VMware vSphere Replication 安全性指南

vSphere Replication 8.2

您可以在 VMware 網站上找到最新的技術文件，網址如下：

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

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

目錄

關於 VMware vSphere Replication 安全性指南

1

《VMware vSphere Replication 安全性指南》提供 vSphere Replication 安全性功能的簡要參考。

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

- vSphere Replication 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

預定對象

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 vSphere Replication 安全性元件的其他人。

vSphere Replication 安全性參考 2

您可以使用「安全性參考」來瞭解 vSphere Replication 的安全性功能，以及為保護您的環境免受攻擊可採取的措施。

本章節討論下列主題：

vSphere Replication 虛擬應用裝置使用的服務、連接埠和外部介面

vSphere Replication 的作業取決於某些服務、連接埠和外部介面。

vSphere Replication 服務

vSphere Replication 的作業取決於在 vSphere Replication 虛擬應用裝置上執行的數個服務。

表 2-1. vSphere Replication 服務

服務名稱	啟動類型	說明
hms	針對 vSphere Replication 應用裝置自動進行。已為 vSphere Replication 附加應用裝置停用。	vSphere Replication 管理服務
hbrsrv	自動	vSphere Replication 服務
sshd	預設為停用狀態。	SSH 服務

表 2-1. vSphere Replication 服務 (續)

服務名稱	啟動類型	說明
ntp	自動	透過網路時間通訊協定與網際網路時間伺服器同步的時間服務。 **備註** 在安裝或升級 vSphere Replication 虛擬應用裝置之後，您必須將應用裝置與時間伺服器同步。
vaos	自動	驅動網路設定、主機名稱設定、ssh 金鑰建立、使用者授權合約接受、開機指令碼執行以及 VAMI 初始化的客體作業系統初始化。

通訊連接埠

vSphere Replication 使用多個通訊連接埠和通訊協定。

vSphere Replication 應用裝置需要某些連接埠處於開啟狀態。

備註 vSphere Replication 伺服器必須能夠對目標 ESXi 主機進行 NFC 流量存取。

表 2-2. vSphere Replication 應用裝置所用的連接埠

來源	目標	連接埠	通訊協定	說明
vSphere Replication 應用裝置	本機 vCenter Server	80	TCP	所有傳輸到本機 vCenter Server Proxy 系統的管理流量。vSphere Replication 將開啟一個 SSL 通道以連線到 vCenter Server 服務。
vSphere Replication 應用裝置	遠端 Lookup Service	443	TCP	對遠端 Lookup Service 的所有呼叫。
vSphere Replication 應用裝置中的 vSphere Replication 伺服器	ESXi 主機 (內部站台)	80	HTTP	用於在初始複寫開始之前建立連線。
vSphere Replication 應用裝置	本機和遠端 vCenter Server	443	TCP	所有到 vSphere Replication 應用裝置的管理流量。
vSphere Replication 應用裝置中的 vSphere Replication 伺服器	次要站台上的 ESXi 主機 (僅內部站台)	902	TCP 與 UDP	vSphere Replication 伺服器用來向目的地 ESXi 主機傳送複寫流量。
瀏覽器	vSphere Replication 應用裝置	5480	HTTPS	vSphere Replication 虛擬應用裝置管理介面 (VAMI) Web UI。
vCenter Server Proxy	vSphere Replication 應用裝置	8043	SOAP	來自來源和目標站台的 vSphere Replication 管理伺服器的內部站台通訊。
vSphere Replication 應用裝置	vSphere Replication 伺服器	8123	SOAP	從 vSphere Replication 管理伺服器到環境中其他 vSphere Replication 伺服器的內部站台管理流量。

表 2-2. vSphere Replication 應用裝置所用的連接埠 (續)

來源	目標	連接埠	通訊協定	說明
來源站台上的 ESXi 主機	目標站台上的 vSphere Replication 伺服器	31031	TCP	從位於來源站台的 ESXi 主機到位於目標站台的 vSphere Replication 應用裝置或 vSphere Replication 伺服器的初始和傳出複寫流量，且不對複寫流量使用網路加密。
來源站台上的 ESXi 主機	目標站台上的 vSphere Replication 伺服器	32032	TCP	從位於來源站台的 ESXi 主機到位於目標站台的 vSphere Replication 應用裝置或 vSphere Replication 伺服器的初始和傳出複寫流量，且對複寫流量使用網路加密。

如果您部署其他 vSphere Replication 伺服器，則必須在這些伺服器上開啟 vSphere Replication 所需的連接埠。

表 2-3. vSphere Replication 伺服器所用的連接埠

來源	目標	連接埠	通訊協定	說明
vSphere Replication 應用裝置中的 vSphere Replication 伺服器	次要站台上的 ESXi 主機 (僅內部站台)	902	TCP 與 UDP	同一個站台上 vSphere Replication 伺服器與 ESXi 主機之間的流量。特別是 NFC 服務到目的地 ESXi 伺服器的流量。
瀏覽器	vSphere Replication 伺服器	5480	HTTPS	管理員的網頁瀏覽器。
vSphere Replication Management Server	vSphere Replication 伺服器	8123	SOAP	從 vSphere Replication 應用裝置或 vSphere Replication Management Server 到 vSphere Replication 伺服器的內部站台管理流量。
來源站台上的 ESXi 主機	vSphere Replication 伺服器	31031	TCP	從位於來源站台的 ESXi 主機到位於目標站台的 vSphere Replication 應用裝置或 vSphere Replication 伺服器的初始和正向複寫流量。
來源站台上的 ESXi 主機	目標站台上的 vSphere Replication 伺服器	32032	TCP	從位於來源站台的 ESXi 主機到位於目標站台的 vSphere Replication 應用裝置或 vSphere Replication 伺服器的初始和正向複寫流量 (使用網路加密)。

當您建立與雲端的連線時，vSphere Replication 應用裝置中的 vCloud Tunneling Agent 會建立通道，以保護將複寫資料傳輸到您雲端組織的安全。

表 2-4. 雲端複寫所需的連接埠

來源	目的地	連接埠	通訊協定	說明
來源站台上的 ESXi 主機	來源站台上的 vCenter Server	80	TCP	vCenter Server 反向 Proxy 會將 VIB (vCloud Availability 防火牆規則) 下載要求轉送至 vSphere Replication 應用裝置。
來源站台上的 vSphere Replication 應用裝置	vCloud API	443	REST over HTTPS	vSphere Replication 應用裝置會連線至此連接埠，以傳送複寫資料至雲端組織。
來源站台上的 ESXi 主機	來源站台上的 vSphere Replication 應用裝置	10000–10010	TCP	vCloud Tunneling Agent 會開啟 vSphere Replication 應用裝置上這些連接埠的其中一個。ESXi 主機會連線至此連接埠，以傳送複寫資料至雲端組織。

開放原始碼和第三方元件

如需開放原始碼授權的完整文字、所有開放原始碼和第三方元件的清單以及在 vSphere Replication 中使用的開放原始碼，您可以前往 http://www.vmware.com/download/open_source.html 並查看 VMware vSphere 開放原始碼連結下的〈VMware vSphere Replication 開放原始碼和授權〉一節。如果某個開放原始碼授權需要，vSphere Replication 開放原始碼公開套件 (ODP) 將包含具有建置和取代軟體程式庫之指示的文字檔。

vSphere Replication 組態檔

部分組態檔包含會影響 vSphere Replication 之安全性的設定。

備註 所有安全性相關資源都受到適當的權限和擁有權保護。請勿變更這些檔案的擁有權或權限。

檔案位置	說明
`/opt/vmware/hms/conf/hms-configuration.xml`	vSphere Replication Management Server 的預設系統組態。
`/opt/vmware/hms/conf/embedded_db.cfg`	內嵌式資料庫的組態檔。

vSphere Replication 私密金鑰、憑證和金鑰儲存區

vSphere Replication 的私密金鑰、憑證和金鑰儲存區位於 vSphere Replication 虛擬應用裝置上。

備註 所有安全性相關資源都受到適當的權限和擁有權保護。請勿變更這些檔案的擁有權或權限。

- `/etc/vmware/ssl/hbrsrv.crt`
- `/etc/vmware/ssl/hbrsrv.key`
- `/opt/vmware/hms/security/hms-keystore.jks`
- `/opt/vmware/hms/security/hms-truststore.jks`

vSphere Replication 授權與使用者授權合約檔案

使用者授權合約 (EULA) 與開放原始碼授權檔案位於 vSphere Replication 虛擬應用裝置中。

檔案	位置
開放原始碼授權	`/usr/share/doc/vmware-vspherereplication/OPEN_SOURCE_LICENSE`
VMware Postgres 授權	`/usr/share/doc/vmware-vspherereplication/VMware_Postgres_9.5.16.0_open_source_licenses.txt`
使用者授權合約	`/opt/vmware/etc/isv/EULA/`*`language_code`*`/0`

vSphere Replication 記錄檔

包含系統訊息的檔案位於 vSphere Replication 虛擬應用裝置中。

檔案位置	說明
`/opt/vmware/hms/logs/hms-configtool.log`	用於記錄虛擬應用裝置管理介面 (VAMI) 組態期間發生的錯誤。
`/opt/vmware/hms/logs/hms.`*`n`*`.log`	用於追蹤 vSphere Replication Management Server 的執行階段資訊。最新的記錄檔標記為 `hms.log`，`hms.`*`n`*`.log` 檔案包含較舊的記錄訊息。具有最高 *n* 值的檔案包含最舊的訊息。
`/opt/vmware/var/log/lighttpd/error.log`	VAMI 錯誤記錄檔。用於追蹤 VAMI 作業中的錯誤。
`/var/log/vmware/`	此資料夾包含 vSphere Replication 伺服器記錄檔。用於追蹤複寫問題。
`/var/opt/apache-tomcat/logs/dr.log`	Site Recovery 使用者介面記錄。
`/opt/vmware/hms/logs/hms-audit.log`	vSphere Replication 稽核記錄。

與安全性相關的記錄訊息

`/opt/vmware/hms/logs/hms.log` 檔案包含採用下列格式的登入和登出事件訊息、授權錯誤訊息，以及憑證驗證錯誤訊息。

- 登入訊息

  ```
  2015-03-23 15:54:05.558 DEBUG jvsl.security.authentication.sessionmap [tcweb-5]
  (..security.authentication.SessionMap) operationID=087657ec-ef0f-494c-9739-
  a4af62a5c049-HMS-1033 | Adding new session to the session
  map:com.vmware.hms.security.authentication.HmsUserSession@234f4bed:[

  com.vmware.vim.binding.hms.UserSession:

  key = site_...1b034,

  userName = root,

  fullName = root ,
  ```

```
loginTime = ...,

lastActiveTime = ...,

hmsServers = null,

locale = en,

messageLocale = en

]
```

- 登出訊息

  ```
  15-03-23 15:54:05.585 INFO jvsl.security.authorization [tcweb-8]
  (..security.authorization.SessionAuthorizer) |
  HmsSessionManager.HmsSessionManagerLogout called on session-manager by root@/
  10.26.233.124:50776 with opId 43263a64-1681-4459-a921-1d9406308dc8-HMS-1036
  ```

- 授權訊息

  ```
  2015-06-25 16:10:35.994 INFO jvsl.security.authorization [tcweb-5]
  (..security.authorization.SessionAuthorizer) | Authorization for method
  "HmsRemoteSiteManager.HmsRemoteSiteManagerFindHmsServer" failed.

  (vim.fault.NoPermission) {

  faultCause = null,

  faultMessage = null,

  object = MoRef: type = HmsRemoteSiteManager, value = site-manager, serverGuid =
  18327b1a-dac2-44d9-972e-fa9dd99fce47,

  privilegeId = HmsRemote.com.vmware.vcHms.Hms.View

  }
  ```

- 憑證驗證錯誤訊息

  ```
  2015-06-25 16:19:13.794 WARN jvsl.sessions [hms-main-thread-1]
  (..hms.net.ServerRegistryHms) | Can not start HMS connection to remote site
  'some-address.com'

  java.util.concurrent.ExecutionException:
  com.vmware.vim.vmomi.client.exception.SslException:
  javax.net.ssl.SSLHandshakeException:
  com.vmware.vim.vmomi.client.exception.VlsiCertificateException: Server
  certificate chain is not trusted and thumbprint doesn't match
  ```

vSphere Replication 使用者帳戶

您必須為 vSphere Replication 設定根帳戶。根帳戶用於存取虛擬應用裝置主控台和虛擬應用裝置管理介面 (VAMI)。

vSphere Replication 目前使用根帳戶做為 VAMI 的管理員。未建立其他使用者。

當您部署 vSphere Replication 虛擬應用裝置時，請在 [OVF 部署] 精靈中為根帳戶設定密碼。

根密碼的長度必須至少為 8 個字元。

指派給預設使用者角色的權限

vSphere Replication 包含一組角色。每個角色包含一組權限，可讓擁有這些角色的使用者完成不同的動作。

請參閱《VMware vSphere Replication 安裝和設定》指南中的〈vSphere Replication 角色和權限〉主題。

vSphere Replication 安全性更新和修補程式

vSphere Replication 虛擬應用裝置採用 VMware Photon OS 2.0 做為客體作業系統。

您可以使用對應的 ISO 檔案來套用最新的安全性更新或修補程式。

在將更新或修補程式套用到客體作業系統之前，請將相依性納入考量。請參閱 vSphere Replication 虛擬應用裝置使用的服務、連接埠和外部介面。

若要接收最新安全公告，可在 http://lists.vmware.com/ 訂閱 VMware 安全公告郵件清單。