

## Guide de démarrage rapide

*Ce guide vous permet de vous familiariser avec une installation classique d'IBM Multi-Cloud Data Encryption.*

### Présentation du produit

IBM Multi-Cloud Data Encryption (MDE) est un produit de sécurité des données complet reposant sur la technologie SPx<sup>®</sup> qui associe le chiffrement des données "au repos" aux puissantes fonctions de protection de PPM (Policy Provisioning Manager). PPM fait office de console de serveur de gestion permettant de mettre en service les agents de chiffrement, de gérer les paramètres de règles d'accès aux données et le cycle de vie des clés, de mettre à jour les agents et de journaliser l'accès des utilisateurs pour 25 000 agents au maximum à partir d'un emplacement central.

### 1 Étape 1 : Accès aux logiciels et à la documentation



- Téléchargez le fichier OVA de Multi-Cloud Data Encryption depuis Passport Advantage.
- Consultez les notes sur l'édition de Multi-Cloud Data Encryption avant l'installation.
- Pour consulter la documentation complète, visitez le site IBM Knowledge Center ([https://www.ibm.com/support/knowledgecenter/SSTD4E\\_2.3.0/doc/kc\\_welcome\\_mde23.html](https://www.ibm.com/support/knowledgecenter/SSTD4E_2.3.0/doc/kc_welcome_mde23.html)). La documentation est également fournie avec le produit.

### 2 Étape 2 : Evaluation de votre configuration matérielle et logicielle



La configuration suivante doit être respectée :

- a. Serveur opérationnel avec système d'exploitation sous licence et hyperviseur pris en charge (VMware ESXi<sup>™</sup>) pour déployer et exécuter PPM
- b. archive de virtualisation ouverte (OVA) de base en package
- c. Programme d'installation de PPM
- d. Un ou plusieurs serveurs cible avec un système d'exploitation pris en charge pour l'agent (Red Hat<sup>®</sup> / CentOS 6.2+ ou 7.2+, AIX 7.1 ou 7.2 et Microsoft Windows Server<sup>®</sup> 2008 R2, Microsoft Windows Server<sup>®</sup> 2012 R2 ou Microsoft Windows Server<sup>®</sup> 2016).
- e. Navigateurs : Google Chrome<sup>®</sup>, Microsoft Internet Explorer<sup>®</sup> 10+, Mozilla Firefox<sup>®</sup> ESR 52+.
- f. Accès réseau entre PPM et tous les agents
- g. 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

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

Pour obtenir des informations complètes, voir les sections *Remarques sur la planification*, *Paramètres des certificats de serveur* et *Annexe : Exemples de certificats de l'autorité de certification* dans le *Guide d'administration d'IBM Multi-Cloud Data Encryption*.

### 3 Étape 3 : Installation d'IBM Multi-Cloud Data Encryption



Installation de MDE PPM, configuration de la base de données interne et définition des certificats.

A l'aide du fichier d'exemple `ibm_sw_mde_X.x.x-XX.bin`, remplacez les X par le nom du fichier, le numéro de version et le numéro de génération.

- a. Déployez l'archive de virtualisation ouverte de base de MDE dans votre hyperviseur. Dans cet exemple, il y est fait référence sous le nom de "machine virtuelle du serveur de gestion".
- b. Connectez-vous en tant qu'administrateur et définissez un nouveau mot de passe.

L'archive de virtualisation ouverte utilise des critères de module d'analyse de protocole standard, que l'administrateur peut configurer. Le mot de passe du module d'analyse de protocole doit comporter plus de 8 caractères et ne peut pas contenir 5 caractères d'un mot de passe précédent.

- c. Notez l'adresse IP de la machine virtuelle MDE.
- d. Téléchargez `ibm-sw_mde_X.x.x-xx.bin` vers MDE à l'aide de la méthode `scp` ou d'une méthode similaire.
- e. Rendez le fichier binaire exécutable.

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

- f. Exécutez le fichier binaire.

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

- g. Sélectionnez "Anglais" et appuyez sur Entrée.
- h. Lisez les pages Licence en utilisant la touche de tabulation <OK> et la touche Entrée pour avancer.
- i. Sélectionnez <Oui> et appuyez sur la touche Entrée pour accepter le contrat de licence.
- j. Une fois l'extraction terminée, appuyez sur la touche Entrée sur <OK> pour revenir à la ligne de commande.
- k. Notez l'emplacement d'installation de RPM.
- l. Installez les packages RPM en tant que superadministrateur.

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

Le serveur de gestion (PPM) est maintenant installé mais pas configuré. Ne redémarrez pas tant que la configuration n'est pas terminée.

Pour obtenir le détail des étapes, consultez la section *Installation du produit* dans le *Guide d'administration d'IBM Multi-Cloud Data Encryption*.

### 4 Étape 4 : Configuration de la langue par défaut



Les langues prises en charge ont été installées lors de l'installation du package RPM sur la machine virtuelle du serveur de gestion ci-dessus.

Procédure d'installation :

- a. Exécutez le script `spsd-langsetup` :

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

- b. Affichez le code de langue par défaut actuel. Si aucune langue n'est définie, le code n'est pas renseigné.
- c. Affichez la liste des codes de langue disponibles.
- d. Entrez le nouveau code de langue par défaut : **en\_US** (exemple).
- e. Réexécutez le script `spsd-language` pour valider le code de langue par défaut défini. Comme dans l'exemple, la mention "La valeur par défaut actuelle est : **en\_US**" s'affiche.

## 5 Étape 5 : Configuration de la base de données



Avant de lancer MDE pour la première fois vous devez configurer une base de données interne ou externe. La base de données interne prend uniquement en charge PostgreSQL et est pré-packagée dans le fichier OVA.

Pour configurer la base de données pour fonctionner avec MDE :

Exécutez le script `spsd-pgsetup` avec l'option de script `"--local"`. Cette option locale configure une nouvelle base de données vide sur le serveur PostgreSQL `--local`.

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

Si vous installez une base de données externe, consultez la section *Configuration d'une base de données* du *Guide d'administration d'IBM Multi-Cloud Data Encryption*.

## 6 Étape 6 : Configuration des certificats



Les certificats sont utilisés pour établir une communication sécurisée entre le serveur de gestion (PPM), les agents de chiffrement et 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.

Dans cet exemple, tous les fichiers de certificat ont été copiés vers `/etc/ppm/certs` sur la machine virtuelle du serveur de gestion. Les noms entre crochets sont des exemples de noms.

Pour configurer un fichier de clés, un fichiers de clés de confiance et un bundle de l'autorité de certification, exécutez :

Pour le magasin de clés :

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

Pour le magasin de clés de confiance :

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

Pour le bundle d'autorité de certification :

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

Pour en savoir plus sur la configuration des certificats, consultez les sections *Paramètres des certificats de serveur* et *Annexe : Exemples de certificats de l'autorité de certification*. du *Guide d'administration d'IBM Multi-Cloud Data Encryption*.

## 7 Étape 7 : Redémarrage



Après avoir installé PPM, configuré une base de données, ajouté des certificats et éventuellement défini une infrastructure de clés publiques (PKI), vous pouvez maintenant redémarrer la machine virtuelle du serveur de gestion MDE.

## 8 Étape 8 : Connexion à la console



Une fois la machine virtuelle déployée, démarrez-la par le biais de l'interface de l'hyperviseur. Vous devez extraire l'adresse IP de la machine virtuelle.

Ouvrez la machine virtuelle du serveur de gestion, connectez-vous en tant qu'administrateur et affichez l'adresse IP de la machine virtuelle du serveur de gestion de MDE en exécutant la commande "ip address".

Pour accéder la console de gestion, entrez ce qui suit dans un navigateur pris en charge :

`https://<adresse_IP_serveur_MDE>`

Le navigateur est dirigé vers la page de connexion de MDE, dans laquelle vous serez invité à vous connecter.

Les données d'identification par défaut utilisées pour la première connexion doivent être modifiées après la première connexion :

Nom d'utilisateur : admin

Mot de passe : admin

Notez que lorsque vous utilisez l'authentification de client de l'infrastructure PKI, le tableau de bord peut être affiché en contournant la page de connexion. (Voir la section *Paramètres de l'infrastructure à clés publiques* du *Guide d'administration d'IBM Multi-Cloud Data Encryption*).

Après la connexion, vous êtes prêt à utiliser IBM Multi-Cloud Data Encryption en mettant à disposition un agent de chiffrement en service.

Il existe quatre types d'agent de chiffrement : agent de type Fichier avec une règle, agent de type Volume, agent de type Volume avec une règle et agent de type Magasin d'objets. Ces agents sont mis en service sur un système d'exploitation d'agent pris en charge (voir Prérequis). Pour obtenir des informations spécifiques sur la mise à disposition des agents, consultez la section *Mise en service et gestion des agents* du *Guide d'administration d'IBM Multi-Cloud Data Encryption*.

## Informations complémentaires



Pour toute information complémentaire, consultez le support produit d'IBM Multi-Cloud Data Encryption à l'adresse <https://www.ibm.com/support/home/>.

