

快速入門手冊

本手冊可讓您開始進行一般 *IBM Multi-Cloud Data Encryption* 安裝。

產品概觀

IBM Multi-Cloud Data Encryption (MDE) 是綜合性的資料安全產品，採用將待用資料加密與強大的 Policy Provisioning Manager (PPM) 保護功能相結合的 SPx® 技術。PPM 用作管理伺服器主控台，可支援供應加密代理程式，設定資料存取原則，管理金鑰生命週期、代理程式更新及在單一集中位置儲存的最多 25,000 個代理程式的使用者存取記載。

1 步驟 1：存取軟體及說明文件



- 從 Passport Advantage® 下載 OVA for Multi-Cloud Data Encryption。
- 安裝之前，請先檢閱 Multi-Cloud Data Encryption 的版本注意事項。
- 如需完整的說明文件，請參閱 IBM Knowledge Center (https://www.ibm.com/support/knowledgecenter/SSTD4E_2.3.0/doc/kc_welcome_mde23.html)。產品也隨附該說明文件。

2 步驟 2：評估您的硬體及系統配置



確保符合下列需求：

- a. 具有授權作業系統及受支援 Hypervisor (VMware ESXi™) 的作業伺服器，以部署及執行 PPM。
- b. 封裝的基本 OVA
- c. PPM 安裝程式
- d. 一個以上目標伺服器，具有支援的代理程式作業系統 (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)。
- e. 瀏覽器：Google Chrome®、Microsoft Internet Explorer® 10+、Mozilla Firefox® ESR 52+。
- f. PPM 與所有代理程式之間的網路存取。
- g. 憑證管理中心簽章憑證 (金鑰儲存庫、信任儲存庫及 CA 憑證組合)，用於在管理伺服器 (PPM) 與所有代理程式之間建立安全階段作業。

對於物件儲存庫代理程式 (OSA)，以下是額外的需求：

- 符合 S3 的物件儲存體：Amazon Web Services S3 (AWS S3)、IBM Cloud Object Storage (COS S3)
- 物件儲存體認證：使用者 ID 和秘密金鑰 (密碼)
- 利用 AWS S3 REST API Library 或 Boto Python Library 將資料指向 OSA 代理程式的應用程式或公用程式

如需完整資訊，請參閱「IBM Multi-Cloud Data Encryption 管理者手冊」中的「規劃考量」、「伺服器憑證設定」及「附錄：憑證管理中心 (CA) 憑證範例」小節。

3 步驟 3：安裝 IBM Multi-Cloud Data Encryption



安裝 MDE PPM、內部資料庫配置及憑證設定。

使用範例（檔案 `ibm_sw_mde_X.x.x-XX.bin`）時，請將 X 取代為檔名、版本及建置號碼。

- a. 將 MDE 基本 OVA 部署到 Hypervisor 中。在此範例中，其將稱為「管理伺服器 VM」。
- b. 以 `admin` 身分登入，並設定新密碼。

OVA 使用可由管理者配置的 PAM 標準準則。PAM 密碼必須超過 8 個字元，且不能包含前一個密碼中的 5 個字元。

- c. 記下 MDE VM 的 IP 位址。
- d. 使用 `scp` 或類似方法將 `ibm-sw_mde_X.x.x-xx.bin` 上傳至 MDE。
- e. 使該 `bin` 檔成為執行檔。

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

- f. 執行 `bin` 檔。

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

- g. 選取「英文」，然後按 Enter 鍵。
- h. 使用標籤 <確定> 以閱讀「授權」頁面，按 Enter 鍵以繼續。
- i. 選取 <是>，並按 Enter 鍵以接受「授權合約」。
- j. 完成解壓縮後，在 <確定> 上按 Enter 鍵，以回到指令行。
- k. 記下 `rpm` 安裝位置。
- l. 以 `root` 身分安裝 RPM。

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

管理伺服器 (PPM) 現已安裝，但未配置。在完成配置之前，請不要重新開機。

如需詳細步驟，請參閱「IBM Multi-Cloud Data Encryption 管理者手冊」中的「產品安裝」小節。

4 步驟 4：配置預設語言



在 `rpm` 安裝期間，已在管理伺服器 VM 上安裝支援的語言。

安裝步驟：

- a. 執行 `spsd-langsetup` Script：

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

- b. 檢視現行預設語言碼。如果沒有設定，將為空白。
- c. 檢視可用的語言碼清單。
- d. 輸入新的預設語言碼：**en_US**（範例）。
- e. 重新執行 `spsd-language` Script 來驗證是否已設定預設語言碼。如範例中所示，它顯示「現行預設值為：**en_US**」。

5 步驟 5：配置資料庫



在首次啟動 MDE 之前，需要先配置內部或外部資料庫。內部資料庫僅支援 PostgreSQL，並在 OVA 的前置套件中提供。

如果要將資料庫配置為使用 MDE：

使用 `"--local"` Script 選項執行 `spsd-pgsetup` Script。此本端選項將在內部 `--local` PostgreSQL Server 上配置新的空資料庫。

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

若要安裝外部資料庫，請參閱「IBM Multi-Cloud Data Encryption 管理者手冊」中的「資料庫區段」小節。

6 步驟 6：配置憑證



憑證用於在管理伺服器 (PPM) 與加密代理程式及 Web 瀏覽器之間建立安全通訊階段作業。PPM 要求所有憑證都由憑證管理中心 (CA) 簽章。CA 會建立信任根目錄，通訊階段作業中的所有參與者都將使用該目錄驗證其他方的身分。

- Java 金鑰儲存庫中將 CA 簽章憑證及其對應的金鑰相結合。
- CA 中用於簽署代理程式憑證的憑證（或憑證組合）必須新增至 PPM 信任儲存庫。
- 下面的 PPM 憑證設定程序中使用所有這三種元件（金鑰儲存庫、信任儲存庫及 CA 憑證組合）。

在本範例中，所有憑證檔案都已複製到管理伺服器 VM 上的 /etc/ppm/certs。使用方括弧附註的名稱是範例名稱。

若要配置金鑰儲存庫、信任儲存庫及 CA 組合，請執行：

針對金鑰儲存庫：

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

針對信任儲存庫：

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

針對 CA 組合：

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

如需憑證設定的相關資訊，請參閱「IBM Multi-Cloud Data Encryption 管理者手冊」中的「伺服器憑證設定」及「附錄：附錄：憑證管理中心 (CA) 憑證範例」。

7 步驟 7：重新開機



安裝 PPM、配置資料庫、新增憑證且選擇性地設定 PKI 之後，您現在可以將 MDE 管理伺服器 VM 重新開機。

8 步驟 8：登入主控台



部署之後，請透過 Hypervisor 介面啟動虛擬機器。您將需要擷取虛擬機器的 IP。

開啟管理伺服器 VM 並以 admin 身分登入，透過執行指令 "ip address" 來顯示 MDE 管理伺服器 VM 的 IP 位址。

若要存取管理主控台，請在受支援的瀏覽器上輸入：

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

這會將瀏覽器導向至將提示您登入的 MDE 登入頁面。

下面列出了首次登入時的預設認證，在登入之後必須進行變更：

使用者名稱：admin

密碼：admin

請注意，使用 PKI 用戶端鑑別時，可能會顯示儀表板而略過登入頁面。（請參閱「IBM Multi-Cloud Data Encryption 管理者手冊」中的「公開金鑰基礎架構 (PKI) 設定」小節。）

登入之後，您現在已準備好透過供應加密代理程式來使用 IBM Multi-Cloud Data Encryption。

加密代理程式有下列四種類型：含原則的檔案代理程式、磁區代理程式、含原則的磁區代理程式以及物件儲存庫代理程式。這些代理程式將供應給支援的代理程式作業系統（請參閱「必要條件」）。如需「代理程式供應」的特定相關資訊，請參閱「IBM Multi-Cloud Data Encryption 管理者手冊」中的「代理程式供應及管理」區段。

其他多資訊



如需相關資訊，請參閱 IBM Multi-Cloud Data Encryption 產品支援，網址為 <https://www.ibm.com/support/home/>。

IBM® Multi-Cloud Data Encryption, Version 2.3 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 及 Security First Corp 是 Security First Corp. 在世界許多管轄區註冊的商標或註冊商標。其他產品及服務名稱可能是 Security First Corp. 或其他公司的商標。

IBM、IBM 標誌及 ibm.com® 是 International Business Machines Corp. 在世界許多管轄區註冊的商標或註冊商標。其他產品及服務名稱可能是 IBM 或其他公司的商標。IBM 商標的最新清單可在 Web 的 "[Copyright and trademark information](http://www.ibm.com/legal/copytrade.shtml)" (www.ibm.com/legal/copytrade.shtml) 中找到。

文件號碼：GC43-5044-01

