

IBM Multi-Cloud Data Encryption
由 SPx[®] 提供技術支援
版本 2.3

常見問題 (FAQ)



附註

在使用本資訊及其支援的產品之前，請閱讀第 11 頁的『[注意事項](#)』中的資訊。

除非新版本另有說明，否則本版適用於 IBM Multi-Cloud Data Encryption 2.3 版（產品編號 5737-C67）及所有後續版次與修訂。

© 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 .**

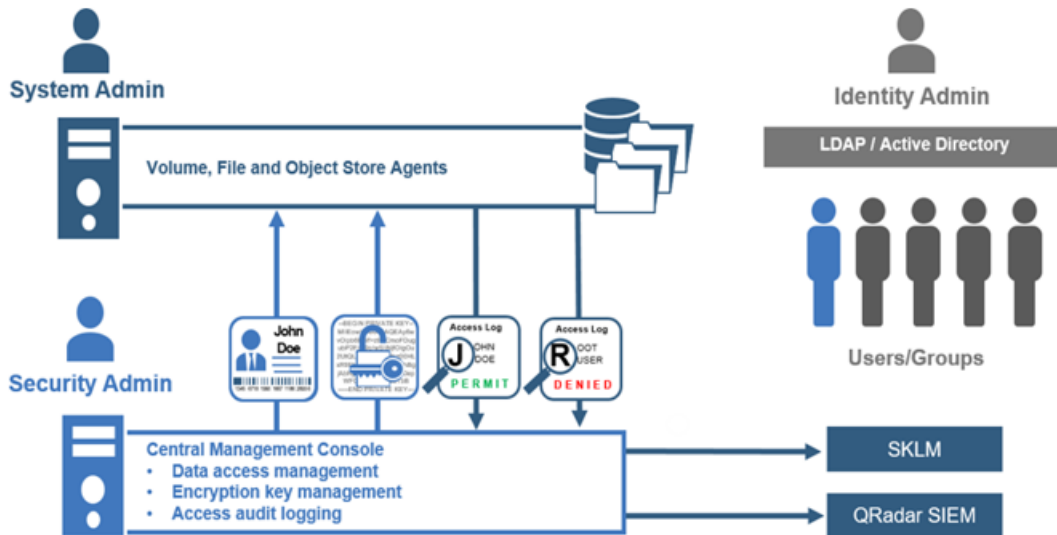
目錄

第 1 章概觀.....	1
第 2 章 MDE - 常見問題 (FAQ).....	3
一般常見問題 (FAQ).....	3
問題：何謂 IBM Multi-Cloud Data Encryption (MDE)？.....	3
問題：IBM Multi-Cloud Data Encryption (MDE) 支援哪些作業系統？.....	3
問題：MDE 代理程式支援哪些檔案系統？.....	3
問題：IBM Multi-Cloud Data Encryption (MDE) 是否需要任何必要條件？.....	3
問題：IBM Multi-Cloud Data Encryption (MDE) 支援哪些瀏覽器？.....	3
問題：IBM Multi-Cloud Data Encryption (MDE) 是否以 FIPS 模式執行？.....	3
問題：使用 Multi-Cloud Data Encryption (MDE) 時，是否需要在將資料傳送至遠端系統時對資料進行加密？是否仍然需要使用 VPN 與遠端系統連線？.....	4
問題：IBM Multi-Cloud Data Encryption (MDE) 「在位元層次編排資料的安全」是什麼意思？.....	4
問題：請說明如何使用 IBM Multi-Cloud Data Encryption (MDE) 來維持資料完整性。.....	4
原則、供應及管理常見問題 (FAQ).....	4
問題：「原則、供應及管理 (PPM)」主控台的用途是什麼？.....	4
問題：「原則、供應及管理 (PPM)」主控台為何使用角色型存取控制？.....	4
問題：在「原則、供應及管理 (PPM)」主控台中，何謂「程序」？其用途是什麼？.....	4
問題：在「原則、供應及管理 (PPM)」主控台中，何謂「選取元」？其用途是什麼？.....	4
問題：在「原則、供應及管理 (PPM)」主控台中，何謂「路徑集」？其用途是什麼？.....	4
問題：在「原則、供應及管理 (PPM)」主控台中，何謂「資料類型」？其用途是什麼？.....	5
問題：在「原則、供應及管理 (PPM)」主控台中，何謂「代理程式」？其用途是什麼？.....	5
問題：何時應該使用磁區代理程式？其運作方式為何？.....	5
問題：何時應該使用包含原則的檔案代理程式？其運作方式為何？.....	5
問題：何時應該使用包含原則的磁區代理程式？其運作方式為何？.....	5
問題：何時應該使用物件儲存庫代理程式？並且其運作方式為何？.....	5
問題：在「原則、供應及管理 (PPM)」主控台中，何謂工作？其用途是什麼？.....	5
問題：對於 IBM Multi-Cloud Data Encryption，何時需要使用外部 PostgreSQL 資料庫？.....	6
憑證常見問題 (FAQ).....	6
問題：PPM 伺服器憑證有哪些需求？.....	6
問題：代理程式憑證有哪些需求？.....	6
問題：PPM 支援「網址轉換 (NAT)」或「埠位址轉換 (PAT)」嗎？.....	6
問題：如何針對「網址轉換 (NAT)」或「埠位址轉換 (PAT)」網路配置中的 PPM 伺服器配置 PPM 伺服器憑證？.....	6
問題：當代理程式位於網址轉換 (NAT) 或埠位址轉換 (PAT) 網路配置中時，我要如何配置代理程式憑證？.....	6
問題：在高可用性 (HA) 配置中的 PPM 伺服器憑證有哪些需求？.....	6
金鑰及金鑰處理常見問題 (FAQ).....	7
問題：IBM Multi-Cloud Data Encryption 可以執行哪些主要處理作業？.....	7
問題：為何應該輪替金鑰？.....	7
問題：為何應該撤銷金鑰？.....	7
問題：為何應該絞碎金鑰？.....	7
問題：IBM Multi-Cloud Data Encryption 是否會為我管理金鑰？.....	7
安裝及設定常見問題 (FAQ).....	7
問題：IBM Multi-Cloud Data Encryption (MDE) 是如何影響一般使用者（亦即，非管理使用者）的？.....	7
問題：MDE Agent 可安裝在 Docker 主機上並處理來自 Docker 儲存器中應用程式的所有讀取/寫入要求嗎？.....	7
配置常見問題 (FAQ).....	7
問題：是否可以使用 IBM Multi-Cloud Data Encryption (MDE) 來加密 HTML 檔案？.....	8

作業常見問題 (FAQ).....	8
問題：如何知道是否已使用 IBM Multi-Cloud Data Encryption (MDE) 來加密資料？.....	8
問題：在對 IBM Multi-Cloud Data Encryption (MDE) 的正式作業實作進行變更之前應採取哪些 預防措施？.....	8
問題：是否可以將事件從 IBM Multi-Cloud Data Encryption (MDE) 轉遞至其他 SIEM（安全資 訊與事件管理）相關性應用程式？.....	8
問題：區分大小寫（大寫）重要嗎？.....	8
問題：作業順序有何意義，以及它為何重要？.....	8
問題：我已提交 Snapshot 啟動工作，且它仍在執行中。它何時將完成？.....	8
高可用性常見問題 (FAQ).....	8
問題：IBM Multi-Cloud Data Encryption (MDE) 部署是否需要高可用性？.....	8
問題：高可用性 (HA) IBM Multi-Cloud Data Encryption 部署是否需要負載平衡器？.....	9
多承租戶常見問題 (FAQ).....	9
問題：多方承租戶特性的用途是什麼？.....	9
注意事項.....	11
商標.....	12
產品說明文件的條款.....	12
隱私權原則考量.....	13

第 1 章 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（透過代理程式）與 Policy Provisioning Manager (PPM)（充當中央管理主控台）的其他強大的保護功能相結合的 SPx® 技術。MDE 可以供應代理程式、資料存取原則設定（作業及加密存取定義），並從單一集中化位置來執行多達 25,000 個代理程式的管理（金鑰生命週期、代理程式更新及使用者存取記載）。MDE 提供一個無縫安全系統，其具有指派代理程式的彈性，可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。它提供超出標準加密範圍的以資料為中心的保護，從而使資料加密更穩健並且免受暴力密碼破解攻擊。它透過定義精細的存取原則來獲得在使用者層次限制、監視及審核資料存取的能力，從而進一步加強保護。



MDE 透過以下不同的管理者角色來提供權責區分：產品管理者與安全管理者。產品管理者角色具有配置及維護 MDE 產品所需的許可權。安全管理者角色具有供應及管理代理程式所需的許可權。圖 1 描述這些角色，將會在第 7 節：MDE 管理使用者管理中進一步討論。

提供了四種可部署的代理程式類型，它們會施行受保護或已加密資料的原則定義。磁區代理程式，施行一或多個受保護磁區的磁區原則定義及關聯。包含原則的檔案代理程式，施行一或多個受保護檔案路徑的檔案型作業存取原則定義及關聯，其中每個受保護的檔案路徑都可以具有其專屬的作業及存取控制原則（透過精細原則規格來定義）。包含原則的磁區代理程式，其利用磁區代理程式的磁區原則保護，並容許針對一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。並且「物件儲存庫代理程式」會加密並以密碼編譯形式分割傳送至一或多個雲端型物件儲存體的資料。

第 2 章 MDE - 常見問題 (FAQ)

一般常見問題 (FAQ)

問題：何謂 IBM Multi-Cloud Data Encryption (MDE)？

回答：MDE 引進並啟用代理程式、原則（作業及加密存取定義）的供應，並從單一集中化位置來執行多達 25,000 個代理程式的管理（生命週期更新及使用者審核）作業。MDE 支援部署四種代理程式類型：「磁區」、「包含原則的檔案」、「包含原則的磁區」及「物件儲存庫」。這些代理程式易於安裝、可讓一般使用者使用順暢，並且為管理者提供配置及部署軟體以符合 IT 環境相符性需求的能力。

問題：IBM Multi-Cloud Data Encryption (MDE) 支援哪些作業系統？

回答：MDE 目前支援下列作業系統：

- Red Hat® Enterprise Linux 6.2 核心版本 2.6.32-220 及後續版次
- Red Hat® Enterprise Linux 7.2+ 核心版本
- CentOS 6.2 核心版本 2.6.32-220 及後續版次
- CentOS 7.2 核心版本及後續版次
- Microsoft Windows Server® 2008R2
- Microsoft Windows Server® 2012
- Microsoft Windows Server® 2012R2
- Microsoft Windows Server® 2016

問題：MDE 代理程式支援哪些檔案系統？

回答：MDE 支援下列檔案系統：

- EXT3
- EXT4
- XFS（Red Hat®/CentOS 6.5 和更新版本）
- NTFS
- ReFS

問題：IBM Multi-Cloud Data Encryption (MDE) 是否需要任何必要條件？

回答：MDE 作為 OVA 遞送，其易於部署在 VMware ESXi™ 或 Microsoft Hyper-V 中並且可以在大部分其他 Hypervisor 中執行。

問題：IBM Multi-Cloud Data Encryption (MDE) 支援哪些瀏覽器？

回答：可以使用 Mozilla Firefox、Google Chrome™、Microsoft Internet Explorer 及 Microsoft Edge 來執行 MDE。

問題：IBM Multi-Cloud Data Encryption (MDE) 是否以 FIPS 模式執行？

回答：是，MDE 符合 FIPS 140.2 標準，如產品資料表中所指定。

問題：使用 Multi-Cloud Data Encryption (MDE) 時，是否需要在將資料傳送至遠端系統時對資料進行加密？是否仍然需要使用 VPN 與遠端系統連線？

回答：MDE 設計為將資料安全地寫入遠端網站（包括公用雲端網站）中，前提是它有權存取該檔案位置。但是，可能需要 VPN 才能連接至遠端網站。

問題：IBM Multi-Cloud Data Encryption (MDE) 「在位元層次編排資料的安全」是什麼意思？

回答：採用 SPx 技術的 MDE 將位元層次的加密、隨機化及含金鑰資料分割，以及鑑別（完整性檢查）、容錯和 COI 架構結合到一個程序中，該程序會將可識別的資料和資訊轉換為完全隨機且無法使用的二進位元素。此 MDE 作業的結果是 Information Assurance (IA) 元素會編排到資料的每一個結構中。安全、資料備援、信任及資訊共用架構全都相互作用並且遵循資料，從而使資料不可分割。從資料建立到資料解構及/或公開發行生命週期，應一直確保資料和資訊受到保護。當資料不再移動（已寫入儲存體中）以及存取資料時，資料保護應一直存在。

問題：請說明如何使用 IBM Multi-Cloud Data Encryption (MDE) 來維持資料完整性。

回答：可以使用訊息鑑別碼來確保資料完整性，必須符合這些鑑別碼，才能讀取資料。

原則、供應及管理常見問題 (FAQ)

問題：「原則、供應及管理 (PPM)」主控台的用途是什麼？

回答：PPM 會管理代理程式（資料保護模型）、原則（作業及加密存取定義）的供應，並從單一集中化位置來執行多達 25,000 個代理程式的管理（生命週期更新及使用者審核）作業。它支援部署四種資料加密代理程式類型：「磁區」、「包含原則的檔案」、「包含原則的磁區」及「物件儲存庫」。「磁區」在區塊裝置層次保護資料。「包含原則的檔案」在檔案層次保護資料並且提供檔案型作業存取控制。「包含原則的磁區」在區塊裝置層次保護資料並且提供檔案型作業存取控制。「物件儲存庫」加密並以密碼編譯形式分割傳送至一或多個雲端型物件儲存體的資料。

問題：「原則、供應及管理 (PPM)」主控台為何使用角色型存取控制？

回答：PPM 利用純靜態角色型存取控制 (RBAC) 設計。使用 PPM 內的功能需要特定的許可權。有兩種不同角色：產品管理者與安全管理者。雖然有一些共用的許可權，但角色區分可以為 IT 領導權提供管理職責的強大區分，從而使不稱職的員工不會破壞另一名員工的 IT 環境。可以新增每種類型的其他角色，以適當地支援更大型或更複雜的 IT 環境。此外，客戶可能會以程式化方式來定義核准工作所需要的管理者數目，以及拒絕工作所需要的管理者數目。因此，對於每一組角色而言，PPM 會追蹤管理者核准和拒絕，以確保獲得足夠的核准才能執行或拒絕工作。如果核准工作的管理者達到所需數目，則將執行工作。如果拒絕工作的管理者達到所需數目（可以不同於核准數目），則將取消工作。這樣可確保精確地控制管理與安全相關作業。會追蹤及記載核准及/或拒絕的順序以用於審核和相符性用途。

問題：在「原則、供應及管理 (PPM)」主控台中，何謂「程序」？其用途是什麼？

回答：程序也稱為「透過原則的程序」，是獲指派 IBM Multi-Cloud Data Encryption 所保護資料之存取控制的程序或應用程式清單。程序關聯於選取元以提供對程序的存取控制給目標系統上的使用者。

問題：在「原則、供應及管理 (PPM)」主控台中，何謂「選取元」？其用途是什麼？

回答：選取元是使用者、群組及程序的無序清單。與資料類型結合，它為安全管理者提供一種簡式方法來識別將要共用 MDE 所保護資料或對這些資料具有一般存取權的實體集合。選取元可以包含選用的「使用者」欄位、選用的「群組」欄位以及「群組來源」（內部或外部，如果 LDAP 已定義），或選用的「透過原則的程序」。

問題：在「原則、供應及管理 (PPM)」主控台中，何謂「路徑集」？其用途是什麼？

回答：路徑集是將由 MDE 原則保護（或可能已不受原則保護，視原則而定）的檔案路徑的無序清單。它為安全管理者提供一種簡式方法來指定或列出將由 MDE 保護的檔案路徑集合。指定路徑集時，安全管理者必須建立路徑集合的名稱。保護從提供的路徑向下遞迴至所有子目錄。「附註」是選用欄位。

問題：在「原則、供應及管理 (PPM)」主控台中，何謂「資料類型」？其用途是什麼？

回答：資料類型是指派給所指定類型之資料的存取定義列的排序清單。每一列都包含一個選取元、I/O 作業、動作定義及相關聯索引鍵。在建立代理程式時，資料類型會與檔案路徑（或路徑集）相關聯，以定義對資料的作業及加密存取控制。

問題：在「原則、供應及管理 (PPM)」主控台中，何謂「代理程式」？其用途是什麼？

回答：PPM 支援四種類型的代理程式，每一種都提供不同類型的保護。它們是「磁區」、「包含原則的檔案」、「包含原則的磁區」及「物件儲存庫」。「磁區」在磁區層次保護資料。「包含原則的檔案」在檔案層次保護資料並且提供檔案型作業存取控制，以及選擇性地提供加密存取控制。「包含原則的磁區」在磁區層次保護資料並且提供檔案型作業存取控制。「物件儲存庫」加密並以密碼編譯形式分割傳送至一或多個雲端型物件儲存體的資料。

問題：何時應該使用磁區代理程式？其運作方式為何？

回答：磁區代理程式以受保護的預先定義磁區形式為 IT 提供固定的資料安全。在部署時，磁區代理程式將會建立一組金鑰，這些金鑰將套用至整個磁區，從而將磁區作為單一單元進行加密保護。儲存及/或編輯、新增或刪除資料時，會立即呼叫加密演算法以確保適當地保護磁區內所有資料的安全。磁區可以分割成一個或多個分割區，每一個分割區都會受到類似的保護。磁區保護最適合用於計劃開放共用中到大型資料的使用者群組。

問題：何時應該使用包含原則的檔案代理程式？其運作方式為何？

回答：「包含原則的檔案」代理程式為 IT 提供非常強大的個別檔案層次保護。部署檔案代理程式時，會將最上層目錄識別為受保護資料的位置。會使用一組金鑰個別地保護儲存在其中的每一個檔案，而對「使用者」、「群組」及「程序」的檔案的存取控制則透過 PPM 定義的原則來管理。此外，安全管理者可以定義可套用至「使用者」、「群組」或「程序」的加密金鑰，如此一來，將以加密方式保護所選檔案，以防共用目錄存取權的其他人存取檔案。存取檔案時，可以選取一個選項，該選項容許記載每一次存取（讀取及/或寫入）以用於審核及追蹤用途。對使用檔案保護的檔案大小或儲存環境大小沒有限制 - 空間使用率會隨著空間內檔案的大小而擴充和成長。包含原則的檔案保護最適合用來保護共用或專用的個別檔案。

問題：何時應該使用包含原則的磁區代理程式？其運作方式為何？

回答：「包含原則的磁區」代理程式會將「使用者」和「群組」檔案存取控制新增至受保護的磁區（或分割區）。在部署時，磁區代理程式將會建立一組金鑰，這些金鑰將套用至整個磁區，從而將磁區作為單一單元進行加密保護。儲存及/或編輯、新增或刪除檔案時，會使用加密演算法以確保適當地保護磁區內所有資料的安全。安全管理者可以使用 PPM 為「使用者」、「群組」及「程序」定義檔案存取控制原則。存取檔案時，可以選取一個選項，該選項容許記載每一次存取（讀取及/或寫入）以用於審核及追蹤用途。「包含原則的磁區保護」最適合用於除了共用中到大型資料之外還需要檔案存取控制的使用者群組。

問題：何時應該使用物件儲存庫代理程式？並且其運作方式為何？

回答：「物件儲存庫代理程式」提供機會將資料儲存在內部部署或雲端中高度可調且有效的物件儲存體內。資料由客戶管制，一律為專用並且可用。存取權由物件儲存體擁有者控制。透過「物件儲存庫代理程式」傳送的資料會在本端加密並在傳輸過程中進一步使用「傳輸層安全 (TLS)」通訊協定進行保護。它確保透過支援 S3 的雲端儲存體來保護內部部署資料。「物件儲存庫代理程式」在 M/N 個模型上運作，確定重建資料所需的資料片段數目 (M)（建立的資料片段總數為 N）。儲存的資料片段（根據授權而定，可儲存在本端或遠端位置）稱為「分享」。使用多個分享可改進資料流程以及新增資料備援和容錯的選項。受支援的分散式分享模型 M/N 為：1:1、2:3 或 2:4。

問題：在「原則、供應及管理 (PPM)」主控台中，何謂工作？其用途是什麼？

回答：PPM 會納入一個工作系統（可從 GUI 存取）以管理和追蹤各種部署、原則及維護作業（與受保護資料及存取資料的人員/項目相關）的核准、計時和執行。當管理者輸入某項作業時，就會建立工作，並且新工作將會新增至工作頁面上顯示的清單中。具有權限的管理者將有核准、拒絕或放棄每項工作的選項。

問題：對於 IBM Multi-Cloud Data Encryption，何時需要使用外部 PostgreSQL 資料庫？

回答：強烈建議對所有正式作業環境使用外部 Postgres 資料庫。建議僅對幾乎沒有成長可能的極小型（少量代理程式、少量使用者和群組，或只有測試或 QA 設定）安裝使用內部資料庫。此外，在高可用性 (HA) 配置中部署 MDE 時，也需要 Postgres 資料庫。

憑證常見問題 (FAQ)

問題：PPM 伺服器憑證有哪些需求？

回答：PPM 伺服器憑證必須包含下列元素：

- 延伸的金鑰屬性，指定「伺服器鑑別」
- 主體替代名稱區段，指定 PPM 伺服器完整網域名稱 (FQDN)

問題：代理程式憑證有哪些需求？

回答：每個代理程式憑證必須包含下列元素：

- 延伸的金鑰屬性，指定「用戶端鑑別」
- 主體替代名稱區段，指定代理程式完整網域名稱 (FQDN)

問題：PPM 支援「網址轉換 (NAT)」或「埠位址轉換 (PAT)」嗎？

回答：是。PPM 伺服器必須可從代理程式連接，才能建立通訊，因為代理程式會起始與 PPM 伺服器的通訊階段作業。建立通訊之後，它會保持開啟。代理程式會使用此連線，將事件資料傳送至 PPM 伺服器。PPM 伺服器會使用此連線，將原則更新項目傳送至代理程式。

問題：如何針對「網址轉換 (NAT)」或「埠位址轉換 (PAT)」網路配置中的 PPM 伺服器配置 PPM 伺服器憑證？

回答：PPM 伺服器憑證必須包含下列元素：

- 延伸的金鑰屬性，指定「伺服器鑑別」
- 主體替代名稱區段，指定 PPM 伺服器完整網域名稱 (FQDN)
- 主體替代名稱區段，指定面向外部的 IP 位址

問題：當代理程式位於網址轉換 (NAT) 或埠位址轉換 (PAT) 網路配置中時，我要如何配置代理程式憑證？

回答：代理程式憑證必須包含下列元素：

- 延伸的金鑰屬性，指定「用戶端鑑別」
- 主體替代名稱區段，指定 PPM 伺服器完整網域名稱 (FQDN)
- 主體替代名稱區段，指定面向外部的 IP 位址

問題：在高可用性 (HA) 配置中的 PPM 伺服器憑證有哪些需求？

回答：PPM 伺服器憑證必須包含下列元素：

- 延伸的金鑰屬性，指定「伺服器鑑別」

- 主體替代名稱區段，指定組成 PPM 叢集的 PPM 伺服器完整網域名稱 (FQDN)，以及與 PPM 虛擬 IP 位址相關的 FQDN。

金鑰及金鑰處理常見問題 (FAQ)

問題：IBM Multi-Cloud Data Encryption 可以執行哪些主要處理作業？

回答：安全管理者可以定義加密金鑰以在 Policy Provisioning Manager (PPM) 內保護資料安全。這些金鑰可與資料類型、資料類型列及磁區相關聯。金鑰處理作業包括建立、輪替、撤銷及清除/處置。

問題：為何應該輪替金鑰？

回答：一般需要定期輪替金鑰，以確保資料受到充分的保護而不會遭到未獲授權的存取。金鑰輪替即是以全新的金鑰取代現行金鑰，並且由於加密本質，需要使用加密演算法進行計算。許多專家建議針對企業 IT 商店，特別是那些使用雲端互動的商店，執行定期金鑰輪替。目前有一些需要定期輪替的標準，例如 PCI-DSS。PPM 金鑰輪替會建立帶有時間戳記的資料記錄，會針對審核用途記載這些記錄以示範相符性。

問題：為何應該撤銷金鑰？

回答：撤銷 Policy Provisioning Manager (PPM) 金鑰將會暫時停用對受保護資料的存取。當資料保護存在問題時，或在必須拒絕存取受保護資料的實例期間，通常會撤銷金鑰。稍後，如果重新配送相同的金鑰，則資料可能會再一次變成可存取。

問題：為何應該絞碎金鑰？

回答：清除金鑰會永久地停用對受保護資料的存取。除非不再需要資料，否則請勿選擇此選項。

問題：IBM Multi-Cloud Data Encryption 是否會為我管理金鑰？

回答：如果安全管理者不想手動管理加密金鑰，則 Policy Provisioning Manager (PPM) 可以為每一個新建原則自動產生金鑰。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。

安裝及設定常見問題 (FAQ)

問題：IBM Multi-Cloud Data Encryption (MDE) 是如何影響一般使用者（亦即，非管理使用者）的？

回答：非管理使用者將可以享受到 IBM Multi-Cloud Data Encryption (MDE) 的安全和高可用性，而不會發現與其正常作業之間有任何差異。存取受管理（受保護）目錄中的檔案並不會影響其存取、寫入或儲存檔案的能力。

問題：MDE Agent 可安裝在 Docker 主機上並處理來自 Docker 儲存器中應用程式的所有讀取/寫入要求嗎？

回答：可以，包含原則的檔案代理程式以及磁區代理程式都可用來保護資料。

- 包含原則的檔案代理程式可用來保護 Docker 磁區路徑，以確保儲存器使用的應用程式資料受到保護。
- 磁區代理程式可用來保護 Docker 儲存器路徑。它有效加密整個儲存器及其所有 I/O。如果 Docker 磁區儲存在 Docker 儲存器路徑外部，則可配置額外的磁區來保護外部 Docker 磁區。
- Docker 主機的關鍵點是它必須在 Red Hat 7.2+ (3.10-*) 上執行受支援的核心

配置常見問題 (FAQ)

問題：是否可以使用 IBM Multi-Cloud Data Encryption (MDE) 來加密 HTML 檔案？

回答：此時不建議保護 HTML 檔案。網站正在顯示作用中的 HTML 檔案，如果加密，則這些檔案可能無法適當地顯示。

作業常見問題 (FAQ)

問題：如何知道是否已使用 IBM Multi-Cloud Data Encryption (MDE) 來加密資料？

回答：即使服務已停止，MDE 保護仍然處於作用中，並且可以存取任何受保護的檔案。

問題：在對 IBM Multi-Cloud Data Encryption (MDE) 的正式作業實作進行變更之前應採取哪些預防措施？

回答：當系統處於作業中時，可以透過 'spxconfig' 指令行或 GUI 進行次要修改。但是，需要詳細的準備工作以及執行建議的備份才能進行重大變更。（如需實作變更之前的正式作業生態系統，請參閱所有產品說明文件。）

問題：是否可以将事件從 IBM Multi-Cloud Data Encryption (MDE) 轉遞至其他 SIEM（安全資訊與事件管理）相關性應用程式？

回答：是。其包括事件聚集及轉遞系統。此系統會將受管理代理程式中的事件與內部產生的事件聚集在一起，並將它們儲存在內部事件日誌中，可以從管理者儀表板檢視這些事件並且可以配置為將事件轉遞至一或多個收件者。

問題：區分大小寫（大寫）重要嗎？

回答：是，區分大小寫非常重要。

- 建立選取器時，「使用者」欄位與「群組」欄位區分大小寫
- 使用 Windows 建立「路徑集」時，磁碟機代號必須大寫，且目錄名稱區分大小寫
- 建立「磁碟」或「具有原則代理程式的磁碟」時，「磁區」標籤區分大小寫
- 值或欄位應該一律採用區分大小寫

問題：作業順序有何意義，以及它為何重要？

回答：它非常重要，因為必須以特定順序完成建立及部署代理程式，以確保成功。

- 在部署檔案代理程式之前，目標磁區必須在線上、已起始設定、已利用所建立目錄格式化且具有適當的許可權。
- 部署磁區代理程式之前，磁區必須存在、在線上且已起始設定，但未格式化。
- 部署具有原則的磁區代理程式之前，磁碟必須存在、在線上且已起始設定，但未格式化。所定義的選取器必須存在於目標機器的本端或 LDAP / AD 階層。

問題：我已提交 Snapshot 啟動工作，且它仍在執行中。它何時將完成？

回答：所有 Snapshot 變更或更新項目都不會生效，除非代理程式能夠與 PPM 伺服器進行通訊。所建立的工作將保留執行中，除非 PPM 與代理程式之間通訊成功或從 PPM 伺服器中移除代理程式。

高可用性常見問題 (FAQ)

問題：IBM Multi-Cloud Data Encryption (MDE) 部署是否需要高可用性？

回答：在需要接近 100% 可用性的資料存取及保護管理服務的 IT 環境中，應該使用高可用性 (HA) MDE 部署。當 PPM 實例需要維護、發生失敗或突然離線時，熱備份實例將會立即接管並回復作業。

問題：高可用性 (HA) IBM Multi-Cloud Data Encryption 部署是否需要負載平衡器？

回答：是。代理程式與 PPM 伺服器之間需要存在兩個負載平衡器（負載平衡器叢集）。部署有兩個以上 PPM 伺服器的每一個位置中，都需要一個負載平衡器叢集。負載平衡器會在本端網路上相互通訊並提供一個虛擬 IP 位址（又稱為「浮動 IP 位址」），代理程式及管理者可以使用該位址來存取 PPM 伺服器。PPM HA 的實務範例有許多：單一位置、多個資料中心等，每一個都有其專屬的部署選項及配置。

多承租戶常見問題 (FAQ)

問題：多方承租戶特性的用途是什麼？

回答：PPM 的多方承租戶功能為 IT 提供者提供依客戶劃分 PPM 控制的能力。因此，每一個客戶在 IT 環境內都有其專屬的隔離 PPM 登入、管理者、原則、儀表板、工作、事件等。客戶可以共用儲存體甚至目錄，但其受保護檔案及磁區將會個別地受到加密保護以防彼此存取。這可讓多個承租戶或客戶安全地共用及利用相同的儲存體空間；同時每個承租戶的資料可以區隔出來並對其他承租戶或客戶不可見。

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 可能以其他語言提供本資料。但是，您可能需要擁有該語言的產品副本或產品版本才能存取它。

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。

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。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集 (DBCS) 資訊的授權查詢，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牴觸，即視為不適用：

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。

所有關於 IBM 未來方針或意向之聲明，僅代表 IBM 的目標與目的，隨時可能變動或撤銷，不另行通知。

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。

本資訊包含企業日常作業所使用的資料及報告範例。為了盡可能地加以完整說明，範例中含有個人、公司、品牌及產品的名稱。所有這些名稱都是虛構的，如有任何類似實際企業所用的名稱及地址之處，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 和 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" 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) 擁有所有與 Apache 相關的商標、服務標記及代表 Apache 專案社群的圖形標誌，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 和 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。非經 IBM 書面許可，貴客戶不得散布、顯示或製作這些出版品或其中任何部分的衍生著作。

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。非經 IBM 書面許可，貴客戶不得在企業外部製作這些出版品的衍生著作，或重製、散布或顯示這些出版品或其中任何部分。

權利

除了此許可權中明確授與之權限外，未對出版品或所含任何資訊、資料、軟體或其他智慧財產，明確或隱含授與任何其他權限、軟體使用權或權利。

IBM 保留隨時自行撤回在此授與權限之權利，當出版品的用途有害於其利益（由 IBM 判定）時，不會適當遵循上述指示。

除非完全遵守一切適用之法律規章（包括所有美國出口法律規章），否則貴客戶不得下載、出口或再出口此資訊。

IBM 不保證這些出版品內容的正確性。出版品依「現狀」提供，且不含任何明示或默示保證，包括但不限於適售性、無侵權行為和符合特定使用目的之默示保證。

隱私權原則考量

IBM 軟體產品，包括軟體即服務解決方案（「軟體供應項目」），可以使用 Cookie 或其他技術來收集產品使用資訊，以協助改進一般使用者體驗，以及自訂與一般使用者的互動或用於其他用途。在許多情況下，「軟體供應項目」不會收集任何個人識別資訊。部分「軟體供應項目」可以協助您收集個人識別資訊。如果此「軟體供應項目」使用 Cookie 來收集個人識別資訊，則會在下面說明關於此供應項目使用 Cookie 的特定資訊。此「軟體供應項目」不會使用 Cookie 或其他技術來收集個人識別資訊。

如果針對此「軟體供應項目」部署的配置可以為客戶提供透過 Cookie 及其他技術來收集一般使用者個人識別資訊的能力，您應當尋求專門的法律建議以瞭解適用於該類資料收集的任何法律條款，包括任何通知及同意需求。

如需為實現這些目的而使用各種技術（包括 Cookie）的相關資訊，請參閱 IBM 隱私權條款 (<http://www.ibm.com/privacy>) 和「IBM 線上隱私權聲明」(<http://www.ibm.com/privacy/details>) 中標題為「Cookie、Web Beacon 與其他技術」的小節以及「IBM 軟體產品和軟體即服務隱私聲明」(<http://www.ibm.com/software/info/product-privacy>)。



產品編號 CC0LSEN

GC43-5028-00



(1P) P/N: CC0LSEN

