IBM Spectrum Protect for Virtual Environments

版本 8.1.7

Data Protection for VMware
安装手册

IBM Spectrum Protect for Virtual Environments

版本 8.1.7

Data Protection for VMware
安装手册

附註：

在使用本資訊及其支援的產品之前，請先閱讀第 113 頁的『注意事項』中的資訊。

除非新版中另有指示，否則本版適用於 IBM Spectrum Protect for Virtual Environments 8.1.7 版（產品編號 5725-X00）以及所有後續版次和修訂。

目錄

關於本出版品

IBM Spectrum Protect™ for Virtual Environments 提供主機遠地區塊層增量備份，可讓您從 Windows 和 Linux 訪客機器的完整 VM 備份，進行檔案回復和即時還原。將 IBM Spectrum Protect for Virtual Environments 與 IBM Spectrum Protect 資料移轉裝置一起使用時，可以使用區塊層增量備份。

本出版品適用對象

本出版品適用於想要安裝並配置 IBM Spectrum Protect for Virtual Environments 的使用者及管理者。

《IBM Spectrum Protect for Virtual Environments：Data Protection for VMware 使用手冊》中說明了概觀資訊、使用者作業、備份及還原實務範例、指令參考手冊及錯誤訊息。

出版品

IBM Spectrum Protect 系列產品包括 IBM Spectrum Protect Plus、IBM Spectrum Protect for Virtual Environments、IBM Spectrum Protect for Databases 及 IBM® 提供的數個其他儲存體管理產品。

若要檢視 IBM 產品說明文件，請參閱 IBM Knowledge Center。

8.1.7 版的新增功能

IBM Spectrum Protect for Virtual Environments 8.1.7 版引進新的特性及更新項目。

如需第 8 版的此版本及舊版中新增特性及更新項目的清單，請參閱 Data Protection for VMware 更新項目。

在本產品說明文件中，新增及變更資訊由變更左側的垂直線 (|) 指出。

第 1 章 安裝及升級 Data Protection for VMware

安裝 IBM Spectrum Protect for Virtual Environments 包括規劃、安裝及起始配置。

可安裝的元件

Data Protection for VMware 包含數個元件，可加以安裝來保護虛擬環境。

根據作業系統環境而定，以下是可供安裝的 Data Protection for VMware 功能：

限制：每一個安裝套件都會附送一個使用者授權檔 (EULA)。 如果您不接受此檔案，便會停止安裝。

表 *1.* 依作業系統的可用 *Data Protection for VMware* 功能

元件	Linux	Windows
IBM Spectrum Protect 回復代理程式 此元件提供虛擬裝載和即時還原功能。		√
回復代理程式指令行介面 用於裝載作業的指令行介面。		√
文件 文件包含 ReadMe 和注意事項檔案。	√	√
Data Protection for VMware 啟用檔案 此元件可讓 IBM Spectrum Protect 執行下列備份類型： • 持續增量增量備份 • 持續增量完整備份 此元件對於應用程式保護是必要的。 如果您卸載備份工作量，則此檔案必須安裝在「vStorage 備用伺服器」上。	√	√
Data Protection for VMware vSphere GUI 這個元件是用於在 VMware vCenter Server 上存取 VM 資料的圖形使用者介面 (GUI)。 GUI 的內容在以下視圖中提供： • Web 瀏覽器視圖。 在支援的 Web 瀏覽器中使用 GUI Web 伺服器主機的 URL 可存取此視圖。 例如： `https://guihost.mycompany.com:9081/TsmVMwareUI/` • VMware vSphere Web Client 中的 IBM Spectrum Protect vSphere Client 外掛程式視圖。 此視圖中的這個畫面專用於與 vSphere Web 用戶端整合，但此視圖的資料及指令可從與其他視圖相同的 GUI Web 伺服器取得。IBM Spectrum Protect vSphere Client 外掛程式 會提供 Web 瀏覽器視圖中的部分可用功能，並會提供一些額外的功能。此視圖中未提供配置及進階報告功能。	√	√

表 1. 依作業系統的可用 *Data Protection for VMware* 功能 (繼續)

元件	Linux	Windows
檔案還原 GUI 此元件是 Web 型 GUI，可讓您從 VMware 虛擬機器備份中還原檔案，而無需管理者協助。 當安裝了 Data Protection for VMware GUI 時，會自動安裝此 GUI。 可透過配置精靈加以啟用。	[1]	√
資料移轉裝置 IBM Spectrum Protect 資料移轉裝置會移動 Data Protection for VMware 的資料。 此功能又稱為資料移轉裝置。 資料移轉裝置會將資料從虛擬環境移至 IBM Spectrum Protect 伺服器。 當您在伺服器上安裝資料移轉裝置時，該伺服器可來作為 vStorage 備用伺服器。 您可以在與 Data Protection for VMware 相同的系統上或另一部伺服器上安裝資料移轉裝置。	√	√

1. 縱使檔案還原介面元件必須在 Windows 系統上安裝及啟用，您仍然可以在 Windows 及 Linux 訪客虛擬機器上使用此介面來還原檔案。
2. 當您安裝 Data Protection for VMware 時，資料移轉裝置包括在安裝中。 一般安裝表示您不需要執行其他僅資料移轉裝置安裝，即可在該機器上取得資料移轉裝置。

Data Protection for VMware 會將備份工作量從虛擬機器卸載到 vStorage 備用伺服器。若要達成此作業，資料移轉裝置必須安裝在 vStorage 備用伺服器上。

Data Protection for VMware vSphere GUI

Data Protection for VMware vSphere GUI (vSphere GUI) 元件是一個圖形使用者介面，可存取 VMware vCenter Server 上的虛擬機器資料。

概觀

Data Protection for VMware vSphere GUI 是可從中完成下列作業的主要介面：

- 起始或排程 VM 備份至 IBM Spectrum Protect 伺服器。
- 起始從 IBM Spectrum Protect 伺服器完整回復虛擬機器。
- 發出關於作業的進度、已完成的最近事件、備份狀態及空間使用情形的報告。 這項資訊可協助您疑難排解在備份處理時發生的錯誤。

提示：隨 GUI 安裝的線上說明中提供如何使用 vSphere GUI 完成作業的相關資訊。按一下任何 GUI 視窗中的**進一步瞭解**以開啟作業協助的線上說明。

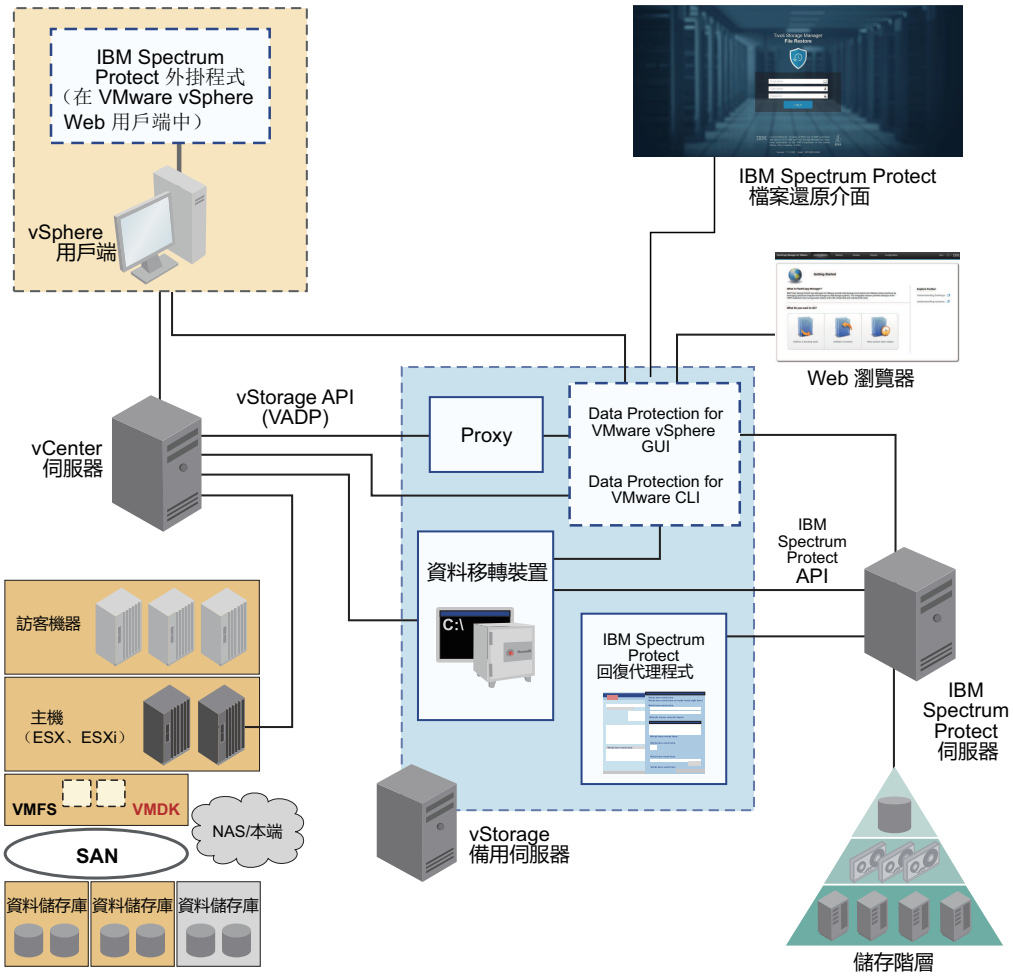

圖 1. *VMware vSphere* 使用者環境中的 *Data Protection for VMware* 系統元件

需求

Data Protection for VMware vSphere GUI 安裝在任何符合作業系統必要條件的系統上。 vSphere GUI 資源需求是最低的，因為它不處理 I/O 資料傳送。

提示：在 vStorage Backup Server 上安裝 vSphere GUI 是最常見的配置。

vSphere GUI 必須具有與下列系統的網路連線：

- vStorage Backup Server
- IBM Spectrum Protect 伺服器
- vCenter Server

此外，Derby 資料庫的埠（預設值 1527）及 GUI Web 伺服器的埠（預設值 9081）必須可用。

配置

您可以將多個 vSphere GUI 登錄至單一 vCenter Server。 此實務範例減少單一 VMware vSphere GUI 所管理的資料中心（以及其虛擬機器訪客）的數目。 vCenter Server 隨後可以管理 vCenter Server 上所定義資料中心數目總計的一部分。

若要更新受管理的資料中心，請跳至**配置** > **編輯配置**。

當您將多個 vSphere GUI 登錄至單一 vCenter Server 時，適用下列準則：

- 每一個資料中心只能由一個已安裝的 vSphere GUI 管理。
- 每一個已安裝的 vSphere GUI 都需要唯一的 VMCLI 節點名稱。
- 對每一個已安裝的 vSphere GUI 使用唯一的資料移轉裝置節點名稱可簡化節點管理。

存取 vSphere GUI

vSphere GUI 的存取方法如下：

- 獨立式 Web 瀏覽器 GUI。 這個 GUI 是透過 GUI Web 伺服器的 URL 書籤來存取，例如：

  `https://hostname:port/TsmVMwareUI/`

  其中：

  - *hostname* 是安裝了 Data Protection for VMware vSphere GUI 的系統名稱
  - *port* 是可透過其來存取 vSphere GUI 的埠號。 預設埠號是 9080。 若為安全埠，則預設值是 9081。
- vSphere Web Client 延伸，其連接至 GUI Web 伺服器以存取 IBM 儲存體中的虛擬機器（又稱為資料保護延伸）。內容是 Web 瀏覽器 GUI 中所提供項目的子集。

在安裝期間，您可以指定一或多種存取方法。

Windows 預設安裝目錄是 `C:\IBM\SpectrumProtect\webserver`。

Linux 預設安裝目錄是 `/opt/tivoli/tsm/tdpvmware/common/webserver`。

IBM Spectrum Protect 回復代理程式

使用回復代理程式服務可從 IBM Spectrum Protect 伺服器裝載任何 Snapshot 磁區。

概觀

您可以使用 iSCSI 通訊協定，從遠端系統存取 Snapshot。

如果您需要在本端檢視在用戶端系統上具有唯讀存取權的 Snapshot，請使用 Data Protection for VMware 8.1.4 版或更舊版本。

此外，回復代理程式還提供即時還原功能及訪客內應用程式保護。 即時還原可讓使用中的磁區在還原作業於背景中進行時保持可用。 應用程式保護可讓安裝在訪客虛擬機器（如 Microsoft Exchange Server 及 Microsoft SQL Server）中的應用程式可供用於備份及還原保護。

回復代理程式可以從遠端系統完成下列作業：

- 收集可以還原之資料的相關資訊，例如：
  - 已備份的虛擬機器。
  - 可供用於已備份的虛擬機器的 Snapshot。
  - 特定 Snapshot 中的可用分割區。

如需指令、參數及回覆碼的相關詳細資訊，請參閱《*IBM Spectrum Protect for Virtual Environments*：*Data Protection for VMware* 使用手冊》中的指令參照區段。

需求

Windows 在 Windows 系統上，回復代理程式 GUI 和指令行介面是在執行 Data Protection for VMware 的完整安裝期間或在資料移轉裝置的進階安裝期間安裝的。

存取回復代理程式

Windows 您可以從**開始**功能表存取回復代理程式：**開始** > **IBM Spectrum Protect** > **IBM Spectrum Protect for Virtual Environments** > **IBM Spectrum Protect 回復代理程式**

IBM Spectrum Protect vSphere Client 外掛程式

IBM Spectrum Protect vSphere Client 外掛程式是 VMware vSphere Web 用戶端延伸，它會提供 Data Protection for VMware vSphere GUI 的視圖。

概觀

IBM Spectrum Protect vSphere Client 外掛程式 提供 Data Protection for VMware vSphere GUI 的瀏覽器視圖中包含的功能子集，以及部分其他功能。

需求

若要安裝 IBM Spectrum Protect vSphere Client 外掛程式，當您執行 IBM Spectrum Protect for Virtual Environments 配置精靈時，必須選取下列選項。

- 在配置精靈的 **vCenter 設定**頁面上，選取**更新登錄**，向關聯的 vCenter 登錄外掛程式。

- 輸入 GUI 主機位址、vCenter 使用者與密碼。

  註：預設網域基於本端網域位址，因此可能無法從外部存取。 如果需要從外部存取，請指定可由 DNS 解析的 GUI 主機位址或 IP 位址。

完成精靈後，外掛程式將向 vCenter 進行登錄。

存取資料保護外掛程式

您可從 vSphere Web 用戶端存取外掛程式：

1. 使用 vCenter 認證登入 vSphere Web 用戶端。資料保護外掛程式位於主功能表 **IBM Spectrum Protect** 下方。
2. 選取此功能表項目會將您移至 IBM Spectrum Protect 延伸的主要區域。與 vCenter 庫存中特定項目相關聯的**監視**及**配置**區段也將具有 IBM Spectrum Protect for Virtual Environments 功能。

Data Protection for VMware 指令行介面

Data Protection for VMware CLI 是隨 Data Protection for VMware vSphere GUI 一起安裝的一個全功能指令行介面。

概觀

您可以使用 Data Protection for VMware CLI 來完成下列作業：

- 起始或排程 VM 備份至 IBM Spectrum Protect 伺服器。
- 從 IBM Spectrum Protect 伺服器起始 VM、VM 檔案或 VM 磁碟 (VMDK) 的完整回復。
- 檢視有關備份資料庫和環境的配置資訊。

雖然 Data Protection for VMware vSphere GUI 是主要作業介面，但 Data Protection for VMware CLI 還提供了有用的次要介面。

例如，Data Protection for VMware CLI 可用來實作不同於 Data Protection for VMware vSphere GUI 所實作的排程機制。 此外，當使用 Script 來評估自動化結果時，Data Protection for VMware CLI 也會非常有用。

存取 Data Protection for VMware 指令行介面

您可以從指令行存取 Data Protection for VMware CLI。

如需可用指令的相關詳細資訊，請參閱《*IBM Spectrum Protect for Virtual Environments*：*Data Protection for VMware* 使用手冊》中的指令參照區段

IBM Spectrum Protect 檔還原介面

您可以從 VMware 虛擬機器備份還原個別檔案。

概觀

檔案還原介面是一種 Web 型介面，您可以在其中從虛擬機器備份還原個別檔案。 此介面的優點是，檔案、軟體及平台擁有者不需要先擁有 IBM Spectrum Protect 備份及還原作業的知識，就可以還原他們自己的檔案。

當您在 vSphere 環境中選取此選項來保護資料時，就會安裝檔案還原介面功能。 在 Data Protection for VMware 配置精靈中，您必須啟用檔案還原功能，才有此介面可用。

存取 IBM Spectrum Protect 檔案還原介面

若要存取檔案還原介面，請開啟 Web 瀏覽器，然後輸入管理者所提供的 URL。 例如：

`https://`*`hostname`*`:9081/FileRestoreUI`

其中 *hostname* 是安裝 Data Protection for VMware vSphere GUI 之系統的主機名稱。

資料移轉裝置功能

資料移轉裝置是將資料移至或移出 IBM Spectrum Protect 伺服器 的 Data Protection for VMware 軟體元件。

概觀

在一般 VMware 環境中，資料移轉裝置用於將虛擬機器備份儲存到資料中心節點。

當您安裝 Data Protection for VMware 時，資料移轉裝置包括在安裝中。 資料移轉裝置與 Data Protection for VMware vSphere GUI 及其他 Data Protection for VMware 元件安裝在同一系統上。

您也可以將資料移轉裝置獨立於其他 Data Protection for VMware 元件，安裝在遠端系統上，從而在多個系統之間重新配送備份工作量。

VMware 環境中不支援 Snapshot 差異備份作業。 您無法在也安裝 Data Protection for VMware 資料移轉裝置之主機的 NetApp 編檔器上，對檔案系統執行 Snapshot 差異備份作業。

設定資料移轉裝置

如需計劃、安裝及配置資料移轉裝置的相關資訊，請檢閱下列清單：

動作	說明
判定保護 vSphere 環境所需的資料移轉裝置數目。	可能需要多個資料移轉裝置節點以保護您的 vSphere 環境。 若要判定所需要的資料移轉裝置節點數目，請參閱 Technote 2007197。 此 Technote 也包括將虛擬或實體機器用於資料移轉裝置節點及資料移轉裝置地區的考量。

動作	說明
安裝 Data Protection for VMware。	若要安裝 Data Protection for VMware，請執行 Data Protection for VMware 安裝程式，並為 Windows 作業系統選取**一般安裝**，或者為 Linux 作業系統選取**完整**。 此安裝選項會安裝所有 Data Protection for VMware 元件，其中包括資料移轉裝置。 如需如何執行 Data Protection for VMware 安裝程式的相關資訊，請參閱第 19 頁的『安裝 Data Protection for VMware 元件』。
定義環境的資料移轉裝置。	Data Protection for VMware 安裝精靈完成後，Data Protection for VMware vSphere GUI 配置精靈會開啟，可讓您設定與 IBM Spectrum Protect 伺服器 的通訊。 在配置精靈的「Data Mover Nodes」頁面上，定義本端資料移轉裝置及您將在個別系統上安裝之任何遠端資料移轉裝置的資訊。 如果您在 Windows 作業系統上進行安裝，並在定義資料移轉裝置時選取**建立服務**，則資料移轉裝置的配置資訊會儲存在下列位置的選項檔案中： `C:\Program Files\Tivoli\TSM\baclient\` 此外，系統會配置資料移轉裝置所需要的服務。 如果您在 Linux 作業系統上安裝資料移轉裝置，或者在 Windows 作業系統上進行安裝，但是在配置期間未選取**建立服務**，則必須完成第 83 頁的『使用 vSphere 外掛程式 GUI 設定資料移轉裝置節點』中的下列步驟，以建立選項檔案及配置所需要的服務。
在遠端系統上安裝及配置其他資料移轉裝置（必要的話）。	若要在遠端系統上安裝資料移轉裝置，請執行 Data Protection for VMware 安裝程式，並採取下列其中一個動作： 在 Windows 作業系統上的配置精靈中，選取**進階安裝** > **僅安裝資料移轉裝置特性**。 在 Linux 作業系統上，從配置精靈的**安裝集**清單中選取**自訂**。 確保已選取 **Data Protection for VMware 資料移轉裝置**。 依預設，會選取這個選項。 安裝完成後，要在遠端系統上設定資料移轉裝置，請遵循第 83 頁的『使用 vSphere 外掛程式 GUI 設定資料移轉裝置節點』中的指示。

規劃安裝 Data Protection for VMware

Data Protection for VMware 可消除在虛擬機器上執行備份的影響，因為將備份工作量從 VMware ESXi 型主機卸載到「vStorage 備用伺服器」。

Data Protection for VMware 與整合的資料移轉裝置一起運作，以完成 VM 的持續增量完整及持續增量增量備份。 該資料移轉裝置節點會將資料移至 IBM Spectrum Protect 伺服器以進行儲存，並在稍後進行 VM 映像檔層次的還原。 可以在磁碟區層次及完整虛擬機器層次上進行即時還原。

提示：資料移轉裝置是分開授權的元件，其中包含其自己的使用者介面和說明文件。 熟悉此產品及其說明文件是必要的，以便將用於保護虛擬機器的完備計劃與 Data Protection for VMware 適當整合。 Data Protection for VMware for Windows 64 位元包括資料移轉裝置功能。

安裝導覽圖

下表列出完成成功安裝處理程序的步驟。

表 2. 適用於 *Data Protection for VMware* 新客戶或現有客戶的安裝作業

步驟	作業	從此處開始
1	檢查系統需求。	確保要安裝 Data Protection for VMware 的系統符合系統需求。
2	檢查使用者許可權需求。	藉由使用所需要的使用者許可權層次，避免潛在的安裝錯誤或延遲。
3	檢查所需通訊埠的可用性。	透過先開啟所需要的通訊埠，再嘗試安裝 Data Protection for VMware，防止安裝失敗或延遲。
4	安裝 Data Protection for VMware： • 使用安裝精靈來安裝 Data Protection for VMware • 第 24 頁的『以無聲自動模式安裝 Data Protection for VMware 元件』 升級 Data Protection for VMware： 升級 Data Protection for VMware	每一個安裝套件都會附送一個使用者授權檔 (EULA)。 如果您不接受這個檔案，則安裝會結束。
5	第 39 頁的『使用精靈配置新的安裝』 如果您打算升級 Data Protection for VMware，則視已安裝的元件而定，可能需要更多的配置作業。如需詳細資料，請參閱《*IBM Spectrum Protect for Virtual Environments*：*Data Protection for VMware* 使用手冊》中的配置主題。	使用配置精靈執行起始配置。 視安裝的功能而定，可能需要執行此章節中說明的其他配置作業。

提示：為協助規劃您特定 Data Protection for VMware 備份環境所需要的 Proxy 主機數量，在 IBM Spectrum Protect Wiki 上提供了下列出版品：
Step by Step Guide To vStorage Backup Server (Proxy) Sizing
此出版品在 IBM Spectrum Protect for Virtual Environments 產品區段中提供。

安裝實務範例

在安裝 Data Protection for VMware 之前，請選擇最符合您商業需求的實務範例。

您可以使用 GUI 或在無聲自動模式中安裝 Data Protection for VMware 及資料移轉裝置：

- 第 21 頁的『使用安裝精靈來安裝 Data Protection for VMware 元件』
- 第 24 頁的『以無聲自動模式安裝 Data Protection for VMware 元件』

如需可用的（依平台）功能和元件清單，請參閱第 1 頁的『可安裝的元件』。

表 3. 安裝實務範例

實務範例編號	說明	您必須完成的作業
1	如果是要在同一個系統上安裝 Data Protection for VMware 及資料移轉裝置的新安裝，請使用此實務範例。	Windows 您可以在 GUI 或無聲自動模式下使用 Suite Installer。 Linux 您可以在 GUI 或無聲自動模式下使用 InstallAnywhere。
2	當您想要在此系統上安裝資料移轉裝置（裝載 Proxy）、回復代理程式及所需要的支援套件時，使用此實務範例。	Windows 您可以使用 Suite Installer 完成進階安裝。 Linux 現在，資料移轉裝置特性已隨 Data Protection for VMware 一起安裝。

系統需求

若要實作 Data Protection for VMware 元件，您的系統必須符合適當的系統需求。

軟體需求

軟體及作業系統需求的詳細資料會隨著時間而變更。 如需最新的軟體需求，請參閱 Technote 1505139。

硬體需求

硬體需求是根據下列項目而定：

- 受保護的伺服器數
- 受保護的磁區數
- 資料集大小
- LAN 和 SAN 連線功能

註：Recovery Agent 元件不支援不需 LAN 的環境中的作業。

下表將說明安裝 Data Protection for VMware 的硬體需求：

表 4. *Data Protection for VMware* 的硬體需求。

元件	需求下限	偏好採用
系統	IntelPentium D 雙核心處理器或相容項目	不適用

表 *4. Data Protection for VMware* 的硬體需求。 *(繼續)*

元件	需求下限	偏好採用
記憶體	4 GB RAM、4 GB 虛擬位址空間	不適用
可用的硬碟	4.4 GB	9.0 GB
網路	1 GbE	10 GbE

註：根據平行處理程序的數目，虛擬機器的備份花費大量記憶體。

記憶體需求可以透過 **dsmc backup vm** 指令進行延伸，並且可以透過下列公式進行計算：

Required memory = (DiskSize / MBLKSize) * ReadBufferSize * VMMAXPARALLEL

其中：

- **DiskSize** 是並行處理的訪客磁碟大小；
- **MBLKSize** 是組合區塊大小。 對於小於 2 TB 的磁碟，它等於 128 MB，對於大於 2 TB 的磁碟，它等於 1 GB。
- **ReadBufferSize** 是用來容納 MBLK 資訊的 IBM Spectrum Protect 內部緩衝區大小。 緩衝區大小等於 256 KB；
- **VMMAXPARALLEL** 是單一備份作業處理程序可以在任何時間一次備份的虛擬機器數目上限。

例如，若要備份 10 個訪客，每個具有 40 GB 磁碟，並在單一備份作業處理程序中執行 VMMAXPARALLEL 2，將需要：

- **DiskSize** = 40 GB = 41943040 KB；
- **MBLKSize** = 128 MB = 131072 KB；
- **ReadBufferSize** = 256 KB；
- **VMMAXPARALLEL** = 2。

所需要記憶體 = (41943040 / 131072) * 256kB * 2 = 163840KB = 160MB。

註：若要在五個平行備份作業處理程序中使用 'VMMAXPARALLEL 2' 備份相同數目的訪客，則（最多）需要上一個範例中所需記憶體的五倍，或者 800 MB。

限制：下列限制適用於備份作業中涉及的 VMware VMDK：

- 對於持續增量增量備份模式，備份作業中涉及的每一個個別 VMDK 都不能超過 8 TB。 如果某個 VMDK 超過 8 TB，則備份作業會失敗。 如果要增加 VMDK 的大小，使其大於預設值 (2 TB)，請使用 vmmaxvirtualdisks 選項來指定大小上限。 如需相關資訊，請在 IBM Knowledge Center 上搜尋 vmmaxvirtualdisks。
- 對於持續增量完整備份模式，備份作業中涉及的每一個個別 VMDK 都不能超過 2 TB。 如果某個 VMDK 超過 2 TB，則備份作業會失敗。

如果要防止任一備份模式期間發生失敗，則可以透過在資料移轉裝置選項檔案中指定 vmskipmaxvirtualdisks yes 來跳過處理 VMDK。 如需相關資訊，請參閱 Vmskipmaxvirtualdisks 。

檔案還原必要條件

在使用 IBM Spectrum Protect Data Protection for VMware 檔案還原介面來還原檔案之前，請確保您的環境符合最低必要條件。

如果要啟用檔案還原功能，則必須將 Data Protection for VMware 安裝在 Windows 系統上。

VMware 虛擬機器必要條件

下列必要條件適用於包含要還原之檔案的 VMware 虛擬機器：

- Linux Windows VMware 工具必須已安裝在虛擬機器上。
- Linux Windows 在檔案還原作業期間，虛擬機器必須處於執行中狀態。
- Windows 資料移轉裝置系統必須與包含所要還原檔案的虛擬機器屬於相同的 Windows 網域，或處於具有信任關係的網域中。
- Windows 將虛擬機器從 Windows 網域中刪除，再在稍後還原時，該虛擬機器必須重新加入網域才能確定網域信任關係。 在還原網域信任關係之前，請勿試圖從虛擬機器進行檔案還原。
- Windows 如果使用者未擁有要還原的檔案，則必須將 Microsoft Windows 的 回存檔案和目錄專用權指派給該虛擬機器的使用者。
- 如需使用 Data Protection for VMware 檔案還原介面所需之 Microsoft Windows 網域帳戶必要條件的進一步資訊，請參閱 Technote 1998066。
- Linux 虛擬機器需要本端使用者鑑別。無法透過 Windows 網域、輕量型目錄存取通訊協定 (LDAP)、Kerberos 或其他網路鑑別方法進行鑑別。
- Linux 在 Red Hat Enterprise Linux 6 作業系統上，sshd 常駐配置檔 (/etc/ssh/sshd_config) 中的 ChallengeResponseAuthentication 選項必須指定 YES 或註銷。例如，下列一項陳述式有效：

  ```
  ChallengeResponseAuthentication yes
  #ChallengeResponseAuthentication no
  ```

  在修改選項之後重新啟動 sshd 常駐程式。

資料移轉裝置必要條件

資料移轉裝置系統表示從一個系統「移動資料」至另一個系統的特定資料移轉裝置。

Windows 資料移轉裝置系統必須與包含所要還原檔案的虛擬機器屬於相同的 Windows 網域。

裝載 Proxy 必要條件

裝載 Proxy 系統代表透過 iSCSI 連線存取已裝載虛擬機器磁碟的 Linux 或 Windows Proxy 系統。 此系統可讓已裝載虛擬機器磁碟上的檔案系統作為還原點，供檔案還原介面進行存取。

Linux Linux 作業系統提供一個常駐程式，來在「邏輯磁區管理程式 (LVM)」磁區群組變成可供系統使用時啟動這些群組。 請在 Linux 裝載 Proxy 系統上設定此常駐程式，以便當 LVM 磁區群組變成可供系統使用時不會啟動這些群組。 如需如何設定此常駐程式的詳細資訊，請參閱適當的 Linux 文件。

Linux Windows Windows 裝載 Proxy 系統與 Linux 裝載 Proxy 系統必須位於相同的子網路上。

Microsoft Windows 網域帳戶必要條件

下列必要條件適用於 Windows 網域帳戶。第一個需求是建立在所有 VM 上具有本端管理權限的 Windows 網域使用者帳戶：

- 若要執行必要的作業以讓虛擬機器訪客能夠進行檔案回復，則您需要一個屬於 Windows 網域且是裝載 Proxy 系統上本端管理者的使用者帳戶。具有此帳戶的管理者在 Data Protection for VMware vSphere GUI 配置精靈或記事本中輸入帳戶認證以啟用進行檔案還原作業的環境。
- 若要建立具有足夠專用權以使用檔案還原介面的使用者帳戶，您可以使用 Windows 群組原則物件來集中管理單一網域使用者，讓它使用本端管理者認證來存取多個機器，以及選擇性地限制不需要的動作。

下列步驟說明如何建立這個使用者帳戶。在網域控制站上，使用 Active Directory 使用者和電腦 MMC 嵌入式管理單元，完成下列步驟：

1. 選取**動作->新建->群組**，並建立名為 **FR Admins** 的新安全群組。群組範圍應該設定為 Global。
2. 建立使用者名稱為 fradmin1 的新網域使用者帳戶，並將其新增至 **FR Admins** 安全群組。您還可以將其他網域使用者帳戶新增至此群組。
3. 若要更好地控制 fradmin1 可以存取的電腦集，請建立新的組織單位
4. 從網域物件中，選取**新建->組織單位**，將其命名為 FR Computers
5. 在 FR Computers 組織單位中移入一些機器。 .

在網域控制站上從群組原則 MMC 嵌入式管理單元中完成下列步驟：

1. 建立新的群組原則物件 FR Admin GPO，該物件會將 **FR Admins** 群組中的管理者，新增至與該群組原則物件所適用之組織單位相關聯的電腦本端管理者群組中。
2. 在群組原則物件中，將該帳戶新增至本端管理者群組以及（選擇性地）遠端桌面使用者。
3. 選取 FR Computers 組織單位並新增最新建立的群組原則物件。

   註：該群組原則物件自身可能已與網域相關聯，但隨後 fradmin1 可能會在該網域中所有電腦的本端管理者群組中。使用明確的組織單位可以提供額外控制。
4. 選用項目：使用群組原則管理來限制本端機器上的不必要動作，例如 Deny log on locally 和 Deny log on through Terminal Services。
5. 在 Data Protection for VMware vSphere GUI 配置精靈或記事本的「檔案還原」頁面中，更新設定以使用在上述步驟中建立的 domain\fradmin1 帳戶。
6. 重新啟動裝載 Proxy 用戶端存取常駐程式 (CAD) 服務。

當您設定了具有適當專用權的帳戶時：

- Windows 在 Data Protection for VMware vSphere GUI 配置精靈或記事本中輸入您的認證以啟用進行檔案還原作業的環境。
- Windows 檔案擁有者使用 Windows 網域使用者認證來存取遠端虛擬機器（其中包含要還原的檔案）。 在登入期間，於檔案還原介面中輸入這些認證。 網域使用者認證會驗證檔案擁有者是否有權登入遠端虛擬機器及遠端虛擬機器中的還原檔案。 這些認證不需要任何特殊許可權。
- Windows 如果檔案擁有者所使用的 Windows 網域使用者帳戶只能存取特定電腦（而不是可以存取該網域內的所有電腦），請確保裝載 Proxy 系統併入此網域使用者帳戶可存取的電腦清單中。 否則，檔案擁有者無法登入檔案還原介面。

磁帶媒體必要條件

不支援從磁帶媒體進行檔案還原。 偏好方法是從磁碟儲存體進行檔案還原。

必要的安裝權限

開始安裝之前，請確保使用者 ID 包含必要的權限層次。

關於這項作業

表 5. 安裝及配置 *Data Protection for VMware* 之前所需的使用者權限

系統	**必要的權限**
Windows	管理者
Linux	Root
vCenter Server	管理者專用權 vCenter Server 角色需要下列專用權：**延伸** > **登錄延伸**、**取消登錄延伸**、**更新延伸**。必須針對安裝期間指定的使用者 ID，將此新角色套用至 VMware vCenter Server 階層中的 vCenter 物件。
IBM Spectrum Protect 伺服器 **限制：**必須啟動伺服器。	管理存取權 （**系統**或**未限定原則網域**專用權）

必要通訊埠

檢視在安裝 Data Protection for VMware 時必須在防火牆中開啟的通訊埠清單。

表格中識別的埠反映一般安裝。 一般安裝由相同的 Windows 系統上的下列元件所組成：

- Data Protection for VMware GUI 伺服器
- vStorage 備用伺服器（資料移轉裝置）
- Windows 裝載 Proxy
- IBM Spectrum Protect 檔還原介面

如果使用非一般安裝，則可能需要更多埠。

限制：Windows 裝載 Proxy 和 Linux 裝載 Proxy 必須位於同一個子網路上。

表 *6.* 必要通訊埠. 此表格識別 Data Protection for VMware 所存取的埠。

TCP 埠	起始器：出埠（從主機）	目標：入埠（到主機）
443	vStorage Backup Server	vCenter Server（安全 HTTP）
443	Data Protection for VMware vSphere GUI 伺服器	vCenter Server
443 只有在資料移轉裝置是 Linux 系統時才需要此設定。	Windows 裝載 Proxy	vCenter Server
443	vStorage 備份伺服器	平台服務控制器
443	Data Protection for VMware vSphere GUI 伺服器	平台服務控制器
443	Windows 裝載 Proxy	平台服務控制器
902 443	vCenter 伺服器	ESXi 主機
902 443	vStorage Backup Server (Proxy)	ESXi 主機（所有受保護的主機）
1500 (**tcpport**)	vStorage Backup Server (Proxy)	IBM Spectrum Protect 伺服器
1500 (**tcpadminport**)	Data Protection for VMware vSphere GUI 伺服器 • 1500 (**tcpadminport**) 是非 SSL 通訊 • 針對 SSL 通訊，**tcpadminport** 是唯一支援與 IBM Spectrum Protect 伺服器進行 SSL 通訊的埠。要用於 SSL 通訊協定的正確埠號通常是由 IBM Spectrum Protect 伺服器 dsmserv.opt 檔中的 **ssltcpadminport** 選項所指定的值。 不過，如果 dsmserv.opt 檔中指定了 **adminonclient no**，則要用於 SSL 通訊協定的正確埠號是由 **ssltcpadminport** 選項所指定的值。**ssltcpadminport** 選項沒有預設值。因此，此值必須由使用者指定。	IBM Spectrum Protect 伺服器
1527 內部 Derby 資料庫		
1501 1581 (**httpport**)	IBM Spectrum Protect 伺服器	vStorage Backup Server • 資料移轉裝置排程器 • Web 用戶端 • Client Acceptor 常駐程式

表 6. 必要通訊埠 (繼續). 此表格識別 Data Protection for VMware 所存取的埠。

TCP 埠	起始器：出埠（從主機）	目標：入埠（到主機）
1581 (**httpport**) 1582、1583 (**webports**)	Data Protection for VMware vSphere GUI 伺服器	vStorage 備份伺服器
9081 GUI Web 伺服器（HTTPS 通訊協定）	vSphere 用戶端	Data Protection for VMware vSphere GUI Server（用於透過 Web 瀏覽器存取 vCenter 的安全 HTTPS 埠）
22 回復代理程式的 SSH 預設埠	回復代理程式	Data Protection for VMware Windows「裝載」主機 • Linux 回復代理程式的 SSH
3260	Linux Data Protection for VMware 檔案還原	Data Protection for VMware Windows「裝載」主機 • iSCSI
3260 回復代理程式的 iSCSI 預設埠	Windows 目標，具有檔案還原的動態磁碟	Data Protection for VMware Windows「裝載」主機 • iSCSI
5985	檔案還原 GUI 作業	Windows 遠端管理
135	Windows 裝載 Proxy	包含要利用 IBM Spectrum Protect 檔案還原介面還原之檔案的 VMware 虛擬機器

VMware vCenter Server 使用者專用權需求

執行 Data Protection for VMware 作業需要某些 VMware vCenter Server 專用權。

使用 Data Protection for VMware vSphere GUI 的 Web 瀏覽器視圖保護 VMware 資料中心所需的 vCenter Server 專用權

登入 Data Protection for VMware vSphere GUI 之瀏覽器視圖的 vCenter Server 使用者 ID

必須具有足夠的 VMware 專用權，以檢視 GUI 管理之資料中心的內容。

例如，VMware vSphere 環境包含五個資料中心。 使用者 『jenn』 只具有其中兩個資料中心的足夠專用權。 因此，『jenn』 在視圖中只能看到其具有足夠專用權的那兩個資料中心。 使用者 『jenn』 無法看到其他三個資料中心（『jenn』 沒有它們的足夠專用權）。

VMware vCenter Server 將一組專用權統一定義為角色。 角色會套用至指定使用者或群組的物件以建立專用權。 從 VMware vSphere Web 用戶端中，您必須建立具有一組專用權的角色。 若要建立 vCenter Server 角色以進行備份及還原作業，請使用 VMware vSphere Client 的**新增角色**功能。

如果您要將專用權延伸到 vCenter 內的所有資料中心，請指定 vCenter Server 並選取延伸到子項勾選框。 否則，如果您在選取延伸到子項勾選框的情況下僅將角色指派給所需的資料中心，則會限制許可權。 瀏覽器 GUI 的強制執行位於資料中心層次。

下列範例顯示如何控制對兩個 VMware 使用者群組的資料中心進行存取。 首先建立一個角色，以包含 Technote 7047438 中定義的所有專用權。 此範例中的這組專用權由名稱為 『TDPVMwareManage』 的角色識別。 群組 1 需要存取權才能管理 Primary1_DC 及 Primary2_DC 資料中心的虛擬機器。 群組 2 需要存取權才能管理 Secondary1_DC 及 Secondary2_DC 資料中心的虛擬機器。

針對群組 1，將 『TDPVMwareManage』 角色指派給 Primary1_DC 和 Primary2_DC 資料中心。 針對群組 2，將 『TDPVMwareManage』 角色指派給 Secondary1_DC 和 Secondary2_DC 資料中心。

每一個 VMware 使用者群組中的使用者都可以使用 Data Protection for VMware GUI，來僅管理其各自資料中心內的虛擬機器。

提示：建立角色時，請考量將額外專用權新增至您稍後對物件完成其他作業時可能需要的角色。

使用資料移轉裝置所需的 vCenter Server 專用權

安裝在 vStorage 備份伺服器（資料移轉裝置節點）上的 IBM Spectrum Protect 資料移轉裝置需要 VMCUser 和 VMCPw 選項。 VMCUser 選項指定您要備份、還原或查詢之 vCenter 或 ESX 伺服器的使用者 ID。 指派給此使用者 ID (VMCUser) 的必要專用權可確保用戶端能夠在虛擬機器及 VMware 環境上執行作業。 這個使用者 ID 必須擁有上方 Technote 中所說明的 VMware 專用權。

若要建立 vCenter Server 角色以進行備份及還原作業，請使用 VMware vSphere Client 的**新增角色**功能。 新增此使用者 ID (VMCUser) 的專用權時，必須選取延伸到子項選項。 此外，請考量新增其他專用權給此角色以用於備份及還原以外的作業。 對於 VMCUser 選項，強制執行是在最上層物件層次進行。

使用 Data Protection for VMware vSphere GUI 的 IBM Spectrum Protect vSphere Client 外掛程式視圖保護 VMware 資料中心所需的 vCenter Server 專用權

IBM Spectrum Protect vSphere Client 外掛程式需要一組不同於登入 GUI 所需專用權的專用權。

在安裝期間，會為 IBM Spectrum Protect vSphere Client 外掛程式建立下列自訂專用權：

- **資料中心** > **IBM Data Protection**
- **廣域** > **配置 IBM Data Protection**

IBM Spectrum Protect vSphere Client 外掛程式所需的自訂專用權會登錄為個別延伸。專用權延伸索引鍵是 com.ibm.tsm.tdpvmware.IBMDataProtection.privileges。

這些專用權容許 VMware 管理者啟用及停用對 IBM Spectrum Protect vSphere Client 外掛程式內容的存取。 只有具備所需 VMware 物件之上述自訂專用權的使用者才能存取 IBM Spectrum Protect vSphere Client 外掛程式內容。 會對每一個 vCenter

Server 登錄一個 IBM Spectrum Protect vSphere Client 外掛程式，且它由配置為支援 vCenter Server 的所有 GUI 主機共用。

從 VMware vSphere Web 用戶端中，您必須針對可使用 IBM Spectrum Protect vSphere Client 外掛程式來完成虛擬機器資料保護功能的使用者，建立一個角色。 針對此角色，除了 Web 用戶端所需的標準虛擬機器管理者角色專用權之外，您還必須指定**資料中心** > **IBM Data Protection** 專用權。 針對每一個資料中心，對您要為其授與許可權的每一個使用者或使用者群組指派此角色，以讓該使用者管理虛擬機器。

vCenter 層次的使用者需要**廣域** > **IBM Data Protection** 專用權。 此專用權容許使用者管理、編輯或清除 vCenter Server 與 Data Protection for VMware vSphere GUI Web 伺服器之間的連線。 請將此專用權指派給熟悉保護其各自 vCenter Server 之 Data Protection for VMware vSphere GUI 的管理者。 您可在該延伸的「連線」頁面上管理 IBM Spectrum Protect vSphere Client 外掛程式連線。

下列範例顯示如何針對兩個使用者群組控制對資料中心的存取。 群組 1 需要管理 NewYork _DC 和 Boston_DC 資料中心的虛擬機器所需的存取權。 群組 2 需要管理 LosAngeles_DC 和 SanFranciso_DC 資料中心的虛擬機器所需的存取權。

從 VMware vSphere 用戶端中，以建立 『IBMDataProtectManage』 角色為例，指派標準虛擬機器管理者角色專用權以及**資料中心** > **IBM Data Protection** 專用權。

針對群組 1，將 『IBMDataProtectManage』 角色指派給 NewYork 和 Boston_DC 資料中心。 針對群組 2，將 『IBMDataProtectManage』 角色指派給 LosAngeles_DC 和 SanFranciso_DC 資料中心。

每一個群組中的使用者都可以在 vSphere Web 用戶端中使用 IBM Spectrum Protect vSphere Client 外掛程式，以僅管理其各自資料中心內的虛擬機器。

與許可權不足相關的問題

當 Web 瀏覽器使用者沒有任何資料中心的足夠許可權時，即會封鎖對視圖的存取。 系統會發出錯誤訊息 GVM2013E，以告知使用者未獲授權來存取任何受管理資料中心，原因是許可權不足。 也會提供其他新訊息來通知使用者許可權不足導致的問題。 若要解決任何與許可權相關的問題，請確保已如之前的小節所述設定使用者角色。 該使用者角色必須具有「vCenter Server 使用者 ID 及資料移轉裝置的必要專用權」表格中所識別的所有專用權，並且這些專用權必須在資料中心層次套用且選取了延伸到子項勾選框。

當 IBM Spectrum Protect vSphere Client 外掛程式使用者沒有資料中心的足夠許可權時，該資料中心及其內容的資料保護功能將變成在該延伸中無法使用。

當 IBM Spectrum Protect 使用者 ID（由 VMCUser 選項指定）包含的許可權不足以進行備份及還原作業時，會顯示下列訊息：

```
ANS9365E VMware vStorage API 錯誤。
「執行此作業的許可權遭到拒絕。」
```

當 IBM Spectrum Protect 使用者 ID 包含的許可權不足以檢視機器時，會顯示下列訊息：

```
備份 VM 指令已啟動。  要處理的虛擬機器總數：1
ANS4155E 在 VMware 伺服器上找不到虛擬機器 'tango'。
ANS4148E 虛擬機器 'foxtrot' 的完整 VM 備份失敗，RC 為 4390
```

如需專用權使用的進一步資訊，請參閱 **Data Protection for VMware vSphere GUI 及資料移轉裝置所需要的 vCenter Server 專用權**上的附註。

若要透過 VMware Virtual Center Server 擷取許可權問題的日誌資訊，請完成下列步驟：

1. 在「vCenter Server 設定」中，選取**記載選項**並將 **vCenter 記載**設定為 **Trivia (Trivia)**。
2. 重建許可權錯誤。
3. 將 **vCenter 記載**重設為其前一個值以防止記錄過多的日誌資訊。
4. 在「系統日誌」中，尋找最新的 vCenter Server 日誌 (vpxd-*wxyz*.log) 並搜尋字串 NoPermission。 例如：

   ```
   [2011-04-27 15:15:35.955 03756 verbose 'App'] [VpxVmomi] Invoke error:
   vim.VirtualMachine.createSnapshot session: 92324BE3-CD53-4B5A-B7F5-96C5FAB3F0EE
   Throw: vim.fault.NoPermission
   ```

   此日誌訊息指出該使用者 ID 未包含足夠許可權來建立 Snapshot (createSnapshot)。

安裝 Data Protection for VMware 元件

您可安裝適用於您作業系統之 Data Protection for VMware 套件中提供的全部或部分元件。

關於這項作業

藉由使用 Data Protection for VMware 安裝程式，可安裝下列元件：

- IBM Spectrum Protect Recovery Agent
- Windows Recovery Agent 指令行介面
- Windows 說明文件（Readme 檔及注意事項檔案）
- Data Protection for VMware 啟用檔案
- Data Protection for VMware vSphere GUI
- 資料移轉裝置特性，其中包括下列項目：
  - 資料移轉裝置 GUI
  - 資料移轉裝置 Web 用戶端
  - 用戶端 API（64 位元）執行時期檔案
  - 管理用戶端指令行
  - VMware vStorage API 執行時期檔案

當您想要安裝資料移轉裝置（裝載 Proxy）、回復代理程式及必要支援套件時，您可以選擇完整安裝，或者使用「進階安裝」選項。

提示：您可在 Data Protection for VMware 軟體所在的相同系統上建立多個資料移轉裝置，也可在遠端系統上建立資料移轉裝置。 此配置會增加可供 Data Protection for VMware 使用的資源。 已安裝資料移轉裝置的系統稱為 vStorage 備份伺服器。

取得 Data Protection for VMware 安裝套件

可以從 IBM 下載網站（例如 IBM Passport Advantage®）取得 Data Protection for VMware 安裝套件。

Linux

開始之前

如果計劃下載檔案，請將檔案大小上限的系統使用者限制設為無限制，以確保可以正確地下載這些檔案：

1. 如果要查詢檔案大小上限值，請發出下列指令：

   ```
   ulimit -Hf
   ```

2. 如果檔案大小上限的系統使用者限制未設為無限制，請透過遵循適合您作業系統之說明文件中的指示，將它變更為無限制。

程序

1. 從下列其中一個網站下載適當的套件檔：
   - 如果是第一次安裝或者是新版本，請移至 Passport Advantage，網址為：http://www.ibm.com/software/lotus/passportadvantage/。 Passport Advantage 是唯一可供您下載授權套件檔的網站。
   - 如需最新資訊、更新項目及維護修正程式，請移至 IBM Spectrum Protect 支援網站：http://www.ibm.com/support/entry/portal/Overview/Software/Tivoli/Tivoli_Storage_Manager。
2. 如果從 IBM 下載網站下載了套件，請完成下列步驟：
   a. 將套件檔下載至您所選擇的目錄。 路徑長度不得超過 40 個字元。 請務必將安裝檔案解壓縮至空目錄。 請勿解壓縮至一個含有先前解壓縮檔案或其他任何檔案的目錄中。

   b. Linux 確保給套件設定了執行檔許可權。 必要的話，透過發出下列指令來變更檔案許可權：

      ```
      chmod a+x package_name.bin
      ```

   c. Linux 透過發出下列指令來解壓縮套件：

      ```
      ./package_name.bin
      ```

      其中 *package_name* 是所下載檔案的名稱。

   d. Windows 透過按兩下 *package_name* 來解壓縮套件，其中 *package_name* 是所下載檔案的名稱。

使用安裝精靈來安裝 Data Protection for VMware 元件

使用安裝精靈來安裝 Data Protection for VMware 元件。

關於這項作業

Windows 可以使用 Suite Installer，同時安裝 Data Protection for VMware 和資料移轉裝置。

Linux 可以使用獨立式安裝程式，同時安裝 Data Protection for VMware 和資料移轉裝置。

在 Windows 系統上安裝 Data Protection for VMware 元件

使用安裝精靈來安裝 Data Protection for VMware 元件及特性。

開始之前

安裝 Data Protection for VMware 元件之前，請確保您符合下列需求：

- 具有管理者專用權的使用者 ID。
- 可以使用管理者專用權透過網路連線 VMware vCenter Server 6.x（或更新版本）。
- 透過管理者存取權（**System** 或 **Unrestricted Policy Domain** 專用權）與 IBM Spectrum Protect 伺服器的網路連線功能。 此伺服器必須可用且在執行中。
- 請確保檢閱了下列需求：
  - 第 10 頁的『系統需求』
  - 第 14 頁的『必要的安裝權限』
  - 第 14 頁的『必要通訊埠』

安裝 Data Protection for VMware 之前，必須注意下列選項：

安裝類型

一般安裝

使用一般安裝，會安裝所有 Data Protection for VMware 元件及特性。

進階安裝

「進階安裝」畫面提供選項來安裝個別資料移轉裝置。 該處理程序將在系統上安裝資料移轉裝置（裝載 Proxy）、回復代理程式及所需要的支援套件。 使用此安裝選項以新增個別資料移轉裝置。 此選項還會安裝應用程式保護以啟用個別資料庫的回復。 安裝之後，您可以使用 IBM Spectrum Protect GUI，透過 VMware vSphere 外掛程式配置資料移轉裝置及服務。

關於這項作業

您可以使用 Suite Installer 來安裝 Data Protection for VMware。 Suite Installer 的 `spinstall.exe` 檔案位於安裝套件的根目錄下。

如需可以安裝的元件及特性清單，請參閱第 1 頁的『可安裝的元件』。

程序

如果要安裝 Data Protection for VMware，請從選擇要安裝之元件的 spinstall.exe 檔所在位置完成下列步驟：

1. 按兩下 spinstall.exe 檔。
2. 遵循精靈指示來安裝所選元件。

下一步

若要存取 Data Protection for VMware vSphere GUI，請參閱下列主題：

- 第 27 頁的『存取 Data Protection for VMware vSphere GUI』

第一次啟動 GUI 時，配置精靈會自動顯示。

在 Linux 系統上安裝 Data Protection for VMware

使用 InstallAnywhere 模式在 Linux 系統上安裝 Data Protection for VMware。

開始之前

安裝 Data Protection for VMware 之前，請確保您符合下列需求：

- 繼續作業前，確保使用者 ID 具有必要的權限層次，以及開啟了必要的通訊埠。
- 安裝程序建立了使用者 tdpvmware。必須以使用者 tdpvmware 身分，使用 root 使用者 ID 來發出所有 **vmcli** 指令。
- 以主控台模式安裝時需要 X Window Server。
- 請確保檢閱了下列需求：
  - 第 10 頁的『系統需求』
  - 第 14 頁的『必要的安裝權限』
  - 第 14 頁的『必要通訊埠』

程序

如果要安裝 Data Protection for VMware，請完成下列步驟：

1. 從按裝資料夾根目錄中，將目錄切換至 CD/Linux/DataProtectionForVMware。
2. 從指令行輸入下列指令：

```
./install-Linux.bin
```

結果

如果收到任何警告或錯誤，請檢查日誌檔以取得相關資訊。 請參閱第 77 頁的『日誌檔活動』。

如果由於失敗而無法安裝 Data Protection for VMware，請參閱第 33 頁的『在 Linux 系統上解除安裝 Data Protection for VMware』 中的「手動移除 Data Protection for VMware」程序。

在 Linux 上執行 Data Protection for VMware 的全新安裝

如果 Linux 安裝遭岔斷，通常可以重新啟動安裝。 但是，如果安裝無法重新啟動，就必須進行全新安裝。

關於這項作業

啟動全新安裝之前，請確保已移除產品。 請執行下列步驟來確保全新環境：

程序

1. 如果安裝了 Data Protection for VMware vSphere GUI，請完成下列作業：
   a. 透過發出下列指令來停止 Data Protection for VMware 指令行介面：
      `/etc/init.d/vmcli stop`
   b. 透過發出下列指令來停止「Data Protection for VMware GUI Web 伺服器」：
      `/etc/init.d/webserver stop`
   c. 透過發出下列指令來移除 .rpm 套件：
      `rpm -e TIVsm-TDPVMwarePlugin`
2. 移除「部署引擎」產品項目：
   a. 發出下列指令以列出所有「部署引擎」項目：
      `/usr/ibm/common/acsi/bin/de_lsrootiu.sh`
   b. 發出下列指令以移除所有「部署引擎」項目：
      `/usr/ibm/common/acsi/bin/deleteRootIU.sh <UUID> <discriminant>`
   c. 移除 /var/ibm/common 目錄。
   d. 移除 /usr/ibm/common 目錄。
   e. 移除 acu_de.log 檔（如果存在），以清除 /tmp 目錄。
   f. 移除 /tmp 目錄，其中包含安裝「部署引擎」的使用者 ID。
   g. 移除 /etc/inittab 系統檔中的所有「部署引擎」項目。 這些項目以 #Begin AC Solution Install block 和 #End AC Solution Install block 定界。 請移除這些定界字元之間的所有文字，並且移除定界文字本身。
   h. 移除 /etc/services 系統檔中的所有「部署引擎」參照。
3. 移除失敗安裝中的所有 Data Protection for VMware 檔案：
   a. 移除 *<USER_INSTALL_DIR>* 中的檔案，此路徑是嘗試安裝但失敗的路徑。 例如：/opt/tivoli/tsm/TDPVMware/
   b. 移除任何桌面捷徑。
4. 備份廣域登錄檔 (/var/.com.zerog.registry.xml)。備份此檔案後，移除所有參照 Data Protection for VMware 的標籤。
5. 移除根目錄下包含 TDPVMware 字串的日誌檔。 例如：IA-TDPVMware-00.log 或 IA-TDPVMware_Uninstall-00.log。
6. 移除執行 Data Protection for VMware 指令行介面 的使用者。
   a. 發出下列指令：
      `userdel -r tdpvmware`
   b. 發出下列指令：
      `groupdel tdpvmware`

提示：在某些版本的 Linux 中，如果不存在其他關聯使用者，則 **userdel** 指令也會移群組。 因此，請忽略任何指令相關的失敗訊息。

結果

完成這些步驟後，啟動全新安裝。

以無聲自動模式安裝 Data Protection for VMware 元件

您可以在背景安裝 Data Protection for VMware。 在進行這個無聲自動安裝時，畫面不會出現任何訊息。

關於這項作業

Windows 可以使用 Suite Installer，同時安裝 Data Protection for VMware 和資料移轉裝置。

Linux 可以使用獨立式安裝程式，同時安裝 Data Protection for VMware 和資料移轉裝置。

以無聲自動模式將 Data Protection for VMware 安裝在 Windows 系統上

使用 Suite Installer 以無聲自動模式安裝所有 Data Protection for VMware 元件及資料移轉裝置特性。

開始之前

安裝 Data Protection for VMware 及資料移轉裝置特性前，請確保系統符合下列各節中的需求：

- 第 10 頁的『系統需求』
- 第 14 頁的『必要的安裝權限』
- 第 14 頁的『必要通訊埠』

關於這項作業

限制：所有特性皆安裝至其預設位置。 如果要找出元件的預設安裝目錄，請參閱第 1 頁的『可安裝的元件』中的子主題。

程序

如果要安裝 Data Protection for VMware，請完成下列步驟：

1. 從命令提示字元，發出下列指令：

   ```
   cd extract_folder\TSMVMWARE_WIN
   ```

2. 輸入下列指令：

   ```
   spinstall.exe /silent
   ```

   第一次裝載磁區時，顯示下列訊息：

```
尚未登錄虛擬磁區驅動程式。 回復代理程式現在可以登錄該驅動程式。
在登錄期間，可能會顯示 Microsoft Windows 標誌警告。
請接受此警告，以容許登錄完成。
您要立即登錄虛擬磁區驅動程式嗎？
```

若要繼續進行，請輸入**是**以登錄「虛擬磁區驅動程式」。

相關工作:

第 33 頁的『在無聲自動模式下解除安裝 Data Protection for VMware for Windows』

以無聲自動模式將 Data Protection for VMware 安裝在 Linux 系統上

可以自訂哪些 Data Protection for VMware 特性以無聲自動方式安裝在 Linux 作業系統上。

開始之前

安裝 Data Protection for VMware 之前，請確保您符合下列需求：

- 繼續作業前，確保使用者 ID 具有必要的權限層次，以及開啟了必要的通訊埠。
- 安裝程序建立了使用者 `tdpvmware`。必須以使用者 `tdpvmware` 身分，使用 root 使用者 ID 來發出所有 **`vmcli`** 指令。
- 以主控台模式安裝時需要 X Window Server。
- 請確保檢閱了下列需求：
  - 第 10 頁的『系統需求』
  - 第 14 頁的『必要的安裝權限』
  - 第 14 頁的『必要通訊埠』

關於這項作業

Data Protection for VMware 為 Linux 作業系統提供了下列無聲自動安裝功能：

表 *7. Data Protection for VMware* 無聲自動安裝功能

特性	說明	預設安裝？
Docs	Readme 檔	是
TDPVMwareDM	此特性的安裝包括啟用檔案。 可讓 IBM Spectrum Protect 執行下列備份類型： • 定期增量 VM 備份 • 完整 VM 持續增量備份 • 增量持續增量備份 如果卸載備份工作量，則必須將此檔案安裝在「vStorage 備用伺服器」上。	是
TDPVMwareGUI	Data Protection for VMware vSphere GUI。 **註：**也包括啟用檔案安裝。	否

程序

若要安裝 Data Protection for VMware，請從您解壓縮安裝套件的目錄中完成下列步驟：

1. 開啟 *path*../Linux/DataProtectionForVMware/installer.properties 檔，並解除註解下列項目以授權（其中 *path* 是安裝資料夾）：

   ```
   LICENSE_ACCEPTED=TRUE
   ```

2. 選擇下列其中一種方法來安裝 Data Protection for VMware 元件：
   - 對於預設安裝，請開啟 CD/Linux/DataProtectionForVMware 資料夾並輸入下列指令：

     ```
     ./install-Linux.bin -i silent -DLICENSE_ACCEPTED=true
     ```

   - 對於自訂安裝，請完成下列步驟：
     a. 以適當的值編輯 installer.properties 檔：
        1) 指定 **INSTALL_MODE=Custom**。 確保移除此陳述式中的 # 記號。
        2) 使用 **CHOSEN_INSTALL_FEATURE_LIST** 選項來指定要安裝的特性。 例如，使用下列值來安裝所有特性：

           ```
           CHOSEN_INSTALL_FEATURE_LIST=Docs,TDPVMwareDM,TDPVMwareGUI
           ```

     b. 從 CD/Linux/DataProtectionForVMware 資料夾中，發出下列指令：

        ```
        ./install-Linux.bin -i silent -f installer.properties
        ```

安裝 Data Protection for VMware 之後採取首要步驟

安裝 Data Protection for VMware 之後，準備配置。 配置 Data Protection for VMware 的偏好方法是使用配置精靈。

配置工作表

請使用此工作表來記錄在配置及管理 Data Protection for VMware 時所需要的資訊。此工作表的目的是為了幫助您記住在配置之後指定的值。

表 *8. Data Protection for VMware* 配置工作表

項目	您的值	注意事項
IBM Spectrum Protect 伺服器資訊		
IBM Spectrum Protect 伺服器位址		
IBM Spectrum Protect 伺服器埠		
IBM Spectrum Protect 伺服器管理者 ID/密碼		
IBM Spectrum Protect 伺服器管理埠		
節點定義選項		
要新增至節點的字首		
登錄新節點時要使用的原則網域		
vCenter 節點名稱/密碼		
VMCLI 節點名稱/密碼		
資料中心節點名稱/密碼 **記住：**您可以建立多個資料中心節點。		資料中心節點名稱依序由指定的字首、底線字元、資料中心名稱所組成。 例如：*nodePrefix_datacenterName*

表 *8. Data Protection for VMware* 配置工作表 *(*繼續*)*

項目	您的值	注意事項
vStorage 備用伺服器上的資料移轉裝置節點名稱/密碼 **記住：**您可以建立多個資料移轉裝置節點。		資料移轉裝置節點依序由資料中心節點名稱、底線字元、DM 所組成。 例如：*datacenterNodename*_DM
遠端伺服器上的資料移轉裝置節點名稱/密碼 **記住：**您可以建立多個不在 vStorage 備用伺服器上的資料移轉裝置節點。		
裝載 Proxy 節點 還原資料時會使用裝載 Proxy 節點。	Windows： Linux：	

存取 Data Protection for VMware vSphere GUI

使用 Data Protection for VMware vSphere GUI，在 VMware vCenter 環境中備份、還原及管理虛擬機器。

開始之前

安裝期間必須選取了使用 vSphere 環境來保護資料的選項，然後才能存取 Data Protection for VMware vSphere GUI。

程序

- 如果安裝期間選取了**啟用透過 Web 瀏覽器來存取 GUI** 選項，則可以從瀏覽器存取 Data Protection for VMware vSphere GUI：
  1. 開啟 Web 瀏覽器並輸入下列 URL：

     `https://hostname:port/TsmVMwareUI`

     其中：
     - *hostname* 是安裝了 Data Protection for VMware vSphere GUI 的系統名稱
     - *port* 是可透過其來存取 vSphere GUI 的埠號。 預設埠號是 9080。若為安全埠，則預設值是 9081。
  2. 使用 vCenter 使用者 ID 及密碼來登入。
- 如果安裝期間未選取**啟用透過 Web 瀏覽器來存取 GUI** 選項，則可以透過完成下列步驟來啟動 Data Protection for VMware vSphere GUI：
  1. 開啟 VMware vSphere Client，並使用 vCenter 使用者 ID 及密碼來登入。
  2. 在 vSphere Client 的「解決方案和應用程式」畫面中，按一下 Data Protection for VMware vSphere GUI 圖示。

升級 Data Protection for VMware

您可以從舊版軟體升級 Data Protection for VMware。

如需與舊版的相容性，請參閱 Technote 1993819。

從 7.1.8 版升級：如果在升級處理程序期間顯示一則訊息，詢問您是否想要改寫現有 `jextract` 檔案，請選取**全部皆是**。

升級 Data Protection for VMware

此程序說明如何升級至 Data Protection for VMware 8.1.7 版。

開始之前

重要：此升級程序適用於未安裝 IBM Spectrum Protect Snapshot for VMware 的系統。

必須具有管理者專用權才能升級 Data Protection for VMware。

以下列方式處理現有 Data Protection for VMware vSphere GUI 的更新項目：

- 開始 Data Protection for VMware vSphere GUI 升級程序之前，會先備份參數檔。
- 使用相同的「Derby 資料庫埠號」及「WebSphere® Application Server 預設基本埠號」。
- Linux 設定檔 (`vmcliprofile`) 中的值用於 Data Protection for VMware 指令行介面。

限制：

- Windows 將 IBM Spectrum Protect for Virtual Environments 安裝至非預設位置後，升級程序會將 IBM Spectrum Protect for Virtual Environments 8.1.7 版特性安裝至預設安裝目錄。 無法升級至非預設位置。 請參閱第 1 頁的『可安裝的元件』中的子主題，找出每個特性的預設安裝目錄。
- Linux Windows 升級程序不會安裝新元件。

  比方說，如果舊版只安裝了 Recovery Agent GUI，則升級程序不會安裝 Recovery Agent 指令行介面。 在這種情況下，您必須重新執行安裝程式，然後選取要安裝的遺漏元件。
- Linux Linux 上的 Recovery Agent 版本，必須和 Windows Proxy 上的 Recovery Agent 版本相同。 因此，如果升級 Linux 上的 Recovery Agent，則也必須升級 Windows Proxy 上的 Recovery Agent 版本。

程序

如果要升級 Data Protection for VMware，請完成下列步驟：

1. 停止任何執行中的 Data Protection for VMware 元件與服務。
2. 卸載任何已裝載的虛擬磁區。 可以使用 Recovery Agent GUI 或指令行介面（**mount del** 指令）來卸載磁區。
3. 遵循第 21 頁的『在 Windows 系統上安裝 Data Protection for VMware 元件』中的指示。

註： Linux 如果已安裝資料移轉裝置 6.x 版，則必須將其解除安裝，然後再安裝 8.1.7 版。 遵循主題「解除安裝 IBM Spectrum Protect Linux x86_64 用戶端」中的指示。

4. 下載程式碼套件。
5. 從您儲存程式碼套件的資料夾，啟動升級程序：

   a. Windows 執行 `spinstall.exe` 檔。

   b. Linux 執行 `install-Linux.bin` 檔。

   您只能在機器上安裝一個 Data Protection for VMware vSphere GUI。 因此，同一機器上不容許多個 Data Protection for VMware vSphere GUI。

以無聲自動模式升級 Windows 64 位元系統上的 Data Protection for VMware

您可以在支援的 64 位元作業系統上，無聲自動升級 Data Protection for VMware。

開始之前

將 Data Protection for VMware 6.x 版安裝至非預設位置後，無聲自動升級程序會將 Data Protection for VMware 8.1.7 版特性安裝至預設安裝目錄。 無法以無聲自動方式升級至非預設位置。 請參閱第 1 頁的『可安裝的元件』小節中的子主題，找出每個特性的預設安裝目錄。

程序

如果要升級 Data Protection for VMware，請完成下列步驟：

1. 停止任何執行中的 Data Protection for VMware 元件。
2. 卸載任何已裝載的虛擬磁區。 可以使用 Recovery Agent GUI 或指令行介面（**mount del** 指令）來卸載磁區。
3. 卸載任何已裝載的虛擬磁區。 可以使用 Recovery Agent GUI 或指令行介面（**mount del** 指令）來卸載磁區。
4. 下載程式碼套件。
5. 導覽至 Data Protection for VMware 的資料夾。
6. 從命令提示字元視窗中，輸入下列指令： `spinstall.exe /silent GUI_MODE=vcenter DIRECT_START=1 VCENTER_HOSTNAME=<hostname> VCENTER_USERNAME=<username> VCENTER_PASSWORD=<pass> /debuglog <file_path>`

以無聲自動模式升級 Linux 系統上的 Data Protection for VMware

可以在支援的 Linux 作業系統上，以無聲自動方式升級 Data Protection for VMware。

關於這項作業

將下列 Data Protection for VMware 參數與無聲自動安裝功能一起使用：

表 *9. Data Protection for VMware* 無聲自動安裝升級參數

參數	說明	預設值
VCENTER_HOSTNAME	VCenter 伺服器完整網域名稱或 IP 位址。	無

表 9. *Data Protection for VMware* 無聲自動安裝升級參數 (繼續)

參數	說明	預設值
VCENTER_USERNAME	vCenter 使用者 ID。 此使用者 ID 必須是有權登錄及取消登錄延伸的 VMware 管理者。	無
VCENTER_PASSWORD	vCenter 密碼。	無
DIRECT_START	若要在 Web 瀏覽器中存取 Data Protection for VMware vSphere GUI，請指定 **DIRECT_START=YES**。 透過指向 GUI Web 伺服器的 URL 書籤來存取 Data Protection for VMware vSphere GUI。 如果不想以 Web 瀏覽器存取 Data Protection for VMware vSphere GUI，請指定 **DIRECT_START=NO**。	YES **重要：**升級完成後，無法變更 **DIRECT_START** 值，除非重新安裝產品。

程序

如果要升級 Data Protection for VMware，請完成下列步驟：

1. 請確保沒有作用中的備份、還原或裝載階段作業。
2. 請確保關閉任何現有的 Data Protection for VMware vSphere GUI 或 Recovery Agent GUI。
3. 下載程式碼套件。
4. 從 Data Protection for VMware 資料夾，移至 Linux 資料夾。
5. 從命令提示字元視窗中，輸入帶有偏好參數的 `./install-Linux.bin -i silent -DLICENSE_ACCEPTED=true` 指令。
   例如： `./install-Linux.bin -i silent -DLICENSE_ACCEPTED=true -VCENTER_HOSTNAME=hostname -VCENTER_USERNAME=username -VCENTER_PASSWORD=password -DIRECT_START=yes -REGISTER_PLUGIN=yes`

在 vCenter Server Linked Mode 環境中升級 Data Protection for VMware

必須及時更新所有 Data Protection for VMware GUI 主機，Data Protection for VMware 元件才能支援最新的 VMware Linked Mode 特性。

關於這項作業

註：此資訊特定於 VMware vCenter 上執行的 vSphere 應用程式 6.0、6.5 及 6.7 版。

VMware vCenter Server Linked Mode 是一個可以提供管理區概觀的工具，以便伺服器可以支援更多的虛擬機器。 IBM Spectrum Protect Data Protection for VMware 外掛程式與 Linked Mode 模式中執行的 VMware 相容。 如需此 VMware 特性的相關資訊，請參閱 vCenter Enhanced Linked Mode 中的 VMware 說明文件

當 vCenter 處於 Linked Mode 時，vSphere 使用者介面中會出現一個包含所有 vCenter 的單一視圖。登入任何鏈結至一起的 vCenter 時也可以看到這個相同的使用者介面。 因此，IBM Spectrum Protect Data Protection 外掛程式會顯示在所有 vCenter 上，即使它僅在單一 vCenter 上安裝及配置亦如此。

雖然該外掛程式在每個 vCenter 上皆可見，但該外掛程式的功能僅在具有與其相關聯之 IBM Spectrum Protect Data Protection for VMware GUI 主機的每個 vCenter 上可用。

升級 vCenter Server Linked Mode 環境時，請考量下列問題：

- 使用處於 Linked Mode 的 vCenter 時，第一個升級的 vCenter 將會導致更新層次的外掛程式可見於所有鏈結的 vCenter。 IBM Spectrum Protect Data Protection for VMware 外掛程式已開發為與較低層次版本的單一 GUI 主機相容。 例如，Data Protection for VMware 8.1.6 版外掛程式仍然與 Data Protection for VMware 8.1.4 版 GUI 主機相容。
- 雖然較低層次的 GUI 主機仍然可以使用更新的外掛程式，但更新版本中引進的功能將不起作用。 必須及時更新所有 GUI 主機，才能使用更新外掛程式的完整功能。

範例

在升級至 8.1.6 版之前，vCenter1 和 vCenter2 處於 Linked Mode 中。 它們均具有 IBM Data Protection for VMware GUI 主機。 vSphere 內的外掛程式與 GUI 主機均為 8.1.4 版。

vCenter1 現在升級至 8.1.6 版。 外掛程式與 GUI host1 現在處於 8.1.6 版。 登入 vSphere for vCenter2 的使用者將看到 8.1.6 版外掛程式而不是 8.1.4 版外掛程式。使用者隨後可以導覽至 **IBM Spectrum Protect -> 配置 -> 連線**，並看到 vCenter1 的 GUI 主機為 8.1.6 版，而 vCenter2 GUI 主機仍為 8.1.4 版。

vCenter2 的 Spectrum Protect 外掛程式的運作方式仍然與其在 8.1.4 版中的運作方式相同。 不同之處在於 8.1.6 版的任何新特性無法在 vCenter2 上使用而只能在 vCenter1 上使用，直至 vCenter2 的 GUI 主機完成升級至 8.1.6 版。

解除安裝 Data Protection for VMware

解除安裝 Data Protection for VMware 的程序，與全新安裝和升級版的解除安裝程序一樣。

在 Windows 上解除安裝 Data Protection for VMware

從 Windows 系統解除安裝 Data Protection for VMware 元件並移除檔案和目錄。

開始之前

如果要確保解除安裝成功，請使用下列指引：

- 如果其他 Data Protection for VMware Web GUI 主機使用 IBM Spectrum Protect vSphere Client 外掛程式，請勿取消登錄 Web 用戶端延伸。

關於這項作業

完成解除安裝後，配置檔及內容檔位於 `C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\config` 目錄中。

程序

1. 停止任何執行中的 Data Protection for VMware 元件。
2. 卸載任何已裝載的虛擬磁區。

3. 使用資料移轉裝置 delete backup 指令，刪除任何現有虛擬機器備份。
4. 使用 dsmcutil remove 指令移除任何已安裝的資料移轉裝置服務。

   如需服務清單，請跳至 C:\Program Files\Tivoli\TSM\baclient\，然後執行指令 dsmcutil list。

   使用類似於下列項目的指令移除服務，對所列出的服務採用將加引號的名稱：

   ```
    dsmcutil remove /name:"TSM Remote Client Agent"
   dsmcutil remove /name:"TSM Client Acceptor"
   ```
5. 按一下**開始** > **控制台** > **程式和功能** > **解除安裝程式**。 解除安裝下列程式：
   - IBM Spectrum Protect for Virtual Environments Data Protection for VMware 套組
   - IBM Spectrum Protect for Virtual Environments Data Protection for VMware 授權
   - IBM Spectrum Protect JVM
6. 從檔案系統中移除下列 Data Protection for VMware 檔案及目錄（如果呈現）。 對於r IBM Spectrum Protect for Virtual Environments 8.1.6 版以及更高版本，請刪除：

   ```
   C:\IBM\SpectrumProtect
   C:\Program Files\IBM\SpectrumProtect
   C:\ProgramData\Tivoli\TSM
   C:\ProgramData\config
   C:\IBM\SpectrumProtect
   C:\Program Files\IBM\SpectrumProtect
   ```

   您也可以移除：

   ```
   C:\Program Files\Tivoli\TSM
   ```

   如果不再需要剩餘日誌檔及配置檔。 如果您希望保留那些檔案，它們位於 C:\Program Files\Tivoli\TSM\baclient 中。 對於 IBM Spectrum Protect for Virtual Environments 8.1.4 版以及更早版本，請刪除：

   ```
   C:\IBM\tivoli
   C:\Program Files (x86)\Common Files\Tivoli\TDPVMware
   C:\Program Files\Common Files\Tivoli
   C:\ProgramData\Tivoli\TSM
   C:\ProgramData\config
   ```

   您也可以移除：

   ```
   C:\Program Files\Tivoli\TSM
   ```

   如果不再需要剩餘日誌檔及配置檔。 如果您希望保留那些檔案，它們位於 C:\Program Files\Tivoli\TSM\baclient 中。

下一步

檢查已從系統中移除的所有元件。

在無聲自動模式下解除安裝 Data Protection for VMware for Windows

您可以透過無聲自動方式在 Windows 作業系統上解除安裝 Data Protection for VMware。

關於這項作業

完成解除安裝後，配置檔及內容檔位於 C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\config 目錄中。

程序

如果要解除安裝 Data Protection for VMware，請完成下列步驟：

1. 停止任何執行中的 Data Protection for VMware 元件。
2. 卸載任何已裝載的虛擬磁區。 可以使用 Recovery Agent GUI 或指令行介面（**mount del** 指令）來卸載磁區。
3. 從命令提示字元視窗，使用 **cd** 指令來切換至下列其中一個資料夾：
   - 如果要自訂解除安裝作業，請移至 X64 資料夾。
   - 若要使用 Suite Installer 解除安裝 Data Protection for VMware，請跳至 <extract folder>TSM4VE_WIN。
4. 在命令提示字元視窗中，執行下列指令：
   - 對於自訂解除安裝作業，請從下列指令中選取：
     – 輸入此指令以解除安裝 Data Protection for VMware 及取消登錄 Data Protection for VMware vSphere GUI：

       ```
       spinstall.exe /s /v"/qn REBOOT=ReallySuppress REMOVE=ALL
       VCENTER_HOSTNAME=<vCenter 主機名稱或 IP>
       VCENTER_USERNAME=<vCenter 使用者名稱>
       VCENTER_PASSWORD=<vCenter 密碼>"
       ```

   - 如果要使用 Suite Installer 來解除安裝所有特性，請輸入下列指令：

     ```
     spinstall.exe /silent /remove
     ```

5. 完成解除安裝後，重新啟動系統。

在 Linux 系統上解除安裝 Data Protection for VMware

在受支援的 Linux 作業系統上解除安裝 Data Protection for VMware 並移除檔案及目錄。

開始之前

如果要確保解除安裝成功，請使用下列指引：

- 從 IBM Spectrum Protect Server 中移除節點。 在解除安裝 Data Protection for VMware 產品之前，您必須執行此動作：
  1. 從 /opt/tivoli/tsm/client/ba/bin/dsmadmc 中執行 dsmadmc。
  2. 您可能需要使用 del 指令，以刪除節點的檔案空間：del file *nodename* *
  3. 使用 q 指令以查詢節點：q filespace *nodename* *
  4. 使用 rem 指令以移除節點：rem node *nodename*
- 停止為資料移轉裝置建立的 dsmcad 服務。 使用技術文件 http://www-01.ibm.com/support/docview.wss?uid=swg21358414 中的指示

1. 使用 ps 指令，以檢查 dsmcad 服務是否在執行中：ps -ef|grep dsmcad
2. 使用 kill 指令，以中止 dsmcad 服務：kill -9 *dsmcad-processID*

- 您必須清除建立資料移轉裝置服務相關的檔案。 跳至安裝目錄，並發出下列指令：

  ```
  /opt/tivoli/tsm/client/ba/bin/dsmutillnx cleanupDmFiles 1
  ```

  按下 Enter 鍵以選取節點名稱，並按下「按下 Enter」以刪除。

  您可以在 dsm.sys 中找到節點名稱
- 從 VMware vSphere 5.5 環境解除安裝 IBM Spectrum Protect vSphere Client 外掛程式時，僅移除其相關聯的專用權標籤和說明。 實際的專用權保留為已安裝。 此問題是已知 VMware 限制。 如需相關資訊，請參閱下列「VMware 知識庫」文章：http://kb.vmware.com/kb/2004601。
- 解除安裝產品後，不會移除「Data Protection for VMware 啟用檔」。

關於這項作業

在 Linux 系統上解除安裝 Data Protection for VMware 時，依預設，解除安裝類型的程序與原始安裝類型相同。 如果要使用不同的解除安裝程序，請指定正確的參數。 比方說，如果您使用無聲自動安裝程序，則可以指定 –i swing 參數，以使用安裝精靈來解除安裝。 請以 root 使用者身分執行解除安裝程序。 root 使用者設定檔必須作為來源。 如果您使用 su 指令切換至 root，請使用 su - 指令來找出 root 設定檔。

當解除安裝程序開始移除程式檔案時，取消解除安裝程序並不會使系統回到全新狀態。 此狀況可能導致重新安裝嘗試失敗。 因此，請完成第 35 頁的『從 Linux 系統手動移除 Data Protection for VMware』 中說明的作業，以清除系統。

如果要解除安裝 Data Protection for VMware，請完成下列步驟：

程序

1. 切換至解除安裝程式的目錄。下列路徑是解除安裝程式的預設位置：/opt/tivoli/tsm/tdpvmware/_uninst/TDPVMware/
2. 視安裝類型而定，請使用下列其中一種方法來解除安裝 Data Protection for VMware：

   註：此程序中的指令必須輸入在同一行。 為符合頁面格式，這些範例顯示兩行。

   - 如果要使用安裝精靈來解除安裝 Data Protection for VMware，請輸入下列指令：

     ```
     ./Uninstall_Tivoli_Data_Protection_for_VMware –i swing
     ```
   - 如果使用主控台來解除安裝 Data Protection for VMware，請輸入下列指令：

     ```
     ./Uninstall_Tivoli_Data_Protection_for_VMware -i console
     ```
   - 如果要以無聲自動方式來解除安裝 Data Protection for VMware，請輸入下列指令：

     ```
     ./Uninstall_Tivoli_Data_Protection_for_VMware -i silent
     -f uninstall.properties
     ```

     uninstall.properties 檔包含 vCenter 連線資訊。 解除安裝 Data Protection for VMware vSphere GUI 需要此資訊。

從 Linux 系統手動移除 Data Protection for VMware

關於這項作業

如果無法使用標準解除安裝程序來解除安裝 Data Protection for VMware，則必須依照下列步驟中的說明，從系統中手動移除 Data Protection for VMware。請以 root 使用者身分完成這項程序。

程序

1. 如果您已安裝 Data Protection for VMware vSphere GUI，請使用此指令從「套件管理程式」資料庫中移除其套件：

   ```
   rpm -e TIVsm-TDPVMwarePlugin
   ```

2. 使用此指令來移除 IBM Spectrum Protect API：

   ```
   rpm -e TIVsm-API64
   gskssl64.linux.x86_64.rpm
   skcrypt64.linux.x86_64
   TIVsm-TDPVMwarePlugin.x86_64.rpm
   TIVsm-DPAPI.x86_64.rpm
   ```

3. 從「部署引擎」移除產品項目：

   a. 發出下列指令來檢視所有項目的清單：

      ```
      /usr/ibm/common/acsi/bin/de_lsrootiu.sh
      ```

   b. 發出下列指令，以移除與 Data Protection for VMware 相關的已安裝裝置項目：

      ```
      /usr/ibm/common/acsi/bin/deleteRootIU.sh <UUID> <discriminant>
      ```

      請確保移除下列裝置項目：

      ```
      FBJRE
      TDPVMwareGUI
      JavaHelp
      TDPVMwareDM
      ```

      解除安裝程式完成後，移除下列目錄（如果呈現）：

      - `/opt/tivoli/tsm/client`
      - `/opt/tivoli/tsm/tdpvmware`

      移除使用者 `tdpvmware` 及相關聯的目錄：

      - `userdel tdpvmware`
      - `/home/tdpvmware`
      - `/etc/adsm`

4. 備份廣域登錄檔 (`/var/.com.zerog.registry.xml`)。 備份此檔案之後，請移除與 Data Protection for VMware 相關的所有標籤。
5. 移除安裝目錄 (`/opt/tivoli/tsm/tdpvmware`) 中的所有檔案。 此外，也請移除桌面上的任何捷徑。
6. 備份 `/root` 目錄下檔名中含有 `TDPVMware` 的日誌檔。 例如，`IA-TDPVMware-00.log` 或 `IA-TDPVMware_Uninstall-00.log`。 在備份這些日誌檔之後，請將它們移除。 將它們移除後，如果安裝程序再次失敗，您可以檢視所發出的任何錯誤。
7. 現在，您可以再次安裝產品，如第 22 頁的『在 Linux 系統上安裝 Data Protection for VMware』中所述。

修改 Data Protection for VMware 的現有安裝

此區段提供在現有 Data Protection for VMware 安裝中修改套件及特性的指示。

使用 Suite Installer，您可以變更系統上安裝的基礎套件。若要修改任何個別套件特性，您可以使用 Windows 的**程式和功能**控制台。

在 Data Protection for VMware 的現有安裝中修改套件

您可以使用 Suite Installer，對 Data Protection for VMware 現有安裝中的套件進行變更。

開始之前

在使用 Suite Installer 之前，確保您具有要處理的來源媒體。 Suite Installer 的 `spinstall.exe` 執行檔位於安裝套件的根目錄下。

關於這項作業

使用 Suite Installer，以修改 Data Protection for VMware 現有安裝中安裝的套件。您可以選擇新增或移除：

- 資料移轉裝置
- Data Protection for VMware

請完成下列步驟：

程序

1. 按兩下 `spinstall.exe` 檔，以執行 Suite Installer 套件。
2. 使用**自訂設定**畫面上的套件勾選框，判定您需要安裝的套件。
3. 選取此安裝所需要的套件。

在 Data Protection for VMware 的現有安裝中修改特性

您可以使用 Windows 的「程式和功能」控制台，對 Data Protection for VMware 現有安裝中的特性進行變更。

開始之前

在修改安裝套件之前，確保您具有要處理的來源媒體。

關於這項作業

使用 Windows，以修改 Data Protection for VMware 的現有安裝中提供的個別套件特性。 您可以選擇修改下列項目的特性：

- 資料移轉裝置
- Data Protection for VMware

請完成下列步驟：

程序

1. 在 Windows **控制台**的**程式和功能**區段中，用滑鼠右鍵按一下 IBM Spectrum Protect for Virtual Environments：Data Protection for VMware 應用程式。

2. 按一下**修改**，以更新套件目前安裝的特性。
3. 選取此安裝所需要的特性。

第 2 章 配置 Data Protection for VMware

本節提供配置 Data Protection for VMware 及啟動相關服務的指示。

提示：安裝 Data Protection for VMware 之後，只有在資料移轉裝置連接至 IBM Spectrum Protect 伺服器且用於資料作業時，IBM License Metric Tool 才會對資料移轉裝置計數。隨後，資料移轉裝置一律併入軟體計算中。未連接至伺服器且未用於資料作業的資料移轉裝置會從授權計算中排除。

使用精靈配置新的安裝

使用配置精靈進行起始配置或完成次要變更。

開始之前

安裝 Data Protection for VMware 所在的系統必須具有與下列伺服器的網路連線：

- vStorage 備份伺服器
- IBM Spectrum Protect 伺服器
- vCenter Server

關於這項作業

若要配置 Data Protection for VMware 環境，請完成下列步驟：

程序

1. 開啟 Web 瀏覽器並輸入 GUI Web 伺服器位址。 例如：

   ```
   https://guihost.mycompany.com:9081/TsmVMwareUI/
   ```

2. 以 vCenter 使用者名稱及密碼登入。
3. 在「入門」視窗中，跳至「配置」視窗並按一下**執行配置精靈**。
4. 遵循精靈每一個頁面中的指示，直到「摘要」視窗顯示。 檢閱設定，然後按一下**完成**，以完成配置並結束精靈。

   提示：每一個配置頁面的相關資訊都在隨 GUI 一起安裝的線上說明中提供。 按一下任何 GUI 視窗中的**進一步瞭解**可以開啟線上說明以取得作業協助。 請參閱執行配置精靈主題。
5. 驗證是否已適當地配置資料移轉裝置節點：
   a. 按一下**配置**標籤以檢視「配置狀態」頁面。
   b. 在「配置狀態」頁面中，選取一個資料移轉裝置節點以在「狀態明細」窗格中檢視其狀態資訊。 當節點顯示警告或錯誤時，請按一下該節點，然後使用「狀態詳細資料」窗格來解決問題。 然後選取節點，再按一下**驗證選取的節點**來驗證問題是否已解決。 按一下**重新整理**以重新整理所有節點。

結果

捷徑：順利完成此精靈作業之後，不需要執行其他配置作業來備份 VM 資料。

使用記事本編輯現有安裝

使用「編輯配置」記事本可編輯現有的配置設定。

開始之前

「編輯配置」記事本對於現有配置提供下列作業：

- 設定或變更 IBM Spectrum Protect 管理者 ID。
- 重設密碼或解除鎖定 VMCLI 節點。
- （vSphere 環境）對 Data Protection for VMware vSphere GUI 網域新增或移除 VMware 資料中心。
- 新增或移除裝載 Proxy 節點。 修改現有裝載 Proxy 節點的密碼。
- 新增或移除資料移轉裝置節點。 修改現有資料移轉裝置節點的密碼。
- 啟用檔案還原。
- 啟用資料移轉裝置節點的標記支援。

關於這項作業

若要編輯現有的配置，請完成下列步驟：

程序

1. 開啟 Web 瀏覽器，然後輸入 GUI Web 伺服器位址。 例如：

   ```
   https://guihost.mycompany.com:9081/TsmVMwareUI/
   ```

   以 vCenter 使用者名稱及密碼登入。
2. 在「入門」視窗中，跳至「配置」視窗，然後按一下**編輯配置**。
3. 跳至編輯作業相關的頁面並遵循指示。 您必須先按一下**確定**以儲存變更，然後再進行另一個「配置設定」頁面。否則，您的變更不會生效。

   重要：隨 GUI 安裝的線上說明中提供每一個配置頁面的相關資訊。按一下任何 GUI 視窗中的**進一步瞭解**可以開啟線上說明以取得作業協助。 請參閱《編輯現有的配置》主題。

結果

更新的設定會顯示在「配置」視窗中。

啟用環境進行檔案還原作業

Windows

當管理者已啟用檔案還原特性時，檔案擁有者即可以在無協助下還原檔案。

開始之前

如果您未驗證是否符合所有必要條件，請檢閱《*IBM Spectrum Protect for Virtual Environments*：*Data Protection for VMware* 使用手冊》中檔案還原必要條件上的主題。

關於這項作業

請在安裝 Data Protection for VMware vSphere GUI 的系統上完成這些步驟。

程序

1. 開啟 Web 瀏覽器，然後輸入 GUI Web 伺服器位址，以啟動 Data Protection for VMware vSphere GUI。 例如：

   `https://<GUI web server address>:9081/TsmVMwareUI/`

   以 vCenter 使用者 ID 及密碼登入。
2. 從「開始使用」視窗中，按一下**配置**，然後在「作業」清單中請選取下列一個作業：
   - 如果您要配置新環境，請完成下列步驟：
     a. 選取**執行用戶端配置精靈**。
     b. 遵循精靈每一個頁面中的指示。 使用下列指引來完成「檔案還原」頁面：
        1) 選取**啟用檔案還原**選項。
        2) 輸入檔案還原介面中顯示的管理者聯絡資訊。 如果您不想要提供聯絡資訊，請清除該勾選框。
        3) 如果環境包含 Windows 虛擬機器的備份，請輸入 Windows 網域使用者認證。否則，清除該勾選框，且不要輸入任何認證。

           提示：檔案還原作業使用 Windows 網域使用者認證來存取遠端虛擬機器上的網路共用。當環境包含 Windows 虛擬機器的備份但沒有認證，或是輸入的認證不正確時，作業會失敗。 因此，僅當沒有 Windows 虛擬機器備份時，才清除這個勾選框。
        4) 按一下檔案還原介面 URL，以驗證介面是否可存取。

           記住：保留檔案還原介面 URL 的記錄。 訪客虛擬機器的擁有者會透過此 URL 存取檔案還原介面。
        5) 按一下**確定**以儲存您的變更。
   - 如果您要更新現有的環境，請完成下列步驟：
     a. 選取**編輯 TSM 配置**。
     b. 在「檔案還原」頁面上，使用下列指引：
        1) 選取**啟用檔案還原**選項。
        2) 輸入檔案還原介面中顯示的管理者聯絡資訊。 如果您不想要提供聯絡資訊，請清除該勾選框。
        3) 如果環境包含 Windows 虛擬機器的備份，請輸入 Windows 網域使用者認證。否則，清除該勾選框，且不要輸入任何認證。

           提示：檔案還原作業使用 Windows 網域使用者認證來存取遠端虛擬機器上的網路共用。當環境包含 Windows 虛擬機器的備份但沒有認證，或是輸入的認證不正確時，作業會失敗。 因此，僅當沒有 Windows 虛擬機器備份時，才清除這個勾選框。
        4) 按一下檔案還原介面 URL，以驗證介面是否可存取。

記住：保留檔案還原介面 URL 的記錄。 訪客虛擬機器的擁有者會透過此 URL 存取檔案還原介面。

5) 按一下**確定**以儲存您的變更。

結果

針對檔案還原作業啟用該環境。 檔案擁有者可以使用 URL 來存取 IBM Spectrum Protect 檔案還原介面，藉以還原他們的檔案。

在 Linux 上設定檔案還原作業

Linux

當 Data Protection for VMware 安裝於 Linux 系統上時，若要啟用檔案還原功能，必須在 Windows 系統上設定其他 Data Protection for VMware 環境。

關於這項作業

當您在 Linux 環境中執行 Data Protection for VMware 時，檔案還原特性必須安裝在 Windows 系統上，以啟用檔案還原特性。

程序

1. 設定要用於檔案還原功能的個別 Windows 伺服器。
2. 在該 Windows 系統上安裝 Data Protection for VMware。 在安裝期間接受預設值。
3. 當您在 Windows 系統上配置 Data Protection for VMware 時，請使用下列節點名稱：
   a. 建立名稱為 `VCENTER_FR` 的 vCenter 節點。
   b. 建立名稱為 `VMCLI_FR` 的 VMCLI 節點。
   c. 重複使用 Linux 環境中的資料中心節點名稱。
   例如：`DATACENTER`。
   d. 請勿建立資料移轉裝置節點。 在此實務中，檔案還原功能不需要資料移轉裝置節點。
   e. 建立以下新的裝載 Proxy 節點配對，其分別名為 `REMOTE_FR_MP_WIN` 與 `REMOTE_FR_MP_LNX`。
4. 在配置精靈中的「檔案還原」頁面上，選取啟用檔案還原選項。
5. 若要存取檔案還原介面，請開啟 Web 瀏覽器並輸入您管理者提供的 URL。 例如：
   `https:\\hostname:9081\FileRestoreUI`

   其中，`hostname` 是已安裝 Data Protection for VMware 之 Windows 系統的主機名稱。

結果

下列範例顯示 IBM Spectrum Protect 伺服器上的 Proxy 節點關係：

```
tsm: SERVER>q proxy

Target Node         Agent Node
---------------     ----------------------------------------------
VCENTER             VMCLI DATACENTER
```

```
VCENTER_FR          VMCLI_FR DATACENTER
DATACENTER          VMCLI VMCLI_FR
                     DATAMOVER1
                     REMOTE_MP_WIN REMOTE_MP_LNX
                     REMOTE_FR_MP_WIN REMOTE_FR_MP_LNX
```

為啟用檔案還原功能而建立的其他節點具有 _FR 字尾。

修改檔案還原作業的選項

Windows

若要容許管理者配置及控制用於檔案還原作業的還原處理，請修改 frConfig.props 檔中的選項。

關於這項作業

請在安裝 Data Protection for VMware vSphere GUI 的系統上完成這些步驟。

程序

1. 跳至 frConfig.props 檔所在的目錄。 例如，開啟命令提示字元並發出下列指令：
   ```
   cd C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\tsmVmGUI
   ```
2. 在管理者模式下使用文字編輯器開啟 frConfig.props 檔，並視需要修改選項。 使用 『檔案還原選項』 中的選項來決定要修改哪些選項。
3. 儲存變更並關閉 frConfig.props 檔。

結果

修改的選項會套用到 IBM Spectrum Protect 檔案還原介面。

檔案還原選項

frConfig.props 選項控制檔案還原作業的配置、支援和還原處理。

enable_contact_info=false | true
指定是否提供檔案擁有者可用來取得支援的管理者聯絡資訊。

false
檔案擁有者不接收管理者聯絡資訊。 此值為預設值。

true
檔案擁有者接收管理者聯絡資訊。

如果您指定 **enable_contact_info=true**，則必須在 **contact_info** 選項中提供資訊。

enable_filerestore=false | true
指定檔案擁有者是否可以從虛擬機器使用 IBM Spectrum Protect 檔案還原介面還原其檔案。

false
檔案擁有者無法使用 IBM Spectrum Protect 檔案還原介面還原其檔案。 此值為預設值。

true
檔案擁有者可以使用 IBM Spectrum Protect 檔案還原介面還原其檔案。

maximum_mount_points=*num_mount_points*
指定可供使用者帳戶使用的同時回復點數目上限。 下限值為 1 個回復點。 上限值為 256 個裝載點。 預設值為 2 個裝載點。

提示：若要防止針對同時還原作業而裝載虛擬機器多次，請將此選項設為較低的值。

mount_session_timeout_minutes=*num_mins*
指定在階段作業取消之前，還原及裝載的回復點可以閒置的時間量（分鐘）。 取消會卸載回復點。 上限值為 8 小時（480 分鐘）。 預設值是 30 分鐘。

提示：若要防止階段作業非預期地取消，請增加分鐘數。

restore_info_duration_hours=*num_hrs*
指定最近還原活動的相關資訊保留在 IBM Spectrum Protect 檔案還原介面中的時間量（以小時為單位）。 請使用還原活動視窗來檢視錯誤資訊及最近完成的作業。 這項資訊提供一種找出最近還原檔案的方式。 上限值為 14 天（336 小時）。 預設值為一週（168 小時）。

contact_info=*administrator information*
提供檔案擁有者可用來取得支援的管理者聯絡資訊。 聯絡資訊會顯示於 IBM Spectrum Protect 檔案還原介面的下列位置中：

- 登入視窗
- 說明功能表中的「關於」窗格
- 介面訊息中的支援資訊鏈結

您可以使用 Data Protection for VMware vSphere GUI 配置精靈或記事本來改寫下列選項：

- **enable_contact_info**
- **enable_filerestore**
- **contact_info**

配置日誌活動以進行檔案還原作業

若要容許管理者針對檔案還原作業控制內容的配置及記載方式，請修改 FRLog.config 檔中的選項。

開始之前

在第一次存取 IBM Spectrum Protect 檔案還原介面時，會產生 FRLog.config 檔。

關於這項作業

請在安裝 Data Protection for VMware vSphere GUI 的系統上完成這些步驟。

程序

1. 跳至 FRLog.config 檔所在的目錄。 開啟命令提示字元並發出下列指令：
   ```
   cd C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\frGUI\
   ```
2. 在管理者模式下使用文字編輯器開啟 FRLog.config 檔，並視需要修改選項。 使用第 45 頁的『檔案還原日誌活動選項』 中的選項來決定要修改哪些選項。

3. 儲存變更並關閉 FRLog.config 檔。
4. 重新啟動 Web 伺服器：
   a. 按一下**開始** > **控制台** > **系統管理工具** > **服務**。
   b. 在 **Data Protection for VMware Web Server Service** 上按一下滑鼠右鍵，然後按一下**重新啟動**。

結果

設定隨即套用至檔案還原作業之記載資訊的內容和格式。

檔案還原日誌活動選項

FRLog.config 選項會控制檔案還原作業資訊的記載內容和格式。

下列選項會在 fr_gui.log 檔中記載檔案還原作業的資訊：

MAX_LOG_FILES=*number*
指定要保留的 fr_gui.log 檔案數目上限。 預設值為 8。

MAX_LOG_FILE_SIZE=*number*
指定 fr_gui.log 檔案的大小上限 (KB)。 預設值為 8192 KB。

下列選項會在 fr_api.log 檔中記載檔案還原服務的資訊。 這些服務是與檔案還原活動相關的內部 API 服務：

API_MAX_LOG_FILES=*number*
指定要保留的 fr_api.log 檔案數目上限。 預設值為 8。

API_MAX_LOG_FILE_SIZE=*number*
指定 fr_api.log 檔案的大小上限 (KB)。 預設值為 8192 KB。

API_LOG_FILE_NAME=*API_log_file_name*
指定 API 日誌檔的名稱。 預設值為 fr_api.log。

API_LOG_FILE_LOCATION=*API_log_file_name*
指定 API 日誌檔的位置。 必須以正斜線 (/) 指定位置。 預設位置是 C:/IBM/SpectrumProtect/webserver/usr/servers/veProfile/logs。

FR.API.LOG=ON | OFF
指定是否對檔案還原服務啟用記載功能。

- 若要對檔案還原服務啟用記載功能，請指定 ON。 預設值為 ON。
- 若要對檔案還原服務停用記載功能，請指定 OFF。

若要對檔案還原作業期間可能遇到的問題進行疑難排解，請參閱檔案還原的追蹤選項。 追蹤選項也是在 FRLog.config 檔案中指定。

為資料移轉裝置節點配置標記支援

在資料移轉裝置節點上啟用標記支援之後，管理者可將資料保護標記套用至 VMware vCenter 中的庫存物件。

開始之前

確保符合下列需求：

- VMware vCenter Server 必須處於 6.0 版更新 1 或更高版本。
- 為了讓 Data Protection for VMware vSphere GUI 利用標記支援正確地運作，請確保在安裝 GUI 期間符合下列需求：
  - 至少一個資料移轉裝置與 Data Protection for VMware vSphere GUI 必須安裝在同一伺服器上。 必須配置這個資料移轉裝置節點，以便儲存 vCenter 伺服器認證。您可以透過執行配置精靈以儲存資料移轉裝置節點密碼，或者透過在資料移轉裝置指令行上使用 **dsmc set password** 指令，以儲存認證。

    如果您使用其他資料移轉裝置，在虛擬機器或實體機器上作為其他資料移轉裝置執行，則可以在其他伺服器上安裝它們。 對於標記支援，還必須使用 VMTAGDATAMOVER YES 選項配置所有這些資料移轉裝置。 這些其他資料移轉裝置不需要將 Data Protection for VMware vSphere GUI 安裝在同一伺服器上，即可作為標籤型資料移轉裝置正確地運作。
  - Linux 對於 Linux 資料移轉裝置，請確保您在 LD_LIBRARY_PATH 環境變數中指定資料移轉裝置安裝目錄，以及 Java™ 共用程式庫 libjvm.so。 當您在資料移轉裝置上啟用 vmtagdatamover 選項時，libjvm.so 的路徑用於標記支援。如需指示，請參閱在 vSphere 環境中設定資料移轉裝置節點。
  - Linux 在 Linux 作業系統上，必須使用預設使用者名稱 (tdpvmware) 來安裝 Data Protection for VMware vSphere GUI。
  - 在 UNIX 及 Linux 用戶端上，TSM.PWD 檔中的現有密碼會移轉至同一位置中的新密碼儲存庫。 對於 root 使用者，密碼儲存庫的預設位置是 /etc/adsm。 對於非 root 使用者，透過 passworddir 選項指定密碼儲存庫的位置。

    移轉後，刪除 TSM.PWD 檔。

註：如需使用標記所需要之專用權使用的進一步資訊，請參閱安裝 Data Protection for VMware 元件

關於這項作業

您可以使用資料保護標籤，以在 VMware 庫存物件中配置虛擬機器的備份原則。 這些資料保護標籤會呈現為可在 IBM Spectrum Protect vSphere Client 外掛程式 中變更的設定。

程序

請使用下列一項方法：

選項	敘述
若要使用 vSphere 外掛程式 GUI 配置資料移轉裝置節點	1. 從 vSphere 外掛程式中，選取 IBM Spectrum Protect。 2. 在**配置**標籤中，選取**資料移轉裝置**。 3. 在**新增資料移轉裝置**畫面中，從下拉功能表中選取資料中心。 4. 接受預設值，或者編輯**資料移轉裝置名稱**、**資料移轉裝置主機名稱**、**vCenter 使用者**及 **vCenter 密碼**的設定。 5. 設定完成後，按一下**新增**。 如需進一步詳細資料，請參閱《Data Protection for VMware vSphere GUI 安裝手冊》中的主題「使用 vSphere 外掛程式 GUI 設定資料移轉裝置節點」。

選項	敘述
若要透過使用 Data Protection for VMware vSphere GUI，在 Windows 或 Linux 上配置新的資料移轉裝置以取得標記支援	1. 在安裝 Data Protection for VMware vSphere GUI 所在的系統上，透過開啟 Web 瀏覽器，並輸入 GUI Web 伺服器位址，從而啟動 GUI。 例如： `https://<GUI web server address>:9081/TsmVMwareUI/` 2. 以 vCenter 使用者 ID 及密碼登入。 3. 跳至**配置**標籤，並選取**編輯 IBM Spectrum Protect 配置**動作。 4. 跳至配置記事本的「資料移轉裝置節點」頁面。 5. 透過完成下列步驟，新增資料移轉裝置節點： a. 對於您想要為其設定標記支援的資料移轉裝置節點，選取**建立服務**。 依預設，選取**標籤型節點**，啟用資料移轉裝置節點以取得標記支援 b. 若要將標籤型節點指定為預設資料移轉裝置節點，請選取**預設資料移轉裝置**。 如果儲存器已在保護集中，則預設資料移轉裝置節點會備份新增至資料中心內任何儲存器的任何新 VM。預設資料移轉裝置還會備份未指派資料移轉裝置標籤之保護集中的任何 VM。 **提示：**對於 Linux 系統，如果您選取新的資料移轉裝置節點作為預設標記節點，則從與該資料中心相關聯的任何其他資料移轉裝置選項檔案中移除 `vmtagdefaultdatamover` 行。 c. 按一下**確定**以儲存您的變更。 `vmtagdatamover` 及 `vmtagdefaultdatamover`（如果設定）選項會新增至資料移轉裝置選項檔案 (`dsm.opt`)。
若要在節點與 Data Protection for VMware vSphere GUI 位於同一伺服器上時，配置現有 Windows 資料移轉裝置節點以取得標記支援	1. 完成之前指示中的步驟 1-3，配置新的資料移轉裝置節點以取得標記支援。 2. 在「資料移轉裝置節點」頁面上，為您想要啟用標記支援的節點選取**標籤型節點**。 3. **選用項目：**若要將標籤型節點指定為預設資料移轉裝置節點，請選取**預設資料移轉裝置**。

選項	敘述
若要配置現有 Linux 資料移轉裝置節點以取得標記支援或者與 Data Protection for VMware vSphere GUI 位於不同伺服器上的現有 Windows 資料移轉裝置節點	1. 在資料移轉裝置選項檔案中新增 vmtagdatamover yes 選項（dsm.sys 適用於 Linux，且 dsm.opt 適用於 Windows）。 2. **選用項目：**若要將標籤型節點指定為預設資料移轉裝置節點，請將 vmtagdefaultdatamover yes 或 vmtagdefaultdatamover *dm_name* 選項新增至資料移轉裝置選項檔案。 **提示：**對於 Linux 系統，如果您選取新的資料移轉裝置節點作為預設標記節點，則從與該資料中心相關聯的任何其他資料移轉裝置選項檔案中移除 vmtagdefaultdatamover 行。

結果

在讓資料移轉裝置節點啟用標記支援之後，該資料移轉裝置在執行備份時，便會查詢 VMware 庫存以取得標記資訊。 然後，資料移轉裝置會根據已設定的資料保護標籤來備份虛擬機器。 如果未針對資料移轉裝置節點來配置標記支援，則執行備份作業期間會忽略所有的資料保護標籤。

相關資訊:

- Vmtagdatamover
- Vmtagdefaultdatamover
- 配置備份原則

配置環境以執行完整虛擬機器即時還原作業

設定專用的 iSCSI 網路，以執行完整虛擬機器即時還原及即時存取作業。

開始之前

使用適當的 VMware 說明文件（ESXi 或 vSphere），可判定配置 iSCSI 虛擬交換器及虛擬機器網路時，需執行的特定步驟。 雖然提供一般準則，但關於如何新增虛擬網路及虛擬交換器的特定說明文件及說明，不在產品說明文件的範圍之內。 在發佈時，VMware vSphere ESXi 及 vCenter 5.5 說明文件於 VMware ESXi 及 vCenter Server 5 說明文件中提供。 「網路」主題包含關於新增及配置虛擬交換器及虛擬網路的資訊。

重要：提供這些配置設定，是為了幫助您設定 VMware 環境，以高效執行完整虛擬機器即時還原及即時存取作業。不過，因為這些設定適用於 VMware 配置作業及 VMware 使用者介面，您必須參考適當的 VMware 說明文件，以取得詳細的逐步指示。

關於這項作業

此程序在每一部 ESXi 主機上需要 iSCSI 配接卡，以用於即時還原作業。 請使用適當的 VMware 說明文件來設定該配接卡。 在發佈時，此 VMware vSphere 資源中提供下列程序。

- 若要設定軟體 iSCSI 配接器，請遵循 VMware 的「配置軟體 iSCSI 配接器」程序中的指示。
- 若要設定硬體 iSCSI 配接卡，請遵循 VMware 的「設定獨立硬體 iSCSI 配接卡」程序中的指示。

1. 在 ESXi 主機上配置 iSCSI 軟體

程序

此作業設定 iSCSI 軟體的基本配置。

1. 登入要用於即時還原作業的 ESXi 主機。
2. 遵循此 VMware 知識庫中的指示，直到 iSCSI 配接卡啟用為止： http://kb.vmware.com/kb/1008083
   IBM Spectrum Protect 會自動探索 iSCSI 目標伺服器。
3. 驗證 ESXi 主機上 iSCSI 配接卡的 IP 位址，是否為資料移轉裝置所使用的子網路位址。
4. 驗證 ESXi 主機上是否已啟用 Storage vMotion 授權。

下一步

在 ESXi 主機上設定 iSCSI 軟體之後，請在資料移轉裝置系統上安裝並配置應用程式。

2. 在資料移轉裝置上安裝並配置應用程式

開始之前

如果已在資料移轉裝置系統上安裝及配置 Recovery Agent 及 IBM Spectrum Protect 資料移轉裝置，請從步驟 3 開始。

程序

本作業在資料移轉裝置系統上設定應用程式及設定，以執行即時還原作業。

1. 在資料移轉裝置系統上安裝 Recovery Agent 及 IBM Spectrum Protect 資料移轉裝置系統。
   在安裝 Data Protection for VMware 程序的步驟 4 中，選取**安裝完整資料移轉裝置以獲得訪客內應用程式保護**安裝類型。
2. 配置資料移轉裝置。
   遵循「用戶端」說明文件中主題「配置資料移轉裝置」內的指示。
3. 設定 iSCSI 伺服器 IP 位址：
   a. 跳至 `C:\Program Files\Tivoli\TSM\baclient\dsm.opt` 檔，並指定下列參數：
      `VMISCSIServeraddress=<資料移轉裝置系統上顯示 iSCSI 目標之網路卡的 IP 位址。>`
   如果您的資料移轉裝置系統有多個網路卡，請確保指定 iSCSI 網路的正確網路卡。

下一步

設定資料移轉裝置系統之後，請在 Recovery Agent CLI 與 Recovery Agent GUI 之間建立連線。

3. 設定 Recovery Agent 連線

開始之前

Recovery Agent 指令行介面 (CLI) 7.1.x 版可以視為 Recovery Agent GUI 的指令行 API。 您可以使用 Recovery Agent CLI，來與 Recovery Agent GUI 進行通訊。

程序

本作業在 Recovery Agent CLI 與 Recovery Agent GUI 之間建立連線。

1. 在資料移轉裝置系統上啟動 Recovery Agent CLI。
   從 **Windows 開始**功能表中，按一下**程式集** > **IBM Spectrum Protect** > **IBM Spectrum Protect for Virtual Environments** > **IBM Spectrum Protect Recovery Agent**。
2. 在命令提示字元視窗中，輸入下列指令：

   ```
   RecoveryAgentShell.exe -c set_connection mount_computer
   <資料移轉裝置系統上顯示 iSCSI 目標之網路卡的 IP 位址。>
   ```

   此指令在 Recovery Agent CLI 與 Recovery Agent GUI 之間建立連線。

下一步

建立連線之後，請配置專用的 iSCSI 網路。

4. 針對 ESXi 主機及資料移轉裝置配置專用的 iSCSI 網路

開始之前

請先檢閱下列準則，然後再繼續進行本作業：

- 使用專用的 iSCSI 網路進行即時還原作業。
- 每部用於即時還原作業的 ESXi 主機都必須有可用的第二個實體網路卡。 第二個網路卡與各 ESXi 主機的軟體 iSCSI 配接卡連結。
- 在虛擬機器中執行的資料移轉裝置系統必須有可用的第二個網路卡。第二個網路卡與 ESXi 主機的軟體 iSCSI 配接卡連結。
- 每部用於即時還原作業的 ESXi 主機都必須有可用的次要 VMware 資料儲存庫。 這個暫用資料儲存庫中包含在作業期間所建立虛擬機器的配置資訊及資料。

程序

本作業針對 ESXi 以及在虛擬機器中執行的資料移轉裝置，設定專用的 iSCSI 網路。

1. 登入要用於即時還原作業的 ESXi 主機。
2. 針對 iSCSI 網路來設定虛擬交換器。
   這些步驟會使用 *vSwitch1* 來代表虛擬交換器。
   a. 針對**連線類型**，請選取 **VMkernel 網路配接卡**。
      iSCSI 網路需要此連線類型。

b. 針對 **VMkernel 網路存取**，請選取**建立 vSphere 標準交換器**。

c. 針對 **VMkernel 連線設定**，請選取**網路標籤**。
請指定一個標籤，指出 *vSwitch1* 及此網路是用於 iSCSI 資料流量。
例如：*VMkernel iSCSI*。

d. 在 **VMkernel IP 連線設定**中，指定 *vSwitch1* 的 IP 位址及子網路遮罩。
請勿變更**子網路遮罩**或 **VMkernel 預設閘道**值。

e. 指定 iSCSI 網路作業所需的核心埠。

3. 針對虛擬交換器網路來設定虛擬交換器。
這些步驟會使用 *vSwitch0* 來代表虛擬交換器。

a. 針對**連線類型**，請選取**虛擬機器**。

b. 針對 **VMkernel 網路存取**，請選取**建立 vSphere 標準交換器**。

c. 跳至**埠群組內容**標籤，並選取**網路標籤**。
指定您之前針對 *vSwitch1* 虛擬機器網路指定的標籤。
例如：*VMkernel iSCSI*。

4. 將新建立的 iSCSI 配接卡與 **VMkernel 網路配接卡**連結。
請遵循 VMware 的「將 iSCSI 配接卡與 VMkernel 配接卡連結」程序中的指示。
在發佈時，此程序是在 VMware ESXi 及 vCenter Server 5 說明文件中提供。

提示：如果掃描 iSCSI 裝置時發生逾時，請減少連接至 ESXi 主機的 iSCSI 裝置數目。 然後，重新掃描 iSCSI 裝置。

5. 驗證 iSCSI 配接卡連結內容是否正確。

a. 在 VMware vSphere Client 中，跳至**硬體** > **儲存體配接卡**。

b. 以滑鼠右鍵按一下 iSCSI 配接卡，並選取 **iSCSI 起始器內容**。確保下列連結內容存在：

表 *10. iSCSI* 網路設定

虛擬機器網路	iSCSI 網路
標準交換器：*vSwitch0*	**標準交換器**：*vSwitch1*
虛擬機器埠群組：*VM Network*	**VMkernel 埠**：*VMkernel iSCSI* **提示：***VMkernel iSCSI* 與 **VMkernel 配接卡** *vmk1* 連結，後者位於 **實體網路配接卡** *vmnic1* 上。
實體配接卡：*vmnic0*	**VMkernel 網路配接卡**：*vmk1*
	實體網路配接卡：*vmnic1*
	虛擬網路配接卡 **IP 位址**：192.168.42.x（iSCSI 網路的子網路）

結果

專用的 iSCSI 網路已備妥，可執行完整 VM 即時還原及即時存取作業。

配置 Data Protection for VMware 的安全設定

Data Protection for VMware 資料移轉裝置、vmcli 指令行介面及 Data Protection for VMware vSphere GUI 元件需要配置，以啟用與 IBM Spectrum Protect 伺服器 的安全連線。

配置安全設定以將資料移轉裝置及 VMCLI 節點連接至 IBM Spectrum Protect 伺服器

連接至 IBM Spectrum Protect 伺服器 7.1.8 版或 8.1.2 版或者更新版本時，有數個配置選項與資料移轉裝置及 VMCLI 節點的 Data Protection for VMware 安全設定相關。 接受那些選項的預設值會透通地配置這些元件的加強安全，並且建議大部分使用案例都配置該項目。

透過使用預設安全設定（捷徑）進行配置

捷徑會詳細說明配置選項，影響資料移轉裝置及 VMCLI 節點與伺服器的連線，以及接受預設值時各個使用案例的行為。 捷徑實務範例會最小化各端點配置處理程序中的步驟。

當節點第一次連接時，此實務範例會自動從伺服器取得憑證，假設 IBM Spectrum Protect 伺服器 **SESSIONSECURITY** 參數設為 **TRANSITIONAL**，這是第一次連線時的預設值。無論您是否第一次將 IBM Spectrum Protect 伺服器 升級至 7.1.8 版以及更新版本第 7 版層次，或者 8.1.2 版以及更新版本第 8 版層次，您可以遵循此實務範例，然後將 Data Protection for VMware 升級至這些層次。

警告： 如果配置 IBM Spectrum Protect 伺服器以進行 LDAP 鑑別，則無法使用此實務範例。 如果使用 LDAP，則可以透過使用 dsmcert 公用程式，手動匯入必要憑證。如需相關資訊，請參閱第 55 頁的『配置而無需自動憑證公佈』。

影響階段作業安全的資料移轉裝置節點選項

下列 dsmc 選項指定資料移轉裝置節點的安全設定。 如需這些選項的相關資訊，請參閱用戶端選項參照。

- SSLREQUIRED。 預設值預設值啟用與 7.1.8 版或 8.1.2 版之前版本伺服器的現有階段作業安全連線，並自動配置 Data Protection for VMware 資料移轉裝置，以透過將 TLS 用於鑑別，安全地連接至 7.1.8 版或 8.1.2 版或者更新版本伺服器。
- SSLACCEPTCERTFROMSERV。 預設值是可讓資料移轉裝置自動接受伺服器的自簽公用憑證，以及自動配置資料移轉裝置，從而在資料移轉裝置連接至 7.1.8 版或 8.1.2 版或者更新版本伺服器時使用該憑證。
- SSL。 預設值否指出在資料移轉裝置與早於 7.1.8 版或 8.1.2 版的伺服器之間傳送資料時，不使用加密。當資料移轉裝置連接至 7.1.8 版或 8.1.2 版或者更新版本的伺服器時，預設值否指出物件資料未加密。 資料移轉裝置與伺服器進行通訊時，會加密所有其他資訊。 值是指出當資料移轉裝置與伺服器進行通訊時，TLS 用來加密所有資訊，包括物件資料。
- SSLFIPSMODE。 預設值否指出不需要經「聯邦資訊存取安全標準 (FIPS)」認證的 TLS 程式庫。

此外，僅當資料移轉裝置使用與早於 7.1.8 版或 8.1.2 版之伺服器的 TLS 連線時，下列選項適用。 當資料移轉裝置連接至更新版本的伺服器時，會忽略這些選項。

- SSLDISABLELEGACYTLS。 值否指出資料移轉裝置不需要將 TLS 1.2 用於 SSL 階段作業。 它容許透過 TLS 1.1 以及較低版本的 SSL 通訊協定進行連線。 當資料移轉裝置與 7.1.7 版或 8.1.1 版或者較早版本的 IBM Spectrum Protect 伺服器 進行通訊時，否是預設值。
- LANFREESSL。 預設值否指出配置不需 LAN 的資料傳送時，如果與儲存體代理程式進行通訊，資料移轉裝置不會使用 TLS。
- REPLSSLPORT。 指定資料移轉裝置與抄寫目標伺服器進行通訊時，為 TLS 啟用的 TCP/IP 埠位址。

影響階段作業安全的 VMCLI 節點選項

下列參數指定 VMCLI 節點的安全設定。 如需這些選項的相關資訊，請參閱設定檔參數。

- VE_TSM_SSL。 預設值否指出在資料移轉裝置與早於 7.1.8 版或 8.1.2 版的伺服器之間傳送資料時，不使用加密。 如果您想要在連接至早於 7.1.8 版的伺服器時，使用 TLS 加密所有資訊，則將此值設為是。
- VE_TSM_SSLACCEPTCERTFROMSERV。 預設值是可讓介面自動接受伺服器的自簽公用憑證，以及自動配置介面，從而在資料移轉裝置連接至 7.1.8 版或 8.1.2 版或者更新版本伺服器時使用該憑證。
- VE_TSM_SSLREQUIRED。 預設值預設值啟用與 7.1.8 版或 8.1.2 版之前版本伺服器的現有階段作業安全連線，並自動配置介面，以透過將 TLS 用於鑑別，安全地連接至 7.1.8 版或 8.1.2 版或者更新版本伺服器。

預設安全設定的使用案例

- 首先，伺服器會升級至 7.1.8 版或 8.1.2 版或者更新版本。 然後，升級 Data Protection for VMware。 現有資料移轉裝置及 VMCLI 節點不使用 SSL 通訊：
  - 資料移轉裝置及 VMCLI 節點的安全選項不需要變更。
  - 節點向伺服器進行鑑別時，會自動更新配置以使用 TLS。
- 首先，伺服器會升級至 7.1.8 版或 8.1.2 版或者更新版本。 然後，升級 Data Protection for VMware。 現有資料移轉裝置及 VMCLI 節點會使用 SSL 通訊：
  - 資料移轉裝置及 VMCLI 節點的安全選項不需要變更。
  - 繼續使用具有現有伺服器公用憑證的 SSL 通訊。
  - 自動加強 SSL 通訊，以使用伺服器需要的 TLS 層次。
- 首先，Data Protection for VMware 會升級至 7.1.8 版或 8.1.2 版或者更新版本。 然後，稍後會升級伺服器。 現有資料移轉裝置及 VMCLI 節點不使用 SSL 通訊：
  - 資料移轉裝置及 VMCLI 節點的安全選項不需要變更。
  - 現有鑑別通訊協定繼續用於早於 7.1.8 版或 8.1.2 版層次的伺服器。
  - 伺服器升級至 7.1.8 版或 8.1.2 版或者更新版本之後，當節點向伺服器進行鑑別時，配置會自動更新為使用 TLS。
- 首先，Data Protection for VMware 會升級至 7.1.8 版或 8.1.2 版或者更新版本。 然後，稍後會升級伺服器。 現有資料移轉裝置及 VMCLI 節點會使用 SSL 通訊：
  - 資料移轉裝置及 VMCLI 節點的安全選項不需要變更。
  - 具有現有伺服器公用憑證的 SSL 通訊會繼續用於早於 7.1.8 版或 8.1.2 版層次的伺服器。

  - 伺服器更新至 7.1.8 版或 8.1.2 版或者更新版本之後，SSL 通訊會自動加強以使用伺服器需要的 TLS 層次。
- 首先，Data Protection for VMware 會升級至 7.1.8 版或 8.1.2 版或者更新版本。然後，資料移轉裝置與 VMCLI 節點會連接至多個伺服器。 伺服器在兩個不同的時間進行升級：
  - 資料移轉裝置及 VMCLI 節點的安全選項不需要變更。
  - 資料移轉裝置與 VMCLI 節點將現有鑑別及階段作業安全通訊協定用於早於 7.1.8 版或 8.1.2 版的伺服器，並在起始連接至 7.1.8 版或 8.1.2 版或者更新版本的伺服器時，自動升級以使用 TLS 鑑別。 系統會管理每個伺服器的階段作業安全。
- 新的用戶端安裝，伺服器處於 7.1.8 版或 8.1.2 版或者更新版本：
  - 根據新的安裝配置 Data Protection for VMware。
  - 安全選項的預設值會自動配置資料移轉裝置及 VMCLI 節點以進行 TLS 加密的階段作業鑑別。
  - 如果用戶端與伺服器之間的所有資料傳送都需要加密，則將 SSL 參數設為是值。
- 新的用戶端安裝，伺服器處於早於 7.1.8 版或 8.1.2 版的版本：
  - 根據新的用戶端安裝配置用戶端。
  - 如果不需要所有資料傳送的 SSL 加密，則接受用戶端階段作業安全參數的預設值。
    - 除非伺服器升級至 7.1.8 版或 8.1.2 版或者更新版本，否則使用非 SSL 鑑別通訊協定。
  - 如果資料移轉裝置與伺服器之間的所有資料傳送都需要加密，則將 SSL 參數設為是值，並繼續 SSL 的手動配置。
    - 如需配置指示，請參閱配置透過 Secure Sockets Layer 進行的 Tivoli Storage Manager 主從式通訊。
    - 伺服器更新至 7.1.8 版或 8.1.2 版或者更新版本之後，SSL 通訊會自動加強以使用伺服器需要的 TLS 層次。

配置而無需自動憑證公佈

此實務範例詳細說明配置選項，影響不接受從伺服器自動公佈憑證時資料移轉裝置與 VMCLI 節點的安全。例如，如果伺服器配置為使用 LDAP 鑑別，或者憑證需要由憑證管理中心 (CA) 進行簽署時，不接受從伺服器自動公佈憑證。

影響階段作業安全的選項

安全設定的選項與第 53 頁的『透過使用預設安全設定（捷徑）進行配置』中說明的那些選項相同，但是您必須將 SSLACCEPTCERTFROMSERV 選項設為否，以確保當節點第一次連接至 7.1.8 版或 8.1.2 版或者更新版本伺服器時，資料移轉裝置節點不會自動接受伺服器的自簽公用憑證。

配置資料移轉裝置節點而無需自動憑證公佈的使用案例

如果自動憑證公佈不可能或不想要，則使用 dsmcert 公用程式來匯入憑證。 從 IBM Spectrum Protect 伺服器 或 CA 取得必要憑證。 CA 可以來自 VeriSign 或 Thawte 等公司，或者是在您的公司內維護的內部 CA。

如果資料移轉裝置與 VMCLI 節點位於同一機器上，則僅需要一個憑證。 如果節點位於不同的機器上，則每個機器需要一個憑證。

- 首先，伺服器會升級至 7.1.8 版或 8.1.2 版。 然後，升級 Data Protection for VMware。 現有資料移轉裝置節點不使用 SSL 通訊：
  - 使用值否設定 SSLACCEPTCERTFROMSERV 選項。
  - 從 IBM Spectrum Protect 伺服器 或從 CA 取得必要憑證，然後使用 dsmcert 公用程式以匯入憑證。 如需配置指示，請參閱配置透過 Secure Sockets Layer 進行的 Tivoli Storage Manager 主從式通訊。
- 首先，伺服器會升級至 7.1.8 版或 8.1.2 版。 然後，升級 Data Protection for VMware。 現有資料移轉裝置節點會使用 SSL 通訊：
  - 資料移轉裝置節點的安全選項不需要變更。 如果節點已具有用於 SSL 通訊的伺服器憑證，則 SSLACCEPTCERTFROMSERV 選項不適用。
  - 繼續使用具有現有伺服器公用憑證的 SSL 通訊。
  - 自動加強 SSL 通訊，以使用伺服器需要的 TLS 層次。
- 首先，Data Protection for VMware 會升級至 7.1.8 版或 8.1.2 版。 然後，稍後會升級伺服器。 現有資料移轉裝置節點不使用 SSL 通訊：
  - 使用值否設定 SSLACCEPTCERTFROMSERV 選項。
  - 現有鑑別通訊協定繼續用於早於 7.1.8 版或 8.1.2 版層次的伺服器。
  - 在資料移轉裝置節點連接至 7.1.8 版或 8.1.2 版或者更新版本伺服器之前：
    - 從 IBM Spectrum Protect 伺服器 或從 CA 取得必要憑證，然後使用 dsmcert 公用程式以匯入憑證。 如需配置指示，請參閱配置透過 Secure Sockets Layer 進行的 Tivoli Storage Manager 主從式通訊。
- 首先，Data Protection for VMware 會升級至 7.1.8 版或 8.1.2 版。 然後，稍後會升級伺服器。 現有資料移轉裝置節點會使用 SSL 通訊
  - 資料移轉裝置節點的安全選項不需要變更。 如果節點已具有用於 SSL 通訊的伺服器憑證，則 SSLACCEPTCERTFROMSERV 選項不適用。
  - 具有現有伺服器公用憑證的 SSL 通訊會繼續用於早於 7.1.8 版或 8.1.2 版層次的伺服器。
  - 伺服器更新至 7.1.8 版或 8.1.2 版或者更新版本之後，SSL 通訊會自動加強以使用伺服器需要的 TLS 層次。
- 首先，Data Protection for VMware 會升級至 7.1.8 版或 8.1.2 版。 然後，資料移轉裝置節點會連接至多個伺服器。 伺服器在兩個不同的時間進行升級：
  - 使用值否設定 SSLACCEPTCERTFROMSERV 選項。
  - 現有鑑別通訊協定繼續用於早於 7.1.8 版或 8.1.2 版層次的伺服器。
  - 在資料移轉裝置節點連接至 7.1.8 版或 8.1.2 版或者更新版本伺服器之前，或者在任何伺服器層次需要 SSL 通訊時：
    - 從 IBM Spectrum Protect 伺服器 或從 CA 取得必要憑證，然後使用 dsmcert 公用程式以匯入憑證。 如需配置指示，請參閱配置透過 Secure Sockets Layer 進行的 Tivoli Storage Manager 主從式通訊。
  - 資料移轉裝置節點將現有鑑別及階段作業安全通訊協定用於早於 7.1.8 版或 8.1.2 版的伺服器，並在起始連接至 7.1.8 版或 8.1.2 版或者更新版本的伺服器時，自動升級以使用 TLS 鑑別。 系統會管理每個伺服器的階段作業安全。

- 新的 Data Protection for VMware 安裝，伺服器處於 7.1.8 版或 8.1.2 版或者更新版本：
  - 根據新的安裝配置 Data Protection for VMware。
  - 使用值否設定 SSLACCEPTCERTFROMSERV 選項。
  - 從 IBM Spectrum Protect 伺服器 或從 CA 取得必要憑證，然後使用 dsmcert 公用程式以匯入憑證。 如需配置指示，請參閱配置透過 Secure Sockets Layer 進行的 Tivoli Storage Manager 主從式通訊。
  - 如果資料移轉裝置與伺服器之間的所有資料傳送都需要加密，則將 SSL 參數設為是值。
- 新的 Data Protection for VMware 安裝，伺服器處於早於 7.1.8 版或 8.1.2 版的版本，會需要 SSL 加密的階段作業：
  - 根據新的安裝配置 Data Protection for VMware。
  - 將 SSL 參數設為是值。
  - 從 IBM Spectrum Protect 伺服器 或從 CA 取得必要憑證，然後使用 dsmcert 公用程式以匯入憑證。 如需配置指示，請參閱配置透過 Secure Sockets Layer 進行的 Tivoli Storage Manager 主從式通訊。
- 新的 Data Protection for VMware 安裝，伺服器處於早於 7.1.8 版或 8.1.2 版的版本，不需要 SSL 加密的階段作業：
  - 根據新的安裝配置 Data Protection for VMware。
  - 使用值否設定 SSLACCEPTCERTFROMSERV 選項。
    - 除非伺服器稍後升級至 7.1.8 版或 8.1.2 版，否則使用非 SSL 鑑別通訊協定。
  - 在資料移轉裝置節點連接至 7.1.8 版或 8.1.2 版或者更新版本伺服器之前：
    - 從 IBM Spectrum Protect 伺服器 或從 CA 取得必要憑證，然後使用 dsmcert 公用程式以匯入憑證。 如需配置指示，請參閱配置透過 Secure Sockets Layer 進行的 Tivoli Storage Manager 主從式通訊。

使用傳輸層安全配置 Data Protection for VMware vSphere GUI 通訊

Data Protection for VMware vSphere GUI 使用「傳輸層安全 (TLS)」通訊協定，提供與 Web 瀏覽器；VMware vCenter Server；以及選擇性地 IBM Spectrum Protect 伺服器 的安全通訊.

關於這項作業

對於與 Web 瀏覽器及 VMware VCenter Server 的通訊，一律啟用 TLS 通訊協定。在 Data Protection for VMware 安裝期間，會產生一個自簽 TLS 數位憑證，該憑證隨後用於連線。

您也可以使用憑證管理中心 (CA) 簽署的憑證，以與 Web 瀏覽器進行通訊。 Data Protection for VMware若要使用 CA 提供的憑證，請參閱將協力廠商憑證用於 Web 瀏覽器階段作業。

對於與 IBM Spectrum Protect 伺服器 的通訊，TLS 通訊協定的使用取決於伺服器的版本。

如果您要使用 IBM Spectrum Protect 伺服器 7.1.7 版或 8.1.1 版或者更早版本

使用 TLS 通訊協定與伺服器進行通訊是選用項目。 您可以透過如第 58 頁的『啟用與 IBM Spectrum Protect 伺服器的安全通訊』中所述建立或更新信任

儲存庫並匯入憑證，手動啟用 Data Protection for VMware vSphere GUI 以透過 TLS 通訊協定與伺服器進行通訊。

如果您要稍後使用 IBM Spectrum Protect 伺服器 7.1.8 版或 8.1.2 版

需要 TLS 通訊協定。 在大部分情況下，透過使用第 53 頁的『透過使用預設安全設定（捷徑）進行配置』中說明的預設安全設定，在第一次使用時自動建立信任儲存庫。 然而，在部分實務範例中，您可能需要手動建立信任儲存庫。 .

重要：當 Data Protection for VMware vSphere GUI 第一次與伺服器進行通訊時，捷徑實務範例會自動取得憑證，假設 IBM Spectrum Protect 伺服器 **SESSIONSECURITY** 參數設為 **TRANSITIONAL**，這是第一次連線時的預設值。 GUI 連接至伺服器之後，**SESSIONSECURITY** 參數設為 **STRICT**。 因為 GUI 使用伺服器管理者 ID 連接至伺服器，如果另一個實體已使用該 ID 進行連接，則嘗試連接至伺服器時，將在 GUI 中顯示一則錯誤訊息。 若要解決此問題，請取得 **SESSIONSECURITY** 參數以返回 **TRANSITIONAL**。

啟用與 IBM Spectrum Protect 伺服器的安全通訊

如果您要使用 IBM Spectrum Protect 伺服器 7.1.7 版或更早版本或 8.1.2 版或更早版本，則使用 TLS 通訊協定進行的伺服器連線是選用項目，如果您想要啟用 Data Protection for VMware vSphere GUI 透過使用通訊協定與伺服器進行通訊，則必須手動啟用通訊。

開始之前

從伺服器管理者取得憑證副本。

關於這項作業

如果您要使用伺服器 7.1.8 版或 8.1.2 版或者更新版本，則需要 TLS 通訊協定，並且會透過使用第 53 頁的『透過使用預設安全設定（捷徑）進行配置』中說明的預設安全設定，在第一次使用時自動建立具有憑證的信任儲存庫。 然而，在部分實務範例中，您可能需要如本主題中所述手動建立信任儲存庫及配置 Data Protection for VMware vSphere GUI。

下列程序使用 Java™ 金鑰及憑證管理工具 **keytool**。

在 Linux 作業系統上，該工具位於 `/opt/tivoli/tsm/tdpvmware/common/jre/jre/bin/` 目錄中。

在 Microsoft Windows 作業系統上，該工具位於 `C:\Program Files\Common Files\Tivoli\TSM\jvm80516\jre` 目錄中。

執行 **keytool** 指令時，您可能需要指定完整路徑。

程序

1. 從指令行，將目錄變更至信任儲存庫位置：
   - 在 Linux 上：`/opt/tivoli/tsm/tdpvmware/common/scripts/`
   - 在 Windows 上：`C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\scripts\`
2. 使用下列指令來建立信任儲存庫，並匯入憑證：

```
keytool -importcert -alias my-cert -file cert.pem -keystore
tsm-ve-truststore.jks -storepass password
```

其中：

-alias *my-cert*
用於識別信任儲存庫中的憑證的唯一別名。

-file *cert.pem*
包含伺服器自簽憑證或 CA 主要憑證的檔案。

-storepass *password*
金鑰儲存庫密碼。 請務必記住密碼，以供未來使用。

3. 啟動 Data Protection for VMware vSphere GUI，然後移至「配置」視窗。
   - 如果您要建立起始配置，請按一下**作業** > **執行 IBM Spectrum Protect 配置精靈**，然後移至「伺服器認證」頁面。
   - 如果您要修改現有配置，請按一下**作業** > **編輯 IBM Spectrum Protect 配置**，然後移至「伺服器認證」頁面。
4. 在 **IBM Spectrum Protect 管理埠**欄位中輸入埠號。 這是容許使用 SSL 或 TLS 進行管理連線的伺服器埠。
5. 選取**在管理埠上使用加密通訊**。
6. 如果要在未來的 GUI 階段作業中使用此設定，請選取**儲存管理者 ID、密碼及埠設定**。
7. 按一下**確定**以套用變更。

使用憑證管理中心的憑證

若要使用憑證管理中心 (CA) 簽署的憑證，您必須完成多個步驟。

關於這項作業

下面的程序中使用稱為 **keytool** 的標準金鑰及憑證管理工具。

在 Linux 作業系統上，其位於 `/opt/tivoli/tsm/tdpvmware/common/jre/jre/bin/` 目錄中。

在 Microsoft Windows 作業系統上，它位於 `C:\Program Files\Common Files\Tivoli\TSM\jvm80516\jre` 目錄中。

從指令行執行 **keytool** 時，您可能需要指定完整路徑。

程序

1. 取得金鑰儲存庫的存取權。
2. 建立憑證簽署申請 (CSR)。
3. 將憑證簽署要求傳送至憑證管理中心以進行簽署。
4. 接收已簽章的憑證並置於 Data Protection for VMware vSphere GUI。

取得金鑰儲存庫的存取權：

憑證儲存在 Java 金鑰儲存庫中。 金鑰儲存庫內容受密碼保護。 若要操作金鑰儲存庫中的憑證，您必須取得金鑰儲存庫的存取權。

關於這項作業

安裝期間會自動產生預設自簽憑證及金鑰儲存庫密碼，因此您無法得知起始密碼。

完成下列程序，以使用新金鑰儲存庫及新自簽憑證來取代原始金鑰儲存庫。 您選擇的新金鑰儲存庫受密碼保護。

如果您已經知道金鑰儲存庫密碼，請跳過此程序。

程序

1. 停止 Data Protection for VMware vSphere GUI 服務。
2. 從指令行，將目錄變更至金鑰儲存庫位置。
   - 在 Linux 上：`/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/`
   - 在 Windows 上：`C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\resources\security\`
3. 將金鑰儲存庫檔 (`key.jks`) 重新命名或移至其他位置來製作備份副本。
4. 發出下列指令來建立新金鑰儲存庫及新自簽憑證：

   ```
   keytool -genkeypair -alias vekey -dname
   CN=fqdn,OU=Tivoli_Storage_Manager_for_VMware,O=IBM -keyalg RSA
   -sigalg SHA256withRSA -keysize 2048 -validity days -keystore
   key.jks -storepass password -keypass password
   ```

   其中：

   -dname CN=*fqdn*,OU=Tivoli_Storage_Manager_for_VMware,O=IBM
   fqdn 是安裝 Data Protection for VMware vSphere GUI 之電腦的 DNS 名稱或完整網域名稱。

   -validity *days*
   憑證的有效期間。

   -storepass *password*
   金鑰儲存庫密碼。 請務必記住密碼，以供未來使用。

   -keypass *password*
   憑證的私密金鑰密碼。 此密碼必須符合金鑰儲存庫密碼。
5. 使用 **securityUtility** 工具對金鑰儲存庫密碼編碼。 發出下列指令。
   - 在 Linux 上：`/opt/tivoli/tsm/tdpvmware/common/webserver/bin/securityUtility encode`
   - 在 Windows 上：`C:\IBM\SpectrumProtect\webserver\bin\securityUtility.bat encode`

   出現提示時，輸入您的金鑰儲存庫，然後儲存輸出（例如，將其複製到剪貼簿中）。
6. 在編輯器中開啟 `bootstrap.properties` 檔案，然後將 `veProfile.keystore.pswd` 內容設為前一個步驟中的編碼值。 `bootstrap.properties` 檔位於下列位置中：

- 在 Linux 上：/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/
- 在 Windows 上：C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\

7. 啟動 Data Protection for VMware vSphere GUI 服務。

相關參考:

第 79 頁的『啟動及執行 Data Protection for VMware 的服務』

建立憑證簽署申請：

取得金鑰儲存庫的存取權之後，您必須建立憑證簽署申請 (CSR)。

程序

完成下列步驟來建立 CSR：

1. 從指令行，將目錄變更至金鑰儲存庫位置。
   - 在 Linux 上：/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/
   - 在 Windows 上：C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\resources\security\
2. 發出下列指令來建立新憑證：

   ```
   keytool -genkeypair -alias mykey -dname
   CN=fqdn,OU=unit,O=organization -keyalg RSA -sigalg SHA256withRSA
   -keysize 2048 -validity days -keystore key.jks -storepass
   password -keypass password
   ```

   其中：

   -alias *mykey*
   mykey 是用於識別金鑰儲存庫中的憑證的唯一別名。 接收已簽章的憑證時會重新命名。

   -dname CN=*fqdn***,OU=***unit***,O=***organization*
   fqdn 是安裝 Data Protection for VMware vSphere GUI 之電腦的 DNS 名稱或完整網域名稱。

   Unit 及 *organization* 是您的原則或憑證管理中心需要的組織資訊。

   -validity *days*
   憑證的有效期間。

   -storepass *password*
   金鑰儲存庫密碼。 如果您不知道或忘記了金鑰儲存庫密碼，請參閱第 60 頁的『取得金鑰儲存庫的存取權』。

   -keypass *password*
   憑證的私密金鑰密碼。 此密碼必須符合金鑰儲存庫密碼。
3. 發出下列指令來建立 CSR：

   ```
   keytool -certreq -alias mykey -file certreq.pem -keystore key.jks
   ```

   其中：

-alias *mykey*
前一個步驟中的憑證別名。

-file *certreq.pem*
用於儲存憑證簽署申請的檔案。

將憑證簽署申請傳送至憑證管理中心：

建立憑證申請 (certreq.pem) 之後，您必須將其傳送至憑證管理中心進行簽署。 請遵循憑證管理中心的特定指示。

接收已簽章的憑證：

從憑證管理中心 (CA) 取得已簽章的憑證之後，您必須接收憑證並置於金鑰儲存庫中。

程序

如果要接收已簽章的憑證，請完成下列步驟：

1. 從指令行，將目錄變更至金鑰儲存庫位置。
   - 在 Linux 上：/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/
   - 在 Windows 上：C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\resources\security\
2. 將您從 CA 接收的檔案複製到此位置。 這些檔案包括 Data Protection for VMware vSphere GUI 的 CA 主要憑證、中繼 CA 憑證（如果有）及已簽章的憑證。
3. 停止 Data Protection for VMware vSphere GUI 服務。
4. 將金鑰儲存庫檔 (key.jks) 複製為其他名稱或複製到其他位置來製作備份副本。
5. 使用下列指令匯入中繼 CA 憑證（如果有）。 當系統提示您信任憑證時，請回答 *yes*。 視需要，針對多個中繼 CA 重複此步驟。

   ```
   keytool -importcert -alias ca-intermediate -file intermediate.pem
   -keystore key.jks -storepass password
   ```

   其中：

   -alias *ca-intermediate*
   用於識別金鑰儲存庫中的憑證的唯一別名。 每一個中繼憑證必須具有唯一別名。

   -file *intermediate.pem*
   從 CA 取得的中繼憑證檔案。

   -storepass *password*
   金鑰儲存庫密碼。
6. 發出下列指令來匯入 CA 主要憑證。 當系統提示您信任此憑證時，請回答 *yes*。

   ```
   keytool -importcert -alias ca-root -file root.pem -keystore
   key.jks -storepass password
   ```

   其中：

   -alias *ca-root*
   用於識別金鑰儲存庫中的憑證的唯一別名。

-file *root.pem*
從 CA 取得的主要憑證檔案。

-storepass *password*
金鑰儲存庫密碼。

7. 發出下列指令來匯入已簽章的憑證：

```
keytool -importcert -alias mykey -file signedcert.pem -keystore
key.jks -storepass password
```

其中：

-alias *mykey*
已簽章的憑證的別名。 該別名必須與產生憑證簽章要求 (CSR) 時使用的相同。

-file *signedcert.pem*
從 CA 接收的已簽章的憑證檔案。

-storepass *password*
金鑰儲存庫密碼。

8. 刪除包含 vekey 別名的現有憑證：

```
keytool -delete -alias vekey -keystore key.jks -storepass password
```

其中 -storepass *password* 是金鑰儲存庫的密碼。

9. 將已簽章的憑證重新命名為 vekey：

```
keytool -changealias -alias mykey -destalias vekey -keystore
key.jks -storepass password
```

其中：

-alias *mykey*
已簽章的憑證的別名。

-storepass *password*
金鑰儲存庫密碼。

10. 啟動 Data Protection for VMware vSphere GUI 服務。

相關參考:

第 79 頁的『啟動及執行 Data Protection for VMware 的服務』

VMware vCenter Server 使用者專用權需求

執行 Data Protection for VMware 作業需要某些 VMware vCenter Server 專用權。

使用 Data Protection for VMware vSphere GUI 的 Web 瀏覽器視圖保護 VMware 資料中心所需的 vCenter Server 專用權

登入 Data Protection for VMware vSphere GUI 之瀏覽器視圖的 vCenter Server 使用者 ID

必須具有足夠的 VMware 專用權，以檢視 GUI 管理之資料中心的內容。

例如，VMware vSphere 環境包含五個資料中心。 使用者 『jenn』 只具有其中兩個資料中心的足夠專用權。 因此，『jenn』 在視圖中只能看到其具有足夠專用權的那兩個資料中心。 使用者 『jenn』 無法看到其他三個資料中心（『jenn』 沒有它們的足夠專用權）。

VMware vCenter Server 將一組專用權統一定義為角色。 角色會套用至指定使用者或群組的物件以建立專用權。 從 VMware vSphere Web 用戶端中，您必須建立具有一組專用權的角色。 若要建立 vCenter Server 角色以進行備份及還原作業，請使用 VMware vSphere Client 的**新增角色**功能。

如果您要將專用權延伸到 vCenter 內的所有資料中心，請指定 vCenter Server 並選取延伸到子項勾選框。 否則，如果您在選取延伸到子項勾選框的情況下僅將角色指派給所需的資料中心，則會限制許可權。 瀏覽器 GUI 的強制執行位於資料中心層次。

下列範例顯示如何控制對兩個 VMware 使用者群組的資料中心進行存取。 首先建立一個角色，以包含 Technote 7047438 中定義的所有專用權。 此範例中的這組專用權由名稱為 『TDPVMwareManage』 的角色識別。 群組 1 需要存取權才能管理 `Primary1_DC` 及 `Primary2_DC` 資料中心的虛擬機器。 群組 2 需要存取權才能管理 `Secondary1_DC` 及 `Secondary2_DC` 資料中心的虛擬機器。

針對群組 1，將 『TDPVMwareManage』 角色指派給 `Primary1_DC` 和 `Primary2_DC` 資料中心。 針對群組 2，將 『TDPVMwareManage』 角色指派給 `Secondary1_DC` 和 `Secondary2_DC` 資料中心。

每一個 VMware 使用者群組中的使用者都可以使用 Data Protection for VMware GUI，來僅管理其各自資料中心內的虛擬機器。

提示：建立角色時，請考量將額外專用權新增至您稍後對物件完成其他作業時可能需要的角色。

使用資料移轉裝置所需的 vCenter Server 專用權

安裝在 vStorage 備份伺服器（資料移轉裝置節點）上的 IBM Spectrum Protect 資料移轉裝置需要 `VMCUser` 和 `VMCPw` 選項。 `VMCUser` 選項指定您要備份、還原或查詢之 vCenter 或 ESX 伺服器的使用者 ID。 指派給此使用者 ID (`VMCUser`) 的必要專用權可確保用戶端能夠在虛擬機器及 VMware 環境上執行作業。 這個使用者 ID 必須擁有上方 Technote 中所說明的 VMware 專用權。

若要建立 vCenter Server 角色以進行備份及還原作業，請使用 VMware vSphere Client 的**新增角色**功能。 新增此使用者 ID (`VMCUser`) 的專用權時，必須選取延伸到子項選項。 此外，請考量新增其他專用權給此角色以用於備份及還原以外的作業。 對於 `VMCUser` 選項，強制執行是在最上層物件層次進行。

使用 Data Protection for VMware vSphere GUI 的 IBM Spectrum Protect vSphere Client 外掛程式視圖保護 VMware 資料中心所需的 vCenter Server 專用權

IBM Spectrum Protect vSphere Client 外掛程式需要一組不同於登入 GUI 所需專用權的專用權。

在安裝期間，會為 IBM Spectrum Protect vSphere Client 外掛程式建立下列自訂專用權：

- **資料中心** > **IBM Data Protection**
- **廣域** > **配置 IBM Data Protection**

IBM Spectrum Protect vSphere Client 外掛程式所需的自訂專用權會登錄為個別延伸。專用權延伸索引鍵是 `com.ibm.tsm.tdpvmware.IBMDataProtection.privileges`。

這些專用權容許 VMware 管理者啟用及停用對 IBM Spectrum Protect vSphere Client 外掛程式內容的存取。 只有具備所需 VMware 物件之上述自訂專用權的使用者才能存取 IBM Spectrum Protect vSphere Client 外掛程式內容。 會對每一個 vCenter Server 登錄一個 IBM Spectrum Protect vSphere Client 外掛程式，且它由配置為支援 vCenter Server 的所有 GUI 主機共用。

從 VMware vSphere Web 用戶端中，您必須針對可使用 IBM Spectrum Protect vSphere Client 外掛程式來完成虛擬機器資料保護功能的使用者，建立一個角色。 針對此角色，除了 Web 用戶端所需的標準虛擬機器管理者角色專用權之外，您還必須指定**資料中心** > **IBM Data Protection** 專用權。 針對每一個資料中心，對您要為其授與許可權的每一個使用者或使用者群組指派此角色，以讓該使用者管理虛擬機器。

vCenter 層次的使用者需要**廣域** > **IBM Data Protection** 專用權。 此專用權容許使用者管理、編輯或清除 vCenter Server 與 Data Protection for VMware vSphere GUI Web 伺服器之間的連線。 請將此專用權指派給熟悉保護其各自 vCenter Server 之 Data Protection for VMware vSphere GUI 的管理者。 您可在該延伸的「連線」頁面上管理 IBM Spectrum Protect vSphere Client 外掛程式連線。

下列範例顯示如何針對兩個使用者群組控制對資料中心的存取。 群組 1 需要管理 `NewYork _DC` 和 `Boston_DC` 資料中心的虛擬機器所需的存取權。 群組 2 需要管理 `LosAngeles_DC` 和 `SanFranciso_DC` 資料中心的虛擬機器所需的存取權。

從 VMware vSphere 用戶端中，以建立 『IBMDataProtectManage』 角色為例，指派標準虛擬機器管理者角色專用權以及**資料中心** > **IBM Data Protection** 專用權。

針對群組 1，將 『IBMDataProtectManage』 角色指派給 `NewYork` 和 `Boston_DC` 資料中心。 針對群組 2，將 『IBMDataProtectManage』 角色指派給 `LosAngeles_DC` 和 `SanFranciso_DC` 資料中心。

每一個群組中的使用者都可以在 vSphere Web 用戶端中使用 IBM Spectrum Protect vSphere Client 外掛程式，以僅管理其各自資料中心內的虛擬機器。

與許可權不足相關的問題

當 Web 瀏覽器使用者沒有任何資料中心的足夠許可權時，即會封鎖對視圖的存取。 系統會發出錯誤訊息 GVM2013E，以告知使用者未獲授權來存取任何受管理資料中心，原因是許可權不足。 也會提供其他新訊息來通知使用者許可權不足導致的問題。 若要解決任何與許可權相關的問題，請確保已如之前的小節所述設定使用者角色。 該使用者角色必須具有「vCenter Server 使用者 ID 及資料移轉裝置的必要專用權」表格中所識別的所有專用權，並且這些專用權必須在資料中心層次套用且選取了延伸到子項勾選框。

當 IBM Spectrum Protect vSphere Client 外掛程式使用者沒有資料中心的足夠許可權時，該資料中心及其內容的資料保護功能將變成在該延伸中無法使用。

當 IBM Spectrum Protect 使用者 ID（由 VMCUser 選項指定）包含的許可權不足以進行備份及還原作業時，會顯示下列訊息：

```
ANS9365E VMware vStorage API 錯誤。
「執行此作業的許可權遭到拒絕。」
```

當 IBM Spectrum Protect 使用者 ID 包含的許可權不足以檢視機器時，會顯示下列訊息：

```
備份 VM 指令已啟動。  要處理的虛擬機器總數：1
ANS4155E 在 VMware 伺服器上找不到虛擬機器 'tango'。
ANS4148E 虛擬機器 'foxtrot' 的完整 VM 備份失敗，RC 為 4390
```

如需專用權使用的進一步資訊，請參閱 **Data Protection for VMware vSphere GUI 及資料移轉裝置所需要的 vCenter Server 專用權**上的附註。

若要透過 VMware Virtual Center Server 擷取許可權問題的日誌資訊，請完成下列步驟：

1. 在「vCenter Server 設定」中，選取**記載選項**並將 **vCenter 記載**設定為 **Trivia (Trivia)**。
2. 重建許可權錯誤。
3. 將 **vCenter 記載**重設為其前一個值以防止記錄過多的日誌資訊。
4. 在「系統日誌」中，尋找最新的 vCenter Server 日誌 (vpxd-*wxyz*.log) 並搜尋字串 NoPermission。 例如：

   ```
   [2011-04-27 15:15:35.955 03756 verbose 'App'] [VpxVmomi] Invoke error:
   vim.VirtualMachine.createSnapshot session: 92324BE3-CD53-4B5A-B7F5-96C5FAB3F0EE
   Throw: vim.fault.NoPermission
   ```

   此日誌訊息指出該使用者 ID 未包含足夠許可權來建立 Snapshot (createSnapshot)。

Data Protection for VMware vSphere GUI使用者角色

Data Protection for VMware vSphere GUI 功能是否可用是根據指派給 IBM Spectrum Protect 管理者 ID 的權限層級。

管理者 ID 必須符合節點名稱。 在較早的產品版本中，**REGISTER NODE** 指令會自動建立名稱符合節點名稱的管理使用者 ID。 從 IBM Spectrum Protect 8.1 版開始，**REGISTER NODE** 指令不會自動建立符合節點名稱的管理使用者 ID。

登錄新的節點時，IBM Spectrum Protect 伺服器管理者必須指定 userid 參數，以及 **REGISTER NODE** 伺服器指令：

```
REGISTER NODE node_name password userid=user_id
```

其中，節點名稱與管理使用者 ID 必須相同。 例如：

```
REGISTER NODE node_a mypassw0rd userid=node_a
```

依預設，節點具有用戶端擁有者權限。

您利用 Data Protection for VMware vSphere GUI 執行的作業基於指派給管理者 ID 專用權類別。

當管理者 ID 沒有未受限原則網域專用權時，您無法在 IBM Spectrum Protect 伺服器上登錄新節點或設定其 Proxy 關係。如果您未輸入管理者 ID 而繼續進行，會建立巨集 Script，讓您可以在 IBM Spectrum Protect 伺服器上執行。

配置 Data Protection for VMware vSphere GUI 時，會要求 IBM Spectrum Protect 管理者 ID。 這份表格列出根據指派給該 ID 的專用權類別而可用的功能：

- 「是」值指出可供 user 角色使用的功能。
- 「否」值指出無法供 user 角色使用的功能。

若要檢視您目前的 Data Protection for VMware vSphere GUI 角色，請將游標移至導覽列中的使用者 ID 上。

表 *11.* 根據 *IBM Spectrum Protect* 管理者 *ID* 專用權需求的可用功能

	操作員	**操作員，含報告**	**受限管理者**	**管理者**
摘要	立即執行備份及還原	操作員加上報告	操作員加上報告及所列出原則網域的排程作業	所有角色，包括起始配置
IBM Spectrum Protect 管理者 ID 專用權類別	無	下列其中一個專用權類別： • 儲存裝置 • 操作員 • 分析師	原則（受限）或下列其中一個專用權類別： • 儲存裝置 • 操作員 • 分析師	原則（未受限）或系統
		備份標籤		
管理**立即執行**備份作業	Yes	Yes	Yes	Yes
管理**排程**備份作業	否[1]	否[1]	是，在原則網域內	Yes
檢視**立即執行**備份作業	Yes	Yes	Yes	Yes
檢視**排程**備份作業	否	Yes	Yes	Yes
刪除**排程**備份作業	否	否	是，在原則網域內	Yes
		還原標籤		
執行**還原**作業	Yes	Yes	Yes	Yes
		報告標籤		
事件	否	Yes	Yes	Yes
最近作業	Yes	Yes	Yes	Yes

表 *11.* 根據 *IBM Spectrum Protect* 管理者 *ID* 專用權需求的可用功能 *(*繼續*)*

	操作員	操作員，含報告	受限管理者	管理者
備份狀態	否	Yes	Yes	Yes
應用程式保護	否	Yes	Yes	Yes
資料中心佔有率	否	Yes	Yes	Yes
		配置標籤		
節點登錄（配置狀態 -> **執行配置精靈**）	否	否	否[2]	Yes
變更 IBM Spectrum Protect 管理者 ID 認證（配置狀態 -> **編輯配置**）	Yes	Yes	Yes	Yes
變更 VMCLI 節點密碼（配置狀態 -> **編輯配置**）	否	否	Yes	Yes
變更 GUI 網域（配置狀態 -> **編輯配置**）	是[3]	是[3]	是[3]	Yes
變更資料移轉裝置節點（配置狀態 -> **編輯配置**）	否	否	否[2]	Yes
變更裝載 Proxy 節點（配置狀態 -> **編輯配置**）	否	否	否[2]	Yes

1. 您無法登錄節點，因為需要不受限網域原則。
2. 您可以新增或移除 VMware 資料中心以及登錄資料中心節點。

若要檢視 IBM Spectrum Protect 管理者 ID 權限層級和對應的 Data Protection for VMware vSphere GUI 角色，請執行下列動作：

1. 移至「配置」視窗。
2. 按一下**編輯配置**。
3. 「Spectrum Protect 伺服器認證」頁面會顯示相關資訊。

重要：

- 如果 IBM Spectrum Protect 伺服器上 IBM Spectrum Protect 管理者 ID 權限層級發生變更，則必須重新啟動 Data Protection for VMware vSphere GUI 才能反映此變更。
- 變更「使用者角色」時，必須按一下**確定**以儲存變更，再移至另一個「配置設定」頁面或嘗試其他配置變更。否則，「使用者角色」變更不會生效。

Data Protection for VMware GUI 登錄金鑰

視您在安裝期間選取的選項而定，您可以使用不同的方法來存取 Data Protection for VMware GUI。 已為 Data Protection for VMware GUI 建立登錄金鑰。

詞組 『Data Protection for VMware GUI』 適用於下列 GUI：

- 在 Web 瀏覽器中存取的 Data Protection for VMware vSphere GUI
- vSphere Web Client GUI 中的 IBM Spectrum Protect vSphere Client 外掛程式

IBM Spectrum Protect vSphere Client 外掛程式 登錄索引鍵為 `com.ibm.tsm.tdpvmware.IBMDataProtection`。 安裝期間選取**登錄 vSphere Web Client 延伸**勾選框時，會登錄此索引鍵。每個 vCenter Server 皆登錄 IBM Spectrum Protect vSphere Client 外掛程式的單一實例。

不會為以 Web 瀏覽器存取的 Data Protection for VMware vSphere GUI 建立登錄索引鍵。

如果要檢視登錄索引鍵，請登入「VMware 受管理物件瀏覽器 (MOB)」。 登入 MOB 後，移至**內容→延伸管理程式**以檢視登錄索引鍵。

配置 Recovery Agent GUI

系統提供了關於如何設定 Recovery Agent GUI 以進行裝載、檔案還原或即時還原作業的指示。

開始之前

嘗試在 Recovery Agent GUI 中執行作業之前，必須完成這些配置作業。

重要：有關如何使用 Recovery Agent GUI 來完成作業的資訊在隨 GUI 一起安裝的線上說明中提供。 按一下任何 GUI 視窗中的**說明**可以開啟線上說明以取得作業協助。

程序

1. 登入您要還原檔案的系統。 「Recovery Agent」必須安裝在系統上。
2. 按一下「Recovery Agent GUI」中的**選取 TSM 伺服器**以連接至 IBM Spectrum Protect 伺服器。 當 Recovery Agent 安裝在與 Data Protection for VMware vSphere GUI 相同的系統上時，且使用 Data Protection for VMware vSphere GUI 配置精靈順利配置應用程式時，存在下列狀況：
   - 資料移轉裝置節點和 IBM Spectrum Protect 伺服器移入 Recovery Agent TSM Server 欄位。
   - 下列欄位移入「TSM Server 資訊」畫面：
     - **鑑別節點**包含可用的資料移轉裝置節點清單。
     - **目標節點**包含可用於所選資料移轉裝置節點的資料中心節點清單。

   當使用配置精靈從本端僅定義一個資料移轉裝置節點時，Recovery Agent 在啟動時使用該節點進行鑑別。Recovery Agent 會記住連接至 IBM Spectrum Protect 伺服器的前次節點名稱。 如果為此節點（要連接的前次節點名稱）選取**使用密碼存取權產生**，Recovery Agent 在啟動時會使用這些認證連接至 IBM Spectrum Protect 伺服器。 如果之前未連接至 IBM Spectrum Protect 伺服器，且僅使用精靈

配置一個資料移轉裝置節點和一個資料中心節點，則 Recovery Agent 在啟動時會使用這些認證連接至 IBM Spectrum Protect 伺服器。

指定下列選項：

伺服器位址
輸入 IBM Spectrum Protect 的 IP 位址或主機名稱。

伺服器埠
輸入與伺服器進行 TCP/IP 通訊所用的埠號。 預設埠號是 1500。

節點存取方法：

Asnodename
選取這個選項時，可使用 Proxy 節點來存取在目標節點中的 VM 備份。 Proxy 節點是指獲授與 "proxy" 權限的節點，可代表目標節點執行作業。

一般而言，IBM Spectrum Protect 管理者會使用 `grant proxynode` 指令，在兩個現有的節點之間建立 Proxy 關係。

如果您選取這個選項，請完成下列步驟：

a. 在**目標節點**欄位中輸入目標節點的名稱（VM 備份所在的節點）。
b. 在**鑑別節點**欄位中輸入 Proxy 節點的名稱。
c. 在**密碼**欄位中輸入 Proxy 節點的密碼。
d. 按一下**確定**來儲存這些設定，並且結束「IBM Spectrum Protect」資訊對話框。

使用這種方法時，「Recovery Agent」使用者只知道 Proxy 節點密碼，而目標節點密碼是受保護的。

Fromnode
選取這個選項時，可使用其存取權僅限於目標節點中特定 VM 的 Snapshot 資料之節點。

一般而言，是從擁有 VM 備份的目標節點使用 `set access` 指令授與存取權給這個節點：

```
set access backup -TYPE=VM vmdisplayname mountnodename
```

例如，此指令為名稱為 `myMountNode` 的節點提供了權限，可從名稱為 `myTestVM` 的 VM 還原檔案：

```
set access backup -TYPE=VM myTestVM myMountNode
```

如果您選取這個選項，請完成下列步驟：

a. 在**目標節點**欄位中輸入目標節點的名稱（VM 備份所在的節點）。
b. 在**鑑別節點**欄位中輸入獲授與有限存取權之節點的名稱。
c. 在**密碼**欄位中輸入獲授與有限存取權之節點的密碼。
d. 按一下**確定**來儲存這些設定，並且結束「IBM Spectrum Protect」資訊對話框。

使用這種方法時，您可以查看完整的已備份 VM 清單。 不過，您只能還原節點獲授與存取權的那些 VM 備份。 此外，不會防止 Snapshot 資料在伺服器上到期。 因此，在這種方法中並不支援即時還原。

直接 選取這個選項，可直接向目標節點（VM 備份所在的節點）鑑別。

如果您選取這個選項，請完成下列步驟：

a. 在**鑑別節點**欄位中輸入目標節點的名稱（VM 備份所在的節點）。

b. 在**密碼**欄位中輸入目標節點的密碼。

c. 按一下**確定**來儲存這些設定，並且結束「IBM Spectrum Protect」資訊對話框。

使用密碼存取權產生

選取此選項且密碼欄位為空時，Recovery Agent 會使用登錄中儲存的現有密碼進行鑑別。 如果未選取，您必須手動輸入密碼。

若要使用此選項，您必須首先手動設定選項所適用之節點的起始密碼。 當您透過在**密碼**欄位中輸入密碼，並選取**使用密碼存取產生**勾選框，第一次連接至 IBM Spectrum Protect 節點時，必須指定起始密碼。

然而，當您使用本端資料移轉裝置節點作為**鑑別節點**時，密碼可能已儲存於登錄中。 為此，選取**使用密碼存取產生**勾選框，且不輸入密碼。

Recovery Agent 會向指定伺服器查詢受保護 VM 的清單，並且顯示這份清單。

3. 按一下**設定**來設定下列的裝載、備份和還原選項：

虛擬磁區寫入快取

在 Windows 備份 Proxy 主機上執行的 Recovery Agent 會儲存在即時還原和裝載期間所建立的資料變更。 這些變更會儲存在寫入快取中的虛擬磁區上。 依預設，會啟用寫入快取，然後指定 `C:\ProgramData\Tivoli\TSM\TDPVMware\mount\` 路徑，快取大小上限為所選取資料夾可用空間的 90%。 如果要防止系統磁區滿載，請將寫入快取變更為系統磁區以外的磁區上的路徑。

暫存檔的資料夾

指定要儲存資料變更的路徑。 寫入快取必須在本端磁碟機上，而且不能設為共用資料夾上的路徑。 如果寫入快取停用或空間用完，則嘗試啟動還原或裝載階段作業會失敗。

快取大小

指定寫入快取的大小。 容許的快取大小上限為所選取資料夾可用空間的 90%。

限制：若要在還原處理期間防止任何岔斷，請從所有防毒軟體保護設定排除寫入快取路徑。

資料存取

指定要存取的資料類型。 如果您使用離線裝置（例如磁帶或虛擬磁帶庫），您必須指定適用的資料類型。

儲存體類型

指定要用來裝載 Snapshot 的下列其中一個來源儲存裝置：

磁碟/檔案

從磁碟或檔案來裝載 Snapshot。 這個裝置是預設值。

磁帶 從磁帶儲存區來裝載 Snapshot。 當選取此選項時，就無法裝載多個 Snapshot 或執行即時還原作業。

VTL 從離線虛擬磁帶庫來裝載 Snapshot。 支援在相同的虛擬磁帶庫上進行並行的裝載階段作業。

註：變更儲存體類型時，必須重新啟動服務，讓變更生效。

停用到期保護

在裝載作業期間，已鎖定 IBM Spectrum Protect 伺服器上的 Snapshot，以防止它在作業期間到期。 可能由於將另一個 Snapshot 新增至已裝載的 Snapshot 序列而發生到期。 這個值會指定在裝載作業期間是否停用到期保護。

- 若要保護 Snapshot 以防止到期，請不要選取這個選項。 已鎖定 IBM Spectrum Protect 伺服器上的 Snapshot，以保護 Snapshot 來防止在裝載作業期間到期。
- 若要停用到期保護，請選取這個選項。 依預設，會選取這個選項。 未鎖定 IBM Spectrum Protect 伺服器上的 Snapshot，且不會保護 Snapshot 來防止在裝載作業期間到期。 因此，Snapshot 可能在裝載作業期間到期。 這個到期可能會產生非預期的結果，並對裝載點產生負面影響。 例如，裝載點可能變成無法使用或包含錯誤。 然而，到期未影響現行作用中副本。 作用中副本不能在作業期間到期。

  當 Snapshot 位於目標抄寫伺服器上時，Snapshot 由於處於唯讀模式而不能鎖定。 伺服器嘗試鎖定會導致裝載作業失敗。 若要避免鎖定嘗試，並防止此類失敗，請透過選取此選項來停用到期保護。

先讀大小（以 16 KB 區塊為單位）

指定在讀取要求傳送至單一區塊後，從儲存裝置擷取的額外資料區塊數目。預設值如下：

- 磁碟或檔案：64
- 磁帶：1024
- VTL：64

任何裝置的上限值是 1024。

先讀快取大小（以區塊為單位）

針對要儲存額外資料區塊的快取指定其大小。 預設值如下：

- 磁碟或檔案：10000
- 磁帶：75000
- VTL：10000

由於每一個 Snapshot 都有其自己的快取記憶體，因此請務必規劃要同步裝載或還原多少 Snapshot。 累加的快取記憶體大小不得超過 75000 個區塊。

驅動程式逾時（以秒為單位）

這個值指定處理來自檔案系統驅動程式之資料要求的時間量。 如果處理未及時完成，則會取消要求，並將錯誤傳回給檔案系統驅動程式。 當您遇到逾時狀況時，請考慮增加這個值。 例如，當網路緩慢，儲存裝置忙碌，或者正在處理多個裝載或即時還原階段作業時，可能會發生逾時。 預設值如下：

- 磁碟或檔案：60
- 磁帶：180

- VTL：60

按一下**確定**來儲存您的變更並結束**設定**。

4. 請確認每一個 IBM Spectrum Protect 伺服器節點（使用 Asnodename 和 Fromnode 選項所指定）容許備份被刪除。 Recovery Agent 會在作業期間建立未用的暫時物件。 BACKDELete=Yes 伺服器選項容許移除這些物件，以便它們不會在節點中累計。
   a. 登入「IBM Spectrum Protect」伺服器，然後在指令行模式中啟動管理用戶端階段作業：

      ```
      dsmadmc -id=admin -password=admin -dataonly=yes
      ```

   b. 輸入下列指令：

      ```
      Query Node <nodename> Format=Detailed
      ```

      請確定每一個節點的指令輸出都包括下列陳述式：

      ```
      Backup Delete Allowed?: Yes
      ```

      如果未包括這個陳述式，請使用下列指令更新每一個節點：

      ```
      UPDate Node <nodename> BACKDELete=Yes
      ```

      針對每一個節點再度執行 Query Node 指令，以確認各個節點皆容許備份被刪除。

5. 如果在 iSCSI 網路中使用 Recover Agent，而且此 Recovery Agent 未使用資料移轉裝置，請移至 C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf 檔並指定 [IMOUNT] 標籤與 **Target IP** 參數：

   ```
   [IMOUNT config]
   Target IP=<IP address of the network card on the system
   that exposes the iSCSI targets.>
   ```

   例如：

   ```
   [General config]
   param1
   param2
   ...
   [IMount config]
   Target IP=9.11.153.39
   ```

   新增或變更 Target IP 參數後，請重新啟動 Recovery Agent GUI 或 Recovery Agent CLI。

啟用從 Recovery Agent 到 IBM Spectrum Protect 伺服器的安全通訊

如果將 IBM Spectrum Protect 伺服器配置為使用 Secure Sockets Layer (SSL) 或傳輸層安全 (TLS) 通訊協定，您可以啟用 Recovery Agent 以透過通訊協定與伺服器通訊。

開始之前

在開始配置伺服器的安全通訊之前，請考量下列需求：

- 為 SSL 啟用的每一個伺服器都必須具有唯一的憑證。 憑證可以是下列其中一個類型：
  - 由伺服器自簽的憑證。

- 由協力廠商憑證管理中心 (CA) 憑證發出的憑證。 CA 憑證可以來自 Symantec 或 Thawte 等公司，或者是在您的公司內維護的內部憑證。

- 由於效能原因，SSL 或 TLS 僅用於需要安全的階段作業。 請考量在伺服器系統上新增更多處理器資源，以管理增加的需求。
- 對於連接到使用 TLS 1.2 版之伺服器的用戶端，憑證簽章演算法必須是「安全雜湊演算法 1 (SHA-1)」或更新版本。 如果您要將自簽憑證用於使用 TSL 1.2 版的伺服器，則必須使用 cert256.arm 憑證。 您的 IBM Spectrum Protect 管理者可能需要變更伺服器上的預設憑證。
- 若要停用沒有 TLS 1.2 安全的安全通訊協定，請將 **SSLDISABLELEGACYtls yes** 選項新增至 C:\windows\system32\fb.opt 或 C:\Windows\SysWOW64\fb.opt 檔案。 TLS 1.2 或更新版本協助防止惡意程式的攻擊。

透過使用 IBM Spectrum Protect 伺服器自簽憑證啟用安全通訊

如果 IBM Spectrum Protect 伺服器正在使用自簽憑證，則必須從伺服器管理者取得該憑證的副本，並配置 Recovery Agent 以透過使用 SSL 或 TLS 通訊協定與伺服器進行通訊。

關於這項作業

每一個伺服器都產生其自己的憑證。 如果伺服器在使用 TLS 1.2 或更新版本，則 6.3 版以及更新版本伺服器產生名為 cert256.arm 的檔案，如果伺服器在使用較早版本的 SSL 或 TLS，則會產生名為 cert.arm 的檔案。 6.3 版之前的伺服器版本產生名為 cert.arm 的檔案，而無論通訊協定為何。 您必須選擇在伺服器上設為預設值的憑證。

憑證檔儲存在伺服器實例目錄中的伺服器工作站上。 例如，C:\IBM\tivoli\tsm\server\bin\cert256.arm。 如果憑證檔不存在，則當您在設定這些選項的情況下重新啟動伺服器時，會建立憑證檔。

程序

若要透過使用自簽憑證，啟用從回復代理程式到伺服器的 SSL 或 TLS 通訊：

1. 將 GSKit 二進位路徑及二進位路徑附加至用戶端上的 PATH 環境變數。 例如：

   ```
   set PATH=C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\bin\;
       C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\lib64;%PATH%
   ```

2. 如果您是第一次在用戶端上配置 SSL 或 TLS，則必須建立用戶端本端金鑰資料庫 dsmcert.kdb。 從 C:\Windows\SysWOW64 目錄，執行 **gsk8capicmd_64** 指令，如下列範例中所示：

   ```
   gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -pw password -stash
   ```

   您提供的密碼用來加密金鑰資料庫。 密碼自動加密儲存在隱藏檔 (dsmcert.sth) 中。用戶端使用隱藏檔來擷取金鑰資料庫密碼。

3. 取得伺服器自簽憑證。
4. 將憑證匯入至 dsmcert.kdb 資料庫。 您必須將每一個用戶端的憑證匯入至 dsmcert.kdb。 從 C:\Windows\SysWOW64 目錄，執行 **gsk8capicmd_64** 指令，如下列範例中所示：

   ```
   gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "Server server_name self-signed key"
   -file path_to_certificate -format ascii -trust enable
   ```

可以將多個伺服器憑證新增至 dsmcert.kdb 資料庫，以便用戶端可以連接至不同的伺服器。 不同的憑證必須具有不同的標籤。 為標籤使用有意義的名稱。

重要： 對於伺服器的災難回復，如果失去憑證，則伺服器會自動產生新的憑證。 然後，每一個用戶端都必須匯入新的憑證。

5. 將伺服器憑證新增至 dsmcert.kdb 資料庫之後，將 ssl yes 選項新增至 C:\Windows\SysWOW64\fb.opt 檔，然後更新 tcpport 選項的值。

   重要：

   通常，會在不同埠上設定伺服器的 SSL 及 TLS 連線，而不是非 SSL 及 TLS 連線。 請不要為 tcpport 值指定非 SSL 或 TLS 埠號。如果 tcpport 的值不正確，回復代理程式無法連接至伺服器。

   您無法將非 SSL 或 TLS 埠連接至已啟用 SSL 或 TLS 的回復代理程式，或者將 SSL 或 TLS 埠連接至未啟用 SSL 或 TLS 的回復代理程式。

6. 在下列回復代理程式配置檔中，設定正確的 SSL 或 TLS 埠：
   - C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf
   - C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgentDMNodes.conf

透過使用協力廠商憑證啟用安全通訊

如果 IBM Spectrum Protect 伺服器使用協力廠商憑證管理中心 (CA)，您必須取得 CA 主要憑證。

關於這項作業

如果憑證是由 CA（例如 Symantec 或 Thawte）發出，則用戶端已備妥用於 SSL 或 TLS，並且您可以跳過下列配置步驟。 如需預先安裝的 CA 主要憑證清單，請在 IBM Knowledge Center 上搜尋**憑證管理中心主要憑證**。

如果憑證不是由預先安裝的主要憑證發出，或者是公司內部維護的內部 CA 憑證，則必須配置 Recovery Agent，以利用 SSL 或 TLS 通訊協定與伺服器進行通訊。

程序

若要透過使用 CA 憑證，啟用從回復代理程式到伺服器的 SSL 或 TLS 通訊：

1. 將 GSKit 二進位路徑及二進位路徑附加至 PATH 環境變數。 例如：

   ```
   set PATH=C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\bin\;
       C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\lib64;%PATH%
   ```

2. 如果您是第一次在用戶端上配置 SSL 或 TLS，則必須建立用戶端本端金鑰資料庫 dsmcert.kdb。 對於用戶端，從 C:\Windows\SysWOW64 目錄，執行 **gsk8capicmd_64** 指令，如下列範例中所示：

   ```
   gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -pw password -stash
   ```

   您提供的密碼用來加密金鑰資料庫。 密碼自動加密儲存在隱藏檔 (dsmcert.sth) 中。用戶端使用隱藏檔來擷取金鑰資料庫密碼。

3. 取得 CA 憑證。

4. 將憑證匯入至 dsmcert.kdb 資料庫。 您必須將每一個用戶端的憑證匯入至 dsmcert.kdb。 對於用戶端，從 C:\Windows\SysWOW64 目錄，執行 **gsk8capicmd_64** 指令，如下列範例中所示：

   ```
   gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "XYZ Certificate Authority"
   -file path_to_CA_root_certificate -format ascii -trust enable
   ```

   可以將多個伺服器憑證新增至 dsmcert.kdb 資料庫，以便用戶端可以連接至不同的伺服器。 不同的憑證必須具有不同的標籤。 為標籤使用有意義的名稱。

   重要： 對於伺服器的災難回復，如果失去憑證，則伺服器會自動產生新的憑證。 每一個用戶端都必須匯入新的憑證。

5. 將伺服器憑證新增至 dsmcert.kdb 資料庫之後，將 ssl yes 選項新增至 C:\Windows\SysWOW64\fb.opt 檔，然後更新 tcpport 選項的值。

   重要：

   通常，會在不同埠上設定伺服器的 SSL 及 TLS 連線，而不是非 SSL 及 TLS 連線。 請不要為 tcpport 值指定非 SSL 或 TLS 埠號。如果 tcpport 的值不正確，回復代理程式無法連接至伺服器。

   您無法將非 SSL 或 TLS 埠連接至已啟用 SSL 或 TLS 的回復代理程式，或者將 SSL 或 TLS 埠連接至未啟用 SSL 或 TLS 的回復代理程式。

6. 在下列回復代理程式配置檔中，設定正確的 SSL 或 TLS 埠：
   - C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf
   - C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgentDMNodes.conf

語言環境設定

語言環境設定識別用於介面、訊息及線上說明的語言。

Data Protection for VMware GUI

『Data Protection for VMware GUI』 一詞適用於下列 GUI：

- 在 Web 瀏覽器中存取的 Data Protection for VMware vSphere GUI
- vSphere Web Client GUI 中的 IBM Spectrum Protect vSphere Client 外掛程式

The Data Protection for VMware GUI 不支援在執行 Data Protection for VMware GUI、VMware vSphere Client 及 IBM Spectrum Protect 伺服器的處理器之間，包含不一致語言環境設定的環境中執行。

在執行 Data Protection for VMware GUI、VMware vSphere Client 及 IBM Spectrum Protect 伺服器的系統之間指定相同的語言環境設定。

當第一次透過「進一步瞭解」鏈結存取 Data Protection for VMware GUI 說明頁面時，該說明會以執行 Data Protection for VMware GUI 之系統的語言環境設定所指定的語言顯示。 第一次存取該語言時，該說明不會以 VMware vSphere Client 的語言環境所指定的語言顯示。 在此狀況下，Data Protection for VMware GUI 說明頁面顯示之後，至少按一下該說明中的兩個鏈結，然後關閉該說明。 下次從「進一步瞭

解」鏈結啟動該說明時，它會以 VMware vSphere Client 的語言環境設定所指定的語言顯示。

IBM Spectrum Protect 檔還原介面

介面內容及訊息提示語言取決於存取 IBM Spectrum Protect 檔案還原介面之 Web 瀏覽器的語言設定。

對於記載到 `fr_api.log` 檔的錯誤訊息，IBM Spectrum Protect 檔案還原介面使用執行 Data Protection for VMware vSphere GUI 之系統的語言環境設定所指定的語言。

日誌檔活動

Data Protection for VMware 會在安裝、備份、裝載及還原作業期間建立和修改數個日誌檔。

Data Protection for VMware 日誌檔是使用 `.sf` 副檔名的純文字檔案。

Windows 日誌放置於下列目錄中：

```
%ALLUSERSPROFILE%\Tivoli\TSM\TDPVMware
```

這些目錄包含每一個 Data Protection for VMware 元件的子目錄。 例如，Recovery Agent 子目錄是 `\mount`，Recovery Agent 指令行介面子目錄是 `\shell`。
您可以從 **Windows** > **開始**功能表中，透過選取**控制台** > **搜尋**並輸入 `*.log` 來搜尋日誌檔。

Linux 日誌放置於下列兩個路徑中：

```
<user.home>/tivoli/tsm/ve/mount/log
/opt/tivoli/tsm/TDPVMware/mount/engine/var
```

您可以透過輸入以下指令來搜尋日誌檔：

```
find /opt/tivoli/ -name "*.log"
```

重要：每次啟動安裝時都會改寫現有的日誌檔。 如果遇到安裝問題且必須重新安裝產品，請從 `%allusersprofile%` 目錄擷取現有的 `TDPVMwareInstallation.log` 檔案，然後再重新嘗試安裝。

註：當 Data Protection for VMware 服務在執行中時，數個日誌檔會保持開啟狀態。因此，部分檔案管理程式不會顯示這些檔案的現行狀態，並且可能將檔案大小報告為零。 選取或開啟其中一個檔案會強制檔案管理程式更新該檔案的詳細資料。

Recovery Agent 日誌檔

Recovery Agent 日誌檔是 `TDP_FOR_VMWARE_MOUNT`*`nnn`*`.sf`。 具有最新資料的日誌檔儲存在號碼為 *040* 的日誌檔 (`TDP_FOR_VMWARE_MOUNT040.sf`) 中。 當日誌檔到達大小上限時，會建立一個新的日誌檔。 除了日誌檔號碼會減 1 之外，日誌檔名稱相同。 具體來說，就是號碼為 *040* 的日誌檔資料，會複製到號碼為 *039* 的日誌檔中。 號碼為 *040* 的日誌檔包含最新的日誌檔資料。 當 *040* 再次到達檔案大小上限時，*039* 的檔案內容會移至 *038*，*040* 的資訊會再次移到 *039*。

Data Protection for VMware GUI 日誌檔

Data Protection for VMware vSphere GUI 將日誌檔放置在此目錄中：

Windows C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\logs

Linux /opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/logs

當您收集日誌檔時，請確保在壓縮檔中併入所有子目錄。

Data Protection for VMware 指令行介面 日誌檔

Data Protection for VMware 指令行介面 將日誌檔放置於下列目錄中：

Windows C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\logs

Linux /opt/tivoli/tsm/tdpvmware/common/logs

當您收集日誌檔時，請確保在壓縮檔中併入所有子目錄。

IBM Spectrum Protect 檔案還原介面日誌檔

IBM Spectrum Protect 檔案還原介面將錯誤訊息記載至 fr_api.log、fr_gui.log 及 messages.log 檔案。 這些檔案位於下列預設目錄中：

Windows C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\logs

Linux /opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/logs

您可以透過在檔案還原日誌活動檔 (FRLog.config) 中設定 API_LOG_FILE_NAME 和 API_LOG_FILE_LOCATION 選項來變更 fr_api.log 檔案的名稱和位置。

檔案還原作業也會由 IBM Spectrum Protect 伺服器記載。 您可以利用伺服器管理指令行用戶端來搜尋這些訊息。

- 若要在指令行模式中啟動管理用戶端階段作業，請在工作站中輸入下列指令：

  ```
  dsmadmc -id=admin -password=admin -dataonly=yes
  ```

  透過輸入帶有所顯示 **-ID** 和 **-PASSWORD** 選項的 **DSMADMC** 指令，系統不會提示您輸入使用者 ID 和密碼。

- 若要搜尋 SQL 摘要延伸表格以檢視檔案還原作業的結果，請從管理指令行用戶端發出 **select** 指令：

  ```
  select * from SUMMARY_EXTENDED where ACTIVITY_TYPE='File Restore'
  ```

  您可以透過在 select 陳述式中包括下列一個以上準則來縮小搜尋範圍：

  - * ENTITY='*DATA_MOVER_NODE_NAME*'
  - * AS_ENTITY='*DATA_CENTER_NODE_NAME*'
  - * SUB_ENTITY='*VM_HOST_NAME*'
  - * START_TIME='*yyyy-MM-dd HH:mm:ss*'

  例如：

  ```
  select * from SUMMARY_EXTENDED where ACTIVITY_TYPE='File Restore'
  and ENTITY='LOCAL_MP_WIN' and AS_ENTITY='DC_NODE' and SUB_ENTITY='testvm'
  and START_TIME>'2017-03-11 17:30:00'
  ```

  START_TIME 準則支援具有下列符號的查詢：等於號 (=)、小於號 (<) 或大於號 (>)。

- 若要搜尋 SQL 活動日誌表格以檢視檔案還原作業的事件，請從管理指令行用戶端發出 **select** 指令：

  ```
  select * from ACTLOG
  ```

  您可以透過在 select 陳述式中包括下列一個以上準則來縮小搜尋範圍：

  - `* NODENAME='DATA_CENTER_NODE_NAME'`
  - `* DATE_TIME='yyyy-MM-dd HH:mm:ss'`

  例如：

  ```
  select * from ACTLOG where NODENAME='DC_NODE' and DATE_TIME>'2017-03-11 17:30:00'
  ```

以大寫字元指定 *DATA_MOVER_NODE_NAME* 和 *DATA_CENTER_NODE_NAME*。

DATE_TIME 準則支援具有下列符號的查詢：等於號 (=)、小於號 (<) 或大於號 (>)。

啟動及執行 Data Protection for VMware 的服務

依預設，當您啟動 Windows 作業系統時，會以「本端系統帳戶」啟動 Recovery Agent。

在 Microsoft Windows 上執行 Recovery Agent 服務

當您從 Windows「開始」功能表啟動 Recovery Agent 時，服務即會自動停止。 從「開始」功能表啟動的 Recovery Agent 完成時，服務即會自動啟動。 此外，對於這些作業系統，服務並不提供 GUI。 若要使用 GUI，請跳至 Windows 的「開始」功能表，然後選取**所有程式** > **IBM Spectrum Protect** > **Data Protection for VMware** > **Recovery Agent**。

Data Protection for VMware 指令行介面

您可以完成下列作業，來驗證 Data Protection for VMware 指令行介面 是否執行中：

Windows 移至**開始** > **控制台** > **系統管理工具** > **服務**，並驗證 Data Protection for VMware 指令行介面 的狀態為已啟動。

Linux 移至 scripts 目錄 (/opt/tivoli/tsm/tdpvmware/common/scripts/)，並發出下列指令：

```
./vmclid status
```

- 如果常駐程式不在執行中，請發出下列指令來手動啟動常駐程式：

  ```
  /opt/tivoli/tsm/tdpvmware/common/scripts/vmcli --daemon
  ```

  下列起始 Script 也可用來停止和啟動常駐程式：

  ```
  ./vmclid stop
  ./vmclid start
  ```

附錄 A. 進階配置作業

您必須使用可用的應用程式介面來手動配置及驗證每一個元件。

開始之前

在進行這項作業之前，請確定下列狀況存在：

- IBM Spectrum Protect 伺服器必須可以登錄節點。
- Data Protection for VMware vSphere GUI 安裝在符合作業系統必要條件的系統上。它必須具有與下列系統的網路連線功能：
  - vStorage Backup Server
  - IBM Spectrum Protect 伺服器
  - vCenter Server

程序

1. 登入 IBM Spectrum Protect 伺服器，然後完成第 82 頁的『在 vSphere 環境中設定 IBM Spectrum Protect 節點』中說明的作業。
2. 登入 vStorage Backup Server，然後完成第 83 頁的『使用 vSphere 外掛程式 GUI 設定資料移轉裝置節點』中說明的作業。
3. 登入安裝 Data Protection for VMware vSphere GUI 的系統，然後完成第 88 頁的『在 vSphere 環境中配置 Data Protection for VMware 指令行介面』中說明的作業。
4. 在安裝 Data Protection for VMware vSphere GUI 的系統上，啟動 vSphere Client 並登入 vCenter。 如果 vSphere 用戶端已在執行中，您必須停止並重新啟動它。
5. 移至 vSphere 用戶端中的起始目錄。 按一下「解決方案和應用程式」畫面中的 Data Protection for VMware vSphere GUI 圖示。

   提示：如果未顯示此圖示，表示並未登錄 Data Protection for VMware vSphere GUI 或發生連線錯誤。

   a. 在「vSphere 用戶端」功能表中，移至**外掛程式** > **管理外掛程式**，以啟動「外掛程式管理程式」。

   b. 如果可以找出 Data Protection for VMware vSphere GUI，但是發生連線錯誤，請發出 `ping` 指令，驗證安裝 Data Protection for VMware vSphere GUI之機器的連線功能。

結果

Data Protection for VMware vSphere GUI 已經可以進行備份及還原作業了。

在 vSphere 環境中設定 IBM Spectrum Protect 節點

本程序說明如何將節點手動登錄至 IBM Spectrum Protect 伺服器，以及如何在 vSphere 環境中授與對於這些節點的 Proxy 權限。

開始之前

重要：

關於這項作業

此程序中的所有步驟都在 IBM Spectrum Protect 伺服器上完成。

提示：使用 Data Protection for VMware vSphere GUI 配置精靈或編輯配置記事本也可以完成此作業。 開啟 Web 瀏覽器，然後跳至 GUI Web 伺服器，以啟動 Data Protection for VMware vSphere GUI。 例如：

```
https://guihost.mycompany.com:9081/TsmVMwareUI/
```

使用 vCenter 使用者名稱及密碼登入。

- 若為起始配置，請跳至**配置** > **執行配置精靈**。
- 若為現有配置，請跳至**配置** > **編輯配置**。

程序

1. 登入「IBM Spectrum Protect」伺服器，然後在指令行模式中啟動管理用戶端階段作業：

   ```
   dsmadmc -id=admin -password=admin -dataonly=yes
   ```

2. 發出 REGister Node 指令，將下列節點登錄至 IBM Spectrum Protect 伺服器：

   a. 代表 VMware vCenter (vCenter 節點) 的節點：

      ```
      REGister Node MY_VCNODE <password for MY_VCNODE>
      ```

   b. 在 IBM Spectrum Protect 與 Data Protection for VMware vSphere GUI (VMCLI 節點) 之間通訊的節點：

      ```
      REGister Node MY_VMCLINODE <password for MY_VMCLINODE>
      ```

   c. 代表資料中心以及其中儲存虛擬機器資料 (資料中心節點) 的節點：

      ```
      REGister Node MY_DCNODE <password for MY_DCNODE>
      ```

   d. 從一個系統「移動資料」到另一個系統（資料移轉裝置節點）的節點：

      ```
      REGister Node MY_DMNODE <password for MY_DMNODE>
      ```

   警告： 將節點登錄至 IBM Spectrum Protect 伺服器時，請勿使用 userid 參數。

3. 發出 GRant PROXynode 指令，為這些節點定義 Proxy 關係：

   記住：目標節點擁有資料，而代理站節點則代表目標節點運作。 當授與 Proxy 權限給目標節點時，代理站節點可以為目標節點執行備份及還原作業。

   a. 發出下列指令，授與 Proxy 權限給 vCenter 節點：

      ```
      GRant PROXynode TArget=MY_VCNODE AGent=MY_DCNODE,MY_VMCLINODE
      ```

      這個指令會授與 MY_DCNODE 及 MY_VMCLINODE 代表 MY_VCNODE 備份及還原虛擬機器的權限。

   b. 發出下列指令，授與 Proxy 權限給 資料中心節點：

```
GRant PROXynode TArget=MY_DCNODE AGent=MY_VMCLINODE,MY_DMNODE
```

這個指令會授與 MY_VMCLINODE 及 MY_DMNODE 代表 MY_DCNODE 備份及還原虛擬機器的權限。

c. （選用項目）授與 Proxy 權限給環境中任何其他的資料中心節點或資料移轉裝置節點。

d. 發出 IBM Spectrum Protect 伺服器 Query PROXynode 指令以驗證 Proxy 關係。 以下顯示預期的指令輸出： 預期的指令輸出為：

```
Target Node         Agent Node
--------------    ------------------------------
MY_VCNODE           MY_DCNODE  MY_VMCLINODE
MY_DCNODE           MY_VMCLINODE  MY_DMNODE
```

下一步

在順利設定 IBM Spectrum Protect 節點之後，下一個手動配置作業是按照『使用 vSphere 外掛程式 GUI 設定資料移轉裝置節點』中的說明來設定資料移轉裝置節點。

使用 vSphere 外掛程式 GUI 設定資料移轉裝置節點

如果您在 vSphere 環境中將備份工作量卸載至 vStorage 備用伺服器，則可以使用「資料移轉裝置」精靈來設定資料移轉裝置來執行作業，並將資料移至 IBM Spectrum Protect 伺服器。

開始之前

設定資料移轉裝置節點需要配置變更、開始必要服務及驗證設定。

您可以使用外掛程式 GUI 執行這些作業，這會簡化及加速建立一系列資料移轉裝置節點。 或者，您可以手動執行工作，如需進一步資訊，請參閱第 84 頁的『在 vSphere 環境中手動設定資料移轉裝置節點』。

在標準 Data Protection for VMware 環境中，將個別 dsm.opt 檔 (Windows) 或 dsm.sys 檔段落 (Linux) 用於每一個 資料移轉裝置節點。 將「vStorage 備用伺服器」上的多個資料移轉裝置節點用於刪除重複資料，且這些節點有權移動相同資料中心節點的資料時，每一個 dsm.opt 檔或 dsm.sys 檔段落都必須包括 dedupcachepath 選項的不同值。

實體資料移轉裝置節點通常使用 SAN 來備份及還原資料。 如果您配置資料移轉裝置節點來直接存取儲存磁區，請關閉自動指派磁碟機代號。 如果不關閉字母指派，資料移轉裝置節點上的用戶端可能會毀損虛擬磁碟的「原始資料對映 (RDM)」。 如果虛擬磁碟的 RDM 毀損，備份將會失敗。

限制：Data Protection for VMware 不支援排程 vStorage Backup Server（用來作為資料移轉裝置）來備份它本身。 請確定已從 vStorage Backup Server 的排程排除其本身。 請使用不同的 vStorage Backup Server 來執行包含 vStorage Backup Server 之虛擬機器的備份。

如果您需要執行上述任何調整，請檢閱主題「在 vSphere 環境中手動設定資料移轉裝置節點」。

關於這項作業

使用 vSphere 外掛程式以配置資料移轉裝置節點。

程序

1. 從 vSphere 外掛程式中，選取 IBM Spectrum Protect。
2. 在**配置**標籤中，選取**資料移轉裝置**。
3. 在**新增資料移轉裝置**畫面中，從下拉功能表中選取資料中心。
4. 根據需要，編輯下列欄位：
   - **資料移轉裝置名稱**：節點名稱，已根據節點字首、資料中心節點名稱、資料移轉裝置名稱及增量數目填入建議的名稱。
   - **資料移轉裝置主機名稱**
   - **vCenter 使用者**，已填入登錄外掛程式的使用者名稱。
   - **vCenter 密碼**

   設定完成後，按一下**新增**。
5. **結果**畫面會顯示：
   - 所配置資料移轉裝置的名稱。
   - 選項檔案的位置。 您可以透過編輯此檔案配置資料移轉裝置。
   - 日誌檔的位置。
   - 所使用的預設選項。
6. 現在，您可以使用 **IBM Spectrum Protect > 配置資料移轉裝置**標籤測試資料移轉裝置。 您也可以透過選取資料移轉裝置，並按一下**驗證**，或者透過在下一次新增資料移轉裝置時檢查狀態，來驗證安裝。
7. 您可以使用 **IBM Spectrum Protect > 排程**標籤，將資料移轉裝置新增至排程。

在 vSphere 環境中手動設定資料移轉裝置節點

如果您在 vSphere 環境中將備份工作量卸載至 vStorage 備用伺服器，則可以手動設定資料移轉裝置節點來執行作業，並將資料移至 IBM Spectrum Protect 伺服器。

開始之前

實體資料移轉裝置節點通常使用 SAN 來備份及還原資料。 如果您配置資料移轉裝置節點來直接存取儲存磁區，請關閉自動指派磁碟機代號。 如果不關閉字母指派，資料移轉裝置節點上的用戶端可能會毀損虛擬磁碟的「原始資料對映 (RDM)」。 如果虛擬磁碟的 RDM 毀損，備份將會失敗。

所需要的服務：資料移轉裝置需要用戶端接收器服務、遠端用戶端代理程式服務及資料移轉裝置排程器服務，如下列步驟中所述。 如果您從資料中心移除資料移轉裝置，請解除安裝並刪除資料移轉裝置的這些服務。

重要：如果資料移轉裝置與 Data Protection for VMware vSphere GUI 安裝在同一 Windows 系統上，並且在資料移轉裝置配置期間選取**建立服務**，則不需要下列步驟。

在標準 Data Protection for VMware 環境中，將個別 `dsm.opt` 檔 (Windows) 或 `dsm.sys` 檔段落 (Linux) 用於每一個 資料移轉裝置節點。將「vStorage 備用伺服器」

上的多個資料移轉裝置節點用於刪除重複資料，且這些節點有權移動相同資料中心節點的資料時，每一個 dsm.opt 檔或 dsm.sys 檔段落都必須包括 dedupcachepath 選項的不同值。 為取得最佳結果，請針對每一個 dsm.opt 檔或 dsm.sys 檔段落指定不同的 schedlogname 及 errorlogname 選項。 步驟 2 中提供最小的一組必要選項。

實體資料移轉裝置節點通常使用 SAN 來備份及還原資料。 如果您配置資料移轉裝置節點來直接存取儲存磁區，請關閉自動指派磁碟機代號。 如果不關閉字母指派，資料移轉裝置節點上的用戶端可能會毀損虛擬磁碟的「原始資料對映 (RDM)」。 如果虛擬磁碟的 RDM 毀損，備份將會失敗。

限制：Data Protection for VMware 不支援排程 vStorage Backup Server（用來作為資料移轉裝置）來備份它本身。 請確定已從 vStorage Backup Server 的排程排除其本身。 請使用不同的 vStorage Backup Server 來執行包含 vStorage Backup Server 之虛擬機器的備份。

關於這項作業

提示：此程序中的所有步驟都在「vStorage 備用伺服器」上完成。

程序

1. Linux 確保 Java 軟體安裝在目標機器上。
2. Linux 設定相關環境變數。
   a. 確保正確地匯出 JAVA_HOME 環境變數：

      ```
      export JAVA_HOME=<jre-or-jdk-install-dir>
      ```

   b. 確保正確地匯出 PATH 環境變數：

      ```
      export PATH=$PATH:$JAVA_HOME/jre/bin
      ```

   c. 確保正確地匯出 LD_LIBRARY_PATH 環境變數。檢查並將它設為用戶端安裝目錄及 Java 共用程式庫 libjvm.so：

      對於 IBM Java：

      ```
      export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin:$JAVA_HOME/jre/bin/classic
      ```

      對於 Oracle Java：

      ```
      export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin:$JAVA_HOME/jre/lib/amd64/server
      ```

3. 在下列位置中建立 dsm.opt 或 dsm.sys 選項檔案：
   - **Windows：**C:\Program Files\Tivoli\TSM\baclient
   - **Linux：**/opt/tivoli/tsm/client/ba/bin
4. 將選項從資料移轉裝置的範例選項檔案複製到 dsm.opt 或 dsm.sys 檔案。 若要尋找資料移轉裝置的範例檔案：
   - 開啟 Web 瀏覽器並輸入 GUI Web 伺服器位址。 例如：

     ```
     https://guihost.mycompany.com:9081/TsmVMwareUI/
     ```

   - 以 vCenter 使用者名稱及密碼登入，並確保已選取**配置模式**。
   - 在配置精靈中，跳至「資料移轉裝置節點」頁面。
   - 找到您想要的資料移轉裝置，然後按一下**檢視**。
   - 將範例選項從 **Windows** 或 **Linux** 標籤複製到選項檔案。

   如果您的環境需要，您可以更新這些選項。

如需選項的說明，請參閱選項參照。

若為即時存取、即時還原或裝載（檔案還原）作業，請確保將 VMISCSISERVERADDRESS 新增至資料移轉裝置選項檔案。 指定在即時作業期間，vStorage Backup Server 上用於 iSCSI 資料傳送之網路卡的 iSCSI 伺服器 IP 位址。 連結至 ESX 主機上的 iSCSI 裝置的實體網路介面卡 (NIC) 所在的子網路，必須與 vStorage Backup Server 上用於 iSCSI 傳送的 NIC 所在的子網路相同。

5. 發出此指令以設定資料移轉裝置節點的 VMware vCenter 使用者及密碼：

   ```
   dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator> <password1>
   ```

6. 完成下列作業來設定用戶端接收器服務及資料移轉裝置排程器服務：

   - Windows 這個程序使用 IBM Spectrum Protect 用戶端 GUI 配置精靈來設定用戶端接收器服務及排程器服務。 依預設，遠端用戶端代理程式服務也可以透過精靈來設定。 如果針對這項作業使用 IBM Spectrum Protect 用戶端服務配置公用程式 (**dsmcutil**)，請確保還安裝遠端用戶端代理程式服務。

     移至**公用程式** > **設定精靈**，以從檔案功能表啟動 IBM Spectrum Protect「用戶端配置」精靈：

     – 選取**協助我配置 TSM Web 用戶端**。 依提示輸入資訊。

       a. 在您要服務何時啟動？選項中，選取**在 Windows 啟動時自動啟動**。

       b. 在您要在完成此精靈時啟動服務嗎？選項中，選取**是**。

       當作業順利完成時，請回到精靈歡迎使用頁面，並繼續進行步驟 b。

       提示：當您在同一台機器上配置多個資料移轉裝置節點時，必須指定不同的埠值給每一個用戶端接收器實例。

     – 選取幫助我配置 TSM 用戶端排程器。 依提示輸入資訊。

       a. 當輸入排程器名稱時，請確定選取**使用用戶端接收器常駐程式 (CAD) 管理排程器**選項。

       b. 在您要服務何時啟動？選項中，選取**在 Windows 啟動時自動啟動**。

       c. 在您要在完成此精靈時啟動服務嗎？選項中，選取**是**。

   - Linux **對於 Linux 上的資料移轉裝置，完成下列步驟：**

     a. 安裝程式會在 /etc/init.d 中為用戶端接收器 (dsmcad) 建立啟動 Script。在 /etc/init.d/dsmcad file 中檢查或設定相關環境變數。

     b. 請在 dsm.sys 檔的 資料移轉裝置節點 段落中指定下列選項：

        – 指定 managedservices 選項和以下兩個參數：

          ```
          managedservices schedule webclient
          ```

          這個設定會指示用戶端接收器同時管理 Web 用戶端和排程器。

        – （選用）如果您要將排程和錯誤資訊導向預設檔案以外的日誌檔，請指定 schedlogname 和 errorlogname 選項，以及用來儲存日誌資訊的完整路徑和檔名。 例如：

          ```
          schedlogname /vmsched/dsmsched_dm.log
          errorlogname /vmsched/dsmerror_dm.log
          ```

     c. 啟動用戶端接收器服務：

用戶端接收器必須先啟動，才能管理排程器作業或是管理 Web 用戶端。 以 root 使用者身分完成下列步驟：

1) 配置用戶端接收器服務及資料移轉裝置排程器服務來用作「vStorage 備用伺服器」。
2) 發出下列指令來啟動用戶端接收器：

   ```
   service dsmcad start
   ```

   若要讓用戶端接收器在系統重新啟動之後自動啟動，請在 Shell 提示時，如下所示新增服務：

   ```
   # chkconfig --add dsmcad
   ```

   提示：如果您想要直接從 Linux 指令行執行 **dsmc** 指令，則還必須將步驟 2 中提及的相當環境變數套用至指令 Shell。

7. 使用 -asnodename 及 -optfile 指令行參數，啟動資料移轉裝置指令行階段作業：

   ```
   dsmc -asnodename=VC1_DC1 -optfile=dsm_DM1.opt
   ```

   請確定起始登入之後，不會提示您輸入密碼。

   警告： 若要預防 IBM Spectrum Protect 排程器失敗，請確定 dsm.opt 檔案 (Windows) 或 dsm.sys 檔案段落 (Linux) 中未設定 asnodename 選項。 排程器會查詢 IBM Spectrum Protect 伺服器有關與 nodename（資料移轉裝置節點）相關聯的排程，而不是與 asnodename（資料中心節點）相關聯的排程。 如果 dsm.opt 或 dsm.sys 中已設定 asnodename，則需要與 asnodename（而不是 nodename）相關聯的排程。 因此，排定的作業失敗。

   請完成下列作業：

   a. 發出下列指令，驗證與 IBM Spectrum Protect 伺服器的連線：

      ```
      dsmc query session
      ```

      這個指令會顯示階段作業的相關資訊，包括現行節點名稱、建立階段作業的時間、伺服器資訊以及伺服器連線資訊。

   b. 請發出下列指令，來確認您可以備份虛擬機器：

      ```
      dsmc backup vm vm1
      ```

      在步驟 5b 及 5d 中，vm1 是 VM 的名稱。

   c. 發出下列指令，驗證備份是否順利完成：

      ```
      dsmc query vm "*"
      ```

   d. 發出下列指令來確認可以還原虛擬機器：

      ```
      dsmc restore vm vm1 -vmname=vm1-restore
      ```

8. 驗證用戶端接收器及代理程式的設定是否正確：

   a. 在 Web 瀏覽器中，輸入 IBM Spectrum Protect vSphere Client 外掛程式 位址。 例如：

      ```
      https://guihost.mycompany.com/vsphere-client/
      ```

   b. 以 vCenter 使用者名稱及密碼登入。

   c. 在 vSphere Web 用戶端中，按一下 **IBM Spectrum Protect** > **配置** > **資料移轉裝置**。

d. 確保**已驗證**顯示在資料移轉裝置的**狀態**直欄中。 如果顯示**失敗**，則將滑鼠移至狀態上方以檢視失敗訊息。

提示：如果安裝 Data Protection for VMware vSphere GUI的系統 IP 位址變更，您必須完成下列動作：

a. 重新設定用戶端接收器，Data Protection for VMware vSphere GUI 才能進行作業。否則，「外掛程式管理程式」會將 Data Protection for VMware vSphere GUI 狀態顯示為「已停用」。

在 vSphere 環境中配置 Data Protection for VMware 指令行介面

在安裝 Data Protection for VMware vSphere GUI 的系統上更新 Data Protection for VMware 指令行介面 設定檔。

開始之前

此設定檔 (vmcliprofile) 位於安裝 Data Protection for VMware vSphere GUI 之系統的下列目錄中：

Linux `/opt/tivoli/tsm/tdpvmware/common/scripts`

Windows 64 位元：`C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\scripts`

關於這項作業

此程序中的所有步驟都在安裝 Data Protection for VMware vSphere GUI 的系統上完成。

提示：使用 Data Protection for VMware vSphere GUI 配置精靈或配置記事本也可以完成此作業。 請跳至 Data Protection for VMware vSphere GUI「配置」視窗，然後按一下**執行配置精靈**或**編輯配置**。

程序

1. 使用下列設定來更新設定檔：

   VE_TSMCLI_NODE_NAME
   指定將 Data Protection for VMware 指令行介面 連接至 IBM Spectrum Protect 伺服器和代理站節點的節點 (MY_VMCLINODE)。

   限制：與 IBM Spectrum Protect 伺服器通訊時，VMCLI 節點不支援 SSL 通訊協定或 LDAP 鑑別。

   VE_VCENTER_NODE_NAME
   指定代表 vCenter 的虛擬節點 (MY_VCNODE)。

   VE_DATACENTER_NAME
   指定對映至資料中心的虛擬節點。 以下顯示正確語法：
   `datacenter_name::datacenter_node_name`
   - `datacenter_name` 值有區分大小寫。
   - 請務必針對環境中的每一個資料中心設定此參數 (MY_DCNODE)。

- Data Protection for VMware vSphere GUI 不支援 vCenter 中同名的資料中心。

VE_TSM_SERVER_NAME

指定 IBM Spectrum Protect 伺服器的主機名稱或 IP。

VE_TSM_SERVER_PORT

指定要用於 IBM Spectrum Protect 伺服器的埠名稱。預設值為 1500。

以下提供具有這些設定的設定檔範例：

```
VE_TSMCLI_NODE_NAME    MY_VMCLINODE
VE_VCENTER_NODE_NAME   MY_VCNODE
VE_DATACENTER_NAME     MyDatacenter1::MY_DCNODE
VE_TSM_SERVER_NAME     tsmserver.mycompany.xyz.com
VE_TSM_SERVER_PORT     1500
```

2. 在 pwd.txt 檔中設定 VMCLI 節點 密碼。
此密碼是用於將 Data Protection for VMware 指令行介面 連接至 IBM Spectrum Protect 伺服器和 資料移轉裝置節點 的節點。它是以 VE_TSMCLI_NODE_NAME 設定檔參數指定。
   a. 發出 echo 指令來建立包含密碼的文字檔：

      Linux `echo password1 > pwd.txt`

      Windows `echo password1> pwd.txt`

      Windows 密碼 (password1) 與大於符號 (>) 之間不得有空格。

   b. 發出此 vmcli 指令來設定 VMCLI 節點的密碼：
      `vmcli -f set_password -I pwd.txt`

      重要：

      - Linux 您必須以 tdpvmware 使用者身分發出 vmcli -f set_password 指令，而不是 root 使用者身分。
      - Linux Windows 如果您打算產生應用程式保護報告，則必須指定 **-type VMGuest** 參數來確認密碼套用至虛擬機器。 例如：

        ```
        vmcli -f set_password -type VMGuest -I password.txt
        ```

3. 驗證 Data Protection for VMware 指令行介面 是否執行中：

   Windows 按一下**開始** > **控制台** > **系統管理工具** > **服務**，並驗證 Data Protection for VMware 指令行介面的狀態為已啟動。

   Linux 移至 scripts 目錄 (/opt/tivoli/tsm/tdpvmware/common/scripts/)，並發出下列指令：

   ```
   ./vmclid status
   ```

   - 如果常駐程式執行中，請繼續進行「步驟 4」。
   - 如果常駐程式不在執行中，請發出下列指令來手動啟動常駐程式：

     ```
     /opt/tivoli/tsm/tdpvmware/common/scripts/vmcli --daemon
     ```

     下列起始 Script 也可用來停止和啟動常駐程式：

```
./vmclid stop
./vmclid start
```

4. 發出下列 vmcli 指令，以驗證 Data Protection for VMware 指令行介面 是否可以辨識 IBM Spectrum Protect 節點配置：

   ```
   vmcli -f inquire_config -t TSM
   ```

5. 驗證節點以確認未發生任何配置錯誤：
   a. 按一下 vSphere Client 的「解決方案及應用程式」視窗中的圖示，啟動 Data Protection for VMware vSphere GUI。
   b. 移至「配置」視窗。
   c. 選取表格中的節點，然後按一下**驗證選取的節點**。 「狀態詳細資料」窗格中即顯示狀態資訊。

下一步

Linux Windows 在順利完成本節中所說明的三個手動配置作業之後：

1. 第 82 頁的『在 vSphere 環境中設定 IBM Spectrum Protect 節點』
2. 第 83 頁的『使用 vSphere 外掛程式 GUI 設定資料移轉裝置節點』

不需要其他的配置作業即可備份虛擬機器資料。

vSphere 環境指令行介面配置核對清單

使用此程序，僅透過指令行介面在 vSphere 環境中配置 Data Protection for VMware。

程序

在 IBM Spectrum Protect 伺服器上完成步驟 1 和步驟 2。

1. 向 IBM Spectrum Protect 伺服器登錄下列節點：
   a. 表示 VMware vCenter 的節點（vCenter 節點）：

      ```
      REGister Node MY_VCNODE <password for MY_VCNODE>
      ```

   b. 在 IBM Spectrum Protect 和 Data Protection for VMware vSphere GUI 之間通訊的節點（VMCLI 節點）：

      ```
      REGister Node MY_VMCLINODE <password for MY_VMCLINODE>
      ```

   c. 表示資料中心且用來儲存 VM 資料的節點（資料中心節點）：

      ```
      REGister Node MY_DCNODE <password for MY_DCNODE>
      ```

   d. 從一個系統「移動資料」至另一個系統的節點（資料移轉裝置節點）：

      ```
      REGister Node MY_DMNODE <password for MY_DMNODE>
      ```

2. 定義這些節點的 Proxy 關係：
   a. 透過發出下列指令，將 Proxy 權限授予 vCenter 節點：

      ```
      GRant PROXynode TArget=MY_VCNODE AGent=MY_DCNODE,MY_VMCLINODE
      ```

      此指令會授與 MY_DCNODE 和 MY_VMCLINODE 代表 MY_VCNODE 備份及還原 VM 的權限。

   b. 透過發出下列指令，將 Proxy 權限授予 資料中心節點：

      ```
      GRant PROXynode TArget=MY_DCNODE AGent=MY_VMCLINODE,MY_DMNODE
      ```

此指令會授與 MY_VMCLINODE 和 MY_DMNODE 代表 MY_DCNODE 備份及還原 VM 的權限。

c. （選用項目）將 Proxy 權限授予環境中的任何其他資料中心節點或資料移轉裝置節點。

d. 透過發出 IBM Spectrum Protect 伺服器 Query PROXynode 指令來驗證 Proxy 關係。 下面顯示了預期的指令輸出：

```
Target Node         Agent Node
--------------    ------------------------------
MY_VCNODE              MY_DCNODE  MY_VMCLINODE
MY_DCNODE            MY_VMCLINODE  MY_DMNODE
```

在「vStorage 備用伺服器」上完成步驟 3 至 9。

3. 為下列資料移轉裝置選項設定適當的值：

   - Windows 請在 dsm.opt 選項檔案中指定這些選項。
   - Linux 請在 dsm.sys 檔的資料移轉裝置節點段落中指定這些選項。

```
NODENAME
PASSWORDACCESS
VMCHOST
VMBACKUPTYPE
MANAGEDSERVICES
TCPSERVERADDRESS
TCPPORT
COMMMETHOD
HTTPPORT
```

註：只有在使用了多個「用戶端接收器服務 (CAD)」時才需要 HTTPPORT。 例如，如果有兩個資料移轉裝置節點（以及兩個 CAD 服務），則每一個資料移轉裝置節點的選項檔案都必須指定不同的 HTTPPORT 值。
下面提供了使用這些選項的範例 dsm.dm.opt 檔：

```
NODename MY_DMNODE
PASSWORDAccess generate
VMCHost vcenter.storage.usca.example.com
VMBACKUPType FUllvm
MANAGEDServices schedule webclient
TCPServeraddress tsmserver.mycompany.xyz.com
TCPPort 1500
COMMMethod tcpip
HTTPPORT 1583
```

4. 發出下列指令，驗證與 IBM Spectrum Protect 伺服器的連線：
   `dsmc query session`
5. 發出此指令以設定資料移轉裝置節點的 VMware vCenter 使用者及密碼：
   `dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator> <password1>`
6. 設定下列 IBM Spectrum Protect 服務：

   - Windows

     a. 安裝「排程器服務」：

     ```
     dsmcutil install scheduler /name:"TSM Central Scheduler Service"
     /node:MY_DMNODE   /password:MY_DMNODEPWD /startnow:no /autostart:no
     ```

     b. 安裝 CAD：

```
dsmcutil install cad /name:"TSM CAD - MY_DMNODE" /node:MY_DMNODE
/password:MY_DMNODEPWD /optfile:c:\tsm\baclient\dsm.dm.opt
/cadschedname:"TSM Central Scheduler Service" /startnow:no
/autostart:yes
```

c. 安裝「遠端用戶端代理程式服務」：

```
dsmcutil install remoteagent /name:"TSM AGENT" /node:MY_DMNODE
/password:MY_DMNODEPWD /optfile:c:\tsm\baclient\dsm.dm.opt
/partnername:"TSM CAD - MY_DMNODE" /startnow:no
```

- Linux 在 dsm.sys 檔的資料移轉裝置節點段落中指定 managedservices 選項：

  確保指定 schedule 和 webclient 參數：

  ```
  managedservices schedule webclient
  ```

  這個設定會指示用戶端接收器同時管理 Web 用戶端和排程器。

7. Linux 如果要配置「用戶端接收器服務」與「資料移轉裝置排程器服務」來用作「vStorage 備用伺服器」，請在 /etc/init.d/dsmcad 檔中設定下列環境變數：

   ```
   export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
   ```

8. Linux 啟動「用戶端接收器服務」： 安裝程式會在 /etc/init.d 中為用戶端接收器常駐程式 (dsmcad) 建立啟動 Script。用戶端接收器常駐程式必須啟動，然後才能管理排程器作業或者管理 Web 用戶端。 啟動時，使用下列指令來啟動常駐程式：

   ```
   service dsmcad start
   ```

   如果要讓「用戶端接收器常駐程式」在系統重新啟動之後自動啟動，請在 Shell 提示時，如下所示新增服務：

   ```
   # chkconfig --add dsmcad
   ```

9. 確認已正確地設定 IBM Spectrum Protect 服務：
   a. 登入遠端系統。
   b. 利用下列位址和埠，使用 Web 瀏覽器來連接 HOST1 系統：
      http://HOST1.xyz.yourcompany.com:1581

在安裝了 Data Protection for VMware vSphere GUI 的系統上完成步驟 10。

10. 在 Data Protection for VMware 指令行介面設定檔 (vmcliprofile) 中給下列選項設定適當的值：

    ```
    VE_TSMCLI_NODE_NAME
    VE_VCENTER_NODE_NAME
    VE_DATACENTER_NAME
    VE_TSM_SERVER_NAME
    VE_TSM_SERVER_PORT
    ```

    下面提供了使用這些選項的範例設定檔：

    ```
    VE_TSMCLI_NODE_NAME    MY_VMCLINODE
    VE_VCENTER_NODE_NAME   MY_VCNODE
    VE_DATACENTER_NAME     MyDatacenter1::MY_DCNODE
    VE_TSM_SERVER_NAME     tsmserver.mycompany.xyz.com
    VE_TSM_SERVER_PORT     1500
    ```

    設定檔位於下列目錄中：

Linux /opt/tivoli/tsm/tdpvmware/common/scripts

Windows 64 位元：C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\scripts

a. 設定 VMCLI 節點的密碼：

1) 發出 echo 指令以建立包含密碼的文字檔：

Linux

```
echo password1 > pwd.txt
```

Windows

```
echo password1> pwd.txt
```

2) 發出此 vmcli 指令以設定 VMCLI 節點的密碼：

重要： Linux 必須以 tdpvmware 使用者身分（而不是 root 使用者身分）發出此指令。

```
vmcli -f set_password -I pwd.txt
```

b. 確認 Data Protection for VMware 指令行介面在執行中：

Windows 從 Windows 命令提示字元發出此指令：

```
net start
```

Linux 發出下列指令：

```
./vmclid status
```

c. 發出下列 vmcli 指令，以驗證 Data Protection for VMware 指令行介面 是否可以辨識 IBM Spectrum Protect 節點配置：

```
vmcli -f inquire_config -t TSM
```

磁帶配置準則

在嘗試磁帶儲存體的備份作業之前，請先檢閱這些準則。

準備備份至磁帶

Linux Windows 在嘗試備份至磁帶之前，必須先在 IBM Spectrum Protect 伺服器上針對磁帶備份設定下列參數：

1. 定義管理類別：

```
define mgmtclass <網域名稱> <原則集名稱> <管理類別名稱>
```

例如：

```
define mgmtclass tape tape DISK
```

2. 定義副本群組：

```
define copygroup <網域名稱> <原則集名稱> <管理類別名稱>
destination=<儲存區名稱>
```

例如：

```
define copygroup tape tape DISK destination=Diskpool
```

3. 啟動原則集：

   ```
   activate policyset <網域名稱> <原則集名稱>
   ```

   例如：

   ```
   activate policyset tape tape
   ```

配置實體磁帶的備份時，有一些額外配置需求。 您必須一律在磁碟上保存 IBM Spectrum Protect meta 資料（控制檔），在磁帶上保存實際 VM 備份資料。

- 使用 VMMC 選項來儲存使用非預設管理類別之管理類別的 VMware 備份（和 VMware 控制檔）。
- 使用 VMCTLMC 選項來指定 VMware 備份期間，專門用於 VMware 控制檔的管理類別。您指定的管理類別會置換預設管理類別。 它也會置換 VMMC 選項指定的管理類別。 VMCTLMC 管理類別必須指定磁碟儲存區，並且不會移轉至磁帶。
- VMMC 選項一律用於控制 VM 備份上的保留。 此選項同時適用於磁碟和磁帶配置。控制檔的保留不使用 VMCTLMC。 控制檔和資料檔屬於相同群組，它們會按照 VMMC 選項的保留原則一起過期。 當同時設定這兩個選項時， VMMC 用於資料檔，VMCTLMC 用於控制檔。

限制：使用不需 LAN 的配置中的儲存體代理程式之還原作業可以從副本儲存區還原檔案，即使可以從主要儲存區擷取資料。 在以下情況下，可能會發生此現象：還原要求適用於特定檔案，或還原要求未使用非查詢方法，以及檔案的主要副本儲存在無法透過不需要 LAN 的路徑存取的儲存區中。 這也可能會影響非還原狀況，如 Data Protection for VMware 備份作業。 在 Data Protection for VMware 環境中，VM 控制檔的偏好儲存方法是磁碟，以便在增量備份處理程序中還原檔案時不需要裝載。 這些 VM 控制檔不僅需要放在磁碟上，而且還不應備份至可透過不需 LAN 的路徑使用的副本儲存區。 如果是，在從 Data Protection for VMware 用戶端進行不需 LAN 的增量備份期間，將使用磁帶裝載來還原檔案。

如果 IBM Spectrum Protect 伺服器環境使用磁碟至磁帶的移轉，請在移轉之前考量下列準則：

- 將磁碟儲存區 MIGDELAY 的值設定成可從磁碟滿足大部分的裝載要求。 一般使用型樣指出，在數日內就會發生高百分比的個別檔案回復。 例如，通常是前次修改時間起算的 3 到 5 日內。 因此，請考慮在磁碟上進行這類短期保存，以將回復作業最佳化。

  此外，如果磁碟儲存區使用用戶端刪除重複資料，請設定能適應經常完整 VM 備份的 MIGDELAY 選項。 在已至少完成 VM 的兩個完整備份之前，請勿將資料從已刪除重複資料儲存區移轉至磁帶。 當資料移至磁帶，就不再是沒有重複的狀態。 比方說，如果完整備份是每週執行，請考慮將 MIGDELAY 設定為至少 10 天的值。 此設定可確保，每一個完整備份在移至磁帶之前，可識別及使用前次備份的重複資料。
- 請使用裝置類別檔儲存區，而不是磁碟裝置類別儲存區。 一般的磁區大小值（由裝置類別 MAXCAPACITY 參數指定）為 8 GB 至 16 GB。 如果是相關聯的儲存區，請考慮套用依檔案空間的並置。 每一個已經備份的 VM 都會在 IBM Spectrum Pro-

tect 伺服器中以個別檔案空間表示。依檔案空間並置可在相同磁區（磁碟檔案）中，為給定 VM 儲存其多個增量備份的資料。 發生移轉至磁帶時，依檔案空間並置會將給定 VM 的多個增量備份一起安置在實體磁帶上。

請使用**設定**對話框來設定「磁帶模式」值。

當裝載或即時還原作業所需的磁帶儲存體與備份作業正在同步使用的磁帶儲存體相同時，備份作業會遭到岔斷。

在 Linux 系統上手動配置 iSCSI 裝置

Linux

此程序會說明如何配置在 iSCSI 裝載作業期間使用的 Linux 系統。 VM Snapshot 是從 IBM Spectrum Protect 伺服器儲存體裝載的。

開始之前

在 iSCSI 裝載期間，會在 Recovery Agent 系統上建立 iSCSI 目標。 Recovery Agent 系統上不需要 Microsoft iSCSI 起始器。

提示：Linux 和 SUSE Linux Enterprise Server 隨附了 Open-iSCSI Initiator。

在繼續進行此作業之前，檢閱下列 iSCSI 需求：

- 您可以從任何系統連接至 iSCSI 目標，以建立包含備份資料的磁區。 您可以從另一個系統裝載此磁區。
- 必須連接至 iSCSI 目標的任何系統上都需要 iSCSI 起始器。
- 必須在要還原資料的系統上安裝 iSCSI 起始器。
- 如果磁區跨越數個磁碟，您必須裝載所有的所需磁碟。 當使用鏡映磁區時，請只裝載其中一個鏡映磁區。 裝載一個磁碟可防止耗時的同步化作業。

關於這項作業

請完成下列步驟，以配置在 iSCSI 裝載作業期間使用的 Linux 系統：

程序

1. 在要還原資料的系統上記錄 iSCSI 起始器名稱。 iSCSI 起始器名稱位於 `/etc/iscsi/initiatorname.iscsi` 檔案中。如果 `InitiatorName=` 值是空的，請使用下列指令建立起始器名稱：

   ```
   twauslbkpoc01:~ # /sbin/iscsi-iname
   ```

   以下是範例起始器名稱：

   ```
   iqn.2005-03.org.open-iscsi:3f5058b1d0a0
   ```

2. 將起始器名稱新增至 `/etc/iscsi/initiatorname.iscsi` 檔案。
   a. 使用 **vi** 指令編輯 `/etc/iscsi/initiatorname.iscsi` 檔案。 例如：

      ```
      twauslbkpoc01:~ # vi /etc/iscsi/initiatorname.iscsi
      ```

   b. 使用起始器名稱更新 **InitiatorName=** 參數。 例如：

      ```
      InitiatorName=iqn.2005-03.org.open-iscsi:3f5058b1d0a0
      ```

3. 在安裝 Recovery Agent（或 iSCSI 目標）的系統上完成下列步驟：

a. 啟動 Recovery Agent。完成「選取 IBM Spectrum Protect 伺服器」及「選取 Snapshot」對話框，然後按一下**裝載**。

b. 在選擇裝載目的地對話框，選取裝載 iSCSI 目標。

c. 建立目標名稱。 請確定它是唯一的，並且可以從執行 iSCSI 起始器的系統識別它。例如：

```
iscsi-mount-tsm4ve
```

d. 輸入在步驟 1 中所記錄的 iSCSI 起始器名稱，然後按一下**確定**。

e. 確認裝載的磁區欄位中顯示您剛裝載的磁區。

4. 找出並啟動在步驟 1 中所選取的起始器系統上的 iSCSI 起始器程式：

a. 發出下列指令來驗證 iSCSI 服務正在執行。
Red Hat Enterprise Linux：

```
service iscsi status
```

SUSE Linux Enterprise Server：

```
service open-iscsi status
```

如果服務未執行，請發出下列指令以啟動服務：
Red Hat Enterprise Linux：

```
service iscsi start
```

SUSE Linux Enterprise Server：

```
service open-iscsi start
```

b. 發出下列指令以連接至 iSCSI 目標：

```
iscsiadm -m discovery -t sendtargets -p <IP/hostname of
Recovery Agent system> --login
```

c. 發出下列指令以驗證新的原始裝置可用：

```
fdisk -l
```

5. 裝載檔案系統：
針對非 LVM 磁區，發出下列指令。 在此範例中，新裝置為 /dev/sdb1：

```
mkdir /mountdir
mount /dev/sdb1 /mountdir
```

對於 LVM 磁區，在 Linux 訪客上完成下列作業：

a. 確定 vgimportclone Script 在 Linux 系統上可用。 基本（預設）LVM 套件未隨附此 Script。 因此，您可能需要將 LVM 套件更新為提供此 Script 的層次。

b. 發出 **vgimportclone** 指令，並包括新的基本磁區群組名稱 (VolGroupSnap01)。例如：

```
vgimportclone --basevgname /dev/VolGroupSnap01 /dev/sdb1
```

c. 發出 **lvchange** 指令，將邏輯磁區標示為作用中。 例如：

```
lvchange -a y /dev/VolGroupSnap01/LogVol00
```

d. 發出下列指令，以裝載磁區：

```
mkdir /mountdir
mount -o ro /dev/VolGroupSnap01/LogVol00 /mountdir
```

6. 檔案還原作業完成之後，發出這些指令：

- 對於非 LVM 磁區，請發出下列指令：
  a. 卸載檔案系統：

     ```
     umount /dev/sdb1 /mountdir
     ```

  b. 移除磁區。 如果磁區隸屬於磁區群組，則首先透過發出下列指令，從磁區群組中移除磁區：

     ```
     vgreduce <your_volume_group> /dev/sdb1
     ```

     然後發出此指令，以移除磁區：

     ```
     pvremove /dev/sdb1
     ```

  c. 登出單一目標：

     ```
     iscsiadm --mode node --targetname <target_name> --logout
     ```

  d. 登出所有目標：

     ```
     iscsiadm --mode node --logout
     ```

- 對於 LVM 磁區，在 Linux 訪客上完成下列作業：
  a. 卸載檔案系統：

     ```
     unmount /mountdir
     ```

  b. 移除邏輯磁區：

     ```
     lvm lvremove LogVol00
     ```

  c. 移除磁區群組：

     ```
     lvm vgremove VolGroupSnap01
     ```

  d. 登出單一目標：

     ```
     iscsiadm --mode node --targetname <target_name> --logout
     ```

  e. 登出所有目標：

     ```
     iscsiadm --mode node --logout
     ```

在 Windows 系統上手動配置 iSCSI 裝置

Windows

此程序會說明如何配置在 iSCSI 裝載作業期間使用的 Windows 系統。 從 IBM Spectrum Protect 伺服器儲存體來裝載 Snapshot。

開始之前

在繼續進行此作業之前，檢閱下列 iSCSI 需求：

- 在 iSCSI 裝載期間，iSCSI 目標會在 Recovery Agent 系統上建立。您可以從任何系統連接至 iSCSI 目標，以建立包含備份資料的磁區。 然後，您也可以從另一個系統裝載此磁區。
- 必須連接至 iSCSI 目標的任何系統上都需要 iSCSI 起始器。
- 確定在要還原資料的系統上安裝 iSCSI 起始器。
- Recovery Agent 系統不需要「Microsoft iSCSI 起始器」。

在繼續進行此作業之前，檢閱下列磁碟及磁區需求。

- 如果磁區跨越數個磁碟，您必須裝載所有的所需磁碟。 當使用鏡映磁區時，請只裝載其中一個鏡映磁區。 裝載一個磁碟可防止耗時的同步化作業。

- 如果在備份系統上使用多個動態磁碟，這些磁碟會指派給相同的群組。 如此一來，Windows Disk Manager 可能會將部分磁碟視為遺失，並在您只裝載一個磁碟時發出錯誤訊息。 請忽略此訊息。 您仍然可以存取備份磁碟上的資料，除非部分資料是在其他磁碟上。 裝載所有的動態磁碟即可以解決這個問題。

關於這項作業

請完成下列作業，以配置在 iSCSI 裝載作業期間使用的 Windows 系統：

程序

1. 在 Recovery Agent 系統上，於 LAN 防火牆及 Windows 用戶端防火牆中開啟埠 3260。 在要還原資料的系統上記錄 iSCSI 起始器名稱。

   iSCSI 起始器名稱顯示在「控制台」的 iSCSI 起始器配置視窗中。 例如：

   ```
   iqn.1991-05.com.microsoft:hostname
   ```

2. 在安裝 Recovery Agent（或 iSCSI 目標）的系統上完成下列作業：
   a. 啟動 Recovery Agent GUI。完成「選取 IBM Spectrum Protect 伺服器」及「選取 Snapshot」對話框，然後按一下**裝載**。
   b. 在選擇裝載目的地對話框，選取**裝載 iSCSI 目標**。
   c. 建立目標名稱。 請確定它是唯一的，並且可以從執行 iSCSI 起始器的系統識別它。例如：

      ```
      iscsi-mount-tsm4ve
      ```

   d. 輸入在步驟 1 中所記錄的 iSCSI 起始器名稱，然後按一下**確定**。
   e. 確認裝載的磁區欄位中顯示您剛裝載的磁區。
   f. 如果在 iSCSI 網路中使用 Recovery Agent，而且此 Recovery Agent 未使用資料移轉裝置，請移至 `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf` 檔並指定 `[IMOUNT]` 標籤與 **`Target IP`** 參數：

      ```
      [IMOUNT config]
      Target IP=<IP address of the network card on the system
      that exposes the iSCSI targets.>
      ```

      例如：

      ```
      [General config]
      param1
      param2
      ...
      [IMount config]
      Target IP=9.11.153.39
      ```

      新增或變更 Target IP 參數後，請重新啟動 Recovery Agent GUI 或 Recovery Agent CLI。
3. 找出並啟動在步驟 1 中所選取的起始器系統上的 iSCSI 起始器程式：
   a. 連接至 iSCSI 目標：
      1) 在「目標」標籤中，輸入在步驟 2 的目標：對話框中所用的 Recovery Agent（iSCSI 目標）的 TCP/IP 位址。按一下**快速連接**。
      2) 快速連接對話框即顯示一個符合在步驟 2c 中所指定的目標名稱之目標。 如果尚未連接它，請選取此目標，然後按一下**連接**。

b. 在起始器系統上，跳至**控制台** > **系統管理工具** > **電腦管理** > **儲存體** > **磁碟管理**。

1) 如果裝載的 iSCSI 目標列為 Type=Foreign，請用滑鼠右鍵按一下**外部磁碟**，然後選取**匯入外部磁碟**。 即會選取「外部磁碟群組」。 按一下**確定**。

2) 下一個畫面即顯示「外部磁碟」的類型、狀況和大小。 按一下**確定**，等待匯入磁碟。

3) 當磁碟匯入完成時，按 **F5** 鍵（重新整理）。裝載的 iSCSI Snapshot 即顯示並包含指派的磁碟機代號。 如果未自動指派磁碟機代號，請用滑鼠右鍵按一下所需的分割區，然後選取**變更磁碟機代號或路徑**。 按一下**新增**，然後選取磁碟機代號。

4. 開啟「Windows 檔案總管」（或其他公用程式），並瀏覽已裝載的 Snapshot 以進行檔案還原作業。

5. 還原檔案之後，完成下列作業：

a. 透過使用「iSCSI 起始器內容」對話框，中斷每一個 iSCSI 目標的連線。

b. 選取 Recovery Agent GUI 中的磁區，然後按一下**卸載**，藉此從步驟 2 卸載磁區。

在 Linux 系統上手動配置裝載 Proxy 節點

Linux

完成此作業，以將裝載 Proxy 節點新增至遠端 Linux 系統。

開始之前

在標準 Data Protection for VMware vSphere GUI 環境中，將個別 `dsm.sys` 檔案段落用於每一個裝載 Proxy 節點。透過使用備用伺服器上安裝的資料移轉裝置，完成此程序中的所有步驟。

關於這項作業

這項作業透過更新資料移轉裝置選項，並驗證 IBM Spectrum Protect 伺服器的連線功能，來設定裝載 Proxy 節點。

程序

1. 請在 `dsm.sys` 檔的 裝載 Proxy 節點 段落中指定這些選項。

NODENAME
指定先前定義的 裝載 Proxy 節點 的名稱。 IBM Spectrum Protect 排程與此節點相關聯。

PASSWORDACCESS
指定 GENERATE 以便自動產生密碼（而非使用者提示）。

MANAGEDSERVICES
指定這個選項可指示用戶端接收器同時管理 Web 用戶端和排程器 (`schedule webclient`)。

TCPSERVERADDRESS
指定 IBM Spectrum Protect 伺服器的 TCP/IP 位址。

TCPPORT

指定 IBM Spectrum Protect 伺服器的 TCP/IP 埠位址。

COMMMETHOD

指定要由 IBM Spectrum Protect 伺服器使用的通訊方法。若為裝載 Proxy 節點，您必須指定 TCP/IP 作為通訊方法。 如果指定另一種方法，則作業會失敗。

HTTPPORT

此選項會指定 TCP/IP 埠位址，且僅當使用多個「用戶端接收器服務 (CAD)」時才必須指定。 例如，如果有兩個裝載 Proxy 節點（以及兩個 CAD 服務），則每一個裝載 Proxy 節點的選項檔都必須指定不同的 HTTPPORT 值。

限制：請勿在 dsm.sys 檔中啟用不需 LAN 的選項 (ENABLELANFREE YES)。 裝載 Proxy 節點不支援這個選項。

以下提供具有這些設定的 dsm.sys 檔範例：

```
Servername     tsm_server1
  NODename datacenter1_MP_LNX
  PASSWORDAccess generate
  MANAGEDServices schedule webclient
  TCPServeraddress tsmserver.myco.com
  TCPPort 1500
  COMMMethod tcpip
  HTTPPORT 1583
```

2. 發出此指令，以設定裝載 Proxy 節點的 VMware vCenter 使用者與密碼：
   `dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator> <password1>`
3. 使用 -asnodename 及 -optfile 指令行參數，啟動資料移轉裝置指令行階段作業：
   `dsmc -asnodename=vctr1_datacenter1 -optfile=dsm_MP_LNX.sys`
   請確定起始登入之後，不會提示您輸入密碼。

   警告： 若要防止 IBM Spectrum Protect 排程器失敗，請確定未在 dsm.sys 檔案段落 (Linux) 中設定 asnodename 選項。 排程器會查詢 IBM Spectrum Protect 伺服器有關與 nodename（裝載 Proxy 節點）相關聯的排程，而不是與 asnodename（資料中心節點節點）相關聯的排程。 如果在 dsm.sys 中設定 asnodename，則會查詢與 asnodename（而不是 nodename）相關聯的排程。 因此，排定的作業失敗。
4. 發出下列指令，驗證與 IBM Spectrum Protect 伺服器的連線：
   `dsmc query session`
   這個指令會顯示階段作業的相關資訊，包括現行節點名稱、建立階段作業的時間、伺服器資訊以及伺服器連線資訊。
5. 完成下列作業來設定用戶端接收器服務 (CAD) 及資料移轉裝置排程器服務：
   - 請在 dsm.sys 檔的 裝載 Proxy 節點 段落中指定這些選項：
     - 指定 managedservices 選項和以下兩個參數：

       ```
       managedservices schedule webclient
       ```

       這個設定會指示用戶端接收器同時管理 Web 用戶端和排程器。
     - 如果您要將排程及錯誤資訊引導至日誌檔（而非預設檔案），請指定 schedlogname 及 errorlogname 選項。每一個選項都必須包含要儲存日誌資訊的完整路徑與檔名。 例如：

```
schedlogname /vmsched/dsmsched_mp_lnx.log
errorlogname /vmsched/dsmerror_mp_lnx.log
```

- 若要配置「用戶端接收器服務」與「資料移轉裝置排程器服務」來用作備份伺服器，請在 /etc/init.d/dsmcad 檔中設定下列環境變數：

  ```
  export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
  ```

- 啟動「用戶端接收器服務」：

  安裝程式會在 /etc/init.d 中為用戶端接收器常駐程式 (dsmcad) 建立啟動 Script。 用戶端接收器常駐程式必須先啟動，才能管理排程器作業或是管理 Web 用戶端。啟動時，使用下列指令來啟動常駐程式：

  ```
  export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
  service dsmcad start
  ```

  若要讓「用戶端接收器常駐程式」在系統重新啟動之後自動啟動，請在 Shell 提示時，如下所示新增服務：

  ```
  # chkconfig --add dsmcad
  ```

6. 驗證用戶端接收器和代理程式的設定是否正確：
   a. 登入遠端系統。
   b. 利用下列位址和埠，使用 Web 瀏覽器來連接 HOST1 系統：

      ```
      http://HOST1.xyz.yourcompany.com:1581
      ```

在 Windows 系統上手動配置裝載 Proxy 節點

Windows

完成此作業，以將裝載 Proxy 節點新增至遠端 Windows 系統。 當您要將第二個 Windows 裝載 Proxy 節點新增至環境時，需要此作業。

開始之前

在進行此作業之前，請確定已配置主要 Windows 裝載 Proxy 節點。

關於這項作業

請在遠端 Windows 裝載 Proxy 系統上完成下列步驟：

程序

1. 在遠端 Windows 裝載 Proxy 系統上安裝下列產品：
   - Recovery Agent
   - IBM Spectrum Protect 資料移轉裝置

   在 IBM Spectrum Protect for Virtual Environments 下載映像檔上存取兩個產品。逐步安裝指示位於「IBM 知識中心」中，網址為
   第 21 頁的『在 Windows 系統上安裝 Data Protection for VMware 元件』
2. 從所建立的 Windows 裝載 Proxy 節點中擷取範例選項檔案內容，並將它新增至遠端 Windows 裝載 Proxy 系統上的選項檔：
   a. 在主要 Windows 裝載 Proxy 系統上，跳至 Data Protection for VMware vSphere GUI 中的「配置」視窗。

b. 按一下「作業」清單中的**編輯 TSM 配置**。 載入配置記事本可能需要一些時間。

c. 跳至「裝載 Proxy 節點配對」頁面。

d. 在表格的「主要節點」直欄中，跳至具有擱置位置的 Windows 裝載 Proxy 節點，然後按一下**檢視設定**。

e. 複製在**裝載 Proxy 設定**對話框中顯示的範例 dsm.opt 檔案內容。

f. 將範例 dsm.opt 檔案內容貼上（或新增）至遠端 Windows 裝載 Proxy 系統上的選項檔。 使用將選項檔案角色識別為遠端裝載 Proxy 節點的慣例命名選項檔案。
例如：dsm.REMOTE1_MP_WIN.opt。

限制：請勿在選項檔案中啟用不需 LAN 的選項 (ENABLELANFREE YES)。 裝載 Proxy 節點不支援這個選項。

3. 發出此資料移轉裝置指令，以設定裝載 Proxy 節點的 VMware vCenter 使用者與密碼：

提示：若要啟動 dsmc 指令行，請開啟 **Windows 開始**功能表，並選取**所有程式 → IBM Spectrum Protect → 備份用戶端指令行**。

```
dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator> <password1>
-optfile=dsm.REMOTE1_MP_WIN.opt
```

4. 發出下列指令，驗證與 IBM Spectrum Protect 伺服器的連線：

```
dsmc query session -optfile=dsm.REMOTE1_MP_WIN.opt
```

這個指令會顯示階段作業的相關資訊，包括現行節點名稱、建立階段作業的時間、伺服器資訊以及伺服器連線資訊。

5. 完成下列步驟來設定用戶端接收器服務 (CAD) 及資料移轉裝置排程器服務：
這個步驟使用「IBM Spectrum Protect 用戶端 GUI 配置」精靈來設定 CAD 及「排程器服務」。 依預設，「遠端用戶端代理程式服務」也可以透過精靈來設定。如果針對這項作業使用 IBM Spectrum Protect 用戶端服務配置公用程式 (dsmcutil)，請確保還安裝遠端用戶端代理程式服務。
移至**公用程式 > 設定精靈**，以從檔案功能表啟動 IBM Spectrum Protect「用戶端配置」精靈：

a. 選取協助我配置 TSM Web 用戶端。 依提示輸入資訊。

1) 在您要服務何時啟動？選項中，選取在 Windows 啟動時自動啟動。

2) 在您要在完成此精靈時啟動服務嗎？選項中，選取是。

當作業順利完成時，請回到精靈歡迎使用頁面，並繼續進行步驟 b。

提示：當您在同一系統上配置多個裝載 Proxy 節點時，必須針對每一個用戶端接收器實例指定不同的埠值。

b. 選取協助我配置 TSM 用戶端排程器。 依提示輸入資訊。

1) 當輸入排程器名稱時，請確定選取使用用戶端接收器常駐程式 (CAD) 管理排程器選項。

2) 在您要服務何時啟動？選項中，選取在 Windows 啟動時自動啟動。

3) 在您要在完成此精靈時啟動服務嗎？選項中，選取是。

6. 驗證用戶端接收器及代理程式的設定是否正確。利用下列位址和埠，使用 Web 瀏覽器來連接 HOST1 系統：

   http://HOST1.xyz.yourcompany.com:1581

在 Linux 系統上手動配置多個用戶端接收器服務

在特定情況下，在單一 Linux 用戶端主機上，使用多個 dsmcad 服務，可能會有很有益處。

關於這項作業

此作業會設定多個 dsmcad 實例，以在系統啟動時自動執行及啟動：

程序

1. 在 dsm.sys 檔案中，建立兩個唯一節點段落（依預設，此檔案位於 /opt/tivoli/tsm/client/ba/bin/ 中）：

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm.sys
SErvername node1
  COMMMethod         TCPip
  TCPPort 1500
  TCPServeraddress   localhost
  nodename           node1
  errorlogname       /opt/tivoli/tsm/client/ba/bin/dsmerror-node1.log
  schedlogname       /opt/tivoli/tsm/client/ba/bin/dsmsched-node1.log
  managedservices    webclient sched
  httpport           1581
  passwordaccess     generate

SErvername node2
  COMMMethod         TCPip
  TCPPort 1500
  TCPServeraddress   localhost
  nodename           node2
  errorlogname       /opt/tivoli/tsm/client/ba/bin/dsmerror-node2.log
  schedlogname       /opt/tivoli/tsm/client/ba/bin/dsmsched-node2.log
  managedservices    webclient sched
  httpport           1582
  passwordaccess     generate
```

   提示：包含特定併入/排除選項，以區分這兩個節點，可能會很有益處。 否則，相同的資料可能會使用兩個節點名稱備份。

2. 建立兩個 dsm.opt 檔案，每一個節點一個（依預設，這兩個檔案位於 /opt/tivoli/tsm/client/ba/bin 中）：

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
servername node1
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
servername node2
```

3. 透過使用兩個節點的認證登入，以啟用 passwordaccess generate：

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
servername node1
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
servername node2
```

4. 複製兩份預設 rc.dsmcad Init Script（依預設，此 Script 位於 /opt/tivoli/tsm/client/ba/bin 中）：

```
# cp /opt/tivoli/tsm/client/ba/bin/rc.dsmcad /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1
# cp /opt/tivoli/tsm/client/ba/bin/rc.dsmcad /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2
```

5. 編輯 rc.dsmcad-node1：
   a. 將以下用於 Red Hat Enterprise Linux 發行套件的行：

      ```
      daemon $DSMCAD_BIN
      ```

      變更為以下行：

      ```
      daemon $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
      ```

   b. 將以下用於 SUSE Linux Enterprise Server 發行套件的行：

      ```
      startproc $DSMCAD_BIN
      ```

      變更為以下行：

      ```
      startproc $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
      ```

6. 編輯 rc.dsmcad-node2：
   a. 將以下用於 Red Hat Enterprise Linux 發行套件的行：

      ```
      daemon $DSMCAD_BIN
      ```

      變更為以下行：

      ```
      daemon $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
      ```

   b. 將以下用於 SUSE Linux Enterprise Server 發行套件的行：

      ```
      startproc $DSMCAD_BIN
      ```

      變更為以下行：

      ```
      startproc $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
      ```

7. 在 /etc/init.d/ 中建立兩個新鏈結，以指向這兩個新 rc.dsmcad Init Script。 這兩個鏈結容許 Linux init 服務，在系統啟動時，啟動 dsmcad 服務：

   ```
   # ln -s /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2 dsmcad-node2
   # ln -s /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1 dsmcad-node1
   # ls -la dsm*
   lrwxrwxrwx. 1 root root 45 Aug  2 08:04 dsmcad-node1 -> /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1
   lrwxrwxrwx. 1 root root 45 Aug  2 08:04 dsmcad-node2 -> /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2
   ```

8. 使用 **chkconfig**，登錄兩個新 rc Script：

   ```
   # chkconfig --add dsmcad-node1
   # chkconfig --add dsmcad-node2
   ```

9. 使用 **service dsmcad start** 指令，來測試配置，以確保 Script 正常載入及啟動，而沒有問題：

```
# service dsmcad-node1 start
Starting dsmcad-node1:                                     [  OK  ]
# service dsmcad-node2 start
Starting dsmcad-node2:                                     [  OK  ]
# ps -ef | grep dsmcad
root 2689 1 0 09:04 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
root 2719 1 0 09:04 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

本範例中，指令文字分為兩行，以符合頁面格式設定。

10. 重新啟動並確認兩個 dsmcad 實例已自動啟動：

```
# ps -ef | grep dsmcad
root 1830 1 0 09:14 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
root 1856 1 0 09:14 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

本範例中，指令文字分為兩行，以符合頁面格式設定。

修改 VMCLI 配置檔

VMCLI 配置檔 (vmcliConfiguration.xml) 包含 Data Protection for VMware vSphere GUI 的設定。

Data Protection for VMware 安裝程序需要使用者指定 vCenter Server IP 位址，以及是否讓 Web 瀏覽器存取 GUI。 然而，在安裝之後，安裝者並無法修改伺服器 IP 位址和 GUI 存取方法。

若要更新這些設定，您可以手動編輯 VMCLI 配置檔 (vmcliConfiguration.xml)。 在安裝期間，會在下列位置中建立此檔案：
在 Windows 系統上：
C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\tsmVmGUI
在 Linux 系統上：
/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/tsmVmGUI/

若要修改是否可透過 Web 瀏覽器存取 GUI，請在 **<enable_direct_start></enable_direct_start>** 參數中輸入下列其中一個值：

- *yes* 可以透過 Web 瀏覽器直接存取 GUI。 例如：

```
<enable_direct_start>yes</enable_direct_start>
```

- *no* 無法透過 Web 瀏覽器直接存取 GUI。 例如：

```
<enable_direct_start>no</enable_direct_start>
```

若要將 GUI 用於 vSphere 保護，請在 **<mode></mode>** 參數中指定下列其中一個值：

- *vcenter* 使用 GUI 進行 vSphere 保護。 例如：

```
<mode>vcenter</mode>
```

若要修改 vCenter 伺服器 IP 位址，請確保已設定 **<mode>vcenter</mode>**，然後在 **<vcenter_url></vcenter_url>** 參數中指定 IP 位址。例如：

```
<vcenter_url>https://vcenter.myco.com/sdk</vcenter_url>
```

vCenter 伺服器 IP 位址的開頭處必須有 `https://` 值。 vCenter 伺服器 IP 位址的結尾處必須有 `/sdk` 值。

範例 *vmcliConfiguration.xml* 檔案

已針對 vSphere 保護配置下列 `vmcliConfiguration.xml` 檔，並已對 GUI 啟用 Web 瀏覽器存取權：

```
<?xml version="1.0" encoding="UTF-8"?>
<vmcliAdaptor>
 <VMCLIPath>C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\scripts\
</VMCLIPath>
 <interruptDelay>900000</interruptDelay>
 <mode>vcenter</mode>
 <vcenter_url>https://vcenter.myco.com/sdk</vcenter_url>
 <enable_direct_start>yes</enable_direct_start>
</vmcliAdaptor>
```

附錄 B. 移轉至持續增量增量備份策略

使用此程序來移轉現有備份排程、原則及資料移轉裝置節點，以在持續增量備份策略中使用。

開始之前

可以使用 Data Protection for VMware 6.2 版及 6.3 版中實作的持續增量完整備份策略。 如果要繼續使用持續增量完整備份策略，則不需要變更原則或排程。 必須確保僅將資料移轉裝置節點升級至 6.4 版（或更新版本），如下列程序中所述。然而，如果您要使用持續增量增量備份策略，則除了將資料移轉裝置節點更新至 6.4 版（或更新版本）之外，您還必須更新移至此持續增量增量備份策略之那些資料移轉裝置節點的排程及原則。

若要將現有 Data Protection for VMware 排程移轉至持續增量增量備份策略，您必須完成此程序中說明的作業。

重要：

- 雖然部分作業離散，但是最終必須升級所有應用程式及元件，才能完全受益於持續增量增量策略。 此出版品提供了引導您完成每個作業所需的所有資訊。
- 可以使用數種方法來完成整個移轉處理程序。 但是，我們將此出版品中記載的方法視為典型 Data Protection for VMware 環境的有效方法。
- 此程序中要移轉的排程，是使用 Data Protection for VMware vSphere GUI 備份精靈來建立的排程。 如果手動建立了要移轉的排程，則也必須手動進行此程序中識別的排程更新。

關於這項作業

程序

1. 升級所有保護單一 vCenter 的「vStorage 備用伺服器」。 請確保同時對所有資料移轉裝置節點完成此升級。
   - 此升級需要在「vStorage 備用伺服器」上安裝 IBM Spectrum Protect 資料移轉裝置 6.4 版（或更新版本）。
   - 作為離散作業，您不必在完成步驟 1 後立即完成步驟 2 或步驟 3。升級資料移轉裝置節點後，您可以繼續在現有環境中備份 VM。 有更便利的機會存在時，您可以完成步驟 2 和步驟 3。

   提示：如果環境使用多個「vStorage 備用伺服器」，請考量僅升級一個伺服器。 然後，確認伺服器順利運作，再升級剩餘的「vStorage 備用伺服器」。
2. 更新備份原則及備份排程以實作持續增量增量備份：
   透過在管理指令行用戶端上發出指令 (`dsmadmc`)，在 IBM Spectrum Protect 伺服器上完成下列備份原則作業：
   a. 為適合持續增量增量備份的網域及原則集建立管理類別。 此範例會給網域 `domain1` 和原則集 `prodbackups` 建立管理類別 `mgmt_ifincr28`。 管理類別名稱用來說明可以保留 28 個備份版本的持續增量增量備份策略：

```
define mgmtclass domain1 prodbackups mgmt_ifincr28
description="Retain 28 backup versions"
```

b. 為持續增量增量備份建立備份副本群組。 此範例會給網域 domain1、原則集 prodbackups 和管理類別 mgmt_ifincr28 建立標準備份副本群組：

```
define copygroup domain1 prodbackups mgmt_ifincr28 standard type=backup
```

standard type=backup 項目是預設值，並非必須指定。 將它們併到此範例中，是為了說明副本群組名稱為 STANDARD，以及副本群組類型為 backup（而不是 archive）。

c. 使用適當的版本、保留和有效期限設定來更新備份副本群組：

記住：在 Data Protection for VMware 6.2 版及 6.3 版中，備份版本、保留和有效期限基於備份鏈精度層次。 此方法表示即使持續增量完整備份和持續增量增量備份都予以採用（作為 6.2 和 6.3 持續增量完整備份策略），版本有效期限只計算完整備份。 在 Data Protection for VMware 6.4 版（或更新版本）中，備份版本、保留和有效期限基於單一備份精度層次。 此方法表示版本有效期限會計算持續增量完整備份和持續增量增量備份。

verexists 參數指定要在伺服器上保留的 VM 備份版本數目上限。 如果持續增量增量備份作業會造成超過此數目，則伺服器會使伺服器儲存體中存在的最舊備份版本過期。 此範例指定 verexists=28。 此值表示伺服器上最多保留 28 個 VM 備份版本。

retextra 參數指定在 VM 備份版本變成非作用中後，要保留的天數上限。 此範例指定 retextra=nolimit。 此值表示無限期保留的非作用中 VM 備份版本數目上限。 然而，指定 verexists 時，nolimit 值會取代為 verexists 值。 因此，在此範例中，會在伺服器上最多保留 28 個非作用中 VM 備份版本。

依照此步驟中說明的設定，備份副本群組會加以更新，如下所示：

```
update copygroup domain1 prodbackups mgmt_ifincr28 verexists=28
retextra=nolimit
```

在此範例中，現有 Data Protection for VMware 6.3 版環境由下列主機和排程所組成：

- 包含兩個 ESX 主機（esxhost1、esxhost2）的 ESX 叢集 (esxcluster)。
- bup_esxcluster_full 排程使用資料移轉裝置節點 dm1，每週對每個 ESX 主機進行持續增量完整備份一次。
- bup_esxcluster_incr 排程使用資料移轉裝置節點 dm2，每日對每個 ESX 主機進行持續增量增量備份一次。

在 Data Protection for VMware vSphere GUI 中完成下列備份排程作業：

a. 按一下 vSphere Client 的「解決方案及應用程式」視窗中的圖示，啟動 Data Protection for VMware vSphere GUI。
b. 在「入門」視窗中，按一下**備份**標籤，以開啟「管理備份排程」視窗。
c. 找出要更新的備份排程（用於持續增量完整備份或增量備份）。 在此程序中，使用持續增量完整 bup_esxcluster_full 排程。
d. 用滑鼠右鍵按一下排程並選取**內容**。
e. 移至「排程」頁面，並指定**備份策略**下拉清單中的**增量**。
f. 按一下**確定**以儲存更新。

g. 找出用於持續增量增量備份的備份排程。用滑鼠右鍵按一下排程並選取**刪除**。由於持續增量完整 bup_esxcluster_full 排程已更新為持續增量增量，因此不再需要此持續增量增量排程。

3. 在具有持續增量增量備份排程後，可以透過合併資料移轉裝置節點來減少資料移轉裝置節點數：
   此範例會將兩個資料移轉裝置節點合併為一個資料移轉裝置節點。
   a. 在「vStorage 備用伺服器」上，開啟命令提示字元並移至 dm1 的選項檔案所在的目錄。
   b. 使用文字編輯器（例如「記事本」），藉由下列選項更新此檔案：
      1) 指定 vmmaxparallel 以控制 dm1 一次所備份的 VM 數目：

         ```
         vmmaxparallel=2
         ```

         預設值及最小值皆為 1。最大值為 50。

         提示：對於您所移除的每個資料移轉裝置節點，將 vmmaxparallel 值增加 1。

         或者，可以指定 vmlimitperhost 以控制 dm1 一次從同一個 ESX 主機所備份的 VM 數目：

         ```
         vmlimitperhost=1
         ```

         如果要防止主機超載，則此選項很有用。 預設值為 0（無限制）。 最小值為 1。最大值為 50。
   c. 登入 IBM Spectrum Protect 伺服器。 使用管理指令行用戶端 (dsmadmc)，來指定可以與伺服器相連接的同步 VM 備份階段作業數目上限。 例如：

      ```
      maxsessions=4
      ```

      預設值為 25。 下限值為 2。

4. 確認所更新的資料移轉裝置節點會正常運作：
   a. 按一下您 vSphere Client 的「解決方案和應用程式」視窗中的圖示，來啟動 Data Protection for VMware vSphere GUI。
   b. 在「入門」視窗中，按一下「配置」標籤以檢視「配置狀態」頁面。
   c. 在「配置狀態」頁面中，選取步驟 1 中所保護的 vCenter。按一下資料移轉裝置節點，以在「狀態詳細資料」窗格中檢視其狀態資訊。 當節點顯示警告或錯誤時，請按一下該節點，然後使用「狀態詳細資料」窗格來解決問題。 然後選取節點，再按一下**驗證選取的節點**來驗證問題是否已解決。按一下「重新整理」以重新測試所有節點。

結果

成功完成每個作業後，環境便隨時可用於持續增量增量備份策略。

限制：將排程從持續增量完整備份類型移轉至持續增量增量備份類型後，請注意下列限制：

- 不支援將所移轉的排程改回為基於 VM（檔案空間）的持續增量完整備份類型。
- 不支援在已移轉的檔案空間上使用舊版 IBM Spectrum Protect 資料移轉裝置。
- 當檔案空間包含一個（或多個）持續增量增量備份時，不支援持續增量完整備份。

帶有 *verexists* 參數的版本控制範例

在此排程移轉範例中，Data Protection for VMware 6.3 版使用下列兩個備份排程：

- `-mode=full`：排程每週持續增量完整備份（星期日），並且要在伺服器上保留的 VM 備份版本數目上限是 4 (`verexists=4`)。
- `-mode=incr`：排程平日持續增量增量備份（星期一至星期六）。

4 週期間取得的備份數目為 28：

- 4 個持續增量完整備份（1 個每週完整備份乘以 4 週）
- 24 個持續增量增量備份（6 個平日增量備份乘以 4 週）

由於 Data Protection for VMware 6.3 版只計算完整備份，因此 `verexists=4` 值會保留所有 28 個備份。

如果要使用 Data Protection for VMware 6.4 版（或更新版本）及持續增量增量備份策略來提供同一層次的保護，請建立下列排程：
`-mode=iffull`：排程每日持續增量完整備份，而且 `verexists` 參數設為 28。
4 週期間取得的備份數目為 28：

- 1 個持續增量完整備份（起始備份乘以 1 日）
- 27 個持續增量增量備份（每日持續增量備份乘以 27 日）

由於 Data Protection for VMware 6.4 版（或更新版本）同時計算持續增量完整備份及持續增量增量備份，因此 `verexists=28` 值會保留所有 28 個備份。

附錄 C. IBM Spectrum Protect 系列產品的協助工具特性

協助工具特性可以幫助有身體障礙的使用者（例如行動不便或視力不佳），順利地使用資訊技術內容。

概觀

IBM Spectrum Protect 系列產品包含下列主要協助工具特性：

- 純鍵盤作業
- 使用螢幕閱讀器的作業

IBM Spectrum Protect 系列產品使用最新的 W3C 標準 WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/)，以確保遵循 US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) 及 Web Content Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/)。若要利用協助工具特性，請使用最新版本的螢幕閱讀器，以及產品支援的最新 Web 瀏覽器。

已針對 IBM Knowledge Center 中的產品說明文件啟用協助工具。 IBM Knowledge Center 的協助工具特性在 IBM Knowledge Center 說明的協助工具區段 (www.ibm.com/support/knowledgecenter/about/releasenotes.html?view=kc#accessibility) 中說明。

鍵盤導覽

此產品使用標準導覽鍵。

介面資訊

使用者介面沒有每秒閃動 2 至 55 次的內容。

Web 使用者介面根據階式樣式表，以正確地呈現內容，以及提供可使用的經驗。 應用程式為視力低下的使用者提供相當的方法來使用系統顯示設定，例如高對比模式。 您可以透過使用裝置或 Web 瀏覽器設定來控制字型大小。

Web 使用者介面包括 WAI-ARIA 導覽地標，您可以用來快速導覽至應用程式中的功能區域。

供應商軟體

IBM Spectrum Protect 系列產品包含並未涵蓋在 IBM 授權合約中的特定供應商軟體。 IBM 不會說明這些產品的協助工具特性。 如需產品的協助工具相關資訊，請與供應商聯絡。

相關的協助工具資訊

除了標準 IBM 服務台及支援網站之外，IBM 提供 TTY 電話服務，供聽障或重聽客戶用來存取銷售及支援服務：

TTY 服務
800-IBM-3383 (800-426-3383)
（北美洲內）

如需 IBM 對協助工具之承諾的相關資訊，請參閱 IBM Accessibility (www.ibm.com/able)。

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或產品副本，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 的產品、程式或服務，使用者必須自行負責作業的評估和驗證責任。

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 (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

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違反規定、可商用性或特定目的之適用性的隱含保證。 有些適用範圍在特定交易上，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本 IBM 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。

如果本程式之被授權人為了 (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。

這裡呈現的所討論效能資料衍生自特定作業條件。實際結果可能不同。

本文件所提及之非 IBM 產品資訊，取自產品的供應商，或其公佈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。

本資訊含有日常企業運作所用之資料和報告範例。 為了儘可能加以完整說明，範例中含有個人、公司、品牌及產品的名稱。 所有這些名稱全為虛構，任何與實際商場企業使用的名稱及地址類似之處，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。 這些範例並未經過各種條件下的完整測試。 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。

這些範例程式或任何衍生成果的每份複本或任何部分，都必須依照下列方式併入著作權聲明：© （ 貴客戶之公司名稱）（年）。 本程式之若干部分係衍生自 IBM 公司的範例程式。 © Copyright IBM Corp. _輸入年份_。

商標

IBM、IBM 標誌和 ibm.com® 是 International Business Machines Corp. 在全球許多國家或地區的商標或註冊商標。 其他產品和服務名稱可能是 IBM 或其他公司的商標。如需 IBM 商標的最新清單，請參閱網站上的「著作權及商標資訊」，網址為 www.ibm.com/legal/copytrade.shtml。

Adobe 是 Adobe Systems Incorporated 在美國及/或其他國家或地區的註冊商標。

Linear Tape-Open、LTO 和 Ultrium 是 HP、IBM Corp. 和 Quantum 在美國及其他國家或地區的商標。

Intel 及 Itanium 是 Intel Corporation 或其子公司在美國及其他國家或地區的商標或註冊商標。

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

Microsoft、Windows 和 Windows NT 是 Microsoft Corporation 在美國及（或）其他國家的商標。

Java 及所有 Java 型的商標和標誌是 Oracle 及（或）其分支機構的商標或註冊商標。

UNIX 是 The Open Group 在美國及其他國家或地區的註冊商標。

VMware、VMware vCenter Server 及 VMware vSphere 是 VMware, Inc. 在美國及/或其他司法管轄區的註冊商標或商標。

產品說明文件的條款

這些出版品的使用許可權，係遵循下列條款而授與。

適用性

這些條款是 IBM 網站的全部使用條款的增補項目。

個人使用

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

您只能在您的企業內重製、散佈及展示這些書籍，但我們保留所有財產權。在未獲得 IBM 明確同意之下，您不能衍生著作這些出版品，或重製、散佈或展示這些出版品或其任何部分到您的企業外部。

權利 除非本許可權中已明確授與，否則將不會以明示或暗示的方式，來提供出版品或其中包含的任何資訊、資料、軟體或其他智慧財產的其他許可權、授權或權利。

如 IBM 認為出版品的使用途徑損及 IBM 的利益，或經 IBM 判斷為未適當遵守上述指示時，IBM 保留撤銷本項授權的權利。

除非完全依循所有適用的法規（包括所有美國出口法規），否則您不得下載、匯出或重新匯出這項資訊。

IBM 不提供這些出版品內容的任何保證。 這些出版品依其「現狀」提供，不附帶任何明示或默示之擔保，其中包括（但不限於）適售性、未涉侵權及適合特定用途之默示擔保責任。

隱私權原則考量

IBM 軟體產品，包括軟體即服務解決方案（即「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，來協助改良一般使用者經驗、調整與一般使用者的互動，或供其他目的之用。 在許多情況下，「軟體供應項目」不會收集個人識別資訊。部分「軟體供應項目」可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，則下面會說明有關此供應項目使用 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。

如果為此「軟體供應項目」部署的配置可讓 貴客戶使用 Cookie 與其他技術，從一般使用者處收集個人識別資訊，則 貴客戶應該洽詢法律顧問是否有任何法律可支援此類資料收集，包括任何注意事項及同意要求。

如需使用各種技術（包括 Cookie）供這些用途使用的相關資訊，請參閱 IBM 的「隱私權條款」(http://www.ibm.com/privacy) 和 IBM 的「線上隱私權聲明」(http://www.ibm.com/privacy/details) 中標題為「Cookie、Web Beacon 和其他技術」的章節以及「IBM 軟體產品和軟體即服務 (Software-as-a-Service) 隱私權聲明」(http://www.ibm.com/software/info/product-privacy)。

名詞解釋

提供了含有 IBM Spectrum Protect 產品系列術語與定義的名詞解釋。

請參閱IBM Spectrum Protect 名詞解釋。

索引

索引順序以中文字，英文字，及特殊符號之次序排列。

〔四劃〕

〔五劃〕

〔六劃〕

〔七劃〕

〔八劃〕

〔九劃〕

〔十劃〕

〔十一劃〕

〔十二劃〕

〔十三劃〕

〔十四劃〕

〔十五劃〕

〔十七劃〕

〔二十二劃〕

D

G

I

K

L

R

S

T

V

W

程式號碼： 5725-X00

Printed in Taiwan