zIIP has failed, audit processing continues without attempting to execute the audit code on the zIIP.

Parent topic: Setting up an IMS environment for auditing

Related reference

- Customizing the agent by using agent parameter keywords

Copying common load modules from SAUILOAD to SAUIIMOD

After the initial SMP/E installation of IBM Guardium S-TAP for IMS, copy common load modules from the SAUILOAD to SAUIIMOD data set using the modules described in this topic.

AUI$NAP
: Module used to trace data
Provided in the SAUILOAD data set
Also needed in the SAUIIMOD data set

AUICPMOD
: An SAUISMAP member
Performs a copy of the AUI$NAP module from the SAUILOAD to the SAUIIMOD data set
Should be customized and submitted after the initial SMP/E installation

Parent topic: Setting up an IMS environment for auditing

Configuring APP_EVENT support

IBM Guardium S-TAP for IMS allows IMS DLI application programs to store user information on the IBM Guardium system. This enables your user data to be linked with DLI DB calls that are made from within the same application checkpoint, unit-of-work, or commit. APP_EVENT calls are linked to audited DLI calls by subsystem ID, application sequence number, and number of commits within a schedule. Follow these steps to install and configure a new IMS database, named AUIAPPEV, to be used for this purpose.

Procedure

1. Perform a Database Descriptor Generator (DBD gen) for the AUIAPPEV database.
   An example of the DBD source to use is in member AUIAPPEV of the SAUISAMP data set.
2. Create a database data set for the AUIAPPEV database.
3. If appropriate for your site, register the DB and DDN to DBRC, specifying NOREOV if possible.
4. If appropriate for your site, create a dynamic allocation (MDA) member for the database data set.
5. Modify application program PSBs to include a PCB for the AUIAPPEV database.
   Use a PROCOPT of *G* and a KEYLENGTH of *0*.
6. If the APP_EVENT feature is to be used by an IMS Online system, perform an ACBGEN for DBD member AUIAPPEV and the modified PSBs.
7. Modify application programs to send APP_EVENT information using the AUIAPPEV PCB:
   a. In the 2000 byte I/O area, modify the application programs to include the information that you want to be sent to the appliance.
   b. Perform a DLI GET call by using the AUIAPPEV PCB.
      A DLI status code of blanks will be returned.

- **APP_EVENT examples**
  Examples of the AUIAPPEV database, a PSB with DBPCB for the AUIAPPEV database included, the Assembler language of an IMS DLI call, and a C program are provided here. These code samples are for example purposes only. There is no guarantee of the reliability, serviceability, or function of these programming examples.

Parent topic: Setting up an IMS environment for auditing

APP_EVENT examples

Examples of the AUIAPPEV database, a PSB with DBPCB for the AUIAPPEV database included, the Assembler language of an IMS DLI call, and a C program are provided here. These code samples are for example purposes only. There is no guarantee of the reliability, serviceability, or function of these programming examples.

AUIAPPEV database

The AUIAPPEV database is used to support the transmittal of environmental information from an application program to the Guardium appliance. The following is an example:

```
DBD                    NAME=AUIAPPEV,ACCESS=(HDAM,OSAM),RMNAME=(DFSHDC40,10,20)
DATASET                DD1=AUIAPPEV,SIZE=2048
SEGM       NAME=ROOT,PARENT=0,BYTES=2000
DBDGEN
FINISH
END
```

PSB with DBPCB for the AUIAPPEV database included

The following is an example of a PSB with DBPCB for the AUIAPPEV database included:

```
PCB             TYPE=DB,PROCOPT=A,KEYLEN=4,DBDNAME=AUEVOL01,  PCBNAME=ODBPCB1
SENSEG          NAME=ROOT,PARENT=0
PCB             TYPE=DB,PROCOPT=G,KEYLEN=0,DBDNAME=AUIAPPEV,  PCBNAME=APPEV01
SENSEG          NAME=ROOT,PARENT=0
PSBGEN          LANG=ASSEM,CMPAT=YES,PSBNAME=AUIPSBAV
END
```

Assembler language of an IMS DLI call

The following is an example in the Assembler language of an IMS DLI call that will send a string to the Guardium appliance:

```
MVC       IOAREA(20),=CL20'THIS IS AN APP_EVENT'    /Set APP_EVENT message
XC      PARM@(12*4),PARM@                           /Clear parameter area
LA       R1,GN                        /Addr of GN literal
ST             R1,PARM@+0                                    /Save in parmlist
L       R2,APPCB@                                            /Addr of AUIAPPEV PCB
ST      R2,PARM@+4                                  /Save in parmlist
LA      R1,IOAREA                                            /Addr of IOAREA
ST       R1,PARM@+8                  /Save in parmlist
OI      PARM@+8,X'80'           /Terminate parmlist
LA       R1,PARM@                 /Addr of parmlist
L       R15,DLI@                /Addr of ASMTDLI program
BASR    R14,R15                                               /Call ASMTDLI
```

C program

The following is an example of a C program:

```
#define    iopcb     (IO_PCB_TYPE *)(__pcblist)        /* I/O PCB */
#define    dbpcb     (PCB_STRUCT_8_TYPE *)(__pcblist)  /* DB PCB  */
#define    aepcb     (PCB_STRUCT_8_TYPE *)(__pcblist)  /* AUIAPPEV DB PCB  */

int  rc = 0;
const static char GU = "GU  ";

struct {
  char output 2000¨;
} iodata ;


....
....

/* create a APP_EVENT */
sprintf(iodata.output, "THIS IS AN APP_EVENT");
rc = ctdli(GU, aepcb, &iodata);
```

Parent topic: Configuring APP_EVENT support

Using agent configuration keywords to customize auditing

Some agent configuration keywords must be used for the product to function. You can also use agent configuration keywords for optional auditing specifications.

Required keywords

The following keywords must be set for the product to function:

APPLIANCE_SERVER
: This is the host name, or IP address, of the IBM Guardium system to which the agent should connect.

LOG_STREAM_DLIO
: This is the log stream name for online DLI calls.

LOG_STREAM_DLIB
: This is the log stream name for batch DLI calls.

You can also audit accesses to database-related data sets using SMF records. To audit accesses to IMS data sets that occur outside of IMS services, use the following keywords:

SMF_SPILL_FILE

This is the data set name.

SMF_DSN_MASK_1
This is the data set mask value.

Optional keywords

To set the following optional specifications, use the keyword that is listed. More information about each specification is provided, following this list.

Enabling Simulation mode
STAP_STREAM_EVENTS(N)

Restricting IMS segment and concatenated key data from being sent to the Guardium appliance
FORCE_LOG_LIMITED(Y)

Using multiple SMF data set masks
SMF_DSN_MASK_2 through SMF_DSN_MASK_10

Disabling SMF auditing at the agent level
SMF_CYCLE_INTERVAL(0)
Note: If SMF_CYCLE_INTERVAL(0) is specified, no additional SMF configuration parameters are required.

Controlling the frequency of SMF z/OS catalog queries
SMF_CYCLE_INTERVAL(time in minutes)

Changing the retention period of incomplete SMF events
SMF_EVENT_EXPIRY(number of days)

Changing the name of the SMF address space JCL
SMF_PROC_NAME(new name)

Auditing IMS data set access
SMF_SELF_AUDIT(Y)

Changing the type of events audited using SMF records
SMF_AUDIT_LEVELS(ALL|UPDATE|DELETE|READ|CREATE|ALTER|RACF)

Overriding the range of ports used for address space communications
LOG_PORT_SCAN_START(41501), LOG_PORT_SCAN_COUNT(24003)

Requesting specific agent messages to be issued to the operator console
WTO_MSG(AUIF507E), WTO_MSG(AUIT013I)

Determining the context of APPLIANCE_SERVER_[1-5] or APPLIANCE_SERVER_[FAILOVER|MULTI_STREAM|HOT_FAILOVER]_[1-5]
APPLIANCE_SERVER_LIST(FAILOVER|MULTI_STREAM|HOT_FAILOVER)

Providing Guardium system failover support
APPLIANCE_SERVER_FAILOVER_[1-5](IP address or host name)

Providing Guardium system multistream support
APPLIANCE_SERVER_MULTI_STREAM_[1-5](IP address or host name)

Providing Guardium system hot failover support
APPLIANCE_SERVER_HOT_FAILOVER_[1-5](IP address or host name)

Providing a spill area for short term outages
OUTAGE_SPILL_AREA_SIZE(megabytes)

Disabling IMS SLDS auditing at the agent level
IMSL_CYCLE_INTERVAL(0)
Note: If IMSL_CYCLE_INTERVAL(0) is specified, no additional IMSL configuration parameters are required.

Controlling the frequency IMS System Log Data Sets are allocated and read
IMSL_CYCLE_INTERVAL(time in minutes)

Changing the name of the IMSL address space JCL
IMSL_PROC_NAME(new name)

Changing the type of events audited using IMS SLDS records
IMSL_AUDIT_LEVELS(ALL|CTL_STRT|USERS|DBOPN|DB_PSB)

Changing the name of the Common Memory Management address space JCL
AUIU_PROC_NAME(new name)

Excluding DLI calls occurring on specific LPARS from being audited
AUIU_EXCLUDE_LPAR(lpar1, lpar2...lpar9)

Running more than one agent in a SYSPLEX
ADS_SHM_ID(100010), ADS_LISTENER_PORT(16055)

Removing Segment data and Concatenated Key values from audited data at the agent level
FORCE_LOG_LIMITED(Y)

Using the System z Integrated Information Processor (zIIP)
ZIIP_AGENT_DLI

Viewing AUI messages that are produced by the IMS Control regions in the AUI agent log
DISPLAY_IMSMSG_DLIO(N|Y)

Viewing AUI messages produced by the IMS DLI/DBB batch jobs in the AUI agent log
DISPLAY_IMSMSG_DLIB(N|Y)

Restricting auditing to specific IMS systems when multiple IMSs share RECON data sets
IMSNAME_EQ_IMSSSID(N|Y)

Enabling/Disabling the IBM Guardium S-TAP for IMS configuration value display at agent startup
TRACE_CONFIG(ON|OFF)

Setting the number of days within which AUILxxxx will process IMS system log data sets (SLDS)
IMSL_SLDS_SRCH(number of days)

- **Simulation mode**
  Simulation mode enables you to simulate agent processing. IBM Guardium S-TAP for IMS uses various z/OS MVS system services to gather audit data and move it to the agent address space. The agent address space evaluates this data according to the specified policy, and transmits the audit record to the Guardium appliance by using TCP/IP. To assess the impact on MVS processing, use the STAP_STREAM_EVENTS parameter to simulate data collection.
- **Specifying multiple SMF data set masks**
  You can use the SMF_DSN_MASK keyword to specify up to nine additional SMF data set masks.
- **Disabling SMF auditing at the agent level**
  You can use the SMF_CYCLE_INTERVAL keyword to disable SMF auditing at the agent level.

- **Controlling the frequency of SMF z/OS catalog queries**
  You can change the frequency of SMF z/OS catalog queries by using the SMF_CYCLE_INTERVAL keyword to specify a value in minutes:
- **Changing the retention period of incomplete SMF events**
  By default, incomplete SMF events will be retained in your SMF spill data set for 5 days. You can change this time range by specifying the SMF_EVENT_EXPIRY keyword:
- **Changing the name of the SMF address space JCL**
  To change the name of the AUIFS*TC* JCL member name, use the SMF_PROC_NAME keyword to change AUIFSTC to a name of your choice:
- **Auditing IMS data set access**
  To obtain a report of IMS artifact access, use the SMF_SELF_AUDIT keyword.
- **Changing the types of events that are audited using SMF records**
  Use the SMF_AUDIT_LEVELS keyword to indicate a list of events to be audited, instead of collecting all event types.
- **Using alternate RECON data sets for SMF and SLDS processing**
  You can optionally use copies of the IMS RECON data sets when processing SMF (AUIF*STC*) and IMS SLDS (AUIL*STC*) data instead of using the live RECON data sets.
- **Overriding the range of ports used for communication between address spaces**
  You can set the available port scan starting point and limit the number of ports to check for availability.
- **Overriding the TCP/IP DNS resolver table**
  IBM Guardium S-TAP for IMS uses TCP/IP as a host path for intra- and inter-address space communication of information such as collection policy details and address space status updates. To receive information from an AUIU*STC*_(Common Storage Management Utility) address space running on a different LPAR in the sysplex, the AUIA*STC*_(agent) address space must determine its own physical IP address and make it known to AUIU*STC*.
- **Specifying agent messages to issue to the operator console**
  You can use the WTO_MSG keyword to specify the messages to issue to the operator console.
- **Creating a spill area for short-term outages**
  Use the OUTAGE_SPILL_AREA_SIZE keyword and parameter to indicate the size in megabytes to allocate for the spill area.
- **Disabling IMS SLDS auditing at the agent level**
  You can turn off the auditing process that uses IMS SLDS records by specifying the IMSL_CYCLE_INTERVAL keyword with a value of zero.
- **Controlling the frequency with which IMS System Log Data Sets are allocated and read**
  You can specify the frequency of IMS RECON data set queries by specifying the IMSL_CYCLE_INTERVAL keyword.
- **Changing the name of the IMSL address space JCL**
  To change the JCL member name AUIL*STC*, use the IMSL_PROC_NAME keyword.
- **Changing the types of events audited using IMS SLDS records**
  To audit some, instead of all event types, you can specify each event type to be audited by using the IMSL_AUDIT_LEVELS keyword.
- **Changing the name of the Common Memory Management address space JCL**
  Use the AUIU_PROC_NAME keyword to change the member name from AUIU*STC* to a name of your choice.
- **Excluding DLI calls on specific LPARS from being audited**
  To stop the transmission of the AUIU*STC* address spaces to all LPARs, the AUIU_EXCLUDE_LPAR keyword can be used to exclude specific LPARS from the target list of eligible LPARS.
- **Running more than one agent in a SYSPLEX**
  If two or more IMS agents are running on one SYSPLEX, use the ADS_SHM_ID and ADS_LISTENER_PORT keywords to differentiate the shared memory segment and port for each agent environment.
- **Restricting auditing to specific IMS systems when multiple IMS systems share RECON data sets**
  If multiple unrelated IMS systems share RECON data sets, and you want to audit only on one or more specific IMS systems, use the keyword IMSNAME_EQ_IMSSSID(Y) to isolate auditing to the desired IMS system.
- **Using the System z Integrated Information Processor (zIIP)**
  You can use the System z® Integrated Information Processor (zIIP) when running IBM Guardium S-TAP for IMS Control region address space, and in the agent address space (AUIA*STC*). Use the ZIIP_AGENT_DLI keyword with the Y parameter to cause the agent to make a zIIP-enabled enclave SRB initialization attempt.
- **Using multiple Guardium systems**
  You can configure multiple Security Guardium systems for automatic failover. By configuring one or more backup systems, you ensure continuous auditing capability. This process is known as failover. You can also enable the streaming of audited data from one or more IBM Guardium S-TAP for IMS agents to up to 6 connected Security Guardium systems. This process is known as multistreaming.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

Simulation mode

Simulation mode enables you to simulate agent processing. IBM® Guardium® S-TAP® for IMS uses various z/OS MVS system services to gather audit data and move it to the agent address space. The agent address space evaluates this data according to the specified policy, and transmits the audit record to the Guardium appliance by using TCP/IP. To assess the impact on MVS processing, use the STAP_STREAM_EVENTS parameter to simulate data collection.

When STAP_STREAM_EVENTS is set to *N*, the parameter stops the agent TCP/IP data transmission process. The agent performs all data collection processes but does not send the audit record to the Guardium appliance.

Parent topic: Using agent configuration keywords to customize auditing

Specifying multiple SMF data set masks

You can use the SMF_DSN_MASK keyword to specify up to nine additional SMF data set masks.

Specifying multiple SMF data set masks

The naming conventions of some environments prohibit the use of a SMF_DSN_MASK_1 value, which allows all required data sets to be read. To audit accesses to database-related data sets from multiple LPARS of your SYSPLEX, you can specify up to nine additional data set mask values: SMF_DSN_MASK_2 through SMF_DSN_MASK_10.

Parent topic: Using agent configuration keywords to customize auditing

Disabling SMF auditing at the agent level

You can use the SMF_CYCLE_INTERVAL keyword to disable SMF auditing at the agent level.

For any IMS systems that are audited by this agent, you can disable audit access to IMS data sets that occur outside the use of IMS services. To do so, specify the following keyword with the value of zero: SMF_CYCLE_INTERVAL(0)

Specifying SMF_CYCLE_INTERVAL(0) turns off auditing process that uses SMF records. The agent address space (AUIA*STC*) will not start the SMF auditing address space (AUIF*STC*).

Parent topic: Using agent configuration keywords to customize auditing

Controlling the frequency of SMF z/OS catalog queries

You can change the frequency of SMF z/OS catalog queries by using the SMF_CYCLE_INTERVAL keyword to specify a value in minutes:

To determine if any new, unread data sets match the specified SMF_DSN_MASK_x values, the SMF processing address space (AUIF*STC*) periodically performs a query against the z/OS catalog, looking for data sets to process. By default, this query is performed when the AUIF*STC* task is started, and repeated every 300 minutes (5 hours). To change the default time value, use the keyword SMF_CYCLE_INTERVAL*(time in minutes)*. If you specify a time value of zero, the SMF auditing feature will be disabled.
Parent topic: Using agent configuration keywords to customize auditing

Changing the retention period of incomplete SMF events

By default, incomplete SMF events will be retained in your SMF spill data set for 5 days. You can change this time range by specifying the SMF_EVENT_EXPIRY keyword:

In some situations, such as a canceled job or end-of-memory events, a type 30 record is not produced for a step or job. To keep these types of records from filling your SMF spill data set, you can set a time limit in days to determine how long incomplete SMF records are retained. The default value is 5 days and can be changed by specifying the SMF_EVENT_EXPIRY keyword to indicate the number of days of your choice: SMF_EVENT_EXPIRY*(number of days)*.
Parent topic: Using agent configuration keywords to customize auditing

Changing the name of the SMF address space JCL

To change the name of the AUIF*STC* JCL member name, use the SMF_PROC_NAME keyword to change AUIFSTC to a name of your choice:

AUIF*STC* is the name of the JCL that provides auditing of data set accesses using SMF records. AUIF*STC* is provided in the product installation sample data set (SAUISAMP). If the name AUIF*STC* conflicts with your site's naming convention standards, or if more than one agent is being used, you can change the name of this JCL. Use the SMF_PROC_NAME keyword to change the member name from AUIF*STC* to a name of your choice: SMF_PROC_NAME*(new name)*.

Ensure that this JCL resides in a procedure data set (PROCLIB) that allows the z/OS START command S taskname to be used.

Parent topic: Using agent configuration keywords to customize auditing

Auditing IMS data set access

To obtain a report of IMS artifact access, use the SMF_SELF_AUDIT keyword.

IBM Guardium S-TAP for IMS reads the IMS RECON data sets and system log data sets produced by IMS (SLDS) to obtain IMS environment information, such as IMS artifact names. IMS artifact names determine the databases and data sets that are used to create audit information.

By default, IBM Guardium S-TAP for IMS does not report accesses of IMS artifacts. To obtain a report of these accesses, specify a value of Y using the SMF_SELF_AUDIT keyword: SMF_SELF_AUDIT*(Y)*.

Parent topic: Using agent configuration keywords to customize auditing

Changing the types of events that are audited using SMF records

Use the SMF_AUDIT_LEVELS keyword to indicate a list of events to be audited, instead of collecting all event types.

When auditing using SMF records is enabled, the default action is to provide auditing for all of the following accesses to data sets:

- Open events with READ access
- Open events with UPDATE/WRITE access
- Open events with ALTER access
- Data set DELETE events
- Data set CREATE events
- Access denied (RACF violation)

To specify some and not all of these events for auditing, you can specify each type of event to be audited by using the SMF_AUDIT_LEVELS keyword: SMF_AUDIT_LEVELS (*ALL*|*READ*|*UPDATE*|*DELETE*|*CREATE*|*ALTER*|*RACF*).
Remember: This keyword affects the SMF auditing level for all IMS subsystems controlled by this agent. If you do not include READ accesses in the SMF_AUDIT_LEVELS parameter, then no READ accesses will be reported for any of the IMS environments that are audited by using the agent.
Note: You can separate parameters for the collection of different event types. For example, to audit UPDATE and READ events, include the UPDATE and READ records as follows:

```
SMF_AUDIT_LEVELS(UPDATE)
SMF_AUDIT_LEVELS(READ)
```

instead of:

```
SMF_AUDIT_LEVELS(UPDATE|READ)
```

Parent topic: Using agent configuration keywords to customize auditing

Using alternate RECON data sets for SMF and SLDS processing

You can optionally use copies of the IMS RECON data sets when processing SMF (AUIF*STC*) and IMS SLDS (AUIL*STC*) data instead of using the live RECON data sets.

To use alternate RECON data sets for SMF and SLDS processing:

1. Add a //AUIARCN DD statement to the AUIF*STC* and AUIL*STC* JCLs that contain the name of the IMS system (as defined in the IMS Definition panel of the Guardium interface).
2. Add the alternate RECON data set names to be used when processing these two types of data sources.
   Note: Specifying alternate RECON data set names only affects AUIF*STC* and AUIL*STC* task processing. It has no effect on processing of any other tasks.

Use IDCAMS, or another VSAM-compatible method, to create cataloged, VSAM copies of your live RECON data sets.

The data set that is specified by the AUIARCN DD statement must be defined as Fixed Block (FB) with a record length of 80 bytes (LRECL=80), and it can be a PDS, PDS/E, or sequential file. The following guidelines apply:

- An asterisk (*) in column 1 indicates that the line is a comment.
- Keywords must start in column 1.
- No spaces are allowed within keywords and parameters.
- Multiple IMSNAME keywords can be specified in one AUIARCN file.
- At least one RECON data set must be included under each IMSNAME identifier.
- Alternate RECON data sets must be cataloged and in IMS format.

Table 1. IMSNAME and RECON data set values, defined:

Value	Purpose
IMSNAME=	Specifies the IMS to which the subsequent RECON1, 2, and 3 keywords pertain.
RECON1=	Specifies the alternate data set name to be used for RECON1.
RECON2=	Specifies the alternate data set name to be used for RECON2.
RECON3=	Specifies the alternate data set name to be used for RECON3.

Example:

```
IMSNAME=IMSV14
RECON1=IMSEA1.ALT.RECON1
RECON2=IMSEA1.ALT.RECON2
RECON3=IMSEA1.ALT.RECON3
*
IMSNAME=IMSV13
RECON1=IMSDA1.ALT.RECON1
RECON2=IMSDA1.ALT.RECON2
```

Parent topic: Using agent configuration keywords to customize auditing

Overriding the range of ports used for communication between address spaces

You can set the available port scan starting point and limit the number of ports to check for availability.

IBM Guardium S-TAP for IMS uses a communications port to pass messages between threads within each address space. The default port is 41500. If the address space determines that port 41500 is not available for use, all subsequent ports up to 65535 are examined, and the first available port is used.
Some installations have restrictions on which ports should be examined and used. Use the LOG_PORT_SCAN _START and LOG_PORT_SCAN_COUNT keywords to set the available port scan starting point and limit the number of ports to be checked for availability:

- LOG_PORT_SCAN_START(41501)
- LOG_PORT_SCAN_COUNT(24003)

The sum of the value of the SCAN_START port number plus the SCAN_COUNT should not exceed 65535.
Parent topic: Using agent configuration keywords to customize auditing

Overriding the TCP/IP DNS resolver table

IBM Guardium S-TAP for IMS uses TCP/IP as a host path for intra- and inter-address space communication of information such as collection policy details and address space status updates. To receive information from an AUIU*STC*_(Common Storage Management Utility) address space running on a different LPAR in the sysplex, the AUIA*STC*_(agent) address space must determine its own physical IP address and make it known to AUIU*STC*.

To determine its physical IP address, the IBM Guardium S-TAP for IMS agent uses the z/OS getaddrinfo function and passes it to the LPAR name specified in the CVTSNAME field of the z/OS CVT control block. The getaddrinfo function uses the DNS resolver table to map the agent's LPAR name to its physical IP address. The DNS resolver table should contain entries that associate each LPAR within the sysplex to its physical IP address. If there is no association found, the agent (AUIA*STC*) uses the z/OS gethostname and getaddrinfo services to obtain the physical IP address of its own LPAR; but the IP addresses of other LPARs in the sysplex cannot be determined. In that case, inter-address space communication is not possible and events that occur on other LPARs are not reported to the Guardium appliance. Similarly, inter-address space communications can fail if users of Dynamic Virtual IP Addressing (VIPA) attempt to associate multiple IP addresses to a single VIPA token.

To determine if the LPAR name, in the CVTSNAME field, is included in the DNS table:

1. Run the Rexx executable that is located in the SAUISAMP data set of member AUIPING.
2. If the ping is successful, the LPAR name is defined in the DNS table and no further action is required.
3. If the ping fails due to an unknown host error, the LPAR name was not found in the DNS table. Contact your network administrator to request the addition of the LPAR name and the associated IP address to the DNS table.

Network administrators can manually associate the LPAR name that is found in the z/OS CVTSNAME field with the name that is used in the DNS revolver table by including the AUIHOST DD statement file in all IMS S-TAP agent task address space JCLs.

cvts_lpar_name(*dns_name*)

Required if AUIHOST DD is specified.
Default: None.
Description: Translates the CVTSNAME to the name in the DNS table.

lpar_name
Found in the z/OS CVTSNAME field.
Use the AUIPING REXX exec found in the SAUISAMP data set to obtain that name.
The *lpar_name* value can be from 1 -- 8 bytes in length.

dns_name
Found in the DNS table that associates the LPAR with an IP address.
The DNS_NAME value must conform to the following z/OS TCP/IP HOSTNAME rules:

- Must contain 1 or more tokens separated by a period.
- Each token must be at least 1 character and less than 64 characters.
- Each token must start with a letter or number.
- Remaining characters in each token must be a letter, number, or hyphen.

Example: PRODA(SYSTEM_1)
wherein:

- *PRODA* is the LPAR name found in the CVTSNAME field of your z/OS system
- *SYSTEM_1* is the mnemonic used in your DNS table to relate this LPAR to a TCP/IP address.

The AUIHOST DD statement file must meet the following standards:

- It must be a sequential file, or a member of a Partitioned Data Set (PDS) or Extended Partitioned Data Set (PDSE).
- It must be defined with a Fixed Blocked (FB) Record Format (RECFM).
- It must have a Logical Record Length (LRECL) of 80 bytes.
- Commented lines can be indicated by an asterisk (*) in column one or by a slash-asterisk (/*) in columns one and two.
- It must contain all host definitions on one line.
- Up to 16 DNS names can be specified.

The following is an example of an AUIHOST DD statement file:

```
MYLPAR20(MYLPAR20.mycompany.com)
MYLPAR21(MYLPAR21.mycompany.com)
MYLPAR22(MYLPAR22.mycompany.com)
MYLPAR23(MYLPAR23.mycompany.com)
MYLPAR24(MYLPAR24.mycompany.com)
MYLPAR25(MYLPAR25.mycompany.com)
MYLPAR26(MYLPAR26.mycompany.com)
```

Parent topic: Using agent configuration keywords to customize auditing

Specifying agent messages to issue to the operator console

You can use the WTO_MSG keyword to specify the messages to issue to the operator console.

IBM Guardium S-TAP for IMS allows you to specify informational, warning, or error messages to be written to the operator console. This allows an automated operations product to take some predefined action or provide a higher level of operator visibility to these messages. You can use the WTO_MSG to specify which messages should be write-to-operated.

- WTO_MSG(AUIF507E)
- WTO_MSG(AUIT013I)

You can specify one message ID per WTO_MSG instance. Messages originating from the AUIA*STC*, AUIF*STC*, AUIL*STC*, and AUIU*STC* address spaces are supported.
Parent topic: Using agent configuration keywords to customize auditing

Creating a spill area for short-term outages

Use the OUTAGE_SPILL_AREA_SIZE keyword and parameter to indicate the size in megabytes to allocate for the spill area.

Short-term communication outages between the agent address spaces and the IBM Guardium system can be handled by using a z/OS data space spill area. Use of the spill area can prevent the loss of audited data by allowing the z/OS agent to save audited data until the connection to the IBM Guardium system is restored. The restoration of the communications link results in the flushing of the data space contents to the IBM Guardium system.

Use the OUTAGE_SPILL_AREA_SIZE keyword and parameter to indicate the size in megabytes to allocate for the spill area: OUTAGE_SPILL_AREA_SIZE*(megabytes)*. If you specify zero or omit this keyword, the spill area will not be allocated or used. The maximum value you can specify is 1024 MB.

Parent topic: Using agent configuration keywords to customize auditing

Disabling IMS SLDS auditing at the agent level

You can turn off the auditing process that uses IMS SLDS records by specifying the IMSL_CYCLE_INTERVAL keyword with a value of zero.

For any IMS systems to be audited by this agent, you can disable audit events that are determined by reading IMS System Log Data Sets (SLDS). To disable the auditing process that uses IMS SLDS records, specify the following keyword with the value of zero: IMSL_CYCLE_INTERVAL*(0)*. The agent address space (AUIA*STC*) will not start the IMS SLDS auditing address space (AUIL*STC*).

Parent topic: Using agent configuration keywords to customize auditing

Controlling the frequency with which IMS System Log Data Sets are allocated and read

You can specify the frequency of IMS RECON data set queries by specifying the IMSL_CYCLE_INTERVAL keyword.

For the product to determine if any new, unread IMS System Log Data Sets LDS data sets have been created by the IMS Online system, the IMSL processing address space (AUIL*STC*) periodically performs a query against the IMS RECON data sets, looking for new SLDS. This query is performed when the AUIL*STC* task is started, and then by default, every 15 minutes. The frequency can be changed by providing a value in minutes by using the IMSL_CYCLE_INTERVAL keyword: IMSL_CYCLE_INTERVAL*(time in minutes)*

A value of zero will cause the IMS SLDS auditing feature to be disabled.

Parent topic: Using agent configuration keywords to customize auditing

Changing the name of the IMSL address space JCL

To change the JCL member name AUIL*STC*, use the IMSL_PROC_NAME keyword.

AUIL*STC* is the name of the JCL that is used to audit data sets using IMS SLDS records. AUIL*STC* is provided in the product installation sample data set (SAUISAMP). If this name conflicts with your site's naming convention standards, or if more than one agent is being used, you can change the name of this JCL.

Use the IMSL_PROC_NAME keyword to change the member name from AUIL*STC* to a name of your choice: IMSL_PROC_NAME*(new name)*

Ensure that this new JCL is in a procedure data set (PROCLIB) that allows the z/OS START command S taskname to be used.

Parent topic: Using agent configuration keywords to customize auditing

Changing the types of events audited using IMS SLDS records

To audit some, instead of all event types, you can specify each event type to be audited by using the IMSL_AUDIT_LEVELS keyword.

When you enable auditing by using IMS SLDS records, the default is to provide auditing for all of the following event types:

- IMS Online region starts and stops
- Users sign on/sign off
- Database Opens and Closes
- PSB|DBD start, stop, lock, unlock, and DBDDUMP

To audit only some of these events, you can specify each event type to be audited using the IMSL_AUDIT_LEVELS keyword: IMSL_AUDIT_LEVELS (*ALL*|*CTL_STRT*|*USERS*|*DBOPN*|*DB_PSB*).

This keyword governs the IMS SLDS auditing level for all IMS subsystems that are controlled by this agent. For example, if user signon/signoff is not included in the IMSL_AUDIT_LEVELS parameter, then no signon or signoff events will be reported from any of the IMS environments that are audited using the agent.

Note: You can separate parameters for the collection of different event types. For example, to audit CTL_STRT and DBOPN events, include the CTL_STRT and DBOPN records as follows:

```
IMSL_AUDIT_LEVELS(CTL_STRT)
IMSL_AUDIT_LEVELS(DBOPN)
```

instead of:

```
IMSL_AUDIT_LEVELS(CTL_STRT|DBOPN)
```

Parent topic: Using agent configuration keywords to customize auditing

Changing the name of the Common Memory Management address space JCL

Use the AUIU_PROC_NAME keyword to change the member name from AUIU*STC* to a name of your choice.

AUIU*STC* is the name of the JCL that is used to build filtering criteria in E/CSA on all LPARS of the SYSPLEX. AUIU*STC* is provided in the product installation sample data set (SAUISAMP). If this name conflicts with your site's naming convention standards, or if more than one agent is being used, you can change the name of this JCL.

Use the AUIU_PROC_NAME keyword to change the member name from AUIU*STC* to a name of your choice: AUIU_PROC_NAME*(new name)*.

Ensure that this JCL resides in a procedure data set (PROCLIB) that allows the z/OS START command S taskname to be used.

Parent topic: Using agent configuration keywords to customize auditing

Excluding DLI calls on specific LPARS from being audited

To stop the transmission of the AUIU*STC* address spaces to all LPARs, the AUIU_EXCLUDE_LPAR keyword can be used to exclude specific LPARS from the target list of eligible LPARS.

By default, the IBM Guardium S-TAP for IMS agent creates Common Memory Management address spaces (AUIU*STC*) on all LPAR members of a SYSPLEX. This allocates E/CSA memory, and inserts DLI call filtering criteria across all LPARS. A single agent monitors IMS control regions and DLI/DBB batch jobs running on any LPAR of the SYSPLEX.

If you do not want to transmit the AUIU*STC* address spaces to all LPARs, the AUIU_EXCLUDE_LPAR keyword can be used to exclude specific LPARS from the target list of eligible LPARS: AUIU_EXCLUDE_LPAR*(lpar1, lpar2...lpar9)*

The LPAR where the agent is running cannot be excluded. All other LPARS can be excluded by using the *ALL option in place of the LPAR name.

For example, AUIU_EXCLUDE_LPAR(*ALL).
Parent topic: Using agent configuration keywords to customize auditing

Running more than one agent in a SYSPLEX

If two or more IMS agents are running on one SYSPLEX, use the ADS_SHM_ID and ADS_LISTENER_PORT keywords to differentiate the shared memory segment and port for each agent environment.

The agent address space (AUIA*STC*) and subordinate address spaces (AUIF*STC* and AUIL*STC*) communicate by using a shared memory segment and communications port. Multiple agents require multiple unique shared memory segments and port values to ensure correct inter-address space communications. If you need to have two or more IBM Guardium S-TAP for IMS agents available on one SYSPLEX, the following keywords provide a method of uniquely identifying the shared memory segment and port for each agent environment:

- ADS_SHM_ID(100010)
- ADS_LISTENER_PORT(16055)

Specification of the ADS_SHM_ID and ADS_LISTENER_PORT requires the addition of a //AUICONFG DD statement to the AUIF*STC* and AUIL*STC* address space JCLs. This DD statement should point to the same data set and member as the AUIA*STC* and AUIU*STC* JCLs for the agent, to ensure that communications between all participant address spaces use the correct memory object and ports.

See Customizing the agent by using agent parameter keywords for complete descriptions of all valid parameters, including the ADS_SHM_ID and ADS_LISTENER_PORT keywords.

Parent topic: Using agent configuration keywords to customize auditing

Restricting auditing to specific IMS systems when multiple IMS systems share RECON data sets

If multiple unrelated IMS systems share RECON data sets, and you want to audit only on one or more specific IMS systems, use the keyword IMSNAME_EQ_IMSSSID(Y) to isolate auditing to the desired IMS system.

The default option, IMSNAME_EQ_IMSSSID(N), causes only the IMS RECON data sets to be used when IBM Guardium S-TAP for IMS attempts to find and match IMS systems to active audit policies.

Specifying IMSNAME_EQ_IMSSSID(Y) causes both the IMS RECON data sets, and the 8-byte IMS subsystem/DBCTL RSENAME to be used when IBM Guardium S-TAP for IMS attempts to find and match IMS systems to active audit policies.

Consider the following example:

RECON data sets A.B.C1/C2/C3 contain information for IMSA and IMSB. Auditing is only desired for IMSB. Policy AUDIT_ALL is installed by using IMS appliance definition *MY_IMS*, which references RECON data sets A.B.C1/C2/C3.

If subsystems IMSA and IMSB both use RECON data sets that are referenced by the policy, AUDIT_ALL, and associated with the IMS definition, *MY_IMS*, then both IMSA and IMSB are audited when the default, IMSNAME_EQ_IMSSSID(N), is specified.

To restrict auditing to IMSB:

1. Specify IMSNAME_EQ_IMSSSID(Y) in the AUICONFG file.
2. Name the IMS definition in the appliance `IMSB`.
3. Relate policy AUDIT_ALL to `IMSB`.
4. Install the policy.

As a result, IMSB is audited with the criteria that is set in policy AUDIT_ALL, and IMSA is not audited.
Note: DLI batch jobs (DLI/DBB) might not be tightly associated with an IMSID, therefore IBM Guardium S-TAP for IMS will report on all DLI batch jobs that use the audited RECON data set. The IMSNAME_EQ_IMSSID parameter does not affect DLI/DBB batch job auditing.
Parent topic: Using agent configuration keywords to customize auditing

Using the System z Integrated Information Processor (zIIP)

You can use the System z® Integrated Information Processor (zIIP) when running IBM Guardium S-TAP for IMS Control region address space, and in the agent address space (AUIA*STC*). Use the ZIIP_AGENT_DLI keyword with the Y parameter to cause the agent to make a zIIP-enabled enclave SRB initialization attempt.

IMS control region

The following processes are moved to the zIIP in the IMS Online Control Region, pending redirection by the operating system:

- DLI call filtering
- IXGWRITE of audited DLI call data to the z/OS System Logger log stream

To use a zIIP in the IMS Online Control region, add a //AUIZIIP DD DUMMY to the IMS control region JCL.

Agent address space

The following processes are moved to the zIIP in the agent address space (AUIA*STC*), pending redirection by the operating system:

- IXGBROWSE read of audited data from the z/OS System Logger log streams for both Online and Batch DLI calls
- TCP/IP send of the data to the Guardium system

To use a zIIP in the agent address space, use the ZIIP_AGENT_DLI keyword with the Y parameter to the configuration file that is pointed to by the AUICONFG DD statement in the agent JCL (AUIA*STC*).

Parent topic: Using agent configuration keywords to customize auditing

Using multiple Guardium systems

You can configure multiple Security Guardium systems for automatic failover. By configuring one or more backup systems, you ensure continuous auditing capability. This process is known as failover. You can also enable the streaming of audited data from one or more IBM Guardium S-TAP for IMS agents to up to 6 connected Security Guardium systems. This process is known as multistreaming.

- **Providing Guardium system failover**
  You can specify up to five additional Guardium systems to be connected to the agent by using the APPLIANCE_SERVER_FAILOVER_x keyword, where x = a digit between one and five.
- **Streaming to multiple Guardium systems**
  Multistream mode enables S-TAP audit events to be sent to multiple connected appliances. You can enable multistreaming to up to 6 IBM Guardium system (APPLIANCE_SERVER + APPLIANCE_SERVER_MULTI_STREAM_*n*, where *n* can be 1 - 5).
- **Keeping connections active when HOT_FAILOVER is enabled**
  When the HOT_FAILOVER feature is enabled by setting the APPLIANCE_SERVER_LIST parameter to *HOT_FAILOVER*, connections for each connected Guardium appliance are kept active by pings. (The following connection types are kept active: DLIO, DLIB, SMF, IMSL, and MLOG.)

Parent topic: Using agent configuration keywords to customize auditing

Providing Guardium system failover

You can specify up to five additional Guardium systems to be connected to the agent by using the APPLIANCE_SERVER_FAILOVER_x keyword, where x = a digit between one and five.

The failover process

IBM Guardium S-TAP for IMS uses the concept of a single primary IBM Guardium system and multiple secondary backup systems.

- When a primary IBM Guardium system goes offline, the IBM Guardium S-TAP for IMS agent automatically establishes a connection to a secondary IBM Guardium system, and the audited data is sent to the secondary system.
- When a primary IBM Guardium system comes back online, the IBM Guardium S-TAP for IMS agent detects it, and reestablishes the connection to the primary IBM Guardium system and restarts, sending data to the primary system.

This allows the use of any IBM Guardium system as a short-term backup, while always attempting to use the primary system as the main data storage medium.

In the following example failover scenario, where none of the systems are online, the IBM Guardium S-TAP for IMS agent attempts to connect to the primary IBM Guardium system at a regular interval and follows the usual failover logic if the primary IBM Guardium system is offline. A connection is reestablished to any of the configured appliances as soon as one becomes available.

Enabling multiple system failover support

IBM Guardium S-TAP for IMS allows the specification of up to five additional IBM Guardium system to be connected to the agent. This feature provides failover protection, which allows the agent to continue to send audited data to one of a number of backup IBM Guardium system in the event of a communication failure with the primary system. You must use the APPLIANCE_SERVER keyword to enable this feature, because the IBM Guardium system that is referenced by this keyword is the primary connection. You can specify additional IBM Guardium system by using the APPLIANCE_SERVER_FAILOVER_x keyword, where x = a digit from 1 to 5.

- APPLIANCE_SERVER_FAILOVER_1(IP address 1)
- APPLIANCE_SERVER_FAILOVER_2(host name 2)
- APPLIANCE_SERVER_FAILOVER_3(IP address 3)
- APPLIANCE_SERVER_FAILOVER_4(IP address 4)
- APPLIANCE_SERVER_FAILOVER_5(host name 5)

Example failover scenario

Audit data flows to the primary IBM Guardium system, A.

The TCP/IP connection from the IBM Guardium S-TAP for IMS agent to the primary IBM Guardium system fails.

A connection is made to the secondary IBM Guardium system, B.

Audit data is now flowing to the secondary IBM Guardium system, B.

The TCP/IP connection from the IBM Guardium S-TAP for IMS agent to the primary IBM Guardium system is reestablished.

Audit data now flows to the primary IBM Guardium system, A.

The IBM Guardium S-TAP for IMS agent and IBM Guardium system B disconnect.

Parent topic: Using multiple Guardium systems

Streaming to multiple Guardium systems

Multistream mode enables S-TAP audit events to be sent to multiple connected appliances. You can enable multistreaming to up to 6 IBM Guardium system (APPLIANCE_SERVER + APPLIANCE_SERVER_MULTI_STREAM_*n*, where *n* can be 1 - 5).

IBM Guardium S-TAP for IMS sends events to a single appliance until a ping occurs, or the number of records that is specified by MEGABUFFER_COUNT is reached. Audited DLI events are distributed amongst additional appliances in a round-robin sequence.

To enable multistreaming, you must specify *MULTI_STREAM* when you configure the APPLIANCE_SERVER_LIST parameter. The APPLIANCE_SERVER and APPLIANCE_SERVER_[MULTI_STREAM]_[1-5] parameters specify the appliances to which you intend to stream events. The appliance that is specified by APPLIANCE_SERVER provides the policy that is used for event matching.

Enabling multistream support

Use the APPLIANCE_SERVER keyword to enable multistream support. The IBM Guardium system that is referenced by the APPLIANCE_SERVER keyword is the primary connection, and it provides the policy used to match DLI events. You can specify additional appliances by using the APPLIANCE_SERVER_MULTI_STREAM_*n* keyword, where *n* is a digit from 1 - 5.

Specify up to 5 additional IBM Guardium system IP addresses or host names. For example:

- APPLIANCE_SERVER_MULTI_STREAM_1(IP address 1)
- APPLIANCE_SERVER_MULTI_STREAM_2(host name 2)
- APPLIANCE_SERVER_MULTI_STREAM_3(IP address 3)
- APPLIANCE_SERVER_MULTI_STREAM_4(IP address 4)
- APPLIANCE_SERVER_MULTI_STREAM_5(host name 5)

Parent topic: Using multiple Guardium systems

Keeping connections active when HOT_FAILOVER is enabled

When the HOT_FAILOVER feature is enabled by setting the APPLIANCE_SERVER_LIST parameter to *HOT_FAILOVER*, connections for each connected Guardium® appliance are kept active by pings. (The following connection types are kept active: DLIO, DLIB, SMF, IMSL, and MLOG.)

If the primary appliance becomes unavailable and failover occurs, the appliance policy that was originally pushed from the primary appliance continues to be active. When all Guardium appliances are connected, the status of each appliance connection, listed in the Guardium interface, is green.

Parent topic: Using multiple Guardium systems

IBM Security Guardium S-TAP for IMS on z/OS agent reference information

The IBM Guardium S-TAP for IMS agent provides access to database and appliance services, in support of the product's remote clients. The agent also reads audited DLI events placed in the z/OS System Logger log streams by the IMS Online and DLI/DBB batch Data collectors and sends the DLI events to the IBM Guardium system using TCP/IP connections.

- **Sample library members**
  Use the following sample library members shipped with IBM Guardium S-TAP for IMS to install and configure the product.
- **Agent environment**
  The agent must be running before you can use product functions related to the IMS subsystems monitored by that agent.
- **APF authorization**
  For security, the agent must be APF-authorized before it can be run.
- **Agent job output**
  The primary output of the agent job consists of log messages written to the AUILOG DD. These messages provide status information about the ongoing operation of the agent, and also record additional messages if errors occur.
- **Stopping the agent**
  When running on z/OS, the agent accepts standard z/OS /MODIFY and /STOP commands. When stopping the agent, all secondary address spaces controlled by the agent will also receive a stop request.
- **Starting and stopping the secondary address spaces**
  This topic describes the /MODIFY commands to start and stop the secondary address spaces.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

Sample library members

Use the following sample library members shipped with IBM Guardium S-TAP for IMS to install and configure the product.

Table 1. Sample library members

Member	Type	Description
AUIAPPEV	DBD source statements	DBD source statements, used to define the optional APP_EVENT DBD
AUIA*STC*	JCL	Primary agent address space JCL
AUICONFG	CONFIG	Configuration file containing only the minimum required keywords
AUICONFX	CONFIG	Configuration file containing all available keywords
AUICPMOD	JCL	JCL to copy utility programs from SAUILOAD to SAUIIMOD data set
AUIEMAC1	MACRO	Edit macro to facilitate changes to other sample library members
AUIF*STC*	JCL	SMF data collection address space JCL

Member	Type	Description
AUIFUSPL	JCL	JCL to create the SMF incomplete event spill file for an agent
AUIL*STC*	JCL	IMS archived log data collection address space JCL
AUILSTR1	JCL	JCL to add CFRM structures for batch and online log streams to a CFRM policy
AUILSTR2	JCL	JCL to add batch and online log streams to your CFRM environment
AUILSTR3	JCL	JCL to add DASD-only log streams to your LOGR environment
AUIMIG10	JCL	JCL used to assist in the upgrade from V9.0 to V10.1.3
AUIMLOG	JCL	JCL used to read the IMS RECONS, detect missing logs, and send notification to the Guardium system
AUIPING	REXX EXEC	EXEC used to determine the LPAR name, as found in the CVTSNAME field, and issue a PING to determine if the LPAR name is in the network DNS table
AUISMFDF	JCL	JCL sample, showing the creation of a GDG file base for SMF data collection
AUISMFDP	JCL	JCL sample, showing the use of program IFASMFDP to filter SMF record types
AUITCPD	JCL	JCL used to generate a network diagnostic report
AUIU*STC*	JCL	Common storage management utility address space JCL

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS agent reference information

Agent environment

The agent must be running before you can use product functions related to the IMS subsystems monitored by that agent.

Important: Before the agent is started, system services should be started, and completely available for use. Examples of system services include JES, TCP/IP and the associated DNS RESOLVER, XCF, and the z/OS System Logger.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS agent reference information

APF authorization

For security, the agent must be APF-authorized before it can be run.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS agent reference information

Agent job output

The primary output of the agent job consists of log messages written to the AUILOG DD. These messages provide status information about the ongoing operation of the agent, and also record additional messages if errors occur.

In the event of exceptional conditions, additional messages might be written to the SYSOUT DD. If an abend occurs, dump information can be written to the CEEDUMP and SYSUDUMP DDs, if they are supplied. That information can be used in diagnosis by product support.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS agent reference information

Stopping the agent

When running on z/OS, the agent accepts standard z/OS /MODIFY and /STOP commands. When stopping the agent, all secondary address spaces controlled by the agent will also receive a stop request.

Important: System services, such as but not limited to the following, should remain available for use until the agent has completed termination: JES, TCP/IP and associated DNS RESOLVER, XCF and the z/OS System Logger.
From SDSF (or anywhere else that you can issue commands), you can issue one of these commands to the agent:

/STOP agent-job-name
: This is the recommended command to use to stop the agent. It initiates a graceful agent shutdown, which causes the agent to:

1. Wait for all existing requests to finish.
2. Exit.

/MODIFY agent-job-name,STOP
: Performs the same function as the /STOP agent-job-name command.

/MODIFY agent-job-name,FORCE
: This initiates an agent hard stop which causes the agent to:

1. Initiate hard cancels on all running threads.
2. Exit as soon as the threads exit.

Note: Use of the FORCE option can result in DUMP-producing ABENDS.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS agent reference information

Starting and stopping the secondary address spaces

This topic describes the /MODIFY commands to start and stop the secondary address spaces.

Commands to start and stop the SMF data collector address space

When the agent address space is started, secondary address spaces under the control of the agent may also be started. These include the SMF data collector address space (SAUISAMP member AUIF*STC*) which collects events using SMF log data as input and sends the events to the Guardium appliance. One IMS Archive Log event Data collector (SAUISAMP member AUIL*STC*) is also started for each IMS with an active collection.

Note: The following commands should be used against the agent's primary address space.

- /MODIFY <jobname>,START COLLECTOR SMF
- /MODIFY <jobname>,STOP COLLECTOR SMF

Optionally, the STOP command may be used to stop the SMF address space:

- /STOP <jobname>

Commands to start and stop the IMS Archive Log Data collector

There is no z/OS command to start the address space because the IMS Archive Log data collector address space is specific to an IMS definition with an active collection. The AUIL*STC* address is started by the agent address space, or activation of a collection.

Stopping a specific AUIL*STC* address space requires the use of the /STOP <jobname>.<token> command. The <token> value to be used can be found during AUIL*STC* startup in the AGENT JOBLOG.

In the following example, AAAAAAAC is the token value:

```
/S AUILRS22.AAAAAAAC
```

Or, when viewing the AUIL*STC* task in TSO SDFS, the token is displayed as the STEPNAME.
Parent topic: IBM Security Guardium S-TAP for IMS on z/OS agent reference information

Data collection

The collection process involves the gathering of audit event data at run time. Specify various filtering criteria to capture all relevant events and limit the amount of data that is collected and stored.

IBM Guardium S-TAP for IMS gathers audited events from the following sources:

- IMS database DLI calls performed from within IMS Online Control regions and DLI/DBB batch jobs
- SMF records
- IMS Log records from IMS System Log Data Sets (SLDS).

A single policy containing selection criteria that indicates the events to be audited, is applied to each source.

- **IMS database DLI calls**
  IBM Guardium S-TAP for IMS can filter audit events generated by database DLI calls by the following call types: Read, Update, Insert, and Delete.
- **SMF records**
  IBM Guardium S-TAP for IMS allows the filtering of audit events generated by access methods outside of IMS DLI services, including z/OS access methods such as VSAM or QSAM requests generated from z/OS batch jobs or TSO.
- **Records from IMS system log data sets (SLDS)**
  IBM Guardium S-TAP for IMS allows the filtering of audit events that are generated by IMS Online Control regions, which are logged to IMS log data sets and are processed from within the AUIL*STC* started task.
- **Filtering stages**
  Stage 0, Stage 1, and Stage 2 filtering is available for Collector Agent audit event collection when processing DLI calls.
- **Policy pushdown**
  This topic describes the policy pushdown process of mapping policies to an IBM Guardium S-TAP for IMS collection profile.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

IMS database DLI calls

IBM Guardium S-TAP for IMS can filter audit events generated by database DLI calls by the following call types: Read, Update, Insert, and Delete.

Note: Database DLI calls that do not result in a DBPCB status code of blanks, GA, or GK, are not audited unless the IMS policy indicates that one or more non-blank DLI codes should be reported. DLI calls performed using an IOPCB or TPPCB are not audited.

Database DLI calls issued from specific PSBs and user IDs can be included or excluded from auditing. PSB names and user IDs can be specified for auditing using fully qualified names, or by using wildcard characters.

Further filtering can be performed by including or excluding specific database and segment names. Wildcard support is available for both the database and segment name.

When auditing IMS DLI calls, you can obtain the concatenated key value of segments that are audited for all or specific database DLI calls, as well as the segment data for UPDATE, and INSERT calls. The segment data can also be obtained for READ and UPDATE calls where these calls are logically linked in the Guardium appliance to provide a before and after image of updated segments.

Parent topic: Data collection

SMF records

IBM Guardium S-TAP for IMS allows the filtering of audit events generated by access methods outside of IMS DLI services, including z/OS access methods such as VSAM or QSAM requests generated from z/OS batch jobs or TSO.

Some IMS Database Batch Utilities access IMS databases using access methods other the IMS Database DLI calls. As a result, the source of auditing records for these batch jobs will be the SMF records produced.

These audit events are based on z/OS SMF records and are processed from within the AUIF*STC* agent subtask. Policy criteria input for SMF data auditing is the same as for IMS DLI calls, but because of the nature of the SMF data, it is used differently.

The following data is not relevant, and therefore not used:

- DLI calls types
- PSB names
- Segment names

Database names are relevant because SMF data is based on data set names (part of the process that converts a policy to a filter, examines the IMS RECON data sets for artifacts in the RECON which relate to the INCLUDED database). These artifacts include database data set names (DSG/AREA/ADS) and database image copy data sets for each database data set. The AUIF*STC* tasks also audit other IMS related data sets.

By default, these data sets have been included because changes to these data sets can have an effect on data integrity:

- IMS RECON data sets
- Logging data sets generated by IMS DLI/DBB batch jobs
- SLDS/RLDS data sets
- IMS Online log data sets (OLDS)

It is possible to ignore the auditing of these data set types, as well as the database image copy data sets, by adding a DUMMY DD statement to the AUIF*STC* JCL.
This table lists the data sets and corresponding DD DUMMY statement to include in the AUIFSTC JCL if you want to exclude the auditing of each of these types.

Table 1. Data sets and DD DUMMY statements

Data set Type	IMS RECONS	IMS LOGS	IMS OLDS	DB Image Copies
DD NAME	AUINRCN	AUINLOG	AUINOLD	AUINICS

Specify filtering of SMF events at the agent level, using access type or security violation, with the use of the SMF_AUDIT_LEVELS keyword in the configuration file. The keyword is pointed to by the AUICONFG DD statement of the agent (AUIA*STC*) JCL. Data set accesses to be audited are:

- OPEN for Read/Update
- Data set Alter/Create/Delete
- Any security product (such as RACF®) violations

The auditing of these accesses can be specified at the agent level (for example, all IMS systems defined to the agent), or at the IMS level. See the *Changing the type of events audited using SMF records* section for more details.

Parent topic: Data collection

Records from IMS system log data sets (SLDS)

IBM Guardium S-TAP for IMS allows the filtering of audit events that are generated by IMS Online Control regions, which are logged to IMS log data sets and are processed from within the AUIL*STC* started task.

Policy criteria input for IMS Log data auditing is the same as for IMS DLI calls, but is used differently because of the nature of IMS log data:

- DLI calls types are not relevant and therefore not used.
- Segment names are not relevant and therefore not used.
- PSB names are checked only when relevant to the event being examined.
- User IDs are checked only when relevant to the event being examined.
- DBD names are checked only when relevant to the event being examined.

In addition to filtering performed using the policy criteria, you can further filter IMS log data by event types, using the Guardium user interface. Using the IMSL_AUDIT_LEVELS keyword, you can set specific events to be audited, including:

- IMS Control Region Starts and Stops
- USER signon and signoffs
- Database OPEN/CLOSE
- DBD and PSB STARTS/STOPS/LOCK/UNLOCK

Occurrences of the DB DBDUMP command can also be audited. Auditing of these events can be specified at the agent level (for example, all IMS systems defined to the agent), or at the IMS level (for example, only for a specific IMS system). For more information, see *Changing the types of events audited using IMS SLDS records*.

Parent topic: Data collection

Filtering stages

Stage 0, Stage 1, and Stage 2 filtering is available for Collector Agent audit event collection when processing DLI calls.

Filtering occurs at one or more of the stages, 0, 1, and 2, depending on what fields are included in your filter. As many audit events as possible are filtered at the earliest possible stage (0, 1, or 2). You can control filtering performance by the fields you include in the rules for the active collection profile.

- **Stage 0 filtering**
  Stage 0 filtering occurs immediately after IMS executes the DLI call and it is determined that the call is a candidate for auditing, meaning one of the supported DLI call types and blanks, or another acceptable DLI status code, is returned.
- **Stage 1 filtering**
  Stage 1 filtering occurs through the use of USERID and PSB name values.
- **Stage 2 filtering**
  Stage 2 filtering occurs through the use of a filtering program that is compiled at the time of policy installation, using the criteria specified in the policy.

Parent topic: Data collection

Stage 0 filtering

Stage 0 filtering occurs immediately after IMS executes the DLI call and it is determined that the call is a candidate for auditing, meaning one of the supported DLI call types and blanks, or another acceptable DLI status code, is returned.

IBM Guardium S-TAP for IMS checks for an active policy for the IMS subsystem and determines if any rules governed by the active policy require the auditing of the DLI call type. If no policy is active, or no rules require the auditing of the DLI call type, processing control is returned to the application program. This is the most efficient form of filtering and should be used when possible.

Consider this example, wherein an active policy contains three rules:

- One rule only addresses INSERT requests.
- The second rule only addresses DELETE requests.
- The third rule only addresses UPDATE requests.

In this example, the READ DLI call is performed, and returns a status code of blanks. Since IBM Guardium S-TAP for IMS determines that no rules in the policy can reference a READ, processing control returns to the application program.

If the event that the DLI call performed in the example was an INSERT request, Stage 1 filtering would be invoked.

Parent topic: Filtering stages

Stage 1 filtering

Stage 1 filtering occurs through the use of USERID and PSB name values.

For Stage 1 filtering to occur, all rules of the active policy must contain identical USERID and PSB name values. Any inconsistencies in these values between rules prevents Stage 1 filtering from occurring.

Stage 1 filtering allows DLI calls that should be rejected, due to USERID or PSB name, to be excluded from the list of values to be audited. This can be due to the items not being included, or being intentionally excluded.

The determination that the USERID or PSB is causing the DLI call to be rejected is made by call to the Stage 2 compiled filters. The call to the Stage 2 complied filters is made when the USERID or PSB name of the current DLI call is not the same as the USERID or PSB name of the previous DLI call made in the same processing region.

In this example, the processing flow is demonstrated when discussing a BMP:

- The first DLI call is made and passes through Stage 0 processing.
- Stage 2 filtering is invoked, and it is determined that DLI calls from this USERID should not be audited. The DLI call is not audited, and control is returned to the application program.
- The next DLI call is made, and the USERID is the same as the previous DLI call in the region. The previous DLI call was not audited due to the USERID value, therefore this DLI call will not be audited.
- This process continues until the BMP STEP terminates with only one DLI call going through to Stage 2 filtering, and the remaining DLI calls are rejected during Stage 1 processing.

The same benefit can be seen with DLI and DBB batch jobs, because the USERID and PSB will not change during the execution step.

This process benefits online transactions and other processing threads where multiple DLI calls are performed from within a single unit-of-work, as well as when DLI calls are performed using C and D IMS command codes where multiple segments are affected by a single DLI call and auditing might be required on more than one segment within the hierarchical path.

Parent topic: Filtering stages

Stage 2 filtering

Stage 2 filtering occurs through the use of a filtering program that is compiled at the time of policy installation, using the criteria specified in the policy.

All DLI calls that are not rejected by Stage 0 and Stage 1 filtering are processed by the compiled filter. The compiled filter determines if the DLI call is to be audited based on all the policy criteria including DBD and segment name.

If the DLI call is to be audited, additional information is returned by the compiled filter, such as if the segment data and concatenated key should be included in the audited data block.

Parent topic: Filtering stages

Policy pushdown

This topic describes the policy pushdown process of mapping policies to an IBM Guardium S-TAP for IMS collection profile.

When the IBM Guardium S-TAP for IMS agent starts, it establishes a dedicated connection to the Guardium appliance for the reading of installed policies. Immediately after the connection is established, any installed policies are pushed down to the IBM Guardium S-TAP for IMS agent by the Guardium appliance. The Guardium appliance pushes down a full policy to all connected IBM Guardium S-TAP for IMS agents each time a policy is installed or uninstalled from the Guardium appliance.

Upon receipt of a policy, the IBM Guardium S-TAP for IMS agent compares the applicable rules with the existing collections, and performs a differential install.

Differential install
: A differential install of the policy indicates that only policies that have been modified since the last install are acted upon.

The following processing occurs in the IBM Guardium S-TAP for IMS agent upon receipt of a policy:

- The new policy is compared to the currently active policy if the new policy contains one or more rules.

    - If the policies are identical, no further processing is required.
- If the new policy does not apply to this subsystem, processing continues without any changes.
    - If there is an active policy, the collection continues using it.
    - If no policy is active, none is started.

Parent topic: Data collection

Creating and modifying IMS definitions

An IMS definition establishes a connection from your Guardium system to the IMS environment that you want to audit. To create and modify IMS definitions from the Guardium system interface, the agent address space (AUIA*STC*) must have a preestablished connection to the Guardium system.

- **Navigating to the IMS Definitions panel**
  IMS definitions can be created, modified, and deleted from the IMS Definitions panel of the Guardium system interface.
- **IMS Definition fields**
  The following fields are available in the IMS Definitions panel for your use in definition an IMS entry. Required fields are indicated with an asterisk.
- **IMSPLEX data sharing and XRF considerations**
  When you are considering IMS data sharing and XRF systems, take the following IMSPLEX data sharing and XRF considerations into account.
- **Adding an IMS definition**
  Add an IMS definition to the IMS Definitions List to include a defined IMS environment in the list of environments to be audited.
- **Modifying an IMS definition**
  You can modify the attributes that are set for an IMS definition on the IMS Definitions List.
- **Deleting an IMS definition**
  Delete an IMS definition from the IMS Definitions List to remove the IMS entry from the list of IMS environments to be audited.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

Navigating to the IMS Definitions panel

IMS definitions can be created, modified, and deleted from the IMS Definitions panel of the Guardium system interface.

Procedure

1. From the Administration Console tab, select the Local Taps menu.
2. Select the IMS Definitions option.

Parent topic: Creating and modifying IMS definitions

IMS Definition fields

The following fields are available in the IMS Definitions panel for your use in definition an IMS entry. Required fields are indicated with an asterisk.

IMS Name

*IMS Entry Name
: A unique 1 - 8 character name to identify this IMS entry.

Description
: An optional description of the IMS Entry.

*Agent Name
: The name of the agent that audits this IMS entry.

RECONs

The RECON data set names are used to logically link the IMS definition, the active policy, the IMS Online Control region, and the DLI/DBB batch jobs that are running on z/OS, to audit the correct IMS instances.

*RECON1 Data Set Name
: The RECON1 data set name that is used by IMS on z/OS.

*RECON2 Data Set Name
: The RECON2 data set name that is used by IMS on z/OS.

RECON3 Data Set Name
: The RECON3 data set name that is used by IMS on z/OS.

IMS Data Sets

The IMS RESLIB data sets are used to determine the IMS release, during processing of the IMS System Log Data Sets (SLDS), using the AUIL*STC* address space. If more than one data set name is required, the data set names can be delimited by a comma.

*RESLIB Data Set Names
: A data set containing the IMS DFSVC000 module.

AUII050I Message Frequency
: Message AUII050I provides the number of DLI calls that are considered for auditing, and the number of DLI calls that were audited, based on the auditing criteria of the active policy. This message is produced based on the number of DLI calls that are considered, based on the following formula:

  Number of DLI calls in thousands (K) or Millions (M)

  or, by using both the formula and the time interval since the last AUII050I message was issued.

Example: If you provide values of `100K` (Number of DLI calls = 100,000) and `0100` (time interval of 1 hour), message AUII050I is issued when 100,000 DLI calls are seen by the product code, or by the 1 hour time interval, whichever comes first. The DLI counts and time interval reset when message AUII050I is issued.

Number of DLI calls
    xxx K|M
Time Interval
    HH:MM

Auditing Levels

Auditing levels can be set for both IMS Log and SMF events. For an explanation of the levels of auditing that are available for IMS Log and SMF events, see Configuration overview for a description of the IMSL_AUDIT_LEVELS and SMF_AUDIT_LEVELS configuration keywords.

IMS LOG Events
- Audit All IMS Log Events
- Audit Control Region Starts/Stops
- Audit User Signon/Signoff
- Audit DBD Open/Close
- Audit DBD/PSB/DUMP/START/STOP/LOCK/UNLOCK

SMF Events
- Audit All SMF Events
- Audit Dataset Open for Update
- Audit Dataset Deletes
- Audit Dataset Open for Read
- Audit Dataset Create
- Audit Dataset Alter
- Audit Dataset RACF® Violations

Parent topic: Creating and modifying IMS definitions

IMSPLEX data sharing and XRF considerations

When you are considering IMS data sharing and XRF systems, take the following IMSPLEX data sharing and XRF considerations into account.

IMSPLEX Data Sharing Considerations

Regardless of the number of LPARS that are involved, only one IMS definition is required in an IMS data sharing environment where all databases are shared by multiple IMS subsystems.

In an IMS data sharing environment where only a subset of databases is shared, an IMS definition must be created for each IMS subsystem with nonshared databases to be audited.

XRF Considerations

Only one IMS definition is required in an IMS XRF environment. IBM Security Guardium S-TAP for IMS on z/OS is not sensitive to which XRF partner is currently active. The product continues to produce audit data in the event of an XRF ACTIVE/BACKUP switch.

Parent topic: Creating and modifying IMS definitions

Adding an IMS definition

Add an IMS definition to the IMS Definitions List to include a defined IMS environment in the list of environments to be audited.

Procedure

1. From the IMS Definitions List, select the Add symbol, indicated by a plus sign, to the list of defined IMS systems.
   Enter the information in the IMS Definitions panel to define the new IMS environment to be audited.
2. Select Apply to save the new IMS definition.

Parent topic: Creating and modifying IMS definitions

Modifying an IMS definition

You can modify the attributes that are set for an IMS definition on the IMS Definitions List.

Procedure

1. Select the entry that you want to modify.
2. Modify the IMS definition fields.
3. Select Apply to save your changes.

Parent topic: Creating and modifying IMS definitions

Deleting an IMS definition

Delete an IMS definition from the IMS Definitions List to remove the IMS entry from the list of IMS environments to be audited.

About this task

IMS definitions can be deleted if no active IMS policies reference the IMS definition name. Only IMS definitions that are not part of an installed policy can be deleted.

Procedure

1. From the IMS Definitions List, select the IMS Definition that you want to delete.
2. Click the Delete icon.
   Click OK in the confirmation message to confirm the IMS entry deletion.

Parent topic: Creating and modifying IMS definitions

Reference information

This chapter provides IBM Guardium S-TAP for IMS reference information.

- **Data collection monitors**
  IBM Guardium S-TAP for IMS collects data from IMS online and batch activities, SMF, IMS archived logs, and IMS RECON data sets, by using the following internal product monitors.
- **IMS Log types and SMF record types that are collected by IBM Guardium S-TAP for IMS**
  The following tables show the IMS log types and SMF records types and descriptions that are collected by IBM Guardium S-TAP for IMS.
- **Fields that are used for IMS policy pushdown**
  The following fields defined in the Guardium system Access Rule Definition panel are used by IBM Guardium S-TAP for IMS to create policies and rules. Use the following information as a guideline.
- **Sizing the z/OS System Logger Log Stream for IBM Guardium S-TAP for IMS**
- **Echoed XML statement definitions**
  IBM Guardium S-TAP for IMS echoes the XML statements that are produced by the Guardium appliance to represent an Audit Policy. These statements are issued to a physical data set, agent AUILOG DD, or both, as determined by the XML_ECHO_DATASET and XML_ECHO_AUILOG parameters. This topic provides definitions of all XML statements that could be echoed from the appliance by the S-TAP.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

Data collection monitors

IBM Guardium S-TAP for IMS collects data from IMS online and batch activities, SMF, IMS archived logs, and IMS RECON data sets, by using the following internal product monitors.

IMS Online Activity Monitor
: The IMS Online Activity Monitor interfaces with IMS DL/I Language call analyzer module (DFSDLA00), and the IMS/VS Fast-Path Inter-region Communications Controller module (DBFIRC10), in order to be sensitive to the DL/I call type, and to access the data that is necessary for producing an audited event. When an INIT call is made to the IMS logger Exit routine (DFSFLGX0), interfaces to the IMS modules are activated, and they remain active until the DFSFLGX0 routine receives a TERM notification.
  For the activity monitor to be recognized by the IMS Online region, the IMS control region must be stopped and restarted with the SAUIIMOD data sets included as the first data sets in the STEPLIB DD concatenation.
  The IMS Online Activity Monitor and the agent communicate data collection criteria by using E/CSA control blocks. Determination of which DL/I calls and databases/segments is made at the time the DL/I call is performed, by using information that is derived from the data collection policy that is created through the IBM Guardium system's Access Rule definition process.
  The z/OS System Logger transports the audit data from the IMS Online Activity Monitor to the agent. All IMS online systems that are controlled by an agent use the same z/OS System Logger log stream. This z/OS system log stream is unique to the agent, and only contains audited events from IMS Online regions.

IMS Batch Activity Monitor
: The IMS Batch Activity Monitor interfaces with IMS DL/I language call analyzer module (DFSDLA00) in order to identify the DL/I call type and data that is necessary to produce an audited event. When the IMS Batch Exit routine (DFSISVI0) is invoked, the interface with the DL/I call analyzer is activated, and remains active until the batch step terminates.
  The IMS Batch Activity Monitor and the agent use E/CSA control blocks to communicate data collection criteria. The DLI calls and databases/segments determination is made at the time the DL/I call is performed, by using information that is derived from the data collection policy, which is created on the IBM Guardium system. The audit data from the IMS Batch Data Collector to the agent is transported through the z/OS System Logger.
  All IMS batch jobs that are controlled by an agent use the same z/OS System Logger log stream. This z/OS system log stream is unique to the agent, and only contains audited events from IMS Batch jobs.

IMS Online and Batch Data Collectors
: The IMS Online and Batch Data Collectors run as separate threads under the control of the agent address space (AUIA*STC*). The function of the data collector is to read audited events from the z/OS System Logger log stream, and send the events to the IBM Guardium system for storage by using a TCP/IP connection.
  Each thread maintains its own persistent TCP/IP connection to the Guardium system.

SMF Data Collector
: The SMF Data Collector reads a subset of SMF records from SMF memory dump data sets to determine whether data sets associated with audited IMS artifacts were read, written, deleted, or renamed. Security violations against these data sets can also be reported.
  IMS artifact associated data set types include database data sets, database image copy data sets, IMS log data sets (OLDS, SLDS and RLDS), and RECON data sets. The list of IMS artifact data sets to be monitored during SMF data collection is derived from the data collection policy that is created through the IBM Guardium system.
  As the processing of the SMF data sets is deferred, the data collection policy in force at the time of the SMF data set READ is the collection policy used, not the data collection policy in effect when the SMF event occurred. The names of the SMF memory dump data sets to be read is based on one or more SMF data set MASK values that are supplied by the use of one or more SMF_DSN_MASK keywords in the agent configuration file (AUICONFG). The data set names to that the SMF MASK refers reflects the SMF memory dump data sets that are created during offloading of the SMF recording data sets, or a copy of these data sets containing a subset of SMF record types that are created explicitly for the use of this product.
  Because an agent can monitor SMF events from all LPARS within a SYSPLEX, all SMF data sets to be read must be accessible from the LPAR on which the agent runs. The SMF Data Collector periodically queries the z/OS catalog for new data set names that meet the SMF MASK value. When cataloged data sets are found, these data sets are dynamically allocated and read by the SMF Data Collector. Auditable events that are found are formatted, and sent to the IBM Guardium system by using a TCP/IP connection.

The SMF Data Collector creates and maintains its own TCP/IP connection to the IBM Guardium system. The frequency that the SMF Data Collector queries the z/OS catalog is determined by the option you set during configuration of this product. The SMF Data Collector can be configured to audit only a subset of events by use of available options when configuring the agent and defining the IMS appliance through the Guardium system interface. The SMF Data Collector is run as a started task under the control of the agent. An example of the JCL for this started task can be found in the SAUISAMP data set in the AUIF*STC* member.
Note: IBM Guardium S-TAP for IMS only reports audited events for SMF record types that are collected by SMF. If specific SMF record types are not collected by your appliance or SMF recording data set memory dump utility, the event cannot be reported. Refer to the IMS Log types and SMF record types that are collected by IBM Guardium S-TAP for IMS topic for a list of SMF record types that are used by IBM Guardium S-TAP for IMS.

IMS Archived Log Data Collector

The IMS Archived Log Data Collector reads IMS Archived Log data sets (SLDS) and provides audit information about the following actions:

- IMS user signon and signoff
- IMS online region starts and stops
- Changes to the status of DBDs and PSBS within the IMS Online environment

The list of IMS artifacts to be monitored during IMS Archived Log collection is derived from the data collection policy you create, by using the Guardium system. As the processing of the IMS Archived Log sets is deferred, the data collection policy in force at the time that the IMS Archived Log data sets are read is the collection policy used (as opposed to the data collection policy in effect when the IMS Archived Log event as written to the IMS log data set).
The IMS Archived Log Collector periodically queries the DBRC RECON data sets that are associated with an IMS that is defined to IBM Guardium S-TAP for IMS to determine if new SLDS data sets were created since the last RECON data set query. New data sets that are found are dynamically allocated and read. Audited events are sent to the IBM Guardium system by using a TCP/IP connection.
The IMS Archive Log Data Collector can be configured to audit only a subset of events, by using the options available when configuring the agent and defining the IMS appliance through the Guardium system interface. The IMS Archived Log Data Collector is run as a started task under the control of the agent. An example of the JCL for this started task can be found in the SAUISAMP data set in the AUIL*STC* member.
IBM Guardium S-TAP for IMS starts one AUIL*STC* task for each set of RECON data sets that is actively monitored with a data collection policy.

- If an IMS data sharing environment with five IMS subsystems that share a single set of RECON data sets exists, only one AUIL*STC* task is started.
- If two separate IMS subsystems by using two separate sets of RECON data sets are being monitored, two separate AUIL*STC* tasks are started.
  Note: To collect events from the IMS archived logs, the DFSSLOGP (Primary Output SLDS) data set must be created and cataloged by your IMS Log Archive Utility process (program DFSUARC0).

IBM Guardium S-TAP for IMS dynamically starts and stops the appropriate number of AUIL*STC* tasks as required.

IMS Missing Log Utility

The IMS Missing Log Utility analyzes IMS RECON data sets to confirm the existence of SLDS/RLDS data sets. This function can be included or excluded, as well as scheduled without regard to the execution cycle setting for the AUIL*STC* task. This utility is run by a job or started task (see SAUISAMP member AUIMLOG for an example). It processes the RECON data sets of IMS systems with active policies audited by the agent and pointed to by the configuration member that is defined in the AUICONFG DD statement in the AUIMLOG JCL. The IMS RECON data sets are analyzed in search of IMS SLDS and RLDS data sets. If these are found, the z/OS appliance catalog is queried by using the SLDS/RLDS data set name. If the SLDS/RLDS data set is not found, a missing log event is sent to the IBM Guardium system.
Note: The AUIMLOG utility must be run under the same user ID, and on the same LPAR, as the AUIA*STC* task.

Common Storage Management Utility

IBM Guardium S-TAP for IMS uses memory in E/CSA to provide information regarding active data collection policies to the IMS Batch and Online Activity Monitors. An IBM Guardium S-TAP for IMS agent can be called to monitor IMS Online regions or DL/I batch jobs on many LPARS within a SYSPLEX. A started task is generated for execution on all LPARS of a SYSPLEX to read all active data collection policies and build the appropriate E/CSA control blocks. This started task is run when the IBM Guardium S-TAP for IMS agent starts and stops, as well as when a change is made to the state of any collection policy. An example of the JCL for this started task can be found in the SAUISAMP data set in the AUIUSTC member.
The LPARs where the AUIU*STC* task is run might be limited by adding the AUIU_EXCLUDE_LPAR keyword and LPAR names to the configuration file, which is specified by the AUICONFG DD statement in the AUIA*STC* JCL.

Parent topic: Reference information

IMS Log types and SMF record types that are collected by IBM Guardium S-TAP for IMS

The following tables show the IMS log types and SMF records types and descriptions that are collected by IBM Guardium S-TAP for IMS.

Table 1. IMS Logtypes collected by IBM Guardium S-TAP for IMS

Log type number	IMS log type	IMS log type description
06	IMS/VS Accounting Record X'06'	IMS Online was started or stopped.
16	A /SIGN command was successfully completed.	A /SIGN command successfully completed.
20	A database was opened.	A database was opened.
21	A database was closed.	A database was closed.
4C	DB/PSB Activity	Activity that is related to database or PSB processing
59xx	DEDB ADS OPEN Log record	DEDB area data set was opened.
5922	DEDB ADS CLOSE Log record	DEDB area data set was closed.
5923	DEDB ADS STATUS Log record	DEDB area data set status was changed.

SMF is used to obtain additional data set activity that is related to the monitored IMS databases and image copies.

Table 2. SMF record types and descriptions

SMF record Number	Type
00	IPL record
14	INPUT or RDBACK data set activity
15	OUTPUT, UPDATE, INOUT, or OUTIN data set activity
17	Scratch data set status
18	Rename non-VSAM data set
30	Common address space work, accounting information
60	VSAM volume data set updated
61	ICF catalog entry define

SMF record Number	Type
62	VSAM component or cluster opened
65	ICF delete activity
66	ICF alter activity
80	RACF® operator record
89	Usage data

Note: When image copies are read, they are collected as SMF type 14. When image copies are written, they are collected as SMF type 15. Image copies are sequential files, with some exceptions. If the image copy is opened as a VSAM file, the image copy is collected as SMF type 60.
Remember: IBM Guardium S-TAP for IMS can only report events that are being collected by SMF. If an SMF record type in this table is not being collected at your site, IBM Guardium S-TAP for IMS cannot report that event.
Parent topic: Reference information

Fields that are used for IMS policy pushdown

The following fields defined in the Guardium system Access Rule Definition panel are used by IBM Guardium S-TAP for IMS to create policies and rules. Use the following information as a guideline.

Table 1. Fields that are used for IMS Policy pushdown

Label	Hover text
Service Name	IMS names to which this rule applies (case sensitive)
Application User	INCLUDE/PSB or EXCLUDE/PSB
Database User	INCLUDE/USERID or EXCLUDE/USERID
Object	INCLUDE/read+update+delete+insert+data+image/DBNAME.SEGNAME or EXCLUDE/DBDNAME.SEGNAME

Service name/IMS name
: Required.
Must be 1 -- 8 characters.
Mixed case is allowed, and field is case sensitive.
Wildcard characters are not allowed.

Application user/PSB
: Must be 1 -- 8 characters.
All typed characters should be folded to uppercase.
Supports % as a wildcard character. % matches zero or more characters.
Note: If the keyword EXCLUDE is used, at least one INCLUDE must also be specified.

Database user/User ID
: Must be 1 -- 8 characters.
All typed characters should be folded to uppercase.
Supports % as a wildcard character. % matches zero or more characters.
Note: If the keyword EXCLUDE is used, at least one INCLUDE must also be specified.

Object/Target DB/Segment
: database_name must be 1 -- 8 characters.
segment_name must be 1 -- 8 characters.
wildcard_pattern supports % as a wildcard character. % matches zero or more characters.
All typed characters should be folded to uppercase.
Note: You must specify at least one INCLUDE with at least one DLI call type. DBD and segment must also be specified.

DLI Call Code
: Used to generate audit records for DLI calls that result in a non-blank status codes. Non-blank status codes can indicate that the DLI call failed or completed with a warning.
The following DLI status codes can be audited:

- FD
- FW
- GA
- GB
- GD
- GE
- GK
- L2
- LB
- LS
- NI
- UC
- US
- UX

You can specify one or more DLI status codes.
For more information about DLI status codes, see the About DLI status codes information in the IBM Knowledge Center.

Audit
: Used to limit the types of DLI calls to be audited.
NOHLVL causes audit information to be collected for only the target segment of a DLI Patch call (Command code C or D) instead of generating audit data for each segment of the hierarchical path. This can reduce the volume of audited data that is sent to, and stored by, the Guardium appliance in cases where the target segment concatenated key is sufficient for auditing purposes.

LTERM Filtering
: Must be 1 -- 8 characters.
All typed characters should be folded to uppercase.
Supports % as a wildcard character. % matches zero or more characters.
Note: If the keyword EXCLUDE is used, at least one INCLUDE must also be specified.

By default, auditing is considered for any DLI call that has a blank/null LTERM (for example, from a BMP or other region type that does not present IMS with an LTERM value). When an LTERM value or a group of LTERMs is specified, an option box is presented to enable you to turn off BLANK LTERM auditing. Turning off BLANK LTERM auditing does not affect the auditing of BMPs; any other region types without an LTERM value are excluded from auditing.

Filtering DLI calls from specific IMS Region types

You can filter out DLI calls from specific IMS Region types. DLI calls that originate from one or more of these region types can be excluded from auditing consideration:

- AER
- BMP
- CICS
- DBCTL
- IFP
- MPP
- ODB

In the Guardium interface, click the pencil icon alongside the Region Types to Exclude field to open a set of check-boxes that enable you to remove regions from auditing

Parent topic: Reference information

Sizing the z/OS System Logger Log Stream for IBM Guardium S-TAP for IMS

This section details the process of sizing the z/OS System Logger Log Streams. The z/OS System Logger Log Stream is used to transport audited DLI call data from the IMS control region or DLI/DBB batch jobs to the IBM® Guardium® S-TAP® for IMS agent (AUIAxxxx address space) where it is reformatted to a PROTOBUF protocol and sent to the target Guardium appliance.

- **Calculating the Optimal Log Stream Size**
  Filtering by using the IMS POLICY from the Guardium appliance occurs in the IMS Control region, therefore only DLI calls that are to be audited are written to the log stream(s).
- **Considerations**
  There are several variables that must be considered when sizing the log stream(s), including:
- **Using IBM Documentation**
  The System Logger Performance and Tuning section of the System Programmer's Guide to: z/OS System Logger provides a detailed description of the processes that are needed to tune the System Logger for use with IBM Guardium S-TAP for IMS and other products.
- **Pertinent Report Fields**
  Some key fields provided in the System Logger Activity Report (IXGRPT1) are the BYT WRITTN TO INTERIM STORAGE, BYT WRITTN TO DASD, and STRUC FULL.
- **Additional Resources**
  IBM provides a spreadsheet utility to assist in the analysis of the log stream SMF88 data and provide suggestions on how to define the log stream for more efficient use in your environment.

Parent topic: Reference information

Calculating the Optimal Log Stream Size

Filtering by using the IMS POLICY from the Guardium appliance occurs in the IMS Control region, therefore only DLI calls that are to be audited are written to the log stream(s).

For most users, the size of the log stream that is provided with the LS_SIZE parameter of the AUILSTR2/3 log stream definition member (LS_SIZE(100)) is appropriate to use when auditing accesses to sensitive data or when auditing DLI calls performed by a group, or groups, of users who have access to all databases for diagnostic purposes.

There might be instances where an LS_SIZE parameter value of 13500 (LS_SIZE(13500)) might be used, such as:

- during product testing, or
- when the number of audited DLI calls exceed twenty-five thousand DLI calls per second, or
- when the audited DLI calls include large concatenated key or large segment fields, which can occur when the IMS POLICY includes the `+DATA` keyword in the TARGET/DB INCLUDE filter statement

Note: Log stream sizing can be an iterative process. When attempting to audit many DLI calls, the CPU, memory, and disk storage capacity of the Guardium appliance should be considered.

Parent topic: Sizing the z/OS System Logger Log Stream for IBM Guardium S-TAP for IMS

Considerations

There are several variables that must be considered when sizing the log stream(s), including:

- the number of IXGWRITEs that are performed every second
- the average number of bytes written, or average buffer size written with each IXGWRITE calls
- the rate that the data is offloaded from the log stream
- the number/rate of IXGDELETEs that are performed

The average number of IXGWRITEs that are performed and the average number of bytes/average buffer size is determined by the volume of audited DLI calls and the size of the DLI call event data that is being captured.

IBM® Guardium® S-TAP® for IMS uses a set of 35K buffers to hold the audited DLI call data. Each buffer is written to the log stream when it fills to capacity, or every five seconds. The time interval is used to ensure that audited DLI call data is sent to the Guardium appliance in a timely manner. Therefore, the frequency of IXGWRITEs can vary greatly depending on the IMS Policy and databases that are being accessed.

The log stream offload process IBM Guardium S-TAP for IMSis performed by the agent address space (AUIAxxxx). The agent address space constantly polls the log stream (once per second) looking for new data to process. When new data is found, the data is read by using the IXGBRWSE call. The data is formatted into a PROTOBUF protocol and sent to the Guardium appliance by using TCP/IP. The IBM Guardium S-TAP for IMS agent will continually read and process log stream data until no new data exists, at which time, polling every second will reoccur.

The log stream data is deleted by using the IXGDELETE call after every three blocks of data are successfully read and sent to the Guardium appliance. This ensures that audited data is not lost in the event of a communication loss between the IBM Guardium S-TAP for IMS agent and the Guardium appliance.

Parent topic: Sizing the z/OS System Logger Log Stream for IBM Guardium S-TAP for IMS

Using IBM Documentation

The System Logger Performance and Tuning section of the System Programmer's Guide to: z/OS System Logger provides a detailed description of the processes that are needed to tune the System Logger for use with IBM® Guardium® S-TAP® for IMS and other products.

You can perform an analysis of the performance and efficiency of the initial log stream size by running program IBM program IXGRPT1 and JCL IXGRPT2 found in 'SYS1.PROCLIB'. This program uses the SMF88 records to help with log stream capacity planning.

SMF88 records can be collected by z/OS by providing the 88 value in the SMPRM parmlib member prior to a system IPL, or by using the z/OS command, "SET SMF=xx" (where xx is the suffix of the parmlib member).

Example:

```
SYS(TYPE(30,70:79,88,89,100,101,110)),
```

The IXGRPT1 utility will assemble sub-routine IXGRA1 and compile and link program IXGRPT1, which can be used to extract SMP88 records in preparation for analysis.

The IXGRPT2 JCL can be used to produce other SMP88/log stream reports.

Parent topic: Sizing the z/OS System Logger Log Stream for IBM Guardium S-TAP for IMS

Pertinent Report Fields

Some key fields provided in the System Logger Activity Report (IXGRPT1) are the BYT WRITTN TO INTERIM STORAGE, BYT WRITTN TO DASD, and STRUC FULL.

BYT WRITTN TO INTERIM STORAGE

The BYT WRITTN TO INTERIM STORAGE value (bytes written to interim storage) indicates the amount of data being written to the log stream during the SMP interval. This value can provide insight as to the volume of data being written to the log stream.

BYT WRITTN TO DASD

The BYT WRITTN to DASD value (bytes written to DASD offload data sets) indicates the number of bytes that were written to the DASD offload/overflow VSAM data sets.

This number indicates that the interim storage filled up, and in order to retain the data, a set of VSAM files are being used as overflow buffers. This number can rise and fall during the day as the volume of audited DLI calls increase and decrease.

Some use of the overflow VSAM files can be acceptable because spikes in audited DLI call data can certainly be expected due to the nature of IMS POLICY filtering. However, constant or extensive use of the VSAM overflow files indicate that the log stream should be sized larger.

STRC FULL

The STRC FULL (Structure Full) value indicates the number of times that the capacity of the CF structure was filled up without an offload occurring. This number should be zero in a properly sized log stream. Structure such as this can indicate that the volume of data written exceeds the offload capability of the IMS STAP agent to read, process, and delete audited data, and a larger structure size should be considered.

An abundance of Structure Full conditions will result in a degradation of performance when collecting audited DLI call data, and if not rectified, might result in data loss. This condition might result in IXGWRITE 0866 errors being issued in the IMS Control region address space.

Parent topic: Sizing the z/OS System Logger Log Stream for IBM Guardium S-TAP for IMS

Additional Resources

IBM provides a spreadsheet utility to assist in the analysis of the log stream SMF88 data and provide suggestions on how to define the log stream for more efficient use in your environment.

You can access the spreadsheet utility with the following link: ftp://www.redbooks.ibm.com/redbooks/SG246898. Read the disclaimer.txt file before using the tool.

Parent topic: Sizing the z/OS System Logger Log Stream for IBM Guardium S-TAP for IMS

Echoed XML statement definitions

IBM® Guardium® S-TAP® for IMS echoes the XML statements that are produced by the Guardium appliance to represent an Audit Policy. These statements are issued to a physical data set, agent AUILOG DD, or both, as determined by the XML_ECHO_DATASET and XML_ECHO_AUILOG parameters. This topic provides definitions of all XML statements that could be echoed from the appliance by the S-TAP.

XML convention

Start of tag data

=<*tag_name*>
End of tag data
=</*tag_name*>
Null/empty tag
=<*tag_name*/>

See Sample XML file for an example of the XML representation of a valid policy.

IMS-specific statements

Table 1. IMS-specific XML statements

XML statement	Definition
<install-info>	Beginning of relevant policy information.
<artifacts>	Start of IMS definitions.
<ims>	Start of individual IMS-specific information.
<name>	Name of IMS as specified in the Guardium appliance policy.
<agent>	Name of the agent to which IMS is connected.
<description>	Appliance IMS description text.
<version>	Currently a value of zero (0).
<plexname>	Not populated.
<recons>	Start of the IMS-specific RECON data set list.
<recon seq="1">	RECON1 data set name. DSN terminated by </recon>.
<recon seq="2">	RECON2 data set name. DSN terminated by </recon>.
<recon seq="3">	RECON3 data set name. DSN terminated by </recon>.
<reslibs>	Start of IMS-specific RESLIB data sets.
<reslib seq="1">	RESLIB 1 in IMS STEPLIB concatenation. DSN terminated by </reslib>.

Log-specific statements

Table 2. Log-specific XML statements

XML statement	Definition
<dbdlibs/>	Not populated.
<psblibs/>	Not populated.
<thresholds-050i>	Start of message AUII050I message frequency parameters.
<max-count>	Number of DLI calls needed to prompt message AUII050I.
<max-time>	Max time interval (HHMM) between AUII050I messages.
<audit-levels>	Start of IMS Logger and SMF auditing criteria.
<collector name="ims">	Start of IMS Logger auditing criteria. Terminated by </collector>.
<audit-level>	Start of audit level criteria.
<signon-signoff value="true"/>	Audit IMS user sign-ons and sign-offs.
<signon-signoff value="false"/>	Do not audit IMS user sign-ons and sign-offs.
<start-stop value="true"/>	Audit IMS Control Region starts and stops.
<start-stop value="false"/>	Do not audit IMS Control Region starts and stops.
<db-open-close value "true"/>	Audit DBD Opens and Closes.
<db-open-close value "false"/>	Do not audit DBD Opens and Closes.
<dbd-psb value="true/"	Audit DBD/PSB/Dump/Start/Stop/Lock/Unlock
<dbd-psb value="false/"	Audit DBD/PSB/Dump/Start/Stop/Lock/Unlock

SMF-specific statements

Table 3. SMF-specific XML statements

XML statement	Definition
<collector name="smf">	Start of SMF auditing criteria. Terminated by </collector>.
<audit-level>	Start of audit-level criteria.
<read value="true"/>	Audit data sets when they are opened with READ intent.
<read value="false"/>	Do not audit data sets when they are opened with READ intent.
<update value="true"/>	Audit data sets when opened with UPDATE intent.
<update value="false"/>	Do not audit data sets when opened with UPDATE intent.
<delete value="true"/>	Audit data set DELETEs.
<delete value="false"/>	Do not audit data set DELETEs.
<create value="true"/>	Audit data set CREATEs.
<create value="false"/>	Do not audit data set CREATEs.
<alter value="true"/>	Audit VSAM data set ALTERs.
<alter value="false"/>	Do not audit VSAM data set ALTERs.
<racf-violations value "true"/>	Audit RACF security violations against data sets.
<racf-violations value "false"/>	Do not audit RACF security violations against data sets.

Policy-specific statements

Table 4. Policy-specific XML statements

XML statement	Definition

XML statement	Definition
<policies>	Start of policy information.
<collection-profile>	Displays the rules defined to the policy. The collection profile policy name appears in the collection-specific statement <collection> for a given <ims>.
<name>	Policy name. Naming convention is: *policy_IMS_name*.
<description>	Concatenation of descriptions of all policies pushed to the appliance.
<rules>	Start of individual policy rules.
<rule>	Start of rule instance.
<active>	Always a value of true.
<filters>	Start of PSB/USERID/LTERM INCLUDES/EXCLUDES within the rule.
<psb-filter>	PSB instance.
<name>	Name of PSB to be audited or ignored.
<type>	Value will be INCLUDE (audit) or EXCLUDE (ignore).
<lterm-filter>	LTERM instance.
<name>	LTERM to be audited or ignored.
<type>	Value will be INCLUDE (audit) or EXCLUDE (ignore).

Database/segment-specific statements

Table 5. Database/segment-specific XML statements

XML statement	Definition
<targets>	Start of DBD/SEGMENT instances within the rule.
<segment-target>	Start of list of databases/segments to be INCLUDED/EXCLUDED.
<type>	Value will be INCLUDE (audit) or EXCLUDE (ignore).
<database-name>	Database to be audited or ignored.
<segment-name>	Segment to be audited or ignored.
<audit-get>	INCLUDE DLI GET calls.
<audit-insert>	INCLUDE DLI INSERT calls.
<audit-update>	INCLUDE DLI UPDATE (REPL) calls.
<audit-delete>	INCLUDE DLI DELETE (DLET) calls.
<capture-before-image>	INCLUDE link between DLI GH and DLI REPL calls.
<capture-segment-data>	INCLUDE segment data when segment is audited.
<hlvl-filter enabled="false">	Do not report hierarchical parent segment during DLI command calls.
<excluded-regions>	Do not audit DLI calls from these region types.

Collection-specific statements

Table 6. Collection-specific XML statements

XML statement	Definition
<collections>	A grouping of the individual <collection> XML tags.
<ims>	IMS name connection to the collection.
<agent-name>	Agent name connection to the collection.
<name>	IMS name connection to the collection.
<collection-profile>	For each agent name and IMS name, IBM Guardium S-TAP for IMS establishes a connection to the collection profile.
<name>	Constructed name of the policy (*policy_IMS_NAME*).
<dli-status-codes>	Two-character DLI status codes to be audited. Terminated by FF value.

Quarantine information

Quarantine XML is only sent from the appliance when the quarantine is triggered by audited events that are sent to the appliance by the agent, and the quarantine is deemed to be in effect. This causes AI status codes (error opening database) to be returned to the application program in the DLI Status code PCB field (DBPCBSTC), and message AUIJ252W to appear in the IMS region or batch job.

Quarantine only works with full-function DLI calls because the AUI hook for Fast-Path occurs after the DLI call has completed. (The DLI call cannot be preempted.)

Table 7. Quarantine-specific XML statements

XML statement	Definition
<quarantine-lists>	Start of quarantine section.
<quarantine-list agent-name="*xxxxxxxx*" ims-name="*yyyyyyyy*"> >	Agent and IMS name are affected.
<quarantine-item>	Start of quarantine details.
<start-ts>yyyy-mm-dd-hh.mm.ss.000000	Quarantine start date/time.
<end-ts>yyyy-mm-dd-hh.mm.ss.000000	Quarantine end date/time.
<user-id>	User ID to be quarantined.

- **Sample XML file**
  This is an example of a valid audit policy.
- **Additional causes of AUIA060W**
  Warning message AUIA060W can appear if the data set location is incorrect. Review these additional possible causes of the message if the explanation and recommendation provided by AUIA060W do not resolve the warning.

Parent topic: Reference information

Sample XML file

This is an example of a valid audit policy.

```
<install-info>
  <artifacts>
    <ims>
      <name>IMSV14AH</name>
      <agent>AUI15A</agent>
      <description>IMS V14 Test IEACRX AUI10A27</description>
      <version>0</version>
      <plexname></plexname>
      <recons>
        <recon seq="1">IMSEA1.RECON1</recon>
        <recon seq="2">IMSEA1.RECON2</recon>
        <recon seq="3">IMSEA1.RECON3</recon>
      </recons>
      <reslibs>
        <reslib seq="1">IMSEA1.SDFSRESL</reslib>
      </reslibs>
      <dbdlibs/>
      <psblibs/>
      <thresholds-050i>
        <max-count>1K</max-count>
        <max-time>0015</max-time>
      </thresholds-050i>
      <audit-levels>
        <collector name="ims">
          <audit-level>
            <signon-signoff value="true"/>
            <start-stop value="true"/>
            <db-open-close value="true"/>
            <dbd-psb value="true"/>
          </audit-level>
        </collector>
        <collector name="smf">
          <audit-level>
            <read value="true"/>
            <update value="true"/>
            <delete value="true"/>
            <create value="true"/>
            <alter value="true"/>
            <racf-violations value="true"/>
          </audit-level>
        </collector>
      </audit-levels>
    </ims>
  </artifacts>
  <policies>
    <collection-profile>
      <name>policy_IMSV14AH</name>
      <description>---: Log Full Details With Values,Auv - Event All,IEA1_ALL_ST_AH</description>
      <rules>
        <rule>
          <active>true</active>
          <filters/>
          <targets>
            <segment-target>
              <type>include</type>
              <database-name>%</database-name>
              <segment-name>%</segment-name>
              <audit-get>true</audit-get>
              <audit-insert>true</audit-insert>
              <audit-update>true</audit-update>
              <audit-delete>true</audit-delete>
              <capture-before-image>false</capture-before-image>
              <capture-segment-data>true</capture-segment-data>
            </segment-target>
          </targets>
          <audit/>
          <excluded-regions></excluded-regions>
        </rule>
      </rules>
    </collection-profile>
  </policies>
  <collections>
    <collection>
      <ims>
        <agent-name>AUI15A</agent-name>
        <name>IMSV14AH</name>
      </ims>
      <collection-profile>
        <name>policy_IMSV14AH</name>
      </collection-profile>
      <dli-status-codes>FDFWGAGBGDGEGKL2LBLSNIUCUSUXFFFF</dli-status-codes>
    </collection>
  </collections>
  <quarantine-lists/>
</install-info>
```

Parent topic: Echoed XML statement definitions

Additional causes of AUIA060W

Warning message AUIA060W can appear if the data set location is incorrect. Review these additional possible causes of the message if the explanation and recommendation provided by AUIA060W do not resolve the warning.

Data set: <LOCATION> in use

Explanation
: An attempt to dynamically allocate the data set failed because the data set was in use by another process. This warning might be temporary. The agent retries the data set 6 times in 3 seconds before skipping the policy XML echoing.

Response
: If this message occurs several times without successful policy XML echoes, check to see that any running user report program is using the data set correctly or whether a TSO user might be editing the data set.

A dynamic allocation error occurred. Data set <LOCATION>, info code: <info-code>, error code: <error-code>.

Explanation
: An attempt to dynamically allocate the data set failed. The specified information and error codes reflect the return and reason codes from the z/OS dynamic allocation services.

Response
: Use the info code and error code to determine the cause of the dynamic allocation failure by referring to the *z/OS MVS Programming: Authorized Assembler Services Guide* in the IBM Knowledge Center. Correct the error and restart the agent.

Catalog Search Interface: error RC = <rc>, RSN = <rsn>.

Explanation
: Using the z/OS Catalog Search Interface routine, the agent attempted to analyze whether the data set is a Generation Data Group (GDG) data set or a non-VSAM data set. An error occurred while calling the routine.

Response
: Consult the *Return Codes for General Purpose Register 15* section of the *IBM Catalog Search Interface User's Guide* in the IBM Knowledge Center. Contact IBM Support if additional assistance is needed.

Data set "<LOCATION>" could not be deleted, info code: <code>, error code <code>.

Explanation
: An attempt was made to delete and reallocate a non-VSAM non-GDG data set in the catalog.

Response
: Ensure that the agent task has RACF (or other security product) authority to delete a data set that contains a high-level qualifier. Attempt to correct the security problem and restart the agent. If the error persists, contact IBM Support and provide the info and error codes.

XML echo data set <LOCATION> is of an unsupported type

Explanation
: Only non-VSAM and GDG base data sets are supported.

Response
: Ensure that the data set type is either a non-VSAM data set or a Generation Data Group. Restart the agent.

Parent topic: Echoed XML statement definitions

Troubleshooting

Use the following topics to diagnose and correct problems that you experience with IBM Guardium S-TAP for IMS.

- **Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS**

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

This information documents the messages and error codes issued by Security Guardium S-TAP for IMS. Messages are presented in ascending alphabetical and numerical order.

Note: To set a z/OS message alert for messages that begin with AUII, or messages AUIJ250I and AUIJ252W, use single-dash formatting between the message number and message text. For all other messages, use a double-dash. For example:

AUIT031I--Starting the command listener thread
: Format most message alerts with double-dashes between the message number and message text.

AUII056I - ZIIP PROCESSING ENABLED FOR IMS STAP
: Format message alerts for AUII*, AUIJ250I, and AUIJ252W with a single dash between the message number and message text.

- **Error messages and codes: AUIAxxxx**
- **Error messages and codes: AUIBxxxx**
- **Error messages and codes: AUIFxxxx**
- **Error messages and codes: AUIGxxxx**
- **Error messages and codes: AUIIxxxx**
- **Error messages and codes: AUIJxxxx**

- **Error messages and codes: AUILxxxx**
- **Error messages and codes: AUIPxxxx**
- **Error messages and codes: AUIRxxxx**
- **Error messages and codes: AUITxxxx**
- **Error messages and codes: AUIUxxxx**
- **Error messages and codes: AUIXxxxx**
- **Error messages and codes: AUIYxxxx**
- **Error messages and codes: AUIZxxxx**

Parent topic: Troubleshooting

Error messages and codes: AUIAxxxx

The following information is about error messages and codes that begin with AUIA.

- **AUIA003E**
  Address Space *<name>* failed to start successfully on *<LPAR name>*.
- **AUIA004E**
  Address Space *<name> (<job number>)* failed to stop successfully on *<LPAR name>* within the timeout period and was abandoned.
- **AUIA005I**
  Starting address space *<name>* on *<LPAR name>*.
- **AUIA006I**
  Address Space *<name> (<job number>)* is online on *<LPAR name>*.
- **AUIA007I**
  Stopping address space *<name> (<job number>)* on *<LPAR name>*.
- **AUIA008I**
  Address Space *<name> (<job number>)* on *<LPAR name>* is offline.
- **AUIA009E**
  Address space *<name>* is not active.
- **AUIA010E**
  Address Space *<name>* is already active.
- **AUIA021I**
  MODIFY command *<command text>* sent to Address Space *<name>*.
- **AUIA022I**
  <Collector name> collector is disabled: interval is set to *<value>*.
- **AUIA023I**
  <Collector name> collector is disabled: proc name for the collector address space has not been specified in the configuration.
- **AUIA024I**
  <Collector name> collector is disabled: not configured.
- **AUIA027E**
  Abend occurred while validating *<log stream>*. Abend code = *<code>*, RSN = *<reason>*.
- **AUIA028S**
  Agent *agent-name* on *PLEX name* for S-TAP version *S-TAP version* is already online. *(ADS_SHM_ID=<Memory Segment ID>)*
- **AUIA029I**
  collector collector is disabled: no Audit IMS Log Events are selected for IMS source *IMS*.
- **AUIA030I**
  collector collector started successfully.
- **AUIA031I**
  collector collector stopped successfully.
- **AUIA033I**
  (GDM) Attempting to establish link with the appliance.
- **AUIA034S**
  (GDM) An attempt to establish the link to the appliance failed.
- **AUIA035W**
  (GDM) Link failed over to a secondary appliance. [host=*host*, port=*port*]
- **AUIA036I**
  (GDM) Link to primary appliance established. [host=*host*, port=*port*]
- **AUIA037I**
  (GDM) Link to primary appliance restored. [host=*host*, port=*port*]
- **AUIA038S**
  (GDM) Link to the appliance lost.
- **AUIA041I**
  Guardium policy processing failed due to prior errors.
- **AUIA042W**
  The Guardium policy is not applicable.
- **AUIA043I**
  The Guardium policy reader thread started.
- **AUIA044I**
  The Guardium policy reader thread is terminating.
- **AUIA045I**
  The guardium policy reader thread is terminating due to prior errors.
- **AUIA048I**
  auiu_taskname is configured to start only on *lpar-name*.
- **AUIA049W**
  auiu_task_name is configured to not start on *lpar_name* but will be started on *lpar_name* because *aui_agent_name* runs on *lpar_name*
- **AUIA050W**
  auiu_task_name is configured to not start on *lpar_name* but no such system exists.
- **AUIA051I**
  auiu_task_name is configured to not start on *lpar_name* and will not be started on *lpar_name*.

- **AUIA052I**
  Discovered <plex-name> system <system-name>.
- **AUIA053I**
  Agent configuration option *<option>* has been updated to *<value>*.
- **AUIA054I**
  Agent configuration option *<option>* is set to *<value>*.
- **AUIA055I**
  The agent is waiting for start-up information from the appliance.
- **AUIA056I**
  Starting the agent collectors.
- **AUIA057I**
  Issuing request to capture agent status.
- **AUIA058I**
  Request to capture agent status has completed successfully.
- **AUIA059I**
  Policy XMl echo
- **AUIA060W**
  Policy XML echo to data set skipped: *<MESSAGE> <LOCATION>*
- **AUIA061I**
  Policy XML echo to data set *<LOCATION>* completed.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIA003E Address Space *<name>* failed to start successfully on *<LPAR name>*.

Explanation

An attempt by the agent to start the named support address space has failed.

User response

Check the named address space logs to identify why it was not able to start. In most cases, this occurs if an address space with that name is already online, there was a JCL error, or there was an issue resolving the loopback address host name. If further assistance is required, contact IBM Software Support.

Parent topic: Error messages and codes: AUIAxxxx

AUIA004E Address Space *<name> (<job number>)* failed to stop successfully on *<LPAR name>* within the timeout period and was abandoned.

Explanation

The specified address space did not stop within the time out period and was consequently abandoned by the master address space.

User response

Check the named address space logs to identify why it did not stop. If further assistance is needed, contact IBM® Software Support.
Parent topic: Error messages and codes: AUIAxxxx

AUIA005I Starting address space *<name>* on *<LPAR name>*.

Explanation

The agent has automatically started the support address named.

User response

This is an informational message only.
Parent topic: Error messages and codes: AUIAxxxx

AUIA006I Address Space *<name> (<job number>)* is online on *<LPAR name>*.

Explanation

The agent has successfully started the support address space named.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA007I Stopping address space *<name> (<job number>)* on *<LPAR name>*.

Explanation

The agent has automatically stopped the support address space named.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA008I Address Space *<name> (<job number>)* on *<LPAR name>* is offline.

Explanation

The named address space has successfully stopped.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA009E Address space *<name>* is not active.

Explanation

The specified address space that the master address space was attempting to control is not online.

User response

Correct and retry.

Parent topic: Error messages and codes: AUIAxxxx

AUIA010E Address Space *<name>* is already active.

Explanation

This message indicates that the address space with the specified name is active already and was expected to be. This message occurs when starting the BATCH (or SMF) collector if they are already running.

User response

Verify that the address space is already running. If the address space is not online and the message occurs, contact IBM® Software Support.
Parent topic: Error messages and codes: AUIAxxxx

AUIA021I MODIFY command *<command text>* sent to Address Space *<name>*.

Explanation

The MODIFY command *<command text>* sent to address space named.

User response

No action is required.

Parent topic: Error messages and codes: AUIAxxxx

AUIA022I *<Collector name>* collector is disabled: interval is set to *<value>*.

Explanation

Named collector is disabled because the interval value is less than or equal to zero.

User response

If this was not intentional, fix the interval value and restart the agent address space.

Parent topic: Error messages and codes: AUIAxxxx

AUIA023I *<Collector name>* collector is disabled: proc name for the collector address space has not been specified in the configuration.

Explanation

The specified collector is disabled because the procedure name for the collector address space has not been specified in the configuration.

User response

To enable this collector, specify the procedure name for collector address space. If the procedure name is specified and this message still occurs, contact IBM® Software Support.
Parent topic: Error messages and codes: AUIAxxxx

AUIA024I *<Collector name>* collector is disabled: not configured.

Explanation

The specified collector is disabled because it has not been configured.

User response

To enable this collector, configure it using the Guardium user interface. If the specified collector is configured and the message still occurs, contact IBM® Software Support.
Parent topic: Error messages and codes: AUIAxxxx

AUIA027E Abend occurred while validating *<log stream>*. Abend code = *<code>*, RSN = *<reason>*.

Explanation

The Log Stream *log stream* validation failed with abend code *code* and reason code *reason*.

User response

Contact IBM Software Support.
Parent topic: Error messages and codes: AUIAxxxx

AUIA028S Agent *agent-name* on *PLEX name* for S-TAP version *S-TAP version* is already online. *(ADS_SHM_ID=<Memory Segment ID>)*

Explanation

The specified agent is already online. Agent names must be unique per sysplex.

User response

Change the *agent-name* and restart the agent, or shut down the other agent.
Parent topic: Error messages and codes: AUIAxxxx

AUIA029I *collector* collector is disabled: no Audit IMS Log Events are selected for IMS source *IMS*.

Explanation

An Audit IMS Log Event must be selected for the IMS source *IMS* for the collector to be enabled.

User response

To enable the collector, select an Audit IMS Log Event for the IMS source.
Parent topic: Error messages and codes: AUIAxxxx

AUIA030I *collector* collector started successfully.

Explanation

The specified collector started.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA031I *collector* collector stopped successfully.

Explanation

The specified collector stopped.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA033I (GDM) Attempting to establish link with the appliance.

Explanation

The agent is attempting to establish a connection to one of the appliances specified in the agent configuration.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA034S (GDM) An attempt to establish the link to the appliance failed.

Explanation

The agent could not establish a connection to any of the appliances specified in the configuration.

User response

Contact your network administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIAxxxx

AUIA035W (GDM) Link failed over to a secondary appliance. [host=*host*, port=*port*]

Explanation

The agent lost connection to the primary appliance and switched to the specified secondary appliance.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA036I (GDM) Link to primary appliance established. [host=*host*, port=*port*]

Explanation

The agent has connected to the specified primary appliance.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA037I (GDM) Link to primary appliance restored. [host=*host*, port=*port*]

Explanation

The agent has reconnected to the specified primary appliance.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA038S (GDM) Link to the appliance lost.

Explanation

All attempts to connect to the appliances specified in the configuration have failed.

System action

Any new policies defined in the appliance will not be pushed down to the IBM® Guardium® S-TAP® for IMS agent.

User response

Verify network connectivity to the appliance. Contact your network administrator or IBM Software Support.
Parent topic: Error messages and codes: AUIAxxxx

AUIA041I Guardium® policy processing failed due to prior errors.

Explanation

The Guardium policies could not be processed.

User response

Check the log for previous errors.
Parent topic: Error messages and codes: AUIAxxxx

AUIA042W The Guardium® policy is not applicable.

Explanation

One or more of the policy rules cannot be used by the current agent.

User response

Check the log for previous errors to determine why the policy is not applicable and fix the policy definition.
Parent topic: Error messages and codes: AUIAxxxx

AUIA043I The Guardium® policy reader thread started.

Explanation

The Guardium policy reader thread started.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA044I The Guardium® policy reader thread is terminating.

Explanation

The Guardium policy reader thread is stopping.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA045I The guardium policy reader thread is terminating due to prior errors.

Explanation

The policy reader thread is stopping due to previously reported errors.

User response

Check the previously issued messages to determine why the policy reader is terminating.
Parent topic: Error messages and codes: AUIAxxxx

AUIA048I *auiu_taskname* is configured to start only on *lpar-name*.

Explanation

The configuration file pointed to by the AUICONFG DD statement contains an AUIU_EXCLUDE_LPAR statement that has the *ALL parameter supplied as the excluded LPAR name.

System action

The AUIUSTC task is scheduled only on the home LPAR where the agent is running.

User response

To schedule the AUIUSTC task for another LPAR, remove or correct the AUIU_EXCLUDE_LPAR statement.
Parent topic: Error messages and codes: AUIAxxxx

AUIA049W *auiu_task_name* is configured to not start on *lpar_name* but will be started on *lpar_name* because *aui_agent_name* runs on *lpar_name*

Explanation

The AUIU_EXCLUDE_LPAR configuration parameter, found in the AUICONFG SAMPLIB member, was used in an attempt to prevent the AUIU task from executing on the LPAR named.

System action

The request to exclude this LPAR from AUIU processing is ignored because the specified LPAR is also where the agent is executing.

User response

Remove the LPAR name from the AUICONFG samplib member's AUIU_EXCLUDE_LPAR parameter. The change will be implemented at the next restart of the agent.
Parent topic: Error messages and codes: AUIAxxxx

AUIA050W *auiu_task_name* is configured to not start on *lpar_name* but no such system exists.

Explanation

The specified *lpar_name* has been included as part of the LPARS that are specified in the AUIU_EXCLUDE_LPAR configuration keyword. The specified *lpar_name* was not found in the list of members of either the SYSJES or *lpar_name* XCF groups.

System action

Processing continues.

User response

This message might indicate that the lpar_name is not available or that there is an error in the specified lpar_name.
Parent topic: Error messages and codes: AUIAxxxx

AUIA051I *auiu_task_name* is configured to not start on *lpar_name* and will not be started on *lpar_name*.

Explanation

The AUIU_EXCLUDE_LPAR configuration, parameter found in the AUICONFG SAMPLIB member, was used in an attempt to prevent the AUIU task from executing on the specified LPAR.

System action

An instance of the AUIU task is not routed to the excluded LPAR.

User response

None.
Parent topic: Error messages and codes: AUIAxxxx

AUIA052I Discovered <plex-name> system <system-name>.

Explanation

This LPAR name was found as a member of the XCF group when performing a z/OS IXCQUERY on the PLEXNAME of SYSJES XCF GROUPS.

System action

Processing continues

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA053I Agent configuration option <*option*> has been updated to <*value*>.

Explanation

This message indicates that command such as: /f AUIASTC,SET CONFIG <*option*> ON/OFF processed successfully.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA054I Agent configuration option <*option*> is set to <*value*>.

Explanation

This message indicates that command such as: /f AUIASTC,GET CONFIG <*option*> processed successfully.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA055I The agent is waiting for start-up information from the appliance.

Explanation

The agent has determined that there is no checkpoint information available for this agent in E/CSA, and is awaiting this data to be sent from the appliance.

System action

The agent waits up to 30 seconds for the checkpoint information, and if none is received, processing continues by using default checkpoint values, such as current blocks from the z/OS log-streams, and SMF and SLDS data sets that were created no earlier than the previous day.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA056I Starting the agent collectors.

Explanation

The agent is starting the auditing threads.

System action

The agent starts the DLIO/DLIB/AUIL/AUIF auditing threads.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA057I Issuing request to capture agent status.

Explanation

A command, such as /f AUIASTC,STATUS, has been issued for processing.

User response

No action is required.

Parent topic: Error messages and codes: AUIAxxxx

AUIA058I Request to capture agent status has completed successfully.

Explanation

A command, such as /f AUIASTC,STATUS has processed successfully.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA059I Policy XMl echo

Explanation

If the XML_ECHO_AUILOG(Y) keyword exists in the AUICONFG, this message will be followed by the echo of all active XML policies on the AUILOG.

System action

As an example, the first three lines of the echo appear as follows:

```
<?xml version="1.0" encoding="IBM-1047" standalone="yes"?>
<!-- 2019-03-25-13.35.57.354196 -->
<install-info>
```

User response

For more information, see Echoed XML statement definitions.
Parent topic: Error messages and codes: AUIAxxxx

AUIA060W Policy XML echo to data set skipped: *<MESSAGE> <LOCATION>*

Explanation

The XML of the policy that was installed from the Security Guardium® system was not echoed to the specified location due to the specified message. If the &Data_Set_Name parameter contains z/OS system variables, <LOCATION> reflects the data set name after symbol substitution has been done.

<MESSAGE> <LOCATION> can be:

- The installed policy has not been changed. The echo is skipped if the newly installed policy has not changed since it was last installed.
- The data set location is not valid. Incorrect use of a system symbol in the &Data_Set_Name parameter can invalidate the location. Additional requirements:
  - The data set name must not exceed 44 characters.
  - The segment length must be greater than zero and less than or equal to 8.
  - The first character in each segment must be a letter (A – Z), #, @, $, or hyphen.

System action

Processing continues.

User response

Correct the &Data_Set_Name parameter and restart the agent. If the error persists, see Additional causes of AUIA060W .
Parent topic: Error messages and codes: AUIAxxxx

AUIA061I Policy XML echo to data set *<LOCATION>* completed.

Explanation

The agent has completed the XML echo of all active policies that were installed from the Security Guardium® system. *<LOCATION>* is the data set name specified by the &Data_Set_name parameter of the XML_ECHO_DATASET keyword.

System action

The data set name reflects the z/OS system variable substitution and the Generation Data Group extension if either exists in the &Data_Set_name parameter.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

Error messages and codes: AUIBxxxx

The following information is about error messages and codes that begin with AUIB.

- **AUIB300I**
  CONNECTION TO z/OS® SYSTEM *type* LOG STREAM WAS SUCCESSFUL - LOG STREAM NAME: *log_stream_name*, LOG STREAM TYPE: *XCF-BASED|DASD_ONLY*, CHECKPOINT VALUE: *check_point_value*, CHECKPOINT PTR: *address_of_checkpoint*

- **AUIB302I**
  DRAIN REQUEST FOR *type* LOG STREAM HAS COMPLETED. LOG STREAM: *name*.
- **AUIB305I**
  DRAIN COMPLETE FOR LOG STREAM *log-stream name*
- **AUIB306E**
  INVALID RECORD FOUND IN *log-stream* LOG STREAM -RECORD IMAGE SNAPPED TO AUI$NAP DD
- **AUIB700I**
  type: *LOGSTREAM CHECKPOINT INFORMATION* - LOG STREAM NAME: *log-stream-name* - CHECKPOINT VALUE: *check_point_value* - LAST UPDATED (UTC): *date_time*

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIB300I CONNECTION TO z/OS® SYSTEM *type* LOG STREAM WAS SUCCESSFUL - LOG STREAM NAME: *log_stream_name*, LOG STREAM TYPE: *XCF-BASED|DASD_ONLY*, CHECKPOINT VALUE: *check_point_value*, CHECKPOINT PTR: *address_of_checkpoint*

Explanation

The connection to the log-stream name (*log_stream_name*) configured to process *log_stream_type* events completed successfully.

System action

Processing continues

User response

No action is required.
Parent topic: Error messages and codes: AUIBxxxx

AUIB302I DRAIN REQUEST FOR *type* LOG STREAM HAS COMPLETED. LOG STREAM: *name*.

Explanation

A DRAIN request, which reads all data from the z/OS® log stream, has completed.

System action

The AUIASTC tasks prepare to terminate.

User response

No action is required.
Parent topic: Error messages and codes: AUIBxxxx

AUIB305I DRAIN COMPLETE FOR LOG STREAM *log-stream name*

Explanation

A DRAIN request used to flush read all existing events from the log-stream-name indicated has completed successfully

System action

The log-stream reader thread will start the termination phase.

User response

No action is required.
Parent topic: Error messages and codes: AUIBxxxx

AUIB306E INVALID RECORD FOUND IN *log-stream* LOG STREAM -RECORD IMAGE SNAPPED TO AUI$NAP DD

Explanation

When reading DLI call audit records from the z/OS System log stream, a malformed audit record was encountered or the version of the audit record was not recognized.

System action

Processing continues after writing a SNAP/DUMP of the offending record to the AUI$NAP DD.

User response

First, verify that the S-TAP version that is running in the IMS Control Region and/or Batch Region is the same as is running in the agent. If adjusting the version does not resolve the issue, forward the AUI$NAP output to IBM Software Support.
Parent topic: Error messages and codes: AUIBxxxx

AUIB700I type: *LOGSTREAM CHECKPOINT INFORMATION* - LOG STREAM NAME: *log-stream-name* - CHECKPOINT VALUE: *check_point_value* - LAST UPDATED (UTC): *date_time*

Explanation

This message provides the highest block ID for the log stream. This is used as the starting checkpoint for processing data from this log stream.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIBxxxx

Error messages and codes: AUIFxxxx

The following information is about error messages and codes that begin with AUIF.

- **AUIF002I**
  SMF log reader interval set to *<n>* minutes.
- **AUIF003E**
  Command *<command>* failed; interval value must be between *<lower-bound>* and *<upper-bound>*.
- **AUIF501I**
  NO NEW CATALOGED SMF DATA SETS FOUND FOR SMF MASK: *smf_mask_value*
- **AUIF502I**
  PROCESSING SMF DATA SET: *smf_data_set_name*
- **AUIF503I**
  PROCESSING COMPLETE FOR SMF DATA SET: *smf_data_set_name*
- **AUIF505I**
  SMF AUDITING IS DISABLED AT THE AGENT LEVEL
- **AUIF506I**
  SMF AUDITING IS DISABLED AT THE IMS LEVEL. IMS NAME: *ims_name*
- **AUIF507E**
  PROCESSING FAILED FOR SMF DATA SET: *data set name*
- **AUIF508I**
  SCANNING RECON DATA SETS FOR IMS ARTIFACT DATA SETS. **RECON1:** *recon1_dsn* **RECON2:** *recon2_dsn* **RECON3:** *recon3_dsn*
- **AUIF702I**
  SMF MASK CHECKPOINT INFORMATION - MASK VALUE : *SMF_mask* - LAST DSN READ: *SMF_dsn* - LAST UPDATED (UTC): *date_time*

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIF002I SMF log reader interval set to *<n>* minutes.

Explanation

The subtask that reads event data from SMF log data sets is scheduled to perform every <n> minutes.

User response

No action is required.
Parent topic: Error messages and codes: AUIFxxxx

AUIF003E Command *<command>* failed; interval value must be between *<lower-bound>* and *<upper-bound>*.

Explanation

This message indicates that *<command>* such as:

```
/f AUIASTC,SET INTERVAL <number>
```

failed because of incorrect *<number>* value. Correct value must be between <lower-bound> and <upper-bound>.

User response

Use an interval value between *<lower-bound>* and *<upper-bound>*. If that does not resolve the issue, contact IBM® Software Support.
Parent topic: Error messages and codes: AUIFxxxx

AUIF501I NO NEW CATALOGED SMF DATA SETS FOUND FOR SMF MASK: *smf_mask_value*

Explanation

When scanning the z/OS® catalog for new data sets that meet the indicated SMF mask value (*smf_mask_value*) and have not been processed by the product, it was determined that no z/OS data sets meet that criteria.

System action

The process will continue to examine other SMF Mask values.

User response

No action is required.
Parent topic: Error messages and codes: AUIFxxxx

AUIF502I PROCESSING SMF DATA SET: *smf_data_set_name*

Explanation

Processing has started for a SMF data set.

System action

Events will be obtained from the SMF data set based on collection profile criteria.

User response

None.
Parent topic: Error messages and codes: AUIFxxxx

AUIF503I PROCESSING COMPLETE FOR SMF DATA SET: *smf_data_set_name*

Explanation

Processing of the SMF data set has completed.

System action

Processing continues with other candidate SMF data sets.

User response

No action is required.
Parent topic: Error messages and codes: AUIFxxxx

AUIF505I SMF AUDITING IS DISABLED AT THE AGENT LEVEL

Explanation

Auditing of SMF events has been disabled at the agent level, as instructed by the settings chosen in the Guardium user interface.

System action

The auditing of events sourced from SMF data sets is not performed.

User response

No action is required.
Parent topic: Error messages and codes: AUIFxxxx

AUIF506I SMF AUDITING IS DISABLED AT THE IMS LEVEL. IMS NAME: *ims_name*

Explanation

Auditing of SMF events has been disabled at the IMS level for the IMS named (*ims_name*) by use of the Guardium interface and the IMS Auditing Levels editor.

System action

The auditing of events sourced from SMF for the IMS named is not performed.

User response

If this is a desired action, then no response is needed. If SMF events should be audited for this IMS, then the IMS configuration should be modified by using the Guardium interface and the IMS Auditing Levels to select any or all SMF events you want to audit.
Parent topic: Error messages and codes: AUIFxxxx

AUIF507E PROCESSING FAILED FOR SMF DATA SET: *data set name*

Explanation

Processing failed during the reading of the data set, specified by name in the message text.

System action

The collection process terminates.

User response

Determine the cause of the failure and correct it by reviewing previously issued S-TAP and z/OS messages.
Parent topic: Error messages and codes: AUIFxxxx

AUIF508I SCANNING RECON DATA SETS FOR IMS ARTIFACT DATA SETS. RECON1: *recon1_dsn* RECON2: *recon2_dsn* RECON3: *recon3_dsn*

Explanation

The AUIFSTC task has started to scan the RECON data sets looking for database data sets, Image copy data sets and optionally IMS SLDS to be audited using SMF records.

System action

The RECON data sets are read using the specified DSN.

User response

No action is required.
Parent topic: Error messages and codes: AUIFxxxx

AUIF702I SMF MASK CHECKPOINT INFORMATION - MASK VALUE : *SMF_mask* - LAST DSN READ: *SMF_dsn* - LAST UPDATED (UTC): *date_time*

Explanation

This message provides the SMF data set mask (*SMF_mask*) and the last SMF data set read (*SMF_dsn*) that matched that mask. This information is used as a checkpoint to indicate which SMF data sets have already been processed, and should not be re-read by the AUIFstc tasks.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIFxxxx

Error messages and codes: AUIGxxxx

The following information is about error messages and codes that begin with AUIG.

- **AUIG001S**
  An unexpected error occurred (/path/to/file.c, linenum).
- **AUIG002S**
  An unexpected error occurred with token "token1" (/path/to/file.c,linenum).
- **AUIG003S**
  An unexpected error occurred with tokens "token1" and "token2" (/path/to/file.c,linenum).
- **AUIG004S**
  An unexpected error occurred with tokens "token1", "token2", "token3", and "token4" (/path/to/file.c,linenum).
- **AUIG005S**
  An unexpected error occurred with tokens "token1", "token2", and "token3" (/path/to/file.c,linenum).
- **AUIG006S**
  An unexpected error occurred with tokens "token1" and "token2" (/path/to/file.c,linenum).
- **AUIG014E**
  dataspace create return code = *return-code-hex*, reason = *reason-code-hex*

- **AUIG015W**
  MALLOC: big alloc coming *memory_size* from GDM Read Buffer
- **AUIG016S**
  MALLOC: zero alloc from *<site>*.
- **AUIG017S**
  MALLOC: negative malloc *memory size* at site *site*.
- **AUIG018S**
  MALLOC failed, got NULL for size *<memory_size>* at site *<site>*.
- **AUIG045E**
  Write failed, sd=*bbbb* desired write len *length* buffer at *address*, ret code *xxxx* reason 0x*yyyyzzzz*
- **AUIG046E**
  Failure to resolve address for host *'HOST'*, ret code *return-code*, reason *hex-value*.
- **AUIG047E**
  Set sockopt failed, level = *hex-value*, option = *hex-value*, ret code *return-code*, reason *hex-value*.
- **AUIG048E**
  Get sockopt failed, ret code *return-code*, reason *hex-value*.
- **AUIG049E**
  BPXFCT failed, ret code *<return-code>*; reason *<reason-code>*.
- **AUIG050E**
  Read failed ret code *xxxx* reason 0x*zzzzzzzz*
- **AUIG051I**
  TCP write disabled
- **AUIG052I**
  Write to megabuffer disabled
- **AUIG053I**
  Unexpected payload received *<hexadecimal string>*. Payload ignored.
- **AUIGF120I**
  Trace Settings: Compilation 0, Requested Runtime 0, ECSA Flag 32, Actual Runtime 0...
- **AUIGF201I**
  Valid stage zero filter criteria found.
- **AUIGF202I**
  No valid stage zero filter criteria found.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIG001S An unexpected error occurred (/path/to/file.c, linenum).

Explanation

An unknown and unexpected internal error occurred in the product due to the specified tokens.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIGxxxx

AUIG002S An unexpected error occurred with token "token1" (/path/to/file.c,linenum).

Explanation

An unknown and unexpected internal error occurred in the product due to the specified tokens.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIGxxxx

AUIG003S An unexpected error occurred with tokens "token1" and "token2" (/path/to/file.c,linenum).

Explanation

An unknown and unexpected internal error occurred in the product due to the specified tokens.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIGxxxx

AUIG004S An unexpected error occurred with tokens "token1", "token2", "token3", and "token4" (/path/to/file.c,linenum).

Explanation

An unknown and unexpected internal error occurred in the product due to the specified tokens.

User response

Contact IBM® Software Support
Parent topic: Error messages and codes: AUIGxxxx

AUIG005S An unexpected error occurred with tokens "token1", "token2", and "token3" (/path/to/file.c,linenum).

Explanation

An unknown and unexpected internal error occurred in the product due to the specified tokens.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIGxxxx

AUIG006S An unexpected error occurred with tokens "token1" and "token2" (/path/to/file.c,linenum).

Explanation

An unknown and unexpected internal error occurred in the product due to the specified tokens.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIGxxxx

AUIG014E dataspace create return code = *return-code-hex*, reason = *reason-code-hex*

Explanation

An attempt to create a data space for spill usage has failed. Spill capability might not be available.

User response

Examine the return code and reason code, and take appropriate action to ensure that data spaces can be created.
Parent topic: Error messages and codes: AUIGxxxx

AUIG015W MALLOC: big alloc coming *memory_size* from GDM Read Buffer

Explanation

More than 10,485,760 bytes was required in order to process collection policies pushed from the Security Guardium® system.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIGxxxx

AUIG016S MALLOC: zero alloc from *<site>*.

Explanation

Zero bytes was required in order to process collection policies pushed from the Security Guardium® system.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIGxxxx

AUIG017S MALLOC: negative malloc *memory size* at site *site*.

Explanation

Negative number of bytes required in order to process collection policies pushed from the Security Guardium® system.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIGxxxx

AUIG018S MALLOC failed, got NULL for size *<memory_size>* at site *<site>*.

Explanation

Attempt to allocate memory failed.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIGxxxx

AUIG045E Write failed, sd=*bbbb* desired write len *length* buffer at *address*, ret code *xxxx* reason 0x*yyyyzzzz*

Explanation

An attempt to read or write to a socket has failed. This error might occur if Security Guardium® S-TAP® for IMS is connected to a peer that is offline.

System action

The system attempts to reestablish the connection to the peer in order to read or write the data.

User response

Identify the cause of the failure by using the *z/OS® UNIX System Services Messages and Codes SA23-2284-xx* manual to look up the return and return codes that are provided in the message text, where *bbbb* is an internal code, *xxxx* is the return code, and *yyyyzzzz* is the reason code. Use the *zzzz* value to determine the error code, as described in the Reason codes (errnojrs) section of the *z/OS UNIX System Services Messages and Codes* manual.
Parent topic: Error messages and codes: AUIGxxxx

AUIG046E Failure to resolve address for host *'HOST'*, ret code *return-code*, reason *hex-value*.

Explanation

An attempt to resolve the given hostname failed.

User response

Verify that the hostname is specified correctly and is resolvable. Contact IBM® Software Support if hostname is correct and resolvable.
Parent topic: Error messages and codes: AUIGxxxx

AUIG047E Set sockopt failed, level = *hex-value*, option = *hex-value*, ret code *return-code*, reason *hex-value*.

Explanation

An attempt to set a socket option failed.

User response

Contact IBM® Software Support
Parent topic: Error messages and codes: AUIGxxxx

AUIG048E Get sockopt failed, ret code *return-code*, reason *hex-value*.

Explanation

An attempt to set a socket option failed.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIGxxxx

AUIG049E BPXFCT failed, ret code *<return-code>*; reason *<reason-code>*.

Explanation

The system BPXFCT call failed while attempting to set socket blocking mode.

User response

See the *MVS Programming: Authorized Assembler Services Guide* for more information about the specified information and error codes.
Parent topic: Error messages and codes: AUIGxxxx

AUIG050E Read failed ret code *xxxx* reason 0x*zzzzzzzz*

Explanation

An attempt to read or write to a socket has failed. This error might occur if Security Guardium® S-TAP® for IMS is connected to a peer that is offline.

System action

The system attempts to reestablish the connection to the peer in order to read or write the data.

User response

Identify the cause of the failure by using the z/OS USS Return Codes and Reason Codes to look up the return and reason codes that are provided in the message text, where *xxxx* is the return code and *zzzzzzzz* is the reason code.
Parent topic: Error messages and codes: AUIGxxxx

AUIG051I TCP write disabled

Explanation

TCP/IP processing has been disabled.

System action

The Guardium appliance will not receive data.

User response

No action is required.
Parent topic: Error messages and codes: AUIGxxxx

AUIG052I Write to megabuffer disabled

Explanation

TCP/IP buffer has been disabled.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIGxxxx

AUIG053I Unexpected payload received *<hexadecimal string>*. Payload ignored.

Explanation

An unexpected string of data was received by the Security Guardium® S-TAP® for IMS agent from the Guardium appliance or associated firewall. The string does not conform to the format that is normally associated with a pushed-down policy or other expected data.

System action

The string is ignored and normal processing continues.

User response

If this message appears occasionally, no action is required. If this message appears frequently, contact IBM Support to diagnose whether a problem exists with the Guardium appliance or firewall.
Parent topic: Error messages and codes: AUIGxxxx

AUIGF120I Trace Settings: Compilation 0, Requested Runtime 0, ECSA Flag 32, Actual Runtime 0...

Explanation

This message is produced during the compilation of a filter, using the policy information that was specified.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIGxxxx

AUIGF201I Valid stage zero filter criteria found.

Explanation

The collection profile compilation process found that the collection profile criteria will allow for Stage zero filtering of IMS DLI events based on USERIDs or PSB names.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIGxxxx

AUIGF202I No valid stage zero filter criteria found.

Explanation

The collection profile compilation process found that the collection profile criteria is not conducive to providing Stage 0 filtering for IMS DLI events. The reasons may include:

- No USERIDS or PSBS were specified in the selection criteria.
- Multiple RULES were defined and differences in the USERID and/or PSB specifications in each rule were different.

System action

Processing continues without Stage Zero filtering capability.

User response

If Stage 0 filtering is desired, adjust the USERID and PSB specifications in each rule to be the same.
Parent topic: Error messages and codes: AUIGxxxx

Error messages and codes: AUIIxxxx

The following information is about error messages and codes that begin with AUII.

Note: To set a z/OS message alert for messages that begin with AUII, use single-dash formatting between the message number and message text. For example:

```
AUII056I
- ZIIP PROCESSING ENABLED FOR IMS STAP
```

- **AUII017I**
  S-TAP® for V10.1.3 initialization complete using RECON1 DSN: *recon1_dsn*
- **AUII018E**
  IBM® Security Guardium® S-TAP for IMS on z/OS® initialization failed
- **AUII019E**
  IBM Security Guardium S-TAP for IMS on z/OS termination failed
- **AUII020E**
  UNABLE TO FIND RECON1 DATA SET NAME

- **AUII021E**
  BLDL FAILED FOR ACTION MODULE *module_name*
- **AUII022E**
  INSUFFICENT STORAGE AVAILABLE FOR *module_name* ACTION MODULE (*stg_type*)
- **AUII023E**
  IMODULE DIRLOAD FAILED FOR ACTION MODULE *module_name*
- **AUII024E**
  Unable to locate IMS SCD address.
- **AUII025E**
  Unable to locate IMS SSCD Extension address.
- **AUII026E**
  UNABLE TO LOCATE THIS IMS SSCT ADDRESS
- **AUII027E**
  INSUFFICIENT STORAGE AVAILABLE FOR AUIPLOG CONTROL BLOCK
- **AUII028E**
  IMODULE LOAD OF ACTION MODULE *module_name* FAILED
- **AUII029E**
  DFSTCBTB LOCATE SERVICE CALL FAILED
- **AUII031E**
  STAP FOR IMS INTERNAL LOGIC ERROR *(rc)*
- **AUII038E**
  ITASK CREATE FOR ACTION MODULE *module_name* FAILED
- **AUII040E**
  ODBA LOAD OF DFSISSI0 FAILED
- **AUII041E**
  ODBA HOOK POINT NOT FOUND (module_name)
- **AUII042W**
  ZIIP PROCESSOR NOT AVAILABLE ON THIS LPAR
- **AUII043W**
  THIS IMS IS NOT CONNECTED TO WORKLOAD MANAGER
- **AUII044E**
  ZIIP PROCESSING REQUEST HAS BEEN REJECTED
- **AUII046E**
  NAME/TOKEN SERVICE *service-name* SERVICE FAILED (*name value*)
- **AUII049E**
  DEDB CALL ANALYSIS INIT FAILURE RC = *return code*
- **AUII050I**
  S-TAP FOR IMS AUDIT STATISTICS
- **AUII052I**
  `USING IMS STAP V10.1.3 MODULE Module_name APAR# Build_date`
- **AUII055I**
  ZIIP PROCESSING HAS BEEN REQUESTED FOR IMS STAP
- **AUII056I**
  ZIIP PROCESSING ENABLED FOR IMS STAP
- **AUII057I**
  process_type PROCESSING FAILED *RC*: return_code *RSN*: reason_code
- **AUII058A**
  STAP FOR IMS COMPONENT HAS ABENDED
- **AUII060W**
  Potential waited PST=*xxxxxxxx* (PST# = *yyyy*)
- **AUII061I**
  Potential Waited PST xxxxxxxx (PST#= zzzz) RELEASED.
- **AUII120I**
  NO COLLECTIONS ACTIVE FOR THIS IMS INSTANCE
- **AUII172I**
  AUIprogram LOADED EXIT *imsexit* FROM DATA SET: *data set name*
- **AUII173E**
  IMS RELEASE *ims-vrl* IS NOT SUPPORTED
- **AUII174E**
  LOAD OF SERVICE MODULE *module_name* FAILED RC = *return_code*
- **AUII175I**
  NON_ZERO RC FROM EXIT *exit_name*: RC = *return_code*
- **AUII176E**
  module_name service_type SERVICE ERROR: RC: *return_code* RS: *reason_code*
- **AUII177E**
  module_name FOUND WITH RENT/REUS ATTRIBUTE IN NON_APF ENVIRONMENT
- **AUII178E**
  DATA SET NAME: *dsn*

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUII017I S-TAP® for V10.1.3 initialization complete using RECON1 DSN: *recon1_dsn*

Explanation

IBM® Guardium® S-TAP for IMS has initialized in the DLI/DBB batch job or IMS control region environment. For successful auditing to occur, the RECON1 DSN indicated in this message should match the RECON1 DSN associated with the IMS definition you have created.

User response

No action is required.
Parent topic: Error messages and codes: AUIIxxxx

AUII018E IBM® Security Guardium® S-TAP® for IMS on z/OS® initialization failed

Explanation

IBM Guardium S-TAP for IMS was unable to initialize in this IMS Control region. The monitoring of IMS databases will not occur.

System action

IMS processing continues without auditing capabilities.

User response

Examine the JES log for other messages to determine the reason for the initialization failure.
Parent topic: Error messages and codes: AUIIxxxx

AUII019E IBM® Security Guardium® S-TAP® for IMS on z/OS® termination failed

Explanation

IBM Guardium S-TAP for IMS was unable to terminate cleanly.

System action

The termination of the IMS online region of DLI/DBB batch job step continues.

User response

This error indicates that an environmental error has occurred. Examine the JES log for other AUI messages to determine the reason for the termination failure.
Parent topic: Error messages and codes: AUIIxxxx

AUII020E UNABLE TO FIND RECON1 DATA SET NAME

Explanation

An attempt to find the RECON1 data set name used by the IMS Online control region or DLI/DBB batch job step has failed. The RECON1 data set name is critical to the determination of the collection profile used to audit IMS events.

System action

IMS processing continues without the IMS auditing feature.

User response

Determine why the RECON1 data set name is not available for this IMS control region or DLI/DBB batch job step. An in-stream RECON1 DD statement must be present in the JCL, or a RECON1 MDALIB member being present in the JOB/STEPLIB DD concatenation is required.
Parent topic: Error messages and codes: AUIIxxxx

AUII021E BLDL FAILED FOR ACTION MODULE *module_name*

Explanation

An attempt to find a required processing module (module_name) has failed.

System action

IMS processing continues without auditing.

User response

Examine the STEPLIB/JOBLIB DD concatenation to ensure the SAUIIMOD product data set is included.
Parent topic: Error messages and codes: AUIIxxxx

AUII022E INSUFFICENT STORAGE AVAILABLE FOR *module_name* ACTION MODULE (*stg_type*)

Explanation

An attempt to obtain storage for the module named (*module_name*) has failed. The storage type field (*stg_type*) indicates if the storage required is 31bit or 24bit based.

System action

IMS processing continues without IMS auditing available.

User response

Increase the region size used by the job step (REGION=).
Parent topic: Error messages and codes: AUIIxxxx

AUII023E IMODULE DIRLOAD FAILED FOR ACTION MODULE *module_name*

Explanation

The DIRLOAD IMS service has failed.

System action

IMS processing continues with auditing.

User response

Determine the cause of the error from the IMS Messages and Codes manual and correct the error. If necessary, contact IBM® Software Support.
Parent topic: Error messages and codes: AUIIxxxx

AUII024E Unable to locate IMS SCD address.

Explanation

An attempt to locate the IMS SCD during product initialization has failed.

System action

IMS processing continues without auditing.

User response

Verify that you are attempting to run the product using a supported IMS release. Contact IBM® Software Support for further assistance.
Parent topic: Error messages and codes: AUIIxxxx

AUII025E Unable to locate IMS SSCD Extension address.

Explanation

An attempt to locate the IMS SSCD Extension address has failed.

System action

IMS processing continues without auditing.

User response

Verify that you are attempting to run the product using a supported IMS release. Contact IBM Software Support for further assistance.
Parent topic: Error messages and codes: AUIIxxxx

AUII026E UNABLE TO LOCATE THIS IMS SSCT ADDRESS

Explanation

The IMS SCCT address cannot be located by the IMS S-TAP initialization process.

System action

IMS processing continues without auditing capabilities.

User response

Contact IBM Software Support.
Parent topic: Error messages and codes: AUIIxxxx

AUII027E INSUFFICIENT STORAGE AVAILABLE FOR AUIPLOG CONTROL BLOCK

Explanation

An attempt to obtain E/CSA to hold the AUIPLOG module has failed.

System action

IMS processing continues without auditing.

User response

Investigate E/CSA usage on the LPAR.
Parent topic: Error messages and codes: AUIIxxxx

AUII028E IMODULE LOAD OF ACTION MODULE *module_name* FAILED

Explanation

An attempt to LOAD module module_name using IMS services has failed.

System action

An attempt to LOAD module module_name using IMS services has failed.

User response

Verify that the SAUIIMOD product data set is available in the STEPLIB/JOBLIB data set concatenation. Contact IBM® Software Support for further assistance.
Parent topic: Error messages and codes: AUIIxxxx

AUII029E DFSTCBTB LOCATE SERVICE CALL FAILED

Explanation

A call to the IMS DFSTCBTB service has failed.

System action

IMS processing continues without auditing.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIIxxxx

AUII031E STAP FOR IMS INTERNAL LOGIC ERROR *(rc)*

Explanation

Security Guardium® S-TAP® for IMS initialization found a logic error.

System action

IMS processing continues without auditing.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIIxxxx

AUII038E ITASK CREATE FOR ACTION MODULE *module_name* FAILED

Explanation

DA call to the DFSCIR IMS service to create an ITASK has failed.

System action

IMS processing continues without auditing.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIIxxxx

AUII040E ODBA LOAD OF DFSISSI0 FAILED

Explanation

An attempt to LOAD IMS module DFSISSI0 has failed.

System action

IMS processing with auditing continues. The product will be unable to determine the correct USERID for events driven from ODBA threads.

User response

Contact Software Support.
Parent topic: Error messages and codes: AUIIxxxx

AUII041E ODBA HOOK POINT NOT FOUND (module_name)

Explanation

An attempt to locate a hook point in the indicated module (module_name) has failed.

System action

IMS processing with auditing continues. The product will be unable to determine the correct USERID for events driven from ODBA threads. An output DD: AUI$NAP is dynamically allocated to SYSOUT, and the area where the hook point was to be located is snapped out to this AUI$NAP DD.

User response

Provide the AUI$NAP output to IBM Software Support.
Parent topic: Error messages and codes: AUIIxxxx

AUII042W ZIIP PROCESSOR NOT AVAILABLE ON THIS LPAR

Explanation

The AUIZIIP DD statement has been found in the IMS Control Region JCL, which indicates that the zIIP processor should be considered for use when filtering DLI calls and writing to the z/OS® System Logger. IMS STAP has determined that zIIP processing is not available on this LPAR.

System action

Processing continues exclusively using general processors.

User response

Remove the AUIZIIP DD statement and restart the IMS sub-system.
Parent topic: Error messages and codes: AUIIxxxx

AUII043W THIS IMS IS NOT CONNECTED TO WORKLOAD MANAGER

Explanation

A request to process DLI call filtering and z/OS® System Logger writes on a zIIP processor has been rejected as the IMS sub-system is not connected to the z/OS Workload Manager.

System action

Processing continues exclusively using general processors.

User response

No action is required.
Parent topic: Error messages and codes: AUIIxxxx

AUII044E ZIIP PROCESSING REQUEST HAS BEEN REJECTED

Explanation

A request to process DLI call filtering and z/OS® System Logger writes on a zIIP processor has been rejected.

System action

Processing continues exclusively using general processors.

User response

Review previously issued AUII messages to determine the root cause of the request rejection.
Parent topic: Error messages and codes: AUIIxxxx

AUII046E NAME/TOKEN SERVICE *service-name* SERVICE FAILED (*name value*)

Explanation

An attempt to drive the z/OS® name/token service has failed.

System action

IMS processing continues without auditing.

User response

Contact IBM® Software Support
Parent topic: Error messages and codes: AUIIxxxx

AUII049E DEDB CALL ANALYSIS INIT FAILURE RC = *return code*

Explanation

An attempt insert product code in the DEDB call analysis area has failed.

System action

IMS processing with DEDB event auditing disabled. An output DD: AUI$NAP is dynamically allocated to SYSOUT, and the area where the code insertion was to be located is snapped out to this AUI$NAP DD.

User response

Provide the AUI$NAP output to IBM® Software Support.
Parent topic: Error messages and codes: AUIIxxxx

AUII050I S-TAP® FOR IMS AUDIT STATISTICS

Explanation

This message provides statistics regarding the number of DLI events which have been processed. This message is issued when:

- The number of DLI calls specified in the message frequency section of the Guardium client's IMS Data Set definition screen has been reached.
- The time specified in the AUII050I message frequency section of the Guardium client's IMS Data Set definition screen has elapsed.
- The collection profile for the IMS is made in active.
- The DLI/DBB batch job or IMS Online Control Region terminates.

The description of values are as follows:

DLI CALLS RECEIVED
: This value indicates the number of IMS DLI calls which had the potential of being audited. This number can be more or less than the number of actual DLI calls performed, because:

  - DLI PATH calls which effect multiple segments within a hierarchical path are treated and counted as individual DLI calls.
  - DLI calls types which are not included in any RULE of the active collection profile are not counted as they are immediately rejected.

DLI CALLS AUDITED
: This value indicates the number of IMS DLI calls which resulted in a DLI event being written to the z/OS® System Logger Log-stream for transmittal to the Guardium® Appliance.

IXGWRITE ERRORS
: This value indicates the number of z/OS System Logger IXGWRITE calls which have failed. One of more AUIJ304E messages will precede the issuance of the AUII050I message if the number of IXGWRITE errors is greater than zero. A non-zero value for the IXGWRITE ERRORS and a zero value for the DLI CALLS LOST DUE TO IXGWRITE ERRORS section of this message indicates that the IXGWRITE errors were subsequently retried and the IXGWRITE calls were then completed successfully.

DLI CALLS LOST DUE TO IXGWRITE ERRORS
: A non-zero value in this section indicates that DLI calls which were audited and either:

  - Could not be placed into a log-stream data buffer (indicated by the issuance of message AUIJ307A).
  - Audited events already in the data buffer could not be written to the z/OS System Logger Log-Stream using the IXGWRITE call and the collection profile for the IMS has been deactivated or the DLI/DBB batch job or IMS Online Control region has been terminated (indicated by the issuance of message AUIJ304E).

System action

Processing continues.

User response

No action is required. This is an informational message only.
Parent topic: Error messages and codes: AUIIxxxx

AUII052I USING IMS STAP V10.1.3 MODULE *Module_name APAR# Build_date*

Explanation

These messages are issued by the IMS S-TAP® code in the IMS Control region during startup to broadcast the maintenance level of the programs that are in use by Security Guardium® S-TAP for IMS.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIIxxxx

AUII055I ZIIP PROCESSING HAS BEEN REQUESTED FOR IMS STAP

Explanation

The AUIZIIP DD statement has been found in the IMS Control Region JCL, which indicates that the zIIP processor should be considered for use when filtering DLI calls and writing to the z/OS® System Logger.

System action

IMS STAP attempts to create an environment to support zIIP processing.

User response

If this was not intended, remove the AUIZIIP DD statement and restart the IMS sub-system.
Parent topic: Error messages and codes: AUIIxxxx

AUII056I ZIIP PROCESSING ENABLED FOR IMS STAP

Explanation

The request for zIIP support for IMS STAP and this IMS Control Region has been acted on and all initialization processes have completed successfully.

System action

IMS STAP will schedule DLI call filtering and writes to the z/OS® System Logger as a zIIP eligible enclave SRB.

User response

If this was not intended, remove the AUIZIIP DD statement and restart the IMS sub-system.
Parent topic: Error messages and codes: AUIIxxxx

AUII057I *process_type* PROCESSING FAILED *RC*: return_code *RSN*: reason_code

Explanation

The AUIZIIP DD statement has been found in the IMS Control Region JCL, which indicates that the zIIP processor should be considered for use when filtering DLI calls and writing to the z/OS® System Logger. A process (process_type) used to enable zIIP processing has failed.

System action

The request to enable zIIP processing is rejected and general processor will be used.

User response

Review IBM® supplied documentation for the process which failed using the return and reason codes (*return_code/reason_code*) to determine the cause of the failure.
Parent topic: Error messages and codes: AUIIxxxx

AUII058A STAP FOR IMS COMPONENT HAS ABENDED

Explanation

The S-TAP® for IMS component has abnormally ended, causing auditing to disable.

User response

Contact IBM® Software Support
Parent topic: Error messages and codes: AUIIxxxx

AUII060W Potential waited PST=*xxxxxxxx* (PST# = *yyyy*)

Explanation

This warning message indicates that IBM® Guardium® S-TAP® for IMS has detected a dependent region that has been waiting for an event to be audited for at least 15 seconds. The dependent region is identified by the PST address *xxxxxxxx*. The PST# value specified as *yyyy* is the region number in hexadecimal format.

System action

IBM Guardium S-TAP for IMS attempts to process the dependent region.

User response

If the dependent region continues processing, then no action is required. If the dependent region remains in a wait state, then it must be stopped or cancelled. Before you stop or cancel the dependent region, take an SVC dump of the IMS Control region and provide it to IBM Software Support for analysis.
Parent topic: Error messages and codes: AUIIxxxx

AUII061I Potential Waited PST xxxxxxxx (PST#= zzzz) RELEASED.

Explanation

This message is a response to message AUII060W (Potential Waited PST xxxxxxxx (PST#= zzzz)). This message indicates that the corresponding IPOST was performed, and the PST is no longer in a WAIT state.

System action

IMS Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIIxxxx

AUII120I NO COLLECTIONS ACTIVE FOR THIS IMS INSTANCE

Explanation

Initialization has completed successfully for Security Guardium® S-TAP® for IMS, but no collections were found that pertain to this batch job or IMS control region.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIIxxxx

AUII172I *AUIprogram* LOADED EXIT *imsexit* FROM DATA SET: *data set name*

Explanation

The *AUIprogram* named found an occurrence of the *imsexit* later within the JOBLIB/STEPLIB concatenation, and has loaded it.

System action

The *imsexit* will be invoked with R13 pointing to the save area originally provided by IMS, as well as its own 512 byte work area, provided in the SXPLAWRK field of the IMS Standard User Exit Parameter list, immediately following each execution of *AUIprogram*.

User response

For the *imsexit* to run, no action is required. If the *imsexit* should not be run in this environment, remove the data set from the JOBLIB/STEPLIB concatenation and restart the IMS control region or batch job.
Parent topic: Error messages and codes: AUIIxxxx

AUII173E IMS RELEASE *ims-vrl* IS NOT SUPPORTED

Explanation

The IMS release being used is not support by this version of the product.

System action

IMS processing continues without auditing.

User response

Review supported IMS releases for the release of this product.
Parent topic: Error messages and codes: AUIIxxxx

AUII174E LOAD OF SERVICE MODULE *module_name* FAILED RC = *return_code*

Explanation

LOAD OF SERVICE MODULE *module_name* FAILED RC = *return_code*

User response

Ensure that the SAUIIMOD product data set is included in the STEPLIB/JOBLIB DD concatenation.
Parent topic: Error messages and codes: AUIIxxxx

AUII175I NON_ZERO RC FROM EXIT *exit_name*: RC = *return_code*

Explanation

The *exit_name* indicated returned a non-zero return code value of *return_code* as specified.

System action

The return code value is returned to IMS.

User response

Correct the *exit_name* program if the non-zero value was returned in error. Review the IMS Customization Guide or IMS Exit Routine Reference for more information.
Parent topic: Error messages and codes: AUIIxxxx

AUII176E *module_name service_type* SERVICE ERROR: RC: *return_code* RS: *reason_code*

Explanation

The *service_type* invoked by the specified *module_name* has failed.

System action

IMS processing continues without auditing.

User response

Review all subsequent AUI error messages to diagnose the problem.
Parent topic: Error messages and codes: AUIIxxxx

AUII177E *module_name* FOUND WITH RENT/REUS ATTRIBUTE IN NON_APF ENVIRONMENT

Explanation

Program *module_name* had the RENT/REUS attribute on in a non-APF-Authorized environment. Security Guardium® S-TAP® for IMS is unable to load the program.

System action

Processing continues with the exit cascading feature disabled.

User response

Re-link the exit with the NOREUSE attribute.
Parent topic: Error messages and codes: AUIIxxxx

AUII178E DATA SET NAME: *dsn*

Explanation

This message is issued in conjunction with a previous message (for example, AUII176E) to indicate an associated data set.

User response

Check the log for the previously issued, associated message and take the action that is advised in that message.
Parent topic: Error messages and codes: AUIIxxxx

Error messages and codes: AUIJxxxx

The following information is about error messages and codes that begin with AUIJ.

- **AUIJ005W**
  UNABLE TO LOAD MESSAGE TABLE *table_name* RSN: *reason_code* WILL USE AUIMGENU
- **AUIJ006E**
  LOAD FAILED FOR MESSAGE TABLE *table_name* RSN: *reason_code*
- **AUIJ007E**
  PROGRAM *program_name* IS NOT EXECUTING APF-AUTHORIZED
- **AUIJ008I**
  ATTEMPTING TO CONNECT TO THE GUARDIUM S-TAP® APPLIANCE. **TCP/IP Address:** *ip_address*, **PORT:** *port_number*, **PING RATE:** *ping_rate*
- **AUIJ009E**
  LOAD FAILED FOR MODULE *module_name*. R1: *abend_code* R15: *reason_code*
- **AUIJ010I**
  IMS STAP *ver* HAS STARTED.
- **AUIJ011I**
  function_type CALL TO GUARDUIM S-TAP APPLIANCE SUCCESSFUL
- **AUIJ012I**
  NUMBER OF *event_type* EVENTS SENT TO APPLIANCE: *counter*
- **AUIJ013E**
  stap_call TO GUARDUIM S-TAP APPLIANCE FAILED *(call source)* IP ADDRESS: *ip_address* STAP_RC = *rc1* STAP_RS = *rs1* GDM_RC = *rc2* PB_RC = *rc3* GDML_RC = *rc4* GDML_RS = *rs2*
- **AUIJ014E**
  OPEN FAILED FOR DD *dd_name*
- **AUIJ015E**
  THIS IMS RELEASE IS NOT SUPPORTED. IMS NAME: *ims-name*, VRL: *ims_version*
- **AUIJ016E**
  UNABLE TO INITIALIZE APPLIANCE INTERFACE *(connection_type)*
- **AUIJ017I**
  PRIMARY STAP CONNECTION RESTORED *(connection_type)* - SUCCESSFULLY CONNECTED TO IP ADDRESS: *ip_address* - PORT : *port*
- **AUIJ018W**
  PREVIOUS STAP CONNECTION FAILED *(connection_type)* - SUCCESSFULLY CONNECTED TO IP ADDRESS: *ip_address* - PORT : *port*
- **AUIJ019E**
  STAP CONNECTION FAILED: NO CONNECTIONS AVAILABLE *(connection_type)* - IP ADDRESS: *ip-address* - PORT : *port*
- **AUIJ020I**
  All EVENTS HAVE BEEN WRITTEN FROM SPILL AREA TO APPLIANCE *(connection_type)*
- **AUIJ021W**
  EVENTS ARE BEING WRITTEN TO THE SPILL AREA *(connection_type)*
- **AUIJ022W**
  SPILL AREA IS FULL: EVENT DATA IS BEING LOST *(connection_type)*
- **AUIJ023E**
  SPILL AREA IS NOT AVAILABLE *(connection_type)*
- **AUIJ024W**
  NUMBER OF *type* EVENTS LOST *count*
- **AUIJ042W**
  ZIIP PROCESSING NOT AVAILABLE ON THIS LPAR (type)
- **AUIJ044W**
  ZIIP PROCESSING REQUEST HAS BEEN REJECTED *(connection_type)*
- **AUIJ055I**
  ZIIP PROCESSING REQUESTED FOR *type* PROCESSING
- **AUIJ056I**
  ZIIP PROCESSING ENABLED FOR type PROCESSING, ENCLAVE TOKEN: *value*
- **AUIJ057W**
  ZIIP PROCESSING FOR *type* EVENTS HAS BEEN DISABLED DUE TO ERRORS - PROCESSING WILL CONTINUE USING GCPU
- **AUIJ058W**
  ZIIP PROCESSING FOR *type* EVENTS HAS BEEN DISABLED - TRACING IS ENABLED BY THE USE OF THE AUI$NAP JCL STATEMENT
- **AUIJ201E**
  VSAM ERROR ENCOUNTERED
- **AUIJ202E**
  VSAM ERROR ENCOUNTERED
- **AUIJ203E**
  VSAM ERROR ENCOUNTERED
- **AUIJ250I**
  AUDITING IMS EVENTS. COLLECTION PROFILE NAME: *collection_profile_name* IMS NAME: *ims_name* AGENT NAME: *agent name* EXCLUDED REGIONS: *region_types*

- **AUIJ251E**
  COMPILED FILTER BUILD FAILED. COLLECTION PROFILE NAME : *collection _profile_name* RC: *return_code* RSN: *reason_code*
- **AUIJ252W**
  GUARDIUM QUARANTINE IS IN EFFECT; DBPCB STATUS CODES OF *AI* MAY OCCUR
- **AUIJ255I**
  AUII050I MESSAGE RECEIVED FROM: JOBNAME: *ims_job_name*; SSID: *ims_ssid*; JOB NUMBER: *job_number*; LPAR: *lpar_name*
- **AUIJ256I**
  AUIJ250I MESSAGE RECEIVED FROM: JOBNAME: *ims_job_name*; SSID : *ims_ssid*; JOB NUMBER: *job_number*; LPAR: *lpar_name*
- **AUIJ257I**
  AUII120I MESSAGE RECEIVED FROM: JOBNAME: *ims_job_name*; SSID: *ims_ssid*; JOB NUMBER: *job_number*; LPAR: *lpar_name*
- **AUIJ258I**
  AUII052I MESSAGE RECEIVED FROM: JOBNAME: *ims_job_name*; SSID: *ims_ssid*; JOB NUMBER: *job_number*; LPAR: *lpar_name*
- **AUIJ259I**
  JOBNAME *job_name* USING IMS STAP V10.1.3 MODULE: *pgm_name* APAR: *fix_number* DATE: *fix_date*
- **AUIJ303W**
  request_type REQUEST FOR LOG STREAM *log_stream_name* FAILED - RC: *return_code* RS: *reason_code* - WILL CONTINUE TO RETRY
- **AUIJ304A**
  IXGCONN REQUEST FOR LOG_STREAM *log_stream_name* FAILED with RC = *return_code* and RS= *reason_code*
- **AUIJ304E**
  IXGWRITE REQUEST FOR *<log-stream-name>* FAILED - RC: *return_code* RS: *reason_code*
- **AUIJ307A**
  AUDITED EVENTS ARE BEING LOST DUE TO IXGWRITE ERRORS AND/OR BUFFER SHORTAGES
- **AUIJ307E**
  thread_type THREAD IS TERMINATING DUE TO PROCESSING ERRORS.
- **AUIJ330E**
  REQUIRED DATA SET IS NOT CATALOGED. - TYPE: *dsn_type*, DSN: *data_set_name*
- **AUIJ331E**
  service_name SERVICE FAILED - RC: *return_code* - RSN: *reason_code*
- **AUIJ332E**
  DATA SET IS NOT VALID WITHIN CONTEXT USED - TYPE: *data_set_type,* DSN: *data_set_name*, REASON: *reason*
- **AUIJ333E**
  Service *SERVICE FAILED* for *DATA SET*: *dsn - R15: return_code*
- **AUIJ335W**
  dd_name DD IS PRESENT IN THIS JCL, *dsn_types* WILL NOT BE AUDITED
- **AUIJ400E**
  INSUFFICIENT MEMORY - MODULE NAME: *program_name* - MEMORY SEGMENT TYPE: *seg_type*
- **AUIJ401E**
  MODULE *module_name* FAILED DURING ATTACH of *program_name* - RETURN CODE: *return_code*
- **AUIJ402E**
  CATALOG SERVICE REQUEST FAILED - MODULE NAME: *module_name* - RC: *return_code* RSN: *reason_code*
- **AUIJ403E**
  DYNAMIC ALLOCATION FAILURE - FUNCTION : *function_code* - DSN: *data-set-name* - RC: *return_code* RSN: *reason_code*
- **AUIJ404E**
  DYNAMIC ALLOCATION FAILURE - FUNCTION: *function_code* -DDN: *dd_name* - RC: *return_code* RSN: *reason_code*
- **AUIJ406W**
  TOO MANY RULES SPECIFIED IN POLICY, REQUEST HAS BEEN TRUNCATED. POLICY: *policy_name*. RULE LIMIT: *max_number_of rules_allowed*
- **AUIJ407I**
  number DATA SETS ADDED TO POLICY *policy_name* FILTER
- **AUIJ408E**
  POLICY *name* RESULTED IN OVER 102400 DATA SETS TO BE AUDITED; DATA SET RESULT SET HAS BEEN TRUNCATED
- **AUIJ500I**
  STARTING *cycle_type* CYCLE
- **AUIJ501I**
  NO NEW CATALOGED SMF DATA SETS FOUND FOR SMF MASK: - *smf_mask_value*
- **AUIJ504I**
  cycle_type CYCLE COMPLETE
- **AUIJ521W**
  CONTROL BLOCK AUIDCCOM NOT FOUND
- **AUIJ510I**
  `ALTERNATE RECON DATA SETS FOUND FOR IMSNAME imsname: RECON1: alt_dsn_1; RECON2: alt_dsn_2, RECON3: alt_dsn_3`
- **AUIJ511E**
  `ALTERNATE RECON DATA SET NOT CATALOGED; DSN:  alt_dsn`
- **AUIJ512E**
  `ALTERNATE RECON DATA SET NOT A VSAM FILE; DSN:  alt_dsn`
- **AUIJ513E**
  `NO VALID ALTERNATE RECON DATA SETS FOUND FOR IMS imsname;  PROCESSING TERMINATED`
- **AUIJ522E**
  INSUFFICIENT E/CSA STORAGE AVAILABLE FOR *control_block* CONTROL BLOCK
- **AUIJ609I**
  event_types ARE BEING EXCLUDED (*excluded_by*)
- **AUIJ800E**
  REQUIRED DD STATEMENT IS MISSING: *dd-name*
- **AUIJ860E**
  VSAM FILE DEFINITION ERROR - DDN: *dd_name* - REASON: *definition_error*
- **AUIJ999E**
  AN INTERNAL LOGIC ERROR HAS OCCURRED - MODULE: module_name RSN: reason_code

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIJ005W UNABLE TO LOAD MESSAGE TABLE *table_name* RSN: *reason_code* WILL USE AUIMGENU

Explanation

An attempt to perform a z/OS® LOAD of the message table named (*table_name*) failed. The reason for the failure is described in the reason code field (*reason_code*). The default U.S. English message table will be used. This message follows the AUI006E message.

System action

Processing continues while using the U.S. English message table.

User response

Determine and correct the cause of the message table load failure.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ006E LOAD FAILED FOR MESSAGE TABLE *table_name* RSN: *reason_code*

Explanation

A z/OS® LOAD attempt failed for the message table (*table_name*) indicated.

System action

If the table name is the U.S. English message table, (AUIMGENU) processing will terminate. Other table names will cause the product to attempt to use the U.S. English message table after issuing the AUIJ005W message continue processing.

User response

Determine and correct the cause of the message table load failure.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ007E PROGRAM *program_name* IS NOT EXECUTING APF-AUTHORIZED

Explanation

The program specified requires APF-Authorization to perform its function.

System action

The program terminates.

User response

Ensure that all data sets included within the STEPLIB DD concatenation of the JCL where this message appeared are APF authorized.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ008I ATTEMPTING TO CONNECT TO THE GUARDIUM S-TAP® APPLIANCE. TCP/IP Address: *ip_address*, PORT: *port_number*, PING RATE: *ping_rate*

Explanation

An attempt is being made to establish a connection with the Guardium® S-TAP appliance using the named TCP/IP address (*ip_address*) and PORT number (*port_number*).

PING RATE (*ping_rate*) indicates how often a message is sent to the appliance to provide the appliance with confirmation that the connection is active. The PINGS are sent at the rate indicated (*ping_rate*) which is shown in hour, minutes, and second (*hh:mm:ss*) format.

System action

The connection to the Guardium S-TAP appliance is attempted.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ009E LOAD FAILED FOR MODULE *module_name*. R1: *abend_code* R15: *reason_code*

Explanation

An attempt to perform a z/OS® LOAD of the named module (module_name) has failed

System action

The function terminates.

User response

Ensure that all required product data sets are included in the STEPLIB DD concatenation of the JCL where this message appeared. The value in R1 (*abend-code*) indicates the ABEND code that would have occurred if the failure had not been trapped by the product. The value in R15 (*reason_code*) indicates the reason code associated with the abend. Documentation regarding the abend codes and possible resolutions can be found in the *IBM® z/OS MVS™ System Code* manual or equivalent.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ010I IMS STAP *ver* HAS STARTED.

Explanation

The Security Guardium® S-TAP® for IMS agent component, using the specified base code level, has started.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ011I *function_type* CALL TO GUARDUIM S-TAP APPLIANCE SUCCESSFUL

Explanation

The function request (*function_type*) to the Guardium® S-TAP® appliance completed successfully. This message usually follows the AUIJ008I message indicating that the connection request has been initiated.

Function request values which can be displayed are:

INIT-DLIB
: Connection request from the tasks which transmits DLI/DBB batch events.

INIT-DLIO
: Connection request from the task which transmits IMS Online DLI events.

INIT_LOG
: Connection request from the task which transmits IMS Archive log events.

INIT-SMF
: Connection request from the task which transmits SMF events.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ012I NUMBER OF *event_type* EVENTS SENT TO APPLIANCE: *counter*

Explanation

By default, this message is issued every 100,000 events sent to the appliance or approximately every 18 minutes. You can modify this frequency by using the agent parameter keyword DLIFREQ. This message provides a status of data being collected and sent to the Guardium® S-TAP® appliance. The count provided (*counter*) is the number of events since the last message was issued. The type of events (*event_type*) can include DLIB (events captured from IMS DLI/DBB batch jobs), DLIO (events captured from IMS Online regions) SMF (events captured from SMF auditing), IMSL (events captured from IMS archive log processing), and MLOG (missing IMS logs found during IMS Archive log processing).

System action

Processing continues.

User response

None action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ013E *stap_call* TO GUARDUIM S-TAP® APPLIANCE FAILED *(call source)* IP ADDRESS: *ip_address* STAP_RC = *rc1* STAP_RS = *rs1* GDM_RC = *rc2* PB_RC = *rc3* GDML_RC = *rc4* GDML_RS = *rs2*

Explanation

The requested call *(call_type)* to the Guardium® S-TAP appliance has failed. A non-zero value GDM_RC field indicates an error.

System action

The process terminates.

User response

Determine the cause of the failure by checking the return and reason code.

- If GDM_RC is not zero, one or more of the PB_RC, GDML_RC and GDML_RS will be set.
- If STAP_RC and STAP_RS are zero but GCM_RC or PB_RC is not zero, an internal error is indicated. Contact IBM® Software Support.
- If STAP_RC and STAP_RS are not zero, contact IBM Software Support.

Parent topic: Error messages and codes: AUIJxxxx

AUIJ014E OPEN FAILED FOR DD *dd_name*

Explanation

A z/OS® OPEN of the data set(s) referenced by the DD named (*dd_name*) failed.

System action

Processing terminates.

User response

Examine the JES log for z/OS issued IEA messages issued regarding this DD statement and take appropriate action.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ015E THIS IMS RELEASE IS NOT SUPPORTED. IMS NAME: *ims-name*, VRL: *ims_version*

Explanation

The IMS named (*ims-name*) was found to be of a release which is not supported by this version of the product.

System action

Processing terminates.

User response

Review the software requirements documented in this user's guide for a list of IMS releases that are supported by this version of the product.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ016E UNABLE TO INITIALIZE APPLIANCE INTERFACE *(connection_type)*

Explanation

An attempt to establish a connection with the appliance has failed.

System action

Processing terminates.

User response

This error is usually due to the TCP/IP address specified in the <appliance-server> parameter of the AUICONFG or other member used in the AUICONFG DD statement used to provide the agent with configuration information being incorrect. This error can also occur if the target of the TCP/IP address is unresponsive.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ017I PRIMARY STAP CONNECTION RESTORED *(connection_type)* - SUCCESSFULLY CONNECTED TO IP ADDRESS: *ip_address* - PORT : *port*

Explanation

Multiple appliances are defined to IBM® Guardium® S-TAP® for IMS, and the primary appliance (ip_address + port) was unavailable for some period of time. This message indicates that the primary appliance has become available and is now being used.

System action

Processing continues sending data to the primary appliance.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ018W PREVIOUS STAP CONNECTION FAILED *(connection_type)* - SUCCESSFULLY CONNECTED TO IP ADDRESS: *ip_address* - PORT : *port*

Explanation

Multiple appliances are defined to the IMS STAP the connection to the active appliance has failed. This message indicates that another secondary appliance (ip_address + port) is now active.

System action

Processing continues sending data to the secondary appliance.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ019E STAP CONNECTION FAILED: NO CONNECTIONS AVAILABLE *(connection_type)* - IP ADDRESS: *ip-address* - PORT : *port*

Explanation

The connection to the active appliance (ip_address + port) has failed and there are no secondary appliances available for use.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ020I All EVENTS HAVE BEEN WRITTEN FROM SPILL AREA TO APPLIANCE *(connection_type)*

Explanation

All audited events that were buffered to the spill area have been sent to the appliance.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ021W EVENTS ARE BEING WRITTEN TO THE SPILL AREA *(connection_type)*

Explanation

A connection to the appliance has been interrupted, and the spill area is being used to buffer audited events until the appliance connection can be reestablished

System action

Processing continues. Audited events are buffered in the spill area.

User response

Investigate the cause of the appliance connection interruption and correct.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ022W SPILL AREA IS FULL: EVENT DATA IS BEING LOST *(connection_type)*

Explanation

A connection to the appliance was interrupted. The spill area was being used to buffer audited events until the appliance connection can be reestablished. The number of audited events that were generated exceeded the number that could be held in the spill area.

System action

Processing continues. Audited events are discarded.

User response

Investigate the cause of the appliance connection interruption and correct. Look for message AUIJ024W, which is issued at task termination or when a connection is reestablished, for the number of lost events.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ023E SPILL AREA IS NOT AVAILABLE *(connection_type)*

Explanation

An attempt to use the spill area to buffer audited events is unsuccessful.

System action

Processing continues. Audited events are discarded.

User response

Specify a value of 1 through 1024 in the SAUISAMP AUICONFG member <SPILL-SIZE> parameter. Review any z/OS error or warning messages that might indicate why the spill area allocation failed.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ024W NUMBER OF *type* EVENTS LOST *count*

Explanation

Attempts to buffer audited events in the spill area have failed. This message indicates the type of audited events (DLIO, DLIB, SMF etc) which were lost (*type*), and the number that were lost (*count*).

System action

Processing continues. Audited events are discarded.

User response

Investigate the cause of the appliance connection interruption and correct.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ042W ZIIP PROCESSING NOT AVAILABLE ON THIS LPAR (type)

Explanation

A request to process data, using a zIIP enabled enclave, has failed because the Workload Manager feature is not available.

System action

Processing continues, using GCPU (General Central Processor Unit) services.

User response

Remove the ZIIP_AGENT_DLI(Y) keyword from the configuration file that is in use, or change the parameter from Y to N.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ044W ZIIP PROCESSING REQUEST HAS BEEN REJECTED *(connection_type)*

Explanation

An attempt to create a zIIP enabled enclave has failed.

System action

Processing continues using GCPU services.

User response

Determine the cause of the failure by reviewing previously issued AUIJ0331E messages and take corrective action.

Parent topic: Error messages and codes: AUIJxxxx

AUIJ055I ZIIP PROCESSING REQUESTED FOR *type* PROCESSING

Explanation

The use of a zIIP enabled enclave has been requested by the use of the ZIIP_AGENT_DLI(Y) configuration file keyword.

System action

An attempt is made to create the enclave.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ056I ZIIP PROCESSING ENABLED FOR type PROCESSING, ENCLAVE TOKEN: *value*

Explanation

A zIIP enabled enclave has been requested and successfully created.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ057W ZIIP PROCESSING FOR *type* EVENTS HAS BEEN DISABLED DUE TO ERRORS - PROCESSING WILL CONTINUE USING GCPU

Explanation

zIIP processing was requested, however due to previously reported errors, this mode of processing could not be enabled.

System action

Processing continues using General Central Processing Unit (GCPU) resources only.

User response

Review the processing log looking for error and warning messages that were issued prior to this message to help determine why zIIP processing could not be initiated.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ058W ZIIP PROCESSING FOR *type* EVENTS HAS BEEN DISABLED - TRACING IS ENABLED BY THE USE OF THE AUI$NAP JCL STATEMENT

Explanation

Event tracing has been enabled through the addition of the AUI$NAP DD SYSOUT=* JCL statement in the agent JCL. The use of zIIP processing has been disabled because event tracing cannot coexist with the zIIP environment.

System action

All processing continues with event tracing on. Processing occurs on the General Central Processing Unit (GCPU).

User response

If the addition of the AUI$NAP DD statement was not intentional, remove it from the agent JCL.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ201E VSAM ERROR ENCOUNTERED

Explanation

FUNCTION

vsam_function
RPL/RECORD TYPE
rpl/record_value
R15
return_code
R0
reason_code
CSI-CALL
function_call
SUBRTN
pgm_routine

While accessing the VSAM repository, an internal logic error was encountered.

System action

Processing terminates.

User response

There are no user actions available for this failure. Contact IBM® Software Support with the content of this message.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ202E VSAM ERROR ENCOUNTERED

Explanation

While accessing the VSAM repository, an internal logic error was encountered.

FUNCTION:
vsam_function
R15:
return_code
ACBOFLGS:
acboflag_value
CSI-CALL:
function_call
SUBRTN:
pgm_routine

System action

Processing terminates.

User response

There are no user actions available for this failure. Contact IBM® Software Support with the content of this message.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ203E VSAM ERROR ENCOUNTERED

Explanation

While accessing the VSAM repository, an internal logic error was encountered.

FUNCTION:
vsam_function
RPL/RECORD TYPE
rpl/record_value
FDBWD:
rpl_fdbwd
OPTCD:
rpl_optcd
CSI-CALL:
function_call
SUBRTN:
pgm_routine

System action

Processing terminates.

User response

There are no user actions available for this failure. Contact IBM Software Support with the content of this message.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ250I AUDITING IMS EVENTS. COLLECTION PROFILE NAME: *collection_profile_name* IMS NAME: *ims_name* AGENT NAME: *agent name* EXCLUDED REGIONS: *region_types*

Explanation

The auditing of IMS events proceeds by using the collection profile (*collection_profile_name*) that is associated with the IMS definition (*ims_name*). The agent name indicates which agent is processing the audited data. Various region types might have been excluded from auditing, such as AER, BMP, CICS, DBCTL, IFP, MPP, ODBA, or NONE.

System action

Auditing continues.

User response

No action is required.
Note: To set a z/OS message alert for this message, use single-dash formatting between the message number and message text; for example, AUIJ250I - AUDITING IMS EVENTS.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ251E COMPILED FILTER BUILD FAILED. COLLECTION PROFILE NAME : *collection_profile_name* RC: *return_code* RSN: *reason_code*

Explanation

An attempt at building a compiled filter using the collection profile named (*collection_profile_name*) failed.

System action

Processing terminates, auditing will not be performed.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ252W GUARDIUM QUARANTINE IS IN EFFECT; DBPCB STATUS CODES OF *AI* MAY OCCUR

Explanation

The Guardium appliance has detected a list of users for whom access is to be restricted for a period of time. This list is based on policy rules and criteria that are set by the Guardium administrator who maintains the auditing rules in your environment.

System action

Processing continues. If a user in the list of quarantined user IDs attempts to issue DB/DLI calls, the DLI call fails. A DB PCB status code of AI, or an AIB return/reason code of 110/C, is returned to the application program.

User response

If access to IMS databases terminate with a DB PCB status code of AI, or an AIB return/reason code of 110/C, contact the Guardium administrator who maintains the auditing rules in your environment to obtain the reason for the quarantine.
Note: To set a z/OS message alert for this message, use single-dash formatting between the message number and message text; for example, AUIJ252W - GUARDIUM QUARANTINE IS IN EFFECT
Parent topic: Error messages and codes: AUIJxxxx

AUIJ255I AUII050I MESSAGE RECEIVED FROM: JOBNAME: *ims_job_name*; SSID: *ims_ssid*; JOB NUMBER: *job_number*; LPAR: *lpar_name*

Explanation

This message echoes message AUII050I, which is generated by the S-TAP code, and can appear in the IMS control region and the DLI/DBB batch job output. This message only appears in the agent if the DISPLAY_IMSMSG_DLIx(Y) configuration option is coded in the AUICONFG file.

System action

Processing continues.

User response

No action is required. See the explanation for message AUII050I for details regarding the available output fields.

Parent topic: Error messages and codes: AUIJxxxx

AUIJ256I AUIJ250I MESSAGE RECEIVED FROM: JOBNAME: *ims_job_name*; SSID : *ims_ssid*; JOB NUMBER: *job_number*; LPAR: *lpar_name*

Explanation

This message echoes message AUIJ250I, which is generated by the S-TAP code, and can appear in the IMS control region and the DLI/DBB batch job output. This message only appears in the agent if the DISPLAY_IMSMSG_DLIx(Y) configuration option is coded in the AUICONFG file.

System action

Processing continues.

User response

No action is required. See the explanation for message AUIJ250I for details regarding the available output fields.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ257I AUII120I MESSAGE RECEIVED FROM: JOBNAME: *ims_job_name*; SSID: *ims_ssid*; JOB NUMBER: *job_number*; LPAR: *lpar_name*

Explanation

This message echoes message AUII120I, which is generated by the S-TAP code, and can appear in the IMS control region and the DLI/DBB batch job output. This message only appears in the agent if the DISPLAY_IMSMSG_DLIx(Y) configuration option is coded in the AUICONFG file.

System action

Processing continues.

User response

No action is required. See the explanation for message AUII120I for details regarding the available output fields.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ258I AUII052I MESSAGE RECEIVED FROM: JOBNAME: *ims_job_name*; SSID: *ims_ssid*; JOB NUMBER: *job_number*; LPAR: *lpar_name*

Explanation

This message echoes message AUII052I, which is generated by the S-TAP code, and can appear in the IMS control region and the DLI/DBB batch job output. This message only appears in the agent if the DISPLAY_IMSMSG_DLIx(Y) configuration option is coded in the AUICONFG file.

System action

Processing continues.

User response

No action is required. See the explanation for message AUII052I for details regarding the available output fields.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ259I JOBNAME *job_name* USING IMS STAP V10.1.3 MODULE: *pgm_name* APAR: *fix_number* DATE: *fix_date*

Explanation

This message echoes message AUII052I, which is generated by the S-TAP code, and can appear in the IMS control region. This message appears in the agent if the DISPLAY_IMSMSG_DLIx(Y) configuration option is coded in the AUICONFG file.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ303W *request_type* REQUEST FOR LOG STREAM *log_stream_name* FAILED - RC: *return_code* RS: *reason_code* - WILL CONTINUE TO RETRY

Explanation

A request (*request_type*) made to the indicated log stream (*log_stream_name*) has failed. This is a recoverable situation and the request will be retried.

System action

Processing will continue with the request being retried.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ304A IXGCONN REQUEST FOR LOG_STREAM *log_stream_name* FAILED with RC = *return_code* and RS= *reason_code*

Explanation

An attempt to connect to the z/OS System Logger log-stream, by using the IXGCONN function, has failed.

System action

Auditing is disabled, but IMS continues processing.

User response

Correct the issue that has caused the IXGCONN failure; then, uninstall and reinstall the policy to cause IMS to reattempt the connection. Or, correct the issue; then, stop and restart the Security Guardium® S-TAP® for IMS agent to cause IMS to reattempt the IXGCONN call.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ304E IXGWRITE REQUEST FOR *<log-stream-name>* FAILED - RC: *return_code* RS: *reason_code*

Explanation

An attempt to write to the z/OS® System Logger log-stream using the IXGWRITE function has failed.

System action

One occurrence of this message is issued once per error type (RC + RSN) within the each issuance of message AUII050I. IXGWRITE calls continues until the collection policy for the IMS system is uninstalled, or the DLI/DBB batch job or IMS control region terminates.

User response

Examine the description of the IXGWRITE error using the RC and RSN codes provided in the IBM® z/OS MVS™ Programming: Assembler Services Reference, Vol. 2 (IAR-XCT) or equivalent, under the IXGWRITE Macro description, and take corrective action. The most common reason for the appearance of this message is the volume and the rate (number of events per second) of DLI events exceeds the capacity of the current z/OS System Logger log stream definition.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ307A AUDITED EVENTS ARE BEING LOST DUE TO IXGWRITE ERRORS AND/OR BUFFER SHORTAGES

Explanation

A number of attempts to write audited events to the z/OS® System Logger Log-stream have failed which has caused has resulted in available space in the data buffers being exhausted. This has resulted in DLI events which are to be audited to be discarded.

System action

DLI events continue to be audited at attempts to write exiting data buffers to the z/OS System Logger Log-stream until. The number of DLI events which were rejected are noted in subsequent AUII050I message.

User response

Review any AUIJ304E messages which have been issued to determine the cause of the z/OS System Logger Log-stream Write failures.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ307E *thread_type* THREAD IS TERMINATING DUE TO PROCESSING ERRORS.

Explanation

The agent has determined that a fatal error or abend occurred in the thread type indicated.

System action

Processing that is associated with this thread will not occur.

User response

Examine previously issued error or abend messages to determine the corrective action to be taken. Then, restart the agent.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ330E REQUIRED DATA SET IS NOT CATALOGED. - TYPE: *dsn_type*, DSN: *data_set_name*

Explanation

The data set name indicated (data_set_name) was not found in the z/OS® catalog.

System action

Processing terminates

User response

Specify the name of a cataloged data set.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ331E *service_name* SERVICE FAILED - RC: *return_code* - RSN: *reason_code*

Explanation

A z/OS® service (*service_name*) failed when executed.

System action

Processing terminates.

User response

Determine the cause of the failure by using the return and reason codes provided. Contact IBM® Software Support for additional assistance.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ332E DATA SET IS NOT VALID WITHIN CONTEXT USED - TYPE: *data_set_type,* DSN: *data_set_name*, REASON: *reason*

Explanation

The data set indicated (*data_set_name*) is not of a type valid for use where it is defined. The reason for the rejection of this data set is found in the REASON field (*reason*).

System action

Processing terminates

User response

Specify a data set of the correct type.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ333E Service *SERVICE FAILED* for *DATA SET*: *dsn - R15: return_code*

Explanation

A z/OS LOCATE or OBTAIN service failed when it was run against the specified data set dsn.

System action

Processing terminates.

User response

Ensure that the data set names exists, and has not been migrated. Determine the cause of the failure by examining the LOCATE/OBTAIN MACRO return codes found in the *IBM DFSMSdfp Advanced Services* manual. Contact IBM Software Support for additional assistance
Parent topic: Error messages and codes: AUIJxxxx

AUIJ335W *dd_name* DD IS PRESENT IN THIS JCL, *dsn_types* WILL NOT BE AUDITED

Explanation

The AUIF*stc* task has encountered a DD in the JCL that prevents a specific type of data set from being audited by SMF.

System action

Accesses to the data set types that are specified in the text of this message are not audited.

User response

If you want to audit accesses to these types of data sets, remove the DD statement. See the Data sets and DD DUMMY statements table in the SMF records section of this user's guide for information on which DDs affect which data set types.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ400E INSUFFICIENT MEMORY - MODULE NAME: *program_name* - MEMORY SEGMENT TYPE: *seg_type*

Explanation

An attempt at obtaining memory in program (*module_name*) has failed due to insufficient memory being available.

System action

Processing terminates

User response

Increase the region size of the started task where this message appeared. Restart the started task and retry the request.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ401E MODULE *module_name* FAILED DURING ATTACH of *program_name* - RETURN CODE: *return_code*

Explanation

An attempt to perform a z/OS® ATTACH of the program_name by module module_name has failed.

System action

Processing terminates.

User response

Determine the cause of the failure by using the return code (*return_code*) provided. Correct and restart the task that issued the message. Contact IBM® Software Support for further assistance if need.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ402E CATALOG SERVICE REQUEST FAILED - MODULE NAME: *module_name* - RC: *return_code* RSN: *reason_code*

Explanation

An attempt use the catalog interface has failed.

System action

Processing terminates

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ403E DYNAMIC ALLOCATION FAILURE - FUNCTION : *function_code* - DSN: *data-set-name* - RC: *return_code* RSN: *reason_code*

Explanation

An attempt to issue a dynamic allocation function (*function_code*) using the data set name indicated (*data_set_name*) has failed.

System action

Processing terminates.

User response

Using the *return_code* and *reason_code* determine the cause for the failure. Correct and retry the request.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ404E DYNAMIC ALLOCATION FAILURE - FUNCTION: *function_code* -DDN: *dd_name* - RC: *return_code* RSN: *reason_code*

Explanation

An attempt to issue a dynamic allocation function (*function_code*) using the DD name indicated (*dd_name*) has failed.

System action

Processing terminates.

User response

Using the *return_code* and *reason_code* determine the cause for the failure. Correct and retry the request.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ406W TOO MANY RULES SPECIFIED IN POLICY, REQUEST HAS BEEN TRUNCATED. POLICY: *policy_name*. RULE LIMIT: *max_number_of rules_allowed*

Explanation

Preprocessing of the rules associated with the indicated policy (*policy_name*) determined that the number of rules that were specified in the policy exceeded the rule limit of *max_number_of rules_allowed*. Allowing an excessive number of rules causes memory constraint and performance issues.

System action

The contents of subsequent rules are discarded. Processing continues using all previous rule content.

User response

Review the rules that are included in the policy, and edit the policy to combine the rule content where permissible. If the resulting policy still requires a greater number of rules than the rule limit permits, contact IBM Software Support.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ407I *number* DATA SETS ADDED TO POLICY *policy_name* FILTER

Explanation

This message provides the number of data set names that are used as input when building the compiled filter for SMF processing.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ408E POLICY *name* RESULTED IN OVER 102400 DATA SETS TO BE AUDITED; DATA SET RESULT SET HAS BEEN TRUNCATED

Explanation

The specified policy has found over 102,400 data sets to audit based on the databases that are specified in the policy rules and the IMS system log data set (SLDS) and recovery log data set (RLDS) RECON entries. Due to memory constraints, the data set occurrence limit per policy is 102,400 per IMS definition.

System action

Remaining data set names for the database description (DBD) that is being processed are included in the list to be audited, which might cause the 102,400 data set limit to be slightly exceeded. The process that determines the DBD and DSN pairings ends, no additional rules within the policy are processed, and a filter is created for the policy based on the 102,400 (or more) data set names. Normal processing continues.

User response

- Change the policy rules to audit fewer databases, or modify the rules to reduce or avoid multiple rules from auditing the same databases.
- Review the IMS RECON data set that is looking for IMS SLDS and RLDS, database image copy data sets, or database data set group (DSG)/area data sets, which no longer physically exist but remain listed in the RECON. Delete the RECON references that are no longer needed.

Parent topic: Error messages and codes: AUIJxxxx

AUIJ500I STARTING *cycle_type* CYCLE

Explanation

The task is starting the processing cycle specified.

System action

Processing starts for the cycle specified.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ501I NO NEW CATALOGED SMF DATA SETS FOUND FOR SMF MASK: - *smf_mask_value*

Explanation

The SMF processing cycle has determined that no new, unprocessed data sets which meet the SMF mask value have been found.

System action

The task waits for the start of the next cycle.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ504I *cycle_type* CYCLE COMPLETE

Explanation

The cycle has completed.

System action

The task waits for the start of the next cycle.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ521W CONTROL BLOCK AUIDCCOM NOT FOUND

Explanation

A critical E/CSA control block was not found.

System action

Processing terminates.

User response

Contact Software Support.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ510I ALTERNATE RECON DATA SETS FOUND FOR IMSNAME *imsname*: RECON1: *alt_dsn_1*; RECON2: *alt_dsn_2*, RECON3: *alt_dsn_3*

Explanation

The AUIARCN DD was found in the JCL. The *imsname* that was used when installing the active IMS policy was found in the AUIARCN file, along with alternate RECON data sets names (*alt_dsn_1/2/3*).

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ511E ALTERNATE RECON DATA SET NOT CATALOGED; DSN: *alt_dsn*

Explanation

When attempting to validate the *alt_dsn* value, the data set was not found in the catalog.

System action

Processing continues to validate other specified data set names.

User response

Correct the data set name or catalog the data set.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ512E ALTERNATE RECON DATA SET NOT A VSAM FILE; DSN: *alt_dsn*

Explanation

When attempting to validate the *alt_dsn* value, the data set was found to in a format invalid for processing. The data set name must be in VSAM format.

System action

Processing continues to validate other specified data set names.

User response

Correct the data set name or catalog the data set.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ513E NO VALID ALTERNATE RECON DATA SETS FOUND FOR IMS *imsname*; PROCESSING TERMINATED

Explanation

The data set validation was completed, and no valid alternate RECON data set names found for the IMSNAME.

System action

Processing terminates.

User response

Add or correct valid RECON data set names.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ522E INSUFFICIENT E/CSA STORAGE AVAILABLE FOR *control_block* CONTROL BLOCK

Explanation

Insufficient E/CSA storage was available to hold the specified control block.

System action

Processing terminates.

User response

Determine the cause of the E/CSA shortage.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ609I *event_types* ARE BEING EXCLUDED (*excluded_by*)

Explanation

If the *excluded_by* value is AGENT, then the reporting of *event_types* is excluded due to the specification of certain configuration keywords. If the *excluded_by* value is IMS, these events are excluded as directed by the IMS definition.

System action

Occurrences of these event types are not reported.

User response

If you want to view reports of this event type, review and modify the agent configuration file (SMF_AUDIT_LEVELS or IMSL_AUDIT_LEVELS keywords) or the Guardium system IMS definition, using the Auditing Levels tab.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ800E REQUIRED DD STATEMENT IS MISSING: *dd-name*

Explanation

A critical error has occurred due to a missing DD statement.

System action

Processing terminates.

User response

This message occurs if a product JCL has been edited and a DD statement has been deleted or omitted. If this is not the case, check for any dynamic allocation error messages. If none are present, or are not user resolvable, contact IBM® Software Support.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ860E VSAM FILE DEFINITION ERROR - DDN: *dd_name* - REASON: *definition_error*

Explanation

When validating the VSAM repository, an allocation definition error was found.

System action

Processing terminates.

User response

The VSAM repository requires specific values for the attribute, LRECL, key length and key position. Review the SAUISAMP product distribution data set member AUISJ001 for the correct file definition specifications.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ999E AN INTERNAL LOGIC ERROR HAS OCCURRED - MODULE: module_name RSN: reason_code

Explanation

An internal logic error has occurred.

System action

Processing terminates

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIJxxxx

Error messages and codes: AUILxxxx

The following information is about error messages and codes that begin with AUIL.

- **AUIL002I**
  Archive log reader interval set to *<number> <time interval in hours/minutes>*.
- **AUIL003E**
  Command *<command-text>*failed; interval value must be between *<lower-bound>* and *<upper-bound>*.
- **AUIL600I**
  NO NEW CATALOGED IMS LOG DATA SETS FOUND
- **AUIL601I**
  PROCESSING IMS LOG DATA SET: *ims_log_data_set_name*
- **AUIL602I**
  PROCESSING COMPLETE FOR IMS LOG DATA SET: *ims_log_data_set_name*
- **AUIL603I**
  SCANNING RECON DATA SETS FOR IMS LOGS TO PROCESS. RECON1: *recon1_dsn* - RECON2: *recon2_dsn* - RECON3: *recon3_dsn*
- **AUIL605I**
  RECON DATA SET SCAN COMPLETE
- **AUIL606W**
  RECON HAS NOCATDS SPECIFIED, RESULTS MAY NOT BE ACCURATE
- **AUIL607W**
  THERE ARE NO ACTIVE IMS POLICIES FOR AGENT *agent_name*
- **AUIL701I**
  IMS LOG CHECKPOINT INFORMATION - IMSID: *IMS_name_from_policy* - RECON1 DSN: *dsn_of_RECON1* - CREATING SSID: *SSID_from_PRILOG* - LAST DSN READ: *dsn_of_SLDS* - LAST UPDATED (UTC): *date_time*

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIL002I Archive log reader interval set to *<number> <time interval in hours/minutes>*.

Explanation

The Archive log reader is scheduled to process archive logs as specified.

User response

No action is required.
Parent topic: Error messages and codes: AUILxxxx

AUIL003E Command *<command-text>*failed; interval value must be between *<lower-bound>* and *<upper-bound>*.

Explanation

This message indicates that *<command>*, such as: /f AUILSTC,SET INTERVAL number failed because of incorrect *number* value. Correct values must be between *<lower-bound>* and *<upper-bound>*.

User response

Use an interval value between *<lower-bound>* and *<upper-bound>*. If that does not resolve the issue, contact IBM® Software Support.
Parent topic: Error messages and codes: AUILxxxx

AUIL600I NO NEW CATALOGED IMS LOG DATA SETS FOUND

Explanation

After examining the RECON data sets, it has been determined that no new IMS SLDS data sets were found that have yet to be processed by the product.

User response

No action is required.
Parent topic: Error messages and codes: AUILxxxx

AUIL601I PROCESSING IMS LOG DATA SET: *ims_log_data_set_name*

Explanation

Processing has started for the IMS SLDS data set indicated (*ims_log_data_set_name*)

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUILxxxx

AUIL602I PROCESSING COMPLETE FOR IMS LOG DATA SET: *ims_log_data_set_name*

Explanation

Processing of the IMS SLDS data set has completed.

System action

Processing continues with other candidate IMS SLDS data sets.

User response

No action is required.
Parent topic: Error messages and codes: AUILxxxx

AUIL603I SCANNING RECON DATA SETS FOR IMS LOGS TO PROCESS. RECON1: *recon1_dsn* - RECON2: *recon2_dsn* - RECON3: *recon3_dsn*

Explanation

To determine the candidate IMS SLDS data sets to be read, the IMS RECON data sets must be queried. This message indicates that this query process has started.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUILxxxx

AUIL605I RECON DATA SET SCAN COMPLETE

Explanation

This message follows the AUIL603I message and indicates that the scan of the RECON data sets is complete.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUILxxxx

AUIL606W RECON HAS NOCATDS SPECIFIED, RESULTS MAY NOT BE ACCURATE

Explanation

When examining the RECON data sets the NOCATDS option was found to be on, meaning any log data sets found might not be cataloged.

System action

Processing continues.

User response

The function that produces this message relies on the log data sets existing in the z/OS® catalog or having been in the z/OS catalog at one time. Having the NOCATDS option on in the RECON data sets might negate the validity of further processing, if the SLDS data sets are not cataloged.
Parent topic: Error messages and codes: AUILxxxx

AUIL607W THERE ARE NO ACTIVE IMS POLICIES FOR AGENT *agent_name*

Explanation

A request to query the RECON data sets of IMS systems defined under the named agent found that there were no IMS systems audited by the agent with an active profile. The function that produces this message relies on having at least one IMS system with an active collection policy.

System action

Processing terminates.

User response

Install a collection policy for an IMS under of the control the agent.
Parent topic: Error messages and codes: AUILxxxx

AUIL701I IMS LOG CHECKPOINT INFORMATION - IMSID: *IMS_name_from_policy* - RECON1 DSN: *dsn_of_RECON1* - CREATING SSID: *SSID_from_PRILOG* - LAST DSN READ: *dsn_of_SLDS* - LAST UPDATED (UTC): *date_time*

Explanation

This message provides the name of the IMS SLDS that was last read when processing data for the SSID (*SSID_from_PRILOG*) found in the set of the DBRC RECON data sets (*dsn_of_RECON1*). This information is used as a checkpoint to indicate which SLDS data sets have already been processed, and should not be re-read by the AUILstc tasks.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUILxxxx

Error messages and codes: AUIPxxxx

The following information is about error messages and codes that begin with AUIP.

- **AUIP001E**
  A protobuf message schema violation was detected; value *value* is not a valid boolean value.
- **AUIP002E**
  A protobuf message schema violation was detected; value *value* is not a valid double value.
- **AUIP003E**
  A protobuf message schema violation was detected; value *value* is not a valid integer value.
- **AUIP004E**
  A protobuf message schema violation was detected; required message *message* property *property* is not present.
- **AUIP005E**
  A protobuf message schema violation was detected; required message *message* sub-message *submessage* is not present.
- **AUIP006S**
  A severe error occurred during protobuf message parsing; an unknown exception occurred.
- **AUIP007E**
  A protobuf message schema violation was detected; property name *property* is invalid.
- **AUIP008E**
  A protobuf message schema violation was detected; property *property* value *value* is invalid.
- **AUIP009E**
  A protobuf message schema violation was detected; message name 'name' is invalid.
- **AUIP010E**
  A protobuf message schema violation was detected; message name *name* is invalid (expected *expected name*).
- **AUIP011E**
  A protobuf message schema violation was detected; value *value* is not a valid bytes value.
- **AUIP012E**
  A protobuf message schema violation was detected; value *value* is not a valid unsigned integer value.
- **AUIP013E**
  An error occurred while parsing item text: String is empty.
- **AUIP014E**
  An error occurred while parsing item text: text.
- **AUIP015E**
  Failed to send error message to appliance: *host/port*.
- **AUIP016E**
  Policy rule <rule> was ignored: IMS name is empty.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIP001E A protobuf message schema violation was detected; value *value* is not a valid boolean value.

Explanation

The specified value is not valid.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP002E A protobuf message schema violation was detected; value *value* is not a valid double value.

Explanation

The specified value is not valid.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP003E A protobuf message schema violation was detected; value *value* is not a valid integer value.

Explanation

The specified value is not valid.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP004E A protobuf message schema violation was detected; required message *message* property *property* is not present.

Explanation

The specified message property is not present.

User response

Contact your administrator or IBM® Software Support
Parent topic: Error messages and codes: AUIPxxxx

AUIP005E A protobuf message schema violation was detected; required message *message* sub-message *submessage* is not present.

Explanation

The specified message submessage is not present.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP006S A severe error occurred during protobuf message parsing; an unknown exception occurred.

Explanation

An error occurred while parsing a protobuf message.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP007E A protobuf message schema violation was detected; property name *property* is invalid.

Explanation

The specified property name is not valid.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP008E A protobuf message schema violation was detected; property *property* value *value* is invalid.

Explanation

The specified property value is not valid.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP009E A protobuf message schema violation was detected; message name 'name' is invalid.

Explanation

The specified message name is not valid.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP010E A protobuf message schema violation was detected; message name *name* is invalid (expected *expected name*).

Explanation

The specified message name is not valued.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP011E A protobuf message schema violation was detected; value *value* is not a valid bytes value.

Explanation

The specified value is not valid.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP012E A protobuf message schema violation was detected; value *value* is not a valid unsigned integer value.

Explanation

The specified value is not valid.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP013E An error occurred while parsing item text: String is empty.

Explanation

A policy message contained an item field with an empty value.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP014E An error occurred while parsing item text: text.

Explanation

A policy message contained an item field with a value *text* could not be parsed successfully.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP015E Failed to send error message to appliance: *host/port*.

Explanation

The IBM® Guardium® S-TAP® for IMS agent was unable to send the error message to the specified appliance.

User response

Contact your administrator or IBM Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP016E Policy rule <rule> was ignored: IMS name is empty.

Explanation

The specified policy rule was ignored because it does not apply to any IMS subsystem, or the IMS name is empty.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

Error messages and codes: AUIRxxxx

The following information is about error messages and codes that begin with AUIR.

- **AUIR002E**
  The provided *parameter 'value'* is too long; should be less than or equal to *maximum length* characters.
- **AUIR004E**
  A maximum of *maximum* data sets are allowed for the *names* libs and a total of *libs-count* were specified.
- **AUIR006E**
  The parameter *parameter* can't be empty.
- **AUIR007W**
  Policy_rule_item *<item-name>* for Policy_rule *<rule-name>* has conflicting *<value-name>* values.
- **AUIR008W**
  IMS 050i Max Time threshold was changed from "2460" to "2359".

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIR002E The provided *parameter 'value'* is too long; should be less than or equal to *maximum length* characters.

Explanation

The value of the specified *parameter* exceeds the maximum length *maximum length*.

User response

Specify a shorter value that does not exceed the specified limit for the parameter.
Parent topic: Error messages and codes: AUIRxxxx

AUIR004E A maximum of *maximum* data sets are allowed for the *names* libs and a total of *libs-count* were specified.

Explanation

The maximum number of data sets was exceeded for the libs specified.

User response

Limit the number of data sets for the specified libs to *maximum*.
Parent topic: Error messages and codes: AUIRxxxx

AUIR006E The parameter *parameter* can't be empty.

Explanation

The parameter value must be specified in the agent configuration.

User response

Update agent configuration, or contact your administrator.
Parent topic: Error messages and codes: AUIRxxxx

AUIR007W Policy_rule_item *<item-name>* for Policy_rule *<rule-name>* has conflicting *<value-name>* values.

Explanation

The Guardium policy was processed but there are conflicting fields in the definition. Only one of the policies has been applied.

User response

Check the policy definition, and change the specified values to eliminate the conflict.
Parent topic: Error messages and codes: AUIRxxxx

AUIR008W IMS 050i Max Time threshold was changed from "2460" to "2359".

Explanation

An invalid time value was supplied through the use of the Message AUII050I Frequency field of the IMS definition screen of the Guardium® appliance. The invalid value was automatically corrected by the agent.

System action

Processing continues.

User response

When convenient, update the invalid time value in the IMS definition to a value within the range of 00:10 -- 23:59.
Parent topic: Error messages and codes: AUIRxxxx

Error messages and codes: AUITxxxx

The following information is about error messages and codes that begin with AUIT.

- **AUIT001E**
  The specified user ID *userid* is not defined or does not have an OMVS segment defined.
- **AUIT006S**
  The product is not properly configured to authenticate users.
- **AUIT008E**
  The configuration file *filename* is invalid; the root element *element* is not <agent-config>.
- **AUIT010E**
  An error occurred while opening the configuration file *filename message text*
- **AUIT012I**
  Performing discovery of available locations.
- **AUIT013I**
  Security Guardium® S-TAP® for IMS agent is terminating.
- **AUIT014I**
  Connected to server *<host>* on port *<port>*.
- **AUIT015I**
  Attempting connection to server *<host>* on port *<port>*.
- **AUIT017I**
  Discovered subsystem *subsystem-id*.
- **AUIT019I**
  Security Guardium S-TAP for IMS agent started on *<lpar _name> (<lpar_ip>)*.
- **AUIT020I**
  Starting the socket selector thread (thread *thread id*).
- **AUIT023I**
  Received shutdown request.
- **AUIT025I**
  The socket selector thread is terminating.
- **AUIT028E**
  An error occurred while authenticating user *user-id error-text*.
- **AUIT031I**
  Starting the command listener thread (thread *thread-id*).
- **AUIT032I**
  Received stop command: *command-text*.
- **AUIT033I**
  Received modify command: *command-text*.
- **AUIT034S**
  Security Guardium S-TAP for IMS agent is terminating due to hard stop request.
- **AUIT044E**
  The connection to the server has been lost.
- **AUIT047E**
  IBM® Security Guardium S-TAP for IMS on z/OS® agent ended with RC = *[rc]*.
- **AUIT048I**
  Issuing request to capture service dump.
- **AUIT049I**
  Request to capture service dump has completed successfully.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIT001E The specified user ID *userid* is not defined or does not have an OMVS segment defined.

Explanation

You specified a user ID that is not defined or does not have an OMVS segment defined.

User response

Security Guardium® S-TAP® for IMS was unable to authenticate the specified user. Either specify a valid user ID, or if the user ID is valid, see your security administrator to have an OMVS segment defined for the user ID.

Parent topic: Error messages and codes: AUITxxxx

AUIT006S The product is not properly configured to authenticate users.

Explanation

Security Guardium® S-TAP® for IMS is not properly configured to authenticate users.

User response

An error occurred while authenticating a remote user request. The error code indicates that the installation configuration required to allow this authentication has not been completed. See IBM Guardium S-TAP for IMS agent for more information about how to complete the required configuration.
Parent topic: Error messages and codes: AUITxxxx

AUIT008E The configuration file *filename* is invalid; the root element *element* is not <agent-config>.

Explanation

The configuration file identified in the message is invalid.

User response

The contents of the specified configuration file are invalid. Correct the file contents to specify <agent-config> as the root XML element.

Parent topic: Error messages and codes: AUITxxxx

AUIT010E An error occurred while opening the configuration file *filename message text*

Explanation

An error occurred while opening the configuration file identified in the message. Additional error information is also contained within the message.

User response

Use the specified message text to diagnose the error that occurred. Specify a valid configuration file that is not in use by any other process.

Parent topic: Error messages and codes: AUITxxxx

AUIT012I Performing discovery of available locations.

Explanation

The Security Guardium® S-TAP® for IMS agent is looking for available locations.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT013I Security Guardium® S-TAP® for IMS agent is terminating.

Explanation

The Security Guardium S-TAP for IMS agent is terminating.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT014I Connected to server *<host>* on port *<port>*.

Explanation

The Security Guardium® S-TAP® for IMS agent task has connected to the S-TAP to the specified host and port.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT015I Attempting connection to server *<host>* on port *<port>*.

Explanation

The Security Guardium® S-TAP® for IMS agent is attempting to connect to the specified host and port number.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT017I Discovered subsystem *subsystem-id*.

Explanation

The Security Guardium® S-TAP® for IMS agent has discovered the identified subsystem.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT019I Security Guardium® S-TAP® for IMS agent started on *<lpar _name> (<lpar_ip>)*.

Explanation

The IBM® Guardium S-TAP for IMS agent has started.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT020I Starting the socket selector thread (thread *thread id*).

Explanation

The Security Guardium® S-TAP® for IMS agent is starting the identified socket selector thread.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT023I Received shutdown request.

Explanation

The Security Guardium® S-TAP® for IMS agent has received a shutdown request.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT025I The socket selector thread is terminating.

Explanation

The Security Guardium® S-TAP® for IMS agent socket selector thread is terminating.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT028E An error occurred while authenticating user *user-id error-text*.

Explanation

An unexpected return code was returned by the *pthread_security_np()* callable service.

User response

Ensure that the configuration required to use this service has been completed. See IBM Guardium S-TAP for IMS agent for more information about the required configuration. Check the agent job log for additional messages which might be generated.

Parent topic: Error messages and codes: AUITxxxx

AUIT031I Starting the command listener thread (thread *thread-id*).

Explanation

The Security Guardium® S-TAP® for IMS agent is starting the command listener thread.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT032I Received stop command: *command-text*.

Explanation

The Security Guardium® S-TAP® for IMS agent received a STOP command.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT033I Received modify command: *command-text*.

Explanation

The Security Guardium® S-TAP® for IMS agent received a MODIFY command.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT034S Security Guardium® S-TAP® for IMS agent is terminating due to hard stop request.

Explanation

Security Guardium S-TAP for IMS agent is terminating due to a user /MODIFY FORCE command.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT044E The connection to the server has been lost.

Explanation

The Security Guardium® S-TAP® for IMS agent task is unable to communicate with the Security Guardium S-TAP for IMS agent.

User response

Resolve any network connectivity issues, then try logging in again.
Parent topic: Error messages and codes: AUITxxxx

AUIT047E IBM® Security Guardium® S-TAP® for IMS on z/OS® agent ended with RC = *[rc]*.

Explanation

Due to a prior error, the agent has ended with the specified return code.

User response

Contact IBM Software Support.
Parent topic: Error messages and codes: AUITxxxx

AUIT048I Issuing request to capture service dump.

Explanation

A command, such as /f AUIASTC,DUMP/DDX, has been issued for processing.

User response

No action is required.
Parent topic: Error messages and codes: AUITxxxx

AUIT049I Request to capture service dump has completed successfully.

Explanation

A command, such as /f AUIASTC,DUMP/DDX has processed successfully.

User response

No action is required.
Parent topic: Error messages and codes: AUITxxxx

Error messages and codes: AUIUxxxx

The following information is about error messages and codes that begin with AUIU.

- **AUIUR002I**
  Migrate Utility for IBM® Security Guardium® S-TAP® for IMS on z/OS® started.
- **AUIUR003I**
  Agent record *<agent name>* was not found in the repository.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIUR002I Migrate Utility for IBM® Security Guardium® S-TAP® for IMS on z/OS® started.

Explanation

The utility to migrate the configuration of an older version of the product to the current product version has started.

User response

No action is required.
Parent topic: Error messages and codes: AUIUxxxx

AUIUR003I Agent record *<agent name>* was not found in the repository.

Explanation

An attempt to read an agent record from the repository while migration failed as the record was not found.

System action

The agent record migration fails, processing continues.

User response

Check the configuration file for agent and repository names and use the Guardium user interface to verify that the specified agent definition is presented in specified repository.
Parent topic: Error messages and codes: AUIUxxxx

Error messages and codes: AUIXxxxx

The following information is about error messages and codes that begin with AUIX.

- **AUIX013E**
  A shared memory error occurred on "*service name*": *error message*.
- **AUIX014E**
  An XML schema violation was detected; value *value* is not a valid boolean value.
- **AUIX015E**
  An XML schema violation was detected; value *value* is not a valid double value.
- **AUIX016E**
  An XML schema violation was detected; value *value* is not a valid integer value.
- **AUIX017E**
  An XML syntax error was detected at offset *offset*; expected *expected-value*, found *found-value*.
- **AUIX018E**
  An XML schema violation was detected; required element *element* attribute *attribute*\" is not present.

- **AUIX019E**
  An XML schema violation was detected; required element *<element>* child *<child-element>* is not present.
- **AUIX020E**
  Memory allocation failed (*number* bytes).
- **AUIX021E**
  An XML schema violation was detected; element *element* child *child-number* has wrong type.
- **AUIX022E**
  An XML syntax error was detected; character reference *character-reference* is invalid.
- **AUIX023E**
  An XML syntax error was detected; entity reference *entity-reference* is invalid.
- **AUIX024E**
  An XML syntax error was detected; more than one element was found at the root of the document.
- **AUIX025E**
  An XML syntax error was detected; no element was found at the root of the document.
- **AUIX026E**
  An XML syntax error was detected; text was found at the root of the document.
- **AUIX027S**
  A severe error occurred during XML parsing; an unknown exception occurred.
- **AUIX028E**
  The command line option *<option name>* is invalid.
- **AUIX034S**
  A severe error occurred during command line processing; an unknown exception occurred.
- **AUIX035E**
  The operation completed successfully.
- **AUIX036E**
  The address family is not supported by the protocol family (*socket-return-code*).
- **AUIX037E**
  The operation is still in progress (*socket-return-code*).
- **AUIX038E**
  Permission is denied (*socket-return-code*).
- **AUIX039E**
  The network is down (*socket-return-code*).
- **AUIX040E**
  No buffer space is available (*socket-return-code*).
- **AUIX041E**
  Too many sockets have been opened (*socket-return-code*).
- **AUIX042E**
  The protocol is not supported (*socket-return-code*).
- **AUIX043E**
  The WSAStartup routine was not called (*socket-return-code*).
- **AUIX044E**
  The protocol is the wrong type for the socket (*socket-return-code*).
- **AUIX045E**
  The socket type is not supported (*socket-return-code*).
- **AUIX046E**
  The destination network is unreachable (*socket-return-code*).
- **AUIX047E**
  The socket handle is invalid (*socket-return-code*).
- **AUIX048E**
  The address is already in use (*socket-return-code*).
- **AUIX049E**
  The function call was interrupted (*socket-return-code*
- **AUIX050E**
  The requested address is not available (*socket-return-code*).
- **AUIX051E**
  The connection was aborted (*socket-return-code*).
- **AUIX052E**
  The connection was refused by the partner (*socket-return-code*).
- **AUIX053E**
  The connection was reset by the partner (*socket-return-code*).
- **AUIX054E**
  The network message is too long (*socket-return-code*).
- **AUIX055E**
  The network dropped the connection when reset (*socket-return-code*).
- **AUIX056E**
  An invalid parameter was specified (*socket-return-code*).
- **AUIX057E**
  The socket is not connected (*socket-return-code*).
- **AUIX058E**
  The operation is not supported (*socket-return-code*).
- **AUIX059E**
  The socket has been closed (*socket-return-code*).
- **AUIX060E**
  The socket is already connected (*socket-return-code*).
- **AUIX061S**
  An unknown error occurred (*socket-return-code*).
- **AUIX062E**
  A socket error occurred on *socket-operation* with RC = *return code*: *message-text*.
- **AUIX063E**
  A socket select error occurred: *message-text*.

- **AUIX064E**
  An XML schema violation was detected; expected root element *element-expected*, but found *element-found* instead.
- **AUIX066E**
  An XML schema violation was detected; element *element* value *value* is invalid.
- **AUIX067E**
  An XML schema violation was detected; element name *element* is invalid.
- **AUIX068E**
  An XML schema violation was detected; element name *element-found* is invalid (expected *element-expected*).
- **AUIX074E**
  An abend occurred: *<abend code>*.
- **AUIX076E**
  An XML schema violation was detected; element *element* attribute *attribute* value *value* is invalid.
- **AUIX085E**
  A dynamic allocation error occurred: info code = *info-code*, error code = *error-code*.
- **AUIX086E**
  A dynamic concatenation error occurred: info code = *info-code*, error code = *error-code*.
- **AUIX087E**
  A dynamic free error occurred: info code = *info-code*, error code = *error-code*.
- **AUIX088E**
  An invalid dynamic allocation parameter was specified: code = *parm-code*.
- **AUIX093S**
  An unexpected error occurred (*file-name*, *line-number*).
- **AUIX094S**
  An unexpected error occurred with token *token*, (*file-name*, *line-number*).
- **AUIX095S**
  An unexpected error occurred with tokens *token* and *token* (*file-name*, *line-number*).
- **AUIX096S**
  An unexpected error occurred with tokens *token*, *token* and *token* (*file-name*, *line-number*).
- **AUIX097S**
  An unexpected error occurred with tokens *token*, *token*, *token*, and *token* (*file-name*, *line-number*.
- **AUIX098E**
  A thread error occurred on *thread-operation* : *message-text*.
- **AUIX101E**
  An event error occurred on *event-operation* : *message-text*.
- **AUIX104E**
  A mutex error occurred on *mutex-operation* : *message-text*.
- **AUIX109E**
  A semaphore error occurred on *semaphore-operation* : *message-text*.
- **AUIX110I**
  The network connection has been disconnected.
- **AUIX114E**
  A dynamic allocation query error occurred: info code = *info-code*, error code = *error-code*.
- **AUIX115E**
  An input command error occurred on \"*command-operation*\": *message-text*.
- **AUIX116I**
  Received input command: *command-text*.
- **AUIX122I**
  Build date *component* = *date*.
- **AUIX123W**
  The action was cancelled.
- **AUIX124S**
  The task is not running APF-authorized.
- **AUIX126E**
  A DLL error occurred on *dll-operation* : *message-text*
- **AUIX127S**
  An error occurred while opening log file *file-name*.
- **AUIX142E**
  An XML schema violation was detected; element *element* value *value* is invalid: expected min *<min-value>* and max *<max value>*.
- **AUIX143E**
  An XML schema violation was detected; element *element* attribute *value* value *value* is invalid: expected min *<minimum>* and max *<maximum>*.
- **AUIX149E**
  Data set *[data set]* is not cataloged.
- **AUIX150E**
  Invalid data set *'data set'*: Data set name must not exceed 44 characters.
- **AUIX151E**
  Invalid data set *{'data set'}*: The segment length must be greater than 0 and less than or equal to 8.
- **AUIX152E**
  Invalid data set *'name'*: The first character in each segment must be alphabetic (A-Z) or national (#, @, $).
- **AUIX153E**
  Invalid data set *'<data set>'*: The non-first characters in the segments must be alphabetic (A-Z), numeric, national (#, @, $), or hyphen.
- **AUIX154E**
  Invalid data set *'<data set>'*: The non-first characters in the SMF segments must be alphabetic (A -- Z), numeric, national (#, @, $), hyphen, asterisk (*) or percent (%).
- **AUIX155E**
  Data set *<data set>* is not APF-authorized.
- **AUIX156E**
  Invalid data set *'<data set>'*: The first character in SMF segment must be alphabetic (A -- Z) or national (#, @, $), asterisk (*) or percent (%).
- **AUIX160E**
  A dynamic allocation query error occurred: info code = *<info-code>*, error code = *<error-code>*, DD name = *<dd-name>*.

- **AUIX183E**
  The number of file descriptors (sockets) has exceeded maximum = <*number*>.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIX013E A shared memory error occurred on "*service name*": *error message*.

Explanation

This error can occur in the primary agent address space. When the error occurs, the primary agent address space will shut down with a CC of 12. This startup error indicates that attempts to create a shared memory segment failed because of an already existing shared memory segment that never belonged to, or currently does not belong to, the primary agent address space.

This message can occur in the secondary address space if the <id> elements in the ADS_SHM_ID and ADS_LISTENER_PORT parameters do not match in the AUICONFG configuration member that is used by the agent primary address space and the secondary address spaces.

User response

Edit SAUISAMP member AUICONFG (or the customized AUICONFG) and specify the correct <id> elements in the ADS_SHM_ID and ADS_LISTENER_PORT parameters.
Parent topic: Error messages and codes: AUIXxxxx

AUIX014E An XML schema violation was detected; value *value* is not a valid boolean value.

Explanation

An XML schema violation was detected; value value is not a valid boolean value.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX015E An XML schema violation was detected; value *value* is not a valid double value.

Explanation

An XML schema violation was detected; value *value* is not a valid double value.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX016E An XML schema violation was detected; value *value* is not a valid integer value.

Explanation

An XML schema violation was detected; value value is not a valid integer value.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX017E An XML syntax error was detected at offset *offset*; expected *expected-value*, found *found-value*.

Explanation

An XML syntax error was detected at offset offset; expected expected-value, found found-value.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX018E An XML schema violation was detected; required element *element* attribute *attribute*\" is not present.

Explanation

An XML schema violation was detected; required element element attribute attribute is not present.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX019E An XML schema violation was detected; required element *<element>* child *<child-element>* is not present.

Explanation

The XML schema must contain the specified elements.

User response

Correct the XML schema and retry.
Parent topic: Error messages and codes: AUIXxxxx

AUIX020E Memory allocation failed (*number* bytes).

Explanation

Memory allocation failed (number bytes).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX021E An XML schema violation was detected; element *element* child *child-number* has wrong type.

Explanation

An XML schema violation was detected; element element child child-number has wrong type.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX022E An XML syntax error was detected; character reference *character-reference* is invalid.

Explanation

An XML syntax error was detected; character reference character-reference is invalid.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX023E An XML syntax error was detected; entity reference *entity-reference* is invalid.

Explanation

An XML syntax error was detected; entity reference entity-reference is invalid.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX024E An XML syntax error was detected; more than one element was found at the root of the document.

Explanation

An XML syntax error was detected; more than one element was found at the root of the document.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX025E An XML syntax error was detected; no element was found at the root of the document.

Explanation

An XML syntax error was detected; no element was found at the root of the document.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX026E An XML syntax error was detected; text was found at the root of the document.

Explanation

An XML syntax error was detected; text was found at the root of the document.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX027S A severe error occurred during XML parsing; an unknown exception occurred.

Explanation

A severe error occurred during XML parsing; an unknown exception occurred.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX028E The command line option *<option name>* is invalid.

Explanation

The command line option, which is specified in the message text, is invalid.

User response

Correct the command line option and retry the operation. Review the IBM® Guardium® S-TAP® for IMS client/server environment information for valid options.

Parent topic: Error messages and codes: AUIXxxxx

AUIX034S A severe error occurred during command line processing; an unknown exception occurred.

Explanation

A severe error occurred during command line processing; an unknown exception occurred.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX035E The operation completed successfully.

Explanation

The operation completed successfully.

User response

No action is required.

Parent topic: Error messages and codes: AUIXxxxx

AUIX036E The address family is not supported by the protocol family (*socket-return-code*).

Explanation

The address family is not supported by the protocol family (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX037E The operation is still in progress (*socket-return-code*).

Explanation

The operation is still in progress (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX038E Permission is denied (*socket-return-code*).

Explanation

Permission is denied (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX039E The network is down (*socket-return-code*).

Explanation

The network is down (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX040E No buffer space is available (*socket-return-code*).

Explanation

No buffer space is available (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX041E Too many sockets have been opened (*socket-return-code*).

Explanation

Too many sockets have been opened (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX042E The protocol is not supported (*socket-return-code*).

Explanation

The protocol is not supported (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX043E The WSAStartup routine was not called (*socket-return-code*).

Explanation

The WSAStartup routine was not called (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX044E The protocol is the wrong type for the socket (*socket-return-code*).

Explanation

The protocol is the wrong type for the socket (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX045E The socket type is not supported (*socket-return-code*).

Explanation

The socket type is not supported (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX046E The destination network is unreachable (*socket-return-code*).

Explanation

The destination network is unreachable (socket-return-code).

User response

Specify the correct host name or IP address.

Parent topic: Error messages and codes: AUIXxxxx

AUIX047E The socket handle is invalid (*socket-return-code*).

Explanation

The socket handle is invalid (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX048E The address is already in use (*socket-return-code*).

Explanation

The address is already in use (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX049E The function call was interrupted (*socket-return-code*

Explanation

The function call was interrupted (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX050E The requested address is not available (*socket-return-code*).

Explanation

The requested address is not available (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX051E The connection was aborted (*socket-return-code*).

Explanation

The connection was aborted (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX052E The connection was refused by the partner (*socket-return-code*).

Explanation

The connection was refused by the partner (socket-return-code).

User response

Verify that the correct port number was specified, and that the partner application has been started and is available.

Parent topic: Error messages and codes: AUIXxxxx

AUIX053E The connection was reset by the partner (*socket-return-code*).

Explanation

The connection was reset by the partner (socket-return-code).

User response

The partner application ended the network connection. If this is unexpected, diagnose the partner application failure. Otherwise, no action is required.

Parent topic: Error messages and codes: AUIXxxxx

AUIX054E The network message is too long (*socket-return-code*).

Explanation

The network message is too long (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX055E The network dropped the connection when reset (*socket-return-code*).

Explanation

The network dropped the connection when reset (socket-return-code

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX056E An invalid parameter was specified (*socket-return-code*).

Explanation

An invalid parameter was specified (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX057E The socket is not connected (*socket-return-code*).

Explanation

The socket is not connected (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX058E The operation is not supported (*socket-return-code*).

Explanation

The operation is not supported (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX059E The socket has been closed (*socket-return-code*).

Explanation

The socket has been closed (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX060E The socket is already connected (*socket-return-code*).

Explanation

The socket is already connected (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX061S An unknown error occurred (*socket-return-code*).

Explanation

An unknown error occurred (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX062E A socket error occurred on *socket-operation* with RC = *return code*: *message-text*.

Explanation

A socket error occurred.

User response

Use the specified message text to diagnose the error.

Parent topic: Error messages and codes: AUIXxxxx

AUIX063E A socket select error occurred: *message-text*.

Explanation

A socket select error occurred.

User response

Use the specified message text to diagnose the error.

Parent topic: Error messages and codes: AUIXxxxx

AUIX064E An XML schema violation was detected; expected root element *element-expected*, but found *element-found* instead.

Explanation

An XML schema violation was detected; expected root element element-expected , but found element-found instead.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX066E An XML schema violation was detected; element *element* value *value* is invalid.

Explanation

An XML schema violation was detected; element element value value is invalid.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX067E An XML schema violation was detected; element name *element* is invalid.

Explanation

An XML schema violation was detected; element name element is invalid.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX068E An XML schema violation was detected; element name *element-found* is invalid (expected *element-expected*).

Explanation

An XML schema violation was detected; element name element-found is invalid (expected element-expected).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX074E An abend occurred: *<abend code>*.

Explanation

This message indicates a callable service abend has occurred. Additional diagnostic information might be present in the message when applicable.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIXxxxx

AUIX076E An XML schema violation was detected; element *element* attribute *attribute* value *value* is invalid.

Explanation

An XML schema violation was detected; element element attribute attribute value value is invalid.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX085E A dynamic allocation error occurred: info code = *info-code*, error code = *error-code*.

Explanation

A dynamic allocation error occurred: info code = info-code, error code = error-code.

User response

See the *MVS™ Programming: Authorized Assembler Services Guide* for more information about the specified information and error codes.

Parent topic: Error messages and codes: AUIXxxxx

AUIX086E A dynamic concatenation error occurred: info code = *info-code*, error code = *error-code*.

Explanation

A dynamic concatenation error occurred: info code = info-code, error code = error-code.

User response

See the *MVS™ Programming: Authorized Assembler Services Guide* for more information about the specified information and error codes.

Parent topic: Error messages and codes: AUIXxxxx

AUIX087E A dynamic free error occurred: info code = *info-code*, error code = *error-code*.

Explanation

A dynamic free error occurred: info code = info-code, error code = error-code.

User response

See the *MVS™ Programming: Authorized Assembler Services Guide* for more information about the specified information and error codes.

Parent topic: Error messages and codes: AUIXxxxx

AUIX088E An invalid dynamic allocation parameter was specified: code = *parm-code*.

Explanation

An invalid dynamic allocation parameter was specified: code = parm-code.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX093S An unexpected error occurred (*file-name*, *line-number*).

Explanation

An unexpected error occurred (file-name, line-number).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX094S An unexpected error occurred with token *token*, (*file-name*, *line-number*).

Explanation

An unexpected error occurred with token token, (file-name, line-number).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX095S An unexpected error occurred with tokens *token* and *token* (*file-name*, *line-number*).

Explanation

An unexpected error occurred with tokens token and token (file-name, line-number).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX096S An unexpected error occurred with tokens *token*, *token* and *token* (*file-name*, *line-number*).

Explanation

An unexpected error occurred with tokens token, token and token (file-name, line-number).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX097S An unexpected error occurred with tokens *token*, *token*, *token*, and *token* (*file-name*, *line-number*.

Explanation

An unexpected error occurred with tokens token, token, token, and token (file-name, line-number.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX098E A thread error occurred on *thread-operation* : *message-text*.

Explanation

A thread error occurred on thread-operation : message-text.

User response

Use the specified message text to diagnose the error.

Parent topic: Error messages and codes: AUIXxxxx

AUIX101E An event error occurred on *event-operation* : *message-text*.

Explanation

An event error occurred on event-operation : message-text.

User response

Use the specified message text to diagnose the error.

Parent topic: Error messages and codes: AUIXxxxx

AUIX104E A mutex error occurred on *mutex-operation* : *message-text*.

Explanation

A mutex error occurred on mutex-operation : message-text.

User response

Use the specified message text to diagnose the error.

Parent topic: Error messages and codes: AUIXxxxx

AUIX109E A semaphore error occurred on *semaphore-operation* : *message-text*.

Explanation

A semaphore error occurred on semaphore-operation : message-text.

User response

Use the specified message text to diagnose the error.

Parent topic: Error messages and codes: AUIXxxxx

AUIX110I The network connection has been disconnected.

Explanation

The network connection has been disconnected.

User response

No action is required.

Parent topic: Error messages and codes: AUIXxxxx

AUIX114E A dynamic allocation query error occurred: info code = *info-code*, error code = *error-code*.

Explanation

A dynamic allocation query error occurred: info code = info-code, error code = error-code.

User response

See the *MVS™ Programming: Authorized Assembler Services Guide* for more information about the specified info and error codes.

Parent topic: Error messages and codes: AUIXxxxx

AUIX115E An input command error occurred on \"*command-operation*\": *message-text*.

Explanation

An input command error occurred on \"command-operation\": message-text.

User response

Contact IBM® Customer Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX116I Received input command: *command-text*.

Explanation

Received input command: command-text.

User response

No action is required.

Parent topic: Error messages and codes: AUIXxxxx

AUIX122I Build date *component* = *date*.

Explanation

Build date component = date.

User response

No action is required.

Parent topic: Error messages and codes: AUIXxxxx

AUIX123W The action was cancelled.

Explanation

The action was cancelled.

User response

No action is required. The operation was cancelled due to user or administrator request.

Parent topic: Error messages and codes: AUIXxxxx

AUIX124S The task is not running APF-authorized.

Explanation

The task is not running APF-authorized.

User response

The Security Guardium® S-TAP® for IMS load library, and the load libraries for all of the IMS subsystems accessed, must be APF-authorized. See IBM Guardium S-TAP for IMS agent for more information about the required configuration steps.

Parent topic: Error messages and codes: AUIXxxxx

AUIX126E A DLL error occurred on *dll-operation* : *message-text*

Explanation

A DLL error occurred on dll-operation : message-text

User response

Contact IBM® Customer Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX127S An error occurred while opening log file *file-name*.

Explanation

An error occurred while opening log file file-name.

User response

Contact IBM® Customer Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX142E An XML schema violation was detected; element *element* value *value* is invalid: expected min *<min-value>* and max *<max value>*.

Explanation

The *element-value* given for *element-name* is out of the range and must be within *min-value* and *max-value*.

User response

Correct the value for the *element-name* in the configuration.

Parent topic: Error messages and codes: AUIXxxxx

AUIX143E An XML schema violation was detected; element *element* attribute *value* value *value* is invalid: expected min *<minimum>* and max *<maximum>*.

Explanation

The element attribute value is not valid.

User response

If the error occurred while reading the agent configuration file, update the configuration. Otherwise, contact IBM® Software Support.
Parent topic: Error messages and codes: AUIXxxxx

AUIX149E Data set *[data set]* is not cataloged.

Explanation

The data set specified in the message text has not been cataloged.

User response

Allocate the data set.
Parent topic: Error messages and codes: AUIXxxxx

AUIX150E Invalid data set *'data set'*: Data set name must not exceed 44 characters.

Explanation

MVS™ data sets cannot exceed 44 characters.

User response

Correct the data set entry, then retry.
Parent topic: Error messages and codes: AUIXxxxx

AUIX151E Invalid data set *{'data set'}*: The segment length must be greater than 0 and less than or equal to 8.

Explanation

The specified data set name has one or more segments that are not between 1 and 8 characters.

User response

Specify a data set where each segment contains more than 0 characters and 8 or fewer characters.
Parent topic: Error messages and codes: AUIXxxxx

AUIX152E Invalid data set *'name'*: The first character in each segment must be alphabetic (A-Z) or national (#, @, $).

Explanation

The data set name provided does not is not a valid name and does not satisfy the MVS™ data set naming requirements.

User response

Correct the data set name and try again.
Parent topic: Error messages and codes: AUIXxxxx

AUIX153E Invalid data set *'<data set>'*: The non-first characters in the segments must be alphabetic (A-Z), numeric, national (#, @, $), or hyphen.

Explanation

The non-first characters in the segments must be alphabetic (A-Z), numeric, national (#, @, $), or hyphen.

User response

Specify a data set where non-first characters in the segments is alphabetic (A-Z), numeric, national (#, @, $), or hyphen.
Parent topic: Error messages and codes: AUIXxxxx

AUIX154E Invalid data set '*<data set>*': The non-first characters in the SMF segments must be alphabetic (A -- Z), numeric, national (#, @, $), hyphen, asterisk (*) or percent (%).

Explanation

The non-first characters in the SMF segments must be alphabetic (A -- Z), numeric, national (#, @, $), hyphen, asterisk (*) or percent (%).

User response

Specify a data set where non-first characters in the SMF segments is alphabetic (A -- Z), numeric, national (#, @, $), hyphen, asterisk (*) or percent (%).
Parent topic: Error messages and codes: AUIXxxxx

AUIX155E Data set *<data set>* is not APF-authorized.

Explanation

The specified data set requires APF authorization.

User response

The specified data set must be APF-authorized. See Configuration overview for more information about the required configuration steps.
Parent topic: Error messages and codes: AUIXxxxx

AUIX156E Invalid data set '*<data set>*': The first character in SMF segment must be alphabetic (A -- Z) or national (#, @, $), asterisk (*) or percent (%).

Explanation

The first character in SMF segment must be alphabetic (A -- Z) or national (#, @, $), asterisk (*) or percent (%).

User response

Specify a data set where first character in SMF segments must be alphabetic (A -- Z) or national (#, @, $), asterisk (*) or percent (%).
Parent topic: Error messages and codes: AUIXxxxx

AUIX160E A dynamic allocation query error occurred: info code = *<info-code>*, error code = *<error-code>*, DD name = *<dd-name>*.

Explanation

A dynamic allocation query error occurred with the specified information code, error code, and DD name.

User response

See the *MVS Programming: Authorized Assembler Services Guide* for more information about the specified info and error codes.
Parent topic: Error messages and codes: AUIXxxxx

AUIX183E The number of file descriptors (sockets) has exceeded maximum = *<number>*.

Explanation

The active program holds too many file or socket descriptors and exceeded system maximum = *<number>*.

User response

Contact your system administrator or IBM Software Support.
Parent topic: Error messages and codes: AUIXxxxx

Error messages and codes: AUIYxxxx

The following information is about error messages and codes that begin with AUIY.

- **AUIY001E**
  A callable services abend *abend* has occurred.
- **AUIY002E**
  GPRS *number-number*: *hex-value hex-value hex-value hex-value*
- **AUIY003E**
  Active module not found.
- **AUIY004E**
  Active module = *module-name*, load point = *hex-address*, offset = *hex-address*
- **AUIY005E**
  PSW = *string string*
- **AUIY006E**
  Callable service invocation failed with return code = *return-code* and reason code = *reason-code*
- **AUIY007I**
  Invoking callable service *callable service*.
- **AUIY008I**
  Returned from callable service *service-name*
- **AUIY009E**
  Invalid data set mask: *data set mask*.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIY001E A callable services abend *abend* has occurred.

Explanation

This message indicates a callable service abend has occurred. Additional diagnostic information is be present in the message when applicable.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIYxxxx

AUIY002E GPRS *number-number*: *hex-value hex-value hex-value hex-value*

Explanation

This message indicates an CSI abend has occurred. Additional diagnostic information is present in the message when applicable.

User response

No action is required.
Parent topic: Error messages and codes: AUIYxxxx

AUIY003E Active module not found.

Explanation

This message indicates a CSI abend has occurred. Additional diagnostic information is present in the message when applicable.

User response

No action is required.
Parent topic: Error messages and codes: AUIYxxxx

AUIY004E Active module = *module-name*, load point = *hex-address*, offset = *hex-address*

Explanation

This message indicates a CSI abend has occurred. Additional diagnostic information is present in the message when applicable.

User response

No action is required.
Parent topic: Error messages and codes: AUIYxxxx

AUIY005E PSW = *string string*

Explanation

This message indicates a CSI abend has occurred. Additional diagnostic information is present in the message when applicable.

User response

No action is required.
Parent topic: Error messages and codes: AUIYxxxx

AUIY006E Callable service invocation failed with return code = *return-code* and reason code = *reason-code*

Explanation

A service requested by the agent task has failed.

User response

View the JES log of the agent task to determine the data set name and reason for the error. Contact IBM® Software Support if you are unable to resolve the error.
Parent topic: Error messages and codes: AUIYxxxx

AUIY007I Invoking callable service *callable service*.

Explanation

The specified callable service has been invoked successfully.

User response

No action is required.
Parent topic: Error messages and codes: AUIYxxxx

AUIY008I Returned from callable service *service-name*

Explanation

Returned from a callable service that is identified in the message.

User response

No action is required.

Parent topic: Error messages and codes: AUIYxxxx

AUIY009E Invalid data set mask: *data set mask*.

Explanation

The specified data set mask is not valid.

User response

Enter a valid data set mask and retry.
Parent topic: Error messages and codes: AUIYxxxx

Error messages and codes: AUIZxxxx

The following information is about error messages and codes that begin with AUIZ.

- **AUIZ002E**
  dd-name DD has already been allocated.
- **AUIZ003W**
  Attached to existing shared memory segment.
- **AUIZ004S**
  Shared memory segment key verification failed ('*key-value*').
- **AUIZ005S**
  Shared memory segment eyecatcher 'value' invalid.
- **AUIZ007S**
  The master address space failed to respond to a connect request.
- **AUIZ008W**
  IBM® Security Guardium® S-TAP® for IMS on z/OS® agent failed to shut down properly last time.
- **AUIZ009S**
  Attempts to attach to shared memory segment *segment key* failed.
- **AUIZ010W**
  Configuration value for <*parameter*> is set below the allowed minimum of <*limit*>.
- **AUIZ011W**
  Configuration value for <*parameter*> is set above the allowed maximum of <*limit*>.

- **AUIZ012I**
  Log-server: listening on port *<port>*.
- **AUIZ013E**
  Log-server: no available port was found in the range *<min-port>-<max-port>*.
- **AUIZ014W**
  Log-server: invalid data received from client *<client-ip>* (*<header-data>*).
- **AUIZ020W**
  Configuration parameter *parameter-name* was ignored: duplicate value specified *specified-value*.
- **AUIZ021E**
  Configuration parameter *option* can't be empty.
- **AUIZ022E**
  At least one active appliance is required.
- **AUIZ023E**
  Duplicate appliance specified: *host/port*.
- **AUIZ024E**
  Duplicate appliance priority specified: *priority*.
- **AUIZ025E**
  Spill size can't be zero if more than one appliance is enabled.
- **AUIZ026E**
  Configuration parameter *<option>* value *<value>* is invalid; expected list *<value-list>*.
- **AUIZ027W**
  Host name can't be resolved *<host-name>*.
- **AUIZ028E**
  Configuration parameter *element-name* value *element-value* is invalid: expected min *value-min* and max *value-max*.
- **AUIZ029E**
  Property *property-name* not found in config.
- **AUIZ030E**
  Configuration parameter *parameter-name* value *parameter-value* is not valid long value.
- **AUIZ031E**
  Configuration parameter *parameter-name* value *parameter-value* is not valid unsigned long value.
- **AUIZ032E**
  Configuration parameter *parameter-name* value *parameter-value* is not valid short value.
- **AUIZ033E**
  Configuration parameter *parameter-name* value *parameter-value* is not valid unsigned short value.
- **AUIZ034E**
  Configuration parameter *parameter-name* value *parameter-value* is not valid boolean value.
- **AUIZ035E**
  Configuration parameter *parameter-name* value *parameter-value* is not valid double value.
- **AUIZ036E**
  Configuration parameter *element-name* value *element-value* length is invalid: expected min *length-min* and max *length-max* characters.
- **AUIZ037I**
  Collection profile *profile* uninstalled successfully.
- **AUIZ038I**
  Collection profile *profile* installed successfully.
- **AUIZ039I**
  Guardium policy processing started.
- **AUIZ040I**
  Guardium policy processing finished [active = *<number1>*, installed = *<number2>*, uninstalled = *<number3>*].
- **AUIZ041E**
  Profile for IMS source *ims_name* was ignored: unknown IMS.
- **AUIZ041W**
  Profile for IMS source *ims_name* was ignored: unknown IMS.
- **AUIZ042W**
  IMS artifact *ims-name* was ignored: invalid IMS definition.
- **AUIZ043E**
  XCF callable service invocation failed: function *function-name*, RC = *nn*, reason code = *hhhhhhhh*, AUIU proc name = *proc-name*, ADS_SHR_MEM ID = *nn*.
- **AUIZ044S**
  Shared memory segment version *S-TAP version found* is not compatible with expected *expected version*.
- **AUIZ045E**
  AUICONFG DD must be allocated.
- **AUIZ046E**
  module-name callable service invocation failed: RC = *return-code*, reason code = *reason-code*.
- **AUIZ047E**
  Specified spill file *data_set_name* does not exist.
- **AUIZ048E**
  Problem encountered for *<spill>*, *<problem area>*: required *<req>*, received *<res>*.
- **AUIZ049E**
  z/OS call failure for *<spill>*, *<problemarea>*: RC= *<rc>*, RSN= *<rsn>*.
- **AUIZ050E**
  Specified Log Stream 'xxx.xxx.xxx' does not exist
- **AUIZ051E**
  Problem encountered while validating *log-stream-name*. Function: *request: CONNECT*, RC = *xx*, RSN = *zzzz*.
- **AUIZ052E**
  Abend occurred while validating *<log stream>*. Abend code = *<code>*, RSN=*<reason>*.
- **AUIZ053E**
  Logging subsystem failed to initialize successfully.
- **AUIZ054E**
  The Batch DLI log Stream and Online DLI log stream names must be different.
- **AUIZ055E**
  Shared memory segment ID *<shm-id>* is not available for use.

- **AUIZ056E**
  Shared memory segment ID *segment_id* is owned by agent *agent_name* and cannot be attached.
- **AUIZ057E**
  A configuration syntax error was detected at line *<number>*; expected "*<token1>*", found "*<token2>*".
- **AUIZ058I**
  Collection profile *<profile-name>* updated successfully.
- **AUIZ059E**
  Configuration parameter *<option>* value *<value>* is invalid: the first character must be alphabetic.
- **AUIZ060E**
  The master address space did not respond within 60 seconds.
- **AUIZ061I**
  AUIHOST file has been detected.
- **AUIZ062I**
  AUIHOST file LPAR name/DNS name overrides in use: CVTS_LPAR_NAME(DNS_NAME)
- **AUIZ063E**
  AUIHOST file format is invalid. RECFM must be FB; LRECL must be 80.
- **AUIZ064E**
  AUIHOST file contains invalid syntax *<line number and string>*
- **AUIZ065W**
  IMS STAP *<name>* TCP/IP streaming disabled due to user settings.
- **AUIZ066E**
  Configuration parameter "DLIFREQ" value *value* is invalid: expected 10K-999K, 1M-10M.
- **AUIZ067W**
  Configuration parameter *<parameter>* value *<wrong value>* is not valid. *<Value>* will be used instead.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIZ002E *dd-name* DD has already been allocated.

Explanation

The *dd-name* DD needed for the task, has been previously allocated.

System action

The task terminates with a return code of 12.

User response

dd-name DD is dynamically allocated. Ensure that the *dd-name* DD is not present in the task JCL. If the *dd-name* is not present in the JCL, contact IBM® Software Support.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ003W Attached to existing shared memory segment.

Explanation

This message corresponds to message AUIZ008W. This message indicates that the memory segment has been cleaned, and is being reused.

User response

No action is required.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ004S Shared memory segment key verification failed ('*key-value*').

Explanation

Shared memory segment validation failed. This usually implies that the shared memory segment is owned by another product or system.

User response

Change shared memory segment id and restart the agent:

```
ADS_SHR_MEM_ID
```

Parent topic: Error messages and codes: AUIZxxxx

AUIZ005S Shared memory segment eyecatcher 'value' invalid.

Explanation

Shared memory segment validation failed. This implies that the shared memory segment is owned by another product or system.

User response

Change shared memory segment ID and restart the agent:

`ADS_SHR_MEM_ID`

Parent topic: Error messages and codes: AUIZxxxx

AUIZ007S The master address space failed to respond to a connect request.

Explanation

A secondary address space failed to connect to the master address space.

User response

Check the listener-port in the address-space-manager-config section of the configuration and verify that it matches in both AUICONFG and members of the primary address space and secondary address spaces.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ008W IBM® Security Guardium® S-TAP® for IMS on z/OS® agent failed to shut down properly last time.

Explanation

When the agent is restarting, the persistent memory object indicates that the agent was abnormally cancelled or terminated without going through the proper clean-up routines, for example, Estae processing. This message might also indicate that another instance of the agent is currently executing.

User response

Verify that there is only one instance of this agent running.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ009S Attempts to attach to shared memory segment *segment key* failed.

Explanation

This error message always occurs in conjunction with error message AUIX013E.

This startup error indicates that attempts to create a shared memory segment failed because of an already existing shared memory segment that never belonged to, or currently does not belong to, the primary agent address space.

This message can occur in the secondary address space if the <id> elements in the <address-space-manager-config> parameters of the AUICONFG config member that is used by the agent primary address space and the secondary address spaces(s) do not match.

User response

Edit SAUISAMP member AUICONFG (or the customized AUICONFG) and specify a different <id> element in the <address-space-manager-config> section.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ010W Configuration value for *<parameter>* is set below the allowed minimum of *<limit>*.

Explanation

Configuration parameter is not valid: *<parameter>* should be not less than *<limit>*.

User response

Change the parameter to comply with the requirements.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ011W Configuration value for *<parameter>* is set above the allowed maximum of *<limit>*.

Explanation

Configuration parameter is not valid: <parameter> should exceed the *<limit>*.

User response

Change the parameter to correspond to the requirements.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ012I Log-server: listening on port *<port>*.

Explanation

Identifies the port number that the Log-server is listening to.

User response

No action is required.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ013E Log-server: no available port was found in the range *<min-port>-<max-port>*.

Explanation

No available port was found in specified range. This usually implies that the range of ports is used by other installations or products.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ014W Log-server: invalid data received from client *<client-ip>* (*<header-data>*).

Explanation

This message indicates that an unexpected connection occurred from *<client-ip>* to log-server port.

System action

The connection is refused, and processing continues.

User response

This warning message can be produced during a system-level port security scan. If you do not want to receive this message, suppress it by using the configuration parameters LOG_FILTER(E) and LOG_FILTER_MSGS_ID(AUIZ014W).

If a port scan was not active when this message was received, it indicates that an unknown message was received by the log-server port. Contact IBM Software Support.

Parent topic: Error messages and codes: AUIZxxxx

AUIZ020W Configuration parameter *parameter-name* was ignored: duplicate value specified *specified-value*.

Explanation

The specified configuration parameter *parameter-name* cannot contain a value that has already been specified for a related parameter.

User response

Fix the duplicate value *specified-value* and restart the agent.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ021E Configuration parameter *option* can't be empty.

Explanation

The configuration parameter *option* contains an invalid value.

User response

Check the valid values for the *option* and correct the configuration file.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ022E At least one active appliance is required.

Explanation

No appliances were specified in the agent configuration, or all specified appliances were disabled.

User response

Check agent configuration and add enabled appliances to configuration.

Parent topic: Error messages and codes: AUIZxxxx

AUIZ023E Duplicate appliance specified: *host/port*.

Explanation

Specified appliance (*host/port*) are duplicates of another appliance specified in the configuration.

User response

Update or remove duplicate appliances in the agent configuration.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ024E Duplicate appliance priority specified: *priority*.

Explanation

Two or more appliances with duplicate priority (*priority*) were specified.

User response

Update or remove appliances with duplicate priorities in the agent configuration.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ025E Spill size can't be zero if more than one appliance is enabled.

Explanation

Spill size should be greater than zero if two or more active appliances are specified.

User response

Specify a valid spill size.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ026E Configuration parameter *<option>* value *<value>* is invalid; expected list *<value-list>*.

Explanation

The configuration parameter *<option>* contains an invalid value.

User response

Check the valid values for the *<option>* and correct the configuration file.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ027W Host name can't be resolved *<host-name>*.

Explanation

An attempt was made to determine the IP address of the host name that was indicated through the use of the z/OS *getaddrinfo* service. The attempt failed.

System action

If the host name is not the local LPAR, processing continues. The TCP/IP address for any events that occur on this LPAR will not be sent to the appliance for reporting. If the host name is the local LPAR where the agent (AUIAstc task) is running, the local host name and IP address will be used for INTER and INTRA task communications.

User response

The z/OS network administrator must verify that the LPAR name exists in the DNS table.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ028E Configuration parameter *element-name* value *element-value* is invalid: expected min *value-min* and max *value-max*.

Explanation

The *element-value* given for *element-name* is out of the range and must be within *min-value* and *max-value*.

User response

Correct the value for the *element-name* in the configuration.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ029E Property *property-name* not found in config.

Explanation

A required property *property-name* could not be loaded from the configuration file because it has been incorrectly specified, specified multiple times, or not specified at all.

User response

Update configuration file and add *property-name* with an appropriate value.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ030E Configuration parameter *parameter-name* value *parameter-value* is not valid long value.

Explanation

The configuration parameter identified by *parameter-name* contains an invalid value. The expected value should be of type *long*.

User response

Correct the configuration value.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ031E Configuration parameter *parameter-name* value *parameter-value* is not valid unsigned long value.

Explanation

The configuration parameter identified by *parameter-name* contains an invalid value. The expected value should be of type *unsigned long*.

User response

Correct the configuration value.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ032E Configuration parameter *parameter-name* value *parameter-value* is not valid short value.

Explanation

The configuration parameter identified by *parameter-name* contains an invalid value. The expected value should be of type *short*.

User response

Correct the configuration value.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ033E Configuration parameter *parameter-name* value *parameter-value* is not valid unsigned short value.

Explanation

The configuration parameter identified by *parameter-name* contains an invalid value. The expected value should be of type *unsigned short*.

User response

Correct the configuration value.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ034E Configuration parameter *parameter-name* value *parameter-value* is not valid boolean value.

Explanation

The configuration parameter identified by *parameter-name* contains an invalid value. The expected value should be of type *boolean*.

User response

Correct the configuration value.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ035E Configuration parameter *parameter-name* value *parameter-value* is not valid double value.

Explanation

The configuration parameter identified by *parameter-name* contains an invalid value. The expected value should be of type *double*.

User response

Correct the configuration value.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ036E Configuration parameter *element-name* value *element-value* length is invalid: expected min *length-min* and max *length-max* characters.

Explanation

The *element-value* given for *element-name* is too long and its length must be within *length-min* and *length-max*.

User response

Correct the value for the *element-name* in the configuration file.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ037I Collection profile *profile* uninstalled successfully.

Explanation

The specified collection profile uninstalled.

User response

No action is required.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ038I Collection profile *profile* installed successfully.

Explanation

The specified collection profile installed.

User response

No action is required.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ039I Guardium® policy processing started.

Explanation

The agent has received a policy message from the appliance and has started to process it.

User response

No action is required.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ040I Guardium® policy processing finished [active = *<number1>*, installed = *<number2>*, uninstalled = *<number3>*].

Explanation

The Guardium policy has been processed. The active, installed, and uninstalled values indicate the number of processed collection profiles.

User response

No action is required.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ041E Profile for IMS source *ims_name* was ignored: unknown IMS.

Explanation

The agent received an IMS policy from the Security Guardium® system which does not relate to this agent instance.

System action

The policy is ignored by this agent.

User response

No action is required.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ041W Profile for IMS source *ims_name* was ignored: unknown IMS.

Explanation

The agent received an IMS policy from the Security Guardium® system which does not relate to this agent instance.

System action

The policy is ignored by this agent.

User response

No action is required.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ042W IMS artifact *ims-name* was ignored: invalid IMS definition.

Explanation

During policy pushdown, an *ims-name* was specified for one of the rules that does not exist in the Guardium® appliance.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ043E XCF callable service invocation failed: function *function-name*, RC = *nn*, reason code = *hhhhhhhh*, AUIU proc name = *proc-name*, ADS_SHR_MEM ID = *nn*.

Explanation

An error occurred attempting to retrieve AUIU tokens from the CF.

User response

If the LPAR is not a sysplex member, no action is necessary. If the LPAR is a sysplex member, please contact IBM® Software Support.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ044S Shared memory segment version *S-TAP version found* is not compatible with expected *expected version*.

Explanation

An attempt to attach to a shared memory segment failed because of version mismatch. This might indicate that the shared memory segment that is identified by ADS_SHR_MEM_ID is already in use by an older version of the product, or another product.

User response

Verify and change the ADS_SHR_MEM_ID that is specified in the agent configuration.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ045E AUICONFG DD must be allocated.

Explanation

The address space requires an AUICONFG DD to be specified in the JCL.

User response

Update the JCL for the address space to include an AUICONFG DD.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ046E *module-name* callable service invocation failed: RC = *return-code*, reason code = *reason-code*.

Explanation

Invocation of the specified module failed due to the specified *return-code* and *reason-code*.

User response

Contact IBM Software Support.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ047E Specified spill file *data_set_name* does not exist.

Explanation

During agent startup, the SMF spill file that is named in the configuration parameter SMF_SPILL_FILE(dsn) was not found.

System action

The agent terminates.

User response

Determine why the file cannot be located. Correct any errors, and restart the agent.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ048E Problem encountered for *<spill>*, *<problem area>*: required *<req>*, received *<res>*.

Explanation

This spill data set *<spill>* could not be validated. The *<problem area>* with the parameters *<req>* and *<res>* gives additional details.

User response

Fix the issue in the *<problem area>* using the required *<req>* value. If necessary, contact IBM® Software Support for additional help.

Parent topic: Error messages and codes: AUIZxxxx

AUIZ049E z/OS call failure for *<spill>*, *<problemarea>*: RC= *<rc>*, RSN= *<rsn>*.

Explanation

An attempt to validate the spill data set has caused an error with the z/OS services. A *<problemarea>* value with return code *<rc>* and reason code *<rsn>* are returned. If the *<problemarea>* value is *OBTAIN*, and the *<rc>* value is 4, the spill database in question might have been migrated. In that case, the spill database should be recalled before processing continues.

User response

If a migrated data set is not the problem, contact IBM Software Support.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ050E Specified Log Stream 'xxx.xxx.xxx' does not exist

Explanation

The z/OS log stream name that was specified in the LOG_STREAM_DLIO or LOG_STREAM_DLIB AUICONFG DD input stream does not exist.

System action

The agent address space terminates.

User response

Correct the log stream name that you provided, or customize and run the AUILSTRx Log Stream definition jobs that are located in the SAUISAMP product data set.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ051E Problem encountered while validating *log-stream-name*. Function: *request: CONNECT*, RC = *xx*, RSN = *zzzz*.

Explanation

There was a failed attempt to validate the z/OS® System Logger Log-Stream, through the use of an IXGCONN call.

System action

Processing terminates.

User response

Determine the cause of the failure by examining the return and reason codes for the IXGCONN macro. These can be found in the manual, *IBM® MVS™ Programming: Authorized Assembler Services References*.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ052E Abend occurred while validating *<log stream>*. Abend code = *<code>*, RSN= *<reason>*.

Explanation

The Log Stream *<log stream>* validation failed with abend code *<code>* and reason code *<reason>*.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIZxxxx

AUIZ053E Logging subsystem failed to initialize successfully.

Explanation

This error can occur for several reasons. It is preceded by the specific occurrence that caused the logging subsystem to fail during initialization.

User response

Review previously issued error messages to determine the cause of the logging failure.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ054E The Batch DLI log Stream and Online DLI log stream names must be different.

Explanation

The log stream name specified for LOG_STREAM_DLIO and LOG_STREAM_DLIB must be different.

User response

Specify different log streams for batch and online in the agent configuration.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ055E Shared memory segment ID *<shm-id>* is not available for use.

Explanation

The shared memory segment ID *<shm-id>* that is specified in the configuration file is not available, or is used by another task.

User response

Check the available *<shm-id>* and update the confugration files. Contact IBM® Software Support if *<shm-id>* is set correctly.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ056E Shared memory segment ID *segment_id* is owned by agent *agent_name* and cannot be attached.

Explanation

The shared memory segment that was identified by the <id> parameter within the address-space-manager-config section of the agent configuration file is already used by the specified agent, *agent_name*.

System action

The agent terminates because it is unable to use the shared memory segment.

User response

To avoid a collision with other agents running on the LPAR, change or include the <id> value in the address-space-manager_config section of the agent configuration file.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ057E A configuration syntax error was detected at line *<number>*; expected "*<token1>*", found "*<token2>*".

Explanation

An invalid value was found in the AUICONFG file and the indicated line.

System action

Processing terminates.

User response

Review Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent for information about permissible configuration values. Correct the syntax error and restart the agent.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ058I Collection profile *<profile-name>* updated successfully.

Explanation

The active collection profile *<profile-name>* has been updated during policy installation.

User response

No action is required.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ059E Configuration parameter *<option>* value *<value>* is invalid: the first character must be alphabetic.

Explanation

The configuration parameter *<option>* contains an invalid value.

User response

Review the valid values for the *<option>* and correct the configuration file.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ060E The master address space did not respond within 60 seconds.

Explanation

The IBM® Guardium® S-TAP® for IMS agent did not send the policy report to the Memory Management Utility (AUIU*STC*) task within 60 seconds of establishing the connection.

System action

The AUIU*STC* task terminates with RC=12.

User response

Contact IBM Software Support.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ061I AUIHOST file has been detected.

Explanation

The AUIHOST DD statement has been detected in the JCL.

System action

The IP address for participating LPARs are resolved by the information contained in this file and described by message AUIxxxI.

User response

If this was not intended, remove the DD statement.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ062I AUIHOST file LPAR name/DNS name overrides in use: CVTS_LPAR_NAME(DNS_NAME)

Explanation

The AUIHOST DD has provided an override for the host named.

System action

The DNS_NAME is the value that is used to perform the gethostbyname call in order to obtain the relevant IP address.

User response

Verify that the supplied LPAR_NAME and DNS_NAME values are correct.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ063E AUIHOST file format is invalid. RECFM must be FB; LRECL must be 80.

Explanation

The file format that was provided by using the AUIHOST DD is incorrect.

System action

The address space terminates.

User response

Verify that the supplied file is a Fixed Block (FB) sequential file, has a logical record length (LRECL) of 80 bytes, and is a either a sequential file or a member of a Partitioned Data Set (PDS or PDS/E). Correct the error and restart the address space.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ064E AUIHOST file contains invalid syntax *<line number and string>*

Explanation

The AUIHOST file supplied contains a record with invalid syntax.

System action

The address space terminates.

User response

Review the Overriding the TCP/IP DNS resolver table topic to verify the required syntax. Correct the record and restart the address space.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ065W IMS STAP <*name*> TCP/IP streaming disabled due to user settings.

Explanation

Simulation mode is on because the STAP_STREAM_EVENTS parameter has been set to N.

System action

Events will not be streamed to the Guardium® system.

User response

To stream events to the Guardium system, set the STAP_STREAM_EVENTS parameter to Y.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ066E Configuration parameter "DLIFREQ" value *value* is invalid: expected 10K-999K, 1M-10M.

Explanation

In the AUICONFG file, the DLIFREQ parameter value is outside of the permitted range. Valid values for the DLIFREQ parameter are 10K -- 999K, or 1M -- 10M.

System action

The AUIA*xxx* task terminates.

User response

Correct the DLIFREQ parameter value.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ067W Configuration parameter <*parameter*> value <*wrong value*> is not valid. <*Value*> will be used instead.

Explanation

Configuration parameter is not valid: <*parameter*> should match <*value*>.

User response

Change the parameter to correspond to the requirements.
Parent topic: Error messages and codes: AUIZxxxx

IBM Security Guardium S-TAP for Data Sets on z/OS

These topics describe how to use IBM Security Guardium S-TAP for Data Sets on z/OS V10.1.3 (also referred to as IBM Guardium S-TAP for Data Sets). The V10.1.3 S-TAP is optimized for the V10.1 Guardium system. IBM Guardium S-TAP for Data Sets collects and correlates data access information from a variety of resources to produce a comprehensive view of business activity for auditors.

About these topics

This information is designed to help database administrators, system programmers, and application programmers perform these tasks:

- Plan for the installation of IBM Guardium S-TAP for Data Sets
- Install and operate IBM Guardium S-TAP for Data Sets
- Configure the IBM Guardium S-TAP for Data Sets environment
- Diagnose and recover from IBM Guardium S-TAP for Data Sets problems

A PDF of this User's Guide is also available here.

- **IBM Security Guardium S-TAP for Data Sets on z/OS overview**
  IBM Security Guardium S-TAP for Data Sets on z/OS (also referred to as IBM Guardium S-TAP for Data Sets) collects and correlates data access information from System Management Facilities (SMF) records and realtime system events to produce a comprehensive view of data set access activity for auditors.
- **Installation requirements for IBM Guardium S-TAP for Data Sets V10.1.3**
  Review the software and authorization prerequisites for installing IBM Guardium S-TAP for Data Sets V10.1.3.
- **Configuring the IBM Guardium S-TAP for Data Sets agent**
  You must configure the IBM Guardium S-TAP for Data Sets agent.
- **IBM Guardium S-TAP for Data Sets administration**
  You must configure the Guardium system to communicate with the IBM Guardium S-TAP for Data Sets agent.
- **Reference information**
  This section provides IBM Guardium S-TAP for Data Sets reference information.
- **Troubleshooting**
  Use these topics to diagnose and correct problems that you might experience with IBM Guardium S-TAP for Data Sets.

Parent topic: S-TAP for z/OS V10.1.3 User's Guide

IBM Security Guardium S-TAP for Data Sets on z/OS overview

IBM Security Guardium S-TAP for Data Sets on z/OS (also referred to as IBM Guardium S-TAP for Data Sets) collects and correlates data access information from System Management Facilities (SMF) records and realtime system events to produce a comprehensive view of data set access activity for auditors.

IBM Guardium S-TAP for Data Sets enables you to collect many different types of information, including:

- Access to VSAM and non-VSAM data sets and security violations that are recorded by SMF.
- Data set operations that are performed against VSAM data sets, such as delete or rename events, recorded by SMF.
- Access to specific records within VSAM data sets, including key-sequenced data sets (KSDS) or relative record data sets (RRDS), captured as they occur.
- Transaction information that is associated with a VSAM KSDS or RRDS logical record operation, performed within a transaction that runs on the Customer Information Control System (CICS) Transaction Server.
- Access to read and update events for a particular VSAM cluster (consisting of one or more physical data sets) for actions performed on the data set as a whole, or actions performed at the individual level for records within the data set.

- **What's new in IBM Guardium S-TAP for Data Sets V10.1.3?**
  Speed and monitoring enhancements are now provided in V10.1.3.
- **IBM Guardium S-TAP for Data Sets components**
  IBM Guardium S-TAP for Data Sets consists of its data collection agent and the Security Guardium system. The IBM Guardium S-TAP for Data Sets agent collects data set access information that is obtained from the SMF record exit interface, as well as record access information that is obtained from individual I/O requests. The Guardium system is a server-based component that provides the product user interface.

Parent topic: IBM Security Guardium S-TAP for Data Sets on z/OS

What's new in IBM Guardium S-TAP for Data Sets V10.1.3?

Speed and monitoring enhancements are now provided in V10.1.3.

Enhanced reporting of partitioned data sets (PDS) and extended partitioned data sets (PDSE) member activity
: IBM Guardium S-TAP for Data Sets can now report on the following types of activity:

  - Member Adds
  - Member Replaces
  - Member Renames
  - Member Deletes
  - STOW Initialization (PDSE directory clearing)

New Simulation option
: Enabling Simulation mode enables you to assess the impact of data collection processing without streaming data to the Guardium appliance.

Increased CICS transaction server support
: IBM Guardium S-TAP for Data Sets supports collection of:

  - CICS Transaction Server 5.3 to capture Record Level Monitoring (RLM) data
  - 8-character CICS local unit of work (with CICS Transaction Server 4.2 and later, until end of service)
  - Dynamic starting and stopping of RLM data collection with new IBM Guardium S-TAP for Data Sets SAMPLIB members

Ability to restrict reporting of sensitive data
: When enabled, the FORCE_LOG_LIMITED parameter enables you to restrict Personally Identifiable Identification (PII) from being sent to the Guardium system.

Reporting of FTP activity
: In addition to monitoring of JES2, JES3, ASCH, TSO, and STC address spaces, IBM Guardium S-TAP for Data Sets provides OMVS address space monitoring. This enables reporting of FTP activity.

Reporting of FTP transmission of non-VSAM data sets
: IBM Guardium S-TAP for Data Sets enables you to audit FTP transmission of non-VSAM data sets to and from monitored systems.

New filtering criteria for data set accesses
: For VSAM and non-VSAM Data Sets Close events, you can filter by input-only, output-only, or both input and output events.

Support for Internet Protocol version 6 (IPV6)
: PH16991 introduces IPV6 support and new subsystem configuration option, PREFER_IPV4_STACK.

Parent topic: IBM Security Guardium S-TAP for Data Sets on z/OS overview

IBM Guardium S-TAP for Data Sets components

IBM Guardium S-TAP for Data Sets consists of its data collection agent and the Security Guardium system. The IBM Guardium S-TAP for Data Sets agent collects data set access information that is obtained from the SMF record exit interface, as well as record access information that is obtained from individual I/O requests. The Guardium system is a server-based component that provides the product user interface.

Guardium system and S-TAP agent communication

Communication between the Guardium system and the agent uses a TCP/IP connection. The collection policies that you create, by using the Guardium system user interface, tell the agent what types of data to collect. The policies specify filter information, such as which jobs and data sets to monitor for data accesses.

Guardium system

Use the Guardium system to gather and generate reports on information from multiple agents that are running on multiple z/OS® systems. The Guardium system:

- Provides the user interface, which processes your requests and displays the resulting information.
- Enables you to create collection policies, which specify the types of data that are to be collected by the agent.

- Stores the collected data.

Agent

The agent collects data from a single z/OS system. Monitoring can be performed at both the data set and record level:

- For data set level monitoring, data is collected directly from SMF records, as presented to various SMF exits with which the agent interfaces.
- For record level monitoring, data is collected when VSAM records are read or written.

Parent topic: IBM Security Guardium S-TAP for Data Sets on z/OS overview

Installation requirements for IBM Guardium S-TAP for Data Sets V10.1.3

Review the software and authorization prerequisites for installing IBM Guardium S-TAP for Data Sets V10.1.3.

- **Software prerequisites**
  IBM Guardium S-TAP for Data Sets requires z/OS Version 2 Release 2 or later, until end of service.
- **User ID authority requirements**
  To install the product, you must have the necessary z/OS user ID authorities.

Parent topic: IBM Security Guardium S-TAP for Data Sets on z/OS

Software prerequisites

IBM Guardium S-TAP for Data Sets requires z/OS® Version 2 Release 2 or later, until end of service.

Customer Information Control System (CICS®) Transaction Server support requires IBM CICS Transaction Server for z/OS V4 Release 2 or later, until end of service.

Parent topic: Installation requirements for IBM Guardium S-TAP for Data Sets V10.1.3

User ID authority requirements

To install the product, you must have the necessary z/OS® user ID authorities.

Your z/OS user ID must have the authority to:

- Define the appropriate SMF record collection parameters in the SMFPRMxx PARMLIB member and APF authorize the load library for the product.
- Update the appropriate procedure library to include the agent started task.

If you choose to enable CICS support, you must also have the authority to:

- Update CICS parameters.
- Add CICS program definitions.
- Update or create CICS system initialization and termination program list tables for startup and shutdown.

If necessary, contact your system administrator to obtain the required authorities.
Parent topic: Installation requirements for IBM Guardium S-TAP for Data Sets V10.1.3

Configuring the IBM Guardium S-TAP for Data Sets agent

You must configure the IBM Guardium S-TAP for Data Sets agent.

Configuration overview

To configure the product, complete the required steps.

- Security: Review and establish the security requirements. You must set up access controls in your security product in order to create, authorize, or update the various data sets that are necessary for product configuration.
- Review the required resource authorizations information, including:
  - APF authorizing the load library
  - Authorizing the z/OS agent started task for the control data set
  - Defining an OMVS segment
- Planning your configuration: Review the steps that are required to plan your configuration.
  - Job cards for the sample JCL in the sample library: Provide valid job cards.
  - Allocating auxiliary storage: Ensure that data will not be lost in the event of an overflow.
- Configuring the SMFPRMxx parameter library member: Ensure a complete audit by configuring the SMFPRMxx parameter library to collect the required SMF record types.
- IAM and ACF2 collection considerations: Review information about capturing IAM data set activity and ACF2 access failures.
- Creating the control data set: Generate the initial partitioned data set members.
- Specifying subsystem options: Review the subsystem changes that you can make to the options member in the control data set.
- Configuring the started task JCL: Determine the location of the started task control job language (JCL), and follow configuration steps and tips.
- CICS Transaction Server support: Review the requirements for enabling the CICS Transaction Server, and follow the instructions for Configuring CICS Transaction Server support.

- **Security**
  IBM Guardium S-TAP for Data Sets requires access to various z/OS data sets and system components. You must set up access controls in your security product in order to create, authorize, or update the various data sets that are necessary for product configuration.

- **Planning your configuration**
  Use this planning list to determine necessary information before continuing. Then, provide a valid job card, and allocate auxiliary storage if necessary, as described in the following sections.
- **Configuring the SMFPRMxx parameter library member**
  To ensure a complete audit, you must configure the active SMFPRMxx member of the z/OS system PARMLIB to collect the required SMF record types needed by IBM Guardium S-TAP for Data Sets.
- **IAM and ACF2 collection considerations**
  IBM Guardium S-TAP for Data Sets can capture IAM data set activity and ACF2 access failures. Learn how to enable IBM Guardium S-TAP for Data Sets to collect this information, and be aware of the following collection considerations. These products implement the collection of SMF data in a nonstandard way and require special consideration.
- **Creating the control data set**
  Complete these steps to create the control data set and generate the initial partitioned data set (PDS) members. These members contain required information, and must be added to the newly created data set for the agent to work correctly.
- **Specifying subsystem options**
  To configure IBM Guardium S-TAP for Data Sets, you must specify a four-character IBM Guardium S-TAP for Data Sets subsystem ID (SUBSYS) to associate with this particular instance of IBM Guardium S-TAP for Data Sets. The SUBSYS identifies the IBM Guardium S-TAP for Data Sets subsystem in messages that are generated by the product.
- **Configuring the started task JCL**
  You must configure the started task JCL statements with values that provide the system with information that is specific to your environment. Follow these steps to configure the started task JCL.
- **CICS Transaction Server support**
  IBM Guardium S-TAP for Data Sets CICS Transaction Server support enables you to filter and capture CICS transaction information.
- **Configuring CICS signon reporting**
  IBM Guardium S-TAP for Data Sets can identify the CICS signon that was used for a specific file access event. Configure the product to enable the agent to send the CICS signon information to the Guardium system.
- **Starting the product**
  Start IBM Guardium S-TAP for Data Sets before starting products that perform similar functions.
- **Sample library members**
  The following sample library members are included for your use in installing and configuring IBM Guardium S-TAP for Data Sets. The following table lists them by type and description.
- **Verifying the installation**
  After you install and configure the IBM Guardium S-TAP for Data Sets agent, verify that the agent is properly installed. Use the JCL that is provided in the AUVJIVP member of the SAUVSAMP sample library.

Parent topic: IBM Security Guardium S-TAP for Data Sets on z/OS

Security

IBM Guardium S-TAP for Data Sets requires access to various z/OS® data sets and system components. You must set up access controls in your security product in order to create, authorize, or update the various data sets that are necessary for product configuration.

To provide IBM Guardium S-TAP for Data Sets with access to the necessary z/OS data sets and system components, you must APF authorize the load library, authorize the z/OS started task for the control data set, and define an OMVS segment to your security product, as described in the following sections.

Security products can include various software tools that are currently available, such as IBM Resource Access Control Facility (RACF®), Computer Associates International Top Secret, and Computer Associates International Access Control Facility (ACF2).

- **APF authorizing the load library**
  IBM Guardium S-TAP for Data Sets requires certain data sets to be accessible and APF authorized on the system on which the agent started task will run. SMF data will be collected by the agent.
- **Authorizing the z/OS agent started task for the control data set**
  The z/OS agent started task must be authorized to read and update the control data set. The control data set is a partitioned data set that contains various members that define options and operating parameters for the product. IBM Guardium S-TAP for Data Sets uses a control data set that is defined in the agent started task.
- **Defining an OMVS segment**
  You must define an OMVS segment to your security product to make use of TCP/IP connectivity and UNIX System Services. An OMVS segment specifies the user ID to be used, the home directory, and the shell program name.

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

APF authorizing the load library

IBM Guardium S-TAP for Data Sets requires certain data sets to be accessible and APF authorized on the system on which the agent started task will run. SMF data will be collected by the agent.

The product data set SAUVLOAD, which contains the product load modules that are required for operation, must be APF authorized on the system on which IBM Guardium S-TAP for Data Sets will be run.

Refer to the z/OS MVS Programming Authorized Assembler Services Guide for guidelines and instructions for using APF.

Parent topic: Security

Authorizing the z/OS agent started task for the control data set

The z/OS® agent started task must be authorized to read and update the control data set. The control data set is a partitioned data set that contains various members that define options and operating parameters for the product. IBM Guardium S-TAP for Data Sets uses a control data set that is defined in the agent started task.

Refer to your security product documentation for more information on authorizing the agent started task.

Parent topic: Security

Defining an OMVS segment

You must define an OMVS segment to your security product to make use of TCP/IP connectivity and UNIX System Services. An OMVS segment specifies the user ID to be used, the home directory, and the shell program name.

If you are using IBM RACF, refer to z/OS UNIX System Services Planning for guidelines and instructions about OMVS segment definitions. If you are using a security product other than RACF, refer to your product's instructions on how to define an OMVS segment.

Parent topic: Security

Planning your configuration

Use this planning list to determine necessary information before continuing. Then, provide a valid job card, and allocate auxiliary storage if necessary, as described in the following sections.

Before configuration, you must determine:

- The user who will configure the product
- The user ID that will be used to run the agent
- Where the Guardium system and the S-TAP agent will run

- **Job cards for the sample JCL in the sample library**
  Some JCL members that are included with the product sample library, SAUVSAMP, have a sample card for the job card. Provide a valid job card that conforms to the JCL standards of your site before submitting any of the JCL members.
- **Allocating auxiliary storage**
  z/OS auxiliary storage consists of DASD space that is allocated to the local page data sets. It is used as temporary backup storage for programs and data located in virtual and physical memory. IBM Guardium S-TAP for Data Sets can allocate auxiliary storage space if the OUTAGE_SPILLAREA_SIZE parameter is set in accordance with the following requirements.

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

Job cards for the sample JCL in the sample library

Some JCL members that are included with the product sample library, SAUVSAMP, have a sample card for the job card. Provide a valid job card that conforms to the JCL standards of your site before submitting any of the JCL members.

Parent topic: Planning your configuration

Allocating auxiliary storage

z/OS auxiliary storage consists of DASD space that is allocated to the local page data sets. It is used as temporary backup storage for programs and data located in virtual and physical memory. IBM Guardium S-TAP for Data Sets can allocate auxiliary storage space if the OUTAGE_SPILLAREA_SIZE parameter is set in accordance with the following requirements.

- The OUTAGE_SPILLAREA_SIZE parameter option instructs the address space to allocate a data space equal in size to the value that you set for OUTAGE_SPILLAREA_SIZE.
- Verify that the current local page space can accommodate a new data space.

Example

Specifying OUTAGE_SPILLAREA_SIZE=64 instructs the address space to allocate 64 MB of data space.

Refer to the z/OS® MVS™ Initialization and Tuning guide for more information about sizing local page data sets.
Parent topic: Planning your configuration

Configuring the SMFPRMxx parameter library member

To ensure a complete audit, you must configure the active SMFPRMxx member of the z/OS® system PARMLIB to collect the required SMF record types needed by IBM Guardium S-TAP for Data Sets.

The record types can be collected at the subsystem or system level. Maximum auditing of VSAM and non-VSAM data set activity can be achieved by ensuring that all defined subsystems record all of the SMF record types that are required by the product.

The defaults used at the system level for those subsystems that are not explicitly defined should also specify collection of the required SMF record types. The required SMF record types are 14, 15, 17, 18, 30, 42, 60, 61, 62, 64, 65, 66, and 80. If any required SMF record types are not defined for collection, message AUV1450W alerts you to define them.

If the appropriate exit is not defined for the operating system level, SMF records will not be collected. Specify the SMF exits as follows:

- For z/OS Version 2 Release 2 and earlier, specify the IEFU83, IEFU84, and IEFU85 SMF exits.
- For z/OS Version 2 Release 3 and later, specify the IEFU86 SMF exit.

These exits can be defined at either the subsystem or system level in a manner consistent with the SMF record type specifications.

For more information about setting up and managing SMF, refer to the z/OS MVS™ System Management Facility (SMF) manual.

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

Related reference

- SMF record types and contexts

IAM and ACF2 collection considerations

IBM Guardium S-TAP for Data Sets can capture IAM data set activity and ACF2 access failures. Learn how to enable IBM Guardium S-TAP for Data Sets to collect this information, and be aware of the following collection considerations. These products implement the collection of SMF data in a nonstandard way and require special consideration.

Innovation Access Method (IAM) from Innovation Data Processing provides capabilities beyond standard VSAM. IAM replaces VSAM access with a proprietary non-VSAM access that simulates VSAM. Because the underlying data sets are non-VSAM, accesses to the IAM-simulated VSAM data sets do not generate VSAM SMF records, such as the SMF type 62 (VSAM OPEN) and SMF type 64 (VSAM CLOSE).

For IAM data sets, IBM Guardium S-TAP for Data Sets does not report the following items:

- Context records for OPEN and UPDATE for IAM data sets (because of the lack of the SMF type 62 records).
- IAM simulation of alternate index and path processing (because of the lack of an IAM SMF CLOSE record).

The CLOSE record counters will report IAM data sets differently from native VSAM processing. Although the IAM CLOSE SMF record offers an extensive array of counters, those corresponding to the VSAM SMF Type 64 record are included in the accumulated counts within the CLOSE context record.

Computer Associates International ACF2 considerations

Unlike some security products, ACF2 does not offer a unique authorization failure code to identify a CONTROL access failure. Instead, it reports these as UPDATE access failures. In ACF2 facilities, no CONTROL context records will be reported.

- **Enabling Innovations Data Processing IAM reporting**
  IAM provides a unique, user-specified record ID, which is written during CLOSE processing. For IBM Guardium S-TAP for Data Sets to report this access:
- **Enabling Computer Associates International ACF2 reporting**
  Access Control Facility (ACF2) from Computer Associates International records access failures to a unique, user-specified record ID. For IBM Guardium S-TAP for Data Sets to report these failures:

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

Enabling Innovations Data Processing IAM reporting

IAM provides a unique, user-specified record ID, which is written during CLOSE processing. For IBM Guardium S-TAP for Data Sets to report this access:

Procedure

1. Determine the user-specified SMF record ID that was selected for IAM.
2. Specify that value in the IBM Guardium S-TAP for Data Sets control data set IAM_SMF_RECORD_ID option.

Parent topic: IAM and ACF2 collection considerations

Enabling Computer Associates International ACF2 reporting

Access Control Facility (ACF2) from Computer Associates International records access failures to a unique, user-specified record ID. For IBM Guardium S-TAP for Data Sets to report these failures:

Procedure

1. Determine the user-specified SMF record ID that was selected for ACF2.
2. Specify that value in the IBM Guardium S-TAP for Data Sets control data set ACF_SMF_RECORD_ID option.

Parent topic: IAM and ACF2 collection considerations

Creating the control data set

Complete these steps to create the control data set and generate the initial partitioned data set (PDS) members. These members contain required information, and must be added to the newly created data set for the agent to work correctly.

Before you begin

Refer to the high-level qualifier that you specified when configuring the started task JCL. The same high-level qualifier must be used in step 1 of the control data set creation procedure.

About this task

The options and definitions that determine how IBM Guardium S-TAP for Data Sets performs processing in your environment are contained in the control data set.

Procedure

1. The JCL to create the control data set is located in the AUVJCNTL member of the SAUVSAMP library. Configure the AUVJCNTL member by replacing AUV.V10R1M3 with the high-level qualifier of the installed IBM Guardium S-TAP for Data Sets load library.
2. Submit the JCL to create the control data set.
   The JCL creates the control data set and populates the data set with these initial members: subsystem options (OPTIONS) and policy rule definition members (RULEDEFS and RULEDEFB).
   Important:
   - Do not modify the contents of the RULEDEFS or RULEDEFB member.
   - Do not modify the value of the default INITIAL_RULEDEF option in the RULEDEFS or RULEDEFB members.
3. Specify the APPLIANCE_SERVER and AUDIT parameters in the OPTIONS member to enable the product to function properly.
4. Optional: Consider whether allocating the control data set as an extended partitioned data set (PDSE) is appropriate for your environment.
   A PDSE dynamically manages internal space, drastically reducing the need to perform the space compressions that are required for a nonextended partitioned data set (PDS). The AUVJCNTL member includes statements that can be used to change the allocation to a PDSE.

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

Specifying subsystem options

To configure IBM Guardium S-TAP for Data Sets, you must specify a four-character IBM Guardium S-TAP for Data Sets subsystem ID (SUBSYS) to associate with this particular instance of IBM Guardium S-TAP for Data Sets. The SUBSYS identifies the IBM Guardium S-TAP for Data Sets subsystem in messages that are generated by the product.

How to use subsystem options

Use either the *keyword=value* or *keyword(value)* format to specify values for these option members.

Option members and descriptions

The IBM Guardium S-TAP for Data Sets subsystem options are in the OPTIONS member of the IBM Guardium S-TAP for Data Sets control data set that is generated by the AUVJCNTL member JCL. These options are the global definitions and general operation options that determine where and how IBM Guardium S-TAP for Data Sets performs its functions.

To specify IBM Guardium S-TAP for Data Sets subsystem options, modify the contents of the OPTIONS member as described.

ACF_SMF_RECORD_ID
: If you are using Access Control Facility (ACF2) from Computer Associates International, you must provide product-specific information for your SMF data to be processed. ACF2 records access failures to a unique record ID. Determine the user-specified SMF record ID that is selected for ACF2 and specify that ID in the IBM Guardium S-TAP for Data Sets CONTROL data set ACF_SMF_RECORD_ID option if you want the product to report these failures.
  ACF2 writes SMF access failure data to a user-defined SMF record ID. Specify a numeric value that identifies the SMF record identification number used by ACF2.
  For ACF2 installations, contact your ACF2 administrator to determine the appropriate numeric value to include with this parameter.
  Note:

  - For z/OS Version 2 Release 3 and later, valid values are 128 – 1151.
  - For z/OS Version 2 Release 2 and earlier, valid values are 128 – 255.

  There is no product default value, however, the SAMPLIB member AUVSOPTS includes a default specification of 230.

APPLIANCE_CONNECT_RETRY_COUNT
: Specify a numeric value that defines the number of times to retry communicating with the Guardium system when an error is encountered during initialization. If the communication is still not successful after the number of retries as specified by this value has been completed, the communication is abandoned and no data is sent. The process also terminates if the number of retries specified is reached with no successful connection.
  Valid values are 0 -- 65535. The default value is 20.

APPLIANCE_NETWORK_REQUEST_TIMEOUT
: Specify a numeric value that defines the number of seconds that must transpire before a timeout is recognized.
  Valid values are 0 -- 65535. The default value, in seconds, is 0.

APPLIANCE_PING_RATE
: Specify a numeric value that defines the number of seconds between pings to the Guardium system. The ping signals the Guardium system that the S-TAP is active and available for communications.
  Valid values are 1 -- 65535. The default value, in seconds, is 5.

APPLIANCE_PORT
: Specify a numeric value that defines the TCP/IP port number for communication with the Guardium system by IBM Guardium S-TAP for Data Sets. Use port 16022 for the V10.1.3 system protocol.
  The default value is 16022.
  If port 16023 is used, encryption support is required for the connection to the appliance.
  Note: Specifying this keyword and parameter designates the port on which the Guardium appliance is listening to the S-TAP. The port is dedicated to the IP address of the appliance. Port 16022 or 16023 can also be in use on z/OS® by another application.
  Valid values are 16022 and 16023.

APPLIANCE_RETRY_INTERVAL
: Specify a numeric value that defines the number of seconds between retries when an error is encountered during an initial attempt to connect to the Guardium system.
  Valid values are 0 -- 65535. The default value, in seconds, is 10.

APPLIANCE_SERVER
: Specify the TCP/IP address for the Guardium system with which IBM Guardium S-TAP for Data Sets is to communicate. In multistream processing scenarios, this address specifies the first Guardium appliance that is to be used.
  The address can be specified as a host name (*security.guardiumvsam.net*) or as four numbers separated by periods (for example, 188.128.6.42).
  Maximum length is 53 characters. There is no default.

APPLIANCE_SERVER_[1-5]
: Specify alternative TCP/IP addresses to use for failover recovery processing and multistream Guardium appliance destinations. Up to five alternative TCP/IP addresses are supported.
  To specify one or more entries, include this parameter with a numeric suffix from 1 - 5. Provide a unique TCP/IP address for each entry.
  The option syntax is as follows:

- APPPLIANCE_SERVER_1=*addr*

or

- APPPLIANCE_SERVER_1(*addr*)

where 1 can be 1, 2, 3, 4, or 5.
Valid values are any valid TCP/IP address. There are no default values. If initialization does not detect this parameter, it does not activate the failover process.
Both the APPLIANCE_SERVER_[1-5] and APPLIANCE _SERVER_FAILOVER_[1-5] parameters can be used to designate servers for multistreaming or failover. Use the APPLIANCE_SERVER_LIST parameter to designate how these parameters are used.
Maximum length is 51 characters.

APPLIANCE_SERVER_FAILOVER_[1-5]

Specify alternative TCP/IP addresses to use for failover and recovery processing. The product supports up to five alternative TCP/IP addresses. To specify one or more entries, include this parameter with a numeric suffix from 1 - 5, each time providing a unique TCP/IP address.
The option syntax is as follows:

```
APPPLIANCE_SERVER_FAILOVER_1=addr
```

or

```
APPPLIANCE_SERVER_FAILOVER_1(addr)
```

where *1* can be 1, 2, 3, 4, or 5.
Valid values are any valid TCP/IP address. There are no default values. If initialization does not detect this parameter, it does not activate the failover process.
Both the APPLIANCE _SERVER_FAILOVER_[1-5] and APPLIANCE_SERVER_[1-5] parameters can be used to designate servers for multistreaming or failover. Use the APPLIANCE_SERVER_LIST parameter to designate how these parameters are used.
Maximum length is 42 characters.

APPLIANCE_SERVER_LIST(MULTI_STREAM|FAILOVER|HOT_FAILOVER)

Set APPLIANCE_SERVER_LIST to *MULTI_STREAM* for a Guardium appliance connection to be established for each server that is identified by the APPLIANCE_SERVER_n or APPLIANCE_SERVER_FAILOVER_n parameters.

- If a connection is lost, S-TAP audit events continue to transmit over the remaining appliance connection.
- Lost connections are retried at regular intervals that are determined by multiplying the APPLIANCE_CONNECT_RETRY_COUNT by the APPLIANCE_PING_RATE.

Set APPLIANCE_SERVER_LIST to *FAILOVER* for one Guardium appliance connection to be active at a time.

- If the connection to the primary appliance is lost, a failover action occurs, which results in an attempt to connect to the next available server. The next available server is identified by the APPLIANCE_SERVER_n or APPLIANCE_SERVER_FAILOVER_n parameter.
- After a failover action occurs, the connection to the primary server is retried at regular intervals that are determined by multiplying the APPLIANCE_CONNECT_RETRY_COUNT by the APPLIANCE_PING_RATE.

Set APPLIANCE_SERVER_LIST to *HOT_FAILOVER* to keep each connected Guardium appliance active via pings. If the primary Guardium appliance (which is set by the APPLIANCE_SERVER parameter) becomes unavailable and failover occurs, *HOT_FAILOVER* maintains the activity of the primary appliance policy.
With all settings of APPLIANCE_SERVER_LIST, if all connections fail, and a spill file is specified (parameter OUTAGE_SPILLAREA_SIZE), events are buffered to the spill file until a connection becomes available. If no spill file is specified, and all connections are lost, data loss occurs.
The default is *FAILOVER*.

AUDIT

Specify a character string from one through 26 characters that defines the name of this IBM Guardium S-TAP for Data Sets agent.
There is no default.

CICS_SUPPORT

Enabling CICS® Transaction Server support activates additional reporting of CICS-specific information on record level events, including:

- CICS File ID
- CICS Function Code
- CICS Program ID
- CICS Region ID
- CICS Terminal ID
- CICS Transaction ID
- CICS User ID
- CICS Logical Unit of Work

Enable or disable CICS support by specifying `ENABLE` or `DISABLE`.
The default is *DISABLE*.
If you enable CICS support, you must also configure CICS for record level monitoring events to be captured for CICS. For more information about CICS support, see CICS Transaction Server support.

FORCE_LOG_LIMITED

Record level monitoring enables you to monitor VSAM file access based on key values. The VSAM key can contain Personally Identifying Information, such as account number, last name, or Social Security number. When the FORCE_LOG_LIMITED option is enabled, IBM Guardium S-TAP for Data Sets does not monitor any record level data. If the file is being monitored by a policy, then only file access is reported; monitoring and reporting of access to specific keys is suppressed.
Specify *Y* to prevent Personally Identifiable Identification (PII) data from being sent to the Guardium system. Data that is sent as part of Record Level Monitoring and CICS is considered PII. This data will not be sent to the Guardium system if FORCE_LOG_LIMITED(*Y*) is specified.
The default is *N*.

IAM_SMF_RECORD_ID

If you are using Innovation Access Method (IAM) from Innovation Data Processing, you must provide product-specific information for your SMF data to be processed. IAM provides a unique user-specified record ID, which it writes during CLOSE processing. For IBM Guardium S-TAP for Data Sets to report this access, determine the user SMF record ID for IAM, and specify that value in the IBM Guardium S-TAP for Data Sets control data set IAM_SMF_RECORD_ID option.
IAM writes SMF statistical data to a user-defined SMF record ID. Specify a numeric value that identifies the SMF record identification number used by IAM.
For IAM installations, consult your IAM administrator to determine the appropriate numeric value to include with this parameter.
Note:

- For z/OS Version 2 Release 3 and later, valid values are 128 – 1151.
- For z/OS Version 2 Release 2 and earlier, valid values are 128 – 255.

There is no product default value; however, the SAMPLIB member AUVSOPTS includes a default specification of 201.

INTERNAL_BUFFER_SIZE

Specify the size of the internal buffer used.

To improve performance, data is stored in an internal buffer that is sent when the buffer is full or during a ping request. If the buffer reaches the INTERNAL_BUFFER_SIZE, data is sent without waiting for the next ping request.

Specifying an INTERNAL_BUFFER_SIZE value that is too large for your environment can cause connection problems that are due to timing out while trying to send a large amount of data. Specifying too small a value might cause unnecessary I/O requests.

Tip: Performance varies based on system load, network load, and the load on the Guardium system, so the correct value for your environment cannot be predetermined. Begin with the default value, and make minor, incremental adjustments to improve performance, if necessary.

Valid values are 0 -- 2047 megabytes. The default is 8.

INITIAL_RULEDEF

You must not change this subsystem option unless IBM Software Support instructs you to do so. If instructed to modify this subsystem option, specify the name of the rule definitions member to use at startup. The default rule definitions member name is RULEDEFS.

MEGABUFFER_COUNT

Specify the number of IBM Guardium S-TAP for Data Sets audit events that are buffered, prior to the product attempting a TCP/IP send operation.

The megabuffer is flushed when either of two conditions is met:

- At regular intervals, based on the APPLIANCE_PING_RATE
- When the number of audit events that are held in the megabuffer reaches the count that is specified by this parameter

When MULTI_STREAM mode is enabled by parameter APPLIANCE_SERVER_LIST, and a megabuffer flush occurs, the audit event data stream is switched to the next available Guardium appliance. The event data stream will switch from appliance to appliance in a round-robin sequence as each megabuffer is sent.

Valid values are 1 -- 8192. The default is 200.

OUTAGE_SPILLAREA_SIZE

Specify the size of the spill file to be used when a connection cannot be made.

If the product includes a spill file, and no secondary APPLIANCE_SERVER_FAILOVER address is specified, or none of the secondary APPLIANCE_SERVER_FAILOVER addresses respond, it writes to the spill file. The spill file is meant for short-term outages only, because when a connection is restored to any Guardium system, it clears the spill file content before continuing to send data.

Valid values are 0 -- 1024 megabytes. If a valid value is not specified, a spill file is not created.

PREFER_IPV4_STACK

Specify the request for an IPV4 address to be issued from the Domain Name Server (DNS). The default value is N.

- Y causes a request to be issued to the DNS for an IPV4 address for the hostname that is specified in the APPLIANCE_SERVER parameter:
  - The DNS lookup request for an IPV4 address is attempted. If an IPV4 address is defined for the hostname, the DNS will respond with the value that will be used to connect to the Guardium appliance.
  - If only an IPV6 address is defined at the DNS, then the DNS will respond with the IPV6 address that will be used to connect to the Guardium appliance.
  - If both IPV4 and IPV6 addresses are defined at the Guardium appliance, the DNS will respond with both addresses, and the IPV4 address will be used to connect to the appliance.
- N or omitting this option from configuration causes a request for an IPV6 address to be issued to the DNS for the hostname that is specified by the APPLIANCE_SERVER parameter.
  - The DNS lookup request for an IPV6 address is attempted. If an IPV6 address is defined for the hostname, the DNS will respond with the value that will be used to connect to the Guardium appliance.
  - If only an IPV4 address is defined at the DNS, then the DNS will respond with the IPV6 address that will be used to connect to the Guardium appliance.
  - If both IPV4 and IPV6 addresses are defined at the Guardium appliance, the DNS will respond with both addresses, and the IPV4 address will be used to connect to the appliance.

Note: Whether or not this option is specified, if the address returned from the DNS is not valid for the hostname, it will result in failure to connect to the appliance, and the IBM Guardium S-TAP for Data Sets started task will terminate.

RLM

Specify the initial status of RLM processing by setting the RLM parameter to either *ENABLE* or *DISABLE*. *ENABLE* enables record level monitoring. *DISABLE* disables record level monitoring.

The default value is *ENABLE*.

SOCKET_CONNECT_TIMEOUT

Specify the length of time for socket connection attempts before failure or timeout.

Setting this value too low results in connection failures when the Guardium system is slow to respond. Setting this value too high causes problems in failover scenarios.

Tip: Performance varies based on system load, network load, and the load on the Guardium system, so the correct value for your environment cannot be predetermined. Begin with the default value, and make minor, incremental adjustments to improve performance, if necessary.

Valid values are 1 -- 65535. The default value, in seconds, is 3.

STAP_STREAM_EVENTS

Specify the initial streaming status by setting the STAP_STREAM_EVENTS parameter to either *Y* or *N*.

- Y indicates that the IBM Guardium S-TAP for Data Sets agent address space will send data to the server in a manner that is consistent with the active policy.
- N indicates that the agent address space will not send data to the server. It will perform all data collection processing in a manner that is consistent with the active policy. The agent address space will issue message AUV1070I at startup: TCP/IP STREAMING DISABLED DUE TO USER SETTING. See Simulation mode for more information.

The default value is *Y*.

SUBSYS

Choose any four-character alphanumerical subsystem ID to identify this particular instance of IBM Guardium S-TAP for Data Sets. For example, `AUV1`, `AUV2`, and so on.

Choose a unique SSID for each agent.

The default subsystem ID is *VTAP*.

SUPPRESS_INCOMPLETE_EVENTS

Enables SMF records without identifying characteristics to either be suppressed or sent to the appliance. Specify the SMF event filtering preference for SMF records with missing identifying characteristics, where:

- *N* indicates that missing field values in SMF records should always pass policy rule filters.
- *Y* indicates that missing field values should not pass the filters and the corresponding events should not be sent to the appliance.

The default value is *N*.
For more information, see SMF record identification considerations.

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

Configuring the started task JCL

You must configure the started task JCL statements with values that provide the system with information that is specific to your environment. Follow these steps to configure the started task JCL.

About this task

The IBM Guardium S-TAP for Data Sets started task JCL is located in the AUVJSTC member of the IBM Guardium S-TAP for Data Sets sample library (SAUVSAMP).
Note: Do not start the started task until you finish configuring IBM Guardium S-TAP for Data Sets. Attempting to start the started task before completing configuration can cause the started task to fail.

Procedure

1. Copy the IBM Guardium S-TAP for Data Sets started task JCL to your system PROCLIB from sample data set member AUVJSTC.
   Tip: Name the IBM Guardium S-TAP for Data Sets started task member AUVSTAPV. This name is easily identifiable with the IBM Guardium S-TAP for Data Sets product.
2. Verify that the statement: //AUVSTAPV PROC OPTSMBR=OPTIONS points to the default member name OPTIONS.
   The default member name OPTIONS was created during creation of the control data set.
3. Configure the started task JCL that you copied to your system PROCLIB by replacing AUV.V10R1M3 with the high-level qualifier of the installed IBM Guardium S-TAP for Data Sets load library.
   Note: For operation of the product, policy activation, and correct processing of data, the following conditions must be met:
   - A DD statement with the DDNAME OPTIONS must be in the IBM Guardium S-TAP for Data Sets started task. This DD statement points to the subsystem OPTIONS member of the IBM Guardium S-TAP for Data Sets control data set, which contains the global settings for the product. When the started task is initiated, it references the data in the subsystem options member to establish global settings, including the subsystem identifier for this specific instance of IBM Guardium S-TAP for Data Sets.
     - By default, the OPTIONS DD statement uses the same data set as the RULEDEFS and RULEDEFB DD statements. If necessary, you can specify a different data set for the OPTIONS DD statement other than that which is used for the DD statements RULEDEFS and RULEDEFB. The OPTIONS member must be present in the data set that is specified for the OPTIONS DD statement.
   - A DD statement with a DDNAME of CONTROL must be in the IBM Guardium S-TAP for Data Sets started task. For example: //CONTROL DD DSN=AUV.V10R1M3.CONTROL,DISP=SHR. This DD statement points to the IBM Guardium S-TAP for Data Sets control data set that contains the collection policy in the RULEDEFS member.
   - The two DD statements with the DDNAMES RULEDEFS and RULEDEFB must be present and must point to the same control data set name that was specified in the CONTROL DD statement. The member names RULEDEFS and RULEDEFB must not be changed. If DDNAMES RULEDEFS and RULEDEFB are not present, are changed, or do not point to the correct data set name, then the agent does not initiate correctly and is unable to collect data.
   - The high-level qualifier you specify for the control data set JCL when allocating the control data set must match the high-level qualifier you specify in the started task JCL.
   - The started task must have the authority to read and update the control data set and load library.
4. After you configure the started task JCL, add it to the z/OS® PROCLIB data set for started task initiation.
   Note:

   IBM Guardium S-TAP for Data Sets accommodates the use of multistream and improves support for large policies by providing a default started task JCL region size of 96 megabytes. When multistream is enabled, a buffer is created for each appliance, based on the INTERNAL_BUFFER_SIZE value. (Valid values are 0 - 2047 megabytes. The default value is 8.) The default started task JCL region size of 96 megabytes can accommodate large policies by providing space for up to six connected appliances with a default INTERNAL_BUFFER_SIZE of 8 megabytes and approximately 150,000 values in a policy.

   You might need to increase the started task JCL region size if:
   - the value specified for INTERNAL_BUFFER_SIZE is greater than 8 megabytes
   - an installed policy contains more than 150,000 values

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

CICS Transaction Server support

IBM Guardium S-TAP for Data Sets CICS® Transaction Server support enables you to filter and capture CICS transaction information.

IBM Guardium S-TAP for Data Sets must be running before CICS is started. If changes to a policy are made while a CICS file is open, the file must be closed and reopened for RLM-related policy changes to take effect.

Verify that the agent is running and correctly configured, and the appropriate work area storage is available.

- To capture data on files that are referenced within a transaction, the IBM Guardium S-TAP for Data Sets agent must be running and correctly configured to monitor each system image on which data sets reside.
- CICS support uses the XFCFROUT Global User Exit (GLUE).
- The GLUE acquires an above-the-line work area from the extended CICS dynamic storage area (ECDSA) of approximately 1412 bytes for each active or suspended transaction that performs at least one VSAM file operation. The work area is released at the end of the transaction.

- **Configuring CICS Transaction Server support**
  For CICS related information to be captured, you must configure CICS Transaction Server support.

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

Configuring CICS Transaction Server support

For CICS® related information to be captured, you must configure CICS Transaction Server support.

About this task

If you configure CICS Transaction Server support, you can capture CICS transaction information that is associated with record level monitoring of logical record activities that occur within a CICS transaction for KSDS and RRDS data sets. Remember to start IBM Guardium S-TAP for Data Sets before starting CICS. If changes to a policy are made while a CICS file is open, the file must be closed and reopened for any RLM-related policy changes to take effect.

Procedure

1. Configure the CICS system options.
   a. Specify the CICS_SUPPORT=ENABLE option, by using the subsystem options that are located in the OPTIONS member of the control data set.
2. Configure the CICS system initialization and system termination program list tables (PLTs), as shown in the example at the end of this topic.
   a. Enter the program AUVPLTPI after the DFHDELIM PLT entry.
   b. Enter the program AUVPLTPS before the DFHDELIM PLT entry.
   c. After creating or modifying the CICS system initialization and system termination PLTs, you must assemble and link them. For more information about creating a PLT, see the CICS Transaction Server for z/OS® Resource Definition Guide.
3. Specify autoinstall in the CICS system initialization parameters to automatically install the AUVPLTPI, AUVPLTPS, and AUVFROUT programs.
   If you do not specify autoinstall in the CICS system initialization parameters, you must define AUVPLTPI, AUVPLTPS, and AUVFROUT in the CICS system definition file (CSD). To install the program definitions in batch, sample JCL has been provided in member AUVCSDUP of the IBM Guardium S-TAP for Data Sets SAUVSAMP library that can be modified and used for the CICS program DFHCSDUP. Alternatively, the CICS CEDA Resource Definition Online transaction can also be used to perform the install of the program definitions. See the CICS Transaction Server for z/OS Resource Definition Guide for more information about installing resource definitions.
   a. Define the following attributes:
      - LANGUAGE (ASSEMBLER)
      - STATUS (ENABLED)
      - CEDF (NO)
      - DATALOCATION (BELOW)
      - EXECKEY (CICS)
      - EXECUTIONSET (FULLAPI)
      - RELOAD (NO)

      For the load modules to be located, the AUVPLTPI, AUVPLTPS, and AUVFROUT programs must be located in a load library located in the CICS DFHRPL concatenation within the CICS startup JCL.
4. Optional: The CICS facilities that implement RLM support, outside of normal CICS PLT initialization, can be enabled and disabled. To do so, define CICS transactions accordingly by using the batch CICS program DFHCSDUP or the CICS CEDA Resource Definition Online transaction.

   To enable the CICS facilities that are used to implement CICS RLM support, the following attributes must be assigned to the transaction:

   - TRANSACTION (*tran*, where *tran* is your chosen transaction ID)
   - PROGRAM (AUVPLTPI)
   - TASKDATAKEY (CICS)
   - TASKDATALOC (ANY)

   To disable the CICS facilities that are used to implement CICS RLM support, the following attributes must be assigned to the transaction:
   - TRANSACTION (*tran*, where *tran* is your chosen transaction ID)
   - PROGRAM (AUVPLTPS)
   - TASKDATAKEY (CICS)
   - TASKDATALOC (ANY)
5. Reference the program initialization and termination PLTs in parameters PLTPI and PLTPSD, as described in the topic, Using CICS system initialization parameters.

Results

If you have configured CICS support, message AUV3004I is displayed during CICS initialization to indicate that the Global User Exit AUVPLTPI XFCFROUT was installed and enabled.

Example

Enter the program AUVPLTPI after the DFHDELIM PLT entry in the CICS system initialization PLT:

```
*
*   CICS PROGRAM LIST TABLE FOR CICS SYSTEM INITIALIZATION
*
         DFHPLT TYPE=INITIAL,SUFFIX=I1
*
*  ENTRIES AHEAD OF DFHDELIM ARE EXECUTED IN FIRST PASS OF PLTPI
*  DURING THE SECOND PHASE OF CICS SYSTEM INITIALIZATION
*
         DFHPLT TYPE=ENTRY,PROGRAM=DFHDELIM
*
*  ENTRIES AFTERF DFHDELIM ARE EXECUTED IN SECOND PASS OF PLTPI
*  DURING THE THIRD PHASE OF CICS SYSTEM INITIALIZATION
*
         DFHPLT TYPE=ENTRY,PROGRAM=AUVPLTPI
*
         DFHPLT TYPE=FINAL
*
         END
```

Enter the program AUVPLTS before the DFHDELIM PLT entry in the CICS system termination PLT:

```
*
*   CICS PROGRAM LIST TABLE FOR CICS SYSTEM TERMINATION
*
         DFHPLT TYPE=INITIAL,SUFFIX=T1
*
```

```
*  ENTRIES AHEAD OF DFHDELIM ARE EXECUTED IN FIRST PASS OF PLTPSD
*  DURING THE FIRST PHASE OF CICS SYSTEM TERMINATION
*
       DFHPLT TYPE=ENTRY,PROGRAM=AUVPLTPS
*
       DFHPLT TYPE=ENTRY,PROGRAM=DFHDELIM
*
*  ENTRIES AFTERF DFHDELIM ARE EXECUTED IN SECOND PASS OF PLTSD
*  DURING THE SECOND PHASE OF CICS SYSTEM TERMINATION
*
*
        DFHPLT TYPE=FINAL
*
        END
```

- **Using CICS system initialization parameters**
  If you created program initialization and termination program list tables to use with IBM Guardium S-TAP for Data Sets, they must be referenced in the CICS system initialization parameters PLTPI and PLTSD.

Parent topic: CICS Transaction Server support

Using CICS system initialization parameters

If you created program initialization and termination program list tables to use with IBM Guardium S-TAP for Data Sets, they must be referenced in the CICS® system initialization parameters PLTPI and PLTSD.

- The suffix of the table that was created as the program initialization PLT must be referenced in the PLTPI parameter.
- The suffix of the table that was created as the program termination PLT must be referenced in the PLTSD parameter.

Here is a sample set of system initialization parameters that specifies the PLTPI and PLTSD suffixes:

```
AICONS=YES,
XRF=NO,
AUXTR=OFF,
AUXTRSW=NO,
APPLID=CICSSYSA,
FCT=NO,
    ...
PLTPI=I1,
PLTSD=T1,
    ...
SYSIDNT=SYSA
```

Parent topic: Configuring CICS Transaction Server support

Configuring CICS signon reporting

IBM Guardium S-TAP for Data Sets can identify the CICS® signon that was used for a specific file access event. Configure the product to enable the agent to send the CICS signon information to the Guardium system.

About this task

Remember: CICS signon records do not indicate a security failure. They are an indication that the identified user successfully accessed the named file or data set.
By default, IBM Guardium S-TAP for Data Sets reports only the CICS address SAF user ID for data set level events and failed security violations. However, for RACF® environments, both CICS and RACF can be configured for the S-TAP agent to report all of the following:

- the CICS signon
- the file or data set name that was accessed
- the access context (ALTER, CONTROL, UPDATE, or READ)

Note:

- Implementation of this facility requires changes to both CICS and RACF. After implementation, the resulting change to SMF type 80 processing results in the SMF80USR field containing the CICS signon for specific file accesses. Consult your CICS and RACF security administrator when considering the implementation of this facility.
- This facility does not report the data set activity, only the security level for the requested access event.
- The following steps are also documented in the *RACF Security Guide*. For more information, see the CICS Transaction Server for z/OS® RACF Security Guide.

To implement security for files managed by the CICS file control:

Procedure

1. Specify `RESSEC(YES)` in the CSD resource definition of the transactions that access the files.
2. Using the CICS file names for identification, define the profiles to RACF in the FCICSFCT or HCICSFCT resource classes, or their equivalent if you have a user-defined resource class names.
   a. For example, use the following commands to define files in the FCICSFCT class, and authorize users to read from or write to the files:

```
RDEFINE FCICSFCT (file1, file2, .., filen)
                UACC(NONE) NOTIFY(sys_admin_userid)
PERMIT file1 CLASS(FCICSFCT)
                ID(group1, group2) ACCESS(UPDATE)
PERMIT file2 CLASS(FCICSFCT)
                ID(group1, group2) ACCESS(READ)
```

3. To define files as members of a profile in the CICS file resource group class with an appropriate access list, use the following commands:

```
RDEFINE HCICSFCT (file_groupname)
                UACC(NONE) ADDMEM(filea, fileb, .., filez)
                NOTIFY(sys_admin_userid)
PERMIT file_groupname
                CLASS(HCICSFCT)
                ID(group_userid) ACCESS(UPDATE)
```

4. Specify `SEC=YES` as a CICS system initialization parameter, or `SECPRFX` if you define profiles with a prefix.
5. Specify `XFCT=YES` for the default resource class names of FCICSFCT and HCICSFCT, or XFCT=class_name for user-defined resource class names.

Results

RACF SMF type 80 records contain the CICS user signon in the SMF80USR field. The data is reported to the Guardium system records User ID field.
Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

Starting the product

Start IBM Guardium S-TAP for Data Sets before starting products that perform similar functions.

Product initialization errors might occur if other products, which are known to intercept processing at the point of open, close, or record management functions for VSAM data sets, are started before IBM Guardium S-TAP for Data Sets. Message AUV1196E will warn you of a product initialization order conflict.

If you receive this error at startup:

1. Shut down IBM Guardium S-TAP for Data Sets and any similar products, including the previous version of this product
2. Close any data sets that are open under IBM Guardium S-TAP for Data Sets.
3. Start IBM Guardium S-TAP for Data Sets before starting similar products. IBM Guardium S-TAP for Data Sets must be running before CICS is started.

- **Starting and stopping the agent started task**
  Follow these steps to start and stop the IBM Guardium S-TAP for Data Sets agent started task.

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

Starting and stopping the agent started task

Follow these steps to start and stop the IBM Guardium S-TAP for Data Sets agent started task.

1. Start the agent started task by issuing the START command from the operator console, for example: START AUVSTAPV
2. Stop the agent started task by issuing the STOP command from the operator console, for example: STOP AUVSTAPV

You can configure the agent started task to start automatically during the z/OS® initial program load (IPL). To set automatic startup, add the appropriate command to the COMMNDxx member in SYS1.PARMLIB, or contact your system administrator.
Parent topic: Starting the product

Sample library members

The following sample library members are included for your use in installing and configuring IBM Guardium S-TAP for Data Sets. The following table lists them by type and description.

Table 1. Sample library members, types, and descriptions

Member	Type	Description
AUVCSDUP	JCL	Sample JCL to create CICS resource definition lists, groups, and program definitions with the CICS DFHCSDUP utility.
AUVJCNTL	JCL	Sample JCL to allocate and initially populate the control data set.
AUVJIVP	JCL	Sample JCL to verify installation.
AUVJSTC	JCL	Sample PROC to start the IBM Guardium S-TAP for Data Sets agent address space.
AUVSOPTS	Data	Initial data used to populate the control data set OPTIONS member.
AUVSRDEF	Data	Initial data used to populate the control data set RULEDEFS and RULEDEFB members.

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

Verifying the installation

After you install and configure the IBM® Guardium® S-TAP® for Data Sets agent, verify that the agent is properly installed. Use the JCL that is provided in the AUVJIVP member of the SAUVSAMP sample library.

Before you begin

Before you begin, complete all required tasks for Configuring the IBM Guardium S-TAP for Data Sets agent.

Procedure

1. You must install a policy on the IBM Guardium system with the characteristics listed below. Remember to replace <HLQ> with a valid high-level qualifier.

```
Job Name.....: AUVJIVP
Data Set Name: <HLQ>.AUVIVP.%%
DB Type......: DATA SET COLLECTION PROFILE
Data Set Type: ALL
```

```
Data Set Event: ALL
Actions......: z/OS AUDIT
```

Note: To see specific records on the IBM Guardium system, you might need to install a policy on the appliance in the first position that specifies Actions: LOG FULL DETAILS WITH VALUES.

2. Create a query on the IBM Guardium system that will report the events received from IBM Guardium S-TAP for Data Sets. Query characteristics are as follows:

```
Domain........: Access
Main Entity...: FULL SQL
Recommended Fields: IMS/DATA SET Event time
IMS/DATA SET Job Name
IMS/DATA SET Step Name
IMS/DATA SET Program Name
IMS/DATA SET Previous DSN
IMS/DATA SET Set Type
IMS/DATA SET Context
```

3. Start the IBM Guardium S-TAP for Data Sets started task.
4. Verify that the required SMF record types are enabled. Message AUV1450W in the Data Sets agent JESMSGLG log will alert you if any SMF record types are not defined.
5. Verify that the IBM Guardium S-TAP for Data Sets agent is connected to the intended appliance. Message AUV2182I in the Data Sets agent JESMSGLG log indicates a successful connection between the agent and the appliance.
6. Make the following modifications to the installation verification JCL in SAUVSAMP member AUVJIVP:
   a. Add a valid job card.
   b. Replace all occurrences of <HLQ> with the same high-level qualifier that was used in the policy as described in Step 1.
7. Submit the modified JCL in SAUVSAMP member AUVJIVP.

Results

Verify that the following data sets contexts appear on the appliance:

Table 1. Data set contexts for installation verification

Step	Description	Data set contexts
GENDATA	Generate input data for subsequent job steps	None
VSAM	Define, load, rename and delete ESDS, KSDS, and RRDS data sets	DATA SET ALTER DATA SET CLOSE DATA SET CREATE DATA SET DELETE DATA SET OPEN DATA SET RENAME DATA SET UPDATE
PDS	Create a PDS and write to a new PDS member	DATA SET CLOSE DATA SET CREATE Member Add
PDSCOPY	Copy a PDS member to another PDS member	DATA SET CLOSE Member Add
PDSREPL	Copy over an existing PDS member	DATA SET CLOSE Member Replace
PDSTEST	Rename a PDS member, create an alias, delete all PDS members, rename the PDS, and delete the PDS	DATA SET CLOSE DATA SET DELETE DATA SET RENAME Member Add Member Delete Member Rename STOW Initialize

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

IBM Guardium S-TAP for Data Sets administration

You must configure the Guardium system to communicate with the IBM Guardium S-TAP for Data Sets agent.

- **Communicating with the Guardium system**
  The Guardium system and the S-TAP for Data Sets agent need to communicate policy rules and collected data by using a TCP/IP connection. For the IBM Guardium S-TAP for Data Sets to communicate with the Guardium system, the following conditions must be met:
- **Communicating with the IBM Guardium S-TAP for Data Sets started task**
  IBM Guardium S-TAP for Data Sets operator commands enable authorized users to perform selected operations. Several types of operator commands can be used to display the status of IBM Guardium S-TAP for Data Sets, to enable and disable certain functions, and to dynamically alter processing without stopping or quiescing the product.

- **Data collection**
  IBM Guardium S-TAP for Data Sets collects data from multiple sources. This section describes the data collection process, as well as filtering stages and their performance impacts.
- **Record level and SMF data set monitoring options**
  You can reduce z/OS CPU and storage usage by setting options for Record level and SMF data set monitoring.
- **Policy pushdown**
  Policy pushdown is a method of controlling the data that is collected by the IBM Guardium S-TAP for Data Sets agent. Policy pushdown enables the agent to evaluate the filtering criteria that you specified.
- **Data set collection filtering parameters**
  Use the following filtering parameters to collect data set event data.
- **CICS collection filtering parameters**
  Use the following filtering parameters to collect transaction data from CICS®.

Parent topic: IBM Security Guardium S-TAP for Data Sets on z/OS

Communicating with the Guardium system

The Guardium system and the S-TAP for Data Sets agent need to communicate policy rules and collected data by using a TCP/IP connection. For the IBM Guardium S-TAP for Data Sets to communicate with the Guardium system, the following conditions must be met:

- The IBM Guardium S-TAP for Data Sets TCP/IP connection must be configured.
- At least one agent per z/OS® image must be specified. When you are configuring an agent instance:
  - Specify the host name or IP address on which the Guardium system is running. This value is specified by the APPLIANCE_SERVER element in the agent configuration file. The complete name of this CONTROL member is OPTIONS.

  When the agent is started, it uses the specified configuration information to connect to the Guardium system.

- **Streaming audit data to multiple systems**
  Multistream mode enables S-TAP audit events to be sent to multiple connected appliances. You can enable multistreaming to up to 6 Guardium appliances (APPLIANCE_SERVER + APPLIANCE_SERVER_*n*, where *n* can be 1 - 5).
- **Keeping connections active when HOT_FAILOVER is enabled**
  When the *HOT_FAILOVER* feature is enabled by the APPLIANCE_SERVER_LIST parameter, each connected Guardium appliance is kept active via pings.

Parent topic: IBM Guardium S-TAP for Data Sets administration

Streaming audit data to multiple systems

Multistream mode enables S-TAP audit events to be sent to multiple connected appliances. You can enable multistreaming to up to 6 Guardium appliances (APPLIANCE_SERVER + APPLIANCE_SERVER_*n*, where *n* can be 1 - 5).

IBM Guardium S-TAP for Data Sets sends events to a single appliance until a ping occurs, or the number of records that is specified by MEGABUFFER_COUNT is reached.

To enable multistreaming, you must specify *MULTI_STREAM* when you configure the APPLIANCE_SERVER_LIST parameter in the OPTIONS member of the CONTROL data set. Parameters APPLIANCE_SERVER and APPLIANCE_SERVER_[1-5] specify the appliances to which you intend to stream events. The appliance that is specified by APPLIANCE_SERVER provides the policy that is used for event matching.

For more information about OPTIONS member parameters, see Specifying subsystem options.

Parent topic: Communicating with the Guardium system

Keeping connections active when HOT_FAILOVER is enabled

When the *HOT_FAILOVER* feature is enabled by the APPLIANCE_SERVER_LIST parameter, each connected Guardium appliance is kept active via pings.

If the primary appliance becomes unavailable and failover occurs, the appliance policy that was originally pushed from the primary appliance continues to be active. When all Guardium appliances are connected, the status of each appliance connection, listed in the Guardium interface, is green.

Parent topic: Communicating with the Guardium system

Communicating with the IBM Guardium S-TAP for Data Sets started task

IBM Guardium S-TAP for Data Sets operator commands enable authorized users to perform selected operations. Several types of operator commands can be used to display the status of IBM Guardium S-TAP for Data Sets, to enable and disable certain functions, and to dynamically alter processing without stopping or quiescing the product.

- **IBM Guardium S-TAP for Data Sets started task commands**
  If you are an authorized user, you can enter commands to display the status of IBM Guardium S-TAP for Data Sets enable and disable certain functions, and dynamically alter processing without shutting down or quiescing the system.

Parent topic: IBM Guardium S-TAP for Data Sets administration

IBM Guardium S-TAP for Data Sets started task commands

If you are an authorized user, you can enter commands to display the status of IBM Guardium S-TAP for Data Sets enable and disable certain functions, and dynamically alter processing without shutting down or quiescing the system.

Commands

Enter operator commands from an MVS™ operator console, or by using a facility that issues MVS commands, such as SDSF.

The command format is MODIFY*stcname*, where *stcname* is the name of the started task, followed by the DISPLAY command.

For example, for record level monitoring, you can enter: MODIFY*stcname*,DISPLAY RLM. You can also use the shorthand for MODIFY, which is F to enter F*stcname*,DISPLAY RLM.

The following table summarizes the commands for displaying monitoring status and for enabling or disabling monitoring:

Table 1. Started task commands and descriptions

Command	Description
DISPLAY RLM	Indicates whether record level monitoring is enabled or disabled
DISPLAY SMFM	Indicates whether SMF monitoring is enabled or disabled
ENABLE RLM	Enables record level monitoring
DISABLE RLM	Disables record level monitoring
ENABLE SMFM	Enables SMF monitoring
DISABLE SMFM	Disables SMF monitoring
DISPLAY STREAM	Indicates whether audit records are being sent to the appliance
DIAG	Displays diagnostic information about the agent. Also displays the counters, which record the number of SMF-based and RLM-based audit records that are created as well as the number of audit records that are sent to the appliance.

Parent topic: Communicating with the IBM Guardium S-TAP for Data Sets started task

Data collection

IBM Guardium S-TAP for Data Sets collects data from multiple sources. This section describes the data collection process, as well as filtering stages and their performance impacts.

Record level and SMF event monitoring

Event information is gathered at run time through record level and SMF event monitoring. For both record level and SMF event monitoring, the filtering options you specify can minimize overhead, and control the performance of the data collection and reporting phases of processing. IBM Guardium S-TAP for Data Sets uses the filtering criteria you define to dynamically tune its processing path for optimal performance.

With few exceptions, you can use the same filtering criteria for both record level and SMF event monitoring.

- Specify the minimal filtering criteria necessary for your policy. Filtering only on the data you require minimizes:
  - Data collection overhead
  - Event processing
  - Event reporting
  - CPU time
  - Memory usage

  Record level monitoring creates the potential for the collection and reporting of large amounts of data. When constructing a policy and specifying filtering criteria, carefully consider the potential amount of data to be collected and processed.
- In the user interface, you can specify lists of elements for some filters, and use generic characters (wildcards) to create more flexibility in your filtering criteria. Generic characters act as placeholders in the specification of a character-based operand, representative of one or more valid characters for the entity on which an operation is performed.
- The use of generic characters can reduce the total number of policy rules required, but an overly inclusive set of selected entities can ultimately reduce efficiency. Excessive use of generic characters can increase the scope of selectivity during the qualification of records for processing, and dramatically reduce efficiency and increase overhead.
- SMF event monitoring can be controlled at a higher level through the specifications in the SMFPRMxx z/OS® system PARMLIB member.

Note:

- Record level monitoring support for a data set is detected, filtered, and activated at OPEN time. Files that are open at the time of an initial or updated policy activation will not be intercepted for RLM processing unless the application permits closing and reopening the file. This is of particular importance for CICS, which typically opens files at initialization or at first-use of a file. If a policy is updated after a CICS file has already been opened, it must be closed and reopened to be eligible for RLM processing.
- Record level monitoring enables you to monitor VSAM file access based on key values. The VSAM key can contain Personally Identifying Information, such as account number, last name, or Social Security number. When the FORCE_LOG_LIMITED option is enabled, IBM Guardium S-TAP for Data Sets does not monitor any record level data. If the file is being monitored by a policy, then only file access is reported; monitoring and reporting of access to specific keys is suppressed.

Filtering stages

Both record level and SMF event monitoring are performed in stages. If a collected event does not pass the lowest filtering stage (0), further processing of that event is not performed. Otherwise, the event is reevaluated during the next stage of filter processing, and IBM Guardium S-TAP for Data Sets determines whether the event should be auditing and reporting.

Stage 0 filtering

Stage 0 filtering should only be used by advanced users. An understanding of each SMF record type is required.
Stage 0 filtering can be performed for SMF event monitoring only. Only SMF events being recorded by SMF can be monitored for processing.
SMF record types to be monitored must be defined in the SMFPRMxx z/OS System Initialization PARMLIB member. If one or more SMF record types to be monitored are not specified, data collection cannot be performed. See the *SMF record types collected by IBM Guardium S-TAP for Data Sets* section of this user's guide for

details on the record types and the associated data collected with each record type.

Stage 1 filtering

Stage 1 filtering can be performed with both record level and SMF event monitoring.
Filter out as much data as possible to achieve the best possible performance.
The filtering criteria specified in the policy associated with this level of filtering include:

- Data set name
- Data set type
- DD name
- Job name
- Job type
- Program name
- Security system user ID
- Security system group ID
- SMF system ID
- Subsystem ID
- Sysplex name
- VSAM record organization*

*VSAM record organization is only available as a filtering criterion for record level monitoring. Only key-sequenced data set (KSDS) and relative record data set (RRDS) organizations are supported.
Some of the possible filtering criteria for Stage 1 filtering include a wider scope of data than others. For example, a user ID can require a much larger subset of data for processing than a data set name requires. You can define the minimum amount of data to be monitored, collected, and reported on by including or excluding selection criteria, creating lists of elements, and specifying relational operators for most criteria.
Stage 1 filtering for record level monitoring: For record level monitoring, Stage 1 filtering occurs at OPEN time for KSDS and RRDS VSAM data sets.
Stage 1 filtering for SMF event monitoring: For SMF event monitoring, Stage 1 filtering occurs in the IBM Guardium S-TAP for Data Sets address space immediately after a monitored SMF record type is obtained by the collector, located at the SMF User Exit collection point.

Stage 2 filtering

Stage 2 filtering for record level and SMF event monitoring applies to the following event types:

- Data set open
- Data set close
- Data set create
- Data set alter
- Data set update
- Data set delete
- Data set rename
- Data set SAF alter
- Data set SAF control
- Data set SAF define
- Data set SAF read
- Data set SAF update
- Member add
- Member replace
- Member rename
- Member delete
- STOW initialize

Default or specified event types are collected and passed on to the Guardium system.
Stage 2 filtering for record level monitoring can be based on the type of logical record access as well as one or more values for the key of the VSAM data set. The types of record level access that can filtered on in Stage 2 are:

- Record insert
- Record delete
- Record update
- Record read

You can use a key value or list of key values, as well as a key range or list of key ranges, to further limit the amount and scope of data collected. The key data can be specified in normal printable characters or in hexadecimal by using the EBCDIC character set.
For key values, you can use generic characters in the specification of the keys. Only those records that pass Stage 2 filtering are collected and passed on to the Guardium system.
If CICS® support is enabled, you can filter the record level monitoring event data that is captured within a CICS transaction. CICS transaction data can be filtered by:

- CICS user ID
- CICS transaction ID
- CICS program ID
- CICS file ID
- CICS region ID
- CICS terminal ID
- CICS function code

Stage 3 filtering

Stage 3 filtering is performed by IBM Guardium S-TAP for Data Sets based on Stage 2 filtering criteria that you define. During policy pushdown and activation, an analysis of the policy filtering criteria is performed. This analysis enables prefiltering processing determinations that can be performed across the product. Stage 3 prefiltering can be very efficient in eliminating certain types of data collection, and ultimately reducing the path length through the product to provide optimal processing performance.
Examples:

- **Record level monitoring:** If no record level monitoring event types are specified in the policy, Stage 2 filtering is eliminated, which reduces overhead significantly.
- **SMF event monitoring:** The exclusion of certain SMF event monitoring types from your filtering criteria allows IBM Guardium S-TAP for Data Sets to bypass collection very early in the SMF User Exit data collection, and eliminates all downstream processing for that SMF record type.

Exclusions

IBM Guardium S-TAP for Data Sets does not collect information on the following types of activities:

On IBM Db2® subsystems
: Activity within address spaces whose STC names have the following endings:

- MSTR (example: QA1XMSTR)
- DIST (example: QA1XDIST)
- IRLM (example: QA1XIRLM)
- DBM1 (example: QA1XDBM1)

On IBM IMS subsystems
: Accesses performed by the following program names:

- DFSMVRC0
- CQSINIT0
- HWSHWS00
- IRTRRC00
- DFSRRC00
- DFSUARC0
- DSPCINT0
- DSPURI00

SMF record identification considerations

In certain cases, such as when an SMF record is generated before the issuing job is run, SMF records can have zeros in the fields that the agent uses for record identification. When this happens, the agent is unable to find a RULEDEFS match for the record by using this field or any dependent fields. To avoid data loss, the agent still sends these records to the appliance even if the policy rule is set to filter out those fields. If one or more identifying fields are empty, you can use the Guardium appliance to highlight them, for example, by marking them with a specific color. The data set audit fields that can be affected by this consideration are:

- Job name
- Job number
- Program name
- DD name
- User ID
- Group ID
- Job type
- Step name
- Step number

To optionally suppress incomplete events from being sent to the appliance, use the SUPPRESS_INCOMPLETE_EVENTS parameter as described in Specifying subsystem options.

Parent topic: IBM Guardium S-TAP for Data Sets administration

Record level and SMF data set monitoring options

You can reduce z/OS® CPU and storage usage by setting options for Record level and SMF data set monitoring.

Record level monitoring performance

During record level monitoring, data is collected when VSAM records are read or written. Record level monitoring can affect performance, TCP/IP traffic, and system load. Record level monitoring intercepts VSAM accesses at the record level, so excessive monitoring of logical record requests can result in large volumes of data being transferred to the Guardium system from the TCP/IP telecommunications link, along with a corresponding increase in CPU and storage use within z/OS. Even in a moderately-sized installation that uses VSAM files, hundreds of millions, if not billions, of logical record requests can be made to VSAM daily. Attempting to monitor and report on all VSAM requests can result in huge volumes of data that can increase system load on z/OS and data traffic on communication links.

To provide flexibility in controlling the impact of record level monitoring, policy options can be used to limit the scope of monitoring. Carefully consider these options with the goal of limiting record level monitoring to the logical record requests in specific data sets that must be monitored in your environment.

Record level monitoring filter options

You can use the record level monitoring to filter based on:

- Data set name
- Data set type
- Job name
- Job type
- Program name
- Security system user ID
- Security system group ID
- SMF system ID
- Subsystem ID
- Sysplex name
- VSAM record organization
- DD name

If CICS® support is enabled you can also filter based on:

- CICS user ID

- CICS transaction ID
- CICS program ID
- CICS file ID
- CICS region ID
- CICS terminal ID
- CICS function code

You can also limit the monitoring of records to particular keys or key ranges:

VSAM KSDS and RRDS data sets
: For KSDS data sets, the key used is defined when the data set is created through an IDCAMS DEFINE.
For RRDS data sets, the key is a relative record number within the data set.
For individual keys, a list of keys is permitted with which a comparison operator can be used. In situations where the key contains unprintable characters, you can define the keys or key ranges by using hexadecimal notation.

Limit the monitoring of record level requests by the type of logical requests, including:

- Record read events
- Update write events
- Insertions
- Deletions

Remember: Each monitored record that matches the various policy filters results in the processing, creation, and transmission of a record monitoring data element to the Guardium system. Use the Guardium system interface to establish as restrictive a set of policy filters as possible. IBM Guardium S-TAP for Data Sets dynamically tunes and minimizes processing based on the filtering criteria chosen. Effectively chosen filters allows for maximum efficiency of record level monitoring processing.

Activating record level monitoring

You must define a policy that includes rules that specify one or more of the record level request filters (reads, update writes, insertions, or deletions) in order to activate record level monitoring.

- If a policy does not contain any of these filters, no additional overhead occurs at the logical record request level.
- If a particular policy rule contains one or more of these filters, only the specific data set defined in the rule (or data sets associated with other policy filters defined in the rule) incurs any additional monitoring overhead.
- Record level monitoring is only valid for use with VSAM data sets (KSDS and RRDS only).

SMF data set monitoring performance and filtering

Use filtering criteria to limit the amount of VSAM data set monitoring to only particular events. By using policy filters, SMF data set monitoring performance is enhanced by reducing CPU usage, storage usage, and TCP/IP traffic to the Guardium system.

Filter down to each specific VSAM data set event with the following filters:

- Data Set Open
- Data Set Update
- Data Set Close
- Data Set Close (input-only)
- Data Set Close (output-only)
- Data Set Delete
- Data Set Rename
- Data Set Create
- Data Set Alter
- Data Set SAF Alter
- Data Set SAF Update
- Data Set SAF Read
- Data Set SAF Define
- Data Set SAF Control

Filter down to each specific non-VSAM data set event with the following filters:

- Data Set Close
- Data Set Close (input-only)
- Data Set Close (output-only)
- Data Set Delete
- Data Set Rename
- Data Set Create
- Data Set SAF Alter
- Data Set SAF Update
- Data Set SAF Read
- Data Set SAF Define
- Data Set SAF Control
- Member Add
- Member Delete
- Member Rename
- Member Replace
- STOW Initialize

You can achieve optimal record level monitoring and SMF data set monitoring performance when you create and use a policy that defines only those events that are required by your organization.

Parent topic: IBM Guardium S-TAP for Data Sets administration

Policy pushdown

Policy pushdown is a method of controlling the data that is collected by the IBM Guardium S-TAP for Data Sets agent. Policy pushdown enables the agent to evaluate the filtering criteria that you specified.

Evaluating a match

When the product is searching for a match for the filtering criteria that you have specified, an evaluation is performed through each data set level. Access rules are used for processing a data set, when the filtering criteria of the following access types match the data:

- Job name
- Program
- Data set name
- Data set type
- DD name
- User ID
- Group ID
- SYSPLEX
- SSID
- SYS ID
- RECORG*
- Job type

*RECORG is valid only for the processing of VSAM record level monitoring.
The following values are not used to evaluate for a match on an access rule. They are used as subfiltering criteria after a match on a data set is found:

- Key
- Key range
- Data set event
- RLM event
- CICS® user ID
- CICS transaction ID
- CICS program ID
- CICS file ID
- CICS region ID
- CICS terminal ID
- CICS function code

Multiple values are allowed in an access rule, as shown in the following example with two access rules:

```
Access Rule 1
        Rule Type = INCLUDE
        Job Name = JOBA
        Key = "111111"
        RLM Event = ALL
Access Rule 2
        Rule Type = INCLUDE
        Job Name = JOBA
        Key = "222222"
        RLM Event = ALL
```

When a match is found on Access Rule 1 for job JOBA, no further scanning of the Access Rules occurs. The keyword *Key* is not used as part of the Access Rule match. To filter on keys "111111" and "222222" for a job that is named JOBA, code the Access Rules as follows:

```
Access Rule 1
        Rule Type = INCLUDE
        Job Name = JOBA
        Key = "111111","222222"
        RLM Event = ALL
```

This rule searches for a match on the job name JOBA. If a match on JOBA is found, the RLM Event and Key values are matched.
Parent topic: IBM Guardium S-TAP for Data Sets administration

Data set collection filtering parameters

Use the following filtering parameters to collect data set event data.

All the fields are optional and most have a default behavior as described. All fields apply to both VSAM and non-VSAM monitoring, unless otherwise specified.

Rule Type
: Indicates whether this rule indicates inclusion or exclusion for events that match the criteria.
Allowed values are: INCLUDE|EXCLUDE: Include collects events that satisfy the specified criteria; exclude does not collect those events. If nothing is specified, then INCLUDE is used.

Job Type
: Indicates the type of jobs that should be considered for a match.
If nothing is specified, all types are collected. You can specify the following values, separated by a comma (,): JOB|STC|TSU|APPC|OMVS, where:

  JOB
  : Jobs

  STC

Started Task

TSU
: Time Sharing User

APPC
: Advanced Program-To-Program Communication

OMVS
: Open MVS access to non-VSAM data sets, particularly that performed by FTP

SYS ID
: Indicates the SMF System IDs to use when searching for a match.
1 - 4 character SMF System ID to match.
Can be optionally followed by a comma (,) and a relational operator. If no relational operator is provided, then EQ is assumed.
Valid wildcards are supported at any position. They are:

- Percent sign (%) for zero or more characters
- Question mark (?) for a single character match

If left blank, then all SMF System IDs are considered a match.
Examples:

SS01
: Matches events that occur on SS01

SS01,EQ
: Matches that occur on SS01

SS%,EQ
: Matches that occur on systems with SS as the first 2 characters in the SMF system ID

RECORG
: Indicates the record organization type to match.
Applies only to VSAM record level monitoring collection.
Can contain zero or more of the following values, separated by a comma (,): KSDS|RRDS, where:

KSDS
: Key-sequenced data set

RRDS
: Relative record data set

If left blank, all record organization types for record level monitoring are considered a match.
Examples:

KSDS
: Matches key-sequenced data set events

KSDS,RRDS
: Matches key-sequenced data set, and relative record data set events

User ID
: Indicates the user ID to use when searching for a match.
1 - 8 character user ID to match.
Can be optionally followed by a comma (,) and a relational operator. If no relational operator is provided, then EQ is assumed.
Wildcards are supported.
If left blank, then activities for all user IDs are considered a match.
Examples:

PDUSER01
: Matches events that are caused by user *PDUSER01*

PDUSER01,EQ
: Matches events that are caused by user *PDUSER01*

PDUSER%,EQ
: Matches events that are caused by users with the prefix *PDUSER*

SSID
: Indicates the AUV ID to use when searching for a match.
1 - 4 character AUV ID optionally followed by a comma (,) and a relational operator. If no relational operator is provided EQ is assumed.
Wildcards are supported.
If left blank, activities for all SSID are considered a match.
Examples:

AUV1
: Matches events from systems with AUV ID of AUV1

AUV1,EQ
: Matches events from systems with AUV ID of AUV1

AUV%,EQ
: Matches events from systems with AUV ID prefix of AUV

SYSPLEX
: Indicates the z/OS sysplex name to use when searching for a match.
The specific 1 - 8 character z/OS sysplex name, optionally followed by a comma (,) and a relational operator. If no relational operator is provided, EQ is assumed.
Wildcards are supported.
If left blank, then activities for all SYSPLEX are considered a match.
Examples:

SYSPLEX1
: Matches events from systems on SYSPLEX1

SYSPLEX1,EQ
Matches events from systems on SYSPLEX1
SYSPLEX%,EQ
Matches events from systems on a plex beginning with SYSPLEX

Program
Indicates the program name to use when searching for a match.
1 - 8 character program name, optionally followed by a comma (,) and a relational operator. If no relational operator is provided, EQ is assumed.
Wildcards are supported.
If left blank, activities from all programs are considered a match.
Examples:

IDCAMS
Matches events that are accessed from IDCAMS
IDCAMS,EQ
Matches events that are accessed from IDCAMS
IDCAM%,EQ
Matches events that are accessed from programs beginning with IDCAM

Group ID
Indicates the group ID to use when searching for a match.
1 - 8 character representing the security system group ID optionally followed by a comma (,) and a relational operator. If no relational operator is provided EQ is assumed.
Wildcards are supported.
If left blank, then activities from all groups are considered a match.
Examples:

GROUP1
Matches events that are caused by someone within GROUP1
GROUP1,EQ
Matches events that are caused by someone within GROUP1
GROUP%,EQ
Matches events that are caused by someone within a group ID beginning with GROUP

Data Set Name
Indicates the data set name to use when searching for a match.
1 - 44 character that represents the data set name for which activity is collected, optionally followed by the comma character (,) and a relational operator. If no relational operator is provided, EQ is assumed.
Wildcards are supported.
If left blank, all data set names are considered a match.
Examples:

HLQ1.MLQ1.LLQ1
Matches events on HLQ1.MLQ1.LLQ1
HLQ1.MLQ1.LLQ1,EQ
Matches events on HLQ1.MLQ1.LLQ1
HLQ%.MLQ%.LLQ%.EQ
Matches events with the data set name mask HLQ%.MLQ%.LLQ%
%.%%,EQ
Matches all data sets with more than one qualifier
%,EQ
Matches all data sets with one qualifier

DD Name
Indicates the DD name to use when searching for a match.
1 - 8 character DD name, optionally followed by a comma (,) and a relational operator. If no relational operator is provided, EQ is assumed.
Wildcards are supported.
If left blank, activities for all DD names are considered a match.
Examples:

PAYFILE
Matches events that are accessed by DD name *PAYFILE*
PAYFILE,EQ
Matches events that are accessed by DD name *PAYFILE*
PAYFIL%,EQ
Matches events that are accessed by DD names beginning with *PAYFIL*

Job Name
Indicates the job name to use when searching for a match.
1 - 8 character name representing the job for which activity must be collected, optionally followed by a comma (,) and a relational operator. If no relational operator is provided, EQ is assumed.
Wildcards are supported.
If left blank, then activities from all jobs are considered a match.
Examples:

AUVJOB01
Matches events that result from a job name AUVJOB01
AUVJOB01,EQ
Matches events that result from a job name AUVJOB01
AUVJOB%,EQ
Matches events that result from any job beginning with AUVJOB

Key

Indicates the keys to consider when searching for a match.
Only applies to VSAM record level monitoring collection.
One or more keys in plain text or hexadecimal format, representing the key for which to match event data during record level monitoring processing.
Multiple keys must be delimited by a comma (,) optionally followed by the comma character (,) and a relational operator. If no relational operator is provided, EQ is assumed.
Plain text keys can be 1 - 255 characters long.
Hexadecimal keys can be 2 - 510 characters long and must always have an even number of characters.
An individual key must be surrounded in double quotation marks ("").
If the key is in hexadecimal format, it must be prefixed with x' and suffixed with a single quotation mark (') . It must be placed inside double quotation marks, for example: "x'F0F0F1'"
A backslash (\) can precede any character to escape the character. For example:

`"\x'0123'"`
: Matches the plain text key "x'0123'" instead of a hexadecimal key. Both types can be supplied together.

Wildcards are supported. If a wildcard is supplied with a hexadecimal key, the wildcard must be in hexadecimal (6C for `'%'`, 6E for `'?'`).
If a provided key is greater than the actual length of the VSAM key, the key will be truncated. If the key provided is shorter than the VSAM key, it will be padded with hex zeroes.
If the Key and Key Range fields are blank, activities for all keys are considered a match.
Examples:

`"KEY01"`
: Matches record level monitoring events with a key of KEY01

`"KEY01","KEY02"`
: Matches record level monitoring events with a key of KEY01 or KEY02

`"x'F0F0'"`
: Matches record level monitoring events with a key that contains the hexadecimal value F0F0

`"x'F0F0'","x'F0F1'"`
: Matches record level monitoring events with a key that contains the hexadecimal value of F0F0 or F0F1

`"KEY01","x'F0F1'"`
: Matches record level monitoring events with a key of KEY01 or a key with the hexadecimal value of F0F1

`"KEY0%"`
: Matches record level monitoring events with a key beginning with KEY0.

`"x'F06C'″`
: Matches record level monitoring events with a key with a hexadecimal value beginning with F0

`"\x'F06C'″`
: Matches record level monitoring events with a key of x'F06C'

Key Range

Indicates the range of keys to consider when searching for a match.
Only applies to VSAM record level monitoring collection.
A pair of keys in plain text, or a pair of keys in hexadecimal, representing the range to match for record level monitoring. This must be specified as <key1>,<key2>.
A pair of keys must both be in plain text, or both be in hexadecimal. Each plain text key in a plain text key pair can be 1 - 255 characters long. Each hexadecimal key in a hexadecimal key pair can be 2 - 510 characters long and must have an even number of characters.
If the keys are in hexadecimal, they must begin with x' and end with a single quotation mark (') . All keys must be enclosed in double quotation marks.
A backslash (\) can precede any characters to escape the character.
There must be an even number of keys in this field.
All key pairs must have the smaller key in the first value and the larger key in the second value; otherwise the key pairs will be rejected.
Wildcards are not supported in this field.
If the provided key is greater than the actual length of the VSAM key, the provided key will be truncated. If the key provided is shorter than the VSAM key, it will be padded with hex zeroes.
If the Key Range and Key fields are blank, activities for all keys are considered a match.
Examples:

`"KEY01","KEY09″`
: Matches record level monitoring events where the key is between KEY01 and KEY09

`"KEY01","KEY09","KEY11","KEY19″`
: Matches record level monitoring events where the key is between KEY01 and KEY09 or between KEY11 and KEY19

`"x'F0F0'","x'F0F9'″`
: Matches record level monitoring events where the key has a hexadecimal value between F0F0 and F0F9

`"x'F0F0'","x'F0F9'","x'F1F0'","x'F1F9'"`
: Matches record level monitoring events where the key has a hexadecimal value between F0F0 and F0F9 or between F1F0 and F1F9

`"\x'F0F0'","\x'F0F9'″`
: Matches record level monitoring events where the key is between x'F0F0' and x'F0F9'

RLM Event

Indicates what type of record level monitoring events should be considered for a match.
Only applies to VSAM record level monitoring collection.
Must contain zero or more of the following values, separated by a comma (,): RINS|RDEL|RWRT|RGET|ALL|SKIP, where:

RINS
: A record insert within a data set of a supported type

RDEL
: A record delete within a data set of a supported type

RWRT
: A record level update within a record of a supported type

RGET
: A record level that is read within a data set of a supported type

`ALL`

: Returns all record level events

SKIP

Returns no record level events

If left blank, then SKIP is the default and nothing is considered a match
Examples:

RINS
: Matches record level monitoring events where the operation was a record insert

RINS,RDEL
: Matches record level monitoring events where the operation was a record insert or a record delete

Data Set Event
: Indicates what type of SMF Data Set Events should be considered for a match.
Must contain zero or more of the following values, separated by a comma (,):

`DSCLI | DSCLO | DSOP | DSCL | DSUP | DSDL | DSRN | DSCR | DSALT | DSRAL | DSRCN | DSRRD | DSRUP | DSRDF | MADD | MREP | MREN | STOWI | ALL | SKIP`

where:

DSOP
: An OPEN event against a supported data set type

DSCL
: A CLOSE event against a supported data set type

DSCLI
: A CLOSE event against a supported data set type that was opened for input

DSCLO
: A CLOSE event against a supported data sets type that was opened for output

DSUP
: An UPDATE event against a supported data set type

DSDL
: A DELETE event against a supported data set type

DSRN
: A RENAME event against a supported data set type

DSCR
: A DEFINE or NEW ALLOCATION event of a supported data set type

DSALT
: An ALTER of the attributes of a supported data set type

DSRAL
: A security facility ALTER access of a supported data set type

DSRCN
: A security facility CONTROL access of a supported data set type

DSRRD
: A security facility READ access of a supported data set type

DSRUP
: A security facility UPDATE access of a supported data set type

DSRDF
: A security facility DEFINE access of a supported data set type

MADD
: A member add event against a supported data set type

MREP
: A member replace event against a supported data set type

MREN
: A member rename event against a supported data set type

MDEL
: A member delete event against a supported data set type

STOWI
: A STOW initialize event against a supported data set type

ALL
: Returns all data set level events

SKIP
: Returns no data set level events

If left blank, ALL is the default and all types are considered a match.
Examples:

DSOP
: Matches data set events where an open occurred.

DSOP,DSCL
: Matches data set events where an open or a close occurred.

Valid relational operators are:

- EQ (Equals)
- NE (Does not equal)
- GE (Greater than or equal to)
- LE (Less than or equal to)
- GT (Greater than)
- LT (Less than)

Note:

- If you are using a relational operator with the Group of Values list, you must ensure that the operator is appended to the last field in the list, otherwise it will be treated as an additional value for that field.

- To use individual values along with those listed in the Group of Values list, the relational operator must be appended to the last field in the Group of Values list, rather than to the individual field.

String comparisons are performed in lexicographical order. Because the strings are in EBCDIC, the order is lowercase, uppercase, and then numeric. Special character positions depend on the hexadecimal value of the special character itself in relation to the other characters.

Data Set Type

Indicates the type of data sets that should be considered for a match.
Must contain zero or one of the following values:

VSAM|NONVSAM|ALL, where:

VSAM
: VSAM data sets

NONVSAM
: Non-VSAM data sets

All
: Both VSAM and non-VSAM data sets

If nothing is specified, then only VSAM data set types are collected.

Parent topic: IBM Guardium S-TAP for Data Sets administration

CICS collection filtering parameters

Use the following filtering parameters to collect transaction data from CICS®.

CICS User ID

Indicates the CICS logon user ID to use when searching for a match
1 - 8 character CICS logon user ID to match
The user ID can be followed by a comma (,) and a relational operator. If no relational operator is specified, then EQ is assumed.
Wildcards are supported.
If left blank, then activities for all CICS logon user IDs are considered a match

Examples:

CICUSR01
: Matches events that are caused by CICS logon user CICUSR01

CICUSR01,EQ
: Matches events that are caused by CICS logon user CICUSR01

CICUSR%,EQ
: Matches events that are caused by CICS logon users with the prefix CICUSR

CICS Transaction ID

Indicates the CICS transaction ID to use when searching for a match
1 - 4 character CICS transaction ID to match
The transaction ID can be followed by a comma (,) and a relational operator. If no relational operator is provided, then EQ is assumed.
Wildcards are supported.
If left blank, then activities for all CICS transaction IDs are considered a match.

Examples:

VTAP
: Matches events that occur within CICS transaction ID VTAP

VTAP,EQ
: Matches events that occur within CICS transaction ID VTAP

VT%,EQ
: Matches events that occur within CICS transaction IDs starting with the prefix VT

CICS Terminal ID

Indicates the CICS terminal ID to use when searching for a match
1 - 4 character CICS terminal ID to match
The terminal ID can be optionally followed by a comma (,) and a relational operator. If no relational operator is provided, then EQ is assumed.
Wildcards are supported.
If left blank, then activities for all CICS terminal IDs are considered a match.

Examples

VTAP
: Matches events that occur within CICS transaction ID VTAP

VTAP,EQ
: Matches events that occur within CICS transaction ID VTAP

VT%,EQ
: Matches events that occur within CICS transaction IDs starting with the prefix VT

CICS Region ID

Indicates the CICS region ID to use when searching for a match. The Region ID is defined in the CICS Transaction Server System Initialization Table parameter SYSIDNT.
1 - 4 character CICS region ID to match
The region ID can be followed by a comma (,) and a relational operator. If no relational operator is provided, then EQ is assumed.
Wildcards are supported.
If left blank, then activities for all CICS region IDs are considered a match.

Examples:

CICA
: Matches events that occur within the CICS region with an ID of CICA

CICA,EQ
: Matches events that occur within the CICS region with an ID of CICA

CIC%,EQ
: Matches events that occur within the CICS regions with a prefix of CIC

CICS Program Name
: Indicates the CICS program name to use when searching for a match.
1 - 8 character CICS program name to match.
The program name can be followed by a comma (,) and a relational operator. If no relational operator is provided, then EQ is assumed.
Wildcards are supported.
If left blank, then activities for all CICS program names are considered a match.

Examples:

PAYROLLA
: Matches events that occur under control of the program that is named PAYROLLA

PAYROLLA,EQ
: Matches events that occur under control of the program that is named PAYROLLA

PAYROLL%,EQ
: Matches events that occur under control of program names that are prefixed with PAYROLL

CICS File ID
: Indicates the CICS file ID to use when searching for a match.
1 - 8 character CICS file ID to match.
The file ID can be followed by a comma (,) and a relational operator. If no relational operator is provided, then EQ is assumed.
Wildcards are supported.
If left blank, then activities for all CICS file IDs are considered a match.

Examples:

HRKSDS01
: Matches events that occur for CICS file ID HRKSDS01

HRKSDS01,EQ
: Matches events that occur for CICS file ID HRKSDS01

HRKSDS%,EQ
: Matches events that occur for CICS file IDs prefixed with HRKSDS

CICS Function Code
: Indicates the CICS function code to use when searching for a match. The function code is defined in the CICS Transaction Server Customization Guide. Search for "File control domain exits, XFCFRIN and XFCFROUT." See the description for the XFCFROUT parameter UEP_FC_FUNCTION. The hex values for the UEP_FC_FUNCTION symbolic names are defined in the DFHUEXIT macro in the CICS SDFHMAC macro library.
Two hex characters represent the single character CICS function code.
The function code can be followed by a comma (,) and a relational operator. If no relational operator is provided, then EQ is assumed.
Wildcards are not supported.
If left blank, then all CICS function codes are considered a match.

Examples

01
: Matches events that occur with the CICS function code defined by the hex character 01

01,EQ
: Matches events that occur with the CICS function code defined by the hex character 01

Parent topic: IBM Guardium S-TAP for Data Sets administration

Reference information

This section provides IBM® Guardium® S-TAP® for Data Sets reference information.

- **Simulation mode**
  Simulation mode enables you to simulate agent processing. IBM Guardium S-TAP for Data Sets uses various z/OS MVS system services to gather audit data and move it to the agent address space. The agent address space evaluates this data according to the specified policy, and transmits the audit record to the Guardium appliance by using TCP/IP. To assess the impact on MVS processing, use the STAP_STREAM_EVENTS parameter to simulate data collection.
- **VSAM and non-VSAM data set types and events**
  IBM Guardium S-TAP for Data Sets agent performs data set and record level monitoring for VSAM and non-VSAM data sets. The data set types, as well as the type of events that IBM Guardium S-TAP for Data Sets collects, are described here.
- **SMF record types and contexts**
  SMF records are correlated to IBM Guardium S-TAP for Data Sets contexts, as shown in the following table.
- **Time-to-reporting considerations**
  Learn about the benefits, considerations, and exceptions that apply to the time-to-reporting feature.

Parent topic: IBM Security Guardium S-TAP for Data Sets on z/OS

Simulation mode

Simulation mode enables you to simulate agent processing. IBM® Guardium® S-TAP® for Data Sets uses various z/OS MVS system services to gather audit data and move it to the agent address space. The agent address space evaluates this data according to the specified policy, and transmits the audit record to the Guardium appliance by

using TCP/IP. To assess the impact on MVS processing, use the STAP_STREAM_EVENTS parameter to simulate data collection.

When STAP_STREAM_EVENTS is set to *N*, the parameter stops the agent TCP/IP data transmission process. The agent performs all data collection processes but does not send the audit record to the Guardium appliance.

The DISPLAY STREAM command display whether the TCP/IP stream of data to the appliance is enabled or disabled. Use this command to verify whether the agent is sending data to the Guardium appliance.

The DIAG command displays the number of created SMF-based records, RLM-based records, and the number of records sent to the appliance. When the agent is in simulation mode (STAP_STREAM_EVENTS=N), the SMF and RLM counters increment with each record created, but the number of records sent to the appliance remains zero. When the agent is not in simulation mode (STAP_STREAM_EVENTS=Y), all counters increment.

Parent topic: Reference information

VSAM and non-VSAM data set types and events

IBM Guardium S-TAP for Data Sets agent performs data set and record level monitoring for VSAM and non-VSAM data sets. The data set types, as well as the type of events that IBM Guardium S-TAP for Data Sets collects, are described here.

Data set level monitoring

The IBM Guardium S-TAP for Data Sets agent collects SMF data for the following data set organizations:

VSAM

ESDS
: Entry sequence data set

KSDS
: Key-sequenced data set

RRDS
: Relative record data set

VRRDS
: Variable length relative record data set

LDS
: Linear data set

Non-VSAM

PS
: Physical sequential

PO
: Partitioned organization

DA
: Direct access

PDSE
: Partitioned organization-extended

The agent audits these data set types by correlating data from a combination of SMF record types to construct one of the following audit events.

VSAM

DATA SET CREATE (DSCR)
: A DEFINE or New Allocation event of a supported data set type

DATA SET OPEN (DSOP)
: An OPEN event against a supported data set type

DATA SET CLOSE (DSCL)
: A CLOSE event against a supported data set type

DATA SET CLOSE INPUT (DSCLI)
: A CLOSE event against a supported data set type that was opened for input

DATA SET CLOSE OUTPUT (DSCLO)
: A CLOSE event against a supported data set type that was opened for output

DATA SET UPDATE (DSUP)
: An UPDATE event against a supported data set type

DATA SET RENAME (DSRN)
: A RENAME event of a supported data set type

DATA SET ALTER (DSALT)
: An ALTER of the attributes of a supported data set type

DATA SET DELETE (DSDL)
: A DELETE event of a supported data set type

Security facility DEFINE violation (DSRDF)
: A security facility DEFINE violation of a supported data set type

Security facility READ violation (DSRRD)
: A security facility READ violation of a supported data set type

Security facility UPDATE violation (DSRUP)
: A security facility UPDATE violation of a supported data set type

Security facility ALTER violation (DSRAL)
: A security facility ALTER violation of a supported data set type

Security facility CONTROL violation (DSRCN)
: A security facility CONTROL violation of a supported data set type

Non-VSAM

DATA SET CREATE (DSCR)
: A DEFINE or New Allocation event of a supported data set type
: For non-SMS data sets, a RENAME event also produces a DATA SET CREATE context record, in addition to a DATA SET RENAME context record.

DATA SET CLOSE (DSCL)
: A CLOSE event against a supported data set type

DATA SET CLOSE INPUT (DSCLI)
: A CLOSE event against a supported data set type that was opened for input

DATA SET CLOSE OUTPUT (DSCLO)
: A CLOSE event against a supported data set type that was opened for output

DATA SET DELETE (DSDL)
: A DELETE event of a supported data set type

DATA SET RENAME (DSRN)
: A RENAME event of a supported data set type

Member add (MADD)
: A member ADD event against a supported data set type

Member replace (MREP)
: A member REPLACE event against a supported data set type

Member rename (MREN)
: A member RENAME event against a supported data set type

Member delete (MDEL)
: A member DELETE event against a supported data set type

STOW initialize (STOWI)
: A STOW initialize event against a supported data set type

Security facility DEFINE violation (DSRDF)
: A security facility DEFINE violation of a supported data set type

Security facility READ violation (DSRRD)
: A security facility READ violation of a supported data set type

Security facility UPDATE violation (DSRUP)
: A security facility UPDATE violation of a supported data set type

Security facility ALTER violation (DSRAL)
: A security facility ALTER violation of a supported data set type

Security facility CONTROL violation (DSRCN)
: A security facility CONTROL violation of a supported data set type

Note: For partitioned organization data sets (PDS and PDSE) that are processed by using EXCP:

- Member additions, updates, and deletions are reported by z/OS® as updates to the base data set.
- IBM Guardium S-TAP for Data Sets reports member additions, updates, and deletions as CLOSE events with an access of OUTPUT.

Record level monitoring

The IBM Guardium S-TAP for Data Sets agent collects record access information for the following VSAM data set types:

KSDS
: Key-sequenced data set

RRDS
: Relative record data set

VRRDS
: Variable length relative record data sets

The agent audits these record level monitoring events:

RECORD INSERT
: A record insert within a data set of a supported type

RECORD DELETE
: A record delete within a data set of a supported type

RECORD READ
: A record read within a data set of a supported type

RECORD UPDATE
: A record update within a data set of a supported type

Parent topic: Reference information

SMF record types and contexts

SMF records are correlated to IBM Guardium S-TAP for Data Sets contexts, as shown in the following table.

Table 1. SMF record types, subtypes, and contexts

Record number	Record subtype	Purpose	SMF context
14		Collecting non-VSAM file activity	CLOSE (non-VSAM input)
15		Collecting non-VSAM file activity	CLOSE (non-VSAM output)
17		Collecting Delete activity	DELETE (non-VSAM)
18		Collecting Rename activity	RENAME (non-VSAM)
30	4, 5	Collecting Job/Step activity	Accounting
42	6	Collecting VSAM type information	Accounting (VSAM)
42	20	Collecting PDS/PDSE member activity	STOW initialization (PDSE directory clearing)
42	21	Collecting PDS/PDSE member activity	DELETE (PDS/PDSE member)
42	24	Collecting PDS/PDSE member activity	ADD/REPLACE (PDS/PDSE member)

Record number	Record subtype	Purpose	SMF context
42	25	Collecting PDS/PDSE member activity	RENAME (PDS/PDSE member)
60*		Collecting VVDS update activity	Data Set ALTER, Data Set CREATE
61*		Collecting DEFINE/CATLG activity	Data Set CREATE
62		Collecting VSAM file activity	OPEN (VSAM)
64		Collecting VSAM I/O statistics	CLOSE (VSAM)
65		Collecting Delete activity	DELETE (VSAM)
66*		Collecting Rename activity	RENAME, ALTER (VSAM)
80		Collecting CICS sign-on security violations	Security Violation

*For more information, see the SMF records section of the *IBM z/OS MVS System Management Facilities (SMF)* documentation, available in the IBM Knowledge Center.

Note:

- There is not a one-to-one correlation between SMF records and context events reported. If more than one SMF record is encountered within a step for a single event, then subsequent records are considered duplicates.
- Audit records for data set events are produced as they occur.
- Data Set CREATE context can appear for RENAME requests of non-SMS, non-VSAM data sets, because the RENAME process generates an SMF type 61 record.

Parent topic: Reference information

Related reference

- Configuring the SMFPRMxx parameter library member

Time-to-reporting considerations

Learn about the benefits, considerations, and exceptions that apply to the time-to-reporting feature.

IBM Guardium S-TAP for Data Sets provides faster real-time reporting for data set level events. When possible, the S-TAP agent immediately delivers data set level information to the Guardium system. The agent presents the data as it occurs, giving you up-to-the-minute results without waiting for jobs to end or SMF type 30 records to be generated.

Benefits

Immediate reporting
: No need to wait for a CICS® address space to terminate, or a TSO user logs off.

Reduced storage usage
: The agent immediately reports data set events to the Guardium system, which substantially reduces the agent storage requirement. The data set event record is complete and ready for transmission to the Guardium system as soon as z/OS® MVS™ creates the source SMF record.

Considerations

Additional event records
: A notable difference as a result of this enhancement is the appearance of data set event records that were not identified in previous versions of this product. Collecting the data set event records in preparation for the SMF type 30 record caused seemingly similar records to merge. For example, a Close event could be reported for a KSDS event, although z/OS DFSMSdfp actually records this as two separate events (one for the Cluster Data component, and one for the Cluster Index component). Improved time-to-reporting now more accurately reflects data set events.

Events Span Data Set Types
: With this feature, and the V10.0 addition of non-VSAM reporting, data set event records might span data set types. For example, when you delete a VSAM KSDS event, z/OS DFSMSdfp deletes a VSAM and a non-VSAM collection of components. Use the DS_TYPE policy filter to adjust this reporting.

Exceptions

To avoid waiting for the SMF type 30 record, the agent scans various z/OS system control blocks in the address space when z/OS is writing the data set SMF record. There are instances when these control blocks are unavailable because of the state of the address space. Before this scan is run, the agent assesses the state of the address space for compatibility. If the address space is not in a compatible state, the agent waits for the SMF type 30 record, which delays reporting of the event until the address space has terminated.

Parent topic: Reference information

Troubleshooting

Use these topics to diagnose and correct problems that you might experience with IBM Guardium S-TAP for Data Sets.

- **Messages and codes**

Parent topic: IBM Security Guardium S-TAP for Data Sets on z/OS

Messages and codes

This information documents the messages and error codes issued by IBM Guardium S-TAP for Data Sets. Messages are presented in ascending alphabetical and numerical order.

- **Error message code descriptions**

Parent topic: Troubleshooting

Error message code descriptions

IBM Guardium S-TAP for Data Sets error messages adhere to the following format: AUV*nnnx*

Where:

AUV
: Indicates that the message was issued by IBM Guardium S-TAP for Data Sets.

nnn
: Indicates the message identification number.

x
: Indicates the severity of the message:

Table 1. Error message severity codes

Severity Code	Description
A	Indicates that operator intervention is required before processing can continue.
E	Indicates that an error occurred, which might or might not require operator intervention.
I	Indicates that the message is informational only.
W	Indicates that the message is a warning to alert you to a possible error condition.

- **AUV1001I**
  RULEDEFS ACTIVATION SUCCESSFUL –*ssss*
- **AUV1002E**
  INSUFFICIENT VIRTUAL STORAGE FOR PRODUCT PROCESSING
- **AUV1003E**
  INSUFFICIENT VIRTUAL STORAGE FOR PRODUCT PROCESSING
- **AUV1004E**
  UNABLE TO LOCATE REQUIRED DDNAME - CONTROL
- **AUV1005E**
  ERROR OCCURRED DURING SWAREQ PROCESSING FOR JFCB FOR DDNAME CONTROL, RC=*rrrrrrrr*
- **AUV1006E**
  UNABLE TO LOCATE REQUIRED DDNAME - OPTIONS
- **AUV1007E**
  ERROR OCCURRED DURING SWAREQ PROCESSING FOR JFCB FOR DDNAME OPTIONS, RC=*rrrrrrrr*
- **AUV1008I**
  RULEDEFS NOT ACTIVATED –*ssss*
- **AUV1009E**
  OPEN FAILED FOR PROCESSING OPTIONS MEMBER; DEFAULT OPTIONS USED
- **AUV1012E**
  ATTACH FOR AUVMAIN FAILED, RC=*rrrrrrrr*
- **AUV1013I**
  PRODUCT TERMINATION IS COMPLETE
- **AUV1014E**
  INVALID START PARAMETERS SPECIFIED; IGNORED
- **AUV1015E**
  INVALID PARM SPECIFIED - *parm*
- **AUV1016E**
  DELIMITER "=" IS MISSING - *parm*
- **AUV1017I**
  START PARAMETER SPECIFIED - *parm*
- **AUV1018E**
  INVALID VALUE SPECIFIED FOR PARAMETER - *parm*
- **AUV1019I**
  START PARAMETER SPECIFIED - *parm*
- **AUV1020E**
  VALUE SPECIFIED FOR PARAMETER - *parm*
- **AUV1021E**
  INVALID OPTION SPECIFIED - *pppppppp*
- **AUV1022E**
  INVALID KEYWORD/DELIMITER - *pppppppp*
- **AUV1023E**
  INVALID VALUE SPECIFIED FOR OPTION - *pppppppp*
- **AUV1024I**
  PROCESSING OPTION SET - SUBSYS=*ssss*
- **AUV1025E**
  INVALID VALUE SPECIFIED FOR OPTION - SUBSYS=*ssss*
- **AUV1026I**
  PROCESSING OPTION SET - INITIAL_RULEDEF=*rrrrrrrr*
- **AUV1027E**
  INVALID VALUE SPECIFIED FOR OPTION -INITIAL_RULEDEF=*rrrrrrrr*
- **AUV1028I**
  PROCESSING OPTION SET - PORT=*nnnnn*
- **AUV1029E**
  INVALID VALUE SPECIFIED FOR OPTION - PORT=*nnnnn*
- **AUV1030I**
  PROCESSING OPTION SET – APPLIANCE_PING_RATE=*nnnnn*
- **AUV1031E**
  INVALID VALUE SPECIFIED FOR OPTION – APPLIANCE_PING_RATE=*nnnnn*

- **AUV1032I**
  PROCESSING OPTION SET – APPLIANCE_RETRY_INTERVAL=*nnnnn*
- **AUV1033E**
  VALUE SPECIFIED FOR OPTION – APPLIANCE_RETRY_INTERVAL=*nnnnn*
- **AUV1034E**
  ERROR IN NAME/TOKEN RETRIEVAL PROCESSING, RC=*rrrrrrrr*
- **AUV1035E**
  NAME/TOKEN ALREADY EXISTS, BUT TOKEN IS ZERO
- **AUV1036E**
  NAME/TOKEN ALREADY EXISTS, BUT TOKEN DOES NOT POINT TO A VALID PRODUCT BLOCK
- **AUV1038E**
  UNABLE TO OBTAIN STORAGE FOR PRODUCT CONTROL BLOCK, RC=*rrrrrrrr*
- **AUV1040E**
  ERROR IN NAME/TOKEN CREATE PROCESSING, RC=*rrrrrrrr*
- **AUV1041I**
  PRODUCT INTERCEPTS HAVE BEEN ESTABLISHED
- **AUV1042E**
  UNABLE TO OBTAIN STORAGE FOR COMMON AREA ROUTINE, RC=*rrrrrrrr*
- **AUV1043E**
  BLDL FAILED FOR *mmmmmmmm*, RC=*rrrrrrrr*
- **AUV1044E**
  UNABLE TO DETERMINE ORIGIN OF *mmmmmmmm*
- **AUV1046E**
  PRIVATE LOAD FAILED FOR *mmmmmmmm*
- **AUV1047E**
  COMMON LOAD FAILED FOR *mmmmmmmm*
- **AUV1048I**
  PROCESSING OPTION SET: APPLIANCE_CONNECT_RETRY_COUNT
- **AUV1049E**
  INVALID VALUE SPECIFIED FOR OPTION – APPLIANCE_CONNECT_RETRY_COUNT=*nnnnn*
- **AUV1050E**
  UNABLE TO ESTABLISH *NNNNNNNNNNNNNNNN* EXIT, RC=*RRRRRRRR*, RS=*SSSSSSSS*
- **AUV1052E**
  UNABLE TO DELETE *NNNNNNNNNNNNNNNN* EXIT, RC=*RRRRRRRR*, RS=*SSSSSSSS*
- **AUV1054E**
  GSSB IS NOT PRESENT
- **AUV1055E**
  GSSB CONTROL BLOCK ID IS INVALID
- **AUV1056I**
  PROCESSING OPTION SET – APPLIANCE_NETWORK_REQUEST_TIMEOUT=*nnnnn*
- **AUV1058E**
  UNABLE TO LOCATE LPDE FOR IGC0005E
- **AUV1058I**
  PROCESSING OPTION SET – APPLIANCE_SERVER=*a**
- **AUV1059E**
  INVALID VALUE SPECIFIED FOR OPTION - APPLIANCE_SERVER=*a**
- **AUV1060I**
  PROCESSING OPTION SET – AUDIT=*a**
- **AUV1061E**
  VALUE SPECIFIED FOR OPTION – AUDIT=*a**
- **AUV1062I**
  PROCESSING OPTION SET – CICS_SUPPORT=*nnnnnnn*
- **AUV1063E**
  INVALID VALUE SPECIFIED FOR OPTION – CICS_SUPPORT=*nnnnnnn*
- **AUV1064W**
  Invalid port specified for APPLIANCE_PORT. Port 16022 will be used instead.
- **AUV1065E**
  UNABLE TO LOCATE LPDE FOR IDA0192A
- **AUV1066E**
  UNABLE TO LOCATE IDA0192A
- **AUV1067E**
  PAGE SERVICE LIST EXHAUSTED FOR *xx* INTERCEPT
- **AUV1068E**
  UNABLE TO OBTAIN STORAGE FOR *xx* INTERCEPT, RC=*rrrrrrrr*
- **AUV1069E**
  UNABLE TO LOCATE IDA0200T
- **AUV1070I**
  TCP/IP STREAMING DISABLED DUE TO USER SETTING
- **AUV1073W**
  MAXIMUM ACTIVE SUBSYSTEMS EXCEEDED (1)
- **AUV1074E**
  DUPLICATE SUBSYSTEM FOUND FOR SSID=*ssss*
- **AUV1077I**
  PII DATA NOT BEING TRANSMITTED DUE TO USER SETTING
- **AUV1080E**
  ERROR IN NAME/TOKEN DELETE PROCESSING, RC=*rrrrrrrr*
- **AUV1081E**
  GETMAIN FAILED FOR JSPB VECTOR TABLE, RC=*rrrrrrrr*
- **AUV1082W**
  IEFU86 EXIT IS NOT DEFINED

- **AUV1100E**
  ACRONYM CHECK FAILED FOR GSSB
- **AUV1101E**
  INSUFFICIENT VIRTUAL STORAGE FOR PRODUCT PROCESSING
- **AUV1102E**
  ERROR OCCURRED IN CROSS-MEMORY INITIALIZATION
- **AUV1103E**
  ATTACH FOR AUVPING FAILED, RC=*rrrrrrrr -ssss*
- **AUV1105E**
  ATTACH FOR AUVSSRP FAILED, RC=*rrrrrrrr -ssss*
- **AUV1105I**
  SUBSYSTEM IS ACTIVE AND ENABLED
- **AUV1106I**
  SUBSYSTEM INITIALIZATION IS COMPLETE
- **AUV1107I**
  PRODUCT TERMINATION HAS BEEN REQUESTED
- **AUV1111E**
  UNABLE TO OBTAIN STORAGE FOR COMMON AREA ROUTINE, RC=*rrrrrrrr*
- **AUV1112E**
  BLDL FAILED FOR *mmmmmmmm*, RC=*rrrrrrrr*
- **AUV1113E**
  UNABLE TO DETERMINE ORIGIN OF *mmmmmmmm*
- **AUV1115E**
  INITIAL LOAD FAILED FOR *mmmmmmmm*
- **AUV1116E**
  DIRECTED LOAD FAILED FOR *mmmmmmmm*
- **AUV1117E**
  NON-ZERO RETURN CODE FROM SYSEVENT, RC=*rrrrrrrr -ssss*
- **AUV1122E**
  INVALID COMMAND SPECIFIED - *cccccccc -ssss*
- **AUV1123E**
  INVALID COMMAND SPECIFIED - *cccccccc -ssss*
- **AUV1123W**
  ACTIVE SUBSYSTEM DETECTED; PRODUCT-LEVEL MODULE NOT RE-INITIALIZED
- **AUV1124E**
  EXCESSIVE OPERANDS SPECIFIED FOR COMMAND - *cccccccc -ssss*
- **AUV1125E**
  INSUFFICIENT OPERANDS SPECIFIED FOR COMMAND - *cccccccc -ssss*
- **AUV1126E**
  INVALID OPERAND SPECIFIED FOR COMMAND - *cccccccc -ssss*
- **AUV1127I**
  SUBSYSTEM IS ACTIVE | INACTIVE AND ENABLED | DISABLED *-ssss*
- **AUV1128E**
  INVALID COMMAND SPECIFIED - *command*
- **AUV1129I**
  THERE ARE CURRENTLY NO SUBSYSTEMS *-ssss*
- **AUV1130I**
  SUBSYSTEM xxxx IS ACTIVE | INACTIVE AND ENABLED | DISABLED *-ssss*
- **AUV1131I**
  RULEDEFS ACTIVATED ON *mm/dd/yyyy* AT *hh:mm:ss* FROM MEMBER *mmmmmmmm -ssss*
- **AUV1132I**
  RULEDEFS NOT ACTIVATED *-ssss*
- **AUV1136I**
  PRODUCT-LEVEL TRACING IS ENABLED | DISABLED *-ssss*
- **AUV1137I**
  SUBSYSTEM-LEVEL TRACING IS ENABLED | DISABLED *-ssss*
- **AUV1138E**
  EXCESSIVE OPERANDS SPECIFIED FOR COMMAND - *cccccccc -ssss*
- **AUV1140I**
  SMF MONITORING SUCCESSFULLY ENABLED – *SSSS*
- **AUV1141I**
  SUBSYSTEM IS NOW ENABLED *-ssss*
- **AUV1142I**
  TCP/IP STREAM SUCCESSFULLY ENABLED *-ssss*
- **AUV1143I**
  SMF MONITORING SUCCESSFULLY DISABLED –*SSSS*
- **AUV1144I**
  TRACING FOR PRODUCT IS NOW ENABLED *-ssss*
- **AUV1145I**
  TRACING FOR SUBSYSTEM IS NOW ENABLED *-ssss*
- **AUV1146E**
  EXCESSIVE OPERANDS SPECIFIED FOR COMMAND - *cccccccc -ssss*
- **AUV1147I**
  TCP/IP STREAM IS *EEEEEEEE -ssss*
- **AUV1149I**
  SUBSYSTEM IS NOW DISABLED *-ssss*
- **AUV1150I**
  TCP/IP STREAM SUCCESSFULLY DISABLED *-ssss*
- **AUV1151E**
  SMF MONITORING DISABLE NOT SUCCESSFUL –*SSSS*

- **AUV1152I**
  TRACING FOR PRODUCT IS NOW DISABLED -*ssss*
- **AUV1153I**
  TRACING FOR SUBSYSTEM IS NOW DISABLED -*ssss*
- **AUV1154E**
  EXCESSIVE OPERANDS SPECIFIED FOR COMMAND - *cccccccc* -*ssss*
- **AUV1155E**
  SMF MONITORING ENABLE FAILED –*SSSS*
- **AUV1156E**
  SMF MONITORING ALREADY ENABLED –*SSSS*
- **AUV1157E**
  OPERANDS SPECIFIED FOR COMMAND - *command*
- **AUV1158E**
  SMF MONITORING ALREADY DISABLED –*SSSS*
- **AUV1175I**
  DDDDDDDD MEMBER ACTIVATION SUCCESSFUL –*SSSS*
- **AUV1176E**
  DDDDDDDD MEMBER ACTIVATION FAILED – SEE JESYSMSG FOR DETAILS –*SSSS*
- **AUV1176I**
  dddddddd MEMBER *mmmmmmmm* ACTIVATION FAILED - SEE JESYSMSG FOR DETAILS -*ssss*
- **AUV1177I**
  dddddddd MEMBER *mmmmmmmm* ACTIVATION FAILED - FAILURE CODE *cccc* -*ssss*
- **AUV1179E**
  DDDDDDDD MEMBER ACTIVATION FAILED - FAILURE CODE *CCCCCCCC* –*SSSS*
- **AUV1184E**
  COMMAND VERB NOT UNIQUE - cccccccc -ssss
- **AUV1185E**
  INVALID COMMAND SYNTAX SPECIFIED - *ssss*
- **AUV1191E**
  INVALID MODULE NAME SPECIFIED - *cccccccc*
- **AUV1192I**
  MODULE *mmmmmmmm vvvv ffffffff dddddddd ttttt*
- **AUV1193I**
  MODULE *mmmmmmmm* LOCATED AT *aaaaaaaa* (*stgloc*)
- **AUV1195E**
  ERROR OCCURRED DURING FREEMAIN FOR GPB, RC=*rrrrrrrr*
- **AUV1196E**
  UNEXPECTED VCON COUNT FOR *xx* INTERCEPT; EXPECTED=*eee*, FOUND=*fff*
- **AUV1200E**
  UNABLE TO OBTAIN VIRTUAL STORAGE FOR WORKAREA
- **AUV1202E**
  UNABLE TO OBTAIN VIRTUAL STORAGE FOR WORKAREA
- **AUV1203E**
  UNABLE TO OBTAIN VIRTUAL STORAGE FOR WORKAREA
- **AUV1204E**
  UNABLE TO OBTAIN VIRTUAL STORAGE FOR WORKAREA
- **AUV1213E**
  ERROR RETRIEVING SSRE
- **AUV1214E**
  UNEXPECTED SSRE QUEUE ERROR
- **AUV1215E**
  UNEXPECTED SSRE QUEUE ERROR
- **AUV1400I**
  RECORD LEVEL MONITORING IS *EEEEEEEE* -*SSSS*
- **AUV1401I**
  RECORD LEVEL MONITORING INTERCEPTS ARE *EEEEEEEE* -*SSSS*
- **AUV1402I**
  CURRENT POLICY *EEE* -*SSSS*
- **AUV1405I**
  RECORD LEVEL MONITORING SUCCESSFULLY ENABLED -*SSSS*
- **AUV1406W**
  RECORD LEVEL MONITORING SUCCESSFULLY ENABLED, BUT NO RLM FILTERS EXIST IN CURRENT POLICY -*SSSS*
- **AUV1408W**
  POLICY CONTAINING RECORD LEVEL MONITORING FILTERS ACTIVATED, BUT RLM IS CURRENTLY DISABLED -*SSSS*
- **AUV1410I**
  PROCESSING OPTION SET - SOCKET_CONNECT_TIMEOUT=*nnnnn*
- **AUV1411E**
  INVALID VALUE SPECIFIED FOR OPTION - SOCKET_CONNECT_TIMEOUT=*nnnnn*
- **AUV1412I**
  PROCESSING OPTION SET - OUTAGE_SPILLAREA_SIZE=*nnnnnnn*
- **AUV1413E**
  INVALID VALUE SPECIFIED FOR OPTION – OUTAGE_SPILLAREA_SIZE=*nnnnnnn*
- **AUV1414I**
  PROCESSING OPTION SET - INTERNAL_BUFFER_SIZE=*nnnnnnn*
- **AUV1415E**
  INVALID VALUE SPECIFIED FOR OPTION INTERNAL_BUFFER_SIZE=*nnnnnnn*
- **AUV1416I**
  PROCESSING OPTION SET - APPLIANCE_SERVER_FAILOVER=a*
- **AUV1417E**
  INVALID VALUE SPECIFIED FOR OPTION - *keyword*=a*

- **AUV1418I**
  PROCESSING OPTION SET - IAM_SMF_RECORD_ID = *nnn*
- **AUV1419E**
  INVALID VALUE SPECIFIED FOR OPTION - IAM_SMF_RECORD_ID = *nnn*
- **AUV1420I**
  PROCESSING OPTION SET - ACF_SMF_RECORD_ID = *nnn*
- **AUV1421E**
  INVALID VALUE SPECIFIED FOR OPTION - ACF_SMF_RECORD_ID = *nnn*
- **AUV1422I**
  PROCESSING OPTION SET - APPLIANCE_SERVER_LIST(*nnn*)
- **AUV1423E**
  INVALID VALUE SPECIFIED FOR OPTION - APPLIANCE_SERVER_LIST(*nnn*)
- **AUV1424I**
  PROCESSING OPTION SET - MEGABUFFER_COUNT =*nnnnnnn*
- **AUV1425E**
  INVALID VALUE SPECIFIED FOR OPTION MEGABUFFER_COUNT =*nnnnnnn*
- **AUV1438I**
  SMF MONITORING IS *EEEEEEEE -SSSS*
- **AUV1439I**
  SMF MONITORING EXITS ARE *EEE -SSSS*
- **AUV1450W**
  SMF RECORDING TEST FAILED, RC=*cc*, TYPE=*nnnn*, SUBSYSTEM=*ssss*
- **AUV1747E**
  SUBSYSTEM IS NOT ACTIVE OR ENABLED
- **AUV1748W**
  POLICY CONTAINING RECORD LEVEL MONITORING FILTERS ACTIVATED, BUT RLM IS CURRENTLY DISABLED -*SSSS*
- **AUV2000E**
  INSUFFICIENT VIRTUAL STORAGE FOR PRODUCT PROCESSING
- **AUV2030E**
  UNRECOGNIZED INTERCEPT ID ENCOUNTERED (*XX*)
- **AUV2040E**
  ERROR OCCURRED DURING SWAREQ PROCESSING FOR JCT, RC=*rrrrrrrr*
- **AUV2041E**
  ERROR OCCURRED DURING SWAREQ PROCESSING FOR SCT, RC=*rrrrrrrr*
- **AUV2042E**
  ERROR OCCURRED DURING SWAREQ PROCESSING FOR JMR, RC=*rrrrrrrr*
- **AUV2097I**
  JCT UNAVAILABLE FOR JSPB LOOK-UP FOR ASID *xxxx*
- **AUV2098I**
  ASID *xxxx* EXCEEDS GJVT MAX; ASVTMAXU=*xxxxxxxx*
- **AUV2104E**
  ERROR OCCURRED IN FREEMAIN OF AUVSMFX1, RC=*RRRRRRRR*
- **AUV2170I**
  ATTEMPTING TO CONNECT TO THE GUARDIUM APPLIANCE
- **AUV2171I**
  CALL TO GUARDIUM APPLIANCE SUCCESSFUL
- **AUV2172E**
  function CALL TO GUARDIUM APPLIANCE FAILED
- **AUV2173E**
  function CALL TO GUARDIUM APPLIANCE FAILED, RC = *rc* RC_STP= *rc* RS_STP= *rs* RC_GDM= *rc* RC_PB = *rc* RC_LST= *rc* RS_LST= *rs*
- **AUV2174E**
  SPILL FILE FULL, DATA LOSS MIGHT OCCUR
- **AUV2175E**
  CONNECTION LOST WITH NO SPILL FILE, DATA LOSS MIGHT OCCUR
- **AUV2176E**
  UNABLE TO OBTAIN STORAGE, DATA LOSS MIGHT OCCUR
- **AUV2177E**
  RULEDEF NOT ACTIVATED - CHECK SYSPRINT FOR REASON
- **AUV2178I**
  SPILL FILE IS *xx*% FULL
- **AUV2179E**
  UNABLE TO OBTAIN REQUESTED STORAGE FOR INTERNAL_BUFFER_SIZE: dddd. PROCESSING CONTINUES.
- **AUV2180W**
  WRITING TO SPILL FILE
- **AUV2181I**
  NO LONGER WRITING TO SPILL FILE
- **AUV2182I**
  CONNECTION ESTABLISHED TO *x*
- **AUV2183W**
  STORAGE SHORTAGE DETECTED; ONE OR MORE EVENTS NOT RECORDED
- **AUV2184W**
  STORAGE SHORTAGE RELIEVED; EVENT RECORDING RESUMED. EVENTS LOST=????????
- **AUV2185I**
  UNEXPECTED PRODUCT STATE DETECTED. ATTEMPTING RESTART.
- **AUV2186E**
  UNABLE TO RESOLVE HOST NAME *a**
- **AUV2900E**
  INVALID STORAGE REQUEST FOR CONTROL BLOCK *nnnn -ssss*
- **AUV2901E**
  INSUFFICIENT VIRTUAL STORAGE FOR CONTROL BLOCK *nnnn -ssss*

- **AUV2902E**
  ACRONYM CHECK FAILED WHILE ATTEMPTING TO FREE *nnnn*, DATA=*dddd -ssss*
- **AUV2903E**
  FAILURE OCCURRED DURING FREEMAIN FOR *nnnn -ssss*
- **AUV3000E**
  ERROR ENABLING AUVFROUT: EIBRCODE=*NNNNNNNNNNN*
- **AUV3001E**
  ERROR OBTAINING GWA ADDR: EIBRCODE=*NNNNNNNNNNN*
- **AUV3003E**
  ERROR STARTING AUVFROUT: EIBRCODE=*NNNNNNNNNNN*
- **AUV3004I**
  AUVPLTPI XFCFROUT GLOBAL USER EXIT SUCCESSFULLY ENABLED AND STARTED
- **AUV3005E**
  ERROR STOPPING AUVFROUT: EIBRCODE=*NNNNNNNNNNN*
- **AUV3006E**
  ERROR OBTAINING GWA ADDR: EIBRCODE=*NNNNNNNNNNN*
- **AUV3008E**
  ERROR DISABLING AUVFROUT: EIBRCODE=*NNNNNNNNNNN*
- **AUV3009I**
  AUVPLTPS XFCFROUT GLOBAL USER EXIT SUCCESSFULLY STOPPED AND DISABLED
- **AUV3010W**
  CICS PLTPI INSTALLED BUT CICS_SUPPORT NOT SPECIFIED IN OPTIONS

Parent topic: Messages and codes

AUV1001I RULEDEFS ACTIVATION SUCCESSFUL –*ssss*

Explanation

This message is issued to the operator console following successful activation of rule definitions using the ACTIVATE RULEDEFS operator command.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1002E INSUFFICIENT VIRTUAL STORAGE FOR PRODUCT PROCESSING

Explanation

Product initialization was unable to obtain the required above-the-line storage.

User response

Increase the amount of available above-the-line storage and attempt to restart the product. If this is not successful, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1003E INSUFFICIENT VIRTUAL STORAGE FOR PRODUCT PROCESSING

Explanation

Product initialization was unable to obtain the required below-the-line storage.

User response

Increase the amount of available below-the-line storage and attempt to restart the product. If this is not successful, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1004E UNABLE TO LOCATE REQUIRED DDNAME - CONTROL

Explanation

During product initialization, the CONTROL DD statement was unable to be located in the product started task procedure.

User response

The CONTROL DD statement is required. Add the CONTROL DD statement to the product started task procedure and retry.
Parent topic: Error message code descriptions

AUV1005E ERROR OCCURRED DURING SWAREQ PROCESSING FOR JFCB FOR DDNAME CONTROL, RC=*rrrrrrrr*

Explanation

An internal error (*rrrrrrrr*) occurred while processing the CONTROL DD statement during product initialization.

User response

Make sure that the CONTROL DD statement points to a valid partitioned data set and retry. If the error persists, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1006E UNABLE TO LOCATE REQUIRED DDNAME - OPTIONS

Explanation

During product initialization, the OPTIONS DD statement was unable to be located in the product started task procedure.

User response

The OPTIONS DD statement is required. Add the OPTIONS DD statement to the product started task procedure and retry.
Parent topic: Error message code descriptions

AUV1007E ERROR OCCURRED DURING SWAREQ PROCESSING FOR JFCB FOR DDNAME OPTIONS, RC=*rrrrrrrr*

Explanation

An internal error (*rrrrrrrr*) occurred while processing the OPTIONS DD statement during product initialization.

User response

Make sure that the OPTIONS DD statement points to a valid data set and retry. If the error persists, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1008I RULEDEFS NOT ACTIVATED –*ssss*

Explanation

This message is issued in response to the DISPLAY RULEDEFS operator command when no rule definitions have been activated.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1009E OPEN FAILED FOR PROCESSING OPTIONS MEMBER; DEFAULT OPTIONS USED

Explanation

Open processing was unsuccessful for the OPTIONS member so the default options were used.

User response

Make sure that the OPTIONS DD statement points to a valid data set and retry. If the error continues, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1012E ATTACH FOR AUVMAIN FAILED, RC=*rrrrrrrr*

Explanation

During product initialization, the startup of an internal task failed. The value *rrrrrrrr* identifies the internal error code.

User response

Examine other error messages that might have occurred at the same time as this message to aid in determining the cause of the failure. If no cause can be determined, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1013I PRODUCT TERMINATION IS COMPLETE

Explanation

This message is issued in response to the product shutdown command at completion of termination processing.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1014E INVALID START PARAMETERS SPECIFIED; IGNORED

Explanation

An invalidly constructed parameter was specified on the START command for the started task; it will be ignored.

User response

Correct the START command parameter and restart the started task.
Parent topic: Error message code descriptions

AUV1015E INVALID PARM SPECIFIED - *parm*

Explanation

An unrecognized parameter was specified on the START command for the started task where parm is the unrecognized parameter.

User response

Correct the START command parameter and restart the started task.
Parent topic: Error message code descriptions

AUV1016E DELIMITER "=" IS MISSING - *parm*

Explanation

The START parameter specified by parm requires an equal sign followed by a keyword value; no equal sign was found.

User response

Correct the START command parameter and restart the started task.
Parent topic: Error message code descriptions

AUV1017I START PARAMETER SPECIFIED - *parm*

Explanation

The TRACING START parameter specified by parm was successfully recognized and processed.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1018E INVALID VALUE SPECIFIED FOR PARAMETER - *parm*

Explanation

The TRACING START parameter keyword value for the parameter specified by *parm* was invalid.

User response

Correct the START parameter keyword value and restart the started task.
Parent topic: Error message code descriptions

AUV1019I START PARAMETER SPECIFIED - *parm*

Explanation

The KEY START parameter specified by parm was successfully recognized and processed.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1020E VALUE SPECIFIED FOR PARAMETER - *parm*

Explanation

The KEY START parameter keyword value for the parameter specified by parm was invalid.

User response

Correct the START parameter keyword value and restart the started task.
Parent topic: Error message code descriptions

AUV1021E INVALID OPTION SPECIFIED - *pppppppp*

Explanation

During product initialization, an invalid keyword was encountered when processing the subsystem options in the OPTIONS member. The value *pppppppp* is the invalid option encountered — or the value "(NONE)" if blank options were specified.

User response

Correct the specified option keyword and restart the product.
Parent topic: Error message code descriptions

AUV1022E INVALID KEYWORD/DELIMITER - *pppppppp*

Explanation

During product installation, while processing the subsystem options in the OPTIONS member, an invalid keyword or delimiter was encountered. The value *pppppppp* indicates the associated keyword.

User response

Correct the specified option keyword or delimiter and restart the product.
Parent topic: Error message code descriptions

AUV1023E INVALID VALUE SPECIFIED FOR OPTION - *pppppppp*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, a keyword was encountered with an invalid value. The value *pppppppp* indicates the option with the incorrect value.

User response

Correct the specified option keyword and restart the product.
Parent topic: Error message code descriptions

AUV1024I PROCESSING OPTION SET - SUBSYS=*ssss*

Explanation

This message is issued during product initialization to display the value (*ssss*) set for the SUBSYS keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1025E INVALID VALUE SPECIFIED FOR OPTION - SUBSYS=*ssss*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the SUBSYS option. The value *ssss* indicates the invalid value.

User response

Correct the specified option keyword and restart the product.
Parent topic: Error message code descriptions

AUV1026I PROCESSING OPTION SET - INITIAL_RULEDEF=*rrrrrrrr*

Explanation

This message is issued during product initialization to display the value (*rrrrrrrr*) specified for the INITIAL_RULEDEF keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1027E INVALID VALUE SPECIFIED FOR OPTION -INITIAL_RULEDEF=*rrrrrrrr*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the INITIAL_RULEDEF option. The value *rrrrrrrr* indicates the invalid value.

User response

Correct the specified option keyword and restart the product.
Parent topic: Error message code descriptions

AUV1028I PROCESSING OPTION SET - PORT=*nnnnn*

Explanation

This message is issued during product initialization to display the value (*nnnnn*) specified for the PORT keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1029E INVALID VALUE SPECIFIED FOR OPTION - PORT=*nnnnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the PORT option. The value *nnnnn* indicates the invalid value.

User response

Correct the specified option keyword and restart the product.
Parent topic: Error message code descriptions

AUV1030I PROCESSING OPTION SET – APPLIANCE_PING_RATE=*nnnnn*

Explanation

This message is issued during product initialization to display the value (*nnnnn*) specified for the APPLIANCE_PING_RATE keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1031E INVALID VALUE SPECIFIED FOR OPTION – APPLIANCE_PING_RATE=*nnnnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the APPLIANCE_PING_RATE option. The value *nnnnn* indicates the invalid value.

User response

Correct the specified option keyword and restart the product.

Parent topic: Error message code descriptions

AUV1032I PROCESSING OPTION SET – APPLIANCE_RETRY_INTERVAL=*nnnnn*

Explanation

This message is issued during product initialization to display the value (*nnnnn*) specified for the APPLIANCE_RETRY_INTERVAL keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1033E VALUE SPECIFIED FOR OPTION – APPLIANCE_RETRY_INTERVAL=*nnnnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the APPLIANCE_RETRY_INTERVAL option. The value *nnnnn* indicates the invalid value.

User response

Correct the specified option keyword and restart the product.
Parent topic: Error message code descriptions

AUV1034E ERROR IN NAME/TOKEN RETRIEVAL PROCESSING, RC=*rrrrrrrr*

Explanation

During product initialization, an internal system error (*rrrrrrrr*) was encountered in establishing the product.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1035E NAME/TOKEN ALREADY EXISTS, BUT TOKEN IS ZERO

Explanation

During product initialization, an internal system error was encountered in establishing the product.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1036E NAME/TOKEN ALREADY EXISTS, BUT TOKEN DOES NOT POINT TO A VALID PRODUCT BLOCK

User response

IPL the system before starting the product. If this does not resolve the problem, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1038E UNABLE TO OBTAIN STORAGE FOR PRODUCT CONTROL BLOCK, RC=*rrrrrrrr*

Explanation

During product initialization, above-the-line CSA storage was unable to be obtained a product control block as indicated by the internal return code *rrrrrrrr*.

User response

Investigate and correct the shortage of above-the-line CSA storage and restart the product. If the problem persists, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1040E ERROR IN NAME/TOKEN CREATE PROCESSING, RC=*rrrrrrrr*

Explanation

During product initialization, an internal system error (*rrrrrrrr*) was encountered in establishing the product.

User response

Please contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1041I PRODUCT INTERCEPTS HAVE BEEN ESTABLISHED

Explanation

This message is issued when all intercepts have been successfully established.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1042E UNABLE TO OBTAIN STORAGE FOR COMMON AREA ROUTINE, RC=*rrrrrrrr*

Explanation

During product initialization, above-the-line CSA storage was unable to be obtained for loading a required product routine as detailed by the internal return code *rrrrrrrr*.

User response

Investigate and correct the shortage of above-the-line CSA storage and restart the product. If the problem persists, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1043E BLDL FAILED FOR *mmmmmmmm*, RC=*rrrrrrrr*

Explanation

During product initialization, a required load module was unable to be successfully located. The value *mmmmmmmm* identifies the load module and the value *rrrrrrrr* specifies the internal return code in error.

User response

Verify that the load modules for the product are accessible either in a STEPLIB in the product started task, or in the system LINKLIST concatenation and then restart the product.
Parent topic: Error message code descriptions

AUV1044E UNABLE TO DETERMINE ORIGIN OF *mmmmmmmm*

Explanation

During product initialization while processing the product load module *mmmmmmmm* an error was encountered.

User response

Verify that the load modules for the product are accessible either in a STEPLIB in the product started task or in the system LINKLIST concatenation and restart the product.
Parent topic: Error message code descriptions

AUV1046E PRIVATE LOAD FAILED FOR *mmmmmmmm*

Explanation

During product initialization, the processing of a product load module *(mmmmmmm*) to be located in above-the-line private storage failed.

User response

Verify that the load modules for the product are accessible either in a STEPLIB in the product started task, or in the system LINKLIST concatenation and then restart the product. In addition, check the available amount of above-the-line private storage available for the product started task. After correcting the problem, restart the product. If the error cannot be determined, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1047E COMMON LOAD FAILED FOR *mmmmmmmm*

Explanation

During product initialization, the processing of a product load module (*mmmmmmm*) to be located in above-the-line common storage, failed.

User response

Verify that the load modules for the product are accessible either in a STEPLIB in the product started task, or in the system LINKLIST concatenation and then restart the product. In addition, check the available amount of above-the-line common storage available for the product started task. After correcting the problem, restart the product. If the error cannot be determined, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1048I PROCESSING OPTION SET: APPLIANCE_CONNECT_RETRY_COUNT

Explanation

This message is issued during product initialization to display the value set (*nnnnn*) specified for the APPLIANCE_CONNECT_RETRY_COUNT keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1049E INVALID VALUE SPECIFIED FOR OPTION – APPLIANCE_CONNECT_RETRY_COUNT=*nnnnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the APPLIANCE_CONNECT_RETRY_COUNT option. The value *nnnnn* indicates the invalid value.

User response

Correct the specified option keyword and restart the product.
Parent topic: Error message code descriptions

AUV1050E UNABLE TO ESTABLISH *NNNNNNNNNNNNNNN* EXIT, RC=*RRRRRRRR*, RS=*SSSSSSSS*

Explanation

During started task initialization or as a result of the ENABLE SMFEXIT1 operator command, an error was encountered attempting to establish the SMF exit named *NNNNNNNNNNNNNNN*. The return code encountered is specified by *RRRRRRRR* and the reason code is specified by *SSSSSSSS*.

This message might be caused by having more than one agent active on a single z/OS image. Only one agent per z/OS image is required.

User response

Verify that no more than one agent is active per z/OS image. If that does not resolve the error, contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1052E UNABLE TO DELETE *NNNNNNNNNNNNNNN* EXIT, RC=*RRRRRRRR*, RS=*SSSSSSSS*

Explanation

During started task termination or as a result of the DISABLE SMFEXIT1 operator command, an error was encountered attempting to delete the SMF exit named *NNNNNNNNNNNNNNN*. The return code encountered is specified by *RRRRRRRR* and the reason code is specified by *SSSSSSSS*.

User response

Contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1054E GSSB IS NOT PRESENT

Explanation

During activation of a policy RULEDEFS member, a necessary Security Guardium® S-TAP® for Data Sets control block could not be located.

User response

Ensure that the Security Guardium S-TAP for Data Sets started task has been successfully started. If no error was encountered during the initialization of the started task, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1055E GSSB CONTROL BLOCK ID IS INVALID

Explanation

During activation of a policy RULEDEFS member, a necessary Security Guardium® S-TAP® for Data Sets control block was located but it is not valid.

User response

Ensure that the Security Guardium S-TAP for Data Sets started task has been successfully started. If no error was encountered during the initialization of the started task, contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1056I PROCESSING OPTION SET – APPLIANCE_NETWORK_REQUEST_TIMEOUT=*nnnnn*

Explanation

This message is issued during product initialization to display the value (*nnnnn*) that is specified for the APPLIANCE_NETWORK_REQUEST_TIMEOUT keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1058E UNABLE TO LOCATE LPDE FOR IGC0005E

Explanation

During product initialization, a required pointer to an operating system module could not be located.

User response

Contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1058I PROCESSING OPTION SET – APPLIANCE_SERVER=*a**

Explanation

This message is issued during product initialization to display the value (*a**) specified for the APPLIANCE_SERVER keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1059E INVALID VALUE SPECIFIED FOR OPTION - APPLIANCE_SERVER=*a**

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the APPLIANCE_SERVER option. The value *a** indicates the invalid value.

User response

Correct the specified option keyword and restart the product.
Parent topic: Error message code descriptions

AUV1060I PROCESSING OPTION SET – AUDIT=*a**

Explanation

This message is issued during product initialization to display the value (*a**) specified for the AUDIT keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1061E VALUE SPECIFIED FOR OPTION – AUDIT=*a**

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the AUDIT option. The value *a** indicates the invalid value.

User response

Correct the specified option keyword and restart the product.
Parent topic: Error message code descriptions

AUV1062I PROCESSING OPTION SET – CICS_SUPPORT=*nnnnnnn*

Explanation

This message is issued during product initialization to display the value *nnnnnnn* that was specified for the CICS_SUPPORT keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1063E INVALID VALUE SPECIFIED FOR OPTION – CICS_SUPPORT=*nnnnnnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the CICS_SUPPORT option. The value *nnnnnnn* indicates the invalid value.

User response

Correct the specified option keyword and restart the product.

Parent topic: Error message code descriptions

AUV1064W Invalid port specified for APPLIANCE_PORT. Port 16022 will be used instead.

Explanation

The APPLIANCE_PORT parameter currently supports a setting of 16022 or 16023. If APPLIANCE_PORT is specified with a value other than 16022 or 16023, message AUV1064W is issued and port 16022 is used instead.

User response

Change the APPLIANCE_PORT parameter setting to one of the supported values, or remove the parameter.
Parent topic: Error message code descriptions

AUV1065E UNABLE TO LOCATE LPDE FOR IDA0192A

Explanation

During Record level monitoring initialization, a required pointer to an operating system module could not be located.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1066E UNABLE TO LOCATE IDA0192A

Explanation

During Record level monitoring initialization, a required operating system module could not be located.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1067E PAGE SERVICE LIST EXHAUSTED FOR *xx* INTERCEPT

Explanation

During Record level monitoring initialization, an unexpected internal error occurred during an attempt to establish a product intercept. The intercept, identified by *xx*, is “O1” for open-intercept one, or “C1” for close-intercept one.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1068E UNABLE TO OBTAIN STORAGE FOR *xx* INTERCEPT, RC=*rrrrrrrr*

Explanation

During Record level monitoring initialization, an error specified as *rrrrrrrr* was encountered during an attempt to obtain common storage for a product control block. The intercept, identified by *xx*, is “O1” for open-intercept one, or “C1” for close-intercept one.

User response

Investigate a potential shortage of common storage and restart the product. If the problem continues, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1069E UNABLE TO LOCATE IDA0200T

Explanation

During Record level monitoring initialization, a required operating system module could not be located.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1070I TCP/IP STREAMING DISABLED DUE TO USER SETTING

Explanation

This message indicates that the STAP_STREAM_EVENTS parameter is set to a value of `N`.

System action

The agent address space will not send data to the server. This feature is also referred to as Simulation Mode. The agent address space will perform all processing necessary to collect data consistent with the active policy.

User response

No action is required. To instruct the agent to stream data to the server, change the STAP_STREAM_EVENTS parameter value to *Y*.
Parent topic: Error message code descriptions

AUV1073W MAXIMUM ACTIVE SUBSYSTEMS EXCEEDED (1)

Explanation

The current iteration of the product being started would exceed the limit of one concurrently active subsystems on a single z/OS® system. Startup for the current iteration is terminated.

User response

If the current iteration of the product is needed, shut down one of the already active subsystems and then restart the current iteration. To display all currently active subsystems use the "`display,subsystems,all`" command.

Parent topic: Error message code descriptions

AUV1074E DUPLICATE SUBSYSTEM FOUND FOR SSID=*ssss*

Explanation

During product initialization, a duplicate product control block was encountered for the subsystem ID *ssss*.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1077I PII DATA NOT BEING TRANSMITTED DUE TO USER SETTING

Explanation

This message indicates that the FORCE_LOG_LIMITED parameter is set to a value of `Y`.

System action

When FORCE_LOG_LIMITED is set to `Y`, the S-TAP agent address space does not collect or send Personally Identifiable Identification (PII) data to the Guardium server. Record Level Monitoring (RLM) and CICS data is considered PII; therefore, it is not collected when FORCE_LOG_LIMITED is set to `Y`.

User response

No action is required. To collect and stream PII data, change the FORCE_LOG_LIMITED parameter value to `N`.
Parent topic: Error message code descriptions

AUV1080E ERROR IN NAME/TOKEN DELETE PROCESSING, RC=*rrrrrrrr*

Explanation

During product initialization, an error occurred that required product termination. During termination, an attempt was made to delete the product's NAME/TOKEN, but the NAME/TOKEN DELETE service encountered an error. *rrrrrrrr* contains the value returned in register 15.

System action

Product termination continues.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1081E GETMAIN FAILED FOR JSPB VECTOR TABLE, RC=*rrrrrrrr*

Explanation

During product initialization, the specified error *rrrrrrrr* occurred while attempting to obtain common storage for a product control block.

User response

Investigate a potential shortage of above-the-line common storage and restart the product. If the problem continues, contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1082W IEFU86 EXIT IS NOT DEFINED

Explanation

The Security Guardium® S-TAP® for Data Sets address space issues this message if it detects an inadequacy in the SMF exit definitions in z/OS V2.3 and later environments. During initialization, Security Guardium S-TAP for Data Sets verifies that the required SMF exit IEFU86 is defined to the system.

For z/OS V2.3 and later, IEFU86 must be defined in the SMFPRMxx system, at the system level of the PARMLIB member, or at the various subsystem levels for Security Guardium S-TAP for Data Sets to collect data set level auditing events.

User response

To audit data set level events, configure z/OS SMF to define the require SMF exits for the appropriate z/OS level. For more information, refer to Configuring the SMFPRMxx parameter library member.
Parent topic: Error message code descriptions

AUV1100E ACRONYM CHECK FAILED FOR GSSB

Explanation

An internal error occurred within the product during product initialization.

User response

Contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1101E INSUFFICIENT VIRTUAL STORAGE FOR PRODUCT PROCESSING

Explanation

Main task startup was unable to obtain enough above-the-line private storage to initialize.

User response

Increase the amount of above-the-line private storage. If the problem persists, contact IBM® Support.

Parent topic: Error message code descriptions

AUV1102E ERROR OCCURRED IN CROSS-MEMORY INITIALIZATION

Explanation

An internal error occurred during main task startup.

User response

Contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1103E ATTACH FOR AUVPING FAILED, RC=*rrrrrrrr -ssss*

Explanation

During initialization of the Security Guardium® S-TAP® for Data Sets started task, an error was encountered during the attach of the subtask named AUVPING for the subsystem *SSSS*. The return code encountered is specified by *RRRRRRRR*.

User response

Ensure that the STEPLIB for the started task contains all of the load modules included with Security Guardium S-TAP for Data Sets. If the STEPLIB appears to correctly contain all of the product load modules, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1105E ATTACH FOR AUVSSRP FAILED, RC=*rrrrrrrr -ssss*

Explanation

During initialization of the Security Guardium® S-TAP® for Data Sets started task, an error was encountered during the attach of the subtask named AUVSSRP for the subsystem *SSSS*. The return code encountered is specified by *RRRRRRRR*.

User response

Ensure that the STEPLIB for the started task contains all of the load modules Included with Security Guardium S-TAP for Data Sets. If the STEPLIB appears to correctly contain all of the product load modules, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1105I SUBSYSTEM IS ACTIVE AND ENABLED

Explanation

This message indicates that the main product task has successfully started and is now active.

User response

No action is required.

Parent topic: Error message code descriptions

AUV1106I SUBSYSTEM INITIALIZATION IS COMPLETE

Explanation

This message is issued when the main product task has successfully completed initialization processing.

User response

No action is required.

Parent topic: Error message code descriptions

AUV1107I PRODUCT TERMINATION HAS BEEN REQUESTED

Explanation

This message is issued when the main product task has initiated subsystem shutdown processing, either due to a command request or because of an unrecoverable error condition.

User response

No action is required if this is due to a command request. If this is due to an unrecoverable error, restart the subsystem address space. Contact IBM® Software Support if the problems persist.

Parent topic: Error message code descriptions

AUV1111E UNABLE TO OBTAIN STORAGE FOR COMMON AREA ROUTINE, RC=*rrrrrrrr*

Explanation

Product subsystem initialization was unable to obtain a sufficient amount of storage to load a required module.

User response

Check and increase the amount available above- and below-the-line storage and restart the product. If the error persists, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1112E BLDL FAILED FOR *mmmmmmmm*, RC=*rrrrrrrr*

Explanation

During product subsystem initialization, a required load module was unable to be successfully located. The value *mmmmmmmm* identifies the load module and the value *rrrrrrr* specifies the internal return code in error.

User response

Verify that the load modules for the product are accessible either in a STEPLIB in the product started task or in the system LINKLIST concatenation and then restart the product.
Parent topic: Error message code descriptions

AUV1113E UNABLE TO DETERMINE ORIGIN OF *mmmmmmmm*

Explanation

An error was encountered during product subsystem initialization while processing the product load module *mmmmmmmm*.

User response

Verify that the load modules for the product are accessible either in a STEPLIB in the product started task or in the system LINKLIST concatenation and then restart the product
Parent topic: Error message code descriptions

AUV1115E INITIAL LOAD FAILED FOR *mmmmmmmm*

Explanation

During product subsystem initialization, a required load module (*mmmmmmmm*) did not load successfully.

User response

Verify that the load modules for the product are accessible either in a STEPLIB in the product started task or in the system LINKLIST concatenation and then restart the product. In addition, check the available amount of above-the-line private storage available for the product started task. After correcting the problem restart the product. If the error cannot be determined, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1116E DIRECTED LOAD FAILED FOR *mmmmmmmm*

Explanation

During product subsystem initialization, a required load module (*mmmmmmmm*) did not load successfully.

User response

Verify that the load modules for the product are accessible either in a STEPLIB in the product started task or in the system LINKLIST concatenation and then restart the product.
Parent topic: Error message code descriptions

AUV1117E NON-ZERO RETURN CODE FROM SYSEVENT, RC=*rrrrrrrr -ssss*

Explanation

During product subsystem initialization, an error (*rrrrrrrr*) was encountered when attempting to make the product started task address space non-swappable for subsystem *ssss*.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1122E INVALID COMMAND SPECIFIED - *cccccccc -ssss*

Explanation

The product subsystem command parser received an error while processing the command (*cccccccc*) issued to the started task for subsystem ID *ssss*.

User response

Correct and re-issue the command.
Parent topic: Error message code descriptions

AUV1123E INVALID COMMAND SPECIFIED - *cccccccc -ssss*

Explanation

An invalid or null product subsystem command (*cccccccc*) was issued to the started task for subsystem ID *ssss*.

User response

Correct and re-issue the command.
Parent topic: Error message code descriptions

AUV1123W ACTIVE SUBSYSTEM DETECTED; PRODUCT-LEVEL MODULE NOT RE-INITIALIZED

Explanation

While a version of the product subsystem was active, an attempt was made to initiate the same product subsystem. The subsequent attempt to start the subsystem fails. Only one instance of the subsystem is allowed on a z/OS® image at a time.

User response

No action required. If you are attempting to initiate a new version of the subsystem, first shut down the currently executing version of the subsystem.
Parent topic: Error message code descriptions

AUV1124E EXCESSIVE OPERANDS SPECIFIED FOR COMMAND - *cccccccc -ssss*

Explanation

More operands than are allowed were specified for the DISPLAY command issued (*cccccccc*) to the product started task for subsystem ID *ssss*.

User response

Re-issue the command using the correct number of operands.
Parent topic: Error message code descriptions

AUV1125E INSUFFICIENT OPERANDS SPECIFIED FOR COMMAND - *cccccccc -ssss*

Explanation

The command entered contains fewer operands than the minimum required. The command entered is *cccccccc*. The subsystem ID is *ssss*.

User response

Re-issue the command using the correct number of operands.
Parent topic: Error message code descriptions

AUV1126E INVALID OPERAND SPECIFIED FOR COMMAND - *cccccccc -ssss*

Explanation

The command entered contains an invalid operand. The command entered is *cccccccc*. The subsystem ID is *ssss*.

User response

Correct the invalid operand and re-issue the command.
Parent topic: Error message code descriptions

AUV1127I SUBSYSTEM IS ACTIVE | INACTIVE AND ENABLED | DISABLED -*ssss*

Explanation

This message is issued in response to the DISPLAY SUBSYSTEM or DISPLAY ALL operator command and shows the ACTIVE or INACTIVE status of the product subsystem and whether or not the subsystem is ENABLED or DISABLED for the subsystem *ssss*.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1128E INVALID COMMAND SPECIFIED - *command*

Explanation

An unrecognized Security Guardium® S-TAP® for Data Sets operator command was issued to the started task where command is the unrecognized command.

User response

Issue a valid operator command to the started task.
Parent topic: Error message code descriptions

AUV1129I THERE ARE CURRENTLY NO SUBSYSTEMS -*ssss*

Explanation

This message is issued in response to the product operator command DISPLAY SUBSYSTEM ALL when no subsystems are located.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1130I SUBSYSTEM xxxx IS ACTIVE | INACTIVE AND ENABLED | DISABLED -*ssss*

Explanation

This message is issued in response to the DISPLAY SUBSYSTEM ALL operator command issued to subsystem *ssss* and shows the ACTIVE or INACTIVE status of each product subsystem as identified by *xxxx* and whether or not the subsystem is ENABLED or DISABLED.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1131I RULEDEFS ACTIVATED ON *mm/dd/yyyy* AT *hh:mm:ss* FROM MEMBER *mmmmmmmm -ssss*

Explanation

This message is issued in response to the DISPLAY RULEDEFS operator command to subsystem ID *ssss* and shows the date *mm/dd/yyyy* and time *hh:mm:ss* at which the active set of RULEDEFS was last activated as well as the member name (*mmmmmmmm*) from which they were activated.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1132I RULEDEFS NOT ACTIVATED -*ssss*

Explanation

This message is issued in response to the DISPLAY RULEDEFS operator command to subsystem ID *ssss* when no RULEDEFS were found to have been activated.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1136I PRODUCT-LEVEL TRACING IS ENABLED | DISABLED -*ssss*

Explanation

This message is issued in response to the DISPLAY TRACING operator command to subsystem ID *ssss* and shows whether or not the product tracing facility is ENABLED or DISABLED.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1137I SUBSYSTEM-LEVEL TRACING IS ENABLED | DISABLED -*ssss*

Explanation

This message is issued in response to the DISPLAY TRACING operator command to subsystem ID *ssss* and shows whether or not the subsystem tracing facility is ENABLED or DISABLED.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1138E EXCESSIVE OPERANDS SPECIFIED FOR COMMAND - *cccccccc -ssss*

Explanation

More operands than are allowed were specified for the ENABLE command issued (*cccccccc*) to the product started task for subsystem ID *ssss*.

User response

Re-issue the command using the correct number of operands.
Parent topic: Error message code descriptions

AUV1140I SMF MONITORING SUCCESSFULLY ENABLED – *SSSS*

Explanation

The ENABLE SMFM command was processed for the specified subsystem *SSSS*. The required SMF monitoring exits have been loaded and enabled.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1141I SUBSYSTEM IS NOW ENABLED -*ssss*

Explanation

This message is issued in response to the ENABLE SUBSYSTEM operator command and indicates that the subsystem *ssss* was successfully enabled.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1142I TCP/IP STREAM SUCCESSFULLY ENABLED -*ssss*

Explanation

This message is issued in response to the ENABLE INTERCEPTS operator command for subsystem *ssss* were successfully enabled.

System action

The agent address space will send data to the server in a manner that is consistent with the active policy.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1143I SMF MONITORING SUCCESSFULLY DISABLED –*SSSS*

Explanation

The DISABLE SMFM command was processed for the specified subsystem *SSSS*. The required SMF monitoring exits have been disabled and unloaded.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1144I TRACING FOR PRODUCT IS NOW ENABLED -*ssss*

Explanation

This message is issued in response to the ENABLE TRACING or ENABLE TRACING ALL operator command for subsystem ID *ssss* and indicates that product level tracing is now enabled.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1145I TRACING FOR SUBSYSTEM IS NOW ENABLED -*ssss*

Explanation

This message is issued in response to the ENABLE TRACING ALL operator command for subsystem ID *ssss* and indicates that subsystem level tracing is now enabled.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1146E EXCESSIVE OPERANDS SPECIFIED FOR COMMAND - *cccccccc -ssss*

Explanation

More operands than are allowed were specified for the DISABLE command issued (*cccccccc*) to the product started task for subsystem ID *ssss*.

User response

Re-issue the command using the correct number of operands.
Parent topic: Error message code descriptions

AUV1147I TCP/IP STREAM IS *EEEEEEEE -ssss*

Explanation

This message is issued in response to the operator command DISPLAY STREAM for subsystem *ssss*. The value *EEEEEEEE* indicates ENABLED or DISABLED.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1149I SUBSYSTEM IS NOW DISABLED -*ssss*

Explanation

This message is issued in response to the DISABLE SUBSYSTEM operator command and indicates that the subsystem *ssss* was successfully disabled.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1150I TCP/IP STREAM SUCCESSFULLY DISABLED -*ssss*

Explanation

This message is issued in response to the DISABLE STREAM operator command for subsystem *ssss*.

System action

The agent address space will not send data to the server. It will perform the steps that are necessary for data collection to be performed in a manner that is consistent with the active policy.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1151E SMF MONITORING DISABLE NOT SUCCESSFUL –*SSSS*

Explanation

The DISABLE SMFM command could not be processed for the specified subsystem *SSSS*. The SMF monitoring exits are still loaded and enabled.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1152I TRACING FOR PRODUCT IS NOW DISABLED -*ssss*

Explanation

This message is issued in response to the DISABLE TRACING or DISABLE TRACING ALL operator command for subsystem ID *ssss* and indicates that product level tracing is now disabled.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1153I TRACING FOR SUBSYSTEM IS NOW DISABLED -*ssss*

Explanation

This message is issued in response to the DISABLE TRACING ALL operator command for subsystem ID *ssss* and indicates that subsystem level tracing is now disabled.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1154E EXCESSIVE OPERANDS SPECIFIED FOR COMMAND - *cccccccc -ssss*

Explanation

More operands than are allowed were specified for the ACTIVATE command issued (*cccccccc*) to the product started task for subsystem ID *ssss*.

User response

Re-issue the command using the correct number of operands.
Parent topic: Error message code descriptions

AUV1155E SMF MONITORING ENABLE FAILED –*SSSS*

Explanation

The ENABLE SMFM command failed to process for the specified *SSSS*. The SMF monitoring exits are not loaded or enabled.

User response

Ensure that the STEPLIB for the started task contains all of the load modules required for the product. If no error can be found, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1156E SMF MONITORING ALREADY ENABLED –*SSSS*

Explanation

The ENABLE SMFM command was issued for the specified subsystem *SSSS* but the SMFEXIT1 exits are already enabled. The SMF exits are still loaded and enabled.

User response

No response is required.
Parent topic: Error message code descriptions

AUV1157E OPERANDS SPECIFIED FOR COMMAND - *command*

Explanation

An operator command as identified by command was issued to the started task for subsystem *SSSS*, but more operands were specified than are permitted for the particular command.

User response

Correct and reissue the operator command.
Parent topic: Error message code descriptions

AUV1158E SMF MONITORING ALREADY DISABLED –*SSSS*

Explanation

The DISABLE SMFM command was issued for the specified subsystem *SSSS* but the SMF monitoring exits are already disabled.

User response

No response is required.
Parent topic: Error message code descriptions

AUV1175I *DDDDDDDD* MEMBER ACTIVATION SUCCESSFUL –*SSSS*

Explanation

A policy member as identified by DDDDDDDD for subsystem SSSS was successfully activated.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1176E *DDDDDDDD* MEMBER ACTIVATION FAILED – SEE JESYSMSG FOR DETAILS –*SSSS*

Explanation

A policy member as identified by *DDDDDDDD* for subsystem *SSSS* could not be successfully activated. The JESYSMSG output data set for the started task contains details of the error(s) encountered.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1176I *dddddddd* MEMBER *mmmmmmmm* ACTIVATION FAILED - SEE JESYSMSG FOR DETAILS -*ssss*

Explanation

This message is issued in response to the ACTIVATE RULEDEFS operator command or the initial RULEDEFS activation (as indicated from the OPTIONS member for subsystem ID *ssss*) to show that the activation of the RULEDEFS from member *mmmmmmmm* was not successful due to syntax errors.

User response

Review the error messages in the JES SYSMSG output for the product started task, and then correct the errors and re-activate the RULEDEFS.
Parent topic: Error message code descriptions

AUV1177I *dddddddd* MEMBER *mmmmmmmm* ACTIVATION FAILED - FAILURE CODE *cccc -ssss*

Explanation

This message is issued in response to the ACTIVATE RULEDEFS operator command, or the initial RULEDEFS activation (as indicated from the OPTIONS member for subsystem ID *ssss)* to show that the activation of the RULEDEFS from member *mmmmmmmm* was not successful due to an internal error as denoted by *cccc*.

User response

Review any error messages in the JES SYSMSG output or the console log for the product started task to determine the possible cause of the error, then correct the errors and re-activate the RULEDEFS. If the problem persists, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1179E *DDDDDDDD* MEMBER ACTIVATION FAILED - FAILURE CODE *CCCCCCCC –SSSS*

Explanation

A policy member as identified by *DDDDDDDD* for subsystem *SSSS* could not be successfully activated. The failure code is identified by *CCCCCCCC*.

User response

Contact IBM® Technical Support.
Parent topic: Error message code descriptions

AUV1184E COMMAND VERB NOT UNIQUE - cccccccc -ssss

Explanation

More than one command exists that matches the abbreviation specified (*cccccccc*) for the command verb. The product subsystem processing the command was *ssss*.

User response

Re-issue the command, using a command verb abbreviation that more uniquely specifies the intended command.
Parent topic: Error message code descriptions

AUV1185E INVALID COMMAND SYNTAX SPECIFIED - *ssss*

Explanation

The command entered contains invalid syntax. The product subsystem processing the command was *ssss*.

User response

Review the command entered and correct the syntax.
Parent topic: Error message code descriptions

AUV1191E INVALID MODULE NAME SPECIFIED - *cccccccc*

Explanation

The command entered specifies an invalid module name. The command entered is *cccccccc*.

User response

Re-issue the command with a correct module name.
Parent topic: Error message code descriptions

AUV1192I MODULE *mmmmmmmm vvvv ffffffff dddddddd ttttt*

Explanation

Module header information is displayed, where *mmmmmmmm* is the name of the module, *vvvv* is the version, *ffffffff* is the FMID *dddddddd* is the assembly date and *ttttt* is the assembly time.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1193I MODULE *mmmmmmmm* LOCATED AT *aaaaaaaa* (*stgloc*)

Explanation

The module address (with offset if specified) is displayed, where *mmmmmmmm* is the name of the module, *aaaaaaaa* is the virtual storage address, and *stgloc* is the storage location ("PRIVATE" or "COMMON").

User response

No action is required.
Parent topic: Error message code descriptions

AUV1195E ERROR OCCURRED DURING FREEMAIN FOR GPB, RC=*rrrrrrrr*

Explanation

During initialization, the product encountered an error and determined that termination was necessary. As part of termination, an attempt was made to freemain the product control block, but the FREEMAIN service encountered an error. *rrrrrrrr* contains the value returned in register 15. Product termination continues.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1196E UNEXPECTED VCON COUNT FOR *xx* INTERCEPT; EXPECTED=*eee*, FOUND=*fff*

Explanation

While setting product intercept *xx*, An unexpected VCON count was encountered for a particular csect. The expected VCON count is *eee* and the actual VCON count is *fff*. This does not necessarily indicate a problem, but a problem is possible.

System action

An SVC memory dump is taken. Depending upon the particular intercept, product initialization might continue or terminate.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1200E UNABLE TO OBTAIN VIRTUAL STORAGE FOR WORKAREA

Explanation

A service task of the main product started task was unable to obtain the required amount of above-the-line storage.

User response

Increase the amount of above-the-line storage for the product task. If the problem persists, contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1202E UNABLE TO OBTAIN VIRTUAL STORAGE FOR WORKAREA

Explanation

A service task of the main product started task was unable to obtain the required amount of above-the-line storage.

User response

Increase the amount of above-the-line storage for the product task. If the problem persists, contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1203E UNABLE TO OBTAIN VIRTUAL STORAGE FOR WORKAREA

Explanation

A product module was unable to obtain the required amount of above-the-line virtual storage.

User response

Increase the amount of above-the-line storage for the Security Guardium® S-TAP® for Data Sets started task and restart. If the problem persists, contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1204E UNABLE TO OBTAIN VIRTUAL STORAGE FOR WORKAREA

Explanation

A service task of the main product started task was unable to obtain the required amount of above-the-line storage.

User response

Increase the amount of above-the-line storage for the Security Guardium® S-TAP® for Data Sets started task. If the problem persists, contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1213E ERROR RETRIEVING SSRE

Explanation

An internal error was encountered.

User response

Contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1214E UNEXPECTED SSRE QUEUE ERROR

Explanation

An internal error was encountered.

User response

Contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1215E UNEXPECTED SSRE QUEUE ERROR

Explanation

An internal error was encountered.

User response

Contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1400I RECORD LEVEL MONITORING IS *EEEEEEEE -SSSS*

Explanation

This message is issued in response to the Security Guardium® S-TAP® for Data Sets operator command DISPLAY RLM for subsystem *SSSS*. The value *EEEEEEEE* indicates *ENABLED* or *DISABLED*.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1401I RECORD LEVEL MONITORING INTERCEPTS ARE *EEEEEEEE* -*SSSS*

Explanation

This message is issued in response to the Security Guardium® S-TAP® for Data Sets operator command DISPLAY RLM for subsystem *SSSS*. The value *EEEEEEEE* indicates ENABLED or DISABLED.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1402I CURRENT POLICY *EEE* -*SSSS*

Explanation

This message is issued in response to the Security Guardium® S-TAP® for Data Sets operator command DISPLAY RLM for subsystem *SSSS*. The value *EEE* indicates either CONTAINS RLM FILTERS or DOES NOT CONTAIN RLM FILTERS.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1405I RECORD LEVEL MONITORING SUCCESSFULLY ENABLED -*SSSS*

Explanation

This message is issued in response to the Security Guardium® S-TAP® for Data Sets operator command ENABLE RLM for subsystem *SSSS*.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1406W RECORD LEVEL MONITORING SUCCESSFULLY ENABLED, BUT NO RLM FILTERS EXIST IN CURRENT POLICY -*SSSS*

Explanation

This message is issued in response to the Security Guardium® S-TAP® for Data Sets operator command ENABLE RLM for subsystem *SSSS*. The enable action was successful, but no filters specifying record level monitoring processing exist in the currently activated policy.

System action

Record level monitoring will not be performed.

User response

To perform record level monitoring, add record level monitoring definitions to the policy and activate it.
Parent topic: Error message code descriptions

AUV1408W POLICY CONTAINING RECORD LEVEL MONITORING FILTERS ACTIVATED, BUT RLM IS CURRENTLY DISABLED -*SSSS*

Explanation

This message is issued in response to the Security Guardium® S-TAP® for Data Sets operator command ENABLE RLM for subsystem SSSS. The policy activation containing record level monitoring filters was successful, but record level monitoring processing is currently disabled.

System action

Record level monitoring will not be performed.

User response

To perform record level monitoring, issue the ENABLE RLM command for subsystem *SSSS*.
Parent topic: Error message code descriptions

AUV1410I PROCESSING OPTION SET - SOCKET_CONNECT_TIMEOUT=*nnnnn*

Explanation

This message is issued during product initialization to display the value (nnnnn) specified for the SOCKET_CONNECT_TIMEOUT keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1411E INVALID VALUE SPECIFIED FOR OPTION - SOCKET_CONNECT_TIMEOUT=*nnnnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the SOCKET_CONNECT_TIMEOUT option. The value *nnnnn* indicates the invalid value.

User response

Correct the specified option keyword and restart.
Parent topic: Error message code descriptions

AUV1412I PROCESSING OPTION SET - OUTAGE_SPILLAREA_SIZE=*nnnnnnn*

Explanation

This message is issued during product initialization to display the value (nnnnnnn) specified for the OUTAGE_SPILLAREA_SIZE keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1413E INVALID VALUE SPECIFIED FOR OPTION – OUTAGE_SPILLAREA_SIZE=*nnnnnnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the OUTAGE_SPILLAREA_SIZE option. The value *nnnnnnn* indicates the invalid value.

User response

Correct the specified option keyword and restart.
Parent topic: Error message code descriptions

AUV1414I PROCESSING OPTION SET - INTERNAL_BUFFER_SIZE=*nnnnnnn*

Explanation

This message is issued during product initialization to display the value (*nnnnnnn*) specified for the INTERNAL_BUFFER_SIZE keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1415E INVALID VALUE SPECIFIED FOR OPTION INTERNAL_BUFFER_SIZE=*nnnnnnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the INTERNAL_BUFFER_SIZE option. The value *nnnnnn* indicates the invalid value.

User response

Correct the specified option keyword and restart.
Parent topic: Error message code descriptions

AUV1416I PROCESSING OPTION SET - APPLIANCE_SERVER_FAILOVER=a*

Explanation

This message is issued during product initialization to display the value a* specified for the APPLIANCE_SERVER_FAILOVER keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1417E INVALID VALUE SPECIFIED FOR OPTION - *keyword*=a*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the keyword. The *keyword* value indicates APPLIANCE_SERVER_FAILOVER_*n*, or its alternate specification, APPLIANCE_SERVER_*n*, where *n* is 1, 2, 3, 4, or 5. The value *a** indicates the invalid value.

User response

Correct the specified option keyword and restart.
Parent topic: Error message code descriptions

AUV1418I PROCESSING OPTION SET - IAM_SMF_RECORD_ID = *nnn*

Explanation

This message is issued during product initialization to display the value *nnn* that is specified for the IAM_SMF_RECORD_ID keyword in the OPTIONS member. This keyword identifies the SMF record ID for the IAM records.

User response

For Security Guardium® S-TAP® for Data Sets to report IAM access, specify the value *nnn* in the control data set IAM_SMF_RECORD_ID option.
Parent topic: Error message code descriptions

AUV1419E INVALID VALUE SPECIFIED FOR OPTION - IAM_SMF_RECORD_ID = *nnn*

Explanation

While processing the subsystem options in the OPTIONS member during product initialization, an incorrect value was encountered for the IAM_SMF_RECORD_ID option. The value *nnn* indicates the invalid value.

User response

Correct the specified option keyword and restart.
Parent topic: Error message code descriptions

AUV1420I PROCESSING OPTION SET - ACF_SMF_RECORD_ID = *nnn*

Explanation

This message is issued during product initialization to display the value specified for the ACF_SMF_RECORD_ID keyword in the OPTIONS member. This keyword identifies the SMF record ID for the ACF2 records.

User response

For Security Guardium® S-TAP® for Data Sets to report access failures to a unique record ID, specify the value *nnn* in the control data set ACF_SMF_RECORD_ID option.
Parent topic: Error message code descriptions

AUV1421E INVALID VALUE SPECIFIED FOR OPTION - ACF_SMF_RECORD_ID = *nnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the ACF_SMF_RECORD_ID option. The value nnn indicates the invalid value.

User response

Correct the specified option keyword and restart.
Parent topic: Error message code descriptions

AUV1422I PROCESSING OPTION SET - APPLIANCE_SERVER_LIST(*nnn*)

Explanation

This message is issued during product initialization to display the value specified for the APPLIANCE_SERVER_LIST keyword in the OPTIONS member. This value *nnn* identifies one of the following selected options:

FAILOVER
: One appliance connection is active at a time. If the connection to the primary appliance is lost, a failover action occurs, which results in an attempt to connect to the next available server. The appliance attempts to reconnect to the primary server at intervals of 12 times the PING_RATE.

MULTI_STREAM
: An appliance connection is established for each server that is listed by the APPLIANCE_SERVER_n or APPLIANCE_SERVER_FAILOVER_n parameter. When a connection is lost, Security Guardium® S-TAP® for Data Sets audit events continue to be spread over the remaining appliance connections. Any lost connections are retried at regular intervals of 12 times the PING_RATE.

HOT_FAILOVER
: Keeps each connected Guardium appliance active via pings. If the primary Guardium appliance becomes unavailable and failover occurs, *HOT_FAILOVER* maintains the activity of the primary appliance policy.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1423E INVALID VALUE SPECIFIED FOR OPTION - APPLIANCE_SERVER_LIST(*nnn*)

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the APPLIANCE_SERVER_LIST option. The value *nnn* indicates the incorrect value.

User response

Correct the specified option keyword and restart.
Parent topic: Error message code descriptions

AUV1424I PROCESSING OPTION SET - MEGABUFFER_COUNT =*nnnnnnn*

Explanation

This message is issued during product initialization to display the value (*nnnnnnn*) that is specified for the MEGABUFFER_COUNT keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1425E INVALID VALUE SPECIFIED FOR OPTION MEGABUFFER_COUNT =*nnnnnnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the MEGABUFFER_COUNT option. The value *nnnnnnn* indicates the incorrect value.

User response

Correct the specified option keyword and restart.
Parent topic: Error message code descriptions

AUV1438I SMF MONITORING IS *EEEEEEEE -SSSS*

Explanation

This message is issued in response to the Security Guardium® S-TAP® for Data Sets operator command DISPLAY SMFEXIT1 for subsystem *SSSS*. The value *EEEEEEEE* indicates *ENABLED* or *DISABLED*.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1439I SMF MONITORING EXITS ARE *EEE -SSSS*

Explanation

This message is issued in response to the Security Guardium® S-TAP® for Data Sets operator command DISPLAY SMFM for subsystem *SSSS*. The value *EEE* indicates ACTIVE/LOADED or NOT ACTIVE/LOADLED.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1450W SMF RECORDING TEST FAILED, RC=*cc*, TYPE=*nnnn*, SUBSYSTEM=*ssss*

Explanation

The Security Guardium® S-TAP® for Data Sets address space issues this message if it detects an inadequacy in the SMF environment. During initialization,Security Guardium S-TAP for Data Sets tests z/OS® MVS™ SMF to determine if SMF is collecting the record types that are necessary for data set level auditing. The S-TAP address space issues this message for each SMF record type *nnnn*, and z/OS MVS subsystem *ssss*, for which the test fails. RC *cc* identifies one of the following return codes:

16
: SMF is not active or has ended abnormally.

36
: Information for the specified record type is not being recorded.

User response

To audit data set level events, configure z/OS MVS SMF to collect the required SMF records. For more information, refer to Configuring the SMFPRMxx parameter library member.
Parent topic: Error message code descriptions

AUV1747E SUBSYSTEM IS NOT ACTIVE OR ENABLED

Explanation

This message is issued when, during the activation of a policy, the Security Guardium® S-TAP® for Data Sets subsystem is found to be disabled or inactive. The policy is not activated.

User response

Ensure that the Security Guardium S-TAP for Data Sets started task has been started and that the subsystem is enabled and the hooks are active. If the problem persists, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1748W POLICY CONTAINING RECORD LEVEL MONITORING FILTERS ACTIVATED, BUT RLM IS CURRENTLY DISABLED -*SSSS*

Explanation

This message is issued in response to the Security Guardium® S-TAP® for Data Sets policy pushdown operation for subsystem *SSSS*. The policy pushdown containing record level monitoring filters was successful, but record level monitoring processing is currently disabled.

System action

Record level monitoring will not be performed.

User response

To perform record level monitoring, issue the ENABLE RLM command for subsystem *SSSS*.
Parent topic: Error message code descriptions

AUV2000E INSUFFICIENT VIRTUAL STORAGE FOR PRODUCT PROCESSING

Explanation

During an attempt to intercept an OPEN/CLOSE event, Security Guardium® S-TAP® for Data Sets was unable to obtain enough virtual storage to perform processing.

User response

Increase the amount of virtual storage for the job. If the error persists, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2030E UNRECOGNIZED INTERCEPT ID ENCOUNTERED (*XX*)

Explanation

Security Guardium® S-TAP® for Data Sets received control with unexpected intercept parameters.

User response

This is an unexpected internal condition. If product maintenance was recently applied, ensure that all steps in the HOLDDATA were performed. If they were, record the ID *XX* and contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2040E ERROR OCCURRED DURING SWAREQ PROCESSING FOR JCT, RC=*rrrrrrrr*

Explanation

During interception of an OPEN or CLOSE event, an internal error specified as *rrrrrrrr* occurred while attempting to access a system control block.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2041E ERROR OCCURRED DURING SWAREQ PROCESSING FOR SCT, RC=*rrrrrrrr*

Explanation

During interception of an OPEN or CLOSE event, an internal error specified as *rrrrrrrr* was encountered while attempting to access a system control block.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2042E ERROR OCCURRED DURING SWAREQ PROCESSING FOR JMR, RC=*rrrrrrrr*

Explanation

During interception of an OPEN or CLOSE event, an internal error specified as *rrrrrrrr* occurred while attempting to access a system control block.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2097I JCT UNAVAILABLE FOR JSPB LOOK-UP FOR ASID *xxxx*

Explanation

During interception of an OPEN or CLOSE event, Security Guardium® S-TAP® for Data Sets was unable to locate a product control block for the address space with the ASID *xxxx*.

System action

Processing is bypassed for the current job.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2098I ASID *xxxx* EXCEEDS GJVT MAX; ASVTMAXU=*xxxxxxxx*

Explanation

During interception of an OPEN or CLOSE event, Security Guardium® S-TAP® for Data Sets detected an unexpected error for the address space with the ASID *xxxx*. The system value for ASVTMAX *xxxxxxxx* is also displayed.

System action

Processing is bypassed for the current job.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2104E ERROR OCCURRED IN FREEMAIN OF AUVSMFX1, RC=*RRRRRRRR*

Explanation

During termination processing of the Security Guardium® S-TAP® for Data Sets started task or during the DISABLE of the SMFEXIT1 exits, the storage occupied by the module AUVSMFX1 could not be successfully freed. The error code encountered is specified by *RRRRRRRR*.

User response

No noticeable effect on system operations should be noticed as, although the module is located in Extended CSA, it consumes only a few kilobytes of storage. However, the cause of the error should be investigated by contacting IBM® Software Support.
Parent topic: Error message code descriptions

AUV2170I ATTEMPTING TO CONNECT TO THE GUARDIUM APPLIANCE

Explanation

This is an informational message issued during product initialization indicating initialization progress.

User response

None required.
Parent topic: Error message code descriptions

AUV2171I CALL TO GUARDIUM APPLIANCE SUCCESSFUL

Explanation

This is an informational message issued during product initialization indicating that the z/OS® host component of successfully connected to Guardium® system.

User response

No action is required.
Parent topic: Error message code descriptions

AUV2172E *function* CALL TO GUARDIUM APPLIANCE FAILED

Explanation

An attempt to communicate with the Guardium® system failed. Before reporting the failure, the agent retried the request the number of times specified on the APPLIANCE_RETRY_INTERVAL parameter for the number of iterations specified on the APPLIANCE_CONNECT_RETRY_COUNT parameter. The *function* will be one of the following:

INIT
: Guardium system initialization, which occurs when the started task starts.

PING
: Cyclical pings to the system that report the agent's status.

SEND-SMF
: Agent transmission of the audit records to the Guardium system.

If any one of these service requests fail, the agent address space is terminated.

User response

Correct any communications issue causing this failure and restart the agent started task. Contact IBM® Software Support for further assistance.
Parent topic: Error message code descriptions

AUV2173E *function* CALL TO GUARDIUM APPLIANCE FAILED, RC = *rc* RC_STP= *rc* RS_STP= *rs* RC_GDM= *rc* RC_PB = *rc* RC_LST= *rc* RS_LST= *rs*

Explanation

An attempt to communicate with the Guardium® system failed. Before reporting the failure, the agent retried the request the number of times specified on the APPLIANCE_RETRY_INTERVAL parameter for the number of iterations specified on the APPLIANCE_CONNECT_RETRY_COUNT parameter. The function will be one of the following:

INIT
: Guardium system initialization, which occurs at started task initialization.

PING
: Cyclical pings to the system that reports the agent's status.

SEND-SMF
: Agent transmission of the audit records to the Guardium system. If any one of these service requests fail, the agent address space is terminated.

The *rc* and *rs* text is replaced with numeric values that can assist IBM® Support with problem diagnosis, if the problem persists.

User response

Correct any communications issue causing this failure and restart the agent started task. Contact IBM Support for further assistance.
Parent topic: Error message code descriptions

AUV2174E SPILL FILE FULL, DATA LOSS MIGHT OCCUR

Explanation

Connection to the Guardium® system has unexpectedly terminated and the spill file with SPILL_BUFFER size is now full. Data loss can occur if this condition continues.

User response

Ensure that the Guardium system is communicating. Increase the SPILL_BUFFER value to increase the amount of data that can be written to the spill file.
Parent topic: Error message code descriptions

AUV2175E CONNECTION LOST WITH NO SPILL FILE, DATA LOSS MIGHT OCCUR

Explanation

The connection to the Guardium® system has unexpectedly terminated. SPILL_BUFFER was not specified in the configuration member.

User response

Determine the cause of the network interruption and correct the problem so that the connection can be re-established. To minimize data loss, specify a SPILL_BUFFER.
Parent topic: Error message code descriptions

AUV2176E UNABLE TO OBTAIN STORAGE, DATA LOSS MIGHT OCCUR

Explanation

An attempt to allocate storage for additional data failed.

User response

Ensure that a sufficient region size is provided in the started task JCL.
Parent topic: Error message code descriptions

AUV2177E RULEDEF NOT ACTIVATED - CHECK SYSPRINT FOR REASON

Explanation

An attempt to process a policy pushdown failed. No RULEDEF was activated as a result.

User response

Check the SYSPRINT for the detailed reason on what caused the failure. Correct the issue, and reissue a policy pushdown.
Parent topic: Error message code descriptions

AUV2178I SPILL FILE IS *xx*% FULL

Explanation

This message is issued while the spill file is in use. It indicates that the spill file has been filled to the percentage indicated.

User response

No action is required.
Parent topic: Error message code descriptions

AUV2179E UNABLE TO OBTAIN REQUESTED STORAGE FOR INTERNAL_BUFFER_SIZE: dddd. PROCESSING CONTINUES.

Explanation

An attempt to allocate storage for the internal buffer has failed. The started task remains up, but data processing does not run as efficiently.

User response

Ensure that a sufficient region size is provided in the started task JCL, or decrease the amount specified for INTERNAL_BUFFER_SIZE in the OPTIONS member. If the problem persists, contact IBM Software Support.
Parent topic: Error message code descriptions

AUV2180W WRITING TO SPILL FILE

Explanation

The connection to the Guardium system has been lost. All data is now being written to a spill file. The data in the spill file will be written to the Guardium system when the connection is restored.

User response

Determine the cause of the network interruption and correct the problem so that the connection can be re-established.
Parent topic: Error message code descriptions

AUV2181I NO LONGER WRITING TO SPILL FILE

Explanation

The connection to the Guardium system has been restored, and the agent is no longer writing to the spill file.

User response

No action is required.
Parent topic: Error message code descriptions

AUV2182I CONNECTION ESTABLISHED TO *x*

Explanation

An attempt to connect to the Guardium system was successful, where *x* is the system with which a connection has been made.

User response

No action is required.
Parent topic: Error message code descriptions

AUV2183W STORAGE SHORTAGE DETECTED; ONE OR MORE EVENTS NOT RECORDED

Explanation

An attempt to allocate virtual storage for an internal product control block failed. Without the control block, the data for the event cannot be captured.

User response

Ensure that a sufficient region size is provided in the started task JCL. A region size of at least 96M is recommended when a large number of events are being monitored.

If the problem persists, evaluate the amount of data that is being captured as defined by the policy. Monitoring a very large number of events can cause storage shortages, especially when Record Level Monitoring (RLM) is being used.

Parent topic: Error message code descriptions

AUV2184W STORAGE SHORTAGE RELIEVED; EVENT RECORDING RESUMED. EVENTS LOST=????????

Explanation

A previous virtual storage shortage was resolved, allowing event recording to be resumed. EVENTS LOST=*????????* indicates the number of events that could not be recorded.

User response

No action is required.
Parent topic: Error message code descriptions

AUV2185I UNEXPECTED PRODUCT STATE DETECTED. ATTEMPTING RESTART.

Explanation

Indicators in product control blocks conflict with the current product state. This could be caused by a non-standard product shutdown or an unexpected product termination. The product will attempt to correct the environment and continue to re-initialize.

User response

No action is required.
Parent topic: Error message code descriptions

AUV2186E UNABLE TO RESOLVE HOST NAME *a**

Explanation

During product initialization, one of the host names (*a**) specified for the APPLIANCE_SERVER or APPLIANCE_SERVER_n option could not be resolved to a valid IP address.

User response

Ensure that all the host names specified in the OPTIONS member are correct and can be resolved to IP addresses. Correct the configuration if needed and restart.
Parent topic: Error message code descriptions

AUV2900E INVALID STORAGE REQUEST FOR CONTROL BLOCK *nnnn -ssss*

Explanation

An internal error occurred while attempting to obtain a control block identified by *nnnn* subsystem ID *ssss*.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2901E INSUFFICIENT VIRTUAL STORAGE FOR CONTROL BLOCK *nnnn -ssss*

Explanation

Sufficient storage was not available to obtain a required control block identified by *nnnn* subsystem ID *ssss*.

User response

Attempt to increase above-the-line or below-the-line storage for the job receiving the error message. If the error persists, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2902E ACRONYM CHECK FAILED WHILE ATTEMPTING TO FREE *nnnn*, DATA=*dddd -ssss*

Explanation

An internal error occurred while attempting to free a control block identified by *nnnn* with the invalid data identified by *dddd* for subsystem ID *ssss*.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2903E FAILURE OCCURRED DURING FREEMAIN FOR *nnnn -ssss*

Explanation

An internal error occurred while attempting to free a control block identified by *nnnn* subsystem ID *ssss*.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV3000E ERROR ENABLING AUVFROUT: EIBRCODE=*NNNNNNNNNNNN*

Explanation

While running the Program List Table Program Initialization module AUVPLTPI, an error was encountered attempting to enable the XFCFROUT Global User Exit program AUVFROUT. The value *NNNNNNNNNNNN* represents the EXEC Interface Block error and response codes.

User response

Interpret the error codes using the documentation provided in the CICS Transaction Server System Programming Reference manual, “Appendix B. EXEC interface block (EIB) response and function codes." Contact IBM Software Support if you are unable to determine the cause of the problem.
Parent topic: Error message code descriptions

AUV3001E ERROR OBTAINING GWA ADDR: EIBRCODE=*NNNNNNNNNNNN*

Explanation

While running the Program List Table Program Initialization module AUVPLTPI, an error was encountered regarding an attempt to obtain the address of the Global Work area. The value *NNNNNNNNNNNN* represents the EXEC Interface Block error and response codes.

User response

Interpret the error codes using the documentation provided in the CICS Transaction Server System Programming Reference manual, “Appendix B. EXEC interface block (EIB) response and function codes." Contact IBM Software Support if you are unable to determine the cause of the problem.
Parent topic: Error message code descriptions

AUV3003E ERROR STARTING AUVFROUT: EIBRCODE=*NNNNNNNNNNNN*

Explanation

While running the Program List Table Program Initialization module AUVPLTPI, an error was encountered regarding an attempt to start the XFCFROUT Global User Exit AUVFROUT. The value *NNNNNNNNNNNN* represents the EXEC Interface Block error and response codes.

User response

Interpret the error codes using the documentation provided in the CICS Transaction Server System Programming Reference manual, “Appendix B. EXEC interface block (EIB) response and function codes." Contact IBM Software Support if you are unable to determine the cause of the problem.
Parent topic: Error message code descriptions

AUV3004I AUVPLTPI XFCFROUT GLOBAL USER EXIT SUCCESSFULLY ENABLED AND STARTED

Explanation

While running the Program List Table Program Initialization module AUVPLTPI, the XFCFROUT Global User Exit AUVFROUT was successfully enabled and started.

User response

No action is required.
Parent topic: Error message code descriptions

AUV3005E ERROR STOPPING AUVFROUT: EIBRCODE=*NNNNNNNNNNNN*

Explanation

While running the Program List Table Program Termination module AUVPLTPS, an error was encountered regarding an attempt to stop the XFCFROUT Global User Exit AUVFROUT. The value *NNNNNNNNNNNN* represents the EXEC Interface Block error and response codes.

User response

Interpret the error codes using the documentation provided in the CICS Transaction Server System Programming Reference manual, “Appendix B. EXEC interface block (EIB) response and function codes." Contact IBM Software Support if you are unable to determine the cause of the problem.
Parent topic: Error message code descriptions

AUV3006E ERROR OBTAINING GWA ADDR: EIBRCODE=*NNNNNNNNNNNN*

Explanation

While running the Program List Table Program Termination module AUVPLTPS, an error was encountered regarding an attempt to obtain the address of the Global Work area. The value *NNNNNNNNNNN* represents the EXEC Interface Block error and response codes.

User response

Interpret the error codes using the documentation that is provided in the CICS Transaction Server System Programming Reference manual, Appendix B. EXEC interface block (EIB) response and function codes. Contact IBM Software Support if you are unable to determine the cause of the problem.
Parent topic: Error message code descriptions

AUV3008E ERROR DISABLING AUVFROUT: EIBRCODE=*NNNNNNNNNNN*

Explanation

While running the Program List Table Program Termination module AUVPLTPS, an error was encountered regarding an attempt to disable the XFCFROUT Global User Exit AUVFROUT. The value *NNNNNNNNNNN* represents the EXEC Interface Block error and response codes.

User response

Interpret the error codes using the documentation provided in the CICS Transaction Server System Programming Reference manual, “Appendix B. EXEC interface block (EIB) response and function codes." Contact IBM Software Support if you are unable to determine the cause of the problem.
Parent topic: Error message code descriptions

AUV3009I AUVPLTPS XFCFROUT GLOBAL USER EXIT SUCCESSFULLY STOPPED AND DISABLED

Explanation

While running the Program List Table Program Termination module AUVPLTPS, the XFCFROUT Global User Exit AUVFROUT was successfully stopped and disabled.

User response

No action is required.
Parent topic: Error message code descriptions

AUV3010W CICS PLTPI INSTALLED BUT CICS_SUPPORT NOT SPECIFIED IN OPTIONS

Explanation

The CICS Support Program List Table Program Initialization program AUVPLTPI was defined to CICS, but the CICS_SUPPORT parameter was not enabled in the OPTIONS start-up parameters for the Security Guardium® S-TAP® for Data Sets started task.

User response

To use full CICS support within the product, you must specify CICS_SUPPORT=ENABLE in the OPTIONS parameters defined to the started task. Make the necessary changes to the OPTIONS parameters and restart the product.
Parent topic: Error message code descriptions