Site Recovery Manager 安全性

Site Recovery Manager 8.1

vmware®

您可以在 VMware 網站上找到最新的技術說明文件，網址為:

https://docs.vmware.com/tw/

如果您對此文件有何想法，請將您的回應意見提交至：

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

內容

關於 VMware Site Recovery Manager 安全性 4

1 Site Recovery Manager 安全性參考 5

Site Recovery Manager 服務 6

Site Recovery Manager 網路連接埠 6

Site Recovery Manager 組態檔 7

Site Recovery Manager 憑證和金鑰 7

Site Recovery Manager 儲存的認證 8

Site Recovery Manager 授權和使用者授權合約檔案 8

Site Recovery Manager 記錄檔 9

Site Recovery Manager 帳戶 10

Site Recovery Manager 安全性更新和修補程式 11

保護 Site Recovery Manager Server 的最佳做法 12

關於 VMware Site Recovery Manager 安全性

*Site Recovery Manager 安全性*提供 Site Recovery Manager 安全性功能的簡要參考。

為協助您保護 Site Recovery Manager 安裝，本指南說明內建到 Site Recovery Manager 中的安全性功能，以及為使其免受攻擊可採取的措施。

- Site Recovery Manager 正確執行作業所需的外部介面、連接埠以及服務
- 擁有安全性含意的組態選項與設定
- 記錄檔的位置及其用途
- 所需的系統帳戶
- 取得最新安全性修補程式的相關資訊

適合對象

這項資訊適用於 IT 決策者、架構設計人員、管理員，以及必須熟悉 Site Recovery Manager 安全性元件的其他人。

Site Recovery Manager 安全性參考

1

使用安全性參考可瞭解 Site Recovery Manager 安裝的安全性功能，以及為使您的環境免受攻擊可採取的措施。

- Site Recovery Manager 服務

  Site Recovery Manager 的作業取決於在 Site Recovery Manager Server 主機機器上執行的數個服務。

- Site Recovery Manager 網路連接埠

  Site Recovery Manager 使用可設定的網路連接埠與用戶端和其他伺服器進行通訊。您必須確保防火牆不會封鎖 Site Recovery Manager 使用的連接埠。

- Site Recovery Manager 組態檔

  部分 Site Recovery Manager 組態檔包含可能會影響您的環境之安全的設定。不正確的設定可能還會影響您的 Site Recovery Manager 環境之正常運作。

- Site Recovery Manager 憑證和金鑰

  Site Recovery Manager 使用 TLS 憑證和私密金鑰來保護網路通訊並使用其他伺服器安全建立驗證。

- Site Recovery Manager 儲存的認證

  Site Recovery Manager 會在 Windows 登錄中以加密格式儲存 Storage Replication Adapter (SRA) 和資料庫的認證。

- Site Recovery Manager 授權和使用者授權合約檔案

  Site Recovery Manager 授權和使用者授權合約檔案位於 Site Recovery Manager Server 主機機器上。

- Site Recovery Manager 記錄檔

  Site Recovery Manager 會將作業資訊記錄至記錄檔。記錄檔不包含諸如私密金鑰和密碼等敏感資訊。

- Site Recovery Manager 帳戶

  Site Recovery Manager 使用 Single Sign-On (SSO) 來存取 vCenter Server 和 Platform Services Controller。

- Site Recovery Manager 安全性更新和修補程式

  當 VMware 提供 Site Recovery Manager 安全性更新和修補程式時，您可將其套用。當主機作業系統的廠商提供主機作業系統的安全性更新和修補程式時，您可將其套用。

- 保護 Site Recovery Manager Server 的最佳做法

  保護 Site Recovery Manager Server 的最佳做法可以保護您的環境免遭可能的安全性問題。

Site Recovery Manager 服務

Site Recovery Manager 的作業取決於在 Site Recovery Manager Server 主機機器上執行的數個服務。

表格 1-1. Site Recovery Manager 需要的服務

服務名稱	啟動時間	說明
VMware vCenter Site Recovery Manager Server	自動	提供核心 Site Recovery Manager 功能。
VMware vCenter Site Recovery Manager 內嵌式資料庫	如果您使用內嵌式資料庫則為自動。	Site Recovery Manager 內嵌式資料庫的 vPostgres 伺服器。
VMware vCenter Site Recovery Manager 用戶端	自動	提供 VMware vCenter Site Recovery Manager 用戶端 (Tomcat、HTML5 使用者介面) 功能。
伺服器	自動	支援透過網路共用檔案的 Windows 服務。
工作站	自動	建立並維護與遠端伺服器之連線的 Windows 服務。
受保護的儲存區	自動	儲存敏感資料的 Windows 服務。

Site Recovery Manager 網路連接埠

Site Recovery Manager 使用可設定的網路連接埠與用戶端和其他伺服器進行通訊。您必須確保防火牆不會封鎖 Site Recovery Manager 使用的連接埠。

Site Recovery Manager Server 接收一個網路連接埠上的所有傳入流量。預設連接埠是 9086。如果您將 Site Recovery Manager 設定為使用內嵌式資料庫，Site Recovery Manager 內嵌式資料庫會在本機回送介面上接收 localhost 網路流量。預設連接埠是 5678。

如果預設連接埠遭到封鎖或者被其他應用程式使用，則在安裝程序期間，您可選取 Site Recovery Manager 的其他連接埠和內嵌式資料庫流量。您必須設定網路原則才能啟用傳入連接埠上的流量。如需您可在安裝後進行變更之連接埠的相關資訊，請參閱 *Site Recovery Manager 安裝與組態*說明文件中的*修改 Site Recovery Manager Server 安裝*主題。

Site Recovery Manager Server 與 Platform Services Controller、vCenter Server 和 ESXi 主機以及本機站台上的陣列進行通訊。您必須確認網路防火牆原則在本機站台上已啟用所有元件的網路連接埠之流量。如需所有 VMware 產品使用的預設連接埠清單，請參閱 http://kb.vmware.com/kb/1012382。

Site Recovery Manager 配對的本機和遠端站台之間的連線必須為私人的，如 VPN。本機 Site Recovery Manager Server 在遠端站台上與 Site Recovery Manager Server、Platform Services Controller 和 vCenter Server 進行通訊，您的網路提供商必須確保使用適當的網路原則才能啟用流量。

如需必須對 Site Recovery Manager 開啟的所有連接埠的清單，請參閱 *Site Recovery Manager 安裝與組態*說明文件中的〈Site Recovery Manager 的網路連接埠〉主題。

Site Recovery Manager 組態檔

部分 Site Recovery Manager 組態檔包含可能會影響您的環境之安全的設定。不正確的設定可能還會影響您的 Site Recovery Manager 環境之正常運作。

表格 1-2. Site Recovery Manager 組態檔

檔案或目錄位置	說明
installation_folder\VMware\VMware vCenter Site Recovery Manager\config\vmware-dr.xml	定義 Site Recovery Manager Server 的系統組態。 **備註** 請勿移動或刪除組態檔。 您可使用 Site Recovery Manager 使用者介面中 [站台配對] 索引標籤上的**進階設定**，來安全變更 Site Recovery Manager 執行個體的系統設定。
installation_folder\VMware\VMware vCenter Site Recovery Manager Embedded Database\bin\vmw_vpg_config\	包含內嵌式資料庫組態檔。 **備註** 請勿修改、移動或刪除組態檔。
installation_folder\VMware\VMware vCenter Site Recovery Manager\config\extension.xml	定義 Site Recovery Manager Server 延伸的組態。extension.xml 檔案包含預設使用者角色的定義和權限。 **備註** 請勿修改、移動或刪除組態檔。
C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\runtime\srm-client\lib\h5dr.properties	定義 Site Recovery Manager HTML 5 使用者介面的組態。 **備註** 請勿移動或刪除組態檔。 您可將 *phonehomeEnabled* 值從 True 變更為 False (反之亦然)，來安全變更 Site Recovery Manager HTML 5 使用者介面的遙測設定。

Site Recovery Manager 憑證和金鑰

Site Recovery Manager 使用 TLS 憑證和私密金鑰來保護網路通訊並使用其他伺服器安全建立驗證。

CA 憑證或私密金鑰或同時選取兩者	位置和說明
Site Recovery Manager Server 端點的 TLS 憑證和金鑰	在 Windows 憑證存放區的 Certificates\vmware-dr\Personal\Certificates 資料夾中。 如果您在安裝期間未提供自訂憑證，Site Recovery Manager 會產生憑證。
在 Site Recovery Manager 安裝期間建立的 solution 使用者之 TLS 憑證和金鑰	在 Windows 憑證存放區的 Certificates\vmware-dr\su-*Site Recovery Manager UUID*\Certificates 資料夾中。
遠端站台上的 solution 使用者之 TLS 憑證和金鑰	在 Windows 憑證存放區的 Certificates\vmware-dr\remote-su-*Site Recovery Manager UUID*\Certificates 資料夾中。 Site Recovery Manager 會在執行配對程序期間建立檔案。
在 Site Recovery Manager 安裝期間建立的 HTML5 UI solution 使用者之 TLS 憑證和金鑰	位於 C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\runtime\srm-client\lib\h5dr.keystore 檔案。

CA 憑證或私密金鑰或同時選取兩者	位置和說明
Tomcat 伺服器端點的 TLS 憑證和金鑰	位於 `C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\runtime\srm-client\conf\h5dr-server.keystore` 檔案。 與 Site Recovery Manager Server 端點之 TLS 憑證和金鑰相同。
Site Recovery Manager Server 的 CA 憑證和 TLS 憑證	*installation_folder*`\VMware\VMware vCenter Site Recovery Manager\bin\`*SRM_Server_IP_addressca*`.p7b` 檔案。 如果您在安裝期間未提供自訂憑證，Site Recovery Manager 會產生憑證。 您可將憑證匯入至用戶端信任金鑰儲存區，以允許使用者隱式信任 Site Recovery Manager Server 憑證。

備註 請勿擷取或共用私密金鑰資訊，以保護您的 Site Recovery Manager 執行個體。

如需有關 Site Recovery Manager 驗證機制的詳細資訊，請參閱《*Site Recovery Manager 安裝與組態指南*》中的 *Site Recovery Manager 驗證*主題。

Site Recovery Manager 儲存的認證

Site Recovery Manager 會在 Windows 登錄中以加密格式儲存 Storage Replication Adapter (SRA) 和資料庫的認證。

如果您是管理員群組的成員，即可存取該認證。

登錄路徑	說明
`HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\Vmware DR\Creds\db:`*datastore name*	用於存取使用 *datastore name* 系統資料存放區的 Site Recovery Manager 資料庫的認證。
`HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\Vmware DR\Creds\storage-arraymanager` *manager id*`-username`	連線至依 *manager id* 識別的陣列管理員時，SRA 必須使用的使用者名稱。
`HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\ Vmware DR\Creds\storage-arraymanager-`*manager id*`-password`	連線至依 *manager id* 識別的陣列管理員時，SRA 必須使用的密碼。

Java 金鑰儲存區 `h5dr.keystore` 的認證儲存在位於 `C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\runtime\srm-client\lib\` 資料夾中的 `h5dr.properties` 檔案。Java 金鑰儲存區 `h5dr-server.keystore` 的認證儲存在位於 `C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\runtime\srm-client\conf\` 資料夾中的 `server.xml` 檔案。

Site Recovery Manager 授權和使用者授權合約檔案

Site Recovery Manager 授權和使用者授權合約檔案位於 Site Recovery Manager Server 主機機器上。

表格 1-3. Site Recovery Manager 授權和使用者授權合約檔案

檔案或目錄	說明
installation_folder\VMware\VMware vCenter Site Recovery Manager\en\	包含 Site Recovery Manager 使用者授權合約檔案的目錄。
installation_folder\VMware\VMware vCenter Site Recovery Manager\en\open_source_license.txt	Site Recovery Manager 開放原始碼授權檔案。
installation_folder\VMware\VMware vCenter Site Recovery Manager Embedded Database\share\EULA-en.rtf	Site Recovery Manager 內嵌式資料庫使用者授權合約檔案。
installation_folder\VMware\VMware vCenter Site Recovery Manager Embedded Database\share\open_source_license.txt	Site Recovery Manager 內嵌式資料庫開放原始碼授權檔案。

Site Recovery Manager 記錄檔

Site Recovery Manager 會將作業資訊記錄至記錄檔。記錄檔不包含諸如私密金鑰和密碼等敏感資訊。

Site Recovery Manager Server 記錄

Site Recovery Manager 將系統記錄檔案儲存在 `C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\Logs` 目錄中。來自 Site Recovery Manager Server 的最新訊息會置於 `vmware-dr-`*`number`*`.log` 檔案中。

如果您重新啟動 Site Recovery Manager Server 或者目前的檔案必須超過設定檔案大小限制，則 Site Recovery Manager 會封存目前的記錄檔並建立新的記錄檔。

若要變更記錄檔目錄，請在 *`installation_directory`*`\VMware\VMware vCenter Site Recovery Manager\config\vmware-dr.xml` 組態檔的目錄 XML 元素中輸入自訂目錄名稱。您還可以透過更新 `vmware-dr.xml` 檔案中的 logLevel XML 元素來變更每個元件的記錄層級。所有元件的預設層級為詳細資訊。

重要事項 設定存取控制清單以限制對記錄檔的存取權。

表格 1-4. 記錄層級

層級	說明
錯誤	僅顯示錯誤記錄項目。
資訊	顯示資訊、錯誤和警告記錄項目。
雜項	顯示資訊、錯誤、警告、詳細資訊和雜項記錄項目。
詳細資訊	顯示資訊、錯誤、警告和詳細資訊記錄項目。
警告	顯示警告和錯誤記錄項目。

Site Recovery Manager 支援的元件如下：

- 預設值
- 複寫

- 復原
- 儲存區
- StorageProvider
- Vdb
- 持續性

vmware-dr-*number*.log 檔案未包含驗證程序以及與遠端站台之連線的相關安全訊息。

Site Recovery 使用者介面記錄

Site Recovery Manager 將 Site Recovery 使用者介面記錄檔儲存在 C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\runtime\srm-clients\logs 目錄中。最新訊息放置在 dr.log 檔案中。

您可以更新 C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\runtime\srm-client\webapps\dr\WEB-INF\classes 目錄中的 log4j.xml 檔案中的層級值元素，來修改每個元件的記錄層級。所有元件的預設層級為資訊。

表格 1-5. 記錄層級

層級	說明
錯誤	僅顯示錯誤記錄項目。
警告	顯示警告和錯誤記錄項目。
資訊	顯示資訊、錯誤和警告記錄項目。
偵錯	顯示偵錯、資訊、錯誤和警告記錄項目。
追蹤	顯示最詳細的資訊。

Site Recovery 使用者介面所使用的 Tomcat 伺服器支援如下的元件：

- Http 非同步 I/O
- 每個處理常式呼叫時間
- VC L10N 目錄
- SRM
- VR
- 通用

Site Recovery Manager 帳戶

Site Recovery Manager 使用 Single Sign-On (SSO) 來存取 vCenter Server 和 Platform Services Controller。

使用者帳戶

vCenter Server 管理員在預設組態中具有 Site Recovery Manager 的管理存取權。安裝 Site Recovery Manager 後當您首次嘗試登入時，您必須使用管理員認證。

如果您具有管理員認證，則可透過使用 vSphere Web Client 為其他使用者授與 Site Recovery Manager 存取權。

如需有關 Site Recovery Manager 角色、使用權限以及權限的詳細資訊，請參閱《*Site Recovery Manager 管理*》說明文件中的 *Site Recovery Manager 使用權限、角色以及權限*。

`Solution` 使用者帳戶

Site Recovery Manager 在安裝期間會建立 `solution` 使用者，並將其用於使用 vCenter Server 進行驗證期間。`solution` 使用者對於每個 Site Recovery Manager 執行個體是唯一的，且供 Site Recovery Manager、vCenter Server 和 Platform Services Controller 在內部使用。

Site Recovery Manager 會在不使用增強型連結模式的站台配對程序期間，在每個遠端站台上建立其他 `solution` 使用者。Site Recovery Manager 會使用 `solution` 使用者以在遠端站台上執行必要的作業。

Site Recovery Manager 在安裝期間為 HTML5 使用者介面建立 `solution` 使用者，並在 vCenter Server 的驗證期間透過 HTML5 UI 予以使用。解決方案使用者對於每個 Site Recovery Manager 執行個體是唯一的，且供 Site Recovery Manager HTML5 UI 用戶端、vCenter Server 和 Platform Services Controller 在內部使用。

備註 您不得刪除和修改與 `solution` 使用者帳戶相關聯的角色和權限。

如需有關本機和遠端站台之間的 `solution` 使用者和驗證之詳細資訊，請參閱《*Site Recovery Manager 安裝與組態*》說明文件中的 *Site Recovery Manager 驗證*主題。

Site Recovery Manager 安全性更新和修補程式

當 VMware 提供 Site Recovery Manager 安全性更新和修補程式時，您可將其套用。當主機作業系統的廠商提供主機作業系統的安全性更新和修補程式時，您可將其套用。

Site Recovery Manager 主機作業系統版本

如需 Site Recovery Manager Server 支援的主機作業系統的相關資訊，請參閱 *Site Recovery Manager 8.1 相容性矩陣圖*，網址為 https://docs.vmware.com/tw/Site-Recovery-Manager/8.1/rn/srm-compat-matrix-8-1.html。

套用 Site Recovery Manager 修補程式和安全性更新

您可以透過執行現有 Site Recovery Manager 安裝的就地升級來套用 Site Recovery Manager 安全性修補程式和更新。如需升級 Site Recovery Manager 的相關資訊，請參閱 *Site Recovery Manager 安裝與組態*中的〈*Site Recovery Manager 伺服器就地升級*〉主題。

保護 Site Recovery Manager Server 的最佳做法

保護 Site Recovery Manager Server 的最佳做法可以保護您的環境免遭可能的安全性問題。

Site Recovery Manager 的保護作業取決於 Site Recovery Manager Server 作業系統的適當組態和維護。

- 僅在支援的主機作業系統、資料庫和硬體上執行 Site Recovery Manager。如果 Site Recovery Manager 未在支援的主機作業系統上執行，Site Recovery Manager 可能無法正確執行。
- 套用最新的作業系統更新和修補程式，以保護主機作業系統免遭惡意攻擊。套用最新的 Site Recovery Manager 更新和修補程式，以解決 Site Recovery Manager 的任何已知問題。
- 將 Site Recovery Manager 做為虛擬機器執行時，請確保 Site Recovery Manager 部署的完整性。請參閱《*vSphere 安全性*》說明文件中的「虛擬機器安全最佳做法」主題。
- 限制軟體安裝並停用 Site Recovery Manager 未使用的服務，以釋放資源並降低伺服器攻擊的可能性。不需要的軟體和服務會耗用 CPU、儲存區、記憶體和頻寬資源，並會增加伺服器攻擊的機會。
- 僅允許管理員存取伺服器。若要限制攻擊者可使用的帳戶數目，請限制可存取伺服器的帳戶數目。
- 檢查 Site Recovery Manager 使用的網路連接埠並設定防火牆，以保護伺服器。