

クイック・スタート・ガイド

このガイドは、*IBM Multi-Cloud Data Encryption* の標準インストールの手順を示す入門書です。

製品の概要

IBM Multi-Cloud Data Encryption (MDE) は、SPx® テクノロジーを採用した包括的なデータ・セキュリティ製品であり、保存データの暗号化と Policy Provisioning Manager (PPM) の強力な保護機能が統合されています。PPM は管理サーバー・コンソールとして機能し、最大 25,000 エージェントについて、暗号化エージェントのプロビジョニング、データ・アクセス・ポリシーの設定、鍵のライフサイクル/エージェントの更新/ユーザー・アクセスのロギングの管理を一元的に行うことができます。

1 ステップ 1: ソフトウェアと資料の入手



- パスポート・アドバンテージから Multi-Cloud Data Encryption の OVA をダウンロードします。
- インストールの前に、Multi-Cloud Data Encryption のリリース・ノートをご確認ください。
- 詳細な資料については、IBM Knowledge Center (https://www.ibm.com/support/knowledgecenter/SSTD4E_2.3.0/doc/kc_welcome_mde23.html) を参照してください。資料は、製品にも付属しています。

2 ステップ 2: ハードウェアとシステム構成の評価



以下の要件が満たされていることを確認してください。

- a. ライセンス交付を受けたオペレーティング・システムおよびサポートされるハイパーバイザー (VMware ESXi™) がインストールされた、PPM をデプロイおよび実行するための運用サーバー
- b. 基本 OVA のパッケージ。
- c. PPM インストーラー
- d. サポートされるエージェント・オペレーティング・システム (Red Hat®/CentOS 6.2 以降または 7.2 以降、AIX 7.1 または 7.2、Microsoft Windows Server® 2008 R2、Microsoft Windows Server® 2012 R2、または Microsoft Windows Server® 2016) がインストールされた 1 つ以上のターゲット・サーバー
- e. ブラウザー: Google Chrome®、Microsoft Internet Explorer® 10 以降、Mozilla Firefox® ESR 52 以降
- f. PPM とすべてのエージェント間のネットワーク・アクセス
- g. 管理サーバー (PPM) およびすべてのエージェントの間でセキュア・セッションを確立するための認証局署名済み証明書 (鍵ストア、トラストストア、および CA 証明書バンドル)

オブジェクト・ストア・エージェント (OSA) の場合、追加の要件は次のとおりです。

- S3 互換オブジェクト・ストレージ: アマゾン ウェブ サービス S3 (AWS S3)、IBM Cloud Object Storage (COS S3)
- オブジェクト・ストレージ資格情報: ユーザー ID と秘密鍵 (パスワード)
- AWS S3 REST API ライブラリーまたは Boto Python ライブラリーを使用して OSA エージェントに対するデータを指すアプリケーションまたはユーティリティー

詳細な情報については、「*IBM Multi-Cloud Data Encryption* 管理者ガイド」の『計画に関する考慮事項』、『サーバー証明書の設定』および、『付録: サンプルの認証局 (CA) 証明書』の各セクションを参照してください。

3 ステップ 3: IBM Multi-Cloud Data Encryption のインストール



MDE PPM、内部データベース構成、および証明書のセットアップをインストールします。

例であるファイル `ibm_sw_mde_X.x.x-XX.bin` を使用し、`X` をファイル名、バージョン、およびビルド番号で置き換えてください。

- a. MDE ベース OVA をハイパーバイザーにデプロイします。この例では、これを「管理サーバー VM」と呼びます。
- b. 管理者としてログインし、新規パスワードを設定します。

OVA は、管理者が構成できる PAM 標準基準を使用します。PAM パスワードは、8 文字より多くする必要があり、前のパスワードにあった 5 文字を含めることはできません。

- c. MDE VM の IP アドレスをメモします。
- d. `scp` または類似の方法を使用して、`ibm-sw_mde_X.x.x-xx.bin` を MDE にアップロードします。
- e. `bin` ファイルを実行可能にします。

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

- f. `bin` ファイルを実行します。

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

- g. 「English」を選択して Enter キーを押します。
- h. Tab <OK> を使用してライセンスのページを読み、Enter キーを押して先に進みます。
- i. <Yes> を選択し、Enter キーを押してご使用条件に同意します。
- j. 抽出が完了したら、<OK> で Enter キーを押してコマンド・ラインに戻ります。
- k. `rpm` のインストール場所をメモします。
- l. RPM を root としてインストールします。

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

管理サーバー (PPM) はインストールされましたが、構成されていません。構成が完了するまでは、リブートしないでください。

詳細な手順については、「IBM Multi-Cloud Data Encryption 管理者ガイド」の『製品のインストール』セクションを参照してください。

4 ステップ 4: デフォルトの言語の構成



管理サーバー VM への `rpm` のインストール (前述) 中に、サポートされる言語がインストールされています。

インストールするには、以下の手順を実行します。

- a. `spsd-langsetup` スクリプトを実行します。

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

- b. 現在のデフォルトの言語コードを確認します。何も設定されていない場合は、ブランクになっています。
- c. 使用可能な言語コードのリストを確認します。
- d. 新しいデフォルトの言語コードを入力します。例えば、**en_US** です。
- e. `spsd-language` スクリプトを再実行して、デフォルトの言語コードが設定されていることを検証します。この例の場合、「現在のデフォルト: **en_US**」と表示されます。

5 ステップ 5: データベースの構成



MDE を初めて始動する前に、内部データベースまたは外部データベースを構成する必要があります。内部データベースがサポートするのは PostgreSQL のみで、OVA にプリパッケージされて提供されます。

MDE と連携して機能するようにデータベースを構成するには、次のようにします。

「local」スクリプト・オプションを指定して `spsd-pgsetup` スクリプトを実行します。この `local` オプションにより内部の「--local」PostgreSQL サーバーに、新しい空のデータベースが構成されます。

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

外部データベースをインストールする場合は、「IBM Multi-Cloud Data Encryption 管理者ガイド」の『データベースのセットアップ』セクションを参照してください。

6 ステップ 6: 証明書の構成



証明書は、管理サーバー (PPM) と暗号化エージェントおよび Web ブラウザーの間でセキュア通信セッションを確立するために使用します。PPM は、すべての証明書が認証局 (CA) によって署名されていることを必要とします。CA によって、通信セッションのすべての参加者が相手方の身元を確認するために使用する信頼のルートが確立されます。

- CA 署名済み証明書とその対応する鍵の組み合わせが、Java 鍵ストアに格納されます。
- エージェント証明書の署名に使用された CA からの証明書 (または証明書バンドル) は、PPM トラストストアに追加する必要があります。
- 3つの構成要素 (鍵ストア、トラストストア、および CA 証明書バンドル) すべてが、下の PPM 証明書のセットアップ・プロセスで使用されます。

この例では、すべての証明書ファイルが、管理サーバー vm 上の /etc/ppm/certs にコピーされます。大括弧が付いている名前は、サンプル名です。

鍵ストア、トラストストア、および CA バンドルを構成するには、次の手順を実行します。

鍵ストア:

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

トラストストア:

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

CA バンドル:

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

証明書のセットアップについて詳しくは、「*IBM Multi-Cloud Data Encryption* 管理者ガイド」の『サーバー証明書の設定』および『付録: サンプルの認証局 (CA) 証明書』の各セクションを参照してください。

7 ステップ 7: リブート



PPM のインストール、データベースの構成、証明書の追加、およびオプションの PKI の設定が終わったら、MDE 管理サーバー VM をリブートできます。

8 ステップ 8: コンソールへのログイン



デプロイしたら、ハイパーバイザー・インターフェースを使用して仮想マシンを開始します。仮想マシンの IP を取得する必要があります。

管理サーバー VM を開き、管理者としてログインして、コマンド「ip address」を実行することで、MDE 管理サーバー VM の IP アドレスを表示します。

管理コンソールにアクセスするには、サポートされているブラウザで、次のように入力します。

`https://<MDE Server IP>>`

これにより、ブラウザが MDE のログイン・ページに移動し、ログインのプロンプトが出されます。

初回ログイン用のデフォルトの資格情報は、ログイン後に変更する必要があります。

ユーザー名: admin

パスワード: admin

なお、PKI クライアント認証を使用している場合、ログイン・ページを省略してダッシュボードが表示される可能性があります。(「IBM Multi-Cloud Data Encryption 管理者ガイド」の『公開鍵基盤 (PKI) の設定』セクションを参照してください。)

ログインすると、暗号化エージェントをプロビジョニングして IBM Multi-Cloud Data Encryption を使用できるようになります。

暗号化エージェントには、ファイル/ポリシー・エージェント、ボリューム・エージェント、ボリューム/ポリシー・エージェント、およびオブジェクト・ストア・エージェントの 4 種類があります。これらのエージェントは、サポートされるエージェント・オペレーティング・システムにプロビジョニングされます (前提条件を参照)。エージェントのプロビジョニング固有の情報については、「IBM Multi-Cloud Data Encryption 管理者ガイド」の『エージェントのプロビジョニングと管理』セクションを参照してください。

詳細情報



詳しくは、<https://www.ibm.com/support/home/> で IBM Multi-Cloud Data Encryption 製品サポートを参照してください。

