

IBM Multi-Cloud Data Encryption
Technologie SPx®
Version 2.3

Guide d'administration



Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 111.

Certaines illustrations de ce manuel ne sont pas disponibles en français à la date d'édition.

Deuxième édition - mai 2019

Cette édition s'applique à la version 2.3 d'IBM Multi-Cloud Data Encryption (numéro de produit 5737-C67) et à toutes les versions et modifications ultérieures sauf indication contraire dans les nouvelles éditions.

Réf. US : SC27-9557-01

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- <http://www.fr.ibm.com> (serveur IBM en France)
- <http://www.ibm.com/ca/fr> (serveur IBM au Canada)
- <http://www.ibm.com> (serveur IBM aux Etats-Unis)

*Compagnie IBM France
Direction Qualité
17, avenue de l'Europe
92275 Bois-Colombes Cedex*

© Copyright IBM France 2019. Tous droits réservés.

© Copyright IBM Corporation et autres 2017, 2019

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

© **Copyright International Business Machines Corporation 2017, 2019.**

Table des matières

Avis aux lecteurs canadiens.....	vii
Chapitre 1. Introduction.....	1
Droit d'utilisation autorisé.....	1
Point de contact.....	1
Contexte et intention du Guide d'administration.....	1
Chapitre 2. Présentation générale.....	3
Présentation du produit	3
Types d'agent.....	4
Agent de type Volume.....	4
Agent de type Fichier avec une règle.....	4
Agent de type Volume avec une règle.....	5
Agent de type Magasin d'objets.....	5
Matrice de fonctionnalités d'agent.....	5
Chapitre 3. Remarques sur la planification.....	7
Prérequis.....	7
Configuration système requise minimale.....	7
Exigences de certificats.....	8
Prise en charge du système de fichiers pour les agents.....	8
Configuration du réseau.....	9
Ports réseau.....	9
Configuration des archives de visualisation ouvertes.....	9
Interface REST.....	9
Chapitre 4. Installation du produit.....	11
Préparation de l'installation.....	11
Licences.....	11
Gestion des machines virtuelles/OVA MDE.....	11
Installation de MDE.....	11
Configuration de la langue.....	12
Configuration d'une base de données.....	13
Base de données interne.....	13
Base de données externe.....	13
Paramètres du certificat serveur.....	14
Magasin de clés, magasin de clés de confiance et autorité de certification.....	14
Paramètres de l'infrastructure à clés publiques.....	15
Démarrage et première connexion.....	15
Chapitre 5. Interface graphique utilisateur (GUI) de MDE.....	17
Navigation de base dans le produit.....	17
Tableau de bord du produit.....	17
Saisie semi-automatique de champ de saisie.....	17
Notifications d'attention.....	17
Propriétés avancées.....	18
Réglage de la langue de l'interface graphique.....	19
Chapitre 6. Tâches.....	21

Description de la tâche.....	21
Approbation par plusieurs administrateurs.....	22
Approbation d'une tâche.....	23
Refus d'une tâche.....	23
Non-intervention sur une tâche.....	23
Informations sur une tâche.....	23
Chapitre 7. Gestion des administrateurs MDE.....	25
Rôles d'un administrateur.....	25
Rôle d'administrateur du produit.....	25
Rôle d'administrateur de la sécurité.....	25
Gestion des administrateurs.....	25
Ajout d'un nouvel administrateur.....	25
Modification du mot de passe administrateur.....	26
Modification du rôle d'administrateur.....	26
Modification du statut d'administrateur.....	26
Suppression d'un administrateur.....	27
Verrouillage d'un compte utilisateur.....	27
Liste des annuaires LDAP.....	27
Source d'utilisateur.....	28
Chapitre 8. Événements.....	29
Journal des événements.....	29
Détails d'un événement.....	30
Exportation d'un événement.....	30
Transfert d'événements.....	30
Arguments d'événements.....	31
Événements d'un agent.....	31
Événements fiables.....	31
Chapitre 9. Gestion des clés d'application des règles.....	33
Ajout d'une clé.....	33
Modification d'une clé.....	33
Rotation de clé.....	33
Révocation de clé.....	35
Broyage de clé.....	35
Clés auto-générées.....	35
Magasin de clés externe.....	36
Magasins de clés KMIP.....	36
Outils HSM (Hardware Security Module).....	37
Chapitre 10. Définition de règle au niveau d'un fichier.....	39
Sélecteurs.....	39
Ensembles de chemins.....	40
Types de données.....	41
Ligne de type de données.....	41
Variables de ligne de type de données.....	41
Processus.....	42
Chapitre 11. Mise en service et gestion des agents.....	45
Ajout d'un agent.....	45
Identité.....	45
Réseau.....	46
Création d'un agent de type Fichier avec une règle, Volume avec une règle et Volume.....	46
Volumes.....	49
Création d'un agent de type Magasin d'objets.....	49
Utilisateurs autorisés.....	52

Outils d'agents.....	53
Vérification et génération.....	54
Activation d'un agent.....	54
Affichage des agents.....	54
Rapport sur les agents.....	55
Installation d'un agent.....	55
Installation d'un agent pour Linux.....	56
Installation d'un agent pour AIX.....	58
Installation d'un agent pour Windows.....	58
Règle active.....	61
Modification d'un agent.....	61
Modification des informations de l'agent.....	61
Ajout/Suppression de certificats.....	62
Outils d'agents.....	62
Accès aux données SU.....	63
Interruption d'une règle.....	64
Modifications apportées à une règle.....	64
Instantanés de l'agent.....	68
Enregistrement des modifications et des instantanés d'un agent.....	68
Gestion des instantanés.....	69
Désinstallation d'un Agent de type Fichier.....	70
Désinstallation des agents de volume.....	71
Désinstallation d'un Agent de type Volume.....	71
Désinstallation d'un agent de type Volume avec une règle.....	72
Désinstallation de l'agent Magasin d'objets.....	73
Suppression d'un agent dans MDE.....	73
Utilitaires d'agent.....	73
Chapitre 12. Opérations.....	75
Sauvegarde et restauration des données de produit.....	75
Sauvegarde des données du produits.....	75
Restauration des données d'un produit.....	75
Mise à jour du noyau.....	76
Mise à niveau.....	76
Pour le serveur MDE.....	76
Pour la machine virtuelle cible de l'agent.....	77
Données de service.....	78
Collecte des données du service.....	78
Suppression des informations sensibles des journaux du PPM.....	78
Annexe A. Exemple de processus d'installation d'agent.....	81
Processus Red Hat / CentOS.....	81
Processus AIX.....	82
Processus Windows Server.....	82
Annexe B. Exemples de certificats de l'autorité de certification.....	85
Annexe C. Exemple de conversion pour créer un fichier PKCS12.....	89
Annexe D. Choses à faire et à ne pas faire.....	91
Modification des clés affectées.....	91
Présentation.....	91
Contexte.....	91
Rotation des clés avec des sauvegardes chiffrées.....	91
Présentation.....	91
Contexte.....	91

Annexe E. Chiffrement sur place.....	93
Options de commande.....	93
<i>Etapas d'audit</i>	93
<i>Etapas de chiffrement</i>	93
Annexe F. Journalisation de débogage d'agent.....	95
Agents Linux.....	95
Agents Windows.....	95
Annexe G. Déploiement non OVA.....	97
Annexe H. Vérification de la version logicielle.....	99
Annexe I. Glossaire.....	101
Remarques.....	111
Marques.....	113
Dispositions pour la documentation du produit.....	113
Politique de confidentialité.....	114

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	IBM Canada
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.








OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

France	Canada	Etats-Unis
 (Pos1)		Home
Fin	Fin	End
 (PgAr)		PgUp
 (PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
 (Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

Chapitre 1. Introduction

Droit d'utilisation autorisé

L'utilisation de ce logiciel est restreinte en vertu des conditions du contrat de licence.

Point de contact

Pour obtenir des informations supplémentaires sur IBM Multi-Cloud Data Encryption (MDE), visitez le site Web du support IBM à l'adresse <https://www.ibm.com/support/home/>.

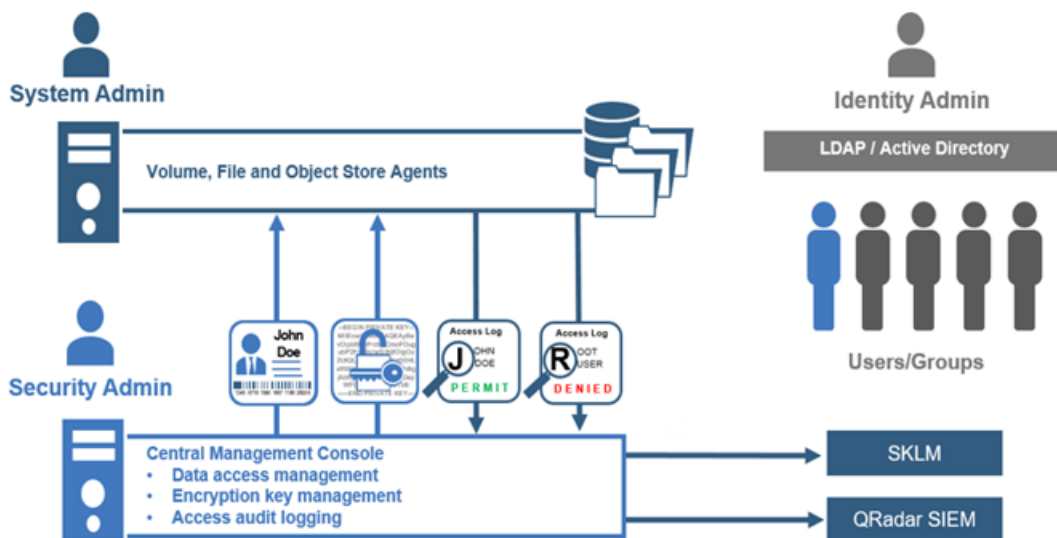
Contexte et intention du Guide d'administration

Le Guide d'administration est la référence principale pour l'installation, l'administration et l'utilisation de MDE pour la mise en service et la gestion de l'agent de chiffrement, la définition des règles (accès et contrôle cryptographique), gestion des clés d'application des règles et sécurisation des données au repos sur les serveurs sélectionnés, qui utilisent des agents déployés. Ce document est destiné à un administrateur système disposant de droits d'accès d'administration et possédant des connaissances de leur réseau d'entreprise pour installer et administrer le produit.

Chapitre 2. Présentation générale

Présentation du produit

IBM Multi-Cloud Data Encryption (MDE) est un produit de sécurisation des données exhaustif, reposant sur la technologie SPx, qui associe un chiffrement sur les données au repos (par le biais d'agents) aux fonctions de protection puissantes supplémentaires de Policy Provisioning Manager (PPM), qui fait office de console de gestion centralisée. A partir d'un emplacement centralisé unique, MDE permet la mise en service des agents, des paramètres de règles d'accès aux données (définition d'accès opérationnelle et cryptographique) et la gestion (cycle de vie des clés, mises à jour des agents et journalisation des accès utilisateur) de 25 000 agents maximum. MDE fournit un système transparent et sécurisé permettant d'affecter des agents qui chiffrent les données au niveau du système de fichiers ou du volume, à l'aide d'une technologie de fractionnement cryptographique unique. Sa protection centrée sur les données dépasse le chiffrement standard, ce qui rend le chiffrement des données plus robuste et impénétrable en cas d'attaque par force brute. La protection est encore augmentée grâce à la possibilité de restreindre, de surveiller et de contrôler l'accès aux données au niveau de l'utilisateur en définissant des règles d'accès à granularité fine.

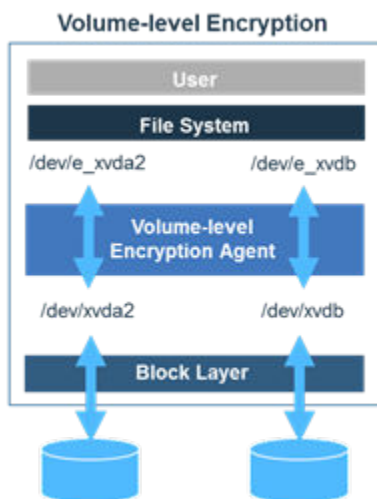


MDE permet de répartir les tâches avec des rôles d'administrateur distincts : administrateur du produit et administrateur de la sécurité. Le rôle Administrateur du produit possède les autorisations nécessaires à la configuration et à la gestion du produit MDE. Le rôle Administrateur de la sécurité possède les autorisations nécessaires à la mise en service et à la gestion des agents. Ces rôles sont décrits en détail dans la section 7 : Gestion des administrateurs MDE.

MDE prend en charge l'installation de quatre types d'agent qui fournissent la protection cryptographique des données utilisée pour appliquer les définitions de règle.

Types d'agent

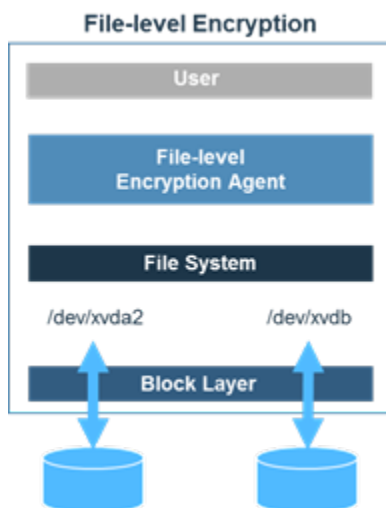
Agent de type Volume



L'Agent de type Volume fournit un chiffrement au niveau d'un volume avec des contrôles de règle d'accès limités. Le chiffrement au niveau du volume assure la sécurité sous la forme d'une unité de stockage prédéfinie protégée en mettant en oeuvre un pilote par bloc sur le système d'exploitation.

Un volume entier est défini et protégé cryptographiquement en tant qu'entité. Au fur et à mesure que des données sont ajoutées, éditées ou supprimées, l'Agent de type Volume s'assure que toutes les données contenues dans le volume sont sécurisées avec une clé de chiffrement gérée par PPM.

Agent de type Fichier avec une règle



L'agent de type Fichier avec une règle combine le chiffrement au niveau du fichier à une règle d'accès aux données. Le chiffrement de niveau de fichier offre une protection à des fichiers individuels au niveau du système de fichiers. Les tailles d'environnement de fichier et de stockage sont uniquement limitées par le système de fichiers et non par l'Agent de type Fichier avec une politique. L'emplacement des données protégées est sécurisé par la clé de groupe de travail pour cette définition de chemin, et tous les fichiers individuels stockés dans ce répertoire et ses répertoires enfant sont chiffrés séparément à l'aide d'un vecteur d'initialisation (IV) unique et non prévisible. Les données protégées peuvent être locales dans le système de fichiers ou montées sur le réseau via NFS.

Les clés de niveau de fichier uniques sont gérées par un système de gestion des clés interne. Le contrôle d'accès basé sur des règles vient en complément du chiffrement, ce qui permet de définir un contrôle d'accès à séparation des droits, de spécifier la journalisation des accès et de limiter les droits d'accès à des fonctions système spécifiques, comme Lecture/Lecture-écriture/Copie/Suppression. Ces contrôles des règles fonctionnent conjointement avec les autorisations LDAP ou Active Directory standard. Si un utilisateur ne possède pas d'autorisation dans LDAP ou Active Directory, l'administrateur de la sécurité ne peut pas remplacer ces contrôles d'accès et autoriser l'accès aux données.

Par défaut, tous les utilisateurs sont exclus de l'accès aux données couvertes par une règle.

L'administrateur de la sécurité doit définir qui a accès. Cela permet aux administrateurs de la sécurité de restreindre l'accès à des données protégées aux administrateurs système, aux administrateurs de fournisseur de cloud et aux superutilisateurs.

Agent de type Volume avec une règle

Un agent de type Volume avec une règle utilise le chiffrement au niveau du volume d'un agent de type volume et les règles de contrôle d'accès opérationnel basé sur les fichiers qui peuvent être appliquées à un ou à plusieurs chemins d'accès à des fichiers protégés.

Agent de type Magasin d'objets

Un agent de type Magasin d'objets opère sur un modèle "M de N", qui détermine le nombre de morceaux de données requis pour reconstruire les données (M) à partir du nombre total de morceaux créés (N). Les morceaux de données stockés, qui peuvent se trouver dans des emplacements locaux ou distants suivant la licence, sont désignés comme "parts". L'utilisation de plusieurs parts permet d'améliorer les flux de données, de même que les options ajoutées de résilience des données et de tolérance aux pannes. Le modèle de partages distribués M sur N pris en charge est 1:1, 2:3 ou 2:4.

Un agent de type Magasin d'objets (OSA) chiffre les données qui sont envoyées au stockage d'objets. Il sert de passe-système pour les fichiers qui sont transmis au stockage d'objets en chiffrant et en fractionnant les données en cours de route. Les fichiers sont extraits du stockage d'objets via l'agent Magasin d'objets et sont déchiffrés au moment de leur extraction. Les fichiers au repos dans le stockage d'objets sont chiffrés. Seuls les utilisateurs autorisés peuvent envoyer et recevoir des données via l'agent Magasin d'objets.

Matrice de fonctionnalités d'agent

Fonction d'agent	Agent de type Volume	Agent de type Volume avec une règle	Agent de type Fichier avec une règle	Agent de type Magasin d'objets
Chiffrer le volume complet	✓	✓		
Chiffrer des fichiers individuellement dans des répertoires protégés désignés			✓	
Règle au niveau du fichier		✓	✓	
Journaux d'audit d'accès aux fichiers		✓	✓	

Protège contre l'accès administrateur aux données utilisateur			✓	
Chiffrer les données dans Object Storage				✓

Chapitre 3. Remarques sur la planification

Prérequis

L'installation d'IBM Multi-Cloud Data Encryption (MDE) est une procédure simple, qui inclut l'installation d'une archive de virtualisation ouverte (OVA) et l'exécution d'un programme d'installation de PPM (Provisioning Policy and Management).

Lors de la préparation, il est recommandé de consulter les instructions d'installation dans leur intégralité avant d'installer le logiciel. Voici une liste des prérequis permettant d'installer et d'utiliser correctement IBM Multi-Cloud Data Encryption.

1. Serveur opérationnel avec système d'exploitation sous licence et hyperviseur pris en charge (VMware ESXi™) pour déployer et exécuter PPM
2. archive de virtualisation ouverte (OVA) de base en package
3. Programme d'installation de PPM
4. Un ou plusieurs serveurs cible avec un système d'exploitation pris en charge pour l'agent (Red Hat® / CentOS 6.2+ ou 7.2+, AIX 7.1 ou 7.2 et Microsoft Windows Server® 2008 R2, Microsoft Windows Server® 2012 R2 ou Microsoft Windows Server® 2016).
5. Navigateurs : Google Chrome®, Microsoft Internet Explorer® 10+, Mozilla Firefox® ESR 52+.
6. Accès réseau entre PPM et tous les agents
7. Certificats signés par l'autorité de certification (magasin de clés, magasin de clés de confiance, bundle de certificats de l'autorité de certification) pour établir une session sécurisée entre le serveur de gestion (PPM) et tous les agents

Voir Exigences de certificats et Paramètres du certificat serveur pour plus de détails et [Annexe B](#), «Exemples de certificats de l'autorité de certification», à la page 85 pour obtenir un exemple.

Éléments requis pour l'agent de type Magasin d'objets (OSA) :

- Stockage d'objets compatible S3 : Amazon Web Services S3 (AWS S3), IBM Cloud Object Storage (COS S3)
- Données d'identification de stockage d'objet : ID utilisateur et clé secrète (mot de passe)
- Une application ou un utilitaire qui optimise la bibliothèque d'API REST AWS S3 ou la bibliothèque Python Boto pour diriger les données dans l'agent OSA

Remarque importante : Il est fortement recommandé que le MDE, les bases de données externes et les agents utilisent le NTP pour coordonner l'heure du système. Cela permet de s'assurer que les horodatages du journal des événements/d'audit sont séquencés correctement.

Configuration système requise minimale

Configuration système requise minimale pour la machine virtuelle de PPM

- 4 processeurs
- 8 Go RAM
- 40 Go de mémoire disponible
- Accès réseau nécessaire

Configuration système minimale requise pour l'agent Linux

- Processeur monocoœur 64 bits cadencé à 2 GHz avec AES-NI activé
 - (recommandé : processeur bicoœur 64 bits @2GHz avec AES-NI activé)
 - 2 Go RAM (recommandé 4 Go RAM)
- 20 Go d'espace disponible sur le disque dur
 - 300 Mo ou plus sont recommandés pour stocker les fichiers journaux
- Accès réseau nécessaire
- Installer / mettre à jour les packages suivants : curl, openssl, et nss sur Red Hat / CentOS
- Accès Internet ou accès à un référentiel local lors de l'installation initiale de l'agent
- Un certificat SSL est requis pour les agents

Configuration système minimale requise pour l'agent Windows

- Processeur monocoœur 64 bits cadencé à 2GHz avec AES-NI activé (recommandé : processeur bicoœur 64 bits cadencé à 2GHz avec AES-NI activé)
- 4 Go de RAM (recommandé : 8 Go de RAM)
- 20 Go d'espace disponible sur le disque dur (300 Mo ou plus sont recommandés pour l'espace du fichier journal)
- Accès réseau nécessaire
- Un certificat SSL est requis pour les agents

Remarque : Un certificat SSL (auto-signé ou d'une autorité de certification) et un fichier de paires de clés sont requis avant de créer des agents. Le certificat est utilisé pour établir une connexion TLS sécurisée entre l'agent et le serveur MDE.

Exigences de certificats

Des certificats sont requis pour établir une connexion sécurisée entre le serveur PPM et les agents. Les conditions suivantes sont requises pour les certificats :

- PPM Server exige que le certificat présenté par un agent soit résolu par cet agent (nom d'hôte DNS ou adresse IP).
- PPM Server exige que le certificat présenté par un agent ait l'utilisation de la clé étendue "Authentification client" définie
- L'agent exige que le certificat présenté par le serveur PPM soit résolu sur le serveur PPM (nom d'hôte DNS ou adresse IP)
- L'agent exige que le certificat présenté par le serveur PPM ait l'utilisation de la clé étendue "Authentification serveur" définie

Le serveur PPM et l'agent doivent être synchronisés sur une source d'horloge fiable pour s'assurer que les certificats sont inclus dans la période de validité.

Un certificat unique est requis pour chaque agent déployé.

Prise en charge du système de fichiers pour les agents

Les agents de type Volume effectuent le chiffrement au niveau du volume. Les agents de type Fichier avec une règle fonctionnent avec ou sur des systèmes de fichiers pris en charge par le système d'exploitation hôte. L'agent de type Fichier avec une règle et l'agent de type Volume avec une règle prennent en charge les systèmes de fichiers suivants :

Serveurs Linux

- EXT3
- EXT4
- XFS (sur Red Hat / CentOS 6.5 ou version ultérieure)
- NFS (NFSv3, NFSv4)

Serveurs Windows

- NTFS
- ReFS (sur Windows Server 2012 R2 ou version ultérieure)

AIX

- JFS2

Configuration du réseau

Pourquoi et quand exécuter cette tâche

MDE nécessite une connexion réseau uniforme entre le ou les serveurs PPM de MDE et les agents. Les protocoles Internet IPv4 et IPv6 sont pris en charge. L'affectation d'adresses IP statiques ou l'utilisation du protocole DHCP avec des locations statiques répond à ce besoin. De plus, il est également possible d'utiliser sur l'écosystème une infrastructure DNS opérationnelle ainsi que des noms d'hôte optimisés.

Ports réseau

Fonction	Port par défaut	Configurable
Web	443	Oui
Base de données	5432	Oui
LDAP externe	Aucun	Oui
Annuaire LDAP	Aucun	Oui
Transfert d'événements de messagerie	Aucun	Oui
Transfert d'événements syslog	Aucun	Oui

Configuration des archives de visualisation ouvertes

L'archive de virtualisation ouverte (OVA) MDE fournie est préconfigurée avec l'attribut MaxAuthTries défini sur 1. Pour une authentification appropriée sur SSH à la machine virtuelle de MDE, l'attribut MaxAuthTries doit être modifié (non recommandé), ou les clients SSH doivent définir l'attribut PubkeyAuthentication sur "no" dans la ligne de commande ou dans la configuration du client SSH local.

Interface REST

MDE prend en charge une interface REST fonctionnant entièrement par programmation. L'URL REST principale est :

https://<IP machine virtuelle>/rest/

Remarque critique

L'API REST permet à un administrateur d'exécuter des fonctions avancées, inaccessibles par le biais de l'interface web. La façon dont l'API REST peut être utilisée peut entraîner un état non pris en charge d'un agent. Il est donc essentiel de bien comprendre la programmation de l'API REST.

Pour plus de détails, reportez-vous au document de spécification de l'API REST d'IBM Multi-Cloud Data Encryption (MDE).

Chapitre 4. Installation du produit

Préparation de l'installation

La procédure d'installation de MDE comporte trois étapes :

1. Prérequis
2. Dispositif Base Open Virtual Appliance (OVA) MDE disponible
3. Hyperviseur pris en charge (VMware ESXi™)

Licences

MDE ne nécessite pas de licence de produit unique pour s'exécuter ou pour configurer des agents au-delà de ce que permet le contrat de licence de logiciel.

Gestion des machines virtuelles/OVA MDE

Après avoir déployé l'OVA MDE, mettez à jour le système pour vous assurer que les dernières versions logicielles et les derniers correctifs de sécurité sont installés.

Remarque : Mettez périodiquement à jour le système pour récupérer les versions logicielles et les correctifs de sécurité les plus récents.

Installation de MDE

Pourquoi et quand exécuter cette tâche

Pour installer le logiciel MDE :

A l'aide de l'exemple de fichier `ibm_sw_mde_X.x.x-XX.bin`, remplacez le numéro de build XX par la version du logiciel disponible et opérez en tant qu'utilisateur root.

Procédure

1. Déployez l'archive de virtualisation ouverte de base de MDE dans votre hyperviseur. Dans cet exemple, elle est nommée "machine virtuelle MDE".
2. Connectez-vous en tant qu'administrateur et définissez un nouveau mot de passe.
La machine virtuelle MDE utilise des critères de la norme PAM qui sont configurables par un administrateur. Le mot de passe PAM doit contenir plus de 8 caractères et ne peut pas contenir 5 caractères du mot de passe précédent.
3. Notez l'adresse IP de la machine virtuelle MDE.
4. Téléchargez le fichier `ibm_sw_mde_X.x.x-XX.bin` dans le MDE en utilisant SCP ou une méthode de transfert de fichier similaire.
5. Rendez le fichier binaire exécutable.

```
[admin@localhost]$ chmod +x ./ibm_sw_mde_X.x.x-XX.bin
```

6. Exécutez le fichier binaire.

```
[admin@localhost]$ ./ibm_sw_mde_X.x.x-XX.bin
```

7. Sélectionnez "English" et appuyez sur Entrée.
8. Lisez les pages de licence et faites défiler l'écran jusqu'à <OK>, puis appuyez sur 'Entrée' pour avancer.
9. Sélectionnez <Oui> et appuyez sur Entrée pour accepter le contrat de licence.
10. Une fois l'extraction terminée, appuyez sur Entrée sur <OK> pour revenir à la ligne de commande.
11. Installez les packages RPM en tant que superadministrateur.

```
[admin@localhost]$ sudo yum -y install rpms/*.rpm
```

12. MDE est maintenant installé, mais pas encore configuré.

Remarque : Ne redémarrez pas la machine virtuelle MDE tant que la configuration n'est pas terminée.

Configuration de la langue

Pourquoi et quand exécuter cette tâche

MDE prend en charge plusieurs langues pour les scripts de la machine virtuelle et l'interface graphique PPM. Vous devez configurer une préférence linguistique par défaut avant d'exécuter le produit.

Remarque : Les langues sont installées via RPM dans la machine virtuelle MDE. Le fichier binaire d'installation est livré avec un ensemble intégré de fichiers RPM de langue. Des langues supplémentaires peuvent être ajoutées après l'installation initiale et peuvent nécessiter un redémarrage du service PPM pour prendre effet.

Pour configurer la langue par défaut, effectuez les étapes ci-dessous :

Procédure

1. Exécutez le script spsd-langsetup.

```
$ sudo /opt/securityfirst/spsd/bin/spsd-langsetup
```

2. Affichez le code de langue par défaut actuel. Si aucune langue n'est définie, le code n'est pas renseigné.

```
Définissez le code de langue par défaut.  
La valeur par défaut en cours est :
```

3. Affichez la liste des codes de langue disponibles. (La liste ci-dessous peut contenir des exemples non disponibles dans votre version du produit.)

```
Codes de langue disponibles :  
en_US  
ja_JP  
ko_KR
```

4. Entrez le nouveau code de langue par défaut.

```
Entrez le nouveau code de langue par défaut : en_US  
Le code de langue par défaut est : en_US
```

5. Réexécutez le script spsd-langsetup pour valider que le code de langue par défaut est défini.

```
Définissez le code de langue par défaut.  
La valeur par défaut en cours est : en_US
```

Configuration d'une base de données

Pourquoi et quand exécuter cette tâche

MDE prend en charge une configuration de base de données interne ou externe. Dans un cas comme dans l'autre, vous devez configurer MDE de manière à communiquer avec la base de données configurée avant de démarrer MDE pour la première fois.

Pour associer une base de données à MDE, vous devez modifier le fichier `/etc/spsd/db.props` de la machine virtuelle MDE. Vous devez effectuer les modifications de ce fichier en tant qu'utilisateur `root`.

Remarque : L'exécution du script `spsd-pgsetup` modifiera automatiquement le fichier `db.props` avec les valeurs saisies aux invites.

Configurez les propriétés du fichier de manière à vous connecter à la base de données interne ou externe appropriée, comme indiqué ci-dessous. Les modifications apportées aux propriétés de la base de données ne seront pas appliquées tant que vous n'aurez pas redémarré MDE.

Remarque critique

Lors de la modification du fichier `db.props`, respectez les contraintes suivantes :

- Pas d'espace entre le nom de la propriété et `"=`
- Pas d'espace entre `"=` et la valeur de la propriété

Base de données interne

Actuellement, MDE prend en charge PostgreSQL en tant que base de données interne.

Base de données Postgres interne

L'archive de virtualisation ouverte (OVA) de MDE est préparée en package avec le logiciel PostgreSQL. Pour configurer la base de données afin qu'elle fonctionne avec MDE, procédez comme suit :

1. Exécutez le script `spsd-pgsetup` avec l'option de script `"--local"`.

```
$ sudo /opt/securityfirst/spsd/bin/spsd-pgsetup --local
```

Remarque : L'option `"--local"` configure une nouvelle base de données vide sur le serveur PostgreSQL `"local"` interne.

Après avoir appliqué ces paramètres, passez à Paramètres du certificat serveur. Si vous envisagez de configurer la base de données sur une cible distante, passez à la base de données externe.

Base de données externe

Actuellement, le seul serveur de base de données externe pris en charge est PostgreSQL. Vous devez vous assurer que vous connaissez les informations suivantes avant d'exécuter ce processus :

- Nom (ou adresse IP) d'un serveur de base de données PostgreSQL accessible
- Numéro de port écouté par le serveur PostgreSQL
- Nom d'une base de données existante sur le serveur ci-dessus
- Nom d'un utilisateur existant défini en tant que propriétaire de la base de données ci-dessus
- Mot de passe de l'utilisateur de la base de données ci-dessus

Pour configurer la base de données afin qu'elle fonctionne avec MDE, exécutez le script `spsd-pgsetup`. Toutes les valeurs fournies dans cette commande sont des exemples :

```
$ sudo /opt/securityfirst/spsd/bin/spsd-pgsetup --host  
ext.postgres.svr1 --port 5432 --dbname policyDB --user policyDBuser  
--pass mypassword123
```

Pour mettre à niveau la base de données vers le dernier schéma, exécutez le script `spsd-pgsetup` avec l'option de script `--upgrade`

```
$ sudo /opt/securityfirst/spsd/bin/spsd-pgsetup --upgrade
```

Remarque : L'exécution du script `spsd-pgsetup` avec l'option `“upgrade”` garantit que les tables de la base de données sont correctement configurées avec la version en cours de PPM.

Après avoir configuré ces paramètres, passez à Paramètres du certificat serveur.

Paramètres du certificat serveur

Magasin de clés, magasin de clés de confiance et autorité de certification

Les certificats permettent d'établir une session de communication sécurisée entre le serveur de gestion (PPM) et les agents ainsi que les navigateurs Web. PPM nécessite que tous les certificats soient signés par une autorité de certification. L'autorité de certification établit une racine de confiance que tous les participants de la session de communication utilisent pour vérifier l'identité de l'autre partie.

- Le certificat signé par l'autorité de certification et sa clé correspondante sont combinés en un fichier de clés Java.
- Le certificat (ou le bundle de certificats) de l'autorité de certification utilisée pour signer les certificats d'agent doivent être ajoutés au magasin de clés de confiance de la console PPM.
- Les trois composants (fichier de clés, fichier de clés de confiance et bundle de certificats de l'autorité de certification) sont utilisés lors de la procédure de configuration des certificats PPM.

Reportez-vous à l'Annexe B, «Exemples de certificats de l'autorité de certification», à la page 85 pour voir un exemple de traitement de certificat de l'autorité de certification.

Le magasin de clés de certificats Web du serveur et le magasin de clés de confiance de certificats Web sont configurés via

le script d'installation, `spsd-certsetup`, situé dans le répertoire `/opt/securityfirst/spsd/bin` de la machine virtuelle MDE.

Pour configurer le magasin de clés, le magasin de clés de confiance et le bundle de l'autorité de certification de l'agent, entrez des exemples en **gras** :

```
$ sudo /opt/securityfirst/spsd/bin/spsd-certsetup --ks /etc/ppm/certs/ppm.jks --kw password
```

```
$ sudo /opt/securityfirst/spsd/bin/spsd-certsetup --ts /etc/ppm/certs/trust.jks --tw password
```

```
$ sudo /opt/securityfirst/spsd/bin/spsd-certsetup --aca /etc/ppm/certs/ca_bundle.pem
```

Important

Les composants de certificat de serveur, tels que le magasin de clés, le magasin de clés de confiance et le bundle de l'autorité de certification, ne sont pas fournis et doivent être générés et téléchargés dans la machine virtuelle MDE via le script de configuration. Si une carte d'accès commune (CAC) est utilisée pour l'authentification, les paramètres de l'infrastructure PKI doivent être activés.

Paramètres de l'infrastructure à clés publiques

Pourquoi et quand exécuter cette tâche

La configuration de l'infrastructure à clés publiques (PKI) permet à PPM de fournir une méthode secondaire d'authentification des utilisateurs PPM. Lorsqu'il est configuré, PPM accepte les certificats clients en tant que méthode d'authentification pour les sessions Web et REST.

Ce certificat doit être signé par une autorité de certification approuvée par PPM. PPM valide le certificat en fonction des règles définies dans le script `spsd-certsetup`.

Exemple d'entrée en **gras** :

```
$ sudo /opt/securityfirst/spsd/bin/spsd-certsetup --crl-on --ocsp-on --pols-on oids  
x.x.x.x.x.x.x,x.y.y.y.y.y.y
```

Important

L'infrastructure PKI peut être configurée dans la même exécution de script que le magasin de clés, le magasin de clés de confiance et le bundle d'autorités de certification. Elle est décomposée ici à des fins éducatives.

Après l'installation de MDE, la configuration d'une base de données, l'ajout de certificats et, éventuellement, la configuration de l'infrastructure PKI, vous pouvez redémarrer la machine virtuelle MDE.

Démarrage et première connexion

Pourquoi et quand exécuter cette tâche

Une fois le déploiement et la configuration terminés, redémarrez le serveur MDE ou démarrez simplement le service “spsd” à partir de la console MDE pour démarrer l'interface utilisateur Web. Vous devez récupérer l'adresse IP ou le nom d'hôte de la machine virtuelle via la console de la machine virtuelle ou l'hyperviseur hôte.

Ouvrez un navigateur Web pris en charge et entrez l'adresse IP ou le nom d'hôte en tant qu'URL pour accéder à la page de connexion MDE.

```
https://<Adresse IP du serveur MDE>
```

A ce stade, vous pouvez modifier le paramètre de langue à partir de la liste disponible des langues prises en charge.



Please Sign In

Login

Les données d'identification par défaut sont les suivantes :

Nom d'utilisateur : admin
Mot de passe : admin

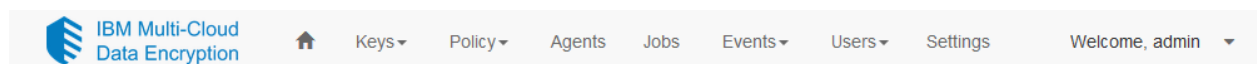
Important

- Les données d'identification par défaut doivent être modifiées après la première connexion
- MDE prend en charge la plupart des versions des navigateurs web Firefox, Chrome, Microsoft Edge et Internet Explorer
- L'authentification du client de l'infrastructure PKI peut passer la page de connexion et accéder directement au tableau de bord

Chapitre 5. Interface graphique utilisateur (GUI) de MDE

Navigation de base dans le produit

MDE contient un menu de navigation situé en haut de la page. Certaines options de menu contiennent des listes de sous-menu. Cliquez sur chaque option de menu pour accéder à la page appropriée ou afficher la liste de sous-menu.



- **Icône d'accueil** - Lien vers la page d'accueil du Tableau de bord du produit.
- **Clés** – Menu contenant des liens vers les pages du sous-menu liées aux clés : Magasins de clés externes et Clés gérées.
- **Règle** - Menu contenant des liens vers les pages du sous-menu liées aux règles : Types de données, Ensembles de chemins d'accès, Processus et Sélecteurs.
- **Agents** – Lien vers la page Agents.
- **Tâches** - Lien vers la page Tâches.
- **Événements** - Menu contenant des liens vers les pages du sous-menu liées à des événements : Transfert et Journaux.
- **Utilisateurs** – Menu contenant les liens vers les page du sous-menu liées aux utilisateurs : Comptes et Annuaire LDAP.
- **Paramètres** - Lien vers la page Paramètres.

Important

MDE prend en charge le contrôle d'accès basé sur les rôles, ce qui signifie que certains éléments de navigation ne sont indisponibles en fonction du rôle de l'utilisateur connecté. De ce fait, certains éléments de navigation peuvent être indisponibles pour tous les administrateurs.

Tableau de bord du produit

La page d'accueil du produit est la page du tableau de bord d'arrivée principale. Elle est destinée à fournir un récapitulatif du statut en cours des événements récents à l'administrateur connecté. La page d'accueil contient les événements récents, les tendances des événements et d'autres données récapitulatives.

Saisie semi-automatique de champ de saisie

L'interface utilisateur comporte des champs de saisie. Certains champs de saisie affichent des critères de correspondance en fonction de la saisie semi-automatique des caractères saisis. Avant qu'une liste de suggestions de saisie semi-automatique ne s'affiche, vous devez parfois saisir plusieurs caractères dans ces champs.

Notifications d'attention

Lors de la première connexion, une bannière de couleur en haut de l'interface utilisateur indique les actions à résoudre.

Si l'administrateur clique sur le texte dans la bannière, il est redirigé vers la page "Problèmes" qui contient les différents éléments.

Home
 >
 Issues

The current number of job approvals allows unilateral action.
 Dismiss

The number of users having Product Administrator role is nearing the threshold of required approvals or required rejections.
 Dismiss

The number of users having Security Administrator role is nearing the threshold of required approvals or required rejections.
 Dismiss

One or more users are defined as having both Product Administrator and Security Administrator roles.
 Dismiss

Le développement d'un des éléments affiche des détails sur la résolution du problème associé.

The current number of job approvals allows unilateral action.
 Dismiss

Summary It is best practice to require a minimum two administrators for job approval.

How to resolve Go to the "Advanced Properties" tab on the "Settings" page, and edit the "Number of approvals required to run a job" field. Note that it may also be wise to do this for number of rejectors as well, depending on company structure.

Resolve

Une fois que tous les problèmes ont été résolus, la bannière disparaît. Toutefois, un administrateur peut choisir de supprimer la bannière de la page en cours.

Important

De nouvelles conditions créant des problèmes "nécessitant une intervention" peuvent survenir, et la bannière s'affichera de nouveau.

Propriétés avancées

L'administrateur du produit est autorisé à configurer les propriétés avancées qui définissent le comportement du produit. Les propriétés avancées sont accessibles à partir de la page des paramètres. Ces propriétés sont étendues à l'instance locale ou potentiellement, si vous utilisez la fonctionnalité haute disponibilité ou à service partagé, à l'écosystème MDE.

Home
 >
 Settings

Advanced Properties

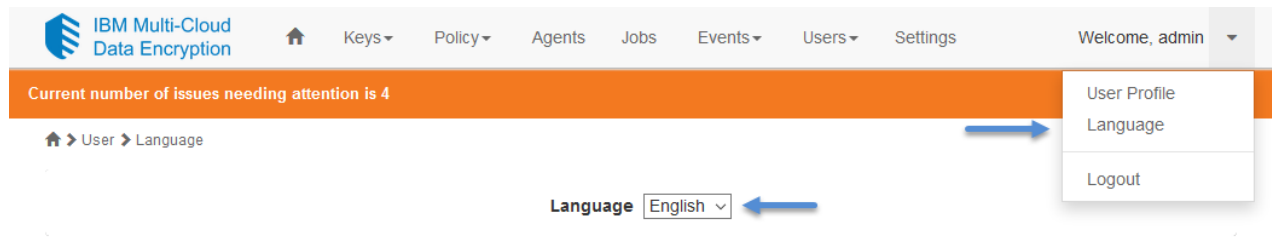
Property	Value	Description	Actions
com.securityfirstcorp.atlantis.bundles.haas.iterations	600000	Number of iterations used by REST API token hashing algorithm	Edit
com.securityfirstcorp.atlantis.jobs.requiredApprovers	1	Number of approvals required to run a job	Edit
com.securityfirstcorp.atlantis.jobs.requiredBuffers	2	The buffer number in between the number of users available and when we issue a warning	Edit
com.securityfirstcorp.atlantis.jobs.requiredRejectors	1	Number of rejections required to reject a job	Edit
events.maxLogLength	50000	Maximum number of entries in event log before rolling starts	Edit
com.securityfirstcorp.atlantis.bundles.userman.iterations	300000	Number of iterations used by user password hashing algorithm	Edit

Pour modifier une propriété, l'administrateur de produit doit cliquer sur le bouton "Modifier". Une fois les modifications appropriées effectuées, cliquez sur le bouton "Enregistrer" pour créer une tâche.

Réglage de la langue de l'interface graphique

Dans l'interface graphique, vous pouvez sélectionner l'une des langues prises en charge lors de l'installation initiale en effectuant une sélection dans la page de connexion ou dans la page d'accueil.

- **Page de connexion** - Situé en haut à droite de la page. Cliquez sur le menu déroulant pour afficher la liste des langues prises en charge.
- **Page d'accueil** - Dans le menu déroulant situé en haut à droite, sélectionnez "Langue" pour afficher la liste des langues prises en charge.

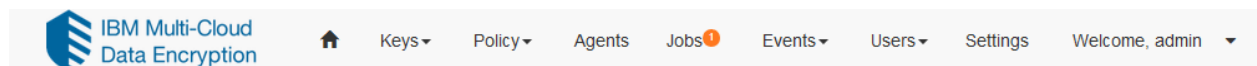


La langue affichée dans l'interface graphique est déterminée par la hiérarchie suivante (le premier paramètre en cours est utilisé) :

1. La valeur du cookie linguistique définie via l'interface utilisateur de PPM.
2. La valeur du paramètre linguistique du navigateur de l'utilisateur.
3. La valeur du code de langue défini via l'interface CLI de PPM, script-langsetup.
4. Le premier module linguistique PPM installé trouvé.

Chapitre 6. Tâches

MDE incorpore un système de tâches pour gérer l'approbation et les délais d'exécution des tâches. De nombreuses fonctionnalités utilisent le système de tâches pour attendre l'approbation avant confirmation. Lorsqu'une tâche est créée, une tâche est ajoutée à la liste dans la page Tâches.



Les administrateurs ont la possibilité d'approuver ou de refuser chacune des tâches ou de ne pas intervenir. Chaque administrateur ne peut agir qu'une seule fois par tâche.

Type	State	Created	Started	Completed	Notes	Actions
User Create	Waiting	2017-09-22T23:21:01Z				Edit Note Approve Reject Abstain Show Info

Description de la tâche

Tâche	Description	Catégorie	Rôle
Propriétés avancées	Modifie une propriété avancée.	Gestion des produits	Administrateur du produit
Modification d'un magasin de clés	Modifie l'emplacement/des détails du magasin de clés d'application des règles.	Paramètres du produit	Administrateur du produit
Rotation de clé	Effectue une rotation d'un ensemble de clés dans l'écosystème de l'agent.	Gestion des clés	Administrateur de la sécurité
Révocation de clé	Révoque un ensemble de clés dans l'écosystème de l'agent.	Gestion des clés	Administrateur de la sécurité
Broyage d'une clé	Supprime définitivement un ensemble de clés dans l'écosystème de l'agent, ce qui entraîne la perte des données.	Gestion des clés	Administrateur de la sécurité
Ajout d'un agent	Assure la mise en service et ajoute un nouvel agent dans l'écosystème.	Gestion des agents	Administrateur de la sécurité
Suppression d'un agent	Supprime un agent dans la gestion de MDE.	Gestion des agents	Administrateur de la sécurité
Modification d'un agent	Modifie les informations concernant un agent.	Gestion des agents	Administrateur de la sécurité

Mise à jour d'une règle	Modifie la règle associée à un agent.	Gestion des agents	Administrateur de la sécurité
Créer un administrateur	Crée un administrateur MDE.	Gestion des administrateurs MDE	Administrateur du produit
Suppression d'un administrateur	Supprime un administrateur MDE.	Gestion des administrateurs MDE	Administrateur du produit
Ajout d'un rôle à un administrateur	Ajoute un rôle à un administrateur MDE.	Gestion des administrateurs MDE	Administrateur du produit
Suppression d'un rôle d'un administrateur	Supprime un rôle à un administrateur MDE.	Gestion des administrateurs MDE	Administrateur du produit
Modification du mot de passe d'un administrateur	Modifie le mot de passe d'un administrateur MDE.	Gestion des administrateurs MDE	Administrateur du produit
Modification du statut d'un administrateur	Active ou désactive le compte d'un administrateur MDE.	Gestion des administrateurs MDE	Administrateur du produit
Enregistrement d'un répertoire	Configure des répertoires de serveur LDAP pour des administrateurs MDE	Gestion des administrateurs MDE	Administrateur du produit
Suppression d'un répertoire	Supprime un annuaire LDAP dans MDE.	Gestion des administrateurs MDE	Administrateur du produit
Mise à jour d'un répertoire	Modifie un répertoire de serveur LDAP.	Gestion des administrateurs MDE	Administrateur du produit

Approbation par plusieurs administrateurs

Le nombre nécessaire d'administrateurs approuvant ou refusant une tâche peut être configuré dans MDE. Par défaut, MDE est configuré pour l'approbation par un seul administrateur. Il est vivement recommandé d'exiger l'approbation d'une tâche par au moins deux administrateurs. L'approbation par plusieurs administrateurs évite qu'un seul administrateur permette une modification dans MDE proprement dit ou dans des instances d'agent géré.

User	Time	Actions	Required Approvals	Required Rejections	Notes
admin	2017-09-22T23:22:35Z	Approve	1	1	

Remarque critique

Le nombre d'administrateurs doit être supérieur ou égal au nombre d'"Approbations nécessaires" ou de "Rejets nécessaires". Assurez-vous qu'il existe le nombre requis d'administrateurs avant de modifier ces valeurs.

Les seuils d'approbation ou de rejet peuvent être redéfinis par le type de tâche. Chaque type de tâche défini par le système, à l'exception de la tâche Changement de propriété, possède un seuil d'approbation et un seuil de rejet dans Propriétés avancées, qui si définis, remplacent les valeurs par défaut du système. Une fois qu'une propriété est définie, elle ne peut pas être révoquée.

La tâche Modification de propriété est le seul type de tâche sans seuil d'approbation et de rejet car il contrôle la modification des propriétés avancées. Pour cette tâche, les seuils d'approbation et de rejet seront toujours plus élevés que les valeurs par défaut du système ou que la valeur de remplacement la

plus haute définie pour tout autre type de tâche. Avec cette action, aucun autre seuil de type de tâche ne pourra être subverti par le biais d'un processus de changement de propriété.

Approbation d'une tâche

Pour approuver une tâche, un administrateur disposant des autorisations appropriées doit accéder à la page Tâches, chercher la tâche appropriée et cliquer sur le bouton Approuver. Une fois que le nombre d'approbations nécessaires par les administrateur est atteint, la tâche est exécutée.

Refus d'une tâche

Pour refuser une tâche, un administrateur disposant des autorisations appropriées doit accéder à la page Tâches, chercher la tâche appropriée et cliquer sur le bouton Refuser. Une fois que le nombre de refus nécessaires par des administrateur est atteint, la tâche est annulée définitivement.

Non-intervention sur une tâche

La non-intervention sur une tâche indique qu'un administrateur a vu une tâche, mais qu'il ne souhaite ni l'approuver ni la refuser. La non-intervention peut être décrite plus clairement comme une position d'"audit" et évite que l'administrateur sélectionne ultérieurement une autre position pour la même tâche.

Informations sur une tâche

Chaque tâche dans MDE possède des informations différentes, qui la décrivent. Vous pouvez cliquer sur le bouton "Afficher les informations" pour afficher des informations spécifiques à la tâche. De plus, les actions (approbation, refus, non-intervention) effectuées sur la tâche par différents administrateurs s'affichent avec le nom d'utilisateur de l'administrateur qui a effectué l'action.

User Create	Done	2017-09-22T23:22:36Z	2017-09-22T23:22:36Z	2017-09-22T23:22:36Z		Hide Info
User	Time	Actions	Required Approvals	Required Rejections	Notes	
admin	2017-09-22T23:22:35Z	Approve	1	1		
Job Properties						
User		ProductAdmin				

Chapitre 7. Gestion des administrateurs MDE

Rôles d'un administrateur

MDE utilise une conception plane de contrôle d'accès basé sur un rôle statique (RBAC). Certaines fonctionnalités de MDE nécessitent des autorisations spécifiques. L'ensemble complet d'autorisations MDE est regroupé dans deux rôles distincts : Administrateur du produit et Administrateur de la sécurité. D'autres administrateurs de chaque rôle peuvent être ajoutés à tout moment.

Rôle d'administrateur du produit

Le rôle Administrateur du produit possède les autorisations nécessaires à la configuration et à la gestion du produit MDE.

Rôle d'administrateur de la sécurité

Le rôle Administrateur de la sécurité possède les autorisations nécessaires à la mise en service et à la gestion des agents. Ces autorisations comprennent notamment : définition des règles et spécifications, gestion des clés, définition du type de données, gestion des agents, configuration du magasin de clés externe et configuration LDAP externe des groupes externes d'une règle.

Gestion des administrateurs

Un administrateur de produit possède les autorisations nécessaires pour ajouter, modifier et supprimer d'autres administrateurs dans MDE.

Ajout d'un nouvel administrateur

Lors de l'ajout d'un nouvel administrateur, un administrateur du produit est invité à entrer son nom.

Edit User

New User Name

Cancel

Add User

Indiquez le nom d'utilisateur unique et une tâche sera créée pour ajouter cet administrateur à MDE.

Type	State	Created	Started	Completed	Actions
Scheduler	Waiting	2019-03-20T16:14:01Z			<div>ApproveRejectAbstainHide Info</div>
<div><div>ApprovedNone</div><div>RejectedNone</div><div>AbstainedNone</div></div> <div><div>Type : User Create</div><div>Frequency : Once</div><div>Starts : Upon approval</div></div> <div><div>Job Properties</div><div>User</div><div>test</div></div>					

Le nombre d'administrateurs de produit requis doit approuver la tâche pour que l'utilisateur soit créé.

Un administrateur qui vient d'être ajouté est créé avec un mot de passe expiré et aucun rôle défini. Un administrateur de produit doit éditer le mot de passe initial, le rôle et le statut. Chacune de ces mises à jour générera une tâche. Les tâches doivent être approuvées pour que le nouvel administrateur ne devienne actif dans MDE.

Modification du mot de passe administrateur

Pour modifier le mot de passe d'un administrateur, accédez à l'utilisateur sélectionné et cliquez sur le bouton Modifier le mot de passe. Une boîte de dialogue de saisie du mot de passe s'affiche.

The screenshot shows a dialog box titled "Edit User". It contains two input fields for "New Password" and "Confirm Password". Below these fields are "Cancel" and "Save" buttons. A red error message "Password Invalid" is displayed, followed by the text: "Passwords must be at least 8 characters, may not match any of the last 8 used passwords and must contain characters from three of the following five categories (click for a listing of each):". A bulleted list follows: "Upper case letters", "Lower case letters", "Numbers", "Symbols", and "Other Unicode characters". At the bottom, it states "Password and Password Confirm must match".

Entrez un mot de passe respectant les règles identifiées. Une fois que vous l'avez saisi, enregistrez les modifications, et une tâche est créée.

Le nombre nécessaire d'administrateurs doit approuver la tâche pour que la modification du mot de passe soit appliquée.

Remarque : Le nouvel administrateur sera invité à modifier le mot de passe lors de sa première connexion.

Modification du rôle d'administrateur

Pour modifier un rôle d'administrateur, localisez la ligne de l'utilisateur et sélectionnez le bouton "Modifier les rôles". Les cases à cocher pour la saisie des rôles s'affichent en ligne.

L'administrateur effectuant une modification peut appliquer le même rôle que celui qu'il possède, par exemple "administrateur intégré", à savoir l'utilisateur initial qui peut appliquer à la fois les rôles Administrateur de produit et Administrateur de la sécurité. Un utilisateur disposant des mêmes rôles est alors capable de faire de même.


ProductAdmin	Disabled	<input type="checkbox"/> Product Administrator <input type="checkbox"/> Security Administrator	2017-09-22T23:25:40Z	<input type="button" value="Save"/> <input type="button" value="Cancel"/>
--------------	----------	---	----------------------	---

Sélectionnez le ou les rôles souhaités et cliquez sur le bouton Enregistrer. Une tâche est alors créée.

Le nombre nécessaire d'administrateurs doit approuver la tâche pour que la modification du rôle soit appliquée.

Modification du statut d'administrateur

Pour modifier le statut d'un administrateur, accéder à l'utilisateur concerné et cliquez sur le bouton "Modifier le statut". Un menu déroulant de saisie du statut s'affiche en ligne.

ProductAdmin	Disable 	None		2017-09-22T23:25:40Z	Save	Cancel
--------------	---	------	--	----------------------	------	--------

Les valeurs de statut sont les suivantes : Activé, Désactivé et Verrouillé.

- **Activé** - L'administrateur est actif et peut effectuer des actions.
- **Désactivé** - L'administrateur est inactif et ne peut pas effectuer d'actions.
- **Verrouillé** - L'administrateur est verrouillé et ne peut pas effectuer d'actions.

Sélectionnez le statut souhaité et cliquez sur "Enregistrer". Une tâche est créée pour modifier le statut de l'utilisateur.

Les administrateurs doivent approuver la tâche en nombre nécessaire pour que la modification du statut soit appliquée.

Suppression d'un administrateur

Pour supprimer un administrateur, localisez la ligne de l'utilisateur cible et cliquez sur le bouton "Supprimer". Une tâche de suppression de l'utilisateur dans MDE commence. Cette action peut uniquement être effectuée par un utilisateur disposant du rôle d'Administrateur de produit.

Type	State	Created	Started	Completed	Notes	Actions
User Delete	Waiting	2017-09-22T23:37:05Z				<div>Edit Note</div> <div>Approve</div> <div>Reject</div> <div>Abstain</div> <div>Show Info</div>

Le nombre nécessaire d'administrateurs doit approuver la tâche pour que l'utilisateur soit supprimé.

Remarque critique

- La suppression d'un administrateur est définitive.
- Vous devez conserver suffisamment d'administrateurs pour respecter la condition d'approbation des tâches nécessaire (consultez la section "Approbation par plusieurs administrateurs").
- Les tâches ne peuvent pas être acceptées correctement si le nombre d'administrateurs est insuffisant.

Verrouillage d'un compte utilisateur

Pour protéger le système et les comptes utilisateur face aux attaques de mots de passe par force brute, les comptes utilisateurs sont verrouillés au bout de dix (10) échecs de connexion consécutifs. Le compte utilisateur sera verrouillé jusqu'à ce que le compte soit activé de manière explicite (voir section Edition du statut de l'administrateur) ou que le service serveur soit redémarré.

Important

- Pour redémarrer le service serveur, exécutez **systemctl restart spsd** dans la console de la machine virtuelle.
- Le verrouillage d'un compte s'effectue indépendamment sur chaque serveur. Un compte verrouillé sur un serveur d'un cluster n'est pas automatiquement verrouillé sur les autres serveurs du cluster.
- Le seuil de verrouillage d'un compte n'est pas configurable par l'utilisateur.

Liste des annuaires LDAP

Un administrateur du produit peut configurer des annuaires LDAP pour la gestion des utilisateurs MDE. Il est possible d'ajouter, de modifier ou de supprimer des annuaires LDAP. Chaque action crée une tâche d'approbation avant d'être appliquée.

Lors de l'ajout/la modification d'un répertoire LDAP, les paramètres disponibles sont les suivants :

- **ID de répertoire** - identification de l'annuaire LDAP.
- **Type** - option de liste déroulante pour LDAP ou Active Directory
- **Nom distinctif de liaison** - nom distinctif complet utilisé pour la liaison au serveur LDAP.

Exemple de syntaxe de nom distinctif de liaison :

```
uid={$username},ou=users,dc=company,dc=com
```

Remarque : Lorsque vous sélectionnez le type “Active Directory”, la section Nom distinctif de liaison est grisée, car ces informations ne sont pas requises.

- **Hôte** - adresse IP/nom d'hôte du serveur LDAP
- **Port** - port du serveur LDAP
- **Sécurisation** - identificateur d'une connexion LDAP sécurisée ou non
- **Actions** - sélectionnez Enregistrer ou Annuler

Directory ID	Type	Bind DN	Host	Port	Secure	Actions
LDAP1	LDAP	uid={\$username},ou=users,dc=company,dc=com	10.10.10.1	536	<input checked="" type="checkbox"/>	<div>Save</div> <div>Cancel</div>

Source d'utilisateur

MDE peut prendre en charge simultanément des utilisateurs définis en interne et en externe. Pour les utilisateurs définis en externe, une valeur s'affiche dans la colonne Répertoire de la liste des utilisateurs. Pour les utilisateurs définis en interne, le champ n'est pas renseigné.

Name	Status	Roles	Directory	PW Modified	Actions
admin	Enabled	Product Administrator, Security Administrator		2017-09-22T23:09:44Z	<div>Edit Password</div> <div>Edit Roles</div> <div>Delete</div>
ProductAdmin	Enabled	Product Administrator		2017-09-22T23:25:40Z	<div>Edit Password</div> <div>Edit Status</div> <div>Edit Roles</div> <div>Delete</div>
SecurityAdmin	Enabled	Security Administrator		2017-09-22T23:42:22Z	<div>Edit Password</div> <div>Edit Status</div> <div>Edit Roles</div> <div>Delete</div>

Chapitre 8. Événements

MDE inclut un système d'agrégation et de transfert d'événements. Ce système agrège des événements provenant d'agents gérés, ainsi que des événements générés en interne, et les stocke dans un journal des événements interne. De plus, il peut être configuré de manière à transférer des événements à un ou à plusieurs destinataires

Journal des événements

Le journal des événements MDE peut être affiché en sélectionnant l'option de menu Événements dans la barre de menus de niveau supérieur.

[Home](#) > [Events](#) > [Logs](#)

☐ Show Redacted Events Reload Export CSV

Show 10 entries Search:

Sequence	ID	Message	Type	Severity	Timestamp	Source
16	PS000D0005	Requested action change-passw...	SYSTEM	INFO	2017-09-22T23:42:22Z	localhost
15	PS000D0001	User admin has requested action ...	AUDIT	INFO	2017-09-22T23:42:22Z	localhost
14	PS000D0005	Requested action change-user-st...	SYSTEM	INFO	2017-09-22T23:42:21Z	localhost
13	PS000D0001	User admin has requested action ...	AUDIT	INFO	2017-09-22T23:42:21Z	localhost
12	PS000D0005	Requested action change-user-ro...	SYSTEM	INFO	2017-09-22T23:42:21Z	localhost
11	PS000D0001	User admin has requested action ...	AUDIT	INFO	2017-09-22T23:42:21Z	localhost
10	PS000D0005	Requested action change-user-st...	SYSTEM	INFO	2017-09-22T23:36:47Z	localhost
9	PS000D0001	User admin has requested action ...	AUDIT	INFO	2017-09-22T23:36:47Z	localhost
8	PS000D0005	Requested action change-user-ro...	SYSTEM	INFO	2017-09-22T23:35:51Z	localhost
7	PS000D0001	User admin has requested action ...	AUDIT	INFO	2017-09-22T23:35:51Z	localhost

Showing 1 to 10 of 16 entries First Previous 1 2 Next Last

Cette page affiche tous les événements dans une liste séquentielle unique. Chaque événement possède un numéro de séquence, un ID, un message, un type, un niveau de gravité, un horodatage de réception et une source comme défini ci-dessous :

- **Numéro de séquence** - numéro attribué à l'ordre dans lequel l'événement est reçu. Il est unique (même si le même événement se répète) et sera incrémenté dans le temps.
- **ID** - identificateur unique de l'événement. Plusieurs instances du même événement possèdent un ID commun.
- **Message** - texte descriptif identifiant la condition de l'événement. Certains événement peuvent prendre en charge l'insertion de variables afin que, même si l'ID d'événement est commun, il soit possible de modifier légèrement le texte.
- **Type** - décrit si l'origine de l'événement correspond à une action système ou à une action de l'utilisateur. Le type est :
 - **SYSTEME** - événements provenant d'une action MDE automatisée.

- **AUDIT** - événements provenant d'une action utilisateur.
- **Gravité** - indication relative du niveau de conscience de l'événement. Les catégories de gravité sont les suivantes :
 - **INFO** - aucune action n'est nécessaire ; pour information uniquement
 - **AVERTISSEMENT** - aucune action immédiate n'est nécessaire ; il est recommandé de surveiller la condition
 - **CRITIQUE** - une action immédiate est nécessaire
- **Horodatage** - indication de l'heure d'origine d'un événement au format UTC (temps universel coordonné)
- **Source** - nom d'hôte ou adresse IP du système (Agent ou MDE) dont provient l'événement.

La taille du journal des événements de MDE peut être configuré à l'aide de Paramètres avancés. Une fois la taille limite définie atteinte, les événements les plus anciens sont éliminés à mesure que de nouveaux événements arrivent.

Détails d'un événement

Un événement peut avoir des arguments étendus qui ne font pas partie du message d'événement. Dans ce cas, l'événement affichera un lien Détails dans la colonne des messages du journal des événements. Si vous cliquez sur le bouton Détails, vous afficherez les arguments étendus.

34	P600140002	Agent 1 logged off, reason code 1006.	Details		2018-04-10T15:02:05Z	localhost
33	DEC2014	Read/write denied for user3 on /home/data/	Details	Absolute process path: Decision: Deny Group name: user3 Operation: Read or Write	2018-04-10T15:01:19Z	cos5-file
32	DEC2010	Read denied for user4 on /home/data/	Details		2018-04-10T15:01:19Z	cos5-file
31	DEC2011	Write permitted for user1 on /home/development/	Details	AUDIT	INFO	2018-04-10T15:01:19Z

Exportation d'un événement

MDE permet à un administrateur d'exporter la liste des événements en tant que format de fichier CSV à partir du bouton Exporter au format CSV sur la page Événements.

🏠 > Events > Logs

☐ Show Redacted Events

Reload Export CSV

Si vous cliquez sur le bouton Exporter au format CSV, le fichier des événements est téléchargé sur l'ordinateur du client. Chaque ligne du fichier des événements est un événement du journal.

Les colonnes du fichier d'événements sont les suivantes : numéro de séquence d'événement, ID d'événement, indicateur modifié, chaîne de message d'événement (avec arguments omis), type d'événement, gravité d'événement, arguments d'événement, horodateur d'événement et source d'événement.

Transfert d'événements

Chaque événement reçu est transféré à chaque destinataire de l'événement configuré. Les événements sont transférés en même temps qu'ils sont insérés dans le journal des événements interne.

Un administrateur du produit ou un administrateur de la sécurité peut modifier les destinataires de l'événement du produit. Une fois configuré, les événements créés ou reçus par MDE sont transférés au ou aux destinataires. Le type de destinataire pris en charge est Syslog.

Email Recipients

[New Email Recipient](#)

Email	Host	Port	Security	User	Password	Format	Actions
No Recipients							

Syslog Recipients

[New Syslog Recipient](#)

Host	Port	Format	Actions
No Recipients			

MDE prend également en charge plusieurs formats de transfert des événements. Les formats pris en charge sont les suivants : modèles d'événements LEEF (Log Event Extended Format), CEF (Common Event Format) et CADF (Cloud Auditing Data Federation).

Arguments d'événements

En plus de la chaîne normale de message d'événement, des arguments d'événements seront envoyés sous forme de paramètres clé/valeur. Ces paramètres seront identifiés par la chaîne concaténée du préfixe avec “spx” et le nom d'argument. Par exemple, si un événement contient un nom d'utilisateur, la paire clé/valeur de la chaîne peut être “spxuser=user1”.

Événements d'un agent

MDE agrège le système et les événements d'audit de chaque agent géré (et connecté). Ces événements sont affichés dans le journal des événements MDE et sont transférés à des destinataires d'événements configurés.

Important

Il est fortement conseillé que MDE, les bases de données externes et tous les agents utilisent NTP pour coordonner l'heure du système. Cela permet de s'assurer que les horodatages du journal des événements/d'audit sont séquencés correctement.

Événements fiables

Les événements envoyés par un agent individuel à MDE sont gérés en temps réel. Cela permet de s'assurer que, si vous vouliez un événement, MDE recontacte l'agent, demande l'événement oublié et l'insère dans le journal des événements dans l'ordre approprié.

Chapitre 9. Gestion des clés d'application des règles

Un administrateur de la sécurité peut définir des clés d'application des règles pour le stockage sécurisé dans MDE. Ces clés peuvent être associées à des types de données et à des volumes pour sécuriser des données et permettre un contrôle d'accès cryptographique.

🏠 > Keys > Managed Keys

Submit Rotation Job				New Key
ID	Name	Created	Notes	Actions
1	Key1	2017-09-22T23:49:12Z		Edit Submit Revocation Job
2	Key2	2017-09-22T23:49:17Z		Edit Submit Revocation Job
3	Key3	2017-09-22T23:49:23Z		Edit Submit Revocation Job

Ajout d'une clé

Lors de l'ajout d'une nouvelle clé, vous devez entrer un nom unique. Les noms de clé ne dépendent pas des minuscules/majuscules. La valeur de la clé n'est pas exposée et ne peut pas être modifiée par un utilisateur. Le champ Remarques est facultatif.

ID	Name	Created	Notes	Actions
	<input type="text"/>		<input type="text"/>	Save Cancel

Important

Les noms de clé peuvent être modifiés, mais la valeur réelle de la clé ne peut pas être modifiée par un utilisateur.

Les clés peuvent être créées sur la page 'Clés' ou dans l'assistant de création d'agent. Toutes les clés "définies par le système" créées dans l'assistant de création d'agent sont générées automatiquement et ne peuvent pas être gérées. Les clés ne peuvent être modifiées que dans la page Clés.

Modification d'une clé

Après avoir créé une clé, l'administrateur de la sécurité peut modifier le nom d'une clé. La modification du nom de clé ne modifie pas les valeurs de clé sous-jacentes actuelles. Le champ Remarques peut lui aussi être modifié.

Rotation de clé

MDE permet à l'administrateur de la sécurité d'effectuer la rotation des clés dans l'écosystème de l'agent. Dans la page Clés, cliquez sur le bouton Envoyer une tâche de rotation de clé.

Vous êtes invité à transférer une clé publique. Cette clé est utilisée pour chiffrer le dépôt des clés pour la clé qui a fait l'objet d'une rotation. Sélectionnez une clé appropriée, ajoutez la clé et cliquez sur Suivant.

Remarque critique

La clé SSL doit être encodée par RSA et PEM.

Key Rotation



This wizard will assist you in selecting keys to be scheduled for rotation. Once the keys are selected, a job to rotate the keys will be queued for approval.

Upload Public Key

Browse...

No file selected.

Add Public Key

Public Key

Next

Une liste de toutes les clés créées par l'utilisateur s'affiche. L'administrateur de la sécurité peut sélectionner un nombre quelconque de clés faisant l'objet d'une rotation.

Key Rotation



Select one or more keys from the list of all keys:

☒ Key1

☐ Key2

☐ Key3

Back

Next

Lorsque vous avez sélectionné la ou les clés souhaitées, une tâche est créée.

Remarque critique

Si une clé est associée à plusieurs agents, tous les agents qui utilisent cette clé seront concernés.

Lors de l'approbation d'une tâche, tous les agents concernés seront avertis de la rotation de la clé. La tâche continue à s'exécuter tant que tous les agents concernés n'ont pas terminé le processus de rotation de la clé. En fonction du nombre d'agents concernés, cette tâche peut prendre longtemps.

Important

Lorsque vous utilisez un magasin de clés externe, il doit être **en ligne** pour que la rotation de clé fonctionne. Si une erreur se produit, assurez-vous que le magasin de clés externe est en ligne et redémarrez le serveur PPM ou redémarrez le service PPM (spds).

Révocation de clé

La révocation de clé supprime une clé de MDE et place cette clé dans un dépôt. La révocation de clé ne peut être effectuée que sur une clé qui n'est pas associée actuellement à une règle active. Avant de révoquer une clé, l'administrateur de la sécurité doit supprimer les règles qui font référence à cette clé.

La suppression du chemin d'accès qui utilise la clé d'une association de règles de l'agent ne déchiffre pas les données sur le disque. Par conséquent, si l'accessibilité aux données est souhaitée, les données doivent être migrées du répertoire protégé avant la suppression d'une règle associée à ce chemin d'accès.

Une fois la révocation terminée, les données restantes au chemin d'accès protégé sont inaccessibles. La clé révoquée est stockée dans un dépôt et supprimée de l'opération normale de PPM.

AVERTISSEMENT

L'administrateur de la sécurité doit mettre à jour la règle de l'agent pour dissocier la clé ciblée de tous les agents avant de révoquer cette clé. Reportez-vous à la section "Modification d'un agent" pour plus d'informations sur la suppression d'un chemin.

Broyage de clé

Le broyage de clé fonctionne comme la révocation de clé. Cependant, une fois l'opération de broyage de clé terminée, la clé n'est pas placée dans un dépôt, rendant les données définitivement inaccessibles.

Important

Cette fonction est uniquement disponible via l'API REST, reportez-vous à la documentation de l'API REST pour plus de détails.

Clés auto-générées

Si un administrateur de la sécurité ne souhaite pas gérer les clés d'application des règles, MDE peut générer automatiquement une clé pour chaque règle qui vient d'être créée. Les clés auto-générées sont toujours uniques lorsqu'elles sont créées et ne sont pas visibles sur la page de gestion des clés.

Remarque critique

Les clés auto-générées ne peuvent pas faire l'objet d'une rotation ou d'une révocation. Si vous souhaitez faire pivoter ou révoquer des clés, utilisez des clés nommées.

Magasin de clés externe

Les clés peuvent être stockées à l'un des deux emplacements suivants : base de données sécurisée interne ou magasin de clés externe. MDE est initialement configuré de manière à n'utiliser que la base de données sécurisée interne. Si l'administrateur de la sécurité envisage d'utiliser un magasin de clés externe, un magasin doit être configuré. Les magasins de clés externes ne sont utilisés que pour la protection des clés. La gestion des clés pour les magasins de clés externes doit être effectuée par le biais de MDE.

Important

Le fournisseur du magasin de clés externe transmet les instructions de configuration du magasin de clés externe.

Magasins de clés KMIP

Pourquoi et quand exécuter cette tâche

Un administrateur de la sécurité doit transférer un magasin de clés Java et un magasin de clés de confiance Java. Pour créer un magasin de clés Java et un magasin de clés de confiance Java, suivez cette procédure :

Procédure

1. Regroupez le fichier de certificat client et un fichier de clé privée du client au format PKCS12 (Public Key Cryptography Standard #12). Dans les étapes suivantes, nous y ferons référence par "client.p12". (Voir l'[Annexe C, «Exemple de conversion pour créer un fichier PKCS12»](#), à la page 89 pour obtenir un exemple de combinaison d'un certificat client et d'une clé privée de client dans un fichier au format PKCS12.
2. Regroupez un fichier de certificat d'autorité de certification public. Dans les étapes suivantes, nous ferons référence à ce fichier par "sklm_ca.pem".

[user@localhost]\$ keytool -importkeystore -srckeystore client.p12 -keystore client.jks -storetype JKS

3. Importez le fichier PKCS12 dans un nouveau magasin de clés Java :

Remarque critique

Au cours de cette étape, vous devrez indiquer un mot de passe. Conservez ce mot de passe pour la suite.

[user@localhost]\$ keytool -v -list -keystore client.jks

4. Obtenez l'alias du fichier :
5. Importez le fichier de certificat de l'autorité de certification dans un nouveau magasin de clés de confiance Java :

```
[user@localhost]$ keytool -import -trustcacerts -alias sklm  
-file sklm_ca.pem -keystore sklmtrust.jks
```

Remarque critique

Au cours de cette étape, vous devrez indiquer un mot de passe. Conservez ce mot de passe pour la suite.

6. Obtenez l'alias du fichier :

keytool -v -list -keystore trust.jks

Voici les paramètres à renseigner pour que le magasin de clés externe soit actif :

- **Nom** - Référence au magasin de clés externe définie par l'utilisateur
- **Etat** : indique à MDE que le magasin de clés externe défini doit remplacer le magasin de clés actif actuel. Si l'état est *actif*, MDE commence à utiliser le magasin de clés. Si l'état est *inactif*, MDE n'utilise plus le magasin de clés.
- **Hôte** : adresse IP du magasin de clés externe.
- **Port** - Numéro de port du magasin de clés externe.
- **Magasin de clés du client**
 - **Alias de magasin de clés** - Alias du magasin de clés collecté.
 - **Fichier du magasin de clés** - Fichier du magasin de clés Java.
 - **Mot de passe associé au magasin de clés du client** - Mot de passe configuré lors de la création du magasin de clés.
- **Magasin de clés de confiance**
 - **Alias du magasin de clés de confiance** - Alias du magasin de clés de confiance collecté.
 - **Fichier du magasin de clés de confiance** - Fichier du magasin de clés de confiance Java.
 - **Mot de passe associé au magasin de clés de confiance** : mot de passe configuré lors de la création du magasin de clés de confiance.
- **Est principal** - Identifie le magasin de clés externe utilisé comme magasin de clés principal pour toutes les opérations de lecture et d'écriture
 - La valeur par défaut est "true" pour le premier magasin de clés défini.
 - S'il n'est pas sélectionné, il est traité comme un magasin de clés "clone" et n'est utilisé que pour les opérations de lecture.
 - Un seul magasin de clés externe peut être désigné comme principal.

KMIP Keystore

New KMIP Keystore

Name	State	Host	Port	Client Keystore	Truststore	Is Master	Actions
<input type="text"/>	In: <input type="button" value="v"/>	<input type="text"/>	5696 <input type="button" value="v"/>	Alias <input type="text"/> Keystore Password <input type="text"/>	Alias <input type="text"/> Truststore Password <input type="text"/>	<input type="checkbox"/>	<input type="button" value="Save"/> <input type="button" value="Cancel"/>
				Keystore Upload <input type="button" value="Browse..."/> No file selected. <input type="button" value="Upload"/>	Truststore Upload <input type="button" value="Browse..."/> No file selected. <input type="button" value="Upload"/>		

Important

Actuellement, MDE prend en charge un produit de magasin de clés externe : IBM Security Key Lifecycle Manager (SKLM) configuré pour KMIP.

Outils HSM (Hardware Security Module)

Pourquoi et quand exécuter cette tâche

Lorsque vous utilisez un outil HSM en tant que magasin de clés externe, vous devez vous assurer que le produit tiers est entièrement configuré et opérationnel conformément aux instructions du fabricant.

Le logiciel client de version 64 bits de l'outil HSM doit être copié vers la machine virtuelle MDE par l'administrateur produit de la console PPM. Ce logiciel doit être extrait et installé à l'aide de l'option SDK et des instructions du fabricant de l'outil HSM pour configurer la communication.

Un utilitaire fourni avec le logiciel client ou un utilitaire connu pour fonctionner avec l'outil HSM permet de créer une clé d'encapsulation. Une clé d'encapsulation est une clé symétrique de 256 ko qui doit être disponible pour une utilisation avec PPM.

Lorsque cette clé d'encapsulation symétrique est créée sur l'outil HSM, un descripteur lui est affecté. Ce descripteur est nécessaire lors de la configuration de l'outil HSM dans la page de l'interface graphique PPM. PPM transmet ce descripteur et la clé de règle à l'outil HSM pour l'encapsulation de la clé de règle et l'outil HSM renvoie la clé encapsulée afin qu'elle soit stockée dans la base de données PPM.

Après l'installation et la configuration du logiciel, assurez-vous que PPM peut communiquer avec l'outil HSM et redémarrez la machine virtuelle PPM.

Dans l'écran Magasins de clés externes, sélectionnez Nouveau magasin de clés HSM.

🏠 > Keys > External Keystores

HSM Keystore

[New HSM KeyStore](#)

Name	State	HSM Token	Key Handle	HSM Password	Actions
No External Keystores					

KMIP Keystore

[New KMIP KeyStore](#)

Name	State	Host	Port	Client Keystore	Truststore	Is Master	Actions
No External Keystores							

Les paramètres suivants doivent être renseignés pour activer un magasin de clés externe :

- **Nom** - Référence au magasin de clés externe définie par l'utilisateur
- **Etat** - Définit l'état prévu pour le magasin de clés
- **Jeton HSM** - HSM utilise le numéro d'emplacement de la partition
- **Descripteur de clé** - Descripteur affecté à la clé qui sera utilisée pour encapsuler les clés de règle
- **Mot de passe HSM** - Mot de passe associé à la partition utilisée par le client.

HSM Keystore

[New HSM KeyStore](#)

Name	State	HSM Token	Key Handle	HSM Password	Actions
<input type="text"/>	Inactive <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Save"/> <input type="button" value="Cancel"/>

Remarque : Produit HSM pris en charge : HSM SafeNet® Luna configuré pour un magasin de clés HSM.

Chapitre 10. Définition de règle au niveau d'un fichier

MDE permet à l'administrateur de la sécurité de définir un contrôle (opérationnel et cryptographique) au niveau d'un fichier sur différents types de données. Les termes ci-dessous sont utilisés lors de la définition d'un contrôle des données au niveau d'un fichier.

- **Sélecteurs** - liste non ordonnée d'utilisateurs et de groupes qui définit qui doit être autorisé à accéder une ressource (ou ensemble de chemins). En option, un processus défini peut être identifié comme un autre composant pour un sélecteur.
- **Ensembles de chemins** - liste des chemins de fichiers à protéger par une règle
- **Types de données** - liste ordonnée de lignes de définition d'accès affectées à un type de données spécifié. Chaque ligne comprend un sélecteur, une opération d'E-S (lecture/écriture) et une action de règle.
- **Processus** - chemin de fichier vers un exécutable. Utilisé dans un sélecteur pour définir des contrôles d'accès avec un exécutable identifié. Facultatif pour un meilleur contrôle d'accès.

Une fois qu'un type de données a été créé, il peut être associé à un ou plusieurs agents mis en service. Les sections ci-dessous décrivent la configuration d'une règle.

Sélecteurs

Un sélecteur est un objet de règle qui définit un ensemble d'utilisateurs et / ou de groupes d'utilisateurs via une ou plusieurs lignes de sélecteur. Lorsque vous ajoutez un nouveau sélecteur, l'administrateur de la sécurité doit indiquer un nom avant d'enregistrer. Les remarques et les lignes du sélecteur peuvent être ajoutées à tout moment en modifiant le sélecteur.

Chaque ligne de sélecteur contient les champs suivants : Utilisateur, Groupe, Processus. L'un des champs doit être rempli avant d'être sauvegardé.

- **Utilisateur** - nom abrégé d'un utilisateur défini par le système cible. Cette valeur est mise en correspondance avec un utilisateur du système d'exploitation de l'Agent cible. Il est facultatif.
- **Groupe** - nom abrégé d'un système cible ou d'un groupe d'utilisateurs défini LDAP. Cette valeur est mise en correspondance avec un groupe d'utilisateurs du système d'exploitation de l'Agent cible. Il est facultatif.
- **Processus** - référence à un nom de processus défini par le produit. Cette valeur correspond au chemin du fichier de processus (et aux valeurs de hachage facultatives) dans le système d'exploitation de l'Agent cible. Il est facultatif.

🏠 > Policy > Selectors

Expand All Collapse All Search Clear New Selector

Name: Save Cancel Add New Row

Notes

User	Group	Process	Actions
<input type="text" value="user01"/>	<input type="text"/>	<input type="text"/>	Delete Row

Les valeurs de chaque ligne de sélecteur sont combinées à l'aide d'un opérateur logique AND. Si plusieurs champs sont définis sur une ligne unique, tous les champs doivent correspondre pour la ligne à faire

correspondre. Un sélecteur correspond si l'une des lignes définies correspond. Le tri des lignes dans un sélecteur n'a pas d'impact sur l'algorithme de correspondance des règles.

Utilisateur	Groupe	Processus	Comportement de correspondance d'agent
✓			Correspond à l'utilisateur
	✓		Correspond à n'importe quel utilisateur du groupe défini
		✓	Correspond au chemin de processus défini et se limite potentiellement aux valeurs de hachage fournies
✓	✓		Correspond à l'utilisateur uniquement s'il agit en tant que membre du groupe défini
✓		✓	Correspond à l'utilisateur uniquement s'il agit via le processus défini
	✓	✓	Correspond à un utilisateur du groupe défini uniquement s'il agit via le processus défini
✓	✓	✓	Correspond à l'utilisateur uniquement s'il agit en tant que membre du groupe défini et agit via le processus défini avec le processus

Important

La résolution des groupes et/ou utilisateurs par le sélecteur fonctionne avec le serveur Active Directory ou le serveur LDAP externe configuré sur lequel l'agent de fichier est installé.

Ensembles de chemins

Un ensemble de chemins est une collection comprenant une ou plusieurs lignes de chemin d'accès à un fichier. Lors de l'ajout d'un ensemble de chemins, l'administrateur de la sécurité doit indiquer un nom pour l'ensemble de chemins. Pour ajouter une ligne à l'ensemble de chemins d'accès, cliquez sur le bouton "Ajouter un chemin". Chaque ligne contient un chemin d'accès à un fichier et des remarques.

🏠 > Policy > Path Sets

Expand All Collapse All

Search

▶ Name:

Notes

Path	Notes	Actions
<input type="text" value="/protected"/>	<div style="border: 1px solid #ccc; height: 30px;"></div>	<input type="button" value="Delete Path"/>

L'administrateur de la sécurité doit indiquer un chemin d'accès à un fichier. La protection est récursive du chemin d'accès vers les sous-répertoires éventuels. Le champ Remarques est facultatif.

Types de données

Un type de données est une collection ordonnée de définitions de ligne de type de données, qui permet le contrôle des données d'accès opérationnel et/ou cryptographique au niveau du fichier. Chaque type de données contient un nom, une clé d'application des règles, des remarques à l'intention de l'utilisateur et une liste ordonnée de lignes.

- **Nom** - référence définie par l'utilisateur au type de données.
- **Remarques à l'intention de l'utilisateur** - champ Remarques défini par l'administrateur de la sécurité.

Ligne de type de données

Chaque ligne de type de données contient les champs suivants : ordre, sélecteur, opération et action.

- **Ordre** - priorité selon laquelle chaque ligne de règle est vérifiée. La première ligne correspondante est utilisée. Ce champ est obligatoire, mais ne s'affiche pas si une seule ligne est présente.
- **Sélecteur** - sélection de sélecteurs définis précédemment. La ligne de règle correspond si l'une des lignes du sélecteur correspond. Ce champ est obligatoire. MDE fournit un sélecteur "Tout sélectionner" correspondant à un utilisateur.
- **Opération** - sélection d'opérations sur les fichiers qui peuvent être effectuées. Les options sont Lecture et Lecture-écriture. Ce champ est obligatoire.
- **Action** : sélection des actions d'accès associées à l'opération. Les options sont Autoriser, Refuser, Autoriser et journaliser et Refuser et journaliser. Ce champ est obligatoire.

Variables de ligne de type de données

Les champs Sélecteur, Opération et Action peuvent éventuellement être définis de manière à être variable. Cela permet à un administrateur de la sécurité de créer des modèles pour un type de données effectué lors de la création d'un agent. Les paramètres de champ disponibles sont les suivants : Peut être modifié, Doit être modifié et Ne peut pas être modifié.

Peut être modifié

Le contenu de ce champ peut être remplacé lors de la création d'un agent.

Doit être modifié

Ce champ doit être défini lors de la création d'un agent.

Non modifiable

Ce champ doit être défini lors de la création du type de données et ne peut pas être modifié lors de la création de l'agent.

Create/Edit Datatype

Name

Notes

Rules

Order	Selector	Operation	Actions	Delete
1 ▾	<div>Not Editable ▾</div> <div>Selector1 <input type="checkbox"/> Select All</div>	<div>Not Editable ▾</div> <div>Read or Write ▾</div>	<div>Not Editable ▾</div> <div>Permit ▾</div>	<div>Delete</div>
▴ 2	<div>Not Editable ▾</div> <div><input checked="" type="checkbox"/> Select All</div>	<div>Not Editable ▾</div> <div>Read or Write ▾</div>	<div>Not Editable ▾</div> <div>Deny, Log ▾</div>	<div>Delete</div>

Add New Row

Save

Cancel

Un type de données ne peut pas être enregistré tant que toutes les lignes ne comportent pas des valeurs et/ou un paramètre de variable.

Processus

Un processus identifie un chemin de système de fichiers vers un exécutable. Un processus est composé des champs suivants :

- **Nom** - nom du processus
- **Chemin d'accès** - chemin absolu vers un exécutable du système de fichiers
- **Système d'exploitation** - champ utilisé pour référencer le type de système d'exploitation (Linux, Windows, AIX).
- **Version** - champ utilisé pour la version du système d'exploitation.
- **Distribution** - champ utilisé pour le nom de la distribution du système d'exploitation (Red Hat, CentOS, Windows, AIX).

🏠 > Policy > Processes

Expand All Collapse All

Search

Clear

New Process

▸ Name

Save Cancel Add Hash

Path	OS	Version	Distribution
<input type="text" value="/user/bin/cat"/>	<div>Linux ▾</div>	<input type="text" value="6.7"/>	<div>CentOS ▾</div>

Hash

Actions

42 IBM Multi-Cloud Data Encryption Technologie SPx® : Guide d'administration

Un processus peut être défini en tant que chemin de fichier uniquement ou avec une liste de valeurs de hachage de processus. Lorsqu'une ou plusieurs valeurs de hachage sont définies, la correspondance de processus est limitée aux hachages répertoriés.

Important

Les valeurs de hachage de processus sont générées via un outil d'agent et doivent être copiées dans PPM. L'outil génère une valeur de hachage pour la version en cours de l'exécutable.

`spxhash -p <chemin vers l'exécutable>`

Exemple :

```
[root@blkdr ~]# spxhash -p /usr/bin/vim
```

```
1202E81EF41273904A6DD381C35B2561F838F7E35B6B26959F8EEB646297A36A7C2
```


Chapitre 11. Mise en service et gestion des agents

MDE prend en charge quatre types d'installation d'agent : Volume, Fichier avec une règle, Volume avec une règle et Magasin d'objets. Chaque type d'agent permet une méthode de protection des données différente.

- **Volume** - l'agent protège les données au niveau d'une unité par bloc.
- **Fichier avec une règle** - l'agent protège les données au niveau du fichier et fournit des règles de contrôle d'accès opérationnel basées sur un fichier.
- **Volume avec une règle** - l'agent protège les données au niveau d'une unité par bloc et fournit également des règles de contrôle d'accès opérationnelles basées sur un fichier.
- **Magasin d'objets** - l'agent protège les données envoyées au stockage d'objets

Ajout d'un agent

Pour ajouter un agent, un administrateur de la sécurité doit accéder à la page Agents de MDE et cliquer sur la liste déroulante Ajouter un agent. Les options d'agent disponibles s'affichent.



Après avoir sélectionné le type d'agent, un assistant s'ouvre pour vous permettre de créer l'agent.

Remarque : Il est recommandé d'ajouter tous les composants de la règle souhaités (Sélecteurs, Ensembles de chemins, Clés, Types de données et Processus) avant de démarrer le processus d'ajout d'agent car ces composants ne peuvent pas être créés pendant le processus.

La mise à disposition d'un agent comporte six sections : Identité d'agent, Information réseau, Règle, Volumes, Utilisateurs autorisés et Outils. Avant de pouvoir ajouter l'agent, toutes les sections obligatoires doivent être renseignées.

Identité

La section Identité nécessite que l'administrateur de sécurité définisse un nom, un identificateur unique universel, un système d'exploitation et des remarques.

The screenshot shows the 'Add File With Policy Agent' wizard. It has a title bar with a close button. The main area is divided into two columns. The left column has two sections: 'Required' and 'Optional'. Under 'Required', there are two radio buttons: 'Agent Identity' (selected) and 'Network Information'. Under 'Optional', there are three radio buttons: 'Policy', 'Authorized Users', and 'Tools'. The right column has four fields: 'Name *' (text input), 'UUID *' (text input with the value '9a5db4d2-0bd2-430b-841d-4cc122a152dd' and a refresh icon), 'Operating System *' (dropdown menu), and 'Notes' (text area). A 'Next' button is at the bottom right.

- **Nom** - référence définie par l'utilisateur pour l'agent.
- **UUID** - identificateur unique utilisé par MDE pour identifier l'agent.

- **Système d'exploitation** - système d'exploitation de l'agent cible.
- **Remarques** - remarques de l'administrateur de la sécurité sur cet agent.

Une fois que tous les champs obligatoires sont renseignés, cliquez sur **Sauvegarder** pour passer à l'étape suivante.

Remarque :

- MDE renseigne automatiquement l'identificateur unique universel mais l'administrateur de sécurité peut le remplacer, s'il le souhaite.
- Les champs obligatoires sont indiqués dans l'interface utilisateur.
- Les noms des agents ne sont pas uniques. C'est pourquoi, si vous utilisez le même nom pour plusieurs agents, la messagerie de journal d'événements peut mal représenter la source de message.

Réseau

L'étape Réseau implique que l'administrateur de la sécurité définisse le nom d'hôte ou l'adresse IP de l'agent et du MDE ainsi que les certificats nécessaires à l'établissement d'une connexion sécurisée entre MDE et l'agent cible.

- **Adresse IP**- adresse IP ou nom d'hôte du serveur sur lequel l'agent est installé.
- **Adresse IP de l'homologue MDE** - adresse IP ou nom d'hôte du MDE, tel qu'il apparaît sur l'instance de serveur de l'agent cible.

Remarque : MDE renseigne automatiquement l'adresse IP de l'homologue MDE, mais l'administrateur de sécurité peut la modifier au besoin.

- **Certificats** - liste des certificats transféré utilisés pour établir une connexion sécurisée entre MDE et l'agent installé. Ce certificat est utilisé pour établir une connexion TLS1.2 mutuellement authentifiée entre l'agent et PPM de MDE.

Pour télécharger un certificat, l'administrateur de sécurité doit cliquer sur **Ajouter un certificat**, accéder au certificat souhaité et l'ouvrir. Il s'affichera dans l'écran Nouvel agent - Réseau.

Remarque : L'agent et PPM ne communiquent pas et l'agent ne chiffre pas les données et n'applique pas les règles si les certificats du magasin de clés et du magasin de clés de confiance n'ont pas été transférés dans MDE et que le certificat correspondant n'est pas affecté à l'agent. Reportez-vous à la section "Paramètres du certificat serveur" pour plus de détails.

Une fois que tous les champs sont renseignés, cliquez sur **Suivant** pour passer à l'étape suivante.

Création d'un agent de type Fichier avec une règle, Volume avec une règle et Volume

L'étape Règle implique que l'administrateur de la sécurité définisse les contrôles opérationnels et cryptographiques sur les chemins d'accès aux fichiers sur l'agent ciblé.

Ajout d'un chemin d'accès

Les agents de type Fichier avec une règle et Volume avec une règle peuvent ajouter une définition de chemin d'accès à la règle d'agent. Chaque chemin d'accès ajouté protège un chemin d'accès à un fichier ou un regroupement de chemins d'accès à des fichiers sur l'agent ciblé. C'est l'administrateur de la sécurité qui définit le nombre de chemins d'accès ajoutés.

Remarque critique

- **Les chemins protégés via une règle doivent exister au moment de l'application de la règle, faute de quoi l'application de la règle échoue.**
- **Les fichiers et sous-répertoires existants doivent être traités manuellement avec la commande `spxconvert` disponible après l'installation de l'Agent de type Fichier avec une règle. La règle est en vigueur même si les fichiers ne sont pas chiffrés.**
- **Les nouveaux fichiers et répertoires ajoutés après l'installation sont automatiquement chiffrés et protégés via une règle.**

Add File With Policy Agent

Required

- ✓ Agent Identity
- ✓ Network Information

Optional

- ⊙ **Policy**
- Authorized Users
- Tools

Add Path

Back Next

Pour ajouter un chemin d'accès, cliquez sur **Ajouter un chemin d'accès**.

Chaque chemin d'accès ajouté implique de saisir un chemin d'accès à un fichier (ou un ensemble de chemins), une clé et un type de données.

Add File With Policy Agent

Required

- ✓ Agent Identity
- ✓ Network Information

Optional

- ⊙ **Policy**
- Authorized Users
- Tools

*** Required**

File Policy Path (or Path Set) *

/home/data Delete

Storage

- ⊙ Local
- Network

Key

- System Defined
- ⊙ User Defined

Name

User Defined Key

Datatype *

testDT

(remember to fill out any empty values below)

Selector	Operation	Actions
Select All	Read or Write	Permit

Add Path

Back Next

- **Chemin d'accès (ou ensemble de chemins d'accès) aux règles concernant les fichiers** - identifie le chemin ou le groupe de chemins que la définition de contrôle d'accès du type de données identifié doit protéger. La protection est réursive du chemin d'accès au fichier indiqué vers les sous-répertoires éventuels.
- **Stockage** – Identifie l'emplacement du chemin d'accès au fichier. Les options sont Local ou Réseau. Si Réseau est sélectionné, des paramètres additionnels doivent être entrés pour configurer correctement le stockage réseau. (Voir les informations de configuration ci-dessous)
- **Clé** - clé utilisée pour chiffrer des chemins associés au type de données. Vous pouvez utiliser un clé définie précédemment par l'utilisateur ou la clé définie par le système gérée par MDE. Ce champ peut être affiché ou non selon si Fichier avec une règle ou Volume avec une règle est utilisé (voir Remarque).
- **Type de données** - sélection d'un type de données précréé. Une fois sélectionné, les informations du type de données sont ajoutées en ligne. Si un type de données avec des variables est utilisé, les variables doivent être saisies avant l'enregistrement.

Remarque :

- Si vous utilisez un ensemble de chemins, vous devez le créer avant d'ajouter le nouvel agent. Faute de quoi, un seul chemin manuel peut être défini.
- Le type de données utilisé doit être créé avant d'ajouter le nouvel agent.
- Si le nouvel agent est de type Volume avec une règle, les Ensembles de chemins ne contiennent pas de clés d'application des règles, car c'est la définition d'une règle de volume qui assure la protection.

Configuration de la mémoire locale

Si vous utilisez la mémoire locale lors de la définition de votre chemin d'accès aux règles de fichiers, sélectionnez l'option **Mémoire locale**. Ceci indiquera à l'agent de protéger le chemin d'accès au fichier absolu défini (ou l'ensemble de chemins). Aucun paramètre additionnel n'est requis.

Configuration du stockage réseau

Si vous utilisez le stockage réseau lorsque vous définissez votre chemin d'accès aux règles concernant les fichiers, sélectionnez l'option "Stockage réseau". Ceci indiquera à l'agent de monter le stockage réseau défini sur le chemin d'accès au fichier absolu défini. Les ensembles de chemins ne peuvent pas être utilisés dans le cas d'un stockage défini sur le réseau. Des paramètres additionnels sont requis.

Le stockage réseau nécessite la définition du protocole, du nom d'hôte et de l'adresse IP, le partage, le nom d'utilisateur, le mot de passe et les options de montage avancées.

- **Protocole** – identifie le type de stockage réseau utilisé. Les options sont : NFSv4, NFSv3
- **Nom d'hôte/Adresse IP** – Nom d'hôte et adresse IP du système de stockage réseau
- **Partage** – Emplacement d'exportation du système de fichier réseau
- **Nom d'utilisateur** – (non requis pour NFSv3) Nom d'utilisateur pour l'authentification dans le système de fichiers réseau
- **Mot de passe** - (non requis pour NFSv3) Mot de passe d'authentification dans le système de fichiers réseau
- **Options de montage avancées** – Options séparées par des virgules à appliquer à la définition NFS

Une fois que tous les champs obligatoires sont renseignés, cliquez sur **Suivant** pour passer à l'étape suivante.

Volumes

Ajout d'un volume

Pourquoi et quand exécuter cette tâche

Les agents de type Volume et Volume avec une règle peuvent ajouter une ou plusieurs définitions de volume à la règle de l'agent. Chaque volume ajouté est une nouvelle unité par bloc protégée sur l'agent ciblé.

Add Volume With Policy Agent

Required

- ✓ Agent Identity
- ✓ Network Information

Optional

- ☐ Policy
- ☒ **Volumes**
- ☐ Authorized Users
- ☐ Tools

Volumes [Delete]

Device Label []

Key [] ☐ Autogenerate Key Required

[Add Volume]

[Back] [Next]

Pour ajouter un volume, cliquez sur **Ajouter un volume**. Chaque volume ajouté nécessite d'entrer un libellé d'unité sous-jacent et une clé d'application de la règle.

- **Libellé de l'unité** - identifie l'unité protégée. Une fois que la règle est déployée sur un agent, le libellé de l'unité doit être associé au volume en exécutant la commande `spxdevice` (voir la section *Installation d'un agent*).
- **Clé** - clé utilisée pour chiffrer le volume. Vous pouvez utiliser une clé définie précédemment ou la clé auto-générée gérée par MDE.

Remarque critique

Si vous n'utilisez pas l'option "Générer automatiquement la clé", vous devez définir la clé d'application de règle ajoutée avant d'ajouter l'agent. Voir la section *Gestion des clés d'application des règles*.

Une fois que tous les champs obligatoires sont renseignés, cliquez sur **Suivant** pour passer à l'étape suivante.

Création d'un agent de type Magasin d'objets

L'agent de type Magasin d'objets (ou agent OSA) de MDE agit en tant qu'intermédiaire entre un client et le stockage d'objets du backend. Les clients de stockage d'objets se connectent à l'agent OSA à l'aide des données d'identification de compartiment au lieu des données d'identification du stockage d'objets du backend.

Les administrateurs peuvent configurer l'agent OSA pour se connecter à un ou plusieurs fournisseurs de stockage d'objets. L'agent OSA chiffre et contrôle la règle sur les données envoyées via l'OSA au stockage d'objet du backend configuré. Si plusieurs backends sont configurés, les données sont réparties et des fragments de données sont envoyés à chaque backend.

Certificats front-end

Les agents de type Magasin d'objets ont besoin de la configuration d'un certificat pour établir une connexion sécurisée entre le client de type Magasin d'objets et l'agent de type Magasin d'objets.

Pour télécharger un certificat, l'administrateur de sécurité doit cliquer sur le bouton “Ajouter un certificat”, accéder au certificat souhaité et l'ouvrir.

Add Object Store Agent

Required

☒ Agent Identity

☒ Network Information

Optional

☒ Front-End Certificates

☐ Bucket Credentials

☐ Buckets

☐ Backends

☐ Authorized Users

☐ Tools

Front-End Certificate

Add Certificate

Subject	CN=localhost,OU=Development,O=Security First Corp.,L=Rancho Santa Margarita,ST=California,C=US
Fingerprint	e9cf021f7092bec53ec27ba29467b2d3e70b2b2e1d5ed6acd738af363860b2bd
Expiry	2016-11-09T23:11:06Z
Private Key	False

Back

Next

Une fois que tous les champs obligatoires sont renseignés, cliquez sur “Suivant” pour passer à l'étape suivante.

Données d'identification du compartiment

MDE peut être configuré pour communiquer avec plusieurs fournisseurs de stockage d'objets. Chaque fournisseur nécessite la configuration d'un compartiment et des données d'identification de compartiment.

Add Object Store Agent

Required

☒ Agent Identity

☒ Network Information

Optional

☒ Front-End Certificates

☒ Bucket Credentials

☐ Buckets

☐ Backends

☐ Authorized Users

☐ Tools

* Required

QHW1UOGRU90BFNYZQ0CH

Delete

Key ID *

QHW1UOGRU90BFNYZQ0CH

API Key *

78dKnlcLBIUkQgl6OLjtBKqNogIzW54S6g5SSiik5JX0wOvZ0xolIZoTa=PGKK3B

Protocol *

IBM S3

XH2BW34YV12A0REPF3TW

Delete

Key ID *

XH2BW34YV12A0REPF3TW

API Key *

3AoMJ9fXv3p1xpU8xoAqfSt=DoEaX=3iY7UOyVn3ovUAQ4ssKAbQQvAv1jmHPeXh

Protocol *

AMZ S3

New Credential

Back

Next

Pour ajouter un nouvel ensemble de données d'identification, cliquez sur le bouton "Nouvelles données d'identification".

Les données d'identification du compartiment nécessitent la définition de l'ID de clé, de la clé d'API et du protocole.

- **ID clé** – Identification de l'accessoire de magasin d'objets

- **Clé d'API** – Mot de passe de type chaîne à fournir à l'API S3 pour la corrélation à l'ID de clé
- **Protocole** – Identification du protocole utilisé pour communiquer avec le fournisseur de stockage d'objets (Swift, IBM S3 et Amazon S3).

MDE générera un appariement ID de clé - clé d'API. Les administrateurs peuvent remplacer ces valeurs générées s'ils le souhaitent. Un administrateur devra sélectionner le protocole souhaité parmi les fournisseurs de stockage d'objets pris en charge.

Une fois que tous les champs obligatoires sont renseignés, cliquez sur “Suivant” pour passer à l'étape suivante.

Compartiments

MDE définit une politique de stockage d'objet via l'association de compartiments. Pour chaque compartiment, vous devez définir : Nom, Consigner les refus et Règle.

Add Object Store Agent

Required

- ✓ Agent Identity
- ✓ Network Information

Optional

- ✓ Front-End Certificates
- ✓ Bucket Credentials
- ⊙ **Buckets**
- Backends
- Authorized Users
- Tools

Bucket Name * testBucket Delete

Log Denials ☒

Policy

Key ID *	Access *	Log	Actions
XH2BW34YV12A0REPF3TW	Read or Write ▾	<input checked="" type="checkbox"/>	Delete
QHW1UOGRU90BFNYZQ0CH	Read or Write ▾	<input checked="" type="checkbox"/>	Delete

New Row

New Bucket

Back Next

- **Nom** – Nom du compartiment de stockage d'objets
- **Consigner les refus** – Sélection d'une case à cocher. Si la case est cochée, l'agent OSA créera des journaux d'audit pour accéder aux refus.
- **Règle** – Définition des contrôles d'accès aux compartiments. La règle peut comprendre plusieurs lignes. Chaque ligne de la définition de règle nécessite : ID clé, Accès, Journal,
- **ID clé** – Entrée d'un ID de clé d'identification de compartiment précréé.
- **Accès** – Sélection des droits d'accès : Lecture ou écriture, Lecture, ou Ecriture.
- **Journal** – Sélection d'une case à cocher. Si la case à cocher est sélectionnée, l'agent OSA créera des journaux d'audit sur les autorisations d'accès du comportement de ligne fourni. .

Une fois que tous les champs obligatoires sont renseignés, cliquez sur “Suivant” pour passer à l'étape suivante.

Systèmes de back-end

Les informations de connexion aux systèmes de backend sont définies via une sélection M:N. Cette sélection définit la redondance et la sécurité des données de stockage d'objets. N représente le nombre de fournisseurs de stockage d'objets de backend configurés ou les "parts". M représente le nombre de parts requises pour reconstruire les données. Les configurations prises en charge sont : 1:1, 2:3, 2:4.

Add Object Store Agent

Required

☒ Agent Identity
☒ Network Information

Optional

☒ Front-End Certificates
☒ Bucket Credentials
☒ Buckets
☒ **Backends**
☐ Authorized Users
☐ Tools

M:N 2:3

* Required

Share 1 *

URL *

ID *

Key *

Protocol *

IBM S3

Share 2 *

URL *

ID *

Key *

Protocol *

IBM S3

Share 3 *

URL *

ID *

Key *

Protocol *

IBM S3

Back

Next

Chaque part nécessite la configuration de : URL, ID, Clé et Protocole.

- **URL** – Adresse URL d'accès du fournisseur de stockage d'objets
- **ID** – ID d'utilisateur du compte utilisé pour accéder au fournisseur de stockage d'objets.
- **Clé** – Clé du compte de l'ID utilisateur utilisé pour accéder au fournisseur de stockage d'objets.
- **Protocole** - Identification du protocole utilisé pour communiquer avec le fournisseur de stockage d'objet (Swift, IBM S3 et Amazon S3).

Une fois que tous les champs obligatoires sont renseignés, cliquez sur “Suivant” pour passer à l'étape suivante.

Utilisateurs autorisés

L'étape Utilisateurs implique que l'administrateur de la sécurité définisse les comptes utilisateur MDE disposant de privilèges de manière à télécharger le bundle d'installation de l'agent.

Si un utilisateur n'est pas répertorié en tant qu'utilisateur autorisé et si cet utilisateur se connecte et consulte l'agent, cet utilisateur ne voit pas les liens de téléchargement dans la page Informations sur l'agent.

Une fois que tous les champs obligatoires sont renseignés, cliquez sur **Suivant** pour passer à l'étape suivante.

Outils d'agents

Les agents prennent en charge des outils spécialisés qui facilitent le transfert de données sous une forme chiffrée. Il existe deux types d'outils : l'outil de sauvegarde/restauration et l'outil Magasin d'objets.

Les outils sont configurés pendant la mise en service des agents ou sur la page Informations sur l'agent. L'outil de sauvegarde/restauration permet de sauvegarder et de restaurer les données chiffrées. Il optimise une clé associée afin de sauvegarder les données chiffrées et permet de restaurer ces données ultérieurement si la clé de règle a été modifiée. L'outil de sauvegarde/restauration est facultatif et il n'est pas obligatoire d'associer un outil à un agent. L'outil Magasin d'objets est obligatoire pour l'agent de type Magasin d'objets.

Matrice des outils d'agent

La disponibilité des outils est basée sur le type d'agent et elle est activée en associant une clé. La matrice des outils par type d'agent est la suivante :

Type d'outil	Volume	Volume avec une règle	Fichier avec une règle	Magasin d'objets
Sauvegarde/ Restauration	✓	✓	✓	
Magasin d'objets				✓

Association d'une clé à un outil

Pour associer une clé à un outil, commencez à taper un nom de clé précédemment défini dans le champ de saisie situé en regard de l'outil souhaité puis sélectionnez la clé appropriée dans la liste.

Cliquez sur **Enregistrer**. Une tâche sera créée. Une fois la tâche approuvée, l'outil configuré sera activé sur l'agent.

Remarque : Les clés auto-générées ne sont pas prises en charge sur Outils. Les clés doivent être définies avant de créer l'agent.

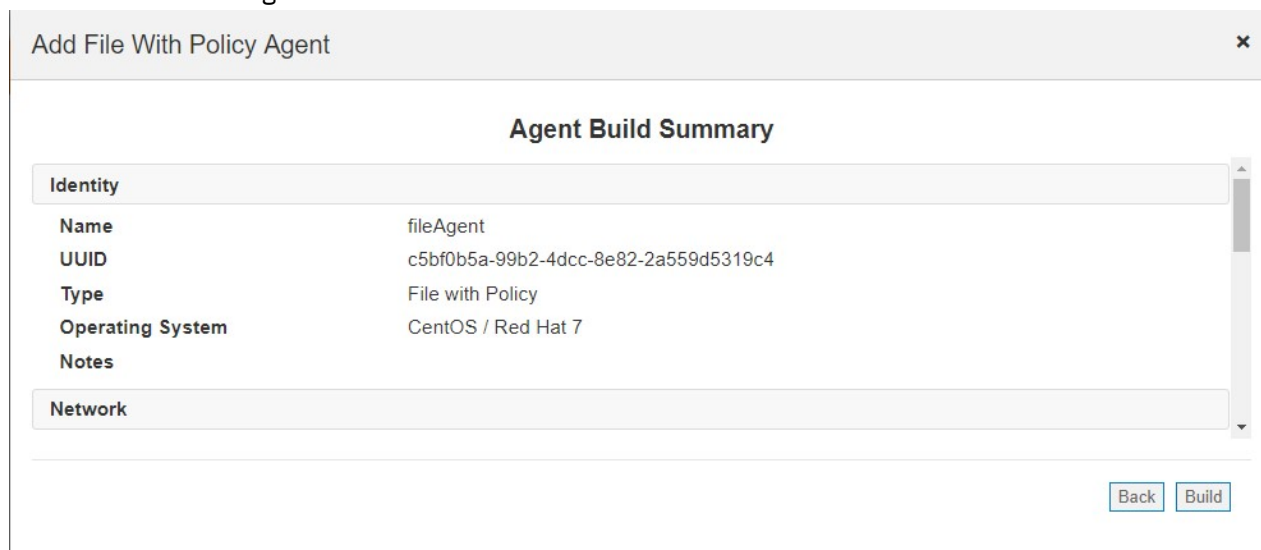
Une fois que tous les champs obligatoires sont renseignés, cliquez sur **Suivant** pour passer à l'étape suivante.

Vérification et génération

Pourquoi et quand exécuter cette tâche

Lorsque toutes les étapes de mise à disposition sont terminées, l'utilisateur accède à l'écran Vérifier.

La page de vérification de la mise à disposition configurée affichera une vue complète de toutes les informations de configuration.



The screenshot shows a window titled "Add File With Policy Agent" with a close button (X) in the top right corner. Inside the window, there is a section titled "Agent Build Summary". Below this title, there are two expandable sections: "Identity" and "Network". The "Identity" section is currently expanded, showing the following details:

Identity	
Name	fileAgent
UUID	c5bf0b5a-99b2-4dcc-8e82-2a559d5319c4
Type	File with Policy
Operating System	CentOS / Red Hat 7
Notes	

Below the "Identity" section is the "Network" section, which is currently collapsed. At the bottom right of the window, there are two buttons: "Back" and "Build".

Passez en revue le contenu pour vérifier qu'il est complet et correct et cliquez sur **Générer** pour terminer le processus de mise à disposition. Une tâche sera créée pour créer l'agent.

Une fois la tâche acceptée, l'agent sera créé et le package d'installation sera prêt à être téléchargé et installé.

Activation d'un agent

Lors de l'approbation de la tâche de génération d'un agent, l'agent qui vient d'être créé est actif dans MDE. Une fois l'agent installé, il utilise l'adresse IP homologue MDE configurée et les certificats fournis pour établir une connexion TLS1.2 mutuellement authentifiée à MDE.

L'agent demande la règle lors de l'installation initiale et au démarrage suivant. MDE répond en envoyant la configuration des règles configurées. Une fois la police reçue, elle est appliquée à l'agent.

Affichage des agents

Pourquoi et quand exécuter cette tâche

La page Agents affiche une liste récapitulative des agents créés.

Agents

Agent Report

Search

Enter Text

Clear

Add Agent

Name	Hostname or IP	Type	Notes	Actions
Agent1	1.1.1.1	Volume with Policy		<div>Details</div> <div>Delete Agent</div>

Pour afficher les détails d'un agent spécifique, cliquez sur le nom de l'agent dans la colonne Nom ou cliquez sur le bouton Détails dans la colonne Actions. Une page Vue détaillée de l'agent s'affiche. Elle contient les informations de mise en service, les téléchargements de bundle d'installation et d'autres informations utiles.

Rapport sur les agents

L'administrateur de la sécurité de MDE peut créer un rapport d'agent. Ce rapport contient des informations sur le nombre total d'agents, le nombre d'agents par type et par système d'exploitation, ainsi que sur les agents connectés dans les 30 jours qui suivent la génération du rapport. La date est basée sur le temps PPM, qui est le temps UTC. Les données sont ventilées par type d'agent.

Agents

Agent Report

Search

Enter Text

Clear

Add Agent

Installation d'un agent

Pourquoi et quand exécuter cette tâche

L'étape de mise en service a configuré toutes les informations nécessaires pour que l'agent installe et déploie une règle sur une instance de serveur cible. Pour installer l'agent, téléchargez le package d'installation, copiez-le sur le système cible, décompressez le contenu et exécutez le script de configuration.

Agent Info Edit Agent Info

Identity

Notes

Name

Agent1

UUID

dab30682-19ee-4763-84d8-12fe2ba91948

IP Address

1.1.1.1

Type

Volume with Policy

Operating System

CentOS / Red Hat 7

Network

MDE Peer IP

1.1.1.0

Certificates

Subject	Fingerprint	Expiry
CN=agent,OU=agent,O=SFC,L=RSM,ST=California,C=US	ea584e4904fffa45a3416eccc753e0f0f655462929d4f1534f369cbccc38165f	2016-11

Browse...

No file selected.

Users

Download Tokens

Authorized Users

admin

Install Files Download URL

/rest/agents/1/install_bundle

Download Zip Bundle

Download Tar Bundle

ID	State
<div>Add Token</div>	

Remarque critique

Assurez-vous que tous les utilisateurs, groupes et chemins d'accès ou unités identifiés dans une règle de mise en service sont créés, associés et configurés sur le système de l'agent.

Installation d'un agent pour Linux

Il existe 4 types d'agents : l'agent de type Volume, l'agent de type Fichier avec une règle, l'agent de type Volume avec une règle et l'agent de type Magasin d'objets. Utilisez le type d'agent désigné lors de la mise en service des agents.

Configuration d'une unité d'Agent de type Volume Linux

Pourquoi et quand exécuter cette tâche

Procédure

1. Créez un volume dans PPM (rappelez-vous le libellé d'unité utilisé à la section 11.1.5).
2. Installez le package "gettext" sur la machine virtuelle de l'agent.
3. Installez l'agent – voir [Annexe A, «Exemple de processus d'installation d'agent»](#), à la page 81 pour obtenir des détails
4. Une fois l'installation terminée, redémarrez la machine virtuelle de l'agent.

5. En tant que superutilisateur, exécutez `spxdevice -e <libellé donné dans PPM> -m <point de montage> -f <système de fichiers> -u <disque à utiliser>`

```
spxdevice -e COS6VOL -m /protected -f ext4 -u /dev/sdb
```

Configuration d'unité pour l'agent de type Fichier avec une règle pour Linux

Pourquoi et quand exécuter cette tâche

Procédure

1. Créez un agent de type Fichier avec une règle dans PPM
2. Créez tous les utilisateurs nécessaires
3. Créez les sous-répertoires nécessaires.
4. Définissez les autorisations appropriées sur les répertoires.
5. Installez le package "gettext" sur la machine virtuelle de l'agent
6. Installez l'agent – voir [Annexe A, «Exemple de processus d'installation d'agent»](#), à la page 81 pour obtenir des détails
7. Une fois l'installation terminée, redémarrez la machine virtuelle de l'agent
8. Vérifiez que la règle du fichier est correcte via la commande "spxinfo -l"

Important

Un astérisque en regard d'un chemin indique des données préexistantes en attente de chiffrement. Pour effectuer le chiffrement sur des structures et des données de répertoire préexistantes et pour déterminer l'état des données à tout moment, MDE fournit un utilitaire de ligne de commande appelé "spxconvert"

Voir [Annexe E, «Chiffrement sur place»](#), à la page 93 pour une description détaillée de la commande et de son utilisation.

Configuration d'une unité d'agent de type Volume avec une règle sous Linux

Pourquoi et quand exécuter cette tâche

Procédure

1. Créez un agent de type Volume avec une règle dans PPM (rappelez-vous le libellé d'unité utilisé).
 2. Installez le package "gettext" sur la machine virtuelle de l'agent
 3. Installez l'agent – voir [Annexe A, «Exemple de processus d'installation d'agent»](#), à la page 81 pour obtenir des détails
 4. Une fois l'installation terminée, redémarrez la machine virtuelle de l'agent
 5. En tant que superutilisateur, exécutez `spxdevice -e <libellé donné dans PPM> -m <point de montage> -f <système de fichiers> -u <disque à utiliser>`
- ```
[root@localhost]# spxdevice -e COS6VOL -m /protected -f ext4 -u /dev/sdb
```
6. Créez tous les sous-répertoires et les utilisateurs nécessaires
  7. Définissez les autorisations appropriées sur les répertoires.
  8. Redémarrez la machine virtuelle de l'agent
  9. lsblk – permet de vérifier que le disque existe. Cette opération peut parfois prendre jusqu'à 30 secondes.
  10. Vérifiez que la règle du fichier est correcte via la commande "spxinfo -l"

#### Important

Sous Linux, le chiffrement de volume peut être configuré sur des unités ou des partitions complètes. Pour utiliser une seule partition, spécifiez simplement une partition vide (par exemple /dev/sdb1) lors de l'utilisation de l'option `spxdevice -u`.

## Configuration d'un agent de type Magasin d'objets dans Linux

### Pourquoi et quand exécuter cette tâche

#### Procédure

1. Créez un agent de type Magasin d'objets dans PPM
2. Installez l'agent - voir [Annexe A, «Exemple de processus d'installation d'agent»](#), à la page 81 pour obtenir des détails
3. Une fois l'installation terminée, redémarrez la machine virtuelle de l'agent

## Installation d'un agent pour AIX

AIX ne prend en charge qu'un seul type d'agent : l'agent de type Fichier avec une règle. Utilisez le type d'agent désigné lors de la mise en service des agents.

### Configuration d'unité pour l'agent de type Fichier avec une règle pour AIX

1. Créez un agent de type Fichier avec une règle dans PPM
2. Créez tous les utilisateurs nécessaires
3. Créez les sous-répertoires nécessaires.
4. Définissez les autorisations appropriées sur les répertoires.
5. Installez l'agent – voir [Annexe A, «Exemple de processus d'installation d'agent»](#), à la page 81 pour obtenir des détails
6. Une fois l'installation terminée, redémarrez la machine virtuelle de l'agent
7. Vérifiez que la règle du fichier est correcte via la commande "`spxinfo -l`"

**Remarque :** Un astérisque en regard d'un chemin indique des données préexistantes en attente de chiffrement. Pour effectuer le chiffrement sur des structures et des données de répertoire préexistantes et pour déterminer l'état des données à tout moment, MDE fournit un utilitaire de ligne de commande appelé "`spxconvert`"

Voir [Annexe E, «Chiffrement sur place»](#), à la page 93 pour une description détaillée de la commande et de son utilisation.

## Installation d'un agent pour Windows

Il existe 3 types d'agent : l'agent Volume, l'agent Fichier avec une règle et l'agent Volume avec une règle. Utilisez le type d'agent désigné lors de la mise en service des agents.

### Configuration d'une unité d'Agent de type Volume sous Windows

#### Pourquoi et quand exécuter cette tâche

#### Procédure

1. Créez un volume dans PPM (rappelez-vous le libellé d'unité utilisé).
2. Installez l'agent - voir [Annexe A, «Exemple de processus d'installation d'agent»](#), à la page 81 pour obtenir des détails
3. Une fois l'installation terminée, redémarrez la machine virtuelle de l'agent

4. Exécutez "spxdevice -e <libellé\_attribué\_dans\_PPM> -d <numéro\_disque\_à\_utiliser>" pour vous connecter au disque complet. Exécution en tant qu'administrateur.

```
spxdevice -e PRODISK -d 1
```

5. Ou exécutez spxdevice -e <libellé\_attribué\_dans\_PPM> -d <numéro\_disque\_à\_utiliser> -m <identificateur\_unité> -f <système\_fichiers> pour vous connecter au disque complet qui sera formaté et monté avec un identificateur d'unité.

```
spxdevice -e PRODISK -d 1 -m E -f NTFS
```

6. Sinon, exécutez "spxdevice -i <numéro\_disque\_à\_utiliser>" pour mettre en préproduction le disque à relier à une partition spécifique

```
spxdevice -i 1
```

7. Ensuite, exécutez "spxdevice -e <libellé\_attribué\_dans\_PPM> -v <identificateur\_unité> -f <système\_fichiers>" pour vous connecter à une partition spécifique et formater la partition avec un système de fichiers

```
spxdevice -e PRODISK -v E -f NTFS
```

**Remarque :** Sous Windows, le chiffrement de volume peut être configuré sur des unités ou des partitions complètes.

- Pour le chiffrement du disque complet, le disque doit être en ligne et initialisé et l'espace disque ne doit pas être formaté. Des identificateurs d'unité doivent être disponibles.
- Pour le chiffrement de la partition, vous devez créer l'unité de support via "spxdevice -i <numéro\_disque>" sur un disque propre. Ensuite, vous devez créer une partition brute (RAW) dotée d'un identificateur d'unité.

Reportez-vous à l'aide dans la commande "spxdevice" pour plus d'options.

## Configuration d'unité pour l'agent de type Fichier avec une règle pour Windows

### Pourquoi et quand exécuter cette tâche

#### Procédure

1. Créez un agent de type Fichier avec une règle dans PPM
2. Créez tous les utilisateurs nécessaires
3. Créez les sous-répertoires nécessaires.
4. Définissez les autorisations appropriées sur les répertoires.
5. Installez l'agent – voir [Annexe A, «Exemple de processus d'installation d'agent»](#), à la page 81 pour obtenir des détails
6. Vérifiez que la règle du fichier est correcte via la commande : spxinfo -l

#### Important

Un astérisque en regard d'un chemin indique des données préexistantes en attente de chiffrement. Pour effectuer le chiffrement sur des structures et des données de répertoire préexistantes et pour déterminer l'état des données à tout moment, MDE fournit un utilitaire de ligne de commande appelé "spxconvert"

Voir [Annexe E, «Chiffrement sur place»](#), à la page 93 pour une description détaillée de la commande et de son utilisation.

#### Important

Sous Windows, assurez-vous qu'un administrateur est autorisé à créer les répertoires cible via une règle, car la règle est en vigueur une fois qu'elle est récupérée.

## Configuration d'une unité d'Agent de type Volume avec une règle sous Windows

### Pourquoi et quand exécuter cette tâche

#### Procédure

1. Créez un Agent de type Volume avec une règle dans PPM (rappelez-vous le libellé d'unité utilisé).
2. Installez l'agent – voir [Annexe A, «Exemple de processus d'installation d'agent»](#), à la page 81 pour obtenir des détails
3. Une fois l'installation terminée, redémarrez la machine virtuelle de l'agent
4. Exécutez “spxdevice -e <libellé\_attribué\_dans\_PPM> -d <numéro\_disque\_à\_utiliser>” pour établir une liaison à l'ensemble du disque. Exécution en tant qu'administrateur.

**PS C:\> spxdevice -e PRODISK -d 1**

5. Ou exécutez “spxdevice -e <libellé\_attribué\_dans\_PPM> -d <numéro\_disque\_à\_utiliser> -m <identificateur\_unité> -f <système\_fichiers>” pour établir une liaison à l'ensemble du disque qui sera formaté et monté avec un identificateur d'unité

**PS C:\> spxdevice -e PRODISK -d 1 -m E -f NTFS**

6. Sinon, exécutez "spxdevice -I <numéro\_disque\_à\_utiliser>" pour mettre en préproduction le disque à relier à une partition spécifique.

**PS C:\> spxdevice -i 1**

7. Ensuite, exécutez “spxdevice -e <libellé\_attribué\_dans\_PPM> -v <identificateur\_unité> -f <système\_fichier>” pour établir une liaison à une partition spécifique et formater la partition avec un système de fichiers.

**PS C:\> spxdevice -e PRODISK -v E -f NTFS**

#### Important

Sous Windows, le chiffrement de volume peut être configuré sur des unités ou des partitions complètes.

- Pour le chiffrement du disque complet, le disque doit être en ligne et initialisé et l'espace disque ne doit pas être formaté. Des identificateurs d'unité doivent être disponibles.
- Pour le chiffrement de la partition, vous devez créer l'unité de support via "spxdevice -i <numéro\_disque>" sur un disque propre. Ensuite, vous devez créer une partition brute (RAW) dotée d'un identificateur d'unité.

Reportez-vous à l'aide de la commande "spxdevice" pour plus d'options.

8. Ajoutez un ou des répertoires protégés sur un volume.
9. Redémarrez l'ordinateur.
10. spxinfo -l (doit afficher une liste de tous les répertoires protégés)

#### Important

Sous Windows, assurez-vous qu'un administrateur est autorisé à créer les répertoires cible via une règle, car la règle est en vigueur une fois que le volume est connecté et disponible.

## Règle active

Chaque agent ne peut comporter qu'une seule règle active. Les agents ne conservent pas leur règle de façon permanente. A chaque redémarrage d'un agent, l'agent demande à MDE d'envoyer la règle active. Si l'agent ne peut pas accéder à MDE, le refus d'accès par défaut est appliqué à tous les répertoires protégés sur l'agent.

Lorsqu'une nouvelle règle est envoyée à l'agent, l'agent envoie un événement à MDE lorsque la règle est appliquée correctement (ou incorrectement). Si les problèmes d'activation de la règle persistent, reportez-vous au fichier `kernel_policy.log` dans les emplacements suivants.

- Linux/AIX : `/var/log/spxagent/spx-policyagent`
- Windows : `C:\Windows\spxagent\PolicyAgent`

## Modification d'un agent

Une fois qu'un agent a été mis en service correctement et approuvé, les modifications apportées à cet agent doivent être effectuées en modifiant l'agent via l'interface graphique sur la page "Informations sur l'agent". Pour modifier un agent, affichez les détails de l'agent. Sur la page Informations sur l'agent, les différentes sections de l'agent peuvent être modifiées indépendamment.

### Modification des informations de l'agent

Si vous cliquez sur le bouton "Modifier les informations sur l'agent", vous pouvez modifier certaines informations sur l'agent : nom, adresse IP, adresse IP de l'homologue MDE et remarques.

Agent Info

Edit Agent Info

Identity

Notes

Name

Agent1

UUID

dab30682-19ee-4763-84d8-12fe2ba91948

IP Address

10.6.1.255

Type

Volume with Policy

Operating System

CentOS / Red Hat 7

Network

MDE Peer IP

10.6.1.105

Certificates

| Subject                                          | Fingerprint                                                      | Expir |
|--------------------------------------------------|------------------------------------------------------------------|-------|
| CN=agent,OU=agent,O=SFC,L=RSM,ST=California,C=US | ea584e4904fffa45a3416eccc753e0f0f655462929d4f1534f369cbccc38165f | 2016- |

Browse...

No file selected.

Les modifications apportées à l'adresse IP de l'homologue MDE sont immédiates dans MDE, mais si l'agent est déjà installé, un nouveau package d'installation doit être créé et installé avant que les modifications soient appliquées.

### Important

Les champs UUID, Système d'exploitation et Type d'agent ne peuvent pas être modifiés après la mise en service initiale.

## Ajout/Suppression de certificats

Les certificats d'agents peuvent être ajoutés et supprimés en cliquant sur les boutons correspondants dans la section des certificats de la page Informations sur l'agent.

Network

MDE Peer IP

1.1.1.0

Certificates

| Subject                                                                                           | Fingerprint                                                     | Expiry               |                                    |
|---------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|----------------------|------------------------------------|
| CN=agent,OU=agent,O=SFC,L=RSM,ST=California,C=US                                                  | ea584e4904ffa45a3416eccc753e0f0f655462929d4f1534f369cbccc38165f | 2016-11-15T14:32:08Z | <a href="#">Delete Certificate</a> |
| <div><a href="#">Browse...</a> No file selected.</div> <div><a href="#">Add Certificate</a></div> |                                                                 |                      |                                    |

Pour mettre à jour un certificat d'agent, procédez comme suit :

1. Générez un nouveau certificat pour l'agent
2. Téléchargez le nouveau certificat vers PPM via la console de gestion
  - a. Sur la page Agents, cliquez sur l'agent à mettre à jour pour afficher la page Informations sur l'agent
  - b. Cliquez sur le bouton “Ajouter un certificat”, sélectionnez le nouveau fichier de certificat et cliquez sur le bouton “OK”
  - c. Le nouveau certificat devrait normalement s'afficher
3. Supprimez l'ancien certificat
  - a. Sur la page Agents, cliquez sur l'agent à mettre à jour pour afficher la page Informations sur l'agent
  - b. Identifiez le certificat devant être supprimé
  - c. Cliquez sur le bouton “Supprimer le certificat” ; une tâche sera créée
  - d. Cliquez sur le bouton “Fermer”
  - e. Sur la page Tâches, cliquez sur le bouton “Approuver” sur la tâche désirée
4. Vérifiez que le certificat a été supprimé de l'agent
  - a. Sur la page Agents, cliquez sur l'agent à mettre à jour pour afficher la page Informations sur l'agent
  - b. Vérifiez que le certificat qui reste est le bon

Si l'agent était déjà installé, un nouveau package d'installation doit être créé et installé avant que les modifications apportées au certificat soient appliquées.

## Outils d'agents

Les outils qui n'ont pas été configurés durant la mise en service d'un agent peuvent maintenant être ajoutés à la page Informations sur l'agent. De plus, les outils configurés peuvent être modifiés.

### Association d'une clé

Pour associer un clé, entrez le nom de la clé dans le champ de texte situé en regard de l'outil, puis sélectionnez la clé dans la liste. Cliquez sur “Enregistrer”. Une tâche sera créée. Une fois approuvé, l'outil configuré sera activé sur l'agent.

Add File With Policy Agent

Required

✓ Agent Identity

✓ Network Information

Optional

✓ Policy

✓ Authorized Users

⊙ Tools

Backup/Restore

Type to filter and select a predefined key

Back
Next

## Modification d'une clé

Pour modifier une clé, cliquez sur le bouton d'édition et entrez le nom de la clé dans le champ de texte situé en regard de l'outil, puis sélectionnez la clé dans la liste.

Cliquez sur “Enregistrer”. Une tâche sera créée. Une fois approuvé, l'outil configuré sera activé sur l'agent.

## Tools

Backup/Restore

User Defined Key

Save
Cancel

## Accès aux données SU

Lorsque des contrôles d'accès aux règles sont appliqués, l'accès aux données SU est refusé par défaut. Cependant, il peut exister un scénario dans lequel l'accès aux données SU est autorisé. Dans ce cas, une case à coche apparaît sur la page Informations sur l'agent qui permet de modifier la configuration.

Other Configuration

☒ Block access when su user substitution is in use

Si vous cochez la case, une tâche sera créée. Une fois approuvée, le paramètre d'accès aux données SU sera modifié en conséquent.

Le tableau suivant montre les contrôles d'accès aux données SU :

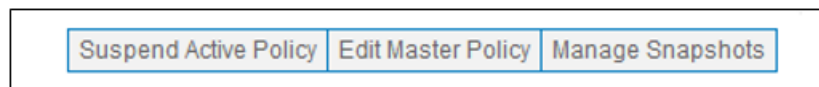
| Type d'agent           | Système d'exploitation | Valeur par défaut de l'accès aux données SU | Accès aux données SU configurable |
|------------------------|------------------------|---------------------------------------------|-----------------------------------|
| Volume                 | CentOS6/RedHat6        | N/A                                         | N/A                               |
| Volume                 | CentOS7/RedHat7        | N/A                                         | N/A                               |
| Volume                 | Windows                | N/A                                         | N/A                               |
| Volume avec une règle  | CentOS6/RedHat6        | Bloqué                                      | Oui                               |
| Volume avec une règle  | CentOS7/RedHat7        | Bloqué                                      | Oui                               |
| Volume avec une règle  | Windows                | N/A                                         | N/A                               |
| Fichier avec une règle | CentOS6/RedHat6        | Bloqué                                      | Oui                               |
| Fichier avec une règle | CentOS7/RedHat7        | Bloqué                                      | Oui                               |
| Fichier avec une règle | AIX                    | Bloqué                                      | Oui                               |

|                        |                 |     |     |
|------------------------|-----------------|-----|-----|
| Fichier avec une règle | Windows         | N/A | N/A |
| Magasin d'objets       | CentOS7/RedHat7 | N/A | N/A |

## Interruption d'une règle

Les agents de type Volume avec une règle et Fichier avec une règle prennent en charge la possibilité d'interrompre une règle active définie. Lorsqu'une règle est interrompue, toutes les actions prises envers les répertoires protégés seront refusées. L'interruption d'une règle active peut être réalisée sans changer la définition d'instantané active.

Pour interrompre une règle, cliquez sur le bouton “Suspendre une règle active” dans l'angle droit de la section Informations sur l'agent. Une tâche sera créée.



Une fois la tâche approuvée, la règle sera immédiatement interrompue et le bouton affichera “Réactiver une règle active”.

Pour réactiver la règle interrompue, cliquez sur le bouton “Réactiver une règle active”. Une tâche sera créée. Après avoir approuvé la tâche, la dernière règle d'instantané active prendra immédiatement effet.

## Modifications apportées à une règle

Des modifications peuvent être apportées à une règle en modifiant une règle appliquée à un chemin d'accès protégé, en ajoutant un nouveau chemin d'accès protégé ou en ajoutant un volume chiffré.

Les modifications apportées à une règle ne modifient pas le statut de chiffrement des données actuelles. Elles n'ont d'influence que sur le traitement des données créées une fois que la règle a été redéployée.

### Remarque critique

Ne supprimez pas la règle de volume d'un agent actif. Cette opération n'est pas prise en charge et pourrait mettre le système cible dans un état instable.

Vous pouvez créer un volume sur un agent actif et laisser l'ancien volume inutilisé.

Autrement, vous pouvez créer et déployer un nouvel agent.

### Modification d'une règle

La modification de la règle d'un agent permet de modifier l'option Chemin d'accès aux règles concernant les fichiers, l'association Ensemble de chemins d'accès/Type de données ou des volumes chiffrés.

Si le type de données est modifié sur un type qui peut être modifié, il est possible de modifier ces champs en ligne. Pour modifier la règle, cliquez sur le bouton "Modifier la règle principale".



## Active Policy

[Edit Master Policy](#) [Manage Snapshots](#)

| File Policy Path Pathset1 |               |           |
|---------------------------|---------------|-----------|
| Datatype                  | Datatype1     |           |
| Selector                  | Operation     | Actions   |
| Selector1                 | Read or Write | Permit    |
| Select All                | Read or Write | Deny, Log |

## Protected Volumes

| Volume Policy Path |        |
|--------------------|--------|
| Device Label       | volume |
| Key                | Key1   |

Figure 1. Exemple d'agent de type Volume avec règle

La page Modifier la règle principale apparaît.

## Edit Master Policy

| File Policy Path (or Path Set) Pathset1       |               |           |
|-----------------------------------------------|---------------|-----------|
| <input type="checkbox"/> Autogenerate Key     |               |           |
| Datatype                                      | Datatype1     |           |
| (remember to fill out any empty values below) |               |           |
| Selector                                      | Operation     | Actions   |
| Selector1                                     | Read or Write | Permit    |
| Select All                                    | Read or Write | Deny, Log |

| Volume Policy Path |                                                |
|--------------------|------------------------------------------------|
| Device Label       | volume                                         |
| Key                | Key1 <input type="checkbox"/> Autogenerate Key |

[Add Volume](#) [Add Path](#)

[Save](#) [Save and Snapshot](#) [Save, Snapshot and Activate](#) [Cancel](#)

## Important

La modification de la règle principale ne modifie aucun instantané.

•

## Ajout d'un chemin d'accès

### Pourquoi et quand exécuter cette tâche

Pour ajouter un nouveau chemin d'accès à placer sous la règle, cliquez sur le bouton "Ajouter un chemin".

Edit Master Policy

File Policy Path (or Path Set)

Pathset1

☐ Autogenerate Key

Datatype

Datatype1

(remember to fill out any empty values below)

| Selector   | Operation     | Actions   |
|------------|---------------|-----------|
| Selector1  | Read or Write | Permit    |
| Select All | Read or Write | Deny, Log |

Volume Policy Path

Device Label

volume

Key

Key1

☐ Autogenerate Key

Add Volume

Add Path

Une nouvelle section s'affiche pour la saisie d'une règle (comme la mise en service initiale).

File Policy Path (or Path Set)

Type policy path or select a predefined path : Required

Delete

☐ Autogenerate Key

Datatype

Type to filter and select a predefined datatype Required

(remember to fill out any empty values below)

| Selector | Operation | Actions |
|----------|-----------|---------|
|----------|-----------|---------|

Add Volume

Add Path

Save

Save and Snapshot

Save, Snapshot and Activate

Cancel

## Ajout d'un volume

### Pourquoi et quand exécuter cette tâche

Pour ajouter un nouveau volume à chiffrer, cliquez sur le bouton Ajouter un volume.

## Edit Master Policy

**File Policy Path (or Path Set)** **Pathset1**

☐ Autogenerate Key

**Datatype**


*(remember to fill out any empty values below)*

| Selector   | Operation     | Actions   |
|------------|---------------|-----------|
| Selector1  | Read or Write | Permit    |
| Select All | Read or Write | Deny, Log |

**Volume Policy Path**

**Device Label**

**Key**  ☐ Autogenerate Key



Une nouvelle section s'affiche pour la saisie (comme la mise en service initiale).

**Volume Policy Path**

**Device Label**  **Required**

**Key**  ☐ Autogenerate Key **Required**

## Suppression d'un chemin

### Pourquoi et quand exécuter cette tâche

Pour supprimer un chemin protégé par une règle, cliquez sur le bouton "Supprimer" correspondant au chemin concerné. Une fois la configuration de la règle sauvegardée, prise en image et activée, ce chemin n'est plus protégé par la règle de contrôle d'accès. Les nouveaux fichiers écrits dans le répertoire ne sont plus chiffrés. Le fichier existant reste à l'état chiffré et n'est pas accessible.

**Remarque :** Pour garantir un accès ininterrompu aux données, copiez ou déplacez les données hors du chemin du répertoire protégé avant de supprimer le chemin de la règle.

## Edit Master Policy

**File Policy Path (or Path Set)**

☐ Autogenerate Key

**Datatype**

*(remember to fill out any empty values below)*

| Selector  | Operation     | Actions |
|-----------|---------------|---------|
| selector1 | Read or Write | Permit  |

**Volume Policy Path**

**Device Label**

**Key**  ☐ Autogenerate Key

## Instantanés de l'agent

Les instantanés de l'agent sont le stockage permanent des configurations de règles associées à l'agent. Les instantanés sont indexés et possèdent un état Actif ou Inactif. Il n'y a qu'un seul instantané actif par agent. C'est la configuration de la règle appliquée actuellement à l'agent. Pour modifier la configuration de la règle d'un agent, l'administrateur doit créer un instantané qui reflète les modifications souhaitées et active le nouvel instantané.

## Enregistrement des modifications et des instantanés d'un agent

Lors de la modification d'une règle d'agent, vous pouvez annuler les modifications, les enregistrer, les enregistrer et en créer un instantané ou les enregistrer, en créer un instantané et les activer.

### Annulation des modifications

L'annulation des modifications rétablit la configuration des règles qui était en place avant la modification.

### Enregistrement des modifications

L'enregistrement des modifications permet de stocker ces modifications pour les utiliser ultérieurement, mais pas de créer d'instantané. De ce fait, les modifications ne peuvent pas être appliquées à l'agent.

### Enregistrer et créer un instantané

L'enregistrement des modifications et la création d'un instantané permettent de stocker ces modifications pour les utiliser ultérieurement et de créer un instantané qui peut être affiché et activé par la suite.

## Enregistrement, création d'un instantané et activation

L'enregistrement, la création d'un instantané et l'activation des modifications permettent de stocker les modifications afin de les utiliser ultérieurement, de créer un instantané qui peut être affiché et de créer immédiatement une tâche pour appliquer ces modifications à l'agent.

**Remarque :** Toute modification ou mise à jour d'un instantané ne prendra effet que lorsque l'agent sera en mesure de communiquer avec le serveur PPM. La tâche créée restera en cours d'exécution jusqu'à ce que la communication entre PPM et l'agent aboutisse ou que l'agent soit retiré du serveur PPM.

## Gestion des instantanés

Tous les instantanés associés à un agent peuvent être affichés à l'aide du bouton "Gérer les instantanés" dans la vue Informations sur l'agent.

Active Policy

Edit Master Policy Manage Snapshots

| File Policy Path | Pathset1      |           |
|------------------|---------------|-----------|
| Datatype         | Datatype1     |           |
| Selector         | Operation     | Actions   |
| Selector1        | Read or Write | Permit    |
| Select All       | Read or Write | Deny, Log |

Lorsque vous cliquez sur le bouton, une boîte de dialogue de gestion des instantanés s'affiche. Dans cette boîte de dialogue, un administrateur de la sécurité peut afficher les détails d'un instantané, activer un instantané, désactiver la règle associée à un instantané et supprimer un instantané.

Agent Snapshots

| ID | State    | Actions                        |
|----|----------|--------------------------------|
| 1  | Inactive | Activate Delete View Details   |
| 2  | Active   | Deactivate Policy View Details |

OK

### Important

La modification de l'instantané actif ne modifie pas la règle principale.

### Afficher les détails

Ce bouton affiche une vue résumée de la règle associée à l'instantané.

**Notes**

**Protection Policy**

**File Policy Path** /protected2

**Datatype** Datatype1

| Selector | Operation | Key | Actions |
|----------|-----------|-----|---------|
|----------|-----------|-----|---------|

[Back](#)

[OK](#)

### Activation d'un instantané

L'activation d'un instantané crée une tâche d'envoi de la règle à l'agent. Une fois l'instantané approuvé, il passe à l'état actif, et sa règle remplace toute police présente sur l'agent.

**Remarque :** Toute modification ou mise à jour d'un instantané ne prendra effet que lorsque l'agent sera en mesure de communiquer avec le serveur PPM. La tâche créée restera en cours d'exécution jusqu'à ce que la communication entre PPM et l'agent aboutisse ou que l'agent soit retiré du serveur PPM.

### Suppression d'un instantané

Un instantané inactif ne peut pas être supprimé. La suppression d'un instantané le supprime définitivement de MDE.

## Désinstallation d'un Agent de type Fichier

### Pourquoi et quand exécuter cette tâche

Si vous souhaitez supprimer un Agent de type Fichier, effectuez la procédure suivante :

Copiez les données des répertoires protégés. Cette opération permet de s'assurer que les données sont accessibles une fois qu'une règle est désactivée.

Effectuez les étapes suivantes pour supprimer le logiciel de l'agent :

### Procédure

#### 1. Linux – exécution en tant que superutilisateur

##### a) Arrêtez le service spx-policyagent

- Utilisation de CentOS 7

```
systemctl stop spx-policyagent
```

- Utilisation de CentOS 6

```
service spx-policyagent stop
```

##### b) Exécutez `cd /opt/ibm/mde/spxagent/spx-fileagent/`.

- c) Exécutez `./fileagent_uninstall.sh`.
  - d) Entrez y pour confirmer l'action de destruction.
  - e) Redémarrez.
2. AIX - exécution en tant que superutilisateur
- a) Arrêtez le service `spx-policyagent`.

```
stopsrc -s spx-policyagent
```

- b) Arrêtez les modules de noyau.

```
/opt/ibm/mde/spxagent/spx-fileagent/module/spx_kctrl_stop
```

- c) Supprimez le RPM.

```
rpm -e fileagent*
```

**Remarque :** Si vous souhaitez spécifier un RPM précis au lieu d'un caractère générique, utilisez

```
rpm -qa | grep fileagent
```

- d) Redémarrez.

### 3. Windows – exécution en tant qu'administrateur

- Via l'interface graphique de Windows
  - Accédez à Ajout/Suppression de programmes dans le Panneau de configuration
  - Sélectionnez l'agent "FileAgent" à désinstaller
  - Redémarrez le système lorsque vous y êtes invité
- Via l'interface CLI PowerShell
  - `msiexec /x <chemin d'accès à FileAgent.msi>`
  - Redémarrez le système lorsque vous y êtes invité

**Important :** Le ou les utilisateurs autorisés ne doivent pas utiliser la commande `mv` (déplacement) pour déplacer des données en direction/provenance de l'emplacement chiffré, car cela peut créer des problèmes au niveau de la règle MDE.

Sauvegardez d'abord les données en direction/provenance des répertoires (chiffrés) à l'aide de la commande `cp` (copie).

## Désinstallation des agents de volume

### Désinstallation d'un Agent de type Volume

- Linux – exécution en tant que superutilisateur.
1. Démontez le volume protégé

```
umount /dev/mapper/<e_volume>
```

2. Arrêtez le service `spx-policyagent`

- Utilisation de CentOS 7

```
systemctl stop spx-policyagent
```

- Utilisation de CentOS 6

```
service spx-policyagent stop
```

3. Exécutez `cd /opt/ibm/mde/spxagent/spx-volumeagent/`.
  4. Exécutez `./volumeagent_uninstall.sh`.
  5. Entrez `y` pour confirmer l'action de destruction.
  6. Redémarrez
- Windows - exécution en tant qu'administrateur
    - Via l'interface graphique de Windows
      - Accédez à Ajout/Suppression de programmes dans le Panneau de configuration
      - Sélectionnez l'agent "VolumeAgent" à désinstaller
      - Redémarrez le système lorsque vous y êtes invité
    - Via l'interface CLI PowerShell
      - `msiexec/x <chemin d'accès à VolumeAgent.msi>`
      - Redémarrez le système lorsque vous y êtes invité

## Désinstallation d'un agent de type Volume avec une règle

### Pourquoi et quand exécuter cette tâche

#### Procédure

1. Linux – exécution en tant que superutilisateur

- a) Démontez le répertoire protégé

```
umount /dev/mapper/<e_volume>
```

- b) Arrêtez le service `spx-policyagent`

- Utilisation de CentOS 7

```
systemctl stop spx-policyagent
```

- Utilisation de CentOS 6

```
service spx-policyagent stop
```

- c) Exécutez `cd /opt/ibm/mde/spxagent/spx-hybridagent/`.

- d) Exécutez `./hybridagent_uninstall.sh`.

- e) Entrez `'y'` pour confirmer l'action de destruction.

- f) Redémarrez.

2. Windows - exécution en tant qu'administrateur

- Via l'interface graphique de Windows
  - Accéder à Ajout/Suppression de programmes dans le Panneau de configuration.
  - Sélectionnez “HybridAgent” comme agent à désinstaller.
  - A l'invite, redémarrez le système.
- Via l'interface CLI PowerShell
  - Exécutez `msiexec /x <chemin d'accès à HybridAgent/msi>`.
  - A l'invite, redémarrez le système.



## Désinstallation de l'agent Magasin d'objets

### Pourquoi et quand exécuter cette tâche

Tous les comptes utilisateur et les autorisations seront stockés dans PPM jusqu'à la suppression de l'agent de PPM.

### Procédure

1. Linux – exécution en tant que superutilisateur
2. Arrêtez le service spx-policyagent

```
systemctl stop spx
```

3. **cd** /opt/ibm/mde/spxagent/spx-objectagent

```
./objectagent_uninstall.sh
```

4. Entrez 'y' pour confirmer l'action de destruction.
5. Redémarrez.

## Suppression d'un agent dans MDE

Un agent géré par MDE peut être supprimé de l'écosystème à l'aide de l'interface utilisateur MDE (GUI).

Pour supprimer un agent, cliquez sur le bouton “Supprimer l'agent”. Une tâche sera créée. Une fois que la tâche est approuvée, l'agent est supprimé de MDE.

| Name   | Hostname or IP | Type               | Notes | Actions                                              |
|--------|----------------|--------------------|-------|------------------------------------------------------|
| Agent1 | 1.1.1.1        | Volume with Policy |       | <a href="#">Details</a> <a href="#">Delete Agent</a> |

### Remarque critique

- La suppression d'un agent dans MDE empêche l'agent de pouvoir se connecter à MDE. De ce fait, les données actuellement protégées sont inaccessibles au redémarrage suivant de l'agent.
- La suppression d'un agent ne déchiffre pas les données.

## Utilitaires d'agent

Les agents MDE fournissent plusieurs utilitaires pour la configuration des agents et la protection des informations sensibles. Pour en savoir plus sur chaque utilitaire, exécutez l'utilitaire contenant l'option “--help”.

| Utilitaire | Fonction                                              | Volume | Volume avec une règle | Fichier avec une règle | Magasin d'objets |
|------------|-------------------------------------------------------|--------|-----------------------|------------------------|------------------|
| spxbackup  | Crée une sauvegarde chiffrée des données identifiées. | Oui    | Oui                   | Oui                    | Non              |

|            |                                                                                                                           |     |     |                             |     |
|------------|---------------------------------------------------------------------------------------------------------------------------|-----|-----|-----------------------------|-----|
| spxconvert | Convertit les données préexistantes dans un répertoire protégé de non chiffré à chiffré, sur la base d'une règle définie. | Non | Non | Oui                         | Non |
| spxdevice  | Mappe un volume de disque ou une partition à un nom d'appareil défini.                                                    | Oui | Oui | Non                         | Non |
| spxhash    | Génère un hachage d'un processus indiqué spécifique à la version.                                                         | Non | Oui | Oui                         | Non |
| spximport  | Importe les données chiffrées dans un répertoire sans chiffrer les données en double.                                     | Non | Non | Oui<br>(Windows uniquement) | Non |
| spxinfo    | Affiche une liste des répertoires protégés via une règle définie                                                          | Non | Oui | Oui                         | Non |
| spxobject  | Affiche une liste des magasins d'objets                                                                                   | Non | Non | Non                         | Oui |
| spxrestore | Restaure une sauvegarde chiffrée de données identifiées.                                                                  | Oui | Oui | Oui                         | Non |

---

# Chapitre 12. Opérations

## Sauvegarde et restauration des données de produit

---

MDE prend en charge la possibilité d'effectuer une sauvegarde par point de cohérence des données PPM du service MDE. Cette sauvegarde par point de cohérence peut être restaurée pour rétablir l'état de MDE au moment de la collecte de la sauvegarde.

**Remarque :** Avant de continuer une sauvegarde ou une restauration, arrêtez le service MDE par le biais de la commande "systemctl stop spsd" sur la machine virtuelle MDE.

```
sudo systemctl stop spsd
```

### Sauvegarde des données du produits

#### Pourquoi et quand exécuter cette tâche

Les sauvegardes de produit sont effectuées en exécutant un script de ligne de commande sur la machine virtuelle MDE.

Le script de sauvegarde spsd-backup se trouve dans la machine virtuelle MDE dans le répertoire /opt/securityfirst/spsd/bin. Il crée automatiquement un fichier et le nomme selon l'horodatage de l'exécution de la sauvegarde.

```
sudo /opt/securityfirst/spsd/bin/spsd-backup --help
Syntaxe : spsd-backup [--nodb] [--help]

--nodb Ne pas sauvegarder la base de données
--help Afficher cette aide
```

Pour exécuter une sauvegarde :

```
sudo /opt/securityfirst/spsd/bin/spsd-backup
Vidage de l'élément buildinfo local
Vidage des propriétés spsd locales
Vidage de la base de données PostgreSQL locale
Terminé - fichier créé spsd-backup-2017-04-04T144448-0700.tar.gz
```

### Restauration des données d'un produit

#### Pourquoi et quand exécuter cette tâche

La restauration d'un produit est effectuée à l'aide d'un script de ligne de commande exécuté sur la machine virtuelle MDE.

Le script de restauration spsd-restore se trouve dans le répertoire /opt/securityfirst/spsd/bin.

```
sudo /opt/securityfirst/spsd/bin/spsd-restore --help
Syntaxe : spsd-restore [--nodb] [--noprops] [--help] FILE

--nodb Ne pas écrire dans la base de données
--noprops Ne pas écrire de propriétés locales
--help Afficher cette aide
```

Pour exécuter une restauration :

```
sudo /opt/securityfirst/spsd/bin/spsd-restore
spsd-backup-2017-04-04T144448-0700.tar.gz
```

**Remarque :** Après la restauration d'un fichier de sauvegarde, MDE applique les modifications au démarrage suivant.

## Mise à jour du noyau

---

### Pourquoi et quand exécuter cette tâche

Lorsqu'une mise à jour du noyau est requise sur un agent exécutant un système d'exploitation Red Hat Enterprise Linux 7 ou CentOS 7, suivez les instructions suivantes :

- Si la mise à jour du système d'exploitation / noyau appartiennent à la même version, le nouveau noyau est automatiquement pris en charge.
- Si la mise à niveau du système d'exploitation / noyau se fait vers une version ultérieure (par ex. RHEL 7.2 -> 7.4), suivez la procédure ci-dessous pour créer une prise en charge pour le nouveau noyau :
  - Exemple : le bundle d'installation d'agent a été décompressé dans /root/agent

```
cd /root/agent/spx-installer
./agent_setup.sh -d /root/agent
Reboot
```

Ces étapes ne sont pas requises pour les agents s'exécutant sur Red Hat Enterprise Linux 6 ou CentOS 6.

## Mise à niveau

---

Effectuez les étapes ci-après pour mettre à niveau le produit MDE vers une nouvelle version.

**Remarque :** Ces étapes s'appliquent à l'archive de virtualisation ouverte (OVA) MDE. Si une installation non OVA a été exécutée, les répertoires peuvent changer.

### Pour le serveur MDE

#### Pourquoi et quand exécuter cette tâche

##### Procédure

1. En tant que superutilisateur, arrêtez le service de règle PPM.

```
systemctl stop spsd
```

2. Sauvegardez les données MDE :

```
/opt/securityfirst/spsd/bin/spsd-backup
```

3. Déplacez le fichier binaire MDE de la nouvelle version vers le répertoire /home/admin.
4. Supprimez le répertoire rpms existant.

```
rm -fr /home/admin/rpms
```

5. Modifiez les droits d'accès au fichier binaire MDE.

```
chmod +x /home/admin/ibm_sw_mde_X.x.x-XX.bin
```

6. Exécutez le fichier binaire MDE de la nouvelle version.

```
/home/admin/ibm_sw_mde_X.x.x-XX.bin
```

7. Installez les RPM.

```
yum -y install /home/admin/rpms/*
```

8. Exécutez le script de mise à niveau.

```
/opt/securityfirst/spsd/bin/spsd-pgsetup --upgrade
```

9. Démarrez à nouveau le service de règle PPM :

```
systemctl start spsd
```

## Mise à niveau à partir d'une version précédente

### Pourquoi et quand exécuter cette tâche

Vous devez effectuer ces étapes pour que la règle soit appliquée.

#### Procédure

1. Accédez à la page Informations sur l'agent
2. Cliquez sur "Modifier la règle principale"
3. Cliquez sur "Enregistrer, Instantané et Activer"
4. Approuvez la tâche
5. Revenez à la machine virtuelle de l'agent et tentez d'effectuer une action de lecture/écriture sur un répertoire dans la règle (connectez-vous au répertoire de la règle en tant qu'utilisateur disposant des droits sur ce répertoire) et vérifiez que l'utilisateur non défini n'est pas autorisé.

## Pour la machine virtuelle cible de l'agent

### Agents Linux/AIX

#### Pourquoi et quand exécuter cette tâche

##### Procédure

1. Créez un nouveau répertoire d'agent et accédez à ce répertoire

```
mkdir [nouveau_répertoire_agent]
cd [nouveau_répertoire_agent]
```

2. Téléchargez ou exécutez la commande curl sur le bundle d'installation de l'agent correspondant

```
curl --header "Accept: application/x-tar" -u
nom_utilisateur:mot_de_passe
https://<Adresse_IP_PPM>/rest/agents/ID_agent/install_bundle> nom_bundle_installation.tar
```

3. Décompressez le bundle d'installation

```
tar xvf <nom_bundle_installation>.tar
```

4. Exécutez les scripts setup.sh pour réinstaller l'agent

```
./setup.sh
```

5. A l'invite, répondez yes pour redémarrer l'agent.
6. Vous pouvez supprimer tous les fichiers d'installation précédents du répertoire d'agent précédent, si vous le souhaitez.

```
rm -rf [/ancien répertoire de l'agent]
```

### Agents Windows

#### Pourquoi et quand exécuter cette tâche

## Procédure

1. Téléchargez le bundle d'installation de l'agent correspondant
2. Décompressez le bundle d'installation
3. Exécutez le programme d'installation .msi pour installer le nouveau logiciel de l'agent
4. Répondez oui pour redémarrer l'agent lorsque vous y êtes invité

## Données de service

---

### Collecte des données du service

La collecte des données du service s'effectue via un script exécuté dans la machine virtuelle MDE.

Le script spsd-service se trouve dans la machine virtuelle MDE dans le répertoire /opt/securityfirst/spsd/bin.

```
sudo /opt/securityfirst/spsd/bin/spsd-service --help
Syntaxe : spsd-service [OPTIONS]

OPTIONS :
--nodb Ne pas vider la base de données
--norest Ne pas extraire de données de l'API REST
--nosys Ne pas extraire de données système (/var/log, /proc etc.)
--withcore Extraire une image-mémoire de spsd
--help Afficher cette aide
```

Pour exécuter une collecte des données du service :

```
sudo /opt/securityfirst/spsd/bin/spsd-service
```

### Suppression des informations sensibles des journaux du PPM

Pour aider à protéger la confidentialité d'une installation PPM lorsque les données de service quittent la limite logique du PPM, les journaux de débogage MDE suivants étiquettent les informations sensibles à l'aide d'une syntaxe d'étiquette spécialisée :

- bundleAll.log
- bundleWarnPlus.log
- debug.log
- warn.log

**Remarque :** Contenus dans un fichier de données de service compressé (résultant du processus de collecte de données de service ci-dessus), ces journaux se trouvent dans le dossier "logs".

Ces balises ont le format #<tagname>(<tagdata>) où <tagdata> est remplacé par les données à baliser et <tagname> est l'un des éléments suivants :

- user - pour baliser des noms d'utilisateurs, qu'il s'agisse d'utilisateurs MDE ou des utilisateurs d'un service externe auquel MDE s'intègre. *Exemple : #user(admin)*
- group - pour baliser des noms de groupe. *Exemple : #group(domainusers)*
- email - pour baliser des adresses e-mail. *Exemple : #email(example@example.com)*
- ip - pour baliser des adresses IP. *Exemple : #ip(192.168.0.5)*
- host - pour baliser des noms d'hôte de réseau. *Exemple : #host(dns.example.com)*
- key - pour baliser des clés cryptographiques **publiques** ou une valeur associée telle qu'un nom de clé gérée. *Exemple : #key(HRKey2)*
- cert - pour baliser des données de certificat telles qu'un nom distinctif d'un agent se connectant. *Exemple : #cert(C=US, ST=UT, L=Provo, O=Example Corp., OU=architecture, CN=docserver4)*

- fingerprint - pour baliser les empreintes digitales d'un certificat. *Exemple :*  
*#fingerprint(41:1A:B9:89:DB:77:90:77:39:D0:DF:5E:98:90:B7:17*

Les balises peuvent être retirées des données du service à l'aide d'un processus similaire à cet exemple qui supprime les données balisées avec #user de bundleAll.log :

```
gunzip spsd-service-2018-01-24T141620-0800.tar.gz
tar xf spsd-service-2018-01-24T141620-0800.tar ./logs/bundleAll.log
sed -i '/\#user/c\REDACTED' logs/bundleAll.log
tar --delete --file=spsd-service-2018-01-24T141620-0800.tar ./logs/bundleAll.log
tar --append --file=spsd-service-2018-01-24T141620-0800.tar ./logs/bundleAll.log
gzip spsd-service-2018-01-24T141620-0800.tar
```





---

# Annexe A. Exemple de processus d'installation d'agent

Les sections qui suivent décrivent la procédure générale d'installation du bundle d'installation de l'agent. Ces méthodes ne sont fournies qu'à titre d'exemple et ne sont pas des instructions d'installation prises en charge.

## Processus Red Hat / CentOS

---

### Pourquoi et quand exécuter cette tâche

#### Transfert du bundle d'installation par le biais de CURL :

##### Procédure

1. Connectez-vous au système cible.
2. Assurez-vous qu'une connexion réseau valide au serveur MDE est établie.
3. Assurez-vous que l'ensemble des utilisateurs, des groupes et des chemins d'accès ou des unités identifiés dans une règle sont créés, associés et configurés sur le système.
4. Connectez-vous à MDE.
5. Dans MDE, mettez un agent en service pour le système cible.
6. Dans MDE, affichez les détails de l'agent et notez l'URL de téléchargement.

### Users

**Authorized Users** admin

**Install Files Download URL** /rest/agents/1/install\_bundle

[Download Zip Bundle](#)

[Download Tar Bundle](#)

7. A partir du système cible, créez un répertoire pour le téléchargement de l'agent et accédez à ce répertoire
8. Téléchargez le bundle TAR à l'aide de la commande curl suivante :

```
[user@localhost]$ curl -k --header "Accept: application/x-tar" -u admin:admin https://<adresse_IP PPM>/<URL_téléchargement> > package.tar
```

Exemple d'utilisation d'un utilisateur défini dans PPM :

```
[user@localhost]$ curl -k --header "Accept: application/x-tar" -u admin:admin-password https://1.1.1.10/rest/agents/1/install_bundle > package.tar
```

Exemple d'utilisation d'un utilisateur défini LDAP dans PPM :

```
[user@localhost]$ curl -k --header "X-Directory: tenant1" --header "Accept: application/x-tar" -u john:secret https://1.1.1.10/rest/agents/1/install_bundle > package.tar
```

(en supposant que l'identificateur de répertoire est "tenant1", le nom d'utilisateur est "john" et le mot de passe est "secret")

9. Sur le système cible, décompressez le package TAR :

```
[user@localhost]$ tar -xf package.tar
```

10. Sur le système cible, exécutez le script de configuration en tant que superutilisateur

```
[user@localhost]$./setup.sh
```

11. Une fois le script de configuration terminé, l'agent est installé et la règle est téléchargée à partir de MDE et est appliquée.

## Processus AIX

---

### Pourquoi et quand exécuter cette tâche

#### Transfert du bundle d'installation :

1. Connectez-vous au système cible.
2. Assurez-vous qu'une connexion réseau valide au serveur MDE est établie.
3. Assurez-vous que l'ensemble des utilisateurs, des groupes et des chemins d'accès ou des unités identifiés dans une règle sont créés, associés et configurés sur le système.
4. Connectez-vous à MDE.
5. Dans MDE, mettez un agent en service pour le système cible.
6. Dans MDE, affichez les détails de l'agent et notez l'URL de téléchargement

#### Users

**Authorized Users** admin

**Install Files Download URL** /rest/agents/1/install\_bundle

Download Zip Bundle

Download Tar Bundle

7. A partir du système cible, créez un répertoire pour le téléchargement de l'agent et accédez à ce répertoire
8. Transférez le bundle sur le système cible.
9. Sur le système cible, décompressez le package TAR :

```
[user@localhost]$ tar -xf package.tar
```

10. Sur le système cible, exécutez le script de configuration en tant que superutilisateur.

```
[user@localhost]$./setup.sh
```

11. Une fois le script de configuration terminé, l'agent est installé et la règle est téléchargée à partir de MDE et est appliquée.

## Processus Windows Server

---

### Pourquoi et quand exécuter cette tâche

#### Transfert du bundle d'installation :

#### Procédure

1. Connectez-vous au système cible.

2. Assurez-vous qu'une connexion réseau valide au serveur MDE est établie.
3. Assurez-vous que l'ensemble des utilisateurs, des groupes et des chemins d'accès ou des unités identifiés dans une règle sont créés, associés et configurés sur le système.
4. Connectez-vous à MDE.
5. Dans MDE, mettez un agent en service pour le système cible.
6. Dans MDE, affichez les détails de l'agent et notez l'URL de téléchargement.

## Users

**Authorized Users** admin

**Install Files Download URL** /rest/agents/1/install\_bundle

[Download Zip Bundle](#)

[Download Tar Bundle](#)

7. Cliquez sur Télécharger le bundle ZIP pour télécharger le fichier ZIP du logiciel de l'agent sur le système local.
8. Transférez le bundle d'installation sur le système cible.
9. Sur le système cible, extrayez le contenu du bundle de fichiers ZIP.
10. Exécutez le fichier MSI du bundle d'installation.

**FileAgent-<version>.msi**

Exemple :

**PS C:\> FileAgent-4.2.11-0030.msi**

11. Une fois le script de configuration terminé et l'agent correctement installé, la règle est appliquée.

**Remarque** : Un redémarrage est nécessaire. Pour ignorer l'invite de redémarrage, vous pouvez exécuter la commande avec l'option de "non redémarrage" : **msiexec /i <agent\_filename\_version.msi> NO\_REBOOT\_PROMPT=1**



# Annexe B. Exemples de certificats de l'autorité de certification

## Pourquoi et quand exécuter cette tâche

MDE requiert des certificats signés par une autorité de certification pour établir une session sécurisée entre le serveur de gestion (PPM) et les agents. Sont nécessaires :

- un magasin de clés
- un magasin de clés de confiance
- un bundle de certificats de l'autorité de certification

Une autorité de certification interne basée sur RSA ou une autorité de certification tierce peut être utilisée pour signer des certificats. Dans l'exemple Linux ci-dessous, les éléments suivants sont créés :

- La demande de signature de certificat (CSR) est créée et envoyée à l'autorité de certification pour être traitée. Le certificat signé et la clé sont combinés pour créer un magasin de clés.
- Un magasin de clés de confiance est créé à l'aide du bundle de certificats de l'autorité de certification.
- Un certificat d'agent est créé. Ces certificats sont requis pour la communication entre PPM et les agents.

Cet exemple est fourni à des fins pratiques. Vous devez adhérer à votre autorité de certification lors de la génération des certificats à signer. Les noms entre crochets [nom.pem] représentent les noms de fichiers qui peuvent être différents ou modifiés lors de l'utilisation de certificats émanant de la société ou de tiers.

Pour créer un magasin de clés, vous devez soumettre une demande de signature de certificat à l'autorité de certification interne de l'entreprise ou à une autorité de certification tierce.

## Procédure

1. Créez un fichier de configuration OpenSSL (par exemple ppm.cnf) contenant les informations suivantes :

```
[req]
default_bits = 4096
distinguished_name = req_distinguished_name
req_extensions = v3_req
prompt = no

[req_distinguished_name]
C = your_country
ST = your_state_or_province
L = your_locale_(city)
O = your_organization
OU = your_org_unit_(department)
CN = your_ppm_host.your_domain

[v3_req]
Extensions to add to a certificate request
basicConstraints = CA:FALSE
extendedKeyUsage = serverAuth
subjectAltName = @alt_names

[alt_names]
DNS.1 = your_ppm_host.your_domain
IP.1 = your_ppm_ip_address
```

Vous devez mettre à jour les sections [req\_distinguished\_name] et [alt\_names] pour refléter les informations propres à votre organisation.

2. Créez une demande de signature de certificat pour PPM

```
openssl req -out [csr.pem] -new -newkey rsa:2048 -keyout [key.pem] -outform pem
```

3. La demande de signature de certificat [csr.pem] doit être signée par l'autorité de certification (CA)
4. Après avoir reçu le certificat signé de l'autorité de certification, vérifiez que l'utilisation de clé étendue et les noms alternatifs du sujet sont présents

```
openssl x509 -in [signed cert] -noout -text
```

5. Combinez le certificat signé et la clé (clé de l'étape 2)

```
a. openssl pkcs12 -export -out [ppm.p12] -inkey [key.pem] -in [signed-cert] -name ppm
b. keytool -importkeystore -srckeystore [ppm.p12] -keystore [ppm.jks] -storetype JKS
```

Pour créer un magasin de clés de confiance, vous devez utiliser le certificat de l'autorité de certification utilisé pour signer les demandes de signature de certificat. Cet ensemble est également appelé bundle de certificats de l'autorité de certification. Remplacez "ca\_bundle.crt" ci-dessous par le nom réel de ce certificat.

- a. Créez un magasin de clés de confiance à l'aide du bundle de certificats de l'autorité de certification. Si le bundle de certificats de l'autorité de certification contient plusieurs certificats, ils doivent être séparés et importés dans un magasin de clés de confiance de manière individuelle.

```
a. keytool -import -trustcacerts -file [ca_bundle-1.crt] -alias CA1 -keystore [trust.jks]
b. keytool -import -trustcacerts -file [ca_buncle-2.crt] -alias CA2 -keystore [trust.jks]
c. continue for each certificate in bundle
```

- b. Copiez les fichiers \*.jks et [ca\_bundle.crt] obtenus sur le serveur PPM dans un répertoire sécurisé (par exemple /etc/ppm/certs). Cet emplacement est spécifié lorsque vous mettez à jour les fichiers de propriétés Web et Agent à l'aide du script spsd-certsetup (voir la configuration du serveur de gestion ci-dessous).

Un certificat d'agent MDE est également requis.

- a. Créez un fichier de configuration OpenSSL (par exemple, host01.cnf) contenant les informations suivantes :

```
[req]
default_bits = 2048
distinguished_name = req_distinguished_name
req_extensions = v3_req
prompt = no

[req_distinguished_name]
C = your_country
ST = your_state_or_province
L = your_locale_(city)
O = your_organization
OU = your_org_unit_(department)
CN = your_agent_host.your_domain

[v3_req]
Extensions to add to a certificate request
basicConstraints = CA:FALSE
extendedKeyUsage = clientAuth
subjectAltName = @alt_names

[alt_names]
DNS.1 = your_agent_host.your_domain
IP.1 = your_agent_ip_address
```

Vous devez mettre à jour les sections [req\_distinguished\_name] et [alt\_names] pour refléter les informations propres à votre organisation.

- b. Créez une demande de signature de certificat d'agent MDE

```
a. openssl req -out [host01.csr] -nodes -sha256 -newkey rsa:2048 -keyout [host01.key] -config [host01.cnf]
```

- c. Soumettez la demande de signature de certificat à l'autorité de certification (CA)
- d. Après avoir reçu le certificat signé de l'autorité de certification, vérifiez que l'utilisation de clé étendue et les noms alternatifs du sujet sont présents

```
a. openssl x509 -in [signed-agent] -noout -text
```

- e. Si le certificat d'agent a été signé par une autorité de certification différente de celle du certificat du PPM, le certificat CA\_bundle doit être importé dans le magasin de clés de confiance du PPM. Veuillez vous reporter à l'étape 5 du processus de création de certificat de PPM ci-dessus

- f. Combinez le certificat signé et la clé

```
a. cat [signed-agent] [host01.key] > [host01.pem]
```

- g. Utilisez la paire cert/clé [host01.pem] lors de la création d'un agent pour cet hôte dans MDE

```
a. [host01.pem] is uploaded using a browser during the PPM agent creation.
```

Copiez [host01.pem] vers votre poste de travail ou vers une ressource partagée afin qu'elle soit accessible durant la création de l'agent PPM.

Suivez le processus ci-dessous pour chaque hôte sur lequel un agent sera installé.

#### Configuration du serveur de gestion

Le processus de configuration du serveur de gestion doit mettre à jour les certificats avant la configuration de tout agent de règles. Cette opération nécessite l'exécution du script fourni (/opt/securityfirst/spsd/bin/spsd-certsetup) sur le serveur (voir la section relative aux paramètres du certificat du serveur du guide d'administration) après le téléchargement du magasin de clés et du magasin de clés de confiance de votre société ainsi que d'un bundle de certificats de l'autorité de certification. Vous devez également redémarrer le service spsd ou réamorcer le serveur de gestion (PPM). Faute de quoi, les agents ne pourront pas communiquer avec le serveur d'administration MDE.

Si les certificats n'ont pas été mis à jour et qu'un agent a été configuré, l'exécution du script de mise à jour des certificats et la mise à jour du certificat d'agent sur la page Informations sur l'agent rétablissent la communication entre l'agent et le serveur de gestion MDE.





---

## Annexe C. Exemple de conversion pour créer un fichier PKCS12

### **Pourquoi et quand exécuter cette tâche**

La procédure ci-dessous permet de combiner la clé privée du client et le certificat client pour former un fichier PKCS12 (Public Key Cryptography Standard #12) unique :

```
[user@localhost]$ openssl pkcs12 -export -out ppmclient.p12 -inkey client_key.pem -in client_cert.pem
-name ppmclient
```

```
[user@localhost]$ keytool -v -list -keystore ppmclient.p12 -storetype pkcs12
```



---

## Annexe D. Choses à faire et à ne pas faire

---

### Modification des clés affectées

---

#### Présentation

J'ai des données dans un répertoire protégé et je souhaite modifier la clé associée à ce répertoire.

#### Contexte

Les données dans un répertoire sont chiffrées avec la clé définie lors de la création des données (ou un déplacement dans ce répertoire). La modification d'une clé de règle ne migre pas les données préexistantes vers la nouvelle clé.

Lorsqu'une règle a été appliquée à un agent et qu'elle est active, il est potentiellement très dangereux de modifier les valeurs de clé des répertoires protégés. Même si cela n'est pas strictement interdit, la modification d'une valeur de la clé peut entraîner une perte de données.

##### A faire

Si l'administrateur souhaite migrer un répertoire entier d'une clé vers une autre clé, il doit d'abord déplacer les données de ce répertoire. Une fois le répertoire vide, la valeur de la clé associée par le biais d'une règle peut être modifiée et appliquée. Ensuite, les données peuvent être remplacées dans ce répertoire et elles sont chiffrées avec la nouvelle clé.

##### A ne pas faire

Ne modifiez pas la valeur de la clé associée à la règle et n'activez pas la règle sans avoir d'abord migré les données du répertoire. Si vous ne suivez pas la méthode recommandée, les données qui se trouvaient initialement dans le répertoire restent chiffrées par la clé initiale. Une fois qu'une règle est modifiée avec la nouvelle clé, les données sont inaccessibles. De plus, en cas de rotation de la clé initiale, les données sont définitivement inaccessibles, car il n'y aurait aucun moyen de rétablir la règle en fonction de la valeur initiale de la clé.

---

### Rotation des clés avec des sauvegardes chiffrées

---

#### Présentation

Je souhaite sauvegarder des données situées dans un répertoire protégé.

#### Contexte

Les données de sauvegarde dans ce format chiffré lient les données à la valeur de la clé lors de la sauvegarde. En cas de rotation d'une clé après l'opération de sauvegarde, elle ne peut pas être restaurée correctement.

Les clés doivent être associées à un emplacement protégé et non à des données. On évitera ainsi les problèmes d'accès non intentionnel aux données en cas de restauration.

##### A faire

Les données dans un répertoire sont chiffrées avec la clé définie lors de la création des données (ou un déplacement dans ce répertoire). Il est recommandé de sauvegarder les données avant la rotation de la clé. L'utilitaire d'agent "spx-backup" peut être utilisé pour effectuer cette opération. Ceci sauvegardera

les données avec une clé qui n'est pas basée sur le répertoire protégé et qui n'est pas affecté par la rotation des clés.

#### A ne pas faire

Soyez prudent lorsque vous copiez le répertoire protégé dans sa forme chiffrée (par exemple, une image de disque ou un instantané de machine virtuelle). Si cette opération est effectuée, les données peuvent être inaccessibles après la rotation de clé initiale.

---

## Annexe E. Chiffrement sur place

Afin de permettre le chiffrement sur des structures de répertoires et des données préexistantes et de déterminer l'état des données à tout moment, MDE fournit un utilitaire de ligne de commande appelé "spxconvert".

Cette fonctionnalité est non seulement capable de chiffrer des données préexistantes, mais elle est également utile lors d'un audit tel que PCI (Payment Card Industry) ou HIPAA (Health Insurance Portability and Accountability Act).

**Remarque :** Cette fonctionnalité ne fonctionne qu'avec les Agents de type Fichier et ne couvre pas les volumes qui nécessitent une migration de données formelle.

---

### Options de commande

Syntaxe de **spxconvert** : (les paramètres sont indiqués entre crochets [ ] et incluent le type)

-h (-?, ?) 'Imprimer cette boîte de dialogue d'aide'

-a 'Effectuer un audit des fichiers chiffrés'

-p [STR] 'Audit du chemin'

-e [STR] 'Chiffrer les fichiers non protégés dans le chemin d'accès'

-c 'Vider toutes les sommes de contrôle avant/après la conversion des fichiers'

-v 'Mode prolix - Impression supplémentaire pour les informations ajoutées'

Audit (-a)

Par défaut, l'audit est effectué sur tous les répertoires de règles. Vous pouvez réduire l'audit à un seul répertoire en utilisant l'option -p. Un audit imprime tous les fichiers non chiffrés d'un répertoire et imprime le nombre total de fichiers chiffrés d'un répertoire.

Encrypt (-e)

Convertissez tous les fichiers non protégés dans le répertoire spécifié. A la fin du processus, tous les fichiers comportant des sommes de contrôle non concordantes sont affichés pour l'utilisateur.

L'indicateur -c facultatif imprime les sommes de contrôle de tous les fichiers à la fin du processus, et pas seulement de ceux qui sont en conflit. Les sommes de contrôle ne peuvent être imprimées qu'une fois l'analyse des performances terminée, car le cache du système doit être vidé après la conversion. Le vidage des caches après chaque fichier aurait un important impact négatif sur les performances.

### Etapas d'audit

1. Affichez s'il existe des éléments en attente de chiffrement :

**spxinfo -l**

1. Affichez des informations détaillées sur les données :

**spxconvert -a -v**

1. Affichez des informations détaillées sur un répertoire spécifique :

**spxconvert -p -v <chemin>**

### Etapas de chiffrement

1. Afficher les éléments en attente de chiffrement :

**spxinfo -l**

1. Afficher toutes les sommes de contrôle avant le chiffrement :

**spxconvert -c -p <chemin>**

1. Chiffrer tous les fichiers dans un chemin spécifique :

**spxconvert -p -v <chemin>**

1. Afficher toutes les sommes de contrôle sur un chemin spécifique après le chiffrement :

**spxconvert -c -p <chemin>**

---

## Annexe F. Journalisation de débogage d'agent

Par défaut, les agents de règles fonctionnent avec des messages de niveau de débogage qui sont omis lors de la journalisation. Pour capturer les messages de niveau de débogage dans le journal de l'agent, l'administrateur système de l'agent doit activer cette fonctionnalité, puis redémarrer l'agent pour lancer la capture des messages de débogage.

Les valeurs valides sont comprises entre 1 et 6 ; cependant, la valeur par défaut est '4' et toute valeur inférieure à '4' peut omettre des informations utiles.

### Remarque critique

- L'activation de la journalisation au niveau du débogage peut révéler des informations système sensibles
- En raison de la nature des messages de débogage, la taille des fichiers journaux d'agent peut augmenter considérablement.

---

## Agents Linux

### Pourquoi et quand exécuter cette tâche

Activez le débogage en localisant le fichier de configuration situé dans **/etc/sysconfig/spx-policyagent** et définissez l'indicateur inscriptible (**chmod +w /etc/sysconfig/spx-policyagent**).

Ajoutez à la fin du fichier, "**LOG\_LEVEL=6**" sans guillemets.

---

## Agents Windows

### Pourquoi et quand exécuter cette tâche

Activez le débogage en localisant la clé de registre située dans **HKLM\SYSTEM\CurrentControlSet\Services\Spx Policy Agent\log level** et définissez la valeur sur '**6**'.





## Annexe G. Déploiement non OVA

Les exemples suivants indiquent comment configurer un environnement non-OVA pour le déploiement PPM. Ces instructions sont uniquement applicables si vous ne déployez pas l'OVA PPM fournie, et créez à la place votre propre environnement RHEL ou CentOS 7.x pour y déployer le logiciel PPM.

Installez ces packages sur tous les noeuds PPM.

**Remarque :** Ceci n'est qu'un exemple de configuration. De nombreux besoins spécifiques à l'environnement peuvent invalider ces instructions. Merci de contacter le support pour obtenir de l'aide.

1. Installez java 1.8 et postgresql 9.2.

**Remarque :** Vous serez invité à entrer un mot de passe durant le processus initdb. Il s'agira du mot de passe postgres "superuser".

```
yum install -y postgresql-server java-1.8.0-openjdk-headless
passwd postgres
su - postgres
initdb --auth=md5 -W
exit
```

2. Installez les règles d'administration de pare-feu.

L'exemple ci-dessous montre comment installer les règles d'administration de pare-feu avec iptables. D'autres méthodes peuvent fonctionner tout aussi bien et peuvent être utilisées conformément aux préférences de votre site. Exemple : `yum install -y iptables iptables-services`

Les deux prochaines commandes supposent que vous avez installé et activé firewalld. Si firewalld n'est pas installé, l'exécution de ces commandes n'aura aucune conséquence négative.

```
systemctl stop firewalld
systemctl disable firewalld
```

Démarrez et videz le service de pare-feu IP Tables

```
systemctl start iptables.service
iptables -F
```

Activez le service iptables - Etape facultative - Vous pouvez sauter cette étape si vous n'avez pas besoin d'un pare-feu basé sur un logiciel local

```
systemctl enable iptables.service
```

Définissez un pare-feu de base - Etape facultative - vous pouvez sauter cette étape si vous n'avez pas besoin d'un pare-feu basé sur un logiciel local

```
iptables -A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --
update --seconds 60 --hitcount 4 --name DEFAULT --rsource -j LOG --log-prefix
"SSH BruteForce: "
iptables -A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --
update --seconds 60 --hitcount 4 --name DEFAULT --rsource -m recent --set --name
ssh --rsource
iptables -A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
service iptables save
```

3. Installez les packages Keepalive, HAProxy et PSMisc.

```
yum install -y haproxy keepalived psmisc
```

4. Téléchargez Zookeeper.

**Remarque :** Si wget n'est pas installé, installez-le :

```
yum install -y wget
wget http://apache.claz.org/zookeeper/zookeeper-3.4.10/zookeeper-3.4.10.tar.gz
mkdir /home/admin
mv zookeeper-3.4.10.tar.gz /home/admin
```

5. Installez et configurez une source horaire de réseau fiable.

L'exemple ci-dessous montre une configuration NTP mais d'autres sources horaires fiables peuvent fonctionner tout aussi bien et être utilisées conformément aux préférences de votre site.

```
yum install -y ntp
sed -i "/server\ [0-9].rhel/ s/rhel/us/" /etc/ntp.conf
sed -i "/server\ [0-9].centos/ s/centos/us/" /etc/ntp.conf
systemctl stop chronyd
systemctl disable chronyd
systemctl start ntpd
systemctl enable ntpd
```

6. Installez le répertoire EPRL

```
yum install -y epel-release
```

7. Installez le générateur de nombres aléatoires imprévisibles (nécessite EPEL).

```
yum install -y haveged
```

8. Installez net-tools pour la collecte des données de service.

```
yum install -y net-tools
```

---

## Annexe H. Vérification de la version logicielle

Utilisez les commandes suivantes pour vérifier la version logicielle.

### Version PPM

Dans l'interpréteur de commande de la machine virtuelle PPM, exécutez la commande suivante :

```
cat /etc/ppm/buildinfo/release
```

### Version de l'agent Linux

Dans l'interface de ligne de commande Linux, exécutez la commande suivante :

```
yum list policyagent
```

### Version de l'agent AIX

Dans l'interface de ligne de commande AIX, exécutez la commande suivante :

```
rpm -qa | grep fileagent
```

### Version de l'agent Windows

Accédez à **Ajout/Suppression de programmes** dans Windows. Faites défiler l'écran pour trouver le nom de l'agent.

| Type d'agent           | Nom de l'agent dans Windows |
|------------------------|-----------------------------|
| Fichier avec une règle | FileAgent                   |
| Volume                 | VolumeAgent                 |
| Volume avec une règle  | HybridAgent                 |



## Annexe I. Glossaire

|                                         |                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| agent                                   | Serveur géré exécutant le chiffrement Security First et un logiciel de contrôle d'accès.                                                                                                                                                                                                              |
| agent de fichier                        | L'agent de fichier applique les définitions de règle d'accès opérationnelles et l'association d'un ou de plusieurs chemins d'accès protégés. Chaque chemin d'accès à un fichier protégé peut posséder son propre contrôle d'accès opérationnel et cryptographique.                                    |
| agent de type Magasin d'objets          | L'agent de type Magasin d'objets chiffre et fractionne les données à envoyer et les stocke de manière sécurisée dans un système de stockage d'objets efficace et hautement évolutif (dans le cloud et/ou sur site).                                                                                   |
| agent de type Volume                    | Un Agent de type Volume applique la définition des règles de volume et l'association d'un ou de plusieurs volumes protégés sur un système cible.                                                                                                                                                      |
| agent de type Volume avec une règle     | Un Agent de type Volume avec une règle utilise la protection de la règle de volume d'un agent de type Volume et permet l'application de règles de contrôle d'accès opérationnel basées sur des fichiers sur un ou plusieurs chemins de fichiers protégés. Egalement connu sous le nom "agent hybride" |
| Amazon Web Services (AWS) S3            | Service de stockage simple qui stocke et extrait des données. Il s'agit d'un stockage d'objets hautement évolutif et économique.                                                                                                                                                                      |
| archive de virtualisation ouverte (OVA) | Fichier archive au format TAR. Ensemble des fichiers OVF compressés en un seul fichier.                                                                                                                                                                                                               |
| autorité de certification               | Organisation approuvée pour signer des certificats numériques. L'autorité de certification vérifie l'identité et la légitimité de la demande de certificat soumise. Si la vérification de la demande aboutit, l'autorité de certification émet des certificats signés.                                |
| broyage de clé                          | Suppression des clés d'application des règles dans l'environnement d'un agent entraînant une restriction d'accès aux données cryptographiques irrécupérables. Cette action rend les données définitivement illisibles.                                                                                |
| CEF (Comma Event Format)                | Type de syntaxe de format d'événement commun transmis à un système d'informations de sécurité et de gestion des événements (SIEM).                                                                                                                                                                    |
| clés auto-générées                      | Clés d'application des règles créées et gérées par MDE. Lors de la création des règles, elles sont désignées par la clé auto-générée.                                                                                                                                                                 |

|                                            |                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cloud Auditing Data Federation (CADF)      | Type de syntaxe de format d'événement commun transmis à un système d'informations de sécurité et de gestion des événements (SIEM).                                                                                                                                                                                          |
| contrôle d'accès basé sur les rôles (RBAC) | Mode de régulation de l'accès à des ressources informatiques ou réseau selon les rôles des utilisateurs dans une entreprise. Dans ce contexte, l'accès est la capacité d'une personne à effectuer une tâche spécifique, comme afficher, créer ou modifier un fichier.                                                       |
| contrôles d'accès cryptographiques         | Possibilité de séparer l'accès utilisateur en utilisant un autre matériel de chiffrement.                                                                                                                                                                                                                                   |
| CSV (Comma Separated Value)                | Format de données qui utilise une virgule pour délimiter les champs et un retour à la ligne pour délimiter les enregistrements.                                                                                                                                                                                             |
| CURL                                       | CURL est un projet logiciel informatique fournissant une bibliothèque et un outil de ligne de commande pour transférer des données à l'aide de différents protocoles.                                                                                                                                                       |
| DHCP (Dynamic Host Configuration Protocol) | Protocole client/serveur qui fournit automatiquement un hôte de protocole Internet (IP) avec son adresse IP et d'autres informations de configuration associées, comme le masque de sous-réseau et la passerelle par défaut.                                                                                                |
| Distinguished Encoding Rules (DER)         | DER est l'une des règles de codage ASN.1 définies dans la spécification ITU-T X.690, 2002. Une règle de codage de la structure de données fournit une syntaxe de transfert qui régit la manière dont les octets d'un flux sont organisés lorsqu'ils sont envoyés d'un ordinateur à l'autre.                                 |
| données protégées                          | Données traitées.                                                                                                                                                                                                                                                                                                           |
| gestionnaire de volumes logiques           | Gestionnaire de périphériques de stockage qui utilise une infrastructure de noyau Linux mappeur de périphériques pour rassembler des périphériques de stockage dans des groupes et alloue des unités logiques à partir de l'espace combiné selon les besoins. La plupart des distributions Linux sont compatibles avec LVM. |
| haute disponibilité (HA)                   | Les opérations du système continuent même en cas d'échec des composants échouent, grâce à la redondance (alimentations, processeurs, unités, logiciels, etc. redondants).                                                                                                                                                   |
| HTTP (Hypertext Transfer Protocol)         | Protocole d'application qui sert de base aux communications de données pour le World Wide Web.                                                                                                                                                                                                                              |

|                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| hyperviseur                                                     | Egalement appelé "moniteur de machine virtuelle". Un hyperviseur ou moniteur de machine virtuelle (MMV) est un composant de logiciel, de microprogramme ou de matériel qui crée, exécute et gère des machines virtuelles. L'ordinateur sur lequel un hyperviseur exécute une ou plusieurs machines virtuelles est appelé "ordinateur hôte", et chaque machine virtuelle est appelée "ordinateur invité". L'hyperviseur VMware est également appelé "hôte ESXi". |
| IBM Cloud Object Storage (COS S3)                               | Plateforme de stockage contenant de grandes quantités de données, telles que des sauvegardes, des archives, des fichiers vidéo et des fichiers d'image et permettant de disposer de données au repos ainsi que de bénéficier d'une disponibilité élevée.                                                                                                                                                                                                        |
| identificateur d'objet (OID)                                    | Mécanisme d'identification normalisé pour nommer un objet ou un concept avec un nom persistant globalement univoque.                                                                                                                                                                                                                                                                                                                                            |
| identificateur unique (UUID)                                    | L'identificateur unique (UUID) est une norme d'identification utilisée lors de la construction d'un logiciel. Un UUID (numéro sur 128 bits) est utilisé pour identifier de façon unique certains objets ou certaines entités sur Internet.                                                                                                                                                                                                                      |
| infrastructure à clés publiques (PKI)                           | Ensemble de rôles, règles et procédures requis pour créer, gérer, distribuer, utiliser, stocker et révoquer des certificats numériques et gérer le chiffrement par clés publiques.                                                                                                                                                                                                                                                                              |
| interface de ligne de commande (CLI)                            | Type d'interaction où l'utilisateur émet des commandes vers l'application sous la forme de lignes de texte (lignes de commande)                                                                                                                                                                                                                                                                                                                                 |
| interface graphique utilisateur (GUI)                           | Type d'interface utilisateur, qui permet à des utilisateurs d'interagir avec MDE par le biais d'icônes graphiques et non d'interfaces textuelles et de commandes saisies.                                                                                                                                                                                                                                                                                       |
| liste de révocation de certificat (CRL)                         | Liste publiée des certificats révoqués par l'autorité de certification (CA) qui a émis les certificats correspondants.                                                                                                                                                                                                                                                                                                                                          |
| Log Event Extended Format (LEEF)                                | LEEF est un format d'événement personnalisé pour IBM Security QRadar qui contient des événements lisibles et faciles à traiter pour QRadar. Ce format prend en charge plusieurs attributs d'événement prédéfinis pour la charge d'événement.                                                                                                                                                                                                                    |
| loi Health Insurance Portability and Accountability Act (HIPAA) | La réglementation HIPAA sur la confidentialité exige que les fournisseurs et les organisations assurent la confidentialité et la sécurité des renseignements médicaux protégés (PHI)                                                                                                                                                                                                                                                                            |
| machine virtuelle (MV)                                          | Emulation d'un système informatique basé sur l'architecture informatique et les fonctions d'un ordinateur réel ou hypothétique.                                                                                                                                                                                                                                                                                                                                 |

|                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| magasin de clés                                                    | Emplacement de stockage des clés d'application des règles configuré.                                                                                                                                                                                                                                                                                                                            |
| magasin de clés de confiance                                       | Un magasin de clés de confiance stocke les certificats émanant de l'autorité de certification (CA) de confiance utilisée pour permettre au serveur de vérifier les certificats dans une connexion SSL.                                                                                                                                                                                          |
| magasin de clés Java (JKS)                                         | Un magasin de clés Java (JKS) est un référentiel de certificats de sécurité - il peut s'agir de certificats d'autorisation ou de certificats de clé publique - plus des clés privées correspondantes. Le kit de développement Java (JDK) fournit un outil (keytool) pour gérer les clés et les certificats dans le magasin de clés. L'extension jks est un format de fichier spécifique à Java. |
| M sur N (M:N)                                                      | Modèle déterminant le nombre d'éléments de données requis pour la régénération des données (M) par rapport au nombre total d'éléments de données (partages) créés (N).                                                                                                                                                                                                                          |
| nom de domaine (DN)                                                | Nom d'une ressource Internet universellement unique et liée à des informations de destination IP                                                                                                                                                                                                                                                                                                |
| norme de chiffrement AES - Nouvelles instructions (AES-NI)         | Spécification pour le chiffrement des données électroniques établie par le National Institute of Standards and Technology (NIST) en 2001 ; protocole de chiffrement utilisé par les produits basés sur SPx.                                                                                                                                                                                     |
| NTP (Network Time Protocol)                                        | Protocole réseau de synchronisation des horloges entre des systèmes informatiques.                                                                                                                                                                                                                                                                                                              |
| Payment Card Industry (PCI)                                        | Norme utilisée pour augmenter les contrôles et la sécurité des données des titulaires de cartes afin de réduire la fraude.                                                                                                                                                                                                                                                                      |
| PEM                                                                | Format d'encodage couramment utilisé pour les certificats de sécurité dont la syntaxe et le contenu sont définis par des normes X.509 v3.                                                                                                                                                                                                                                                       |
| point de distribution de liste de révocation de certificat (CRLDP) | Champ de point de départ dans le certificat qui contient des informations sur le certificat révoqué par l'autorité de certification émettrice, y compris le nom, éventuellement les raisons de la révocation et le nom de l'émetteur de la liste de révocation de certificat.                                                                                                                   |
| PostgreSQL                                                         | PostgreSQL (prononcé "post-gress-Q-L") est un système de gestion de base de données (SGBD) relationnelle open source, développé par une équipe internationale de bénévoles. PostgreSQL n'est contrôlé par aucune société ni entité privée, et le code source est disponible gratuitement.                                                                                                       |



|                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| protocole LDAP (Lightweight Directory Access Protocol)                   | Protocole standard du secteur, ouvert, non lié à un fournisseur, d'accès et de gestion des informations de répertoire distribué sur un réseau. Protocole logiciel permettant à une personne d'effectuer une recherche dans des organisations, des personnes et d'autres ressources, comme des fichiers et des unités sur un réseau.                                                            |
| protocole OCSP (Online Certificate Status Protocol)                      | Protocole interne utilisé pour obtenir le statut de révocation des certificats numériques X.509.                                                                                                                                                                                                                                                                                               |
| Public Key Cryptography Standard #12 (PKCS12)                            | Norme cryptographique à clés publiques qui définit un format de fichier d'archive pour stocker de nombreux objets cryptographiques en un seul fichier. Elle est couramment utilisée pour regrouper une clé privée avec son certificat X.509 ou pour regrouper tous les membres d'une chaîne de confiance. Elle peut être chiffrée et signée.                                                   |
| ReFS                                                                     | Nouveau système de fichiers de Microsoft introduit avec Windows Server 2012 et conçu pour optimiser la disponibilité, l'évolutivité et l'intégrité des données.                                                                                                                                                                                                                                |
| Representational State Transfer Application Program Interface (API REST) | Une API RESTful, également connue sous le nom de service Web RESTful, est basée sur la technologie REST (Representational State Transfer), un style architectural et une approche des communications souvent utilisés dans le développement de services Web.                                                                                                                                   |
| révocation de clé                                                        | Suppression des clés d'application des règles dans l'environnement d'un agent entraînant une restriction d'accès aux données cryptographiques récupérables. Cette action rend les données temporairement illisibles.                                                                                                                                                                           |
| rotation de clé                                                          | Migration des clés d'application des règles dans l'environnement d'un agent entraînant une modification invisible pour les utilisateurs de l'accès aux données.                                                                                                                                                                                                                                |
| RSA                                                                      | Chiffrement à clé publique développé par Rivest, Shamir et Adelman (RSA) utilisant une clé publique et une clé privée pour sécuriser les données.                                                                                                                                                                                                                                              |
| Secure Copy Protocol (scp)                                               | La commande scp est utilisée sous Linux pour transférer des fichiers entre systèmes via le protocole Secure Shell (SSH).                                                                                                                                                                                                                                                                       |
| Secure Socket Layer (SSL)                                                | Protocole cryptographique permettant de chiffrer la communication de données sur Internet à l'aide d'une clé asymétrique pour échanger des clés symétriques. Une autorité de certification et une infrastructure à clés publiques sont nécessaires pour permettre la vérification du certificat et du propriétaire, ainsi que pour générer, signer et administrer la validité des certificats. |

|                                 |                                                                                                                                                                                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| sélecteur                       | Utilisateurs et groupes définis par le système d'exploitation, qui peuvent accéder aux données, aux ensembles de chemins d'accès et aux autres fonctions liées aux règles.                                                                            |
| service de nom de domaine (DNS) | Service Internet qui convertit des noms de domaine en adresse IP.                                                                                                                                                                                     |
| SSH (Secure Socket Shell)       | Protocole réseau qui permet aux administrateurs d'accéder à un ordinateur distant de façon sécurisée. Le sigle SSH fait également référence à la suite d'utilitaires utilisés pour mettre en oeuvre ce protocole.                                     |
| système de fichiers NT (NTFS)   | Système de fichiers propriétaire développé par Microsoft dans le système d'exploitation Windows NT et utilisé pour stocker et récupérer des fichiers sur un disque dur prenant en charge la sécurité, la compression et l'audit au niveau du fichier. |
| temps universel coordonné (UTC) | Norme de <a href="#">temps</a> principale fixant l'heure dans le monde.                                                                                                                                                                               |
| <b>Terme</b>                    | <b>Définition</b>                                                                                                                                                                                                                                     |
| Transport Layer Security (TLS)  | Protocole cryptographique assurant des communications en toute sécurité sur un réseau informatique                                                                                                                                                    |
| vecteur d'initialisation (IV)   | Nombre aléatoire arbitraire ou imprévisible pouvant être utilisé avec une clé secrète pour le chiffrement de données utilisé une seule fois dans une session.                                                                                         |
| VMware ESXi™                    | Emulation d'un système informatique donné, basé sur une architecture informatique et les fonctions d'un ordinateur réel ou hypothétique.                                                                                                              |

## Remarques

Ce document peut être disponible dans d'autres langues auprès d'IBM. Toutefois, pour pouvoir accéder à une version traduite du document, il peut être nécessaire de disposer d'une copie ou d'une version du produit dans cette langue.

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing

IBM Corporation

North Castle Drive

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations

IBM Canada Ltd.

3600 Steeles Avenue East

Markham, Ontario

L3R 9Z7 Canada

**Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales.**

LE PRESENT DOCUMENT EST LIVRE "EN L'ETAT" SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies. Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Director of Licensing

IBM Corporation

North Castle Drive, MD-NC119

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations

IBM Canada Ltd.

3600 Steeles Avenue East

Markham, Ontario

L3R 9Z7 Canada

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le programme sous licence décrit dans ce document et tous les éléments sous licence disponibles sont fournis par IBM selon les conditions du Contrat sur les produits et services IBM, les conditions internationales d'utilisation de logiciels IBM ou d'un contrat équivalent.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

#### LICENCE DE COPYRIGHT :

Le présent document contient des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sous différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. Les exemples de programmes sont livrés "EN L'ETAT", sans aucune garantie. IBM n'est en aucun cas responsable des dommages liés à l'utilisation de ces exemples de programmes. Selon la façon dont vous affichez ces informations, certaines images et illustrations risquent de ne pas s'afficher.

#### Marques[r]

SPx et Security First Corp sont des marques de Security First Corp. dans de nombreux pays. D'autres produits et services peuvent être des marques de Security First Corp. ou d'autres sociétés.

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produit et de service peuvent appartenir à IBM ou à des tiers. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web "Copyright and trademark information" à l'adresse : <http://www.ibm.com/legal/copytrade.shtml>.

Adobe, le logo Adobe, PostScript et le logo PostScript sont des marques d'Adobe Systems Incorporated aux Etats-Unis et/ou dans certains autres pays.

Apache Software Foundation (ASF) est propriétaire de toutes les marques liées à Apache, marques de services et logos pour le compte des communautés de projet Apache, et les noms de tous les projets Apache sont des marques de l'ASF.

Node.JS est une marque de Joyent, Inc. CORPORATION DELAWARE 345 California Street; Suite 2000 San Francisco CALIFORNIE 94104.

Unicode et le logo Unicode sont des marques d'Unicode, Inc. aux Etats-Unis et dans d'autres pays.

Les marques CentOS sont des marques de Red Hat, Inc. ("Red Hat").

"Red Hat", Red Hat Linux, le logo Red Hat "Shadowman" et les produits mentionnés sont des marques de Red Hat, Inc. aux Etats-Unis et dans d'autres pays.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

Java ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

#### Dispositions de la documentation du produit[r]

Les droits d'utilisation de ces documents sont soumis aux dispositions suivantes :

**Applicabilité** : ces dispositions complètent les conditions d'utilisation du site web d'IBM.

**Usage personnel** : vous pouvez reproduire ces documents pour votre usage personnel, non commercial, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez pas distribuer, afficher ou dériver le travail de ces documents, ou une partie, sans le consentement exprès d'IBM.

**Usage commercial** : vous ne pouvez reproduire, distribuer et afficher ces documents qu'au sein de votre entreprise, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez pas

procéder à des travaux dérivés de ces publications, ni les reproduire, les distribuer ou les afficher en totalité ou partiellement en dehors de votre entreprise sans le consentement exprès d'IBM.

**Droits :** en dehors de ce qui est accordé dans cette autorisation, aucune autre autorisation, licence ou droit n'est accordé, expressément ou tacitement, sur les documents ou les informations, données, logiciels ou autres éléments couverts par la propriété intellectuelle contenus. IBM se réserve le droit de retirer les autorisations accordées ici si, à sa discrétion, l'utilisation des publications s'avère préjudiciable à ses intérêts ou si, selon son appréciation, les instructions susmentionnées n'ont pas été respectées. Vous ne pouvez télécharger, exporter ou réexporter ces informations qu'en total accord avec toutes les lois et règlements applicables dans votre pays, y compris les lois et règlements américains relatifs à l'exportation.

IBM N'OCTROIE AUCUNE GARANTIE SUR LE CONTENU DE CES PUBLICATIONS. LES DOCUMENTS SONT FOURNIS "EN L'ETAT" ET SANS AUCUNE GARANTIE, EXPRESSE OU TACITE, Y COMPRIS SANS S'Y LIMITER, LES GARANTIES TACITES DE COMMERCIALISATION, DE NON-CONTREFAÇON ET D'ADAPTATION A UN BUT PARTICULIER.

### **Considérations relatives aux règles de confidentialité[r]**

Les Logiciels IBM, y compris les Logiciels sous forme de services ("Offres Logiciels") peuvent utiliser des cookies ou d'autres technologies pour collecter des informations sur l'utilisation des produits, améliorer l'acquis utilisateur, personnaliser les interactions avec celui-ci, ou dans d'autres buts. Bien souvent, aucune information personnelle identifiable n'est collectée par les Offres Logiciels. Certaines Offres Logiciels vous permettent cependant de le faire. Si la présente Offre Logiciels utilise des cookies pour collecter des informations personnelles identifiables, des informations spécifiques sur cette utilisation sont fournies ci-dessous. Cette Offre Logiciels n'utilise pas de cookies ou d'autres techniques pour collecter des informations personnelles identifiables

Si les configurations déployées de cette Offre Logiciels vous permettent, en tant que client, de collecter des informations permettant d'identifier les utilisateurs par l'intermédiaire de cookies ou par d'autres techniques, vous devez solliciter un avis juridique sur la réglementation applicable à ce type de collecte, notamment en termes d'information et de consentement.

Pour plus d'informations sur l'utilisation à ces fins des différentes technologies, y compris celle des cookies, consultez les Points principaux de la Déclaration IBM de confidentialité sur Internet (<http://www.ibm.com/privacy>) et la section "Cookies, pixels espions et autres technologies" de la Déclaration IBM de confidentialité sur Internet sur le site <http://www.ibm.com/privacy/details>, ainsi que la section "IBM Software Products and Software-as-a-Service Privacy Statement" sur le site <http://www.ibm.com/software/info/product-privacy> (en anglais).

Numéro de produit : 5737-C67



## Remarques

---

Le présent document a été développé pour des produits et des services proposés aux Etats-Unis et peut être mis à disposition par IBM dans d'autres langues. Toutefois, pour pouvoir accéder à une version traduite du document, il peut être nécessaire de disposer d'une copie ou d'une version du produit dans cette langue.

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

*IBM Director of Licensing  
IBM Corporation  
North Castle Drive, MD-NC119  
Armonk, NY 10504-1785  
U.S.A.*

Pour le Canada, veuillez adresser votre courrier à :

*IBM Director of Commercial Relations  
IBM Canada Ltd.  
3600 Steeles Avenue East  
Markham, Ontario  
L3R 9Z7 Canada*

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse suivante :

*Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan Ltd.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokyo 103-8510, Japan*

**Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales.**

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Certaines juridictions n'autorisent pas l'exclusion des garanties tacites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font

pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

*IBM Director of Licensing  
IBM Corporation  
North Castle Drive, MD-NC119  
Armonk, NY 10504-1785  
U.S.A.*

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'ICA, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Tous les tarifs indiqués sont les prix de vente actuels suggérés par IBM et sont susceptibles d'être modifiés sans préavis. Les tarifs appliqués peuvent varier selon les revendeurs.

Ces informations sont fournies uniquement à titre de planification. Elles sont susceptibles d'être modifiées avant la mise à disposition des produits décrits.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

#### LICENCE DE COPYRIGHT :

Le présent document contient des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sous différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. Ces exemples de programmes sont fournis "en l'état", sans garantie d'aucune sorte. IBM n'est en aucun cas responsable des dommages liés à l'utilisation de ces exemples de programmes.



Toute copie totale ou partielle de ces programmes exemples et des oeuvres qui en sont dérivées doit comprendre une notice de copyright, libellée comme suit :

© (Nom de votre entreprise) (année). Des segments de ce code sont dérivés des exemples de programmes d'IBM Corp. © Copyright IBM Corp. \_indiquer la ou les années\_.

Si vous visualisez ces informations en ligne, il se peut que les photographies et illustrations en couleur n'apparaissent pas à l'écran.

## Marques

---

SPx et Security First Corp sont des marques de Security First Corp. dans de nombreux pays. D'autres produits et services peuvent être des marques de Security First Corp. ou d'autres sociétés.

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produit et de service peuvent appartenir à IBM ou à des tiers. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web "Copyright and trademark information" à l'adresse : <http://www.ibm.com/legal/copytrade.shtml>.

Adobe, le logo Adobe, PostScript et le logo PostScript sont des marques d'Adobe Systems Incorporated aux Etats-Unis et/ou dans certains autres pays.

Apache Software Foundation (ASF) est propriétaire de toutes les marques liées à Apache, marques de services et logos pour le compte des communautés de projet Apache, et les noms de tous les projets Apache sont des marques de l'ASF.

Node.JS est une marque de Joyent, Inc. CORPORATION DELAWARE 345 California Street; Suite 2000 San Francisco CALIFORNIE 94104.

Unicode et le logo Unicode sont des marques d'Unicode, Inc. aux Etats-Unis et dans d'autres pays.

Les marques CentOS sont des marques de Red Hat, Inc. ("Red Hat").

"Red Hat", Red Hat Linux, le logo Red Hat "Shadowman" et les produits mentionnés sont des marques de Red Hat, Inc. aux Etats-Unis et dans d'autres pays.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

Java ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

## Dispositions pour la documentation du produit

---

Les droits d'utilisation relatifs à ces publications sont soumis aux dispositions suivantes.

### **Domaine d'application**

Ces dispositions s'ajoutent aux conditions d'utilisation relatives au site Web IBM.

### **Usage personnel**

Vous pouvez reproduire ces informations pour votre usage personnel, non commercial, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez pas distribuer, afficher ou dériver le travail de ces documents, ou une partie, sans le consentement exprès d'IBM.

### **Usage commercial**

Vous pouvez reproduire, distribuer et publier ces informations uniquement au sein de votre entreprise, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez pas procéder à des travaux dérivés de ces publications, ni les reproduire, les distribuer ou les afficher en totalité ou partiellement en dehors de votre entreprise sans le consentement exprès d'IBM.

## Droits

Excepté les droits d'utilisation expressément accordés dans le présent document, aucun autre droit, licence ou autorisation, implicite ou explicite, n'est accordé pour ces publications ou autres informations, données, logiciels ou droits de propriété intellectuelle contenus dans ces publications.

IBM se réserve le droit de retirer les autorisations accordées ici si, à sa discrétion, l'utilisation des publications s'avère préjudiciable à ses intérêts ou si, selon son appréciation, les instructions susmentionnées n'ont pas été respectées.

Vous ne pouvez télécharger, exporter ou réexporter ces informations qu'en conformité complète avec l'ensemble des lois et des règlements applicables dans votre pays, y compris les lois et règlements américains relatifs à l'exportation.

IBM N'OCTROIE AUCUNE GARANTIE SUR LE CONTENU DE CES PUBLICATIONS. LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU TACITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES PUBLICATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

## Politique de confidentialité

---

Les Logiciels IBM, y compris les Logiciels sous forme de services ("Offres Logiciels") peuvent utiliser des cookies ou d'autres technologies pour collecter des informations sur l'utilisation des produits, améliorer l'acquis utilisateur, personnaliser les interactions avec celui-ci, ou dans d'autres buts. Bien souvent, aucune information personnelle identifiable n'est collectée par les Offres Logiciels. Certaines Offres Logiciels vous permettent cependant de le faire. Si la présente Offre Logiciels utilise des cookies pour collecter des informations personnelles identifiables, des informations spécifiques sur cette utilisation sont fournies ci-dessous. Cette Offre Logiciels n'utilise pas de cookies ou d'autres techniques pour collecter des informations personnelles identifiables

Si les configurations déployées de cette Offre Logiciels vous permettent, en tant que client, de collecter des informations permettant d'identifier les utilisateurs par l'intermédiaire de cookies ou par d'autres techniques, vous devez solliciter un avis juridique sur la réglementation applicable à ce type de collecte, notamment en termes d'information et de consentement.

Pour plus d'informations sur l'utilisation à ces fins des différentes technologies, y compris celle des cookies, consultez les Points principaux de la Déclaration IBM de confidentialité sur Internet (<http://www.ibm.com/privacy>) et la section "Cookies, pixels espions et autres technologies" de la Déclaration IBM de confidentialité sur Internet sur le site <http://www.ibm.com/privacy/details>, ainsi que la section "IBM Software Products and Software-as-a-Service Privacy Statement" sur le site <http://www.ibm.com/software/info/product-privacy> (en anglais).





SC43-5049-01

