

IBM Multi-Cloud Data Encryption
Powered by SPx[®]
版本 2.3

管理者手冊



附註

在使用本資訊及其支援的產品之前，請閱讀第 103 頁的『[注意事項](#)』中的資訊。

本版本適用於 IBM Multi-Cloud Data Encryption 2.3 版（產品編號 5737-C67）以及所有後續版次和修訂，直到新版本中另有聲明為止。

© 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.

© **Copyright International Business Machines Corporation 2017, 2019.**

目錄

第 1 章簡介.....	1
授權使用許可權.....	1
聯絡點.....	1
管理手冊的背景及目的.....	1
第 2 章一般概觀.....	3
產品概觀.....	3
代理程式類型.....	3
磁區代理程式 (Volume Agent).....	3
具有原則的檔案代理程式.....	4
具有原則的磁區代理程式 (Volume with Policy Agent).....	4
物件儲存庫代理程式 (Object Store Agent).....	5
代理程式功能矩陣.....	5
第 3 章規劃考量.....	7
必要條件.....	7
最低系統需求.....	7
憑證需求.....	8
代理程式的檔案系統支援.....	8
網路設定.....	8
網路埠.....	9
OVA 配置.....	9
REST 介面.....	9
第 4 章產品安裝.....	11
準備安裝.....	11
授權.....	11
MDE OVA/VM 管理.....	11
安裝 MDE.....	11
語言設定.....	12
資料庫設定.....	12
內部資料庫.....	13
外部資料庫.....	13
伺服器憑證設定.....	13
金鑰儲存庫、信任儲存庫及憑證管理中心.....	13
公開金鑰基礎架構 (PKI) 設定.....	14
啟動及第一次登入.....	14
第 5 章 MDE 圖形使用者介面 (GUI).....	17
基本產品導覽.....	17
產品儀表板.....	17
文字框自動完成.....	17
注意通知.....	17
進階內容.....	18
GUI 語言設定.....	18
第 6 章工作.....	21
工作說明.....	21
多管理者核准.....	22
工作核准.....	22

工作拒絕.....	22
工作放棄.....	22
工作資訊.....	22
第 7 章 MDE 管理使用者管理.....	25
管理使用者角色.....	25
產品管理者角色.....	25
安全管理者角色.....	25
管理使用者管理.....	25
新增管理使用者.....	25
編輯管理使用者密碼.....	25
編輯管理使用者角色.....	26
編輯管理使用者狀態.....	26
移除管理使用者.....	26
使用者帳戶鎖定.....	27
LDAP 目錄清單.....	27
使用者來源.....	28
第 8 章事件.....	29
事件日誌.....	29
事件詳細資料.....	30
事件匯出.....	30
事件轉遞.....	30
事件引數.....	30
代理程式事件.....	31
可靠的事件.....	31
第 9 章 原則強制執行金鑰管理.....	33
新增金鑰.....	33
編輯金鑰.....	33
金鑰旋轉.....	33
金鑰撤銷.....	35
金鑰解構.....	35
自動產生的金鑰.....	35
外部金鑰儲存庫.....	35
KMIP 金鑰儲存庫.....	35
硬體安全模組 (HSM).....	37
第 10 章 檔案層次原則定義.....	39
選取元.....	39
路徑集.....	40
資料類型.....	40
資料類型列.....	40
資料類型列變數.....	41
處理程序.....	41
第 11 章 代理程式供應及管理.....	43
新增代理程式.....	43
身分.....	43
網路.....	44
包含原則的檔案、包含原則的磁區及物件儲存庫建立.....	44
磁區.....	46
物件儲存庫代理程式建立.....	47
授權使用者.....	50
代理程式工具.....	51
檢閱及建置.....	51
代理程式啟動.....	52

檢視代理程式.....	52
代理程式報告.....	52
安裝代理程式.....	53
針對 Linux 安裝代理程式.....	53
針對 AIX 安裝代理程式.....	55
針對 Windows 安裝代理程式.....	55
作用中的原則.....	57
編輯代理程式.....	57
編輯代理程式資訊.....	57
新增/刪除憑證.....	58
代理程式工具.....	59
SU 資料存取.....	59
暫停原則.....	60
原則變更.....	60
代理程式 Snapshot.....	64
儲存代理程式編輯及 Snapshot.....	64
管理 Snapshot.....	64
解除安裝檔案代理程式.....	66
解除安裝磁區代理程式.....	67
解除安裝磁區代理程式.....	67
解除安裝具有原則的磁區代理程式.....	67
解除安裝物件儲存庫代理程式.....	68
從 MDE 中移除代理程式.....	68
代理程式公用程式.....	69
第 12 章 作業.....	71
產品資料備份及還原.....	71
產品資料備份.....	71
產品資料還原.....	71
核心更新.....	72
升級.....	72
針對 MDE 伺服器.....	72
針對代理程式目標 VM.....	73
服務資料.....	74
收集服務資料.....	74
移除 PPM 日誌中的機密性資訊.....	74
附錄 A 範例代理程式安裝程序.....	77
Red Hat / CentOS 程序.....	77
AIX 處理程序.....	78
Windows 伺服器處理程序.....	78
附錄 B 憑證管理中心 (CA) 憑證範例.....	81
附錄 C 轉換以建立 PKCS12 檔案範例.....	85
附錄 D 注意事項.....	87
變更已指派的金鑰.....	87
概觀.....	87
背景.....	87
旋轉具有加密備份的金鑰.....	87
概觀.....	87
背景.....	87
附錄 E 就地加密.....	89
指令選項.....	89

審核步驟.....	89
加密步驟.....	89
附錄 F 代理程式除錯記載.....	91
Linux 代理程式.....	91
Windows 代理程式.....	91
附錄 G 非 OVA 部署.....	93
附錄 H 軟體版本檢查.....	95
附錄 I 名詞解釋.....	97
注意事項.....	103
商標.....	104
產品說明文件的條款.....	104
隱私權原則考量 privacy policy consi.....	105

第 1 章 簡介

授權使用許可權

此軟體的使用受到授權合約條款的限制。

聯絡點

如需 IBM Multi-Cloud Data Encryption (MDE) 的相關資訊，請造訪 IBM 支援中心網站，網址為：<https://www.ibm.com/support/home/>。

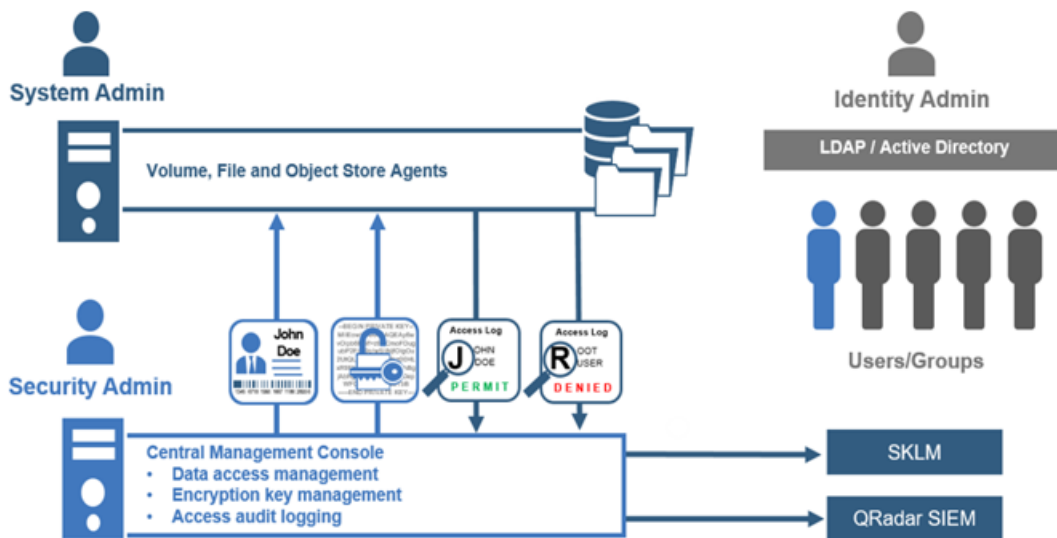
管理手冊的背景及目的

《管理手冊》是安裝、管理及使用 MDE 的主要參照，用於加密代理程式供應及管理、原則定義（存取及加密控制）、原則強制執行金鑰管理，以及確保使用所部署代理程式之所選取伺服器上待用資料的安全。此文件供具有公司網路管理存取權及知識的系統管理者用來安裝及管理產品。

第 2 章 一般概觀

產品概觀

IBM Multi-Cloud Data Encryption (MDE) 是由 SPx® 技術支援的綜合性資料安全產品，其會結合待用資料加密（透過代理程式）與用作中央管理主控台之 Policy Provisioning Manager (PPM) 的其他強大保護特性。MDE 容許供應代理程式、進行資料存取原則設定（作業及加密存取定義），以及從單一集中化位置執行多達 25,000 個代理程式的管理（金鑰生命週期、代理程式更新項目及使用者存取登入）。MDE 提供具有彈性的無縫安全系統以指派代理程式，使用唯一的加密分割技術在檔案系統層次或磁區層次加密資料。該技術提供的資料中心保護遠超出標準加密，讓資料加密更為強大堅固，從而免受暴力密碼破解攻擊。而且它進一步加強保護，這層保護透過定義精細的存取原則，能夠在使用者層次限制、監視及審核資料存取。

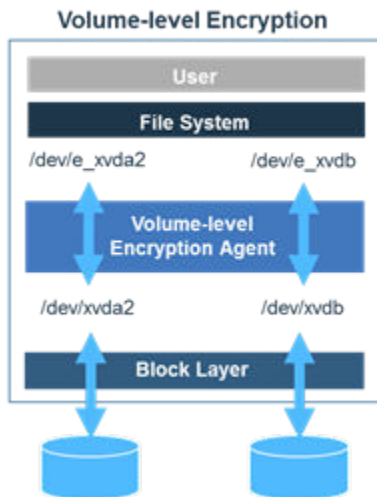


MDE 透過不同的管理者角色提供權責區分：產品管理者與安全管理者。產品管理者角色已被委託配置及維護 MDE 產品所需要的許可權。安全管理者角色已被委託供應及管理代理程式所需要的許可權。這些角色在「第 7 節：MDE 管理使用者管理」中進一步進行討論。

MDE 支援安裝四種代理程式類型，以提供用來施行原則定義的加密資料保護。

代理程式類型

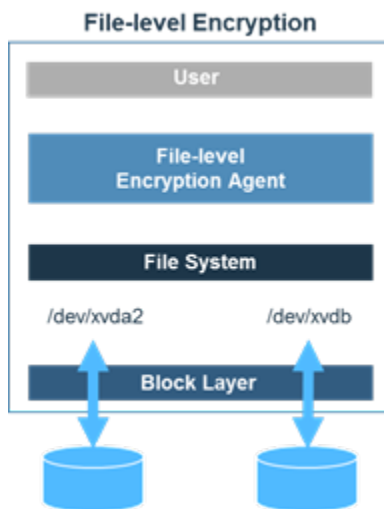
磁區代理程式 (Volume Agent)



「磁區」代理程式為磁區層次加密提供有限的存取原則控制。磁區層次加密透過作業系統中的區塊驅動程式實作，以受保護且預先定義的儲存裝置形式提供安全。

整個磁區作為一個單元進行定義及加密保護。隨著新增、編輯或刪除資料，「磁區」代理程式可確保使用 PPM 管理的加密金鑰對磁區內的所有資料進行加密保護。

具有原則的檔案代理程式



具有原則的檔案代理程式會結合檔案層次加密與資料存取原則。檔案層次加密在檔案系統層次提供個別檔案保護。檔案及儲存環境大小僅由檔案系統而非「具有原則的檔案」代理程式限制。受保護資料的位置由該路徑定義的工作群組金鑰確保安全，且其內部及之下儲存的所有個別檔案會使用無法預期的唯一起始設定向量 (IV) 單獨加密。受保護的資料可儲存在本端檔案系統中或透過 NFS 安裝在網路上。

唯一的檔案層次金鑰是由內部金鑰管理系統進行處理。基於原則的存取控制位於加密的最上層，容許定義最低授權的存取控制，將存取權的存取記載及限制指定給特定系統功能，例如讀取/讀寫/複製/刪除。這些原則控制與標準 LDAP 或 Active Directory 許可權一起運作。如果使用者沒有 LDAP 或 Active Directory 中資料的許可權，則安全管理者無法改寫那些存取控制及授權資料存取。

依預設，所有使用者都無法存取原則所涵蓋的資料。安全管理者需要定義具有存取權的人員。這樣安全管理者就可以限制系統管理者、雲端供應商管理者及 root 使用者存取受保護的資料。

具有原則的磁區代理程式 (Volume with Policy Agent)

具有原則的磁區代理程式利用磁區層次的磁區代理程式加密，以及基於檔案的作業存取控制原則，可以針對一或多個受保護檔案路徑進行套用及施行。

物件儲存庫代理程式 (Object Store Agent)

物件儲存庫代理程式在「N 之 M」模型上運作，該模型可以判斷在所建立的資料總數 (N) 中，重建其中資料 (M) 所需的資料數量。所儲存的資料（視授權而定可以儲存在本端或遠端位置）稱為「共用」。使用多種共用可以改進資料流程，以及新增資料備援及容錯的選項。受支援的 M:N 分散式共用模型是 1:1、2:3 或 2:4。

物件儲存庫代理程式 (OSA) 會加密傳送至物件儲存體的資料。將檔案傳輸至物件儲存體時，該代理程式會充當這些檔案的傳輸通道，並在傳輸過程中加密並分割資料。透過物件儲存庫代理程式從物件儲存體中擷取的檔案會在擷取時進行解密。會加密物件儲存體中的待用檔案。只有授權使用者才能透過物件儲存庫代理程式傳送/接收資料。

代理程式功能矩陣

代理程式功能	磁區代理程式 (Volume Agent)	具有原則的磁區代理程式 (Volume with Policy Agent)	具有原則的檔案代理程式	物件儲存庫代理程式 (Object Store Agent)
加密整個磁區	✓	✓		
個別加密指定受保護目錄中的檔案			✓	
檔案層次原則		✓	✓	
檔案存取審核日誌		✓	✓	
防止管理者存取使用者資料			✓	
加密物件儲存體中的資料				✓

第 3 章 規劃考量

必要條件

IBM Multi-Cloud Data Encryption (MDE) 的安裝是直接轉遞程序，其中包括安裝基本 Open Virtual Appliance (OVA) 及執行「供應原則與管理 (PPM)」安裝程式。

準備時，最好先檢閱完整安裝指示，然後再安裝軟體。以下是成功安裝及操作 IBM Multi-Cloud Data Encryption 的必要條件清單。

1. 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。
2. 已封裝基本 OVA
3. PPM 安裝程式
4. 具有受支援代理程式作業系統的一或多個目標伺服器 (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)。
5. 瀏覽器：Google Chrome®、Microsoft Internet Explorer® 10+、Mozilla Firefox® ESR 52+。
6. PPM 與所有代理程式之間的網路存取。
7. 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。

如需更多詳細資料，請參閱「憑證需求和伺服器憑證設定」；如需範例，請參閱第 81 頁的『[附錄 B 憑證管理中心 \(CA\) 憑證範例](#)』。

對於物件儲存庫代理程式 (OSA)，還有下列額外的需求：

- S3 相容物件儲存體：Amazon Web 服務 (AWS S3) 和 IBM 雲端物件儲存體 (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 程式庫或 Boto Python 程式庫來讓資料指向 OSA 代理程式的應用程式或公用程式

重要附註：強烈建議 MDE、外部資料庫及代理程式利用 NTP 協調系統時間。這將確保事件 / 審核日誌時間戳記適當地排序。

最低系統需求

PPM VM 最低系統需求

- CPU 4
- 8 GB RAM
- 40 GB 可用儲存體
- 需要網路存取權

Linux 代理程式最低系統需求

- 已啟用 AES-NI 的一個核心 64 位元 CPU @2GHz
 - （建議使用已啟用 AES-NI 的 2 個核心 64 位元 CPU @2GHz）
 - 2 GB RAM（建議使用 4 GB RAM）
- 20 GB 可用硬碟空間
 - 建議日誌檔案空間為 300 MB 或以上

- 需要網路存取權
- 在 Red Hat/CentOS 上安裝/更新下列套件：curl、openssl 及 nss
- 起始代理程式安裝期間的網際網路存取或本端儲存庫存取
- 代理程式需要 SSL 憑證

Windows 代理程式最低系統需求

- 已啟用 AES-NI 的單核心 64 位元 CPU @2GHz - 建議使用已啟用 AES-NI 的雙核心 64 位元 CPU @2GHz
- 4 GB RAM - 建議使用 8 GB RAM
- 20 GB 的可用硬碟空間 - 建議日誌檔案空間為 300 MB 或以上
- 需要網路存取權
- 代理程式需要 SSL 憑證

註：建立代理程式之前 SSL（自簽或憑證管理中心）憑證/金鑰組檔案。利用憑證在代理程式與 MDE 伺服器之間建立安全的 TLS 連線。

憑證需求

在 PPM 伺服器與代理程式之間建立安全連線需要憑證。憑證需求包含下列各項：

- PPM 伺服器要求代理程式所提供的憑證必須解析為該代理程式（DNS 主機名稱或 IP 位址）
- PPM 伺服器要求代理程式所提供的憑證必須具有用戶端鑑別延伸金鑰用法集
- 代理程式要求 PPM 伺服器所提供的憑證必須解析為該 PPM 伺服器（DNS 主機名稱或 IP 位址）
- 代理程式要求 PPM 伺服器所提供的憑證必須具有伺服器鑑別延伸金鑰用法集

PPM 與代理程式應該同步為可靠時間來源，以確保憑證在有效期間內。

每一個已部署的代理程式都需要唯一憑證。

代理程式的檔案系統支援

「磁區」代理程式在磁區層次執行加密。「具有原則的檔案」代理程式將使用主機作業系統的受支援檔案系統或在主機作業系統的受支援檔案系統上執行。「具有原則的檔案」代理程式及「具有原則的磁區」代理程式支援下列檔案系統：

Linux 伺服器

- EXT3
- EXT4
- XFS（在 Red Hat/CentOS 6.5 或更新版本上）
- NFS (NFSv3, NFSv4)

Windows 伺服器

- NTFS
- ReFS（在 Windows Server 2012 R2 或更新版本上）

AIX

- JFS2

網路設定

關於這項作業

MDE 需要 MDE PPM 伺服器與代理程式之間存在一致的網路連線。支援網際網路通訊協定 IPv4 和 IPv6。搭配使用靜態 IP 指派或 DHCP 與靜態租賃將滿足此需要。此外，將能夠適當地運作 DNS 基礎架構，以及在生態系統內利用主機名稱。

網路埠

功能	預設埠	可配置
Web	443	是
資料庫	5432	是
外部 LDAP	無	是
LDAP 目錄	無	是
電子郵件事件轉遞	無	是
Syslog 事件轉遞	無	是

OVA 配置

提供的 MDE OVA 已預先配置，且 MaxAuthTries 設為 1。若要順利透過 SSH 對 MDE VM 進行鑑別，則 MaxAuthTries 將需要進行變更（不建議），或者 SSH 用戶端將需要在指令行上或本端 SSH 用戶端配置中，將 PubkeyAuthentication 設為 "no"。

REST 介面

MDE 支援完整程式化 REST 介面。根 REST URL 為：

`https://<Virtual Machine IP>/rest/`

嚴重附註

REST API 將容許管理者執行不可透過 Web 介面存取的進階功能。REST API 可能透過可讓代理程式進入不受支援狀態的方式使用；因此，瞭解 REST API 程式設計知識是必要的。

如需相關詳細資料，請參閱 IBM Multi-Cloud Data Encryption (MDE) REST API 規格文件。

第 4 章 產品安裝

準備安裝

MDE 安裝程序具有三個步驟：

1. 必要條件
2. MDE 基本 Open Virtual Appliance (OVA) 可用
3. 支援的 Hypervisor (VMware ESXi™)

授權

MDE 不需要唯一的產品授權，即可在超出軟體授權合約所提供的範圍執行或配置代理程式。

MDE OVA/VM 管理

部署 MDE OVA 之後，更新系統以確保安裝最新的安全修補程式及軟體版本。

註：定期更新系統以套用安全修補程式以及更新的軟體版本。

安裝 MDE

關於這項作業

若要安裝 MDE 軟體：

例如使用檔案 `ibm_sw_mde_X.x.x-XX.bin` 將建置號碼 XX 替換為可用軟體的版本，並以 root 使用者身分操作。

程序

1. 將 MDE 基本 OVA 部署至 Hypervisor。在此範例中，它將會稱為“MDE VM”。
2. 以管理者身分登入，並設定新的密碼。

MDE VM 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，並且不能包含與前一個密碼相同的 5 個字元。

3. 記下 MDE VM 的 IP 位址。
4. 使用 SCP 或類似的檔案傳送方法，將 `ibm_sw_mde_X.x.x-XX.bin` 上傳至 MDE。
5. 讓 bin 檔成為執行檔。

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

6. 執行 bin 檔。

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

7. 選取「英文」，然後點擊 Enter 鍵。
8. 閱讀授權頁面，定位到「確定」，點擊 'Enter' 鍵以繼續。
9. 選取「是」，點擊 Enter 鍵以接受授權合約。
10. 完成擷取後，在「確定」上點擊 Enter 鍵以返回指令行。

11. 以 root 使用者身分安裝 RPM。

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

12. 現在已安裝好 MDE，但是尚未配置。

註：在配置完成之前，請勿重新啟動 MDE VM。

語言設定

關於這項作業

MDE 對 VM Script 和 PPM GUI 支援多種語言。在執行產品之前，您將需要配置預設語言喜好設定。

註：語言是透過 RPM 安裝到 MDE VM 中。安裝程式二進位檔隨附一組內建的語言 RPM。在起始安裝之後可以新增其他語言，但是可能需要重新啟動 PPM 服務才能生效。

如果要配置預設語言，請遵循以下步驟：

程序

1. 執行 spsd-langsetup Script。

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

2. 檢視現行預設語言碼。如果未設定任何語言碼，它將會是空白的。

```
設定預設語言碼。  
現行預設語言碼為：
```

3. 檢視可用的語言碼清單。（下面清單可能顯示您的產品版本中無法使用的範例）。

```
可用的語言碼：  
en_US  
ja_JP  
ko_KR
```

4. 輸入新的預設語言碼。

```
輸入新的預設語言碼：en_US  
預設語言碼將會是 en_US
```

5. 重新執行 spsd-langsetup Script 以驗證是否已設定預設語言碼。

```
設定預設語言碼。  
現行預設語言碼為：en_US
```

資料庫設定

關於這項作業

MDE 支援內部或外部資料庫配置。在任一情況下，您將需要在第一次啟動 MDE 之前，配置 MDE 以與所配置的資料庫進行通訊。

若要建立資料庫與 MDE 的關聯，您將需要修改 MDE VM /etc/spsd/db.props 檔。您將需要以 root 使用者身分編輯此檔案。

註：執行 spsd-pgsetup Script 將會使用在提示中輸入的值自動修改 db.props 檔。

配置檔案內容，以如下所示連接至適當的內部或外部資料庫。在重新啟動 MDE 之前，資料庫內容變更不會生效。

嚴重附註

修改 **db.props** 時，遵循下列限制項：

- 內容名稱與 = 之間無空格
- = 與內容值之間無空格

內部資料庫

目前，MDE 支援 PostgreSQL 作為內部資料庫。

內部 Postgres 資料庫

MDE OVA 與安裝的 PostgreSQL 軟體預先封裝在一起。如果要將資料庫配置為使用 MDE，請遵循以下步驟：

1. 執行帶有 "--local" Script 選項的 `spsd-pgsetup` Script。

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

註：“--local” 選項會在內部「本端」PostgreSQL Server 上配置新的空資料庫。

在套用這些設定之後，請繼續進行「伺服器憑證設定」。如果您打算在遠端目標上設定資料庫，請繼續進行「外部資料庫」。

外部資料庫

目前，只有受支援的外部資料庫伺服器為 PostgreSQL。在執行此程序之前，您必須確定已知下列資訊：

- 可存取的 PostgreSQL 資料庫伺服器的名稱（或 IP 位址）
- 上述 PostgreSQL 伺服器在其上接聽的埠號
- 上述伺服器上的現有資料庫的名稱
- 被定義為上述資料庫之擁有者的現有使用者名稱
- 上述資料庫使用者的密碼

如果要將資料庫配置為使用 MDE，請執行 `spsd-pgsetup` Script。此指令中提供的所有值均為範例值：

```
$ sudo /opt/securityfirst/spsd/bin/spsd-pgsetup --host  
ext.postgres.svr1 --port 5432 --dbname policyDB --user policyDBuser  
--pass mypassword123
```

如果要將資料庫升級至最新綱目，請執行帶有 “--upgrade” Script 選項的 `spsd-pgsetup` Script

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

註：執行帶有 "upgrade" 選項的 `spsd-pgsetup` Script 會確保資料庫表格適當配置為 PPM 的現行版本。

在配置這些設定之後，請繼續進行「伺服器憑證設定」。

伺服器憑證設定

金鑰儲存庫、信任儲存庫及憑證管理中心

利用憑證在管理伺服器 (PPM) 與代理程式以及 Web 瀏覽器之間建立安全通訊階段作業。PPM 需要所有憑證都由憑證管理中心 (CA) 簽署。CA 會建立信任的根，通訊階段作業中的所有參與者都用它來驗證其他一方的身分。

- CA 簽署的憑證及其對應的金鑰都結合至 java 金鑰儲存庫。
- 必須將 CA 中用來簽署代理程式憑證的憑證（或憑證組合）新增至 PPM 信任儲存庫。

· 所有三個元件（金鑰儲存庫、信任儲存庫及 CA 憑證組合）都在下面的 PPM 憑證安裝程序中使用。
如需憑證管理中心憑證處理程序的範例，請參閱第 81 頁的『[附錄 B 憑證管理中心 \(CA\) 憑證範例](#)』。
透過安裝 Script `spsd-certsetup`（位於 MDE VM 的 `/opt/securityfirst/spsd/bin` 目錄中）
配置伺服器 web 憑證金鑰儲存庫及 web 憑證信任儲存庫。

若要配置金鑰儲存庫、信任儲存庫及代理程式 CA 組合，請以**粗體**輸入範例：

```
$ sudo /opt/securityfirst/spsd/bin/spsd-certsetup --ks /etc/ppm/certs/ppm.jks --kw password
$ sudo /opt/securityfirst/spsd/bin/spsd-certsetup --ts /etc/ppm/certs/trust.jks --tw password
$ sudo /opt/securityfirst/spsd/bin/spsd-certsetup --aca /etc/ppm/certs/ca_bundle.pem
```

附註

不會提供伺服器憑證元件（如金鑰儲存庫、信任儲存庫及 CA 組合），必須透過安裝 Script 上傳至 MDE VM。如果使用共用存取卡 (CAC) 進行鑑別，則需要啟用 PKI 設定。

公開金鑰基礎架構 (PKI) 設定

關於這項作業

PKI 配置可讓 PPM 提供 PPM 使用者鑑別的次要方法。當配置好時，PPM 將接受用戶端憑證作為 Web 和 REST 階段作業的鑑別方法。

此憑證必須由受 PPM 信任的 CA 所簽署。PPM 將根據 `spsd-certsetup` Script 中所定義的規則來驗證憑證。

粗體範例輸入：

```
$ sudo /opt/securityfirst/spsd/bin/spsd-certsetup --crl-on --ocsp-on --pols-on oids
x.x.x.x.x.x.x.x,Y.Y.Y.Y.Y.Y
```

附註

可以在與金鑰儲存庫、信任儲存庫和 CA 組合相同的 Script 執行中配置 PKI。在這裡突然進行以取得指示值。

在安裝 MDE、配置資料庫、新增憑證及選擇性地設定 PKI 之後，現在您可以重新啟動 MDE VM。

啟動及第一次登入

關於這項作業

在部署和配置完成後，重新啟動 MDE 伺服器或是直接從 MDE 主控台啟動服務 "spsd" 以啟動 Web GUI。您將需要透過虛擬機器主控台或主機 Hypervisor 擷取虛擬機器的 IP 位址或主機名稱。

開啟受支援的 Web 瀏覽器，然後輸入 IP 位址或主機名稱作為 URL 以到達 MDE 登入頁面。

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

此時，您可以從可用的支援語言清單變更語言設定。



Please Sign In

Login

預設認證為：

使用者名稱：admin
密碼：admin

附註

- 第一次登入之後，需要變更預設認證
- MDE 支援大部分版本的 Firefox、Chrome、Microsoft Edge 及 Internet Explorer Web 瀏覽器
- 使用 PKI 用戶端鑑別時，它可能會略過登入頁面並直接跳至儀表板

第 5 章 MDE 圖形使用者介面 (GUI)

基本產品導覽

MDE 在頁面頂端包含一個導覽功能表。部分功能表項目包含子功能表清單。按一下每一個功能表項目，以導覽至適當的頁面，或者顯示子功能表清單。



- 首頁圖示 - 產品儀表板首頁的鏈結。
- 金鑰 - 包含金鑰相關子功能表頁面鏈結的功能表：外部金鑰儲存庫及受管理金鑰。
- 原則 - 包含原則相關子功能表頁面鏈結的功能表：資料類型、路徑集、處理程序及選取元。
- 代理程式 - 「代理程式」頁面的鏈結。
- 工作 - 「工作」頁面的鏈結。
- 事件 - 包含事件相關子功能表頁面鏈結的功能表：轉遞及日誌。
- 使用者 - 包含使用者相關子功能表頁面鏈結的功能表：帳戶及 LDAP 目錄。
- 設定 - 「設定」頁面的鏈結。

附註

MDE 支援角色型存取控制 (RBAC)，這意味著根據已登入使用者的角色，部分導覽項目將無法使用。因此，部分導覽項目可能無法用於所有管理使用者。

產品儀表板

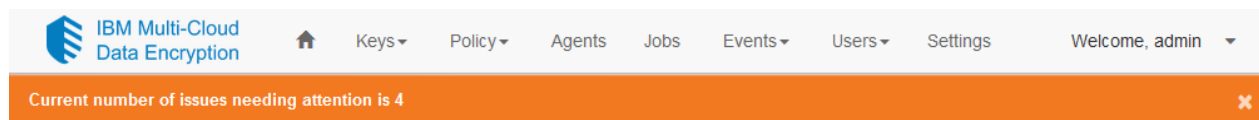
產品首頁是主要登入儀表板頁面。旨在為登入的管理者提供最近事件之現行狀態的摘要視圖。首頁包含最近的事件、事件趨勢及其他摘要資料。

文字框自動完成

文字輸入欄位貫穿整個使用者介面。部分文字輸入欄位將根據所輸入字元的自動完成清單來顯示比對準則。這些欄位可能需要多個字元，然後才會呈現自動完成建議清單。

注意通知

第一次登入時，使用者介面頂端將有一個彩色橫幅，指出需要解決的問題。



按一下橫幅中的文字，將管理者重新導向至其中顯示個別項目的「問題」頁面。

- ▶ The current number of job approvals allows unilateral action. [Dismiss](#)
- ▶ The number of users having Product Administrator role is nearing the threshold of required approvals or required rejections. [Dismiss](#)
- ▶ The number of users having Security Administrator role is nearing the threshold of required approvals or required rejections. [Dismiss](#)
- ▶ One or more users are defined as having both Product Administrator and Security Administrator roles. [Dismiss](#)

展開個別項目將提供有關如何解決問題的詳細資料。

- ▼ The current number of job approvals allows unilateral action. [Dismiss](#)

Summary It is best practice to require a minimum two administrators for job approval.

How to resolve Go to the "Advanced Properties" tab on the "Settings" page, and edit the "Number of approvals required to run a job" field. Note that it may also be wise to do this for number of rejectors as well, depending on company structure.

[Resolve](#)

解決所有未解決的問題之後，將不會顯示橫幅；不過，管理者可以選擇針對現行頁面跳出橫幅。

附註

可能會產生建立新的「需要注意」問題的新條件，且橫幅將重新出現。

進階內容

容許產品管理者配置用於定義產品行為的進階內容。可以透過設定頁面存取進階內容。這些內容的範圍限制為本端實例，而如果利用「高可用性 (HA)」或多租戶功能，則範圍可能限制為 MDE 生態系統。

Advanced Properties

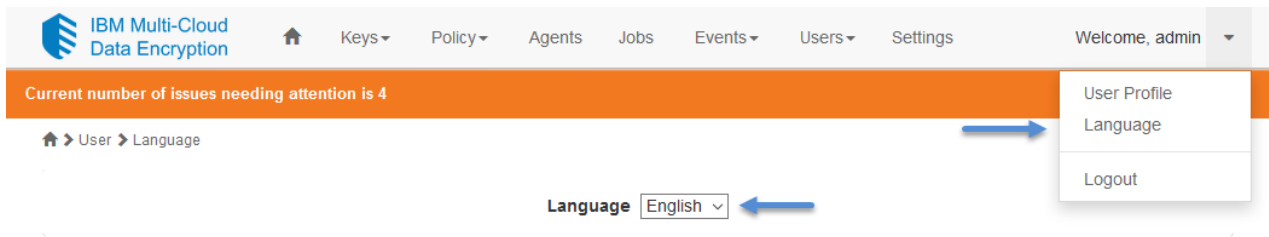
Property	Value	Description	Actions
com.securityfirstcorp.atlantis.bundles.haas.iterations	600000	Number of iterations used by REST API token hashing algorithm	Edit
com.securityfirstcorp.atlantis.jobs.requiredApprovers	1	Number of approvals required to run a job	Edit
com.securityfirstcorp.atlantis.jobs.requiredBuffers	2	The buffer number in between the number of users available and when we issue a warning	Edit
com.securityfirstcorp.atlantis.jobs.requiredRejectors	1	Number of rejections required to reject a job	Edit
events.maxLogLength	50000	Maximum number of entries in event log before rolling starts	Edit
com.securityfirstcorp.atlantis.bundles.userman.iterations	300000	Number of iterations used by user password hashing algorithm	Edit

若要編輯內容，產品管理者必須按一下「編輯」按鈕。進行適當的變更之後，按一下「儲存」按鈕，將會建立工作。

GUI 語言設定

在 GUI 中，從登入頁面或首頁選取時，您可以變更為在起始安裝期間安裝的其中一種受支援語言。

- **登入頁面** - 在頁面右上角找到。按一下下拉功能表以取得受支援的語言清單。
- **首頁** - 在右上角的下拉功能表中找到，選取「語言」以取得受支援的語言清單。

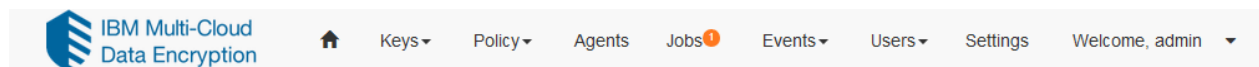


在 GUI 中顯示的語言由下列階層決定（會使用第一個呈現設定）：

1. 透過 PPM 的使用者介面設定的語言 Cookie 的值。
2. 使用者瀏覽器語言設定的值。
3. 透過 PPM CLI script-langsetup 設定的語言碼的值。
4. 第一個找到的已安裝的 PPM 語言套件。

第 6 章 工作

MDE 納入工作系統，以管理執行中作業的核准及計時。多種功能在確認之前利用工作系統等待核准。建立工作時，會將新的工作新增至「工作」頁面上的清單。



管理者將可以選擇核准、拒絕或放棄每一個工作。每一個管理者都只能對每個工作採取動作一次。

Type	State	Created	Started	Completed	Notes	Actions
User Create	Waiting	2017-09-22T23:21:01Z				Edit Note Approve Reject Abstain Show Info

工作說明

工作	說明	種類	角色
進階內容	修改進階內容	產品管理	產品管理者
修改金鑰儲存庫	變更原則強制執行金鑰儲存庫的位置/詳細資料	產品設定	產品管理者
金鑰旋轉	旋轉代理程式生態系統中的一組金鑰	金鑰管理	安全管理者
金鑰撤銷	從代理程式生態系統中撤銷一組金鑰	金鑰管理	安全管理者
金鑰清除	從代理程式生態系統中永久地移除一組金鑰，造成資料流失。	金鑰管理	安全管理者
新增代理程式	將新的代理程式供應及新增至生態系統	代理程式管理	安全管理者
刪除代理程式	從 MDE 管理中移除代理程式	代理程式管理	安全管理者
修改代理程式	修改代理程式的相關資訊	代理程式管理	安全管理者
原則更新	修改與代理程式相關聯的原則	代理程式管理	安全管理者
建立新的管理使用者	建立新的 MDE 管理者	MDE 管理使用者管理	產品管理者
刪除管理使用者	移除 MDE 管理者	MDE 管理使用者管理	產品管理者
新增管理使用者角色	將角色新增至 MDE 管理者	MDE 管理使用者管理	產品管理者
移除管理使用者角色	從 MDE 管理者移除角色	MDE 管理使用者管理	產品管理者
變更管理使用者密碼	變更 MDE 管理者的密碼	MDE 管理使用者管理	產品管理者
變更管理使用者狀態	啟用或停用 MDE 管理使用者帳戶	MDE 管理使用者管理	產品管理者

登錄目錄	配置 MDE 管理使用者的 LDAP 伺服器目錄	MDE 管理使用者管理	產品管理者
刪除目錄	從 MDE 移除 LDAP 伺服器目錄	MDE 管理使用者管理	產品管理者
更新目錄	修改 LDAP 伺服器目錄	MDE 管理使用者管理	產品管理者

多管理者核准

可在 MDE 內配置需要的核准者及拒絕者數目。依預設，針對單一管理者核准配置 MDE。強烈建議需要兩個或以上管理者進行工作核准。多管理者核准可防止單一管理者在 MDE 本身內或對任何受管理代理程式實例進行變更。

User	Time	Actions	Required Approvals	Required Rejections	Notes
admin	2017-09-22T23:22:35Z	Approve	1	1	

嚴重附註

管理使用者數目必須符合或超出「需要核准」或「需要拒絕」的工作數目。請確定有必要數目的管理使用者，然後再變更這些值。

可以按工作類型來置換核准和拒絕臨界值。系統所定義的每一個工作類型（「內容變更」工作除外）在「進階內容」中都有核准和拒絕臨界值，設定該臨界值時，將會置換系統預設值。內容一旦設定就無法取消設定

「內容變更」工作是唯一一個沒有核准和拒絕臨界值的工作類型，因為此工作用於控制「進階內容」的修改。針對此工作，核准和拒絕臨界值將一律高於系統預設值，或高於針對任何其他工作類型所定義的最高置換值。此動作將會確保無法透過內容變更程序來破壞任何其他工作類型的臨界值。

工作核准

若要核准工作，具有適當許可權的管理者必須導覽至「工作」頁面，尋找適當的工作，以及按一下「核准」按鈕。達到必要數目的管理者核准之後，工作將執行。

工作拒絕

若要拒絕工作，具有適當許可權的管理者必須導覽至「工作」頁面，尋找適當的工作，以及按一下「拒絕」按鈕。達到必要數目的管理者拒絕之後，將永久地取消工作。

工作放棄

放棄工作指出管理者已看到工作，但是不想要進行核准或拒絕。放棄可能選取好說明為「審核」位置，並阻止管理者未來在同一工作上選取不同位置。

工作資訊

MDE 內的每一個工作都具有不同的說明資訊。可以按一下「顯示資訊」按鈕，即會顯示工作特定資訊。此外，由不同管理者對工作採取的任何動作（核准、拒絕、放棄）將與採取該動作的管理者使用者名稱一起顯示。

User Create	Done	2017-09-22T23:22:36Z	2017-09-22T23:22:36Z	2017-09-22T23:22:36Z		<div>Hide Info</div>
-------------	------	----------------------	----------------------	----------------------	--	----------------------

User	Time	Actions	Required Approvals	Required Rejections	Notes
admin	2017-09-22T23:22:35Z	Approve	1	1	

Job Properties

User	ProductAdmin
------	--------------

第 7 章 MDE 管理使用者管理

管理使用者角色

MDE 會利用純靜態「角色型存取控制 (RBAC)」設計。MDE 內的特定功能需要特定許可權。完整的 MDE 許可權集會分組為兩個不同角色：產品管理者與安全管理者。隨時可以新增每個角色的其他管理者。

產品管理者角色

產品管理者角色已被委託配置及維護 MDE 產品所需要的許可權。

安全管理者角色

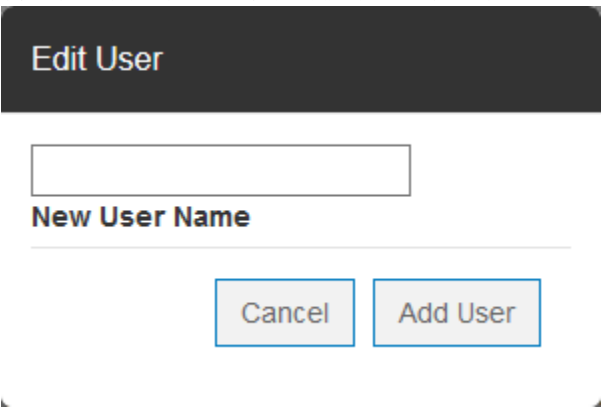
產品管理者角色已被委託供應及管理代理程式所需要的許可權。這些許可權包括但不限於：外部原則群組的原則定義及規格、金鑰管理、資料類型定義、代理程式管理、外部金鑰儲存庫配置及外部 LDAP 配置。

管理使用者管理

產品管理者擁有在 MDE 內新增、修改及移除其他管理使用者所需要的許可權。

新增管理使用者

新增管理使用者時，系統將提示產品管理者，以輸入新的管理使用者名稱。



填寫唯一使用者名稱，然後將建立工作以將此管理使用者新增至 MDE。

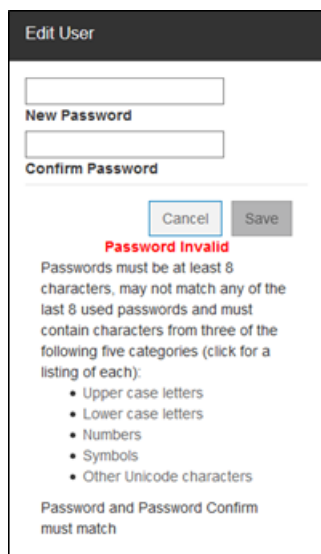
Type	State	Created	Started	Completed	Actions
Scheduler	Waiting	2019-03-20T16:14:01Z			<div><div>Approve</div><div>Reject</div><div>Abstain</div><div>Hide Info</div></div>
<div><div><div>Approved</div><div>None</div></div><div><div>Rejected</div><div>None</div></div><div><div>Abstained</div><div>None</div></div></div>					
Type : User Create		Frequency : Once		Starts : Upon approval	
Job Properties					
User				test	

必須有必要數目的產品管理者核准工作，才能建立使用者。

系統會建立新增的管理使用者，該使用者具有到期的密碼，且未定義角色。產品管理者必須編輯密碼、角色及狀態。這些更新中的每一個都會產生工作。必須先核准工作，然後新的管理使用者才能夠在 MDE 中變成作用中。

編輯管理使用者密碼

若要編輯管理使用者的密碼，請導覽至適當的使用者，並選取「編輯密碼」按鈕。將會顯示輸入密碼對話框。



輸入符合所識別規則的密碼。輸入之後，儲存變更，將會建立工作。

必須有必要數目的管理使用者核准工作，密碼變更才會生效

註：新增的管理者在首次登入時，系統將提示變更密碼。

編輯管理使用者角色

若要編輯管理使用者的角色，請找到使用者列，並選取「編輯角色」按鈕。角色項目勾選框將出現在行內。

執行編輯的管理使用者將能夠套用其具有的角色，例如「內建管理者角色」，這是可以套用產品管理者及安全管理者角色的起始使用者。具有相同角色的使用者則能夠這樣做。

ProductAdmin	Disabled	<input type="checkbox"/> Product Administrator <input type="checkbox"/> Security Administrator		2017-09-22T23:25:40Z	<button>Save</button> <button>Cancel</button>
--------------	----------	---	--	----------------------	---

選取所需的角色，按一下「儲存變更」按鈕，將會建立工作。

必須有必要數目的管理使用者核准工作，角色變更才會生效。

編輯管理使用者狀態

若要編輯管理使用者的狀態，請導覽至生效的使用者，並選取「編輯狀態」按鈕。狀態項目下拉清單將出現在行內。

ProductAdmin	Disable ▼	None		2017-09-22T23:25:40Z	<button>Save</button> <button>Cancel</button>
--------------	------------------------	------	--	----------------------	---

狀態值為：已啟用、已停用及已鎖定。

- **已啟用** – 管理使用者處於作用中，能夠執行動作。
- **已停用** – 管理使用者處於非作用中，無法執行動作
- **已鎖定** – 管理使用者已鎖定，無法執行動作。

選取想要的狀態，然後按一下「儲存」，將會建立工作來修改使用者狀態。

必須有必要數目的管理使用者核准工作，狀態變更才會生效。

移除管理使用者

若要移除管理使用者，請找到目標使用者列，然後按一下「刪除」按鈕。將啟動工作，以從 MDE 移除使用者。此動作僅可由具有產品管理者角色的使用者執行。

Type	State	Created	Started	Completed	Notes	Actions
User Delete	Waiting	2017-09-22T23:37:05Z			Edit Note	Approve Reject Abstain Show Info

必須有必要數目的管理使用者核准工作，才能移除使用者。

嚴重附註

- 移除管理使用者是永久性動作。
- 必須維持足夠的管理使用者，才能滿足必要的工作核准條件（請參閱「多管理者核准」小節）。
- 如果沒有足夠的管理使用者，則無法順利接受工作。

使用者帳戶鎖定

為了保護系統和使用者帳戶免遭暴力密碼破解攻擊，會在 10 次連續失敗登入嘗試之後鎖定使用者帳戶。在明確啟用使用者帳戶（請參閱「編輯管理使用者狀態」一節）或重新啟動伺服器服務之前，使用者帳戶將一直處於鎖定狀態。

附註

- 若要重新啟動伺服器服務，請在虛擬機器主控台中執行 **systemctl restart spsd**。
- 帳戶鎖定是以每個伺服器為基礎。在叢集中的某個伺服器上鎖定的帳戶不會在該叢集內的其他伺服器上自動鎖定。
- 使用者不能配置帳戶鎖定臨界值。

LDAP 目錄清單

產品管理者可以配置 LDAP 目錄以進行 MDE 使用者管理。可以新增、修改或刪除 LDAP 目錄。每一個工作在生效之前，都將建立一個工作以供核准。

新增/修改 LDAP 目錄時，可用的設定為：

- **目錄 ID** - LDAP 目錄的身分。
- **類型** - LDAP 或 Active Directory 的下拉選項
- **連結 DN** - 用來連結至 LDAP 伺服器的完整識別名稱。

連結 DN 範例語法如下所示：

```
uid={username},ou=users,dc=company,dc=com
```

註：選取類型 "Active Directory" 時，「連結 DN」區段呈灰色顯示，因為不需要此資訊。

- **主機** - LDAP 伺服器的 IP/主機名稱
- **埠** - LDAP 伺服器的埠
- **安全** - 安全或未受保護 LDAP 連線的 ID
- **動作** - 選取「儲存」或「取消」

Directory ID	Type	Bind DN	Host	Port	Secure	Actions
LDAP1	LDAP	uid={username},ou=users,dc=company,dc=com	10.10.10.1	536	<input checked="" type="checkbox"/>	Save Cancel

使用者來源

MDE 可以同步支援內部與外部定義的使用者。外部定義的使用者將在使用者清單的「目錄」直欄中顯示值。內部定義的使用者的該欄位將為空白。

Name	Status	Roles	Directory	PW Modified	Actions
admin	Enabled	Product Administrator, Security Administrator		2017-09-22T23:09:44Z	Edit Password Edit Roles Delete
ProductAdmin	Enabled	Product Administrator		2017-09-22T23:25:40Z	Edit Password Edit Status Edit Roles Delete
SecurityAdmin	Enabled	Security Administrator		2017-09-22T23:42:22Z	Edit Password Edit Status Edit Roles Delete

第 8 章 事件

MDE 包括事件聚集及轉遞系統。此系統會聚集受管理代理程式的事件，以及內部產生的事件，並將它們儲存在內部事件日誌中。此外，還可以將其配置為將事件轉遞至一或多個收件者

事件日誌

可以透過選取最上層功能表列上的「事件」功能表項目查看 MDE 事件日誌。

[Home](#) > [Events](#) > [Logs](#)

☐ Show Redacted Events Reload Export CSV

Show 10 entries Search:

Sequence	ID	Message	Type	Severity	Timestamp	Source
16	PS000D0005	Requested action change-passw...	SYSTEM	INFO	2017-09-22T23:42:22Z	localhost
15	PS000D0001	User admin has requested action ...	AUDIT	INFO	2017-09-22T23:42:22Z	localhost
14	PS000D0005	Requested action change-user-st...	SYSTEM	INFO	2017-09-22T23:42:21Z	localhost
13	PS000D0001	User admin has requested action ...	AUDIT	INFO	2017-09-22T23:42:21Z	localhost
12	PS000D0005	Requested action change-user-ro...	SYSTEM	INFO	2017-09-22T23:42:21Z	localhost
11	PS000D0001	User admin has requested action ...	AUDIT	INFO	2017-09-22T23:42:21Z	localhost
10	PS000D0005	Requested action change-user-st...	SYSTEM	INFO	2017-09-22T23:36:47Z	localhost
9	PS000D0001	User admin has requested action ...	AUDIT	INFO	2017-09-22T23:36:47Z	localhost
8	PS000D0005	Requested action change-user-ro...	SYSTEM	INFO	2017-09-22T23:35:51Z	localhost
7	PS000D0001	User admin has requested action ...	AUDIT	INFO	2017-09-22T23:35:51Z	localhost

Showing 1 to 10 of 16 entries First Previous 1 2 Next Last

此頁面在單一順序清單中顯示所有事件。每一個事件都具有序號、ID、訊息、類型、嚴重性、接收時間戳記及來源，定義如下：

- **序號** – 認作事件接收順序的數字。它是唯一的（即使同一事件重複出現），並將隨著時間推移而增加。
- **ID** – 事件的唯一 ID。同一事件的多個實例將具有共用 ID。
- **訊息** – 識別觸發事件之條件的說明文字。部分事件可能支援變數插入，因此當事件 ID 可能是共用時，文字可能略有不同。
- **類型** – 說明事件是源自系統動作還是使用者動作。類型為：
 - **系統** – 源自自動化 MDE 動作的事件。
 - **審核** – 源自使用者動作的事件。
- **嚴重性** – 事件狀態提示層次的相關指示。嚴重性種類為：
 - **資訊** – 不需要任何動作，僅供參考
 - **警告** – 不需要立即執行動作；建議條件監視
 - **重要** – 需要立即執行動作
- **時間戳記** – 以世界標準時間 (UTC) 格式指示的事件起源時間。

· **來源** – 起始事件之系統（代理程式或 MDE）的主機名稱或 IP。

可以透過「進階設定」配置 MDE 事件日誌大小。達到設定的大小限制之後，將在收到新的事件時，輪替掉最舊的事件。

事件詳細資料

事件可能具有不屬於事件訊息一部分的延伸引數。如果有，則事件將會在事件日誌的訊息直欄中顯示一個「詳細資料」鏈結。按一下「詳細資料」按鈕將會顯示延伸引數

34	PS00140002	Agent 1 logged off: reason code 1006.	Details	Absolute process path:	2018-04-10T15:02:05Z	localhost
33	DEC02014	Read/write denied for user3 on /home/data/	Details	Decision: Deny	2018-04-10T15:01:19Z	cos5-file
32	DEC02010	Read denied for user4 on /home/data/	Details	Group name: user3	2018-04-10T15:01:19Z	cos5-file
31	DEC02011	Write permitted for user1 on /home/development/	Details	Operation: Read or Write	2018-04-10T15:01:19Z	cos5-file

事件匯出

MDE 容許管理者從「事件」頁面上的「匯出 CSV」按鈕，以 CSV 檔案格式匯出事件清單。

Home > Events > Logs

☐ Show Redacted Events

Reload Export CSV

按一下「匯出 CSV」按鈕，會將事件檔案下載至用戶端機器。事件檔案中的每一列都是日誌中的事件。

事件檔案中的直欄如下所示：事件序號、事件 ID、已編寫旗標、事件訊息字串（省略了引數）、事件類型、事件嚴重性、事件引數、事件時間戳記及事件來源。

事件轉遞

收到的每個事件都將轉遞至每一個已配置的事件收件者。會在插入內部事件日誌中時平行轉遞事件。

產品或安全管理者可以修改產品的事件收件者。配置之後，MDE 建立或接收的所有事件都將轉遞至收件者。支援的收件者類型為 Syslog。

Home > Events > Forwarding

Email Recipients

New Email Recipient

Email	Host	Port	Security	User	Password	Format	Actions
No Recipients							

Syslog Recipients

New Syslog Recipient

Host	Port	Format	Actions
No Recipients			

MDE 還支援多個格式的已轉遞事件。受支援的格式為：「日誌事件延伸格式 (LEEF)」、「一般事件格式 (CEF)」及「雲端審核資料聯合 (CADF)」事件模型。

事件引數

除了一般事件訊息字串之外，還會將事件引數作為鍵/值參數傳送。這些參數將透過 "spx" 字首與引數名稱的連結字串來識別。例如，如果事件包含使用者名稱，則鍵/值配對字串可能為 "spxuser=user1"。

代理程式事件

MDE 從每個受管理（且已連接）的代理程式聚集系統及審核事件。這些事件會顯示在 MDE 事件日誌中，並轉遞至任何已配置的事件收件者。

附註

強烈建議 **MDE**、外部資料庫及所有代理程式利用 **NTP** 來協調系統時間。這將確保適當地排定事件/審核日誌時間戳記的順序。

可靠的事件

系統會即時處理從個別代理程式傳送至 MDE 的事件。這會確保如果遺漏事件，MDE 將返回到代理程式，要求遺漏的事件，並按照適當的順序將它插入事件日誌。

第 9 章 原則強制執行金鑰管理

安全管理者可以為 MDE 內的安全儲存體定義原則強制執行金鑰。這些金鑰可以與資料類型及磁區相關聯，以確保資料的安全，並提供加密存取控制。

🏠 > Keys > Managed Keys

Submit Rotation Job New Key				
ID	Name	Created	Notes	Actions
1	Key1	2017-09-22T23:49:12Z		Edit Submit Revocation Job
2	Key2	2017-09-22T23:49:17Z		Edit Submit Revocation Job
3	Key3	2017-09-22T23:49:23Z		Edit Submit Revocation Job

新增金鑰

新增金鑰時，必須輸入唯一的名稱。金鑰名稱不區分大小寫。金鑰值並未公開，且無法由使用者進行編輯。附註欄位是選用項。

ID	Name	Created	Notes	Actions
	<input type="text"/>		<input type="text"/>	Save Cancel

附註

金鑰名稱可以變更，但是實際金鑰值無法由使用者進行變更。

可以在「金鑰」頁面上，或者在使用代理程式建立精靈期間，新增金鑰。在代理程式精靈期間建立的所有「定義資料類型或資料類型列定義的」金鑰都是自動產生的，無法管理。只能在「金鑰」頁面上編輯金鑰。

編輯金鑰

建立金鑰之後，安全管理者可以修改金鑰的名稱。變更金鑰名稱不會變更實際基礎金鑰值。此外，可以修改附註欄位。

金鑰旋轉

MDE 可讓安全管理者在代理程式生態系統內旋轉金鑰。從「金鑰」頁面上，按一下「提交金鑰旋轉工作」按鈕。

系統將提示您上傳公開金鑰。此金鑰將用來加密所旋轉金鑰的金鑰委託。選擇適當的金鑰，新增金鑰，然後按「下一步」。

嚴重附註

SSL 金鑰必須進行 RSA 及 PEM 編碼。

Key Rotation



This wizard will assist you in selecting keys to be scheduled for rotation. Once the keys are selected, a job to rotate the keys will be queued for approval.

Upload Public Key

Browse...

No file selected.

Add Public Key

Public Key

Next

將顯示所有使用者建立的金鑰的清單。安全管理者可以選取任何數目的金鑰以旋轉。

Key Rotation



Select one or more keys from the list of all keys:

☒ Key1

☐ Key2

☐ Key3

Back

Next

選取想要的金鑰之後，將建立工作。

嚴重附註

如果金鑰與多個代理程式相關聯，則將影響使用該金鑰的所有代理程式。

工作核准時，將通知所有受影響的代理程式該金鑰旋轉。工作將繼續執行，直到所有受影響的代理程式已完成金鑰旋轉處理程序為止。根據受影響代理程式的數目，此工作可能需要較長時間才能完成。

附註

使用外部金鑰儲存庫時，它必須位於線上，金鑰旋轉才會成功。如果發生錯誤，請確保外部金鑰儲存庫位於線上，並重新啟動 PPM 伺服器或重新啟動 PPM 服務 (spsd)。

金鑰撤銷

金鑰撤銷會從 MDE 中撤銷金鑰，並將該金鑰放置在委託中。金鑰撤銷只能在目前未與任何作用中原則相關聯的金鑰上完成。在撤銷金鑰之前，安全管理者必須移除參照該金鑰的原則。

從代理程式原則關聯中移除利用金鑰的路徑並不會解密磁碟上的資料，因此如果希望資料可存取性，則必須先將資料移轉出受保護的目錄，然後再移除與該路徑相關聯的原則。

撤銷完成之後，受保護路徑中的所有剩餘資料將不可存取。撤銷的金鑰將儲存在委託中，並從一般 PPM 作業中移除。

警告

安全管理者必須更新代理程式原則來取消目標金鑰與所有代理程式的關聯，然後才能撤銷該金鑰。如需刪除路徑的相關資訊，請參閱「編輯代理程式」的相關小節。

金鑰解構

金鑰解構的運作方式與金鑰撤銷相同；然而，完成金鑰解構作業之後，金鑰不會放置到委託之中，這導致資料永久地無法存取。

附註

此功能只能透過 REST API 提供，如需詳細資料，請參閱 REST API 說明文件。

自動產生的金鑰

如果安全管理者不想要管理原則強制執行金鑰，則 MDE 可以為每一個新建的原則自動產生金鑰。自動產生的金鑰在建立時一律是唯一的，並且在金鑰管理頁面上不可見。

嚴重附註

無法旋轉或撤銷自動產生的金鑰。如果您需要旋轉或撤銷金鑰的能力，請改用指定的金鑰。

外部金鑰儲存庫

可以在以下兩個位置之一儲存金鑰：內部安全資料庫或外部金鑰儲存庫。MDE 起始設定為僅使用內部安全資料庫。如果安全管理者計劃利用外部金鑰儲存庫，則必須配置一個。外部金鑰儲存庫僅用於金鑰保護。必須透過 MDE 對外部金鑰儲存庫進行金鑰管理。

附註

用來設定外部金鑰儲存庫的指示由外部金鑰儲存庫供應商提供。

KMIP 金鑰儲存庫

關於這項作業

安全管理者將需要上傳 Java 金鑰儲存庫及 Java 信任儲存庫。遵循下列步驟，以建立 Java 金鑰儲存庫及 Java 信任儲存庫：

程序

1. 使用 PKCS12（公開金鑰密碼化標準 12 號）格式收集用戶端憑證檔及用戶端私密金鑰檔。對於稍後的步驟，我們將此稱為 "client.p12"。（請參閱第 85 頁的『[附錄 C 轉換以建立 PKCS12 檔案範例](#)』，以取得將用戶端憑證及用戶端私密金鑰結合至 PKCS12 格式化檔案的範例。
2. 收集公用 CA 憑證檔。對於稍後的步驟，我們將此檔案稱為 "sklm_ca.pem"。

```
[user@localhost]$ keytool -importkeystore -srckeystore client.p12 -keystore client.jks -storetype JKS
```

3. 將 PKCS12 檔匯入至新的 Java 金鑰儲存庫：

嚴重附註

在此步驟期間，將要求密碼。保留此密碼，以供稍後使用。

```
[user@localhost]$ keytool -v -list -keystore client.jks
```

4. 從檔案取得別名：
5. 將 CA 憑證檔匯入至新的 Java 信任儲存庫：

```
[user@localhost]$ keytool -import -trustcacerts -alias sklm  
-file sklm_ca.pem -keystore sklmtrust.jks
```

嚴重附註

在此步驟期間，將要求密碼。保留此密碼，以供稍後使用。

6. 從檔案取得別名：

```
keytool -v -list -keystore trust.jks
```

將需要填寫下列設定，外部金鑰儲存庫才能處於作用中：

- **名稱** - 外部金鑰儲存庫的使用者定義參照
- **狀態** - 這將告知 MDE，所定義的外部金鑰儲存庫應該置換現行作用中金鑰儲存庫。如果狀態是作用中，則 MDE 將開始使用金鑰儲存庫。如果狀態是非作用中，則 MDE 將不再使用金鑰儲存庫。
- **主機** - 外部金鑰儲存庫的 IP 位址。
- **埠** - 外部金鑰儲存庫的埠號。
- **用戶端金鑰儲存庫**
 - **金鑰儲存庫別名** - 收集的金鑰儲存庫別名。
 - **金鑰儲存庫檔** - Java 金鑰儲存庫檔。
 - **用戶端金鑰儲存庫密碼** - 金鑰儲存庫建立時的密碼設定。
- **信任儲存庫**
 - **信任儲存庫別名** - 收集的信任儲存庫別名。
 - **信任儲存庫檔案** - Java 信任儲存庫檔案。
 - **信任儲存庫密碼** - 信任儲存庫建立時的密碼設定。
- **是主要** - 識別用來作為所有讀取及寫入作業之主要金鑰儲存庫的外部金鑰儲存庫
 - 對於第一個定義的金鑰儲存庫，預設為 “true”。
 - 如果未選取，則會被視為「複本」金鑰儲存庫，且只會用於讀取作業。
 - 只能將一個外部金鑰儲存庫指定為主要。

KMIP Keystore

New KMIP KeyStore

Name	State	Host	Port	Client Keystore	Truststore	Is Master	Actions
<input type="text"/>	In: <input type="button" value="v"/>	<input type="text"/>	5696 <input type="button" value="v"/>	<div>Alias</div> <input type="text"/> <div>Keystore Password</div> <input type="password"/>	<div>Alias</div> <input type="text"/> <div>Truststore Password</div> <input type="password"/>	<input type="checkbox"/>	<input type="button" value="Save"/> <input type="button" value="Cancel"/>
				<div>Keystore Upload</div> <div><input type="button" value="Browse..."/> No file selected.</div> <div><input type="button" value="Upload"/></div>	<div>Truststore Upload</div> <div><input type="button" value="Browse..."/> No file selected.</div> <div><input type="button" value="Upload"/></div>		

附註

目前，MDE 支援外部金鑰儲存庫產品：為 KMIP 配置的 IBM 安全金鑰生命週期管理者 (SKLM)。

硬體安全模組 (HSM)

關於這項作業

使用 HSM 作為外部金鑰儲存庫時，您將需要根據製造商的指示確保協力廠商產品已完整配置並作業。

PPM 產品管理者必須將 HSM 的 64 位元版本用戶端軟體複製到 MDE VM。應使用 HSM 製造商的有關設定及配置通訊的產品指示，連同 SDK 選項來擷取及安裝該軟體。

會使用用戶端軟體隨附的公用程式或是經驗證使用 HSM 的公用程式來建立封套金鑰。封套金鑰是一個 256 對稱金鑰，必須可供與 PPM 搭配使用。

在 HSM 上建立了此對稱封套金鑰時，會指派一個控點給它。在 PPM GUI 頁面中配置 HSM 時將需要此控點。PPM 會將此控點和原則金鑰傳遞到 HSM 以覆蓋原則金鑰，而 HSM 將會傳回要儲存在 PPM 資料庫中的已覆蓋金鑰。

在安裝及配置軟體之後，請確保 PPM 可以與 HSM 通訊、重新啟動 PPM VM。

從「外部金鑰儲存庫」畫面中，選取「新建 HSM 金鑰儲存庫」。

Home	>	Keys	>	External Keystores
----------------------	---	----------------------	---	--------------------

HSM Keystore

[New HSM KeyStore](#)

Name	State	HSM Token	Key Handle	HSM Password	Actions
<i>No External Keystores</i>					

KMIP Keystore

[New KMIP KeyStore](#)

Name	State	Host	Port	Client Keystore	Truststore	Is Master	Actions
<i>No External Keystores</i>							

必須填寫下列設定，外部金鑰儲存庫才能處於作用中：

- **名稱** - 外部金鑰儲存庫的使用者定義參照
- **狀態** - 此設定所要的金鑰儲存庫狀態
- **HSM 記號** - HSM 使用分割區的插槽號碼
- **金鑰控點** - 這個控點會指派給將用來覆蓋原則金鑰的金鑰
- **HSM 密碼** - 這是與客戶將使用的分割區相關聯的密碼。

HSM Keystore New HSM KeyStore

Name	State	HSM Token	Key Handle	HSM Password	Actions
<input type="text"/>	Inactive ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Save"/> <input type="button" value="Cancel"/>

註：支援的 HSM 產品：為 HSM 金鑰儲存庫配置的 SafeNet® Luna HSM。

第 10 章 檔案層次原則定義

MDE 可讓安全管理者定義對各種類型資料的檔案層次控制（作業及加密）。定義檔案層次資料控制時，會使用下方的術語。

- **選取元** - 使用者和群組的無序清單，定義容許存取任何資源（或路徑集）的人員。可以選擇將定義的處理程序識別為選取元的另一個元件。
- **路徑集** - 要由原則保護之檔案路徑的清單
- **資料類型** - 指派給指定資料類型之存取定義列的有序清單。每一列都包含一個選取元、I/O（讀寫）作業及原則動作。
- **處理程序** - 執行檔的檔案路徑。在選取元中用來透過識別的執行檔定義存取控制。選用以取得更加強的存取控制。

建立資料類型之後，它可以與一或多個所供應代理程式相關聯。下列小節將說明原則的配置。

選取元

「選取元」是一個原則物件，透過一或多個選取元列定義一組使用者及 / 或使用者群組。新增選取元時，安全管理者必須在儲存之前先提供名稱。隨時可以透過編輯選取元新增選取元附註及列。

每一個選取元列都包含下列欄位：使用者、群組、處理程序。在儲存之前必須先移入其中一個欄位。

- **使用者** - 目標系統定義之使用的簡稱。這與目標代理程式作業系統中的使用者相符。此欄位是選用項。
- **群組** - 目標系統或 LDAP 定義使用者群組的簡稱。這與目標代理程式作業系統中的使用者群組相符。此欄位是選用項。
- **處理程序** - 產品定義的處理程序名稱參照。這與目標代理程式的作業系統中的處理程序檔案路徑（以及選用的雜湊值）相符。此欄位是選用項。

🏠 > Policy > Selectors

Expand All Collapse All Search Clear New Selector

Name: Save Cancel Add New Row

Notes

User	Group	Process	Actions
<input type="text" value="user01"/>	<input type="text"/>	<input type="text"/>	Delete Row

每一個選取元列中的值都使用邏輯 AND 運算進行結合。如果在單一系列中設定多個欄位，則所有欄位都必須符合要符合的列。如果所有已定義列均相符，則選取元相符。選取元內的列排序不會影響原則比對演算法。

使用者	群組	程序	代理程式比對行為
✓			比對使用者
	✓		比對已定義群組中的任何使用者
		✓	比對已定義的處理程序路徑，並可能限制為任何提供的雜湊值

✓	✓		比對使用者（前提是作為已定義群組的成員運作）
✓		✓	比對使用者（前提是透過已定義的處理程序運作）
	✓	✓	比對已定義群組中的任何使用者（前提是透過已定義的處理程序運作）
✓	✓	✓	比對使用者（前提是作為已定義群組的成員運作，並透過已定義的處理程序與處理程序運作）

附註

使用者及/或群組解析選取元會使用已安裝代理程式的已配置外部 LDAP 伺服器或 Active Directory 伺服器。

路徑集

路徑集是一個或多個未排序檔案路徑列的集合。新增路徑集時，安全管理者必須提供路徑集的名稱。若要將列新增至路徑集，請按一下「新增路徑」按鈕。每一列都包含檔案路徑及附註。

🏠 > Policy > Path Sets

Expand All Collapse All Search Enter Text Clear New Path Set

Name: Pathset1 Save Cancel Add Path

Notes

Path	Notes	Actions
/protected		Delete Path

安全管理者必須提供檔案路徑。保護會從所提供路徑向下在所有子目錄中遞迴。附註欄位是選用項。

資料類型

資料類型是資料類型列定義的有序集成，容許對資料進行檔案層次作業及/或加密存取控制。每一個資料類型都包含列的名稱、原則強制執行金鑰、使用者附註及有序清單。

- **名稱** - 使用者定義的資料類型參照
- **使用者附註** - 安全管理者定義的附註欄位。

資料類型列

每一個資料類型列都包含下列欄位：順序、選取元、作業及動作。

- **順序** - 每一個原則列的檢查優先順序。使用第一個相符列。此欄位是必要項，但是如果僅存在一列，則將不會顯示此欄位。

- **選取元** - 先前定義之選取元的選項。如果選取元中的任何列相符，則原則列將相符。這個欄位是必要項。MDE 提供將符合任何使用者的「全選」選取元。
- **作業** - 可以執行的檔案作業選項。選項為「讀取」及「讀寫」。這個欄位是必要項。
- **動作** - 與作業相關聯之存取動作的選項。選項為「允許」、「拒絕」、「允許、記載」及「拒絕、記載」。這個欄位是必要項。

資料類型列變數

「選取元」、「作業」及「動作」欄位可以選擇性地設為變數。這容許安全管理者為將在代理程式建立期間完成的資料類型建立範本。可用的欄位設定為：「可以編輯」、「必須編輯」及「不可編輯」。

可以編輯

代理程式建立期間，可以選擇性地改寫此欄位。

必須編輯

代理程式建立期間，必須設定此欄位。

不可編輯

此欄位必須在資料類型建立期間進行設定，且在代理程式建立期間無法變更。

Create/Edit Datatype

Name

Datatype1

Notes

Rules

Order	Selector	Operation	Actions	Delete
1	<div>Not Editable</div> <div>Selector1</div> <div><input type="checkbox"/> Select All</div>	<div>Not Editable</div> <div>Read or Write</div>	<div>Not Editable</div> <div>Permit</div>	<div>Delete</div>
2	<div>Not Editable</div> <div><input checked="" type="checkbox"/> Select All</div>	<div>Not Editable</div> <div>Read or Write</div>	<div>Not Editable</div> <div>Deny, Log</div>	<div>Delete</div>

Add New Row

Save

Cancel

無法儲存資料類型，直到所有列都具有值及/或變數設定為止。

處理程序

處理程序識別到執行檔的檔案系統路徑。處理程序由下列欄位組成：

- **名稱** - 處理程序的名稱
- **路徑** - 到檔案系統執行檔的絕對路徑
- **作業系統** - 用來參照作業系統類型（Linux、Windows、AIX）的欄位。
- **版本** - 用於作業系統版本的欄位。
- **發行套件** - 用於作業系統發行套件名稱（Red Hat、CentOS、Windows、AIX）的欄位。

🏠 > Policy > Processes

Expand All Collapse All Search Clear New Process

▶ Name Save Cancel Add Hash

Path	OS	Version	Distribution
<input type="text" value="/usr/bin/cat"/>	<input type="text" value="Linux"/>	<input type="text" value="6.7"/>	<input type="text" value="CentOS"/>

Hash	Actions
------	---------

處理程序可以僅定義為檔案路徑，或是定義為處理程序雜湊值的清單。當定義了一或多個雜湊值時，處理程序相符項將受限為列出的雜湊。

附註

會透過代理程式工具產生處理程序雜湊值，並應複製到 PPM 中。這套工具將會輸出執行檔現行版本的雜湊值。

spxhash -p <path to executable>

範例：

```
[root@blkdr ~]# spxhash -p /usr/bin/vim
```

```
1202E81EF41273904A6DD381C35B2561F838F7E35B6B26959F8EEB646297A36A7C2
```


第 11 章 代理程式供應及管理

MDE 支援四種類型的代理程式安裝：「磁區」、「具有原則的檔案」、「具有原則的磁區」以及「物件儲存庫」。每個代理程式類型都啟用不同的資料保護方法。

- **磁區** - 代理程式在區塊裝置層次保護資料
- **具有原則的檔案** - 代理程式在檔案層次保護資料，並提供檔案型作業存取控制原則
- **具有原則的磁區** - 代理程式在區塊裝置層次保護資料，同時提供檔案型作業存取控制原則
- **物件儲存庫** - 代理程式會保護傳送至物件儲存體的資料。

新增代理程式

若要新增代理程式，安全管理者必須導覽至 MDE 的「代理程式」頁面，然後按一下「新增代理程式」下拉清單。將會列出可用的代理程式選項。



選取代理程式類型之後，精靈會開啟，以允許您建立代理程式。

註：建議先新增所有預期的原則元件（選取元、路徑集、金鑰、資料類型及處理程序），然後再啟動「新增代理程式」處理程序，因為在處理程序期間無法建立這些元件。

用於供應代理程式的區段有六個：代理程式身分、網路資訊、原則、磁區、授權的使用者及工具。必須先完成所有必要區段，然後才能新增代理程式。

身分

「身分」區段需要安全管理者定義名稱、UUID、作業系統以及附註。

A screenshot of the 'Add File With Policy Agent' form. The form has a title bar with a close button. It is divided into two main sections: 'Required' and 'Optional'. Under 'Required', there are three fields: 'Name *', 'UUID *', and 'Operating System *'. The 'Name' field is empty. The 'UUID' field contains the value '9a5db4d2-0bd2-430b-841d-4cc122a152dd' and has a refresh button. The 'Operating System' field is a dropdown menu. Under 'Optional', there are three radio buttons: 'Policy', 'Authorized Users', and 'Tools'. There is also a 'Notes' text area. A 'Next' button is located at the bottom right of the form.

- **名稱** - 使用者定義的代理程式參照。
- **UUID** - MDE 用來識別代理程式的唯一 ID。
- **作業系統** - 目標代理程式的作業系統。
- **附註** - 此代理程式的安全管理者附註。

輸入所有必要欄位之後，按**儲存**以跳至下一步。

註：

- MDE 會自動填寫 UUID，但是安全管理者可以根據需要取代它。
- 必要欄位在 GUI 中指出
- 代理程式的名稱不是唯一的；因此，如果將同一個名稱用於多個代理程式，事件日誌訊息可能錯誤顯示訊息來源

網路

網路步驟需要安全管理者定義主機名稱以及 MDE 的主機名稱或 IP 位址，以及在 MDE 與目標代理程式之間建立安全連線需要的憑證。

- **IP 位址**- 正在安裝代理程式的伺服器的 IP 位址或主機名稱。
- **MDE 對等 IP** - 從目標代理程式伺服器實例看到的 MDE 的 IP 位址或主機名稱。

註：MDE 會自動填寫 MDE 對等 IP，但是安全管理者可以根據需要修改它。

- **憑證** - 用來在 MDE 與所安裝代理程式之間建立安全連線的已上傳憑證清單。此憑證用來在代理程式與 MDE PPM Server 之間建立交互已鑑別 TLS1.2 連線。

若要上傳憑證，安全管理者必須按一下**新增憑證**，導覽至想要的憑證並開啟它。憑證將會顯示在「新建代理程式-網路」畫面中。

註：如果金鑰儲存庫和信任儲存庫憑證未上傳至 MDE，且代理程式未獲指派相符的憑證，則代理程式和 PPM 將不會通訊，且代理程式不會加密資料及施行原則。如需相關詳細資料，請參閱「伺服器憑證設定」小節。

輸入所有必要欄位之後，按**下一步**以跳至下一步。

包含原則的檔案、包含原則的磁區及物件儲存庫建立

原則步驟需要安全管理者定義目標代理程式上檔案路徑的作業及加密控制。

新增路徑

具有原則的檔案與具有原則的磁區代理程式可以將路徑定義新增至代理程式原則。每一個新增的路徑都會保護目標代理程式上的個別檔案路徑或檔案路徑群組。新增的路徑數目是由安全管理者進行定義。

嚴重附註

- 原則套用時，透過原則保護的路徑必須存在，否則原則套用將失敗。
- 必須使用在安裝「具有原則代理程式的檔案」之後可用的 **spxconvert** 指令手動處理現有的檔案和子目錄。即使檔案未加密，原則仍會生效。
- 將透過原則自動加密並保護在安裝之後新增的新檔案和目錄。

Add File With Policy Agent

Required

☒ Agent Identity
☒ Network Information

Optional

☒ Policy
☐ Authorized Users
☐ Tools

Add Path

Back
Next

若要新增路徑，請按一下**新增路徑**。

每一個新增的路徑都需要整個檔案路徑或路徑集、索引鍵以及資料類型。

Add File With Policy Agent

Required

☒ Agent Identity
☒ Network Information

Optional

☒ Policy
☐ Authorized Users
☐ Tools

* Required

File Policy Path (or Path Set) *

Delete

Storage
☒ Local
☐ Network

Key
☐ System Defined
☒ User Defined

Name

Datatype *

(remember to fill out any empty values below)

Selector	Operation	Actions
Select All	Read or Write	Permit

Add Path

Back
Next

- **檔案原則路徑（或者路徑集）** - 識別要由所識別資料類型存取控制定義保護的路徑或路徑群組。保護會從所提供路徑至所有子目錄遞迴。
- **儲存體** - 識別檔案路徑的位置。選項為「本端」或「網路」。如果選取「網路」，則必須輸入其他參數才能適當地配置網路儲存體。（請參閱下面的配置資訊）
- **金鑰** - 用來加密與資料類型相關聯之路徑的金鑰。可以使用任何先前定義的使用者定義的金鑰或 MDE 管理的系統定義的金鑰。根據是使用具有原則的檔案還是使用具有原則的磁區，此欄位可能可見，也可能不可見（請參閱「附註」）。
- **資料類型** - 預先建立的資料類型選項。選取之後，會在行內新增資料類型資訊。如果使用具有變數的資料類型，則必須在儲存之前輸入變數。

註：

- 如果使用路徑集，則必須在新增代理程式之前予以建立。否則，可以定義單一手動路徑。
- 必須在新增代理程式之前建立所使用的資料類型。
- 如果新的代理程式是「具有原則的磁區」類型，則由於透過磁區原則定義達成保護，路徑集不會包含原則強制執行金鑰。

本端儲存體配置

如果在定義檔案原則路徑時使用本端儲存體，請選取**本端儲存體**選項。它會指引代理程式保護所定義的絕對檔案路徑（或路徑集）。不需要其他參數。

網路儲存體配置

如果在定義檔案原則路徑時使用網路儲存體，請選取「網路儲存體」選項。它會指引代理程式將定義的網路儲存體裝載至定義的絕對檔案路徑。路徑集不能搭配使用定義的網路儲存體。需要其他參數。

網路儲存體需要下列項目的定義：通訊協定、主機名稱/IP、共用、使用者名稱、密碼及進階裝載選項。

- **通訊協定** – 識別要利用之網路儲存體的類型。選項為：NFSv4、NFSv3
- **主機名稱/IP** – 網路儲存體系統的主機名稱/IP
- **共用** – 網路檔案系統匯出位置
- **使用者名稱** – （NFSv3 不需要此項）網路檔案系統的鑑別使用者名稱
- **密碼** – （NFSv3 不需要此項）網路檔案系統的鑑別密碼
- **進階裝載選項** – 要套用至 NFS 定義的選項（以逗點區隔）

輸入所有必要欄位之後，按**下一步**以跳至下一步。

磁區

新增磁區

關於這項作業

磁區及具有原則的磁區代理程式類型可以將一個或多個磁區定義新增至代理程式原則。新增的每一個磁區都是目標代理程式上新的受保護區塊裝置。

Add Volume With Policy Agent

Required

- ✓ Agent Identity
- ✓ Network Information

Optional

- Policy
- **Volumes**
- Authorized Users
- Tools

Volumes [Delete]

Device Label []

Key []

☐ Autogenerate Key Required

[Add Volume]

[Back] [Next]

若要新增磁區，請按一下**新增磁區**。每一個新增的磁區都需要輸入基礎裝置標籤及原則強制執行金鑰。

- **裝置標籤** - 識別受保護的裝置。將原則部署至代理程式之後，需要透過執行 `spxdevice` 指令將裝置標籤與磁區相關聯（請參閱安裝代理程式小節）。
- **金鑰** - 用來加密磁區的金鑰。可以使用任何先前定義的金鑰或 MDE 管理的自動產生金鑰。

嚴重附註

除非使用「自動產生金鑰」選項，否則必須在新增代理程式之前定義所新增的原則強制執行金鑰。請參閱原則強制執行金鑰管理小節。

輸入所有必要欄位之後，按**下一步**以跳至下一步。

物件儲存庫代理程式建立

MDE 物件儲存體代理程式 (OSA) 用作用戶端與後端物件儲存體之間的媒介。物件儲存體用戶端儲存區認證而不是物件儲存體認證連接到 OSA。

管理者可以配置 OSA 以連接到一個以上物件儲存體提供者。OSA 會針對透過 OSA 傳送到已配置後端物件儲存體的資料加密和實施原則。如果配置了多個後端，則會分割資料，並且會將資料片段傳送至每一個後端。

前端系統憑證

物件儲存庫代理程式需要配置憑證來在物件儲存庫用戶端與物件儲存庫代理程式之間建立安全的連線。

若要上傳憑證，安全管理者必須按一下「新增憑證」按鈕，導覽至想要的憑證並開啟它。

Add Object Store Agent

Required

☒ Agent Identity

☒ Network Information

Optional

☒ **Front-End Certificates**

☐ Bucket Credentials

☐ Buckets

☐ Backends

☐ Authorized Users

☐ Tools

Front-End Certificate

Add Certificate

Subject	CN=localhost,OU=Development,O=Security First Corp.,L=Rancho Santa Margarita,ST=California,C=US
Fingerprint	e9cf021f7092bec53ec27ba29467b2d3e70b2b2e1d5ed6acd738af363860b2bd
Expiry	2016-11-09T23:11:06Z
Private Key	False

Back

Next

輸入所有必要欄位之後，按「下一步」以跳至下一步。

儲存區認證

MDE 可配置為與多個物件儲存體提供者通訊。每一個提供者將需要配置儲存區和儲存區認證。

Add Object Store Agent

Required

✓ Agent Identity

✓ Network Information

Optional

✓ Front-End Certificates

⊙ Bucket Credentials

○ Buckets

○ Backends

○ Authorized Users

○ Tools

* Required

QHW1UOGRU90BFNYZQ0CH

Delete

Key ID *

QHW1UOGRU90BFNYZQ0CH

API Key *

78dKnlcLBiUkQgl6OLjtBKqNoglZw54S6g5SSiik5JX0wOvZ0xolIZoTa=PGKK3B

Protocol *

IBM S3

XH2BW34YV12A0REPF3TW

Delete

Key ID *

XH2BW34YV12A0REPF3TW

API Key *

3AoMJ9fXv3p1xpU8xoAqfSt=DoEaX=3iY7UOyVn3ovUAQ4ssKAbQQvAv1jmHPeXh

Protocol *

AMZ S3

New Credential

Back

Next

若要新增新的認證集，請按一下「新增認證」按鈕。

儲存區認證需要以下項目的定義：索引鍵 ID、API 金鑰和通訊協定。

- **索引鍵 ID** – 物件儲存庫識別的識別
- **API 金鑰** – 要提供給 S3 API 以與索引鍵 ID 產生關聯的字串密碼
- **通訊協定** – 用來與物件儲存體提供者（Swift、IBM S3 和 Amazon S3）通訊的通訊協定的識別。

MDE 將產生索引鍵 ID 和 API 金鑰配對。管理者可以根據需要置換這些產生的值。管理者需要從支援的物件儲存體提供者中選取所需的通訊協定。

輸入所有必要欄位之後，按「下一步」以跳至下一步。

儲存區

MDE 透過關聯儲存區來定義物件儲存體原則。每一個儲存區都需要以下項目的定義：名稱、日誌詳細資料和原則。

Add Object Store Agent

Required

- ✓ Agent Identity
- ✓ Network Information

* Required

Bucket Name *

Delete

Optional

- ✓ Front-End Certificates
- ✓ Bucket Credentials
- ⊙ **Buckets**
 - Backends
 - Authorized Users
 - Tools

Log Denials

☒

Policy

Key ID *	Access *	Log	Actions
<input type="text" value="XH2BW34YV12A0REPF3TW"/>	<div>Read or Write ▾</div>	<input checked="" type="checkbox"/>	<div>Delete</div>
<input type="text" value="QHW1UOGRU90BFNYZQ0CH"/>	<div>Read or Write ▾</div>	<input checked="" type="checkbox"/>	<div>Delete</div>
<div>New Row</div>			

New Bucket

Back

Next

- **名稱** – 物件儲存體儲存區的名稱
 - **日誌詳細資料** – 一個勾選框選項。如果勾選，物件儲存庫代理程式將建立審核日誌以存取詳細資料。
 - **原則** – 儲存區存取控制的定義。原則可以包含多列。原則定義的每一個列都需要：索引鍵 ID、存取權限和日誌。
 - **索引鍵 ID** – 預先建立的儲存區認證索引鍵 ID 的項目。
 - **存取權限** – 包含下列選項：讀取或寫入、讀取或寫入存取專用權。
 - **日誌** – 一個勾選框選項。如果勾選，物件儲存庫代理程式將針對所提供列行為的存取允許的審核日誌。
- 輸入所有必要欄位之後，按「下一步」以跳至下一步。

後端

後端連線資訊透過 M:N 選項定義。此選項定義物件儲存體資料的備用和安全。N 表示要配置或「共用」的後端物件儲存體提供者數目。M 表示重新建構資料所需的共用數目。受支援的配置是 1:1、2:3、2:4。

Add Object Store Agent

Required

✓ Agent Identity

✓ Network Information

Optional

✓ Front-End Certificates

✓ Bucket Credentials

✓ Buckets

⊙ Backends

○ Authorized Users

○ Tools

M:N 2:3

* Required

Share 1 *

URL *

ID *

Key *

Protocol *

IBM S3

Share 2 *

URL *

ID *

Key *

Protocol *

IBM S3

Share 3 *

URL *

ID *

Key *

Protocol *

IBM S3

Back

Next

每一個共用都需要配置以下項目：URL、ID、金鑰和通訊協定。

- **URL** – 物件儲存體提供者的存取 URL
- **ID** – 用於存取物件儲存體提供者的帳戶使用者 ID。
- **金鑰** – 用於存取物件儲存體提供者的使用者 ID 帳戶金鑰。
- **通訊協定** – 用來與物件儲存體提供者（Swift、IBM S3 和 Amazon S3）通訊的通訊協定的識別。

輸入所有必要欄位之後，按「下一步」以跳至下一步。

授權使用者

使用者步驟需要安全管理者定義 MDE 使用者帳戶，該帳戶有權下載代理程式安裝軟體組。

如果使用者未被列為授權使用者，且該使用者登入並檢視代理程式，則該使用者不會在「代理程式資訊」頁面中看到下載鏈結。

輸入所有必要欄位之後，按下一步以跳至下一步。

代理程式工具

代理程式支援用於輔助以加密形式傳送資料的特殊化工具。有兩種類型的工具：備份/還原以及物件儲存庫。

工具是在代理程式供應期間或在「代理程式資訊」頁面上配置的。「備份/還原」工具用於備份及還原已加密資料。它利用關聯的金鑰來備份已加密資料，並提供在以後還原已加密資料的功能，即使原則金鑰已旋轉也不例外。備份/還原工具是選用項目，不需要用來將工具關聯至代理程式。「物件儲存庫」工具是物件儲存庫代理程式的必要項目

代理程式工具矩陣

工具可用性基於代理程式類型並透過關聯鍵進行啟用。依代理程式類型的工具矩陣如下所示：

工具類型	磁區	具有原則的磁區	具有原則的檔案	物件儲存庫
備份/還原	✓	✓	✓	
物件儲存庫				✓

工具鍵關聯

若要將鍵與工具關聯，請先開始在所要工具旁邊的文字框中鍵入先前定義的鍵名稱，然後從清單中選取適當的鍵。

按一下**儲存**，將會建立工作。核准之後，將會在代理程式上啟用已配置的工具。

註：工具不支援自動產生的鍵。必須先建立代理程式才能定義鍵。

輸入所有必要欄位之後，按下一步以跳至下一步。

檢閱及建置

關於這項作業

所有供應步驟均已完成後，系統會讓使用者導航到「檢閱」畫面。

供應設定的檢閱頁面將顯示包含所有配置資訊的完整視圖。

Add File With Policy Agent

Agent Build Summary

Identity

Name

fileAgent

UUID

c5bf0b5a-99b2-4dcc-8e82-2a559d5319c4

Type

File with Policy

Operating System

CentOS / Red Hat 7

Notes

Network

Back

Build

檢閱內容的完整性與正確性，然後按一下**建置**以完成供應程序。將會建立工作來新增代理程式。

工作核准時，將建立代理程式，安裝套件將可用於下載及安裝。

代理程式啟動

代理程式建置工作核准時，新建立的代理程式在 MDE 中將處於作用中。安裝代理程式之後，它將使用配置的 MDE 對等 IP 及提供的憑證，以建立與 MDE 的相互鑑別 TLS1.2 連線。

代理程式將在起始安裝及後續啟動時要求原則。MDE 將使用已配置的原則配置來回應。收到原則之後，將在代理程式上施行原則。

檢視代理程式

關於這項作業

「代理程式」頁面將顯示所建立代理程式的摘要清單。

Agents

Agent Report

Search

Enter Text

Clear

Add Agent

Name	Hostname or IP	Type	Notes	Actions
Agent1	1.1.1.1	Volume with Policy		<div>DetailsDelete Agent</div>

若要查看任何特定代理程式的詳細資料，請按一下「名稱」直欄中的代理程式名稱，或按一下「動作」直欄中的「詳細資料」按鈕。這將開啟代理程式詳細視圖頁面，其中會顯示供應資訊、安裝軟體組下載及其他有用資訊。

代理程式報告

MDE 安全管理者可以建立代理程式報告。此報告包含下列資訊：代理程式總數、依類型和作業系統的代理程式計數，以及自報告產生之日起 30 天內登入的代理程式數。日期基於 PPM 時間，這是世界標準時間。資料將按代理程式類型分類。

安裝代理程式

關於這項作業

供應步驟已將代理程式安裝及部署原則所需要的所有資訊配置到目標伺服器實例。若要安裝代理程式，請下載安裝套件，將它複製到目標系統，解壓縮內容，然後執行安裝 Script。

Agents > Agent1

Agent Info

Edit Agent Info

Identity

Notes

Name

Agent1

UUID

dab30682-19ee-4763-84d8-12fe2ba91948

IP Address

1.1.1.1

Type

Volume with Policy

Operating System

CentOS / Red Hat 7

Network

MDE Peer IP

1.1.1.0

Certificates

Subject	Fingerprint	Expiry
CN=agent,OU=agent,O=SFC,L=RSM,ST=California,C=US	ea584e4904fffa45a3416eccc753e0f0f655462929d4f1534f369cbccc38165f	2016-11

No file selected.

Users

Download Tokens

Authorized Users

admin

Install Files Download URL

/rest/agents/1/install_bundle

Download Zip Bundle

Download Tar Bundle

ID	State
<input type="button" value="Add Token"/>	

嚴重附註

確保在代理程式系統中建立、連接及配置供應原則中識別的所有使用者、群組及路徑或裝置。

針對 Linux 安裝代理程式

有 4 種代理程式類型：「磁區」代理程式、「具有原則的檔案」代理程式、「具有原則的磁區」代理程式及「物件儲存庫」代理程式。使用代理程式供應期間所指定的代理程式類型。

Linux 磁區代理程式裝置配置

關於這項作業

程序

1. 在 PPM 中建立磁區（請記住在 11.1.5 節中所用的裝置標籤）。
2. 在代理程式 VM 上安裝“gettext”套件。
3. 安裝代理程式 – 如需詳細資料，請參閱第 77 頁的『[附錄 A 範例代理程式安裝程序](#)』。
4. 安裝完成時，重新啟動代理程式 VM。
5. 以 root 身分，執行 `spxdevice -e <label given in PPM> -m <mount point> -f <file system> -u <disk to use>`

```
spxdevice -e COS6VOL -m /protected -f ext4 -u /dev/sdb
```

Linux 具有原則代理程式的檔案裝置配置

關於這項作業

程序

1. 在 PPM 中建立具有原則的檔案代理程式
2. 建立任何需要的使用者
3. 建立任何需要的子目錄
4. 在目錄上設定適當的許可權
5. 在代理程式 VM 上安裝“gettext”套件
6. 安裝代理程式 – 如需詳細資料，請參閱第 77 頁的『[附錄 A 範例代理程式安裝程序](#)』。
7. 安裝完成時，重新啟動代理程式 VM
8. 透過指令“`spxinfo -l`”驗證檔案原則是否正確

附註

路徑旁邊的星號表示有正在加密擱置中的預先存在資料。為了要對預先存在的目錄結構和資料執行就地加密，以及隨時判定資料的狀態，MDE 提供一個稱為“`spxconvert`”的指令行公用程式。請參閱第 89 頁的『[附錄 E 就地加密](#)』以取得指令及其用法的詳細說明及其用法。

Linux 具有原則代理程式的磁區裝置配置

關於這項作業

程序

1. 在 PPM 中建立具有原則代理程式的磁區（請記住使用的裝置標籤）
2. 在代理程式 VM 上安裝“gettext”套件
3. 安裝代理程式 – 如需詳細資料，請參閱第 77 頁的『[附錄 A 範例代理程式安裝程序](#)』。
4. 安裝完成時，重新啟動代理程式 VM
5. 以 root 身分，執行 `spxdevice -e <label given in PPM> -m <mount point> -f <file system> -u <disk to use>`

```
[root@localhost]# spxdevice -e COS6VOL -m /protected -f ext4 -u /dev/sdb
```

6. 建立任何需要的子目錄和使用者
7. 在目錄上設定適當的許可權
8. 重新啟動代理程式 VM
9. `lsblk` – 用來驗證磁碟是否存在 - 有時可能會花費 ~30 秒
10. 透過指令“`spxinfo -l`”驗證檔案原則是否正確

附註

在 Linux 中，可以在完整裝置或分割區上設定磁區加密。如果要使用單一分割區，只要在使用 `spxdevice -u` 選項時指定空分割區（例如 `/dev/sdb1`）即可。

Linux 物件儲存庫代理程式配置

關於這項作業

程序

1. 在 PPM 中建立物件儲存庫代理程式
2. 安裝代理程式 – 如需詳細資料，請參閱第 77 頁的『[附錄 A 範例代理程式安裝程序](#)』
3. 安裝完成時，重新啟動代理程式 VM

針對 AIX 安裝代理程式

AIX 支援單一代理程式類型：具有原則的檔案代理程式。使用代理程式供應期間所指定的代理程式類型。

AIX 具有原則的檔案代理程式裝置配置

1. 在 PPM 中建立具有原則的檔案代理程式
2. 建立任何需要的使用者
3. 建立任何需要的子目錄
4. 在目錄上設定適當的許可權
5. 安裝代理程式 – 如需詳細資料，請參閱第 77 頁的『[附錄 A 範例代理程式安裝程序](#)』
6. 安裝完成時，重新啟動代理程式 VM
7. 透過指令 “`spxinfo -l`” 驗證檔案原則是否正確

註：路徑旁邊的星號表示有正在加密擱置中的預先存在資料。為了要對預先存在的目錄結構和資料執行就地加密，以及隨時判定資料的狀態，MDE 提供一個稱為 “`spxconvert`” 的指令行公用程式

請參閱第 89 頁的『[附錄 E 就地加密](#)』以取得指令及其用法的詳細說明及其用法。

針對 Windows 安裝代理程式

有 3 種代理程式類型：「磁區」代理程式、「具有原則的檔案」代理程式及「具有原則的磁區」代理程式。使用代理程式供應期間所指定的代理程式類型。

Windows 磁區代理程式裝置配置

關於這項作業

程序

1. 在 PPM 中建立磁區（請記住使用的裝置標籤）。
2. 安裝代理程式 – 如需詳細資料，請參閱第 77 頁的『[附錄 A 範例代理程式安裝程序](#)』
3. 安裝完成時，重新啟動代理程式 VM
4. 執行 “`spxdevice -e <label given at PPM> -d <disk number to use>`” 以連接至整個磁碟。必須以管理者身分執行。

```
spxdevice -e PRODISK -d 1
```

5. 或執行 `spxdevice -e <label given at PPM> -d <disk number to use> -m <drive letter> -f <file system>` 以連接至將以磁碟機代號格式化並裝載的整個磁碟。

```
spxdevice -e PRODISK -d 1 -m E -f NTFS
```

6. 或者，執行 “spxdevice -i <disk number to use>” 來暫置磁碟以連接至特定的分割區

```
spxdevice -i 1
```

7. 接下來執行 “spxdevice -e <label given at PPM> -v <drive letter> -f <filesystem>” 以連接至特定的分割區並以檔案系統格式化分割區

```
spxdevice -e PRODISK -v E -f NTFS
```

註：在 Windows 中，可以在完整裝置或分割區上設定磁區加密。

- 如果是整個磁碟加密，磁碟必須在線上並已起始設定，且絕不可格式化磁碟空間。磁碟機代號必須可用。
- 如果是分割區加密，必須在全新磁碟上透過 “spxdevice -i <disk number>” 建立支援裝置。然後，必須建立具有磁碟機代號的原始分割區。

如需其他選項，請參閱 "spxdevice" 指令中的說明。

Windows 具有原則代理程式的檔案裝置配置

關於這項作業

程序

1. 在 PPM 中建立具有原則的檔案代理程式
2. 建立任何需要的使用者
3. 建立任何需要的子目錄
4. 在目錄上設定適當的許可權
5. 安裝代理程式 – 如需詳細資料，請參閱第 77 頁的『[附錄 A 範例代理程式安裝程序](#)』
6. 透過指令驗證檔案原則是否正確：spxinfo -l

附註

路徑旁邊的星號表示有正在加密擱置中的預先存在資料。為了要對預先存在的目錄結構和資料執行就地加密，以及隨時判定資料的狀態，MDE 提供一個稱為 “spxconvert” 的指令行公用程式
請參閱第 89 頁的『[附錄 E 就地加密](#)』以取得指令及其用法的詳細說明及其用法。

附註

在 Windows 上，確定管理使用者獲允許透過原則建立目標目錄，因為在擷取原則後，該原則就會生效。

Windows 具有原則代理程式的磁區裝置配置

關於這項作業

程序

1. 在 PPM 中建立具有原則代理程式的磁區（請記住使用的裝置標籤）
2. 安裝代理程式 – 如需詳細資料，請參閱第 77 頁的『[附錄 A 範例代理程式安裝程序](#)』
3. 安裝完成時，重新啟動代理程式 VM
4. 執行 "spxdevice -e <label given at PPM> -d <disk number to use>" 以連接至整個磁碟。必須以管理者身分執行。

PS C:\> spxdevice -e PRODISK -d 1

5. 或執行 "spxdevice -e <label given at PPM> -d <disk number to use> -m <drive letter> -f <file system>" 以連接至將以磁碟機代號格式化並裝載的整個磁碟

PS C:\> spxdevice -e PRODISK -d 1 -m E -f NTFS

6. 或者，執行 “spxdevice -I <disk number to use>” 來暫置磁碟以連接至特定的分割區。

PS C:\> spxdevice -i 1

7. 接下來執行 "spxdevice -e <label given at PPM> -v <drive letter> -f <filesystem>" 以連接至特定的分割區並以檔案系統格式化分割區。

PS C:\> spxdevice -e PRODISK -v E -f NTFS

附註

在 Windows 中，可以在完整裝置或分割區上設定磁區加密。

- 如果是整個磁碟加密，磁碟必須在線上並已起始設定，且絕不可格式化磁碟空間。磁碟機代號必須可用。
- 如果是分割區加密，必須在全新磁碟上透過 “spxdevice -i <disk number>” 建立支援裝置。然後，必須建立具有磁碟機代號的原始分割區。

如需其他選項，請參閱 “spxdevice” 指令中的說明。

8. 將受保護的目錄新增至磁區
9. 重新啟動電腦
10. spxinfo -l（應該顯示所有受保護目錄的清單）

附註

在 Windows 上，確定管理使用者獲允許透過原則建立目標目錄，因為在連接磁區且可用後，該原則就會生效。

作用中的原則

每一個代理程式只能具有一個作用中的原則。代理程式不會以持續性方法儲存其原則。代理程式每次重新啟動時，代理程式都會從 MDE 要求目前作用中的原則。如果代理程式無法存取 MDE，則預設拒絕存取權將適用於代理程式上的所有受保護目錄。

將新的原則傳送至代理程式時，如果成功（或未成功）套用原則，則代理程式會將事件傳送至 MDE。如果原則啟動問題持續存在，請參閱以下位置中的 policy_kernel.log 檔：

- Linux/AIX：/var/log/spxagent/spx-policyagent
- Windows：C:\Windows\spxagent\PolicyAgent

編輯代理程式

順利供應及核准代理程式之後，對該代理程式所做的任何變更都必須在「代理程式資訊」頁面上透過 GUI 編輯代理程式來完成。若要編輯代理程式，請檢視代理程式詳細資料。在「代理程式資訊」頁面上，可以獨立編輯代理程式的各區段。

編輯代理程式資訊

按一下「編輯代理程式資訊」按鈕，將容許修改部分代理程式資訊：名稱、IP 位址、MDE 對等 IP 及附註。

Agent Info

[Edit Agent Info](#)

Identity

Notes

Name Agent1
UUID dab30682-19ee-4763-84d8-12fe2ba91948
IP Address 10.6.1.255
Type Volume with Policy
Operating System CentOS / Red Hat 7

Network

MDE Peer IP 10.6.1.105

Certificates

Subject	Fingerprint	Expir
CN=agent,OU=agent,O=SFC,L=RSM,ST=California,C=US	ea584e4904fffa45a3416ecc753e0f0f655462929d4f1534f369cbccc38165f	2016-

[Browse...](#) No file selected.

MDE 對等 IP 的變更將立即反映在 MDE 內，但是如果已安裝代理程式，則必須先建立及安裝新的安裝套件，然後變更才會生效。

附註

起始供應之後，UUID、作業系統及代理程式類型不可編輯。

新增/刪除憑證

可以透過按一下「代理程式資訊」頁面憑證區段中的適當按鈕，新增及刪除代理程式憑證。

Network

MDE Peer IP 1.1.1.0

Certificates

Subject	Fingerprint	Expiry	
CN=agent,OU=agent,O=SFC,L=RSM,ST=California,C=US	ea584e4904fffa45a3416ecc753e0f0f655462929d4f1534f369cbccc38165f	2016-11-15T14:32:08Z	Delete Certificate

[Browse...](#) No file selected.

[Add Certificate](#)

若要更新代理程式憑證，請遵循下列步驟：

1. 為代理程式產生新憑證
2. 透過管理主控台將新憑證上傳至 PPM
 - a. 從「代理程式」頁面，按一下要更新的代理程式以顯示「代理程式資訊」頁面
 - b. 按一下「新增憑證」按鈕，選取新憑證檔並按一下「確定」按鈕
 - c. 應該會顯示新憑證
3. 刪除舊憑證
 - a. 從「代理程式」頁面，按一下要更新的代理程式以顯示「代理程式資訊」頁面
 - b. 確定要刪除的憑證
 - c. 按一下「刪除憑證」按鈕，將會建立工作
 - d. 按一下「跳出」按鈕

- e. 從「工作」頁面，對所要工作按一下「核准」按鈕
4. 驗證憑證是否已從代理程式中刪除
 - a. 從「代理程式」頁面，按一下要更新的代理程式以顯示「代理程式資訊」頁面
 - b. 驗證是否保留了適當的憑證

如果已安裝代理程式，則必須先建立及安裝新的安裝套件，然後憑證變更才會生效。

代理程式工具

現在，可以在「代理程式資訊」頁面上新增未在代理程式供應期間配置的工具。此外，還可以修改已配置的工具。

關聯鍵

若要關聯鍵，請在工具旁邊的文字框中鍵入鍵名稱，然後從清單中選取鍵。按一下「儲存」，將會建立工作。核准之後，將會在代理程式上啟用已配置的工具。

修改鍵

若要修改鍵，請按一下編輯按鈕，在工具旁邊的文字框中鍵入鍵名稱，然後從清單中選取鍵。

按一下「儲存」，將會建立工作。核准之後，將會在代理程式上啟用已配置的工具。

Tools

SU 資料存取

套用原則存取控制時，預設值是拒絕 SU 資料存取。可能會有容許 SU 資料存取的情況。如果有，則在「代理程式資訊」頁面上會有一個勾選框可容許修改設定。

切換勾選框將會建立工作。核准之後，將會相應地變更 SU 資料存取設定。

下表顯示 SU 資料存取控制：

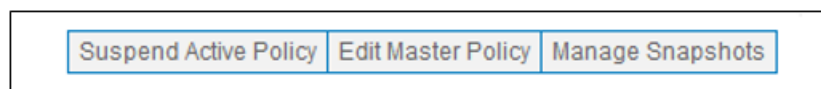
代理程式類型	作業系統	SU 資料存取預設值	SU 資料存取可配置
磁區	CentOS6/RedHat6	不適用	不適用

磁區	CentOS7/RedHat7	不適用	不適用
磁區	Windows	不適用	不適用
具有原則的磁區	CentOS6/RedHat6	封鎖	是
具有原則的磁區	CentOS7/RedHat7	封鎖	是
具有原則的磁區	Windows	不適用	不適用
具有原則的檔案	CentOS6/RedHat6	封鎖	是
具有原則的檔案	CentOS7/RedHat7	封鎖	是
具有原則的檔案	AIX	封鎖	是
具有原則的檔案	Windows	不適用	不適用
物件儲存庫	CentOS7/RedHat7	不適用	不適用

暫停原則

「具有原則的磁區」及「具有原則的檔案」代理程式支援暫停已定義作用中原則的能力。暫停原則時，將會拒絕針對受保護目錄的所有動作。暫停作用中原則時，可以不必變更作用中的 Snapshot 定義。

若要暫停原則，請按一下「代理程式資訊」原則區段右上角中的「暫停作用中原則」按鈕，將會建立一個工作。



核准工作之後，原則將會立即暫停，並且按鈕將會切換為顯示「重新啟用作用中原則」。

若要重新啟用已暫停的原則，請按一下「重新啟用作用中原則」按鈕，將會建立一個工作。核准工作之後，前次作用中的 Snapshot 原則將會立即生效。

原則變更

可以透過修改套用至受保護路徑的原則、新增受保護的路徑，或者新增已加密的磁區，從而進行原則變更。

對原則的變更不會修改現行資料的加密狀態。重新部署原則之後，它們將僅影響所建立資料的處理。

嚴重附註

不要從作用中代理程式刪除磁區原則。這麼做不受支援，並可能使目標系統處於不一致狀態。

您可以在作用中代理程式上建立新的磁區，並將舊磁區保留為未使用。

此外，您可以建立及部署新的代理程式。

編輯原則

編輯代理程式的原則，容許修改檔案原則路徑、路徑集與資料類型關聯，或者加密的磁區。

如果資料類型變更為可以編輯的項，則那些欄位的行內編輯將可用。若要編輯原則，請按一下「編輯主要原則」按鈕。

File Policy Path Pathset1		
Datatype	Datatype1	
Selector	Operation	Actions
Selector1	Read or Write	Permit
Select All	Read or Write	Deny, Log

Protected Volumes

Volume Policy Path	
Device Label	volume
Key	Key1

圖 1. 具有原則的磁區代理程式範例

這將啟動「編輯主要原則」頁面。

Edit Master Policy

File Policy Path (or Path Set) Pathset1		
<input type="checkbox"/> Autogenerate Key		
Datatype	Datatype1	
(remember to fill out any empty values below)		
Selector	Operation	Actions
Selector1	Read or Write	Permit
Select All	Read or Write	Deny, Log

Volume Policy Path	
Device Label	volume
Key	Key1
<input type="checkbox"/> Autogenerate Key	

[Add Volume](#)
[Add Path](#)

[Save](#)
[Save and Snapshot](#)
[Save, Snapshot and Activate](#)
[Cancel](#)

附註

「編輯主要原則」不會修改任何 Snapshot。

新增路徑

關於這項作業

若要將新的路徑新增至原則下的位置，請按一下「新增路徑」按鈕。

Edit Master Policy

File Policy Path (or Path Set)

Pathset1

☐ Autogenerate Key

Datatype

Datatype1

(remember to fill out any empty values below)

Selector	Operation	Actions
Selector1	Read or Write	Permit
Select All	Read or Write	Deny, Log

Volume Policy Path

Device Label

volume

Key

Key1

☐ Autogenerate Key

Add Volume

Add Path

這將開啟新的區段以供原則輸入（類似於原始供應）。

File Policy Path (or Path Set)

Type policy path or select a predefined path

Required

Delete

☐ Autogenerate Key

Datatype

Type to filter and select a predefined datatype

Required

(remember to fill out any empty values below)

Selector	Operation	Actions
----------	-----------	---------

Add Volume

Add Path

Save

Save and Snapshot

Save, Snapshot and Activate

Cancel

新增磁區

關於這項作業

若要新增磁區以加密，請按一下「新增磁區」按鈕。

Edit Master Policy

File Policy Path (or Path Set) **Pathset1**

☐ Autogenerate Key

Datatype


(remember to fill out any empty values below)

Selector	Operation	Actions
Selector1	Read or Write	Permit
Select All	Read or Write	Deny, Log

Volume Policy Path

Device Label

Key ☐ Autogenerate Key



這將開啟新的區段以供輸入（類似於原始供應）。

Volume Policy Path

Device Label **Required**

Key ☐ Autogenerate Key **Required**

刪除路徑

關於這項作業

如果要從原則保護刪除路徑，請針對想要的路徑按一下「刪除」按鈕。在已儲存、建立其 Snapshot 及啟動原則配置後，該路徑將不再受存取控制原則保護。將不再加密寫入目錄中的新檔案。現有的檔案將保持處於已加密狀態，並且將無法存取。

註：若要確保不中斷對資料的存取，請在從原則中刪除路徑之前，將資料複製/移動出受保護的目錄路徑。

Edit Master Policy

File Policy Path (or Path Set)

Pathset1

Delete

☐ Autogenerate Key

Datatype

Datatype1

(remember to fill out any empty values below)

Selector	Operation	Actions
selector1	Read or Write	Permit

Volume Policy Path

Device Label

volume

Key

Key01

☐ Autogenerate Key

Add Volume

Add Path

Save

Save and Snapshot

Save, Snapshot and Activate

Cancel

代理程式 Snapshot

代理程式 Snapshot 是代理程式相關聯原則配置的永久儲存體。Snapshot 已編製索引，且狀態為作用中或非作用中。每個代理程式只有一個作用中 Snapshot。這是目前已套用至代理程式的原則配置。若要修改代理程式原則配置，管理者必須建立新的 Snapshot，以反映想要的變更並啟動新的 Snapshot。

儲存代理程式編輯及 Snapshot

完成編輯代理程式原則後，您可以取消變更，儲存變更，儲存及 Snapshot 變更，或者儲存、Snapshot 及啟動變更。

Save

Save and Snapshot

Save, Snapshot and Activate

Cancel

取消變更

取消變更將回復為修改之前已存在的原則配置。

儲存變更

儲存變更將會儲存變更以供未來使用，但是不會建立 Snapshot，因此變更不會套用至代理程式。

儲存並建立 Snapshot

儲存變更並建立變更 Snapshot 將會儲存變更以供未來使用，並且會建立可在稍後檢視及啟動的 Snapshot。

儲存、建立 Snapshot 及啟動

儲存變更、建立變更 Snapshot 及啟動變更將會儲存變更以供未來使用，並且會建立可以檢視的 Snapshot，以及立即建立工作以將這些變更套用至代理程式。

註：在代理程式能夠與 PPM 伺服器通訊之後，任何 Snapshot 變更或更新項目才會生效。所建立的工作將一直保持執行中，直到 PPM 與代理程式之間的通訊順利進行或從 PPM 伺服器中移除代理程式為止。

管理 Snapshot

與代理程式相關聯的所有 Snapshot 都可以透過「代理程式資訊」視圖上的「管理 Snapshot」按鈕進行檢視。

Active Policy

Edit Master PolicyManage Snapshots

File Policy PathPathset1

DatatypeDatatype1

Selector	Operation	Actions
Selector1	Read or Write	Permit
Select All	Read or Write	Deny, Log

按一下按鈕將啟動 Snapshot 管理對話框。從這裡，安全管理者可以檢視 Snapshot 詳細資料、啟動 Snapshot、停用與 Snapshot 相關聯的原則及刪除 Snapshot。

Agent Snapshots

ID	State	Actions
1	Inactive	ActivateDeleteView Details
2	Active	Deactivate PolicyView Details

OK

附註

變更作用中的 Snapshot 不會修改主要原則。

檢視詳細資料

此按鈕會啟動與 Snapshot 相關聯之原則的摘要視圖。

Agent Snapshots

Snapshot Detail

Notes

Protection Policy

File Policy Path/protected2

DatatypeDatatype1

Selector	Operation	Key	Actions
----------	-----------	-----	---------

Back

OK

啟動 Snapshot

啟動 Snapshot 會建立工作，以將原則傳送至代理程式。核准之後，Snapshot 將轉移至作用中狀態，且其原則將改寫代理程式上呈現的所有原則。

註：在代理程式能夠與 PPM 伺服器通訊之後，任何 Snapshot 變更或更新項目才會生效。所建立的工作將一直保持執行中，直到 PPM 與代理程式之間的通訊順利進行或從 PPM 伺服器中移除代理程式為止。

刪除 Snapshot

可以刪除非作用中 Snapshot。刪除 Snapshot 會將它永久地從 MDE 中移除。

解除安裝檔案代理程式

關於這項作業

如果您想要移除檔案代理程式，可以透過下列步驟達到此目的：

從受保護目錄複製出資料。這將確保在取消啟動原則之後，資料無法存取。

執行下列步驟以移除代理程式軟體：

程序

1. Linux – 以 root 身分執行

a) 停止 spx-policyagent 服務

· 使用 CentOS 7 執行

```
systemctl stop spx-policyagent
```

· 使用 CentOS 執行

```
service spx-policyagent stop
```

b) 執行 `cd /opt/ibm/mde/spxagent/spx-fileagent/`。

c) 執行 `./fileagent_uninstall.sh`。

d) 鍵入 y 以確認破壞性動作。

e) 重新開機。

2. AIX – 以 root 身分執行

a) 停止 spx-policyagent 服務。

```
stopsrc -s spx-policyagent
```

b) 停止核心模組。

```
/opt/ibm/mde/spxagent/spx-fileagent/module/spx_kctrl_stop
```

c) 移除 RPM。

```
rpm -e fileagent*
```

註：如果您需要確切的 rpm 名稱而不是萬用字元執行，請確切的

```
rpm -qa | grep fileagent
```

d) 重新開機。

3. Windows – 以管理者身分執行

· 透過 Windows GUI

– 導覽至控制台中的新增/移除程式

- 選取 “FileAgent” 進行解除安裝
- 當系統提示時，重新啟動系統
- 透過 PowerShell CLI
 - msixexec /x <path to FileAgent.msi>
 - 當系統提示時，重新啟動系統

重要：授權的使用者不得使用 mv (move) 指令，從已加密位置移動資料或將資料移至其中，因為這可能會建立 MDE 原則的問題。

首先透過對受保護（已加密）目錄使用 cp (copy) 指令來備份資料。

解除安裝磁區代理程式

解除安裝磁區代理程式

- Linux – 以 root 身分執行。

1. 解除裝載受保護的磁區

```
umount /dev/mapper/<e_volume>
```

2. 停止 spx-policyagent 服務

- 使用 CentOS 7 執行

```
systemctl stop spx-policyagent
```

- 使用 CentOS 執行

```
service spx-policyagent stop
```

3. 執行 cd /opt/ibm/mde/spxagent/spx-volumeagent/。

4. 執行 ./volumeagent_uninstall.sh。

5. 鍵入 y 以確認破壞性動作。

6. 重新開機

- Windows – 以管理者身分執行

- 透過 Windows GUI

- 導覽至控制台中的新增/移除程式
- 選取 VolumeAgent 以解除安裝
- 當系統提示時，重新啟動系統

- 透過 PowerShell CLI

- msixexec/x <VolumeAgent.msi 的路徑>
- 當系統提示時，重新啟動系統

解除安裝具有原則的磁區代理程式

關於這項作業

程序

1. Linux – 以 root 身分執行

a) 卸載受保護目錄

```
umount /dev/mapper/<e_volume>
```

b) 停止 spx-policyagent 服務

- 使用 CentOS 7 執行

```
systemctl stop spx-policyagent
```

- 使用 CentOS 執行

```
service spx-policyagent stop
```

c) 執行 `cd /opt/ibm/mde/spxagent/spx-hybridagent/`。

d) 執行 `./hybridagent_uninstall.sh`。

e) 鍵入 `y`，以確認破壞性動作。

f) 重新開機。

2. Windows – 以管理者身分執行

- 透過 Windows GUI
 - 導覽至控制台中的新增/移除程式。
 - 選取 "HybridAgent" 進行解除安裝。
 - 當系統提示時，重新啟動系統。
- 透過 PowerShell CLI
 - 執行 `msiexec /x <path to HybridAgent/msi>`。
 - 當系統提示時，重新啟動系統。

解除安裝物件儲存庫代理程式

關於這項作業

除非從 PPM 中刪除代理程式，否則所有使用者帳戶及許可權都將保持儲存在 PPM 中。

程序

1. Linux – 以 root 身分執行
2. 停止 spx-policyagent 服務

```
systemctl stop spx
```

3. `cd /opt/ibm/mde/spxagent/spx-objectagent`

```
./objectagent_uninstall.sh
```

4. 鍵入 `y`，以確認破壞性動作
5. 重新開機。

從 MDE 中移除代理程式

可以從生態系統中使用 MDE 使用者介面 (GUI) 移除由 MDE 管理的代理程式。

要移除代理程式，請按一下「移除代理程式」按鈕，將會建立工作。工作得到核准之後，將會從 MDE 中移除代理程式。

Name	Hostname or IP	Type	Notes	Actions
Agent1	1.1.1.1	Volume with Policy		Details Delete Agent

嚴重附註

- 從 MDE 中移除代理程式將讓代理程式無法連接至 MDE，導致目前受保護的資料在下一代理程式重新啟動時變得無法存取。
- 移除代理程式不會解密資料。

代理程式公用程式

MDE 代理程式提供多個公用程式來幫助配置代理程式以及保護機密性資訊。如需每一個公用程式的更多詳細資料，請使用 "--help" 選項執行公用程式。

公用程式	功能	磁區	具有原則的磁區	具有原則的檔案	物件儲存庫
spxbackup	建立已識別資料的已加密備份。	是	是	是	否
spxconvert	根據已定義的原則，將受保護的目錄中預先存在的資料從未加密轉換為已加密。	否	否	是	否
spxdevice	將磁碟區/分割區對映至已定義的裝置名稱。	是	是	否	否
spxhash	產生所指出處理程序的特定版本專用的雜湊。	否	是	是	否
spximport	將已加密的資料匯入到目錄中，而不雙重加密該資料。	否	否	是 (僅限 Windows)	否
spxinfo	列出透過已定義的原則保護的目錄	否	是	是	否
spxobject	列出物件儲存庫	否	否	否	是
spxrestore	還原已識別資料的已加密備份。	是	是	是	否

第 12 章 作業

產品資料備份及還原

MDE 支援對 MDE PPM 資料進行復原點備份的能力。這個復原點備份可以還原，以讓 MDE 回到備份收集時的狀態。

註：在執行備份或還原之前，請透過 MDE VM 中的 "systemctl stop spsd" 指令停止 MDE 服務。

```
sudo systemctl stop spsd
```

產品資料備份

關於這項作業

產品備份是透過在 MDE VM 內執行的指令行 Script 完成。

備份 Script spsd-backup 位於 MDE VM 中的 /opt/securityfirst/spsd/bin 目錄內。它會自動建立新檔案，並以完成此備份時的時間戳記命名它。

```
sudo /opt/securityfirst/spsd/bin/spsd-backup --help
用法：spsd-backup [--nodb] [--help]
-----
--nodb 不要備份資料庫
--help 顯示此說明
```

若要執行備份：

```
sudo /opt/securityfirst/spsd/bin/spsd-backup
傾出本端建置資訊
傾出本端 spsd 內容
傾出本端 PostgreSQL 資料庫 a
完成 - 已建立 spsd-backup-2017-04-04T144448-0700.tar.gz
```

產品資料還原

關於這項作業

產品還原是透過在 MDE VM 內執行的指令行 Script 完成。

還原 Script spsd-restore 位於 /opt/securityfirst/spsd/bin 目錄中。

```
sudo /opt/securityfirst/spsd/bin/spsd-restore --help
用法：spsd-restore [--nodb] [--noprops] [--help] FILE
-----
--nodb 不要寫入資料庫
--noprops 不要寫入本端內容
--help 顯示此說明
```

若要執行還原：

```
sudo /opt/securityfirst/spsd/bin/spsd-restore
spsd-backup-2017-04-04T144448-0700.tar.gz
```

註：還原備份檔之後，下一次啟動 MDE 將套用變更。

核心更新

關於這項作業

當執行 Red Hat Enterprise Linux 7 或 CentOS 7 作業系統的代理程式需要進行核心更新時，請使用下列準則：

- 如果作業系統/核心更新處於相同版本，則會自動支援新核心。
- 如果作業系統/核心升級至更高版本（亦即 RHEL 7.2 -> 7.4），請執行下列步驟以建置對新核心的支援：
 - 範例：代理程式安裝軟體組解壓縮至 /root/agent

```
cd /root/agent/spx-installer
./agent_setup.sh -d /root/agent
Reboot
```

對於在 Red Hat Enterprise Linux 6 或 CentOS 6 上執行的代理程式，不需要執行這些步驟。

升級

請遵循下列步驟將 MDE 產品升級至新版本。

註：這些步驟適用於 MDE 開放式虛擬化軟體驅動裝置。如果執行非 OVA 安裝，目錄可能會有所變化。

針對 MDE 伺服器

關於這項作業

程序

1. 以 root 身分停止 PPM 原則服務。

```
systemctl stop spsd
```

2. 備份 MDE 資料：

```
/opt/securityfirst/spsd/bin/spsd-backup
```

3. 將新版本 MDE bin 檔案移至 /home/admin 目錄。
4. 刪除現有 rpms 目錄。

```
rm -fr /home/admin/rpms
```

5. 變更對於 MDE bin 檔案的存取權。

```
chmod +x /home/admin/ibm_sw_mde_X.x.x-XX.bin
```

6. 執行新版本的 MDE bin 檔案。

```
/home/admin/ibm_sw_mde_X.x.x-XX.bin
```

7. 安裝 RPM。

```
yum -y install /home/admin/rpms/*
```

8. 執行 Upgrade Script。

```
/opt/securityfirst/spsd/bin/spsd-pgsetup --upgrade
```

9. 再次啟動 PPM 原則服務備份：

```
systemctl start spsd
```

從舊版升級

關於這項作業

必須執行這些步驟才能讓原則運作！

程序

1. 導覽至「代理程式資訊」頁面
2. 按一下「編輯主要原則」
3. 按一下「儲存、Snapshot 及啟動」
4. 核准工作
5. 返回代理程式 VM 並嘗試對原則中的目錄執行讀寫動作、以原則中對於該目錄具有權限的使用者身分登入，然後驗證是否不容許非定義使用者。

針對代理程式目標 VM

Linux/AIX 代理程式

關於這項作業

程序

1. 建立新的代理程式目錄，並切換至新的代理程式目錄

```
mkdir [agent_new_directory]  
cd [agent_new_directory]
```

2. 下載或向下捲動各別代理程式的安裝軟體組

```
curl --header "Accept: application/x-tar" -u  
username:password  
https://<PPM IP address>/rest/agents/Agent ID #/install_bundle> install_bundle_name.tar
```

3. 解壓縮安裝軟體組

```
tar xvf <install_bundle_name>.tar
```

4. 執行 setup.sh Script 以重新安裝代理程式

```
./setup.sh
```

5. 出現提示時，回答是以重新啟動代理程式。
6. 如果需要，您可以從前一個代理程式目錄中刪除先前的所有安裝程式檔案。

```
rm -rf [/previous Agent directory]
```

Windows 代理程式

關於這項作業

程序

1. 下載各別代理程式的安裝軟體組
2. 解壓縮安裝軟體組

3. 執行 .msi 安裝程式以安裝新的代理程式軟體
4. 出現提示時，回答「是」以重新啟動代理程式

服務資料

收集服務資料

服務資料收集是透過在 MDE VM 內執行 Script 來完成。

spsd-service Script 位於 MDE VM 的 /opt/securityfirst/spsd/bin 目錄中。

```
sudo /opt/securityfirst/spsd/bin/spsd-service --help
用法: spsd-service [OPTIONS]
-----
選項:
  --nodb 不要傾出資料庫
  --norest 不要從 REST API 取回任何資料
  --nosys 不要取回系統資料 (/var/log、/proc 等)
  --withcore 在 spsd 當機時取回
  --help 顯示此說明
```

若要執行服務資料收集：

```
sudo /opt/securityfirst/spsd/bin/spsd-service
```

移除 PPM 日誌中的機密性資訊

為了協助保護服務資料不在 PPM 邏輯界限內時的 PPM 安裝隱私，下列 MDE 除錯日誌使用特殊化的語法標籤來標記機密性資訊：

- bundleAll.log
- bundleWarnPlus.log
- debug.log
- warn.log

註：在服務資料 Tarball（上方服務資料收集程序的結果）內，這些日誌可能位於 logs 資料夾中。

標籤格式化為 #<tagname>(<tagdata>)，其中 <tagdata> 會取代為要標記的資料，<tagname> 是下列其中一項：

- user - 標記使用者名稱，無論是 MDE 使用者還是與 MDE 整合的外部服務的使用者。範例：#user(admin)
- group - 標記群組名稱。範例：#group(domainusers)
- email - 標記電子郵件位址。範例：#email(example@example.com)
- ip - 標記 IP 位址。範例：#ip(192.168.0.5)
- host - 標記網路主機名稱。範例：#host(dns.example.com)
- key - 標記公用加密金鑰或相關值（如受管理金鑰名稱）。範例：#key(HRKey2)
- cert - 標記憑證資料，例如所連接代理程式的識別名稱。範例：#cert(C=US, ST=UT, L=Provo, O=Example Corp., OU=architecture, CN=docserver4)
- fingerprint - 標記憑證指紋。範例：#fingerprint(41:1A:B9:89:DB:77:90:77:39:D0:DF:5E:98:90:B7:17)

可以使用處理程序從服務資料中移除標籤，例如，在此範例中，從 bundleAll.log 日誌移除 #user 標籤資料：

```
gunzip spsd-service-2018-01-24T141620-0800.tar.gz
tar xf spsd-service-2018-01-24T141620-0800.tar ./logs/bundleAll.log
sed -i '/\#user/c\REDACTED' logs/bundleAll.log
tar --delete --file=spsd-service-2018-01-24T141620-0800.tar ./logs/bundleAll.log
```



```
tar --append --file=spsd-service-2018-01-24T141620-0800.tar ./logs/bundleAll.log  
gzip spsd-service-2018-01-24T141620-0800.tar
```


附錄 A 範例代理程式安裝程序

下列小節概述代理程式安裝軟體組的一般安裝程序。這些僅是範例方法，而不是受支援的安裝指示。

Red Hat / CentOS 程序

關於這項作業

透過 **CURL** 傳送安裝軟體組：

程序

1. 登入目標系統
2. 確保與 MDE 伺服器的網路連線有效
3. 確保在系統中建立、連接及配置原則中識別的所有使用者、群組及路徑或裝置
4. 登入 MDE
5. 在 MDE 內，供應目標系統的代理程式
6. 在 MDE 內，檢視代理程式詳細資料並記錄下載 URL

Users

Authorized Users admin

Install Files Download URL/rest/agents/1/install_bundle

[Download Zip Bundle](#)

[Download Tar Bundle](#)

7. 從目標系統中，建立用於代理程式下載的目錄，然後變更至該目錄
8. 使用下列 curl 指令下載 TAR 軟體組：

```
[user@localhost]$ curl -k --header "Accept: application/x-tar" -u admin:admin https://<PPM IP>/<Download URL> > package.tar
```

使用 PPM 所定義使用者的範例：

```
[user@localhost]$ curl -k --header "Accept: application/x-tar" -u admin:admin-password https://1.1.1.10/rest/agents/1/install_bundle > package.tar
```

使用 PPM LDAP 所定義使用者的範例：

```
[user@localhost]$ curl -k --header "X-Directory: tenant1" --header "Accept: application/x-tar" -u john:secret https://1.1.1.10/rest/agents/1/install_bundle > package.tar
```

(assuming directory identifier "tenant1", with user "john" and password "secret")

9. 從目標系統中，解壓縮套件：

```
[user@localhost]$ tar -xf package.tar
```

10. 從目標系統中，以 root 使用者身分執行安裝 Script

```
[user@localhost]$ ./setup.sh
```

11. 完成安裝 Script 之後，即已安裝代理程式，並將從 MDE 下載原則且原則生效。

AIX 處理程序

關於這項作業

傳送安裝軟體組：

1. 登入目標系統
2. 確保與 MDE 伺服器的網路連線有效
3. 確保在系統中建立、連接及配置原則中識別的所有使用者、群組及路徑或裝置
4. 登入 MDE
5. 在 MDE 內，供應目標系統的代理程式
6. 在 MDE 內，檢視代理程式詳細資料並記錄下載 URL

Users

Authorized Users admin

Install Files Download URL /rest/agents/1/install_bundle

[Download Zip Bundle](#)

[Download Tar Bundle](#)

7. 從目標系統中，建立用於代理程式下載的目錄，然後變更至該目錄
8. 將軟體組傳送至目標系統。
9. 從目標系統中，解壓縮套件：

```
[user@localhost]$ tar -xvf package.tar
```

10. 從目標系統中，以 root 使用者身分執行安裝 Script。

```
[user@localhost]$ ./setup.sh
```

11. 完成安裝 Script 之後，即已安裝代理程式，並將從 MDE 下載原則且原則生效。

Windows 伺服器處理程序

關於這項作業

傳送安裝軟體組：

程序

1. 登入目標系統
2. 確保與 MDE 伺服器的網路連線有效
3. 確保在系統中建立、連接及配置原則中識別的所有使用者、群組及路徑或裝置
4. 登入 MDE
5. 在 MDE 內，供應目標系統的代理程式
6. 在 MDE 內，檢視代理程式詳細資料並記錄下載 URL

Users

Authorized Users admin

Install Files Download URL /rest/agents/1/install_bundle

[Download Zip Bundle](#)

[Download Tar Bundle](#)

7. 按一下「下載 ZIP 軟體組」，以將代理程式軟體的 ZIP 檔軟體組下載至本端系統
8. 將安裝軟體組傳送至目標系統
9. 在目標系統上，解壓縮 Zip 檔軟體組的內容
10. 執行安裝軟體組的 msi 檔

FileAgent-<version>.msi

範例：

PS C:\> FileAgent-4.2.11-0030.msi

11. 完成安裝 Script 並已適當安裝代理程式之後，原則將生效。

註：需要重新開機。若要略過所要求的重新開機提示，您可以執行帶 no reboot 選項的指令：

msiexec /i <agent_filename_version.msi> NO_REBOOT_PROMPT=1

附錄 B 憑證管理中心 (CA) 憑證範例

關於這項作業

MDE 需要「憑證管理中心」所簽署的憑證，才能在管理伺服器 (PPM) 與代理程式之間建立安全階段作業。它將需要：

- 金鑰儲存庫
- 信任儲存庫
- CA 憑證組合

可以使用根據內部公司 RSA 的「憑證管理中心」或第三方「憑證管理中心」來簽署憑證。在下面的 Linux 範例中，建立了下列項目：

- 已建立「憑證簽署要求 (CSR)」，並已傳送至「憑證管理中心」待簽署。已結合已簽署的憑證與金鑰以建立金鑰儲存庫。
- 已使用「憑證管理中心」的憑證組合建立信任儲存庫。
- 已建立代理程式憑證。在 PPM 與代理程式之間進行通訊需要這些憑證。

提供本範例是為了便於您參考，在產生要簽署的憑證時須遵循「憑證管理中心」。方括弧內的名稱 [name.pem] 代表的是在使用公司或第三方憑證時不同或改變的檔名。

如果要建立金鑰儲存庫，您將需要提交 CSR 給內部公司「憑證管理中心」或第三方「憑證管理中心」。

程序

1. 建立一個包含下列資訊的 OpenSSL 配置檔（亦即 ppm.cnf）：

```
[req]
default_bits          = 4096
distinguished_name     = req_distinguished_name
req_extensions         = v3_req
prompt                = no

[req_distinguished_name]
C      = your_country
ST     = your_state_or_province
L      = your_locale_(city)
O      = your_organization
OU     = your_org_unit_(department)
CN     = your_ppm_host.your_domain

[ v3_req ]
# Extensions to add to a certificate request
basicConstraints      = CA:FALSE
extendedKeyUsage      = serverAuth
subjectAltName        = @alt_names

[alt_names]
DNS.1    = your_ppm_host.your_domain
IP.1     = your_ppm_ip_address
```

您需要更新 [req_distinguishd_name] 和 [alt_names] 區段以反映您的組織資訊。

2. 建立 PPM CSR

```
openssl req -out [csr.pem] -new -newkey rsa:2048 -keyout [key.pem] -outform pem
```

3. CSR [csr.pem] 必須由憑證管理中心 (CA) 簽署
4. 從 CA 收到已簽章的憑證之後，請驗證延伸金鑰用法和主體替代名稱是否存在

```
openssl x509 -in [signed cert] -noout -text
```

5. 將已簽章的憑證與金鑰結合（來自步驟 2 的金鑰）

```
a. openssl pkcs12 -export -out [ppm.p12] -inkey [key.pem] -in [signed-cert] -name ppm
b. keytool -importkeystore -srckeystore [ppm.p12] -keystore [ppm.jks] -storetype JKS
```

如果要建立信任儲存庫，您將需要它用來簽署 CSR 的「憑證管理中心」憑證。這又稱為 CA 憑證組合。請將下面的“ca_bundle.crt”取代為此憑證的實際名稱。

- 使用憑證管理中心 (CA) 憑證組合建立信任儲存庫。如果 CA 憑證組合中有多個憑證，則必須將這些憑證分隔並逐個匯入信任儲存庫中。

```
a. keytool -import -trustcacerts -file [ca_bundle-1.crt] -alias CA1 -keystore [trust.jks]
b. keytool -import -trustcacerts -file [ca_bundle-2.crt] -alias CA2 -keystore [trust.jks]
c. continue for each certificate in bundle
```

- 將產生的 *.jks 和 [ca_bundle.crt] 檔案複製到安全目錄（即 /etc/ppm/certs）中的 PPM 伺服器。當您使用 spsd-certsetup Script 更新 Web 和代理程式內容檔時，將會指定此位置（請參閱下面的「管理伺服器設定」）

還需要 MDE 代理程式憑證。

- 建立一個包含下列資訊的 OpenSSL 配置檔（亦即 host01.cnf）：

```
[req]
default_bits = 2048
distinguished_name = req_distinguished_name
req_extensions = v3_req
prompt = no

[req_distinguished_name]
C = your_country
ST = your_state_or_province
L = your_locale_(city)
O = your_organization
OU = your_org_unit_(department)
CN = your_agent_host.your_domain

[ v3_req ]
# Extensions to add to a certificate request
basicConstraints = CA:FALSE
extendedKeyUsage = clientAuth
subjectAltName = @alt_names

[alt_names]
DNS.1 = your_agent_host.your_domain
IP.1 = your_agent_ip_address
```

You need to update the [req_distinguished_names] and [alt_names] sections to reflect your organization's information.

- 建立 MDE 代理程式 CSR

```
a. openssl req -out [host01.csr] -nodes -sha256 -newkey rsa:2048 -keyout [host01.key] -config [host01.cnf]
```

- 要求憑證管理中心 (CA) 所簽署的 CSR
- 從 CA 收到已簽章的憑證之後，請驗證延伸金鑰用法和主體替代名稱是否存在

```
a. openssl x509 -in [signed-agent] -noout -text
```

- 如果代理程式憑證是由不同於 PPM 憑證的 CA 所簽署，則必須將 CA_bundle 憑證匯入 PPM 信任儲存庫中。請參閱上方 PPM 憑證建立程序 (CSR) 的步驟 5
- 結合已簽章的憑證與金鑰

```
a. cat [signed-agent] [host01.key] > [host01.pem]
```


g. 在 MDE 中建立此主機的代理程式時使用 [host01.pem] 憑證/金鑰組

a. 在建立 PPM 代理程式期間使用瀏覽器上傳 [host01.pem]。

將 [host01.pem] 複製到工作站或共用資源，以便在建立 PPM 代理程式期間可存取它。

針對將安裝代理程式的每一個主機重複此處理程序。

管理伺服器設定

在配置任何「原則代理程式」之前，必須先更新「管理伺服器設定」的憑證。在上傳您公司的金鑰儲存庫和信任儲存庫以及 CA 憑證組合之後，這將需要在伺服器上執行所提供的 Script (/opt/securityfirst/spsd/bin/spsd-certsetup) (請參閱「管理者手冊」中的「伺服器憑證設定」小節)。它還將需要重新啟動 spsd 服務或重新啟動「管理伺服器 (PPM)」。不這麼做將會導致代理程式無法與 MDE 管理伺服器通訊。

如果尚未更新憑證，但是已配置代理程式，則執行憑證更新 Script，然後在「代理程式資訊」頁面上更新代理程式憑證，將會還原代理程式與 MDE 管理伺服器之間的通訊。

附錄 C 轉換以建立 PKCS12 檔案範例

關於這項作業

使用下列步驟，將用戶端私密金鑰與用戶端憑證結合至單一 PKCS12（公開金鑰密碼化標準 12 號）檔：

```
[user@localhost]$ openssl pkcs12 -export -out ppmclient.p12 -inkey client_key.pem -in client_cert.pem  
-name ppmclient
```

```
[user@localhost]$ keytool -v -list -keystore ppmclient.p12 -storetype pkcs12
```

附錄 D 注意事項

變更已指派的金鑰

概觀

我在受保護目錄內具有資料，且我希望修改與該目錄相關聯的金鑰。

背景

目錄內的資料會使用建立資料時（或將資料移至該目錄時）定義的金鑰進行加密。變更原則金鑰不會將業已存在的資料移轉至新的金鑰。

原則已套用至代理程式並處於作用中時，修改受保護目錄的金鑰值可能非常危險。雖然未嚴格禁止，但修改金鑰值可能導致資料流失。

執行

如果管理者要將整個目錄從一個金鑰移轉至另一個金鑰，則必須先將資料從該目錄移出。目錄清空後，可以變更及套用與原則相關聯的金鑰值。然後，可以將資料移回該目錄，即會以新的金鑰來加密該資料。

不執行

在未先將資料從目錄移出的情況下，請勿修改與原則相關聯的金鑰值以及啟動原則。如果未遵循最佳實務方法，則將繼續使用原始金鑰加密目錄中最初呈現的資料。將原則修改為新金鑰後，資料將變成無法存取。此外，如果輪替原始金鑰，則由於無法將原則修改回原始金鑰值，資料將永久地無法存取。

旋轉具有加密備份的金鑰

概觀

我希望備份受保護目錄中的資料。

背景

使用加密格式備份資料，會在備份時將該資料連結至金鑰值。如果在執行備份作業之後輪替金鑰，則它無法適當地還原。

金鑰應該與受保護的位置（而不是資料）相關聯。這將防止還原時發生意外的資料存取問題。

執行

目錄內的資料會使用建立資料時（或將資料移至該目錄時）定義的金鑰進行加密。最好在旋轉金鑰之前備份資料。可以使用代理程式公用程式 "spx-backup" 來執行此作業。此作業將會備份資料以及不基於受保護的目錄並且不受金鑰旋轉影響的金鑰。

不執行

複製加密格式（例如，磁碟映像檔或 VM Snapshot）的受保護目錄時須小心。如果這樣做，則在輪替原始金鑰之後，資料可能變成無法存取。

附錄 E 就地加密

為了容許對預先存在的目錄結構及資料加密，並隨時判定資料的狀態，MDE 提供了名為 "spxconvert" 的指令行公用程式。

此功能不僅能夠加密業已存在的資料，還在通過支付卡產業 (PCI) 或醫療保險轉移和責任法 (HIPAA) 等審核時有用。

註：此功能將僅處理「檔案」代理程式，不覆蓋需要正式資料移轉的磁區。

指令選項

spxconvert 用法：（參數使用方括弧 [] 指出並包括類型）

-h (-?, ?) 「列印此說明對話框」

-a 「執行加密的檔案審核」

-p [STR] 「審核路徑」

-e [STR] 「加密路徑中任何未受保護的檔案」

-c 「傾出檔案轉換前/後的所有總和檢查」

-v 「詳細 - 額外列印新增的資訊」

審核 (-a)

依預設，會針對原則目錄中的所有檔案執行審核。這可以使用 -p 選項縮短至單一目錄。審核將列印目錄中未加密的任何檔案，並列印目錄內已加密檔案總數的檔案計數。

加密 (-e)

轉換指定目錄中任何未受保護的檔案。完成時，將對使用者顯示包含不符總和檢查的任何檔案。選用性 -c 旗標將在完成時列印所有檔案的總和檢查，而非只是衝突的總和檢查。為了效能只能在完成時列印總和檢查，因為必須在轉換之後清除系統快取。在每一個檔案之後清除快取會對效能造成巨大的負面影響。

審核步驟

1. 顯示是否有任何項目加密在擱置中：

spxinfo -l

1. 顯示資料的詳細資訊：

spxconvert -a -v

1. 顯示特定目錄的詳細資訊：

spxconvert -p -v <path>

加密步驟

1. 顯示加密在擱置中的項目：

spxinfo -l

1. 顯示加密之前的所有總和檢查：

spxconvert -c -p <path>

1. 加密特定路徑中的任何檔案：

spxconvert -p -v <path>

1. 顯示加密之後特定路徑上的所有總和檢查：

spxconvert -c -p <path>

附錄 F 代理程式除錯記載

依預設，「原則」代理程式執行時不會記載除錯層次訊息。為了擷取代理程式日誌中的除錯層次訊息，代理程式的系統管理者必須啟用該功能，然後重新啟動代理程式以使除錯層次訊息開始被擷取。

有效值為 1-6；但預設值為 4，如果設定的值小於 4，則可能會省略任何有用的資訊。

嚴重附註

- 啟用除錯層次記載可能會揭露機密系統資訊
- 由於除錯傳訊的本質，代理程式日誌檔案的大小可能會大幅增加。

Linux 代理程式

關於這項作業

找出位於 `/etc/sysconfig/spx-policyagent` 的配置檔並設定可寫入旗標 (`chmod +w /etc/sysconfig/spx-policyagent`) 來啟用除錯。

將 “**LOG_LEVEL=6**”（不帶引號）附加至檔案的底端。

Windows 代理程式

關於這項作業

找出位於 `HKLM\SYSTEM\CurrentControlSet\Services\Spx Policy Agent\log level` 的登錄機碼並將值設定為 ‘6’ 來啟用除錯。

附錄 G 非 OVA 部署

下面是有關如何為 PPM 部署設定非 OVA 環境的範例說明。只有在您不是部署已套用的 PPM OVA，而是建立您自己的 RHEL 或 CentOS 7.x 環境以在其中部署 PPM 軟體時，這些說明才適用。

在所有 PPM 節點上安裝套件。

註：這只是一個範例設定。有許多環境特定的需要將會導致這些說明不適用。請於支援人員聯絡以取得其他協助。

1. 安裝 java 1.8 和 postgresql 9.2。

註：在 initdb 處理程序期間，系統將提示您輸入密碼。此密碼是 postgres "superuser" 密碼。

```
yum install -y postgresql-server java-1.8.0-openjdk-headless
passwd postgres
su - postgres
initdb --auth=md5 -W
exit
```

2. 安裝防火牆原則。

下面的範例顯示如何使用 iptables 來安裝防火牆原則。也可以使用其他方法，請根據網站喜好設定使用。範例：`yum install -y iptables iptables-services`

下面兩個指令假定您已安裝並啟用 firewalld。如果尚未安裝 firewalld，執行中這些指令不會帶來危害。

```
systemctl stop firewalld
systemctl disable firewalld
```

啟動並更新 IP Tables 防火牆服務

```
systemctl start iptables.service
iptables -F
```

啟用 iptables 服務 - 選用步驟 - 如果您不需要基於本端軟體的防火牆，則可以跳過

```
systemctl enable iptables.service
```

定義基本防火牆 - 選用步驟 - 如果您不需要基於本端軟體的防火牆，則可以跳過

```
iptables -A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --
update --seconds 60 --hitcount 4 --name DEFAULT --rsource -j LOG --log-prefix
"SSH BruteForce: "
iptables -A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --
update --seconds 60 --hitcount 4 --name DEFAULT --rsource -m recent --set --name
ssh --rsource
iptables -A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
service iptables save
```

3. 安裝 Keepalive、HAProxy 和 PSMisc 套件。

```
yum install -y haproxy keepalived psmisc
```

4. 下載 Zookeeper。

註：如果未安裝 wget，請予以安裝：

```
yum install -y wget
wget http://apache.claz.org/zookeeper/zookeeper-3.4.10/zookeeper-3.4.10.tar.gz
mkdir /home/admin
mv zookeeper-3.4.10.tar.gz /home/admin
```

5. 安裝並配置可靠的網路時間來源。

範例顯示 NTP 配置，但是其他可靠的時間來源也可用，請根據網站喜好設定使用。

```
yum install -y ntp
sed -i "/server\ [0-9].rhel/ s/rhel/us/" /etc/ntp.conf
sed -i "/server\ [0-9].centos/ s/centos/us/" /etc/ntp.conf
systemctl stop chronyd
systemctl disable chronyd
systemctl start ntpd
systemctl enable ntpd
```

6. 為 Enterprise Linux (EPRL) 儲存庫安裝額外的套件

```
yum install -y epel-release
```

7. 安裝無法預期的隨機數字產生器（需要 EPEL）。

```
yum install -y haveged
```

8. 安裝 net-tools 用於收集服務資料。

```
yum install -y net-tools
```

附錄 H 軟體版本檢查

檢查下列指令以檢查軟體版本。

PPM 版本

從 PPM VM Shell 中，執行下列指令：

```
cat /etc/ppm/buildinfo/release
```

Linux 代理程式版本

從 Linux CLI 中，執行下列指令：

```
yum list policyagent
```

AIX 代理程式版本

從 AIX CLI 中，執行下列指令：

```
rpm -qa | grep fileagent
```

Windows 代理程式版本

在 Windows 中，導覽至**新增/移除程式**。捲動以尋找代理程式名稱。

代理程式類型	在 Windows 中的代理程式名稱
具有原則的檔案	FileAgent
磁區	VolumeAgent
具有原則的磁區	HybridAgent

附錄 I 名詞解釋

術語	定義
進階加密標準新指示 (Advanced Encryption Standard New Instructions, AES-NI)	2001 年美國國家標準與技術機構 (NIST) 建立的電子資料加密規格；基於 SPx 的產品使用的加密協議。
代理程式 (Agent)	執行 Security First 加密與存取控制軟體的受管理伺服器。
Amazon Web 服務 (AWS) S3 (Amazon Web Services (AWS) S3)	一個簡單的儲存服務，可儲存和擷取資料，是高度可擴展且便宜的物件儲存體。
自動產生的金鑰 (Auto-Generated Keys)	由 MDE 建立及管理的原則強制執行金鑰。這些金鑰在原則建立期間由 Autogenerate 金鑰指出。
憑證管理中心 (Certificate Authority)	授信簽署數位憑證的組織。CA 可驗證已提交憑證申請的身分及合法性。如果申請驗證成功，則 CA 會發出已簽章的憑證。
憑證撤銷清單 (Certificate Revocation List, CRL)	由已發出對應憑證之憑證管理中心 (CA) 撤銷的憑證已發佈清單。
憑證撤銷清單配送點 (Certificate Revocation List Distribution Point, CRLDP)	憑證內保留發證 CA 已撤銷憑證相關資訊的起始點欄位，包括名稱，可選擇包括撤銷理由及 CRL 發證者名稱。
雲端審核資料聯合 (Cloud Auditing Data Federation, CADF)	轉遞至安全資訊及事件管理 (SIEM) 系統的一般事件格式語法類型。
逗點事件格式 (Comma Event Format, CEF)	轉遞至安全資訊及事件管理 (SIEM) 系統的一般事件格式語法類型。
逗點區隔值 (Comma Separated Value, CSV)	使用逗點作為欄位定界字元，並使用換行作為記錄定界字元的資料格式。
指令行介面 (Command Line Interface, CLI)	使用者以文字行（指令行）的形式向應用程式發出指令的互動類型
世界標準時間 (Coordinated Universal Time, UTC)	世界用來規定時鐘與時間的主要時間標準。
加密存取控制 (Cryptographic Access Controls)	能夠透過利用不同的加密資料分隔使用者存取權。
CURL	CURL 是電腦軟體專案，可提供程式庫及指令行工具來使用各種協議傳送資料。
識別編碼規則 (Distinguished Encoding Rules, DER)	DER 是在 ITU-T X.690 2002 規格中定義的其中一種 ASN.1 編碼規則。資料結構的編碼規則會提供傳送語法，可控管在電腦之間傳送時如何組織串流中的位元組。
網域名稱 (Domain Name, DN)	全球唯一且鏈結至 IP 目的地資訊的網際網路資源名稱
網域名稱服務 (Domain Name Service, DNS)	將網域名稱轉換為 IP 位址的網際網路服務。
動態主機配置通訊協定 (Dynamic Host Configuration Protocol, DHCP)	自動提供網際網路通訊協定 (IP) 主機以及其他 IP 位址和其他相關配置資訊（例如子網路遮罩及預設閘道）的主從式通訊協定。

檔案代理程式 (File Agent)	根據一個或多個受保護檔案路徑的作業存取原則定義及關聯，施行檔案型作業的檔案代理程式。每一個受保護的檔案路徑都可以具有其自己的作業及加密存取控制。
圖形使用者介面 (Graphical User Interface, GUI)	可讓使用者透過圖形圖示（而不是文字型介面及鍵入的指令）與 MDE 互動的使用者介面類型
醫療保險轉移和責任法 (Health Insurance Portability and Accountability Act, HIPAA)	HIPAA 隱私權法規需要提供者及組織來確保受保護健康資訊 (PHI) 的機密性及安全性
高可用性 (High Availability, HA)	即使元件由於備用（備用電源供應器、CPU、磁碟機、軟體等）而失敗，系統作業仍會繼續
超文字傳送通訊協定 (Hypertext Transfer Protocol, HTTP)	作為全球資訊網資料通訊基礎的應用程式通訊協定。
Hypervisor	也稱為虛擬機器監視器。Hypervisor 或虛擬機器監視器 (VMM) 是一個電腦軟體、韌體或硬體，會建立、執行及管理虛擬機器。Hypervisor 在其上執行一個或多個虛擬機器的電腦稱為主機；每一個虛擬機器都稱為訪客機器。VMware Hypervisor 也稱為 ESXi 主機。
IBM 雲端物件儲存體 (COS S3) (IBM Cloud Object Storage (COS S3))	該儲存體平台可存放大量資料，例如備份、保存檔、視訊檔案和影像檔，可提供靜態資料和高可用性。
起始設定向量 (Initialization Vector, IV)	可以與用於資料加密之秘密金鑰一起使用的任意或無法預期的亂數，在任何階段作業中只能採用一次。
Java 金鑰儲存庫 (Java KeyStore, JKS)	Java 金鑰儲存庫 (JKS) 是安全憑證 – 授權憑證或公開金鑰憑證 – 加上對應私密金鑰的儲存庫。Java 開發套件 (JDK) 提供工具 (keytool) 來管理金鑰儲存庫中的金鑰及憑證。jks 副檔名是 Java 特定的檔案格式。
金鑰撤銷 (Key Revocation)	從代理程式環境中移除原則強制執行金鑰會產生可回復的加密資料存取限制。此動作讓資料暫時地無法讀取。
金鑰旋轉 (Key Rotation)	在代理程式環境內移轉原則強制執行金鑰不會對資料存取產生任何使用者可見的變更。
金鑰解構 (Key Shredding)	從代理程式環境中移除原則強制執行金鑰會產生不可回復的加密資料存取限制。此動作讓資料永久地無法讀取。
金鑰儲存庫 (Keystore)	原則強制執行金鑰的所配置儲存位置。
輕量型目錄存取通訊協定 (Lightweight Directory Access Protocol, LDAP)	供應商中立的開放性業界標準通訊協定，用來透過網路存取及維護分散式目錄資訊。此軟體通訊協定可讓任何人找到組織、個人及其他資源，例如網路中的檔案及裝置。
日誌事件延伸格式 (Log Event Extended Format, LEEF)	LEEF 是 IBM Security QRadar 的自訂事件格式，包含 QRadar 可讀取的容易處理的事件。它支援事件有效負載的數個預先定義的事件屬性。
邏輯磁區管理程式 (Logical Volume Manager, LVM)	一種儲存裝置管理程式，可使用裝置對映器 Linux Kernel 架構將儲存裝置收集成群組，並根據需要從合併空間配置邏輯單元。大部分 Linux 發行套件都支援 LVM。

M:N (M of N, M:N)	該模型可以判斷在所建立的資料總數 (N) 中，重建其中資料 (M) 所需的資料（共用）數量。
NT 檔案系統 (NT File System, NTFS)	由 Microsoft Windows NT 作業系統開發的專有檔案系統，用來儲存並擷取硬碟上支援檔案層次安全、壓縮及審核的檔案。
網路時間通訊協定 (Network Time Protocol, NTP)	電腦系統之間用於時鐘同步化的網路通訊協定。
物件 ID (Object Identifier, OID)	用於使用廣域明確持續性名稱命名任何物件或概念的 ID 標準化機制。
物件儲存庫代理程式 (Object Store Agent)	物件儲存庫代理程式會加密並分割要傳送的資料，並安全地儲存在高度可擴展、高效率的物件儲存體中 – 在雲端中或內部部署的伺服器上。
線上憑證狀態通訊協定 (Online Certificate Status Protocol, OCSP)	用來取得 X.509 數位憑證的撤銷狀態的內部通訊協定。
開放式虛擬化保存檔 (Open Virtualization Archive, OVA)	tar 保存檔。這是壓縮至單一檔案的所有 OVF 檔。
支付卡產業 (Payment Card Industry, PCI)	用來增加持卡人資料控制及安全來減少詐騙的標準。
PEM	廣泛使用的安全憑證編碼格式，其語法及內容是由 X.509 第 3 版標準進行定義。
PostgreSQL	PostgreSQL（發音為 post-gress-Q-L）是全球自願者團隊開發的開放程式碼關聯式資料庫管理系統 (DBMS)。PostgreSQL 不受任何公司或其他專用實體管制，且原始碼免費提供。
受保護 (Protected)	所有已處理的資料。
公開金鑰密碼化標準 #12 (Public Key Cryptography Standard #12, PKCS12)	一種公開金鑰加密標準，可定義保存檔格式來將許多加密物件儲存為單一檔案。一般用來將私密金鑰與其 X.509 憑證組合或組合信任鏈的所有成員。可以加密和簽署。
公開金鑰基礎架構 (Public Key Infrastructure, PKI)	建立、管理、配送、使用、儲存及撤銷數位憑證和管理公開金鑰加密所需的一組角色、原則及程序。
ReFS	由 Windows Server 2012 引入的 Microsoft 的新檔案系統，旨在最大化資料可用性、可調整性及資料完整性。
具象狀態傳送應用程式介面 (Representational State Transfer Application Program Interface, REST API)	REST API（也稱為 REST Web 服務）基於具象狀態傳送 (REST) 技術，該技術是 Web 服務開發中常用的架構樣式及通訊方法。
角色型存取控制 (Role Based Access Control, RBAC)	根據企業內個別使用者角色規範對電腦或網路資源之存取的方法。在此環境定義中，個別使用者可透過存取來執行特定作業，例如檢視、建立或修改檔案。
RSA	由 Rivest、Shamir 及 Adelman (RSA) 開發的使用公開和私密金鑰來確保資料安全的公開金鑰加密法。
安全複製通訊協定 (Secure Copy Protocol, scp)	在 Linux 中使用 scp 指令來透過 Secure Shell (SSH) 通訊協定在系統之間傳送檔案。
Secure Socket Layer (SSL)	利用非對稱金鑰交換對稱金鑰加密網際網路上資料通訊的加密通訊協定。需要憑證管理中心及公開金鑰基礎架構才能驗證憑證及擁有者，以及產生、簽署及管理憑證的有效性。

Secure Socket Shell (SSH)	為管理者提供安全的遠端電腦存取方法的網路通訊協定。SSH 也是指實作此通訊協定的公用程式套組。
選取元 (Selector)	作業系統定義的使用者和群組，可以存取資料、路徑集和其他原則相關功能。
傳輸層安全 (Transport Layer Security, TLS)	安全提供電腦網路通訊的加密通訊協定
信任儲存庫 (Truststore)	信任儲存庫儲存授信憑證管理中心 (CA) 中的憑證，該中心用來透過 SSL 連線中的伺服器驗證憑證。
唯一的 ID (Unique Identifier, UUID)	通用唯一 ID (UUID) 是軟體建構中使用的 ID 標準。UUID (128 位元數字) 用來唯一地識別網際網路上的部分物件或實體。
虛擬機器 (Virtual Machine, VM)	基於電腦架構及真實或假設電腦之功能的電腦系統模擬。
VMware ESXi™	基於電腦架構及真實或假設電腦之功能的特定電腦系統模擬。
磁區代理程式 (Volume Agent)	磁區代理程式施行目標系統上一個或多個受保護磁區的磁區原則定義及關聯。
具有原則的磁區代理程式 (Volume with Policy Agent)	它利用磁區代理程式的磁區原則保護，並容許針對一個或多個受保護的檔案路徑套用及施行檔案型作業存取控制原則。也稱為混合式代理程式

注意事項[r]

本資訊係針對 IBM 在美國所提供之產品與服務所開發。

IBM 提供本資料的其他語言版本。然而，您可能需要擁有該語言的產品副本或產品版本，才能進行存取。

在其他國家中，IBM 不見得有提供本文件所提及之各項產品、服務或功能。請洽詢當地的 IBM 業務代表，以取得當地目前提供的產品和服務之相關資訊。本文件在提及 IBM 的產品、程式或服務時，不表示或暗示只能使用 IBM 的產品、程式或服務。只要未侵犯 IBM 之智慧財產權，任何功能相當之產品、程式或服務皆可取代 IBM 之產品、程式或服務。不過，任何非 IBM 之產品、程式或服務，使用者必須自行負責作業之評估和驗證責任。

本文件所說明之主題內容，IBM 可能擁有其專利或專利申請案。提供本文件不代表提供這些專利的授權。您可以書面提出授權查詢，來函請寄到：

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785 U.S.A.

下列段落不適用於英國，若與任何其他國家之法律條款抵觸，亦不適用於該國：

International Business Machines Corporation 只依「現況」提供本出版品，不提供任何明示或默示之保證，其中包括且不限於不侵權、可商用性或特定目的之適用性的隱含保證。有些地區在特定交易上，不允許排除明示或暗示的保證，因此，這項聲明不一定適合您。

本資訊中可能會有技術上或排版印刷上的訛誤。因此，IBM 會定期修訂；並將修訂後的內容納入新版中。IBM 隨時會改進及/或變更本出版品所提及的產品及/或程式，不另行通知。

本資訊中任何對非 IBM 網站的敘述僅供參考，IBM 對該網站並不提供任何保證。這些網站所提供的資料不是 IBM 本產品的資料內容，如果要使用這些網站的資料，您必須自行承擔風險。

IBM 得以各種 IBM 認為適當的方式使用或散布 貴客戶提供的任何資訊，而無需對 貴客戶負責。如果本程式之獲授權人為了 (i) 在個別建立的程式和其他程式（包括本程式）之間交換資訊，以及 (ii) 相互使用所交換的資訊，因而需要相關的資訊，請洽詢：

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785 U.S.A.

上述資料之取得有其特殊要件，在某些情況下必須付費方得使用。

IBM 基於 IBM 客戶合約、IBM 國際程式授權合約或雙方之任何同等合約的條款，提供本資訊所提及的授權程式與其所有適用的授權資料。

本文件所提及之非 IBM 產品資訊，取自產品的供應商，或其發佈的聲明或其他公開管道。IBM 並未測試過這些產品，也無法確認這些非 IBM 產品的執行效能、相容性或任何對產品的其他主張是否完全無誤。有關非 IBM 產品的性能問題應直接洽詢該產品供應商。

有關 IBM 未來方向或意圖的所有陳述隨時可能變更或撤銷，而不會另行通知，且僅代表目標和目的。

本資訊包含每日業務運作中使用之資料及報告的範例。為了盡可能完整地說明它們，範例包括個人、公司、品牌及產品的名稱。所有這些名稱均係虛構，若與實際企業的名稱及地址發生任何雷同，則純屬巧合。

著作權：

本資訊含有原始語言之範例應用程式，用以說明各作業平台中之程式設計技術。貴客戶可以為了研發、使用、銷售或散布符合範例應用程式所適用的作業平台之應用程式介面的應用程式，以任何形式複製、修改及散布這些範例程式，不必向 IBM 付費。這些範例並未在所有情況下完整測試。故 IBM 不保證或默示保證這些樣本程式之可靠性、服務性或功能。這些程式範例以「現狀」提供，且無任何保證。IBM 對因使用這些程式範例而產生的任何損害概不負責。根據您正在檢視本資訊的方式，部分影像及圖解可能不會顯示。

商標[r]

SPx 與 Security First Corp 是 Security First Corp. 在世界許多管轄區域註冊的商標或註冊商標。其他產品及服務可能是 Security First Corp. 或其他公司的商標。

IBM、IBM 標誌及 ibm.com 是 International Business Machines Corp. 在世界許多管轄區域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" 中找到，網址為：<http://www.ibm.com/legal/copytrade.shtml>。

Adobe、Adobe 標誌、PostScript 及 PostScript 標誌是 Adobe Systems Incorporated 在美國及（或）其他國家或地區的註冊商標或商標。

Apache Software Foundation (ASF) 擁有所有 Apache 相關商標、服務標示及圖形標誌（代表我們的 Apache 專案社群），並且所有 Apache 專案的名稱都是 ASF 的商標。

Node.JS 是 Joyent, Inc. (CORPORATION DELAWARE 345 California Street; Suite 2000 San Francisco CALIFORNIA 94104) 的註冊商標。

Unicode 及 Unicode 標誌是 Unicode, Inc. 在美國及其他國家或地區的註冊商標。

CentOS Marks 是 Red Hat, Inc. ("Red Hat") 的商標。

"Red Hat"、Red Hat Linux、Red Hat "Shadowman" 標誌及所列產品是 Red Hat, Inc. 在美國及其他國家或地區的商標或註冊商標。

Linux 是 Linus Torvalds 在美國及（或）其他國家或地區的註冊商標。

Microsoft、Windows、Windows NT 及 Windows 標誌是 Microsoft Corporation 在美國及/或其他國家或地區的商標。

Java 和所有以 Java 為基礎的商標及標誌是 Oracle 及（或）其子公司的商標或註冊商標。

產品條款說明文件[r]

這些出版品之使用權係根據下列條款進行授與：

適用性：這些條款是 IBM 網站之使用條款的補充條款。

個人用途：貴客戶可以為了非商務性的私人用途而複製這些出版品，但必須保留所有專利注意事項。如果沒有 IBM 的明文同意，貴客戶不能散布、顯示或衍生這些出版品或其中的任何部分。

商業用途：貴客戶可以在企業內複製、散布和顯示這些出版品，但必須保留所有專利注意事項。如果沒有 IBM 的明文同意，貴客戶不能在您的企業外衍生這些出版品，或複製、散布或顯示這些出版品或其中的任何部分。

權限：除了本項許可權所明確授予者之外，並未明示或暗示授予出版品或任何資訊、資料、軟體或其中的其他智慧財產的任何其他許可權、授權或權利。IBM 保留在判定出版品的使用將損害其利益或判定未適當遵守上述指示時，撤銷此處所授予之許可權的權利。除非完全符合所有適當的法律和規章，其中包括所有美國輸出法律和規章，否則，貴客戶不能下載、輸出或再輸出本項資訊。

IBM 不提供這些出版品內容的任何保證。這些出版品只依「現狀」提供，不含任何明示或暗示的保證，其中包括且不限於可商用性或符合特定效用的暗示保證。

隱私權原則考量[r]

IBM 軟體產品（包括軟體即服務解決方案（「軟體產品與服務」））可能使用 Cookie 或其他技術來收集產品使用資訊，以協助改良一般使用者體驗，自訂與一般使用者的互動，或者用於其他目的。在許多情況下，軟體產品與服務不會收集任何個人識別資訊。部分軟體產品與服務可以協助您收集個人識別資訊。如果此軟體產品與服務使用 Cookie 收集個人識別資訊，則下方說明此產品與服務之 Cookie 使用的特定資訊。此軟體產品與服務不會使用 Cookie 或其他技術來收集個人識別資訊。

如果為此軟體產品與服務部署的配置可讓您透過 Cookie 及其他技術作為客戶收集一般使用者的個人識別資訊，您應該探查您自己的有關適用於此類資料收集之任何法律的法律建議，其中包括注意事項及同意書的所有需求。

如需將各種技術（包括 Cookie）用於這些目的的相關資訊，請參閱 IBM's Privacy Policy（網址為 <http://www.ibm.com/privacy>）及 IBM's Online Privacy Statement（網址為 <http://www.ibm.com/privacy/details>）標題為 "Cookies, Web Beacons and Other Technologies" 及 "IBM Software Products and Software-as-a-Service Privacy Statement" 的小節（網址為 <http://www.ibm.com/software/info/product-privacy>）。

產品編號：5737-C67

美國列印

注意事項

本資訊係針對 IBM 在美國所提供之產品與服務所開發。IBM 提供本資料的其他語言版本。然而，您可能需要擁有該語言的產品副本或產品版本，才能進行存取。

在其他國家，IBM 不見得有提供本文件所提及之各項產品、服務或功能。請洽詢當地的 IBM 業務代表，以取得當地目前提供的產品和服務之相關資訊。本文件在提及 IBM 的產品、程式或服務時，不表示或暗示只能使用 IBM 的產品、程式或服務。只要未侵犯 IBM 之智慧財產權，任何功能相當之產品、程式或服務皆可取代 IBM 之產品、程式或服務。不過，任何非 IBM 之產品、程式或服務，使用者必須自行負責作業之評估和驗證責任。

本文件所說明之主題內容，IBM 可能擁有其專利或專利申請案。提供本文件不代表提供這些專利的授權。您可以書面提出授權查詢，來函請寄到：

*IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US*

如果是有關雙位元組字元集 (DBCS) 的授權查詢，請洽詢所在國的 IBM 智慧財產部門，或書面提出授權查詢，來函請寄到：

*Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan*

下列段落不適用於英國，若與任何其他國家之法律條款抵觸，亦不適用於該國：

International Business Machines Corporation 只依「現況」提供本出版品，不提供任何明示或默示之保證，其中包括且不限於不侵權、可商用性或特定目的之適用性的隱含保證。

有些地區在特定交易上，不允許排除明示或暗示的保證，因此，這項聲明不一定適合您。

本資訊中可能有技術上或排版印刷上的訛誤。因此，IBM 會定期修訂；並將修訂後的內容納入新版中。IBM 隨時會改進及/或變更本出版品所提及的產品及/或程式，不另行通知。

本資訊中任何對非 IBM 網站的敘述僅供參考，IBM 對該網站並不提供任何保證。這些網站所提供的資料不是 IBM 本產品的資料內容，如果要使用這些網站的資料，您必須自行承擔風險。

IBM 得以各種 IBM 認為適當的方式使用或散布 貴客戶提供的任何資訊，而無需對 貴客戶負責。

如果本程式之獲授權人為了 (i) 在個別建立的程式和其他程式（包括本程式）之間交換資訊，以及 (ii) 相互使用所交換的資訊，因而需要相關的資訊，請洽詢：

*IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US*

上述資料之取得有其特殊要件，在某些情況下必須付費方得使用。

IBM 基於 IBM 客戶合約、IBM 國際程式授權合約或雙方之任何同等合約的條款，提供本文件所提及的授權程式與其所有適用的授權資料。

本文件中所含的任何效能資料是在控制環境中得出。因此，在其他作業環境中獲得的結果可能有明顯的差異。部分測量可能是在開發階段的系統上測定，無法保證這些測量在一般可用的系統上維持不變。再者，有些測定可能是透過推測方式來評估。實際結果可能不同。本文件的使用者應驗證適用於其特定環境的資料。

本文件所提及之非 IBM 產品資訊，取自產品的供應商，或其發佈的聲明或其他公開管道。IBM 並未測試過這些產品，也無法確認這些非 IBM 產品的執行效能、相容性或任何對產品的其他主張是否完全無誤。有關非 IBM 產品的性能問題應直接洽詢該產品供應商。

有關 IBM 未來方向或意圖的所有陳述隨時可能變更或撤銷，而不會另行通知，且僅代表目標和目的。

顯示的所有 IBM 價格都是 IBM 的最新建議零售價，可隨時變更而不另行通知。經銷商價格可能有所不同。

本資訊僅用於規劃用途。在所述產品上市之前，這裡的資訊可能會隨時變更。

本資訊包含每日業務運作中使用之資料及報告的範例。為了盡可能完整地說明它們，範例包括個人、公司、品牌及產品的名稱。所有這些名稱均係虛構，若與實際企業的名稱及地址發生任何雷同，則純屬巧合。

著作權：

本資訊含有原始語言之範例應用程式，用以說明各作業平台中之程式設計技術。貴客戶可以為了研發、使用、銷售或散布符合範例應用程式所適用的作業平台之應用程式介面的應用程式，以任何形式複製、修改及散布這些範例程式，不必向 IBM 付費。這些範例並未在所有情況下完整測試。故 IBM 不保證或默示保證這些樣本程式之可靠性、服務性或功能。這些程式範例以「現狀」提供，且無任何保證。IBM 對因使用這些程式範例而產生的任何損害概不負責。

這些程式範例或任何衍生著作的每一份副本或任何部分，都必須按如下所示包含版權聲明：

© (貴公司名稱) (年份). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _輸入年份_.

如果您是檢視本資訊的電子檔形式，則可能不會顯示照片及彩色圖解。

商標

SPx 與 Security First Corp 是 Security First Corp. 在世界許多管轄區域註冊的商標或註冊商標。其他產品及服務可能是 Security First Corp. 或其他公司的商標。

IBM、IBM 標誌及 ibm.com 是 International Business Machines Corp. 在世界許多管轄區域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" 中找到，網址為：<http://www.ibm.com/legal/copytrade.shtml>。

Adobe、Adobe 標誌、PostScript 及 PostScript 標誌是 Adobe Systems Incorporated 在美國及（或）其他國家或地區的註冊商標或商標。

Apache Software Foundation (ASF) 擁有所有 Apache 相關商標、服務標示及圖形標誌（代表我們的 Apache 專案社群），並且所有 Apache 專案的名稱都是 ASF 的商標。

Node.JS 是 Joyent, Inc. (CORPORATION DELAWARE 345 California Street; Suite 2000 San Francisco CALIFORNIA 94104) 的註冊商標。

Unicode 及 Unicode 標誌是 Unicode, Inc. 在美國及其他國家或地區的註冊商標。

CentOS Marks 是 Red Hat, Inc. ("Red Hat") 的商標。

"Red Hat"、Red Hat Linux、Red Hat "Shadowman" 標誌及所列出產品是 Red Hat, Inc. 在美國及其他國家或地區的商標或註冊商標。

Linux 是 Linus Torvalds 在美國及（或）其他國家或地區的註冊商標。

Microsoft、Windows、Windows NT 及 Windows 標誌是 Microsoft Corporation 在美國及/或其他國家或地區的商標。

Java 和所有以 Java 為基礎的商標及標誌是 Oracle 及（或）其子公司的商標或註冊商標。

產品說明文件的條款

這些出版品之使用權係根據下列條款進行授與：

適用性

這些條款是 IBM 網站之任何使用條款的補充條款。

個人用途

貴客戶可以為了非商務性的私人用途而複製這些出版品，但必須保留所有專利注意事項。如果沒有 IBM 的明文同意，貴客戶不能散布、顯示或衍生這些出版品或其中的任何部分。

商業用途

貴客戶可以在企業內複製、散布和顯示這些出版品，但必須保留所有專利注意事項。如果沒有 IBM 的明文同意，貴客戶不能在您的企業外衍生這些出版品，或複製、散布或顯示這些出版品或其中的任何部分。

權利

除了本項許可權所明確授予者之外，並未明示或暗示授予出版品或任何資訊、資料、軟體或其中的其他智慧財產的任何其他許可權、授權或權利。

IBM 保留在判定出版品的使用將損害其利益或判定未適當遵守上述指示時，撤銷此處所授予之許可權的權利。

除非完全符合所有適當的法律和規章，其中包括所有美國輸出法律和規章，否則，貴客戶不能下載、輸出或再輸出本項資訊。

IBM 不提供這些出版品內容的任何保證。這些出版品只依「現狀」提供，不含任何明示或暗示的保證，其中包括且不限於可商用性或符合特定效用的暗示保證。

隱私權原則考量 privacy policy consi

IBM 軟體產品（包括軟體即服務解決方案（「軟體產品與服務」））可能使用 Cookie 或其他技術來收集產品使用資訊，以協助改良一般使用者體驗，自訂與一般使用者的互動，或者用於其他目的。在許多情況下，軟體產品與服務不會收集任何個人識別資訊。部分軟體產品與服務可以協助您收集個人識別資訊。如果此軟體產品與服務使用 Cookie 收集個人識別資訊，則下方說明此產品與服務之 Cookie 使用的特定資訊。此軟體產品與服務不會使用 Cookie 或其他技術來收集個人識別資訊。

如果為此軟體產品與服務部署的配置可讓您透過 Cookie 及其他技術作為客戶收集一般使用者的個人識別資訊，您應該探查您自己的有關適用於此類資料收集之任何法律的法律建議，其中包括注意事項及同意書的所有需求。

如需將各種技術（包括 Cookie）用於這些目的的相關資訊，請參閱 IBM's Privacy Policy（網址為 <http://www.ibm.com/privacy>）及 IBM's Online Privacy Statement（網址為 <http://www.ibm.com/privacy/details>）標題為 "Cookies, Web Beacons and Other Technologies" 及 "IBM Software Products and Software-as-a-Service Privacy Statement" 的小節（網址為 <http://www.ibm.com/software/info/product-privacy>）。



SC43-5046-01

