

## 快速入门指南

本指南可帮助您开始 *IBM Multi-Cloud Data Encryption* 典型安装。

### 产品概述

IBM Multi-Cloud Data Encryption (MDE) 是由 SPx® 技术支持并将静态数据加密与强大的 Policy Provisioning Manager (PPM) 保护功能相结合的综合数据安全产品。PPM 充当着管理服务器控制台，可通过单个中央位置供应加密代理程序、设置数据访问策略、管理密钥生命周期、更新代理程序以及记录多达 25,000 个代理程序的用户访问日志。

### 1 步骤 1：访问软件和文档



- 从 Passport Advantage® 下载 Multi-Cloud Data Encryption 的 OVA。
- 在安装 Multi-Cloud Data Encryption 前复审它的发行说明。
- 要获取完整文档，请参阅 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))。该文档还与产品一起提供。

### 2 步骤 2：评估您的硬件和系统配置



确保满足以下需求：

- a. 使用特许操作系统和受支持的系统管理程序 (VMware ESXi™) 部署和运行 PPM 的操作服务器。
- b. 已打包的基本 OVA
- c. PPM 安装程序
- d. 一个或多个具有受支持的代理程序操作系统 (Red Hat® / CentOS 6.2+ 或 7.2+、AIX 7.1 或 7.2 以及 Microsoft Windows Server® 2008 R2、Microsoft Windows Server® 2012 R2 或 Microsoft Windows Server® 2016) 的目标服务器。
- e. 浏览器：Google Chrome®、Microsoft Internet Explorer® 10+、Mozilla Firefox® ESR 52+。
- f. PPM 和所有代理程序之间的网络访问。
- g. 用于在管理服务器 (PPM) 和所有代理程序之间建立安全会话的认证中心签名证书 (密钥库、信任库和 CA 证书捆绑包)。

对于对象存储代理程序 (OSA)，下面是附加需求：

- 与 S3 兼容的对象存储器：Amazon Web Services S3 (AWS S3)、IBM Cloud Object Storage (COS S3)
- 对象存储器凭证：用户标识和密钥 (密码)
- 利用 AWS S3 REST API Library 或 Boto Python Library 以使数据指向 OSA 代理程序的应用程序或实用程序

要获取完整信息，请参阅《IBM Multi-Cloud Data Encryption 管理员指南》中的“规划注意事项”、“服务器证书设置”和“附录：样本认证中心 (CA) 证书”部分。

### 3 步骤 3：安装 IBM Multi-Cloud Data Encryption



安装 MDE PPM、内部数据库配置和证书设置。

通过使用示例，将文件 `ibm_sw_mde_X.x.x-XX.bin` 中的 X 替换为文件名、版本和构建号。

- a. 将 MDE 基本 OVA 部署到您的系统管理程序。在此示例中被称为“管理服务器 VM”。
- b. 以管理员身份登录并设置新密码。

OVA 使用管理员可配置的 PAM 标准条件。PAM 密码必须超过 8 个字符且不能包含 5 个来自先前密码的字符。

- c. 记录 MDE VM 的 IP 地址。
- d. 使用 `scp` 或类似方法将 `ibm-sw_mde_X.x.x-xx.bin` 上传到 MDE。
- e. 使 `bin` 文件变为可执行文件。

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

- f. 运行 `bin` 文件。

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

- g. 选择“英语”，然后按“Enter”键。
- h. 使用<确定>选项卡阅读“许可证”页面，然后按“Enter”键前进。
- i. 选择<是>，然后按“Enter”键接受许可协议。
- j. 完成解压缩之后，在<确定>上按“Enter”键返回到命令行。
- k. 请记录 `rpm` 安装位置。
- l. 以 `root` 用户身份安装 RPM。

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

现已安装管理服务器 (PPM)，但尚未配置。在完成配置前，请不要重新引导。

有关详细步骤，请参阅《IBM Multi-Cloud Data Encryption 管理员指南》中的“产品安装”部分。

### 4 步骤 4：配置缺省语言



将 RPM 安装到上述管理服务器 VM 上时，安装了受支持的语言。

安装步骤：

- a. 运行 `spsd-langsetup` 脚本：

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

- b. 查看当前缺省语言代码。如果未设置，那么该项为空。
- c. 查看可用语言代码的列表。
- d. 输入新的缺省语言代码：**en\_US**（示例）。
- e. 重新执行 `spsd-language` 脚本验证是否已设置缺省语言代码。在示例中，此操作显示“当前缺省语言代码为：**en\_US**”。

### 5 步骤 5：配置数据库



在首次启动 MDE 前，将需要配置内部或外部数据库。内部数据库仅支持 PostgreSQL，并在 OVA 中以预包装的形式提供。

要配置数据库以使用 MDE，请执行以下步骤：

使用“`--local`”脚本选项运行 `spsd-pgsetup` 脚本。此本地选项在内部“`--local`”PostgreSQL 服务器上配置新的空数据库。

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

如果要安装外部数据库，请参阅《IBM Multi-Cloud Data Encryption 管理员指南》中的“数据库设置”部分。

## 6 步骤 6：配置证书



证书用于在管理服务器 (PPM) 和加密代理程序与 Web 浏览器之间建立安全通信会话。PPM 要求认证中心 (CA) 签署所有证书。CA 建立通信会话中的所有参与者用于验证另一方身份的信任根。

- 由 CA 签署的证书及其相应密钥组成 Java 密钥库。
- 必须将用于签署代理程序证书的来自 CA 的证书（或证书捆绑包）添加到 PPM 信任库。
- 以下 PPM 证书设置过程中使用了所有三个组件（密钥库、信任库和 CA 证书捆绑包）。

在此示例中，已将所有证书文件复制到管理服务器 vm 上的 /etc/ppm/certs。使用括号标注的名称为示例名称。

要配置密钥库、信任库和 CA 捆绑包，请运行：

对于密钥库：

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

对于信任库：

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

对于 CA 捆绑包：

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

有关证书设置的更多信息，请参阅《IBM Multi-Cloud Data Encryption 管理员指南》中的“服务器证书设置”和“附录：样本认证中心 (CA) 证书”部分。

## 7 步骤 7：重新引导



在安装 PPM、配置数据库、添加证书以及（可选）设置 PKI 后，您可以重新引导 MDE 管理服务器 VM。

## 8 步骤 8：登录控制台



部署后，通过系统管理程序界面启动虚拟机。您将需要检索虚拟机的 IP。

打开管理服务器 VM，以管理员身份登录，然后通过运行命令“ip address”显示 MDE 管理服务器 VM 的 IP 地址。

要访问管理控制台，请在受支持的浏览器上输入以下地址：

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

此操作会将浏览器定向到系统提示您登录的 MDE 登录页面。

用于首次登录的缺省凭证在登录后更改并且必须更改：

用户名：admin

密码：admin

请注意，在使用 PKI 客户机认证时，仪表板的显示内容可能会绕过登录页面。（请参阅《IBM Multi-Cloud Data Encryption 管理员指南》中的“公共密钥基础结构 (PKI) 设置”部分。）

登录后，通过供应加密代理程序，即可使用 IBM Multi-Cloud Data Encryption。

有四种类型的加密代理程序：“使用策略的文件”代理程序、“卷”代理程序、“使用策略的卷”代理程序和“对象存储”代理程序。向受支持的代理程序操作系统供应这些代理程序（请参阅“先决条件”）。有关代理程序供应的具体信息，请参阅《IBM Multi-Cloud Data Encryption 管理员指南》中的“代理程序供应和管理”部分。

## 更多信息



有关更多信息，请参阅 IBM Multi-Cloud Data Encryption 产品支持 (<https://www.ibm.com/support/home/>)。

IBM® Multi-Cloud Data Encryption V2.3 Licensed Materials - Property of IBM. © Copyright IBM Corporation and others 2017, 2019. US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

SPx 和 Security First Corp 是 Security First Corp. 在全球许多管辖区域的商标或注册商标。其他产品和服务名称可能是 Security First Corp. 或其他公司的商标。

IBM、IBM 徽标和 ibm.com® 是 International Business Machines Corp. 在全球许多管辖区域的商标或注册商标。其他产品和服务名称可能是 IBM 或其他公司的商标。当前的 IBM 商标列表，可从 Web 站点 ([www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml)) 的“版权和商标信息”部分获取。

文档号码：GC43-5043-01

