IBM Security Multi-Cloud Data Encryption

バージョン **2.2**

クイック・スタート・ガイド

このガイドは、**IBM Security 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・セキュリティー製品であり、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。
- 製品資料一式を参照するには、製品とともに提供されている IBM Multi-Cloud Data Encryption 製品資料を参照してください。

2 ステップ 2: インストールの前提条件

以下の要件が満たされていることを確認してください。

- 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、Policy Provisioning Manager (PPM) をデプロイおよび実行するための運用サーバー
- 基本 OVA のパッケージ。
- PPM インストーラー
- 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 以降および 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
- 以下のパッケージが Red Hat / CentOS エージェント上でインストール/更新されていること: curl、openSSL、および nss
- ブラウザー: Google Chrome、Internet Explorer 10 以降、Microsoft Edge、Firefox ESR 52 以降
- PPM とすべてのエージェントとの間の安定した通信のためのネットワーク・アクセス。
- 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) が必須であり、証明書には次のとおりであることが必要です。
  - PPM サーバーは、エージェントから提示される証明書が、そのエージェント (DNS ホスト名または IP アドレス) に解決されることを要求します
  - PPM サーバーは、エージェントから提示される証明書に、クライアント認証拡張鍵使用が設定されていることを要求します
  - エージェントは、PPM サーバーから提示される証明書が、その PPM サーバー (DNS ホスト名または IP アドレス) に解決されることを要求します
  - エージェントは、PPM サーバーから提示される証明書に、サーバー認証拡張鍵使用が設定されていることを要求します

  証明書が確実に有効期間内であるようにするため、PPM とエージェントは、信頼できる時刻ソースに同期する必要があります。

  デプロイされたエージェントごとに、固有の証明書が必要です

詳しくは、ソフトウェア・ダウンロードに付属の「MDE 管理者ガイド」を参照してください (証明書の例については『付録 II』を参照)。

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

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

以下に、本製品のインストール方法 (インストール手順、内部データベースの構成、および証明書のセットアップを含む) を簡単に紹介します。詳しい手順については、「管理者ガイド」を参照してください。

MDE PPM のインストール

ここに示す例の ibm_sw_mde_X.x.x-XX.bin ファイルの X 部分をファイル名、バージョン番号、およびビルド番号に置き換えてください。

1. 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。
2. 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。
3. MDE VM の IP アドレスをメモします。
4. 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。
5. 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
   ```
6. bin ファイルを実行します。

   ```
   [admin@localhost]$ ./ibm_sw_mde_X.x.x-XX.bin
   ```
7. 「English」を選択して Enter キーを押します。
8. ライセンスのページを読み、Tab <OK> を使用して Enter キーを押して先に進みます。
9. <Yes> を選択し、Enter キーを押してご使用条件に同意します。
10. 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。
11. rpm のインストール場所をメモします。
12. 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。

4 ステップ 4: 言語のセットアップ

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。

1. **spsd-langsetup** スクリプトを実行します。

   ```
   $ sudo /opt/securityfirst/spsd/bin/spsd-langsetup
   ```
2. 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。
3. 使用可能な言語コードのリストを確認します。
4. 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。
5. 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: データベースのセットアップ

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。

内部データベースは PostgreSQL のみをサポートし、OVA に同梱されています。

1. 「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、「管理者ガイド」の『データベースのセットアップ』を参照してください。

6 ステップ 6: 証明書

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、「管理者ガイド」の『サーバー証明書の設定』および『付録 II』のサンプルの認証局 (CA) 証明書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: 開始と初回ログイン

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ーで、次のように入力します。

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

これにより、ブラウザーが 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ます。(「管理者ガイド」の『公開鍵基盤 (PKI) の設定』を参照)

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 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についての具体的な情報は、「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』を参照してください。

9 ステップ 9: 使用の開始

エージェントのプロビジョニングと管理

MDE 管理ユーザーの管理

ポリシー実施鍵の管理

公開鍵基盤 (PKI) の設定

詳細情報

製品資料一式を参照するには、IBM Multi-Cloud Data Encryption のIBM Support Web サイトにアクセスしてください。

Printed in Ireland