

IBM Multi-Cloud Data Encryption
Technologie SPx®
Version 2.3

Foire aux questions (FAQ)



Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 13.

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

Première 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 : GC27-9558-00

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 .**

Table des matières

Avis aux lecteurs canadiens.....	V
Chapitre 1. Présentation.....	1
Chapitre 2. MDE - Foire aux questions (FAQ).....	3
Questions fréquentes - Général.....	3
Q : Qu'est-ce qu'IBM Multi-Cloud Data Encryption (MDE) ?.....	3
Q : Quels sont les systèmes d'exploitation pris en charge par IBM Multi-Cloud Data Encryption (MDE) ?.....	3
Q : Quels systèmes de fichiers sont pris en charge par les agents MDE ?.....	3
Q : Y a-t-il des prérequis avant d'installer IBM Multi-Cloud Data Encryption (MDE) ?.....	3
Q : Quels sont les navigateurs pris en charge par IBM Multi-Cloud Data Encryption (MDE) ?.....	3
Q : IBM Multi-Cloud Data Encryption (MDE) s'exécute-t-il en mode FIPS ?.....	3
Q : Lors de l'utilisation de Multi-Cloud Data Encryption (MDE), dois-je chiffrer mes données en les envoyant sur un système distant ? Ai-je toujours besoin de ma connexion VPN à un système distant ?.....	4
Q : Lorsque vous dites qu'IBM Multi-Cloud Data Encryption (MDE) "tisse la sécurité dans les données au niveau des bits", qu'entendez-vous ?.....	4
Q : Expliquez-moi comment l'intégrité des données est préservée avec IBM Multi-Cloud Data Encryption (MDE).....	4
Questions fréquentes - PPM.....	4
Q : Qu'est-ce que Policy Provisioning Manager (PPM) ?.....	4
Q : Pourquoi Policy Provisioning Manager (PPM) utilise-t-il le contrôle d'accès basé sur les rôles ?.....	4
Q : Dans la console Policy Provisioning Manager (PPM), que sont les processus ? Et à quoi servent-ils ?.....	5
Q : Dans la console Policy Provisioning Manager (PPM), qu'est-ce qu'un sélecteur ? Et à quoi sert-il ?.....	5
Q : Dans la console Policy Provisioning Manager (PPM), qu'est-ce qu'un ensemble de chemins d'accès ? Et à quoi sert-il ?.....	5
Q : Dans la console Policy Provisioning Manager (PPM), qu'est-ce qu'un type de données ? Et à quoi sert-il ?.....	5
Q : Dans la console Policy Provisioning Manager (PPM), qu'est-ce qu'un agent ? Et à quoi sert-il ?.....	5
Q : Quand dois-je utiliser l'agent de type Volume ? Et comment fonctionne-t-il ?.....	6
Q : Quand dois-je utiliser l'agent de type Fichier avec une règle ? Et comment fonctionne-t-il ?.....	6
Q : Quand dois-je utiliser l'agent de type Volume avec une règle ? Et comment fonctionne-t-il ?.....	6
Q : Quand dois-je utiliser un agent de type Magasin d'objets ? Et comment fonctionne-t-il ?.....	6
Q : Dans la console Policy Provisioning Manager (PPM), qu'est-ce qu'une tâche ? Et à quoi sert-elle ?.....	7
Q : Pour IBM Multi-Cloud Data Encryption, quand dois-je utiliser une base de données PostgreSQL externe ?	7
Questions fréquentes - Certificats.....	7
Q : Quelles sont les conditions requises pour les certificats du serveur PPM ?.....	7
Q : Quelles sont les conditions requises pour les certificats d'agent ?.....	7
Q : PPM prend-il en charge les connexions NAT (conversion d'adresses réseau) ou PAT (conversion d'adresse de port) ?.....	7

Q : Comment configurer les certificats de serveur PPM pour un serveur PPM dans une configuration réseau NAT (conversion d'adresses réseau) ou PAT (conversion d'adresse de port) ?	7
Q : Comment configurer les certificats d'agent lorsqu'un agent se trouve dans une configuration réseau NAT (conversion d'adresses réseau) ou PAT (conversion d'adresse de port) ?	8
Q : Quelles sont les conditions requises pour les certificats du serveur PPM dans une configuration à haute disponibilité (HA) ?	8
Questions fréquentes - Clés et gestion des clés	8
Q : Quelles sont les opérations de gestion des clés exécutées par IBM Multi-Cloud Data Encryption ?	8
Q : Pourquoi dois-je effectuer une rotation des clés ?	8
Q : Quand dois-je révoquer les clés ?	8
Q : Pourquoi dois-je broyer les clés ?	8
Q : IBM Multi-Cloud Data Encryption gère-t-il les clés à ma place ?	8
Questions fréquentes - Installation et configuration	9
Q : Quel est l'impact d'IBM Multi-Cloud Data Encryption (MDE) sur les utilisateurs finaux (c'est-à-dire les utilisateurs qui ne sont pas administrateurs) ?	9
Q : Un agent MDE peut-il être installé sur un hôte Docker et peut-il gérer toutes les demandes de lecture/écriture provenant des applications se trouvant dans des conteneurs Docker ?	9
Questions fréquentes - Configuration	9
Q : Puis-je chiffrer des fichiers HTML avec IBM Multi-Cloud Data Encryption (MDE) ?	9
Questions fréquentes - Fonctionnement	9
Q : Comment puis-je savoir que mes données sont protégées avec IBM Multi-Cloud Data Encryption (MDE) ?	9
Q : Avant d'apporter des modifications à une mise en oeuvre de production d'IBM Multi-Cloud Data Encryption (MDE), quelles sont les précautions à prendre ?	9
Q : Puis-je transférer des événements d'IBM Multi-Cloud Data Encryption (MDE) vers d'autres applications de corrélation SIEM (gestion des informations et des événements de sécurité) ?	10
Q : Le respect de la casse (capitalisation) est-il important ?	10
Q : Qu'entend-on par Ordre d'opération et pourquoi est-ce important ?	10
Q : J'ai soumis une tâche d'activation d'instantané et elle est toujours en cours d'exécution. Quand se terminera-t-elle ?	10
Questions fréquentes - Haute disponibilité	10
Q : A quel moment ai-je besoin de la haute disponibilité pour un déploiement IBM Multi-Cloud Data Encryption (MDE) ?	10
Q : Ai-je besoin d'équilibres de charge pour un déploiement haute disponibilité d'IBM Multi-Cloud Data Encryption ?	11
Questions fréquentes - Service partagé	11
Q : Quel est l'objectif de la fonction de service partagé ?	11
Remarques	13
Marques	15
Dispositions pour la documentation du produit	15
Politique de confidentialité	16

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

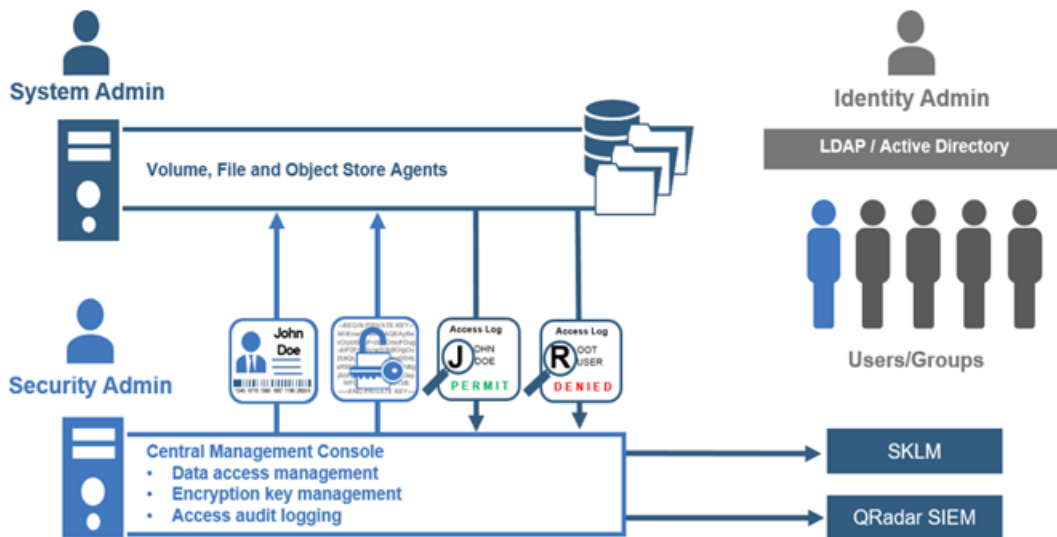
Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, 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. Présentation

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 dispose des autorisations nécessaires à la mise en service et à la gestion des agents. La Figure 1 décrit ces rôles, qui sont décrits plus en détail à la section 7 : Gestion des administrateurs MDE.

Quatre types d'agent sont disponibles. Ils peuvent être déployés pour mettre en oeuvre les définitions de règle d'administration des données protégées ou chiffrées. Un agent de type volume applique la définition des règles de volume et l'association d'un ou de plusieurs volumes protégés. Un agent de type fichier avec une règle applique les définitions de règle d'accès opérationnelles basées sur les fichiers et l'association d'un ou de plusieurs chemins d'accès aux fichiers protégés, chacun de ces chemins pouvant disposer de ses propres règles opérationnelles et d'accès aux fichiers, définies par des spécifications à granularité fine. Un agent de type Volume avec une règle utilise la protection par des règles de volume d'un agent de type Volume et permet d'appliquer des règles de contrôle d'accès opérationnelles basées sur un fichier pour un ou plusieurs chemins d'accès à des fichiers. Enfin, un agent de type Magasin d'objets chiffre et fractionne par chiffrement les données envoyées à un ou plusieurs stockages d'objets sur cloud.

Chapitre 2. MDE - Foire aux questions (FAQ)

Questions fréquentes - Général

Q : Qu'est-ce qu'IBM Multi-Cloud Data Encryption (MDE) ?

R : MDE introduit et permet la mise en service d'agents, de règles (définition d'accès opérationnelle et cryptographique) et de la gestion (mises à jour du cycle de vie et audit des utilisateurs) de 25 000 maximum à partir d'un emplacement centralisé unique. MDE prend en charge le déploiement de quatre types d'agent : volume, fichier avec une règle, volume avec une règle et magasin d'objets. Ces agents sont faciles à installer et transparents pour l'utilisateur final. Ils permettent aux administrateurs de configurer et de déployer le logiciel afin de répondre aux exigences de conformité de l'environnement informatique.

Q : Quels sont les systèmes d'exploitation pris en charge par IBM Multi-Cloud Data Encryption (MDE) ?

R : MDE prend actuellement en charge les systèmes d'exploitation suivants.

- Red Hat Enterprise Linux 6.2 - version de noyau 2.6.32-220 et versions ultérieures
- Red Hat Enterprise Linux - versions de noyau 7.2+
- CentOS 6.2 - version de noyau 2.6.32-220 et versions ultérieures
- CentOS 7.2 - version de noyau et versions ultérieures
- Microsoft Windows Server 2008R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012R2
- Microsoft Windows Server 2016

Q : Quels systèmes de fichiers sont pris en charge par les agents MDE ?

R : MDE prend en charge les systèmes de fichiers suivants :

- EXT3
- EXT4
- XFS (Red Hat/CentOS 6.5 et versions ultérieures)
- NTFS
- ReFS

Q : Y a-t-il des prérequis avant d'installer IBM Multi-Cloud Data Encryption (MDE) ?

R : MDE est fourni sous forme d'archive de virtualisation ouverte (OVA), qui se déploie facilement dans VMware ESXi™ ou Microsoft Hyper-V et peut s'exécuter dans la plupart des hyperviseurs.

Q : Quels sont les navigateurs pris en charge par IBM Multi-Cloud Data Encryption (MDE) ?

R : MDE peut s'exécuter avec Mozilla Firefox, Google Chrome™, Microsoft Internet Explorer et Microsoft Edge.

Q : IBM Multi-Cloud Data Encryption (MDE) s'exécute-t-il en mode FIPS ?

R : Oui, MDE respecte la norme compatible FIPS 140.2, comme indiqué sur la fiche technique du produit.

Q : Lors de l'utilisation de Multi-Cloud Data Encryption (MDE), dois-je chiffrer mes données en les envoyant sur un système distant ? Ai-je toujours besoin de ma connexion VPN à un système distant ?

R : MDE est conçu pour écrire des données de façon sécurisée sur des sites distants, dont des sites de cloud publics, tant qu'il a accès à l'emplacement des fichiers. Cependant, il peut être nécessaire de recourir à un VPN pour se connecter au site distant.

Q : Lorsque vous dites qu'IBM Multi-Cloud Data Encryption (MDE) "tisse la sécurité dans les données au niveau des bits", qu'entendez-vous ?

R : MDE, en reposant sur la technologie SPx, combine chiffrement, fractionnement des données aléatoire et avec des clés au niveau des bits, authentification (contrôles d'intégrité), tolérance aux pannes et infrastructure COI dans un processus qui transforme des données et des informations identifiables en éléments totalement aléatoires, inutilisables et binaires. Le résultat de l'opération de MDE est que l'élément Information Assurance (IA) est tissé dans la trame même des données. La sécurité, la résilience des données, la confiance et l'infrastructure de partage d'informations sont totalement intégrés aux données, ce qui les rend inséparables. La protection des données et des informations est assurée de leur création jusqu'à leur destruction et/ou pendant toute le cycle de vie de diffusion publique. La protection des données est maintenue lorsque les données sont au repos (écrites dans un espace de stockage) et lorsque les utilisateurs y accèdent.

Q : Expliquez-moi comment l'intégrité des données est préservée avec IBM Multi-Cloud Data Encryption (MDE).

R : L'intégrité des données est garantie à l'aide de codes d'authentification des messages, qui doivent correspondre aux données à lire.

Questions fréquentes - PPM

Q : Qu'est-ce que Policy Provisioning Manager (PPM) ?

R : PPM gère la mise en service des agents (modèle de protection des données), des règles (définition d'accès opérationnelle et cryptographique) et de la gestion (mises à jour du cycle de vie et audit des utilisateurs) de 25 000 agents maximum à partir d'un emplacement centralisé unique. Il prend en charge le déploiement de quatre types d'agent de chiffrement de données : volume, fichier avec une règle, volume avec une règle et magasin d'objets. Le type volume protège les données au niveau des unités par bloc. Le type de fichier avec une règle protège les données au niveau des fichiers et fournit un contrôle d'accès opérationnel basé sur un fichier. Le type volume avec une règle protège les données au niveau des unités par bloc avec un contrôle d'accès opérationnel basé sur un fichier. Le magasin d'objets chiffre et fractionne par chiffrement les données envoyées à un ou plusieurs stockages d'objets sur cloud.

Q : Pourquoi Policy Provisioning Manager (PPM) utilise-t-il le contrôle d'accès basé sur les rôles ?

R : PPM utilise une conception plane et statique de contrôle d'accès basé sur les rôles (RBAC). Les fonctionnalités de PPM nécessitent des autorisations spécifiques. Il existe deux rôles distincts : Administrateur du produit et Administrateur de la sécurité. Alors que certaines autorisations sont communes, la séparation des rôles offre à la direction informatique une fonction puissante de séparation des tâches d'administration, ce qui permet d'éviter qu'un employé malveillant sabote l'environnement informatique. Il est possible d'ajouter des rôles supplémentaires de chaque type afin de prendre correctement en charge des environnements informatiques plus importants ou plus complexes. De plus, un client peut définir, par programmation, le nombre d'administrateurs nécessaires à l'approbation d'une tâche, ainsi que le nombre d'administrateurs nécessaires au refus d'une tâche. Ainsi, pour chaque ensemble de rôles, les approbations et les refus des administrateurs sont suivis par PPM afin de s'assurer

que le nombre d'approbations pour l'exécution ou de refus est suffisant. Si le nombre nécessaire d'administrateurs approuvent la tâche, la tâche est exécutée. Si le nombre nécessaire d'administrateurs refusent la tâche (peut différer de l'approbation), la tâche est annulée. Cela permet de s'assurer d'un contrôle précis des tâches liées à l'administration et à la sécurité. L'ordre des approbations et/ou des refus est suivi et journalisé à des fins d'audit et de conformité.

Q : Dans la console Policy Provisioning Manager (PPM), que sont les processus ? Et à quoi servent-ils ?

R : Les processus, également appelés "Processus via une règle", sont des listes de processus ou d'applications disposant du contrôle d'accès pour les données protégées par IBM Multi-Cloud Data Encryption. Les processus sont liés à un sélecteur afin de fournir un contrôle d'accès des processus via les utilisateurs sur un système cible.

Q : Dans la console Policy Provisioning Manager (PPM), qu'est-ce qu'un sélecteur ? Et à quoi sert-il ?

R : Un sélecteur est une liste non ordonnée d'utilisateurs, de groupes et de processus. Combiné dans un type de données, il permet à l'administrateur de la sécurité d'identifier facilement des collections d'entités qui doivent partager des données protégées par MDE ou y avoir un accès commun. Un sélecteur peut comprendre un champ Utilisateur facultatif, un champ Groupe facultatif ainsi qu'un champ Source du groupe (interne ou externe, si LDAP est défini) ou un "Processus via une règle" facultatif.

Q : Dans la console Policy Provisioning Manager (PPM), qu'est-ce qu'un ensemble de chemins d'accès ? Et à quoi sert-il ?

R : Un ensemble de chemins d'accès est une liste non ordonnée de chemins d'accès à des fichiers qui doivent être protégés par une règle MDE (ou doivent potentiellement être exclus de la protection par des règles en fonction de la règle). Il permet à l'administrateur de la sécurité de spécifier ou de répertorier facilement des collections de chemins d'accès qui doivent être protégés par MDE. Lorsque vous spécifiez un ensemble de chemins d'accès, l'administrateur de la sécurité doit créer un nom pour la collection de chemins d'accès. La protection est récursive du chemin d'accès indiqué vers les sous-répertoires éventuels. Le champ Remarques est facultatif.

Q : Dans la console Policy Provisioning Manager (PPM), qu'est-ce qu'un type de données ? Et à quoi sert-il ?

R : Un type de données est une 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, une définition d'action et une clé associée. Lors de la création d'un agent, un type de données est associé à un chemin d'accès à un fichier (ou à un ensemble de chemins d'accès) pour définir le contrôle d'accès opérationnel et cryptographique des données.

Q : Dans la console Policy Provisioning Manager (PPM), qu'est-ce qu'un agent ? Et à quoi sert-il ?

R : PPM prend en charge quatre types d'agent, fournissant chacun un type de protection différent. Les agents sont les suivants : volume, fichier avec une règle, volume avec une règle et magasin d'objets. Le type volume protège les données au niveau du volume. Le type fichier avec une règle protège des données au niveau du fichier et fournit un contrôle d'accès opérationnel basé sur un fichier et un contrôle d'accès cryptographique facultatif. Le type volume avec une règle protège des données au niveau du volume et fournit un contrôle d'accès opérationnel basé sur un fichier. Le magasin d'objets chiffre et fractionne par chiffrement les données envoyées à un ou plusieurs stockages d'objets sur cloud.

Q : Quand dois-je utiliser l'agent de type Volume ? Et comment fonctionne-t-il ?

R : Un agent de type Volume offre aux opérations informatiques la sécurité des données au repos sous forme de volume prédéfini protégé. Lors du déploiement, l'agent de type volume crée un ensemble de clés, qui est appliqué au volume entier, et le protège ainsi cryptographiquement en tant qu'unité unique. Lorsque des données et des fichiers sont stockés et/ou modifiés, ajoutés ou supprimés, les algorithmes cryptographiques sont appelés pour s'assurer que toutes les données dans le volume sont sécurisées correctement. Un volume peut être divisé en une ou plusieurs partitions, chaque partition étant protégée de la même façon. La protection de volume est particulièrement adaptée pour les groupes d'utilisateurs qui envisagent de partager ouvertement des quantités de données modérées ou importantes.

Q : Quand dois-je utiliser l'agent de type Fichier avec une règle ? Et comment fonctionne-t-il ?

R : Un agent de type Fichier avec une règle offre aux opérations informatiques une protection très puissante au niveau de chaque fichier. Lorsqu'un agent de type fichier est déployé, le répertoire de premier niveau est identifié comme l'emplacement pour les données protégées. Chaque fichier stocké dans ce répertoire est protégé individuellement par un ensemble de clés, tandis que le contrôle d'accès aux fichiers pour les utilisateurs, les groupes et les processus est administré par le biais des règles définies par PPM. De plus, un administrateur de la sécurité peut définir une clé de chiffrement, qui peut être appliquée à des utilisateurs, à des groupes ou à des processus, de sorte que les fichiers sélectionnés soient protégés cryptographiquement des autres, qui partagent l'accès au répertoire. Lors de l'accès aux fichiers, il est possible de sélectionner une option permettant de consigner chaque accès (en lecture ou en écriture) à des fins d'audit et de suivi. Il n'y a pas de limite de taille pour les fichiers ou l'environnement de stockage avec une protection de fichier. L'utilisation de l'espace se développe et croît en fonction de la taille des fichiers qu'il contient. La protection de fichier avec une règle est particulièrement adaptée pour protéger des fichiers individuels partagés ou utilisés de façon privée.

Q : Quand dois-je utiliser l'agent de type Volume avec une règle ? Et comment fonctionne-t-il ?

R : Un agent de type Volume avec une règle ajoute à un volume (ou une partition) protégé un contrôle d'accès aux fichiers Utilisateur et Groupe. Lors du déploiement, l'agent de type volume crée un ensemble de clés, qui est appliqué au volume entier, et le protège ainsi cryptographiquement en tant qu'unité unique. Lorsque des données et des fichiers sont stockés et/ou modifiés, ajoutés ou supprimés, les algorithmes cryptographiques sont utilisés pour s'assurer que toutes les données dans le volume sont sécurisées correctement. Un administrateur de la sécurité peut définir des règles de contrôle d'accès aux fichiers pour les utilisateurs, les groupes et les processus en utilisant PPM. Lors de l'accès aux fichiers, il est possible de sélectionner une option permettant de consigner chaque accès (en lecture ou en écriture) à des fins d'audit et de suivi. La protection de volume avec une règle est particulièrement adaptée pour les groupes d'utilisateurs qui ont besoin, outre la possibilité de partager des quantités de données modérées ou importantes, d'avoir un contrôle d'accès aux fichiers.

Q : Quand dois-je utiliser un agent de type Magasin d'objets ? Et comment fonctionne-t-il ?

R : Un agent de type Magasin d'objets permet de stocker des données dans le stockage d'objets hautement évolutif et efficace, que ce soit sur site ou dans le cloud. Les données sont contrôlées par le client et sont toujours privées et disponibles. L'accès est contrôlé par le propriétaire du stockage d'objets. Les données envoyées via l'agent de type Magasin de données sont chiffrées localement et sont ensuite protégées lors du transit via le protocole TLS (Transport Layer Security). Ainsi, vous gardez la sécurisation des données entre le stockage sur site et le stockage en cloud S3. Un agent de type Magasin de données fonctionne sur la base d'un modèle "M sur N", qui détermine le nombre d'éléments de données requis pour régénérer les données (M) par rapport au nombre total d'éléments créés (N). Les éléments de données stockés, qui peuvent se trouver à des emplacements locaux ou distants en fonction de la licence, sont appelés "partages". L'utilisation de plusieurs partages permet d'améliorer le flux de

données et vous permet également de disposer de nouvelles options pour la résilience des données et la tolérance aux pannes. Le modèle de partages distribués M sur N pris en charge est 1:1, 2:3 ou 2:4.

Q : Dans la console Policy Provisioning Manager (PPM), qu'est-ce qu'une tâche ? Et à quoi sert-elle ?

R : PPM intègre un système de tâches, accessible à partir de l'interface utilisateur graphique, pour gérer et suivre l'approbation, les délais et l'exécution des différentes tâches de déploiement, de règle et de maintenance, liées aux données protégées, et qui/quoi y a accès. Lorsqu'un administrateur saisit une tâche, une tâche est créée et ajoutée à la liste affichée dans la page Tâches. Les administrateurs disposant des droits appropriés ont la possibilité d'approuver ou de refuser une tâche ou de ne pas intervenir sur cette tâche.

Q : Pour IBM Multi-Cloud Data Encryption, quand dois-je utiliser une base de données PostgreSQL externe ?

R : Une base de données Postgres externe est vivement recommandée pour tous les environnements de production. Une base de données interne n'est recommandée que pour les très petites installations (quelques agents, quelques utilisateurs et groupes ou simplement pour les tests ou la configuration des opérations d'assurance qualité), peu susceptibles de croître. Une base de données Postgres est également nécessaire lors du déploiement de MDE dans une configuration haute disponibilité.

Questions fréquentes - Certificats

Q : Quelles sont les conditions requises pour les certificats du serveur PPM ?

R : Les certificats du serveur PPM doivent contenir les éléments suivants :

- Des attributs de clés étendus spécifiant l'authentification serveur
- Une section Autre nom d'objet spécifiant le nom de domaine complet du serveur PPM (FQDN)

Q : Quelles sont les conditions requises pour les certificats d'agent ?

R : Les certificats d'agent doivent contenir les éléments suivants.

- Des attributs de clés étendus spécifiant l'authentification client
- Une section Autre nom d'objet spécifiant le nom de domaine complet (FQDN) de l'agent

Q : PPM prend-il en charge les connexions NAT (conversion d'adresses réseau) ou PAT (conversion d'adresse de port) ?

R : Oui. Le serveur PPM doit être joignable par l'agent pour que la communication soit établie lorsque l'agent initie la session de communication avec le serveur PPM. Une fois que la communication est établie, elle reste ouverte. L'agent enverra des données d'événement au serveur PPM via cette connexion. Le serveur PPM enverra des mises à jour des règles à l'agent via cette connexion.

Q : Comment configurer les certificats de serveur PPM pour un serveur PPM dans une configuration réseau NAT (conversion d'adresses réseau) ou PAT (conversion d'adresse de port) ?

R : Les certificats du serveur PPM doivent contenir les éléments suivants :

- Des attributs de clés étendus spécifiant l'authentification serveur
- Une section Autre nom d'objet spécifiant le nom de domaine complet du serveur PPM (FQDN)
- Une section Autre nom d'objet spécifiant l'adresse IP externe

Q : Comment configurer les certificats d'agent lorsqu'un agent se trouve dans une configuration réseau NAT (conversion d'adresses réseau) ou PAT (conversion d'adresse de port) ?

R : Les certificats d'agent doivent contenir les éléments suivants.

- Des attributs de clés étendus spécifiant l'authentification client
- Une section Autre nom d'objet spécifiant le nom de domaine complet du serveur PPM (FQDN)
- Une section Autre nom d'objet spécifiant l'adresse IP externe

Q : Quelles sont les conditions requises pour les certificats du serveur PPM dans une configuration à haute disponibilité (HA) ?

R : Les certificats du serveur PPM doivent contenir les éléments suivants :

- Des attributs de clés étendus spécifiant l'authentification serveur
- Une section Autre nom d'objet spécifiant le nom de domaine complet du serveur PPM (FQDN) composant le cluster PPM et le nom de domaine FQDN associé à l'adresse IP virtuelle PPM.

Questions fréquentes - Clés et gestion des clés

Q : Quelles sont les opérations de gestion des clés exécutées par IBM Multi-Cloud Data Encryption ?

R : Un administrateur de la sécurité peut définir des clés de chiffrement pour sécuriser des données avec Policy Provisioning Manager (PPM). Ces clés peuvent être associées à des types de données, à des lignes de type de données et à des volumes. Les opérations de gestion des clés incluent la création, la rotation, la révocation et le broyage/l'élimination.

Q : Pourquoi dois-je effectuer une rotation des clés ?

R : Il est généralement nécessaire d'effectuer une rotation périodique des clés pour vous assurer que les données sont suffisamment protégées contre les accès non autorisés. La rotation des clés consiste à remplacer les clés actuelles par une nouvelle clé et, compte tenu de la nature du chiffrement, elle nécessite un calcul à l'aide d'algorithmes cryptographiques. De nombreux experts recommandent une rotation périodique des clés pour les boutiques informatiques d'entreprise, en particulier celles qui interagissent avec le cloud. Actuellement, certaines normes, comme la norme PCI-DSS, nécessitent une rotation périodique des clés. La rotation des clés PPM crée des enregistrements de données horodatés, qui sont journalisés à des fins d'audit afin de démontrer la conformité.

Q : Quand dois-je révoquer les clés ?

R : La révocation d'une clé avec Policy Provisioning Manager (PPM) désactive temporairement l'accès aux données protégées. Les clés sont généralement révoquées lorsque l'on s'interroge sur la protection des données ou dans les cas où l'accès à des données protégées doit être refusé. Les données peuvent redevenir accessibles par la suite si la même clé est redistribuée.

Q : Pourquoi dois-je broyer les clés ?

R : Le broyage des clés désactive définitivement l'accès à des données protégées. Ne sélectionnez cette option que si vous n'avez plus besoin des données.

Q : IBM Multi-Cloud Data Encryption gère-t-il les clés à ma place ?

R : Si un administrateur de la sécurité ne souhaite pas gérer manuellement les clés de chiffrement, Policy Provisioning Manager (PPM) 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.

Questions fréquentes - Installation et configuration

Q : Quel est l'impact d'IBM Multi-Cloud Data Encryption (MDE) sur les utilisateurs finaux (c'est-à-dire les utilisateurs qui ne sont pas administrateurs) ?

R : Un administrateur bénéficie de la sécurité et de la haute disponibilité d'IBM Multi-Cloud Data Encryption (MDE) sans remarquer de différences avec les opérations normales. L'accès aux fichiers dans un répertoire géré (protégé) n'a aucun impact sur sa capacité à accéder à des fichiers, à écrire dans des fichiers ou à les stocker.

Q : Un agent MDE peut-il être installé sur un hôte Docker et peut-il gérer toutes les demandes de lecture/écriture provenant des applications se trouvant dans des conteneurs Docker ?

R : Les agents de type Fichier avec une règle et Volume peuvent tous les deux être utilisés pour la protection des données.

- L'agent de type Fichier avec une règle peut être utilisé pour protéger le chemin d'accès au volume Docker qui garantit que les données d'application utilisées par le conteneur sont protégées.
- L'agent de type Volume peut être utilisé pour protéger le chemin d'accès au conteneur Docker. Il chiffre efficacement le conteneur dans son intégralité ainsi que toutes ses opérations d'E-S. Si le volume Docker est stocké hors du chemin d'accès au conteneur Docker, un volume supplémentaire peut être configuré pour protéger le volume Docker externe.
- L'hôte Docker doit notamment exécuter un noyau pris en charge sur Red Hat 7.2+ (3.10-*)

Questions fréquentes - Configuration

Q : Puis-je chiffrer des fichiers HTML avec IBM Multi-Cloud Data Encryption (MDE) ?

R : Pour le moment, il n'est pas recommandé de protéger des fichiers HTML. Les sites web affichent des fichiers HTML actifs, qui peuvent s'afficher incorrectement lorsqu'ils sont chiffrés.

Questions fréquentes - Fonctionnement

Q : Comment puis-je savoir que mes données sont protégées avec IBM Multi-Cloud Data Encryption (MDE) ?

R : La protection de MDE est active même si un utilisateur accède à des fichiers protégés alors que le service est arrêté.

Q : Avant d'apporter des modifications à une mise en oeuvre de production d'IBM Multi-Cloud Data Encryption (MDE), quelles sont les précautions à prendre ?

R : Des modifications mineures peuvent être apportées alors que le système est en cours de fonctionnement en utilisant la ligne de commande 'spxconfig' ou l'interface utilisateur graphique. En revanche, des modifications significatives nécessitent une préparation détaillée et des sauvegardes

recommandées. (Avant d'appliquer les modifications, consultez la documentation de tous les produits concernés par l'écosystème de production.)

Q : Puis-je transférer des événements d'IBM Multi-Cloud Data Encryption (MDE) vers d'autres applications de corrélation SIEM (gestion des informations et des événements de sécurité) ?

R : Oui. Il comporte un système d'agrégation et de transfert d'événements. Ce système agrège des événements provenant d'agents gérés avec des événements générés en interne et les stocke dans un journal des événements interne, qui peut être consulté dans le tableau de bord de l'administrateur et peut être configuré de manière à transférer des événements à un ou plusieurs destinataires.

Q : Le respect de la casse (capitalisation) est-il important ?

R : Oui, il est très important de respecter la casse.

- Lorsque vous créez des sélecteurs, les champs Utilisateur et Groupe sont sensibles à la casse
- Lorsque vous créez un ensemble de chemins avec Windows, l'identificateur d'unité doit apparaître en majuscule et le nom du répertoire est sensible à la casse
- Lorsque vous créez un agent de type Volume ou Volume avec règle, l'étiquette du volume est sensible à la casse
- Le respect de la casse doit toujours être pris en compte pour une valeur ou un champ

Q : Qu'entend-on par Ordre d'opération et pourquoi est-ce important ?

R : L'ordre d'opération est important car la création et le déploiement d'un agent doivent être effectués dans un ordre spécifique pour fonctionner.

- Avant de déployer un agent de type Fichier, le volume cible doit être en ligne, initialisé, formaté avec des répertoires créés et avec les droits appropriés.
- Avant de déployer un agent de type Volume, le volume doit exister, être en ligne et initialisé mais pas formaté.
- Avant de déployer un agent de type Volume avec une règle, le volume doit exister, être en ligne et initialisé, mais pas formaté. Des sélecteurs définis doivent exister dans la hiérarchie LDAP / AD ou locale de la machine cible.

Q : J'ai soumis une tâche d'activation d'instantané et elle est toujours en cours d'exécution. Quand se terminera-t-elle ?

R : Les modifications ou mises à jour d'un instantané ne prendront 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.

Questions fréquentes - Haute disponibilité

Q : A quel moment ai-je besoin de la haute disponibilité pour un déploiement IBM Multi-Cloud Data Encryption (MDE) ?

R : Un déploiement haute disponibilité de MDE doit être utilisé dans les environnements informatiques nécessitant des services de gestion de l'accès aux données et de la protection d'accès approchant d'une disponibilité totale. Si l'instance de PPM doit faire l'objet d'une maintenance, échoue ou s'éteint accidentellement, l'instance de secours à chaud s'active immédiatement et reprend l'opération.

Q : Ai-je besoin d'équilibreurs de charge pour un déploiement haute disponibilité d'IBM Multi-Cloud Data Encryption ?

R : Oui. Deux équilibreurs de charge (cluster d'équilibreurs de charge) sont nécessaires entre les agents et les serveurs PPM. Un cluster d'équilibreurs de charge est nécessaire à chaque emplacement de déploiement comportant au moins deux serveurs PPM. Les équilibreurs de charge communiquent entre eux sur un sous-réseau local et fournissent une adresse IP virtuelle (également appelée "adresse IP flottante") utilisée par les agents et les administrateurs pour accéder aux serveurs PPM. Il existe de nombreux scénarios pour la haute disponibilité avec PPM : emplacement unique, centres de données multiples, etc., chacun avec ses propres options de déploiement et configurations.

Questions fréquentes - Service partagé

Q : Quel est l'objectif de la fonction de service partagé ?

R : Les fonctions de service partagé de PPM permettent aux prestataires informatiques de compartimenter les contrôles de PPM par client. Ainsi, chaque client possède ses propres nom de connexion PPM, administrateurs, règles, tableaux de bord, tâches, événements, etc. dans l'environnement informatique. Les clients pourraient partager leur espace de stockage et même des répertoires, mais leurs fichiers et volumes protégés seraient protégés individuellement par une méthode cryptographique. Cela permet à différents titulaires ou clients de partager et d'utiliser de façon sécurisée le même espace de stockage, tandis que les données de chaque titulaire sont séparées et invisibles pour les autres titulaires ou clients.

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).



GC43-5030-00

