OpenManage Integration for VMware vCenter 5.3 版

安全性配置指南

3 月 2021 年
修正版 A00

DELL EMC

註、警示與警告

註:「註」表示可以幫助您更有效地使用產品的重要資訊。

警示:「警示」表示有可能會損壞硬體或導致資料遺失，並告訴您如何避免發生此類問題。

警告:「警告」表示可能的財產損失、人身傷害或死亡。

目錄

表

1

前言

在改善產品線的過程中，Dell EMC 會定期發佈其軟體和硬體的修訂版本。目前使用中的軟體或硬體版本可能不支援本文件中所說明的某些功能。產品版本資訊會提供產品功能的最新資訊。

如果產品無法正常運作或未按照本文件所說明的方式運作，請聯絡您的 Dell EMC 技術支援專業人員。本文件在發佈時是正確無誤的。若要確定本文件為最新版本，請前往 **https://www.dell.com/support**。

用途

本文件包含 OpenManage Integration for VMware vCenter (OMIVV) 的安全性功能與功能資訊。

對象

本文件適用於負責管理 OMIVV 安全性的人員。

修訂歷史

下表顯示本文件的修訂歷史。

表 1. 修訂歷史

修訂版	日期	說明
A00_5.2.0	2020 年 10 月	OpenManage Integration for VMware vCenter 5.2 安全性組態指南初始版本。
A00_5.3.0	2021 年 3 月	已在驗證與資料安全性主題中新增 RESTful 應用程式發展介面相關資訊。

相關說明文件

您可以在 **https://www.dell.com/support** 取得 OMIVV 的完整文件集。按一下**瀏覽所有產品**，然後按一下**軟體** > **虛擬化解決方案**。按一下 **OpenManage Integration for VMware vCenter** 以存取下列文件：

- *OpenManage Integration for VMware vCenter 5.3 版使用者指南*
- *OpenManage Integration for VMware vCenter 5.3 版版本資訊*
- *OpenManage Integration for VMware vCenter 5.3 版相容性比較表*
- *OpenManage Integration for VMware vCenter 5.3 版應用程式發展介面指南*
- *OpenManage Integration for VMware vCenter 5.3 版安裝指南*

您可在 https://www.dell.com/support 上尋找包含白皮書在內的技術成品。

2

本文件使用的詞彙

表 2. 本文件使用的詞彙

術語	說明
OMIVV	OpenManage Integration for VMware vCenter
OVF	開放虛擬化格式
HTTP	超文字傳輸通訊協定
HTTPS	超文字安全傳輸通訊協定
NFS	網路檔案系統
CIFS	一般網際網路檔案系統
OM MP	OpenManage Management pack for vRealize Operations
CMC	Chassis Management Controller (M1000e、FX、VRTX)
OME-M	OpenManage Modular Edition (MX7000)
iDRAC	Integrated Dell Remote Access Controller
SNMP	Simple Network Management Protocol
VM	虛擬機器
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
PEM	隱私權強化郵件
RPM	Red Hat Package Manager
作業系統	作業系統

3

部署模型

在 VMware vCenter 環境中，您可以將 OpenManage Integration for VMware vCenter (OMIVV) 部署為 OVF。

主題：

開放虛擬化格式 (OVF) 部署

如果您擁有 VMware vSphere 虛擬機器環境，建議您以開放虛擬化格式 (OVF) 部署 OMIVV。

OVF 部署模型包含一個預先設定的套裝，包含 OMIVV 軟體和執行 OMIVV 軟體的 Linux 作業系統。

OVF 環境也包括預先設定的防火牆，針對 OMIVV 通訊需求與受監視系統所調整。

OVF 使用 OVF 範本檔案部署。如需更多有關將 OMIVV 部署為 OVF 的資訊，請參閱 **https://www.dell.com/support** 上的 *OpenManage Integration for VMware vCenter 5.3 安裝指南*。

安全性設定檔

OMIVV 具有預設的安全性設定檔，以提供安全的 HTTP 存取。強烈建議您取代經過認證機構 (CA) 簽署的認證，以獲得更強固的安全性。

4

產品與子系統安全性

主題：

安全性控制對應

OMIVV 會使用 iDRAC 執行 PowerEdge 伺服器的部署、清查和更新，並從 iDRAC 接收 SNMP 設陷。

OMIVV 的使用者介面為「裝置系統管理」網頁。OMIVV 附掛程式 UI 從 VMware vCenter 用戶端運作，並提供主機硬體監控和管理功能。

所有系統認證都儲存在 OMIVV 安全儲存裝置中。

下圖顯示 OMIVV 的安全性控制對應：

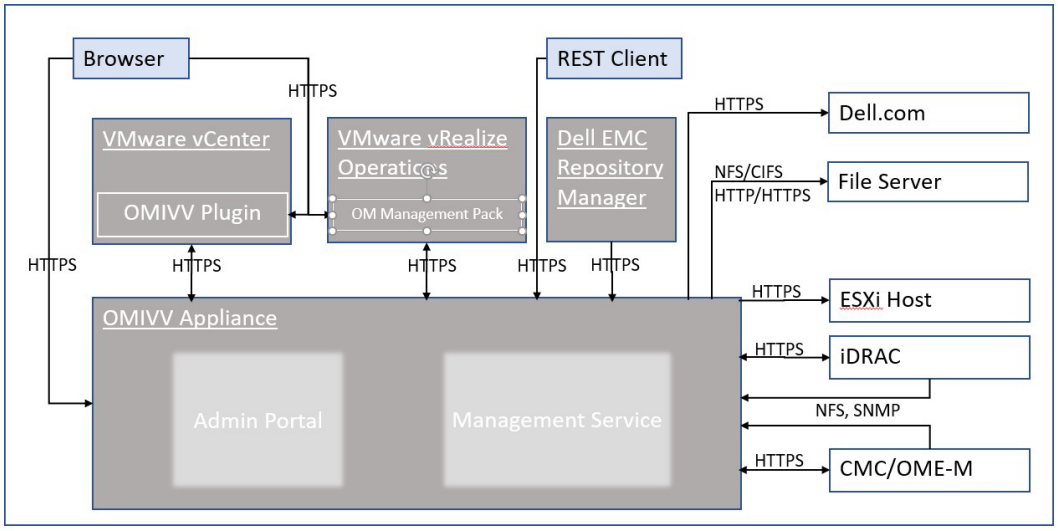

圖 1. 安全性控制對應

認證

存取控制

存取控制設定可針對未經授權的存取提供資源保護。VMware vCenter 使用者透過在 VMware vCenter 中設定的適當角色和許可權存取 OMIVV 附掛程式頁面。會為 OMIVV 裝置的系統管理員帳戶提供 OMIVV 管理主控台和 RESTful 應用程式發展介面的存取許可權。

預設使用者帳戶

OMIVV 包含下列預設使用者帳戶：

- 本機使用者帳戶
- 唯讀使用者帳戶
- Root 帳戶

本機使用者帳戶

OMIVV 提供單一的預設本機系統管理使用者帳戶。此內部帳戶的使用者名稱為 admin。

本機系統管理員僅可存取 Dell EMC OMIVV 管理主控台內的所有作業。

第一次部署 OMIVV 時，系統會提示您設定密碼。請按照螢幕上的指示設定密碼。

唯讀使用者帳戶

OMIVV 提供單一的預設本機唯讀使用者帳戶。唯讀帳戶的使用者名稱是 readonly。

系統管理員僅能使用 VM 遠端主控台登入 OMIVV。

此帳戶可在故障診斷期間使用，以檢視重要的裝置狀態和記錄。

第一次部署 OMIVV 時，系統會提示您設定密碼。請按照螢幕上的指示設定密碼。

root 帳戶

OMIVV 應用裝置擁有作業系統的 root 帳戶。

您無法存取此預設帳戶。技術支援小組會使用 root 帳戶為欄位問題除錯。

外部使用者帳戶

當使用者擁有適當的 vCenter 角色和許可權時，VMware vCenter 使用者可以從 vCenter HTML5 用戶端存取 OMIVV 附掛程式使用者介面元素。如需角色和權限的詳細資訊，請參閱 非管理員使用者必須具備的權限 第頁的 13。

登入安全性設定

失敗的登入行為

OMIVV 包含安全性設定，適用於多次未成功的驗證。

本機使用者帳戶鎖定

在連續 6 次嘗試登入本機使用者帳戶失敗後，OMIVV 會暫時將使用者鎖定一分鐘。

自動工作階段逾時

閒置瀏覽器工作階段逾時

根據預設，若持續 15 分鐘無活動狀態，OMIVV 工作階段便會逾時，並自動將您登出。

認證類型與安裝考量

vCenter 使用者認證

OMIVV 根據 vCenter 認證以存取附掛程式頁面，並取決於處理 vCenter 作業的 RESTful 應用程式發展介面 。附掛程式頁面和處理 vCenter 作業的 RESTful 應用程式發展介面需要 Dell EMC 註冊時在 vCenter 建立的權限。

註冊新的 vCenter 伺服器

事前準備作業

您的 vCenter 帳戶應具有建立使用者的必要權限。如需必要權限的詳細資訊，請參閱非管理員使用者必須具備的權限 第頁的 13。

關於此工作

您可以在安裝 OMIVV 後，註冊 OMIVV 裝置。OMIVV 使用系統管理員使用者帳戶，或具有 vCenter 操作權限的非系統管理員使用者帳戶。單一 OMIVV 裝置例項可支援 15 個 vCenter 伺服器 (不論有無連結模式) 和最多 2,000 個 ESXi 主機。

如果您嘗試註冊超過 15 vCenter，則會顯示下列錯誤訊息：

您的授權只允許 <x> 個 vCenter，且全都已經註冊。

若要註冊新 vCenter 伺服器，請進行下列步驟：

步驟

1. 前往 https://<裝置 IP 或主機名稱>。
2. 在 **VCENTER 註冊**頁面的右窗格中，按一下**註冊新的 vCenter 伺服器**。
   隨即會顯示**註冊新的 vCENTER** 頁面。
3. 請在**註冊新的 VCENTER** 對話方塊的 **vCenter 名稱**底下，執行下列工作：
   a. 在 **vCenter 伺服器 IP 或主機名稱**方塊中，輸入 vCenter IP 位址或主機的 FQDN。
      Dell EMC 建議您使用完整網域名稱 (FQDN)，向 VMware vCenter 註冊 OMIVV。無論是何種註冊，vCenter 的主機名稱必須由 DNS 伺服器正確解析。以下是使用 DNS 伺服器的建議做法：
      - 當您部署具有有效 DNS 註冊的 OMIVV 裝置時，請指派一個靜態 IP 位址和主機名稱。靜態 IP 位址可以確保在系統重新啟動時，OMIVV 裝置的 IP 位址維持不變。
      - 確認 OMIVV 主機名稱資訊出現在 DNS 伺服器的正向與反向對應區域中。
   b. 在**說明**方塊中輸入說明 (選填)。
4. 在 **vCenter 使用者帳戶**底下，執行下列步驟：
   a. 在 **vCenter 使用者名稱**方塊中，輸入系統管理員的使用者名稱或具有必要權限之非系統管理員的使用者名稱。
   b. 在**密碼**方塊中，輸入密碼。
   c. 在**確認密碼**方塊中，再次輸入密碼。
   d. 選取**註冊 vSphere Lifecycle Manager** 核取方塊。
      選取**註冊 vSphere Lifecycle Manager** 核取方塊可讓您使用 vCenter 7.0 及更新版本的 vSphere Lifecycle Manager 功能。
5. 按一下**註冊**。
   如果 vCenter 註冊失敗，則會顯示下列錯誤訊息：
   由於認證錯誤，無法聯絡指定的 vCenter 伺服器 <x>。請檢查使用者名稱和密碼。

結果

註冊 vCenter 伺服器之後，OMIVV 已註冊為 vCenter 附掛程式，「Dell EMC OpenManage Integration」圖示會顯示在 vSphere 用戶端中，您可以從其中存取 OMIVV 功能。

註: 針對 OMIVV 裝置的所有 vCenter 作業，OMIVV 會使用註冊使用者的權限，而非登入 VMware vCenter 的使用者或 OMIVV 裝置本機帳戶的權限。例如：使用者 X 具有必要權限並向 vCenter 註冊 OMIVV；使用者 Y 僅具有 Dell 權限。現在，使用者 Y 可以登入 vCenter 並可從 OMIVV 觸發韌體更新工作。執行韌體更新工作時，OMIVV 使用使用者 X 的權限，讓主機進入維護模式或重新啟動主機。

註: 如果要將自訂的認證機構 (CA) 簽署的認證上傳至 OMIVV，請務必先上傳新認證，再進行 vCenter 註冊。如果進行 vCenter 註冊後才上傳新的自訂憑證，vSphere 用戶端就會顯示通訊錯誤。若要修正此問題，請登出後再登入 vCenter。如果問題仍然存在，請在 vCenter 伺服器上重新啟動 vSphere 用戶端服務。

使用非系統管理帳戶註冊 vCenter 伺服器

事前準備作業

您可以使用 vCenter 系統管理員認證或具有 Dell 權限的非系統管理員使用者身分，為 OMIVV 應用裝置註冊 vCenter Server。

關於此工作

若要讓具有必要權限的非管理員使用者登錄 vCenter 伺服器，請執行以下步驟：

步驟

1. 建立一個角色或修改現有角色使該角色具備所需權限。
   若要進一步了解角色所需的權限清單，請參閱非管理員使用者必須具備的權限。
   關於在 vSphere 用戶端 (HTML-5) 中建立或修改角色並選取權限的步驟，請參閱 VMware vSphere 說明文件
2. 在定義角色並選取角色的權限之後，將使用者指派給新建立的角色。
   如需關於指派角色權限的詳細資訊，請參閱 VMware vSphere 說明文件。
   具有必要權限的 vCenter Server 非系統管理員使用者，現在已可註冊及/或取消註冊 vCenter、修改認證或更新憑證。
3. 以具必要權限的非系統管理員使用者身分，註冊 vCenter 伺服器。
4. 註冊完成之後，請將 Dell 權限指派給在步驟 1 中建立或修改的角色。請參閱將 Dell 權限指派給現有角色 第頁的 14。

結果

具有必要權限的非管理員使用者，現在已可使用 Dell EMC 主機享有 OMIVV 功能。

非管理員使用者必須具備的權限

非系統管理員使用者若要以 vCenter 註冊 OMIVV，必須具備以下權限：

非系統管理員使用者以 OMIVV 註冊 vCenter Server 時，如果沒有指派以下權限，便會顯示訊息：

- 警示
  - 建立警示
  - 修改警示
  - 移除警示
- 擴充
  - 登錄擴充
  - 解除登錄擴充
  - 更新擴充外
- 通用
  - 取消工作
  - 記錄事件
  - 設定
- 健全狀況更新提供者
  - 登錄
  - 取消登錄

    - 更新
- 主機
    - CIM
        - CIM 互動
- Host.Config
    - 進階設定
    - 變更設定
    - 連線
    - 維護
    - 網路組態
    - 查詢修補程式
    - 安全性設定檔和防火牆
- 清查
    - 新增主機至叢集
    - 新增獨立主機
    - 修改叢集
- Lifecycle Manager：一般權限
    - 讀取

    註: vSphere Lifecycle Manager 一般權限僅適用於 vCenter 7.0 及更新版本。
- 主機設定檔
    - 編輯
    - 檢視
- 權限
    - 修改權限
    - 修改角色
- 工作階段
    - 驗證工作階段
- 工作
    - 建立
    - 更新

註: 如果 vCenter 伺服器是用非系統管理員使用者的身份進行註冊以存取任何 OMIVV 功能，則非系統管理員使用者必須具備 Dell 權限。如需指派 Dell 權限的詳細資訊，請參閱將 Dell 權限指派給現有角色 第頁的 14。

將 Dell 權限指派給現有角色

關於此工作

如果 Dell 權限未指派給登入的使用者且該使用者存取 OMIVV 的特定頁面，將會顯示 2000000 錯誤。

您可編輯現有的角色，以指定 Dell 權限。

步驟

1. 使用具有管理權限的身分登入 vSphere 用戶端 (HTML-5)。
2. 在 vSphere 用戶端 (HTML-5) 中展開**功能表**，然後按一下**管理 → 角色**。
3. 從**角色提供者**下拉式清單中選取 vCenter 伺服器。
4. 從**角色**清單中選取 **Dell 操作**，然後按一下**權限**。
5. 若要指派 Dell 的權限，請按一下編輯圖示 [ ]。
   編輯角色頁面會隨即顯示。
6. 在左窗格中，按一下 **Dell**，然後針對所選角色選取下列 Dell 權限，再按一下**下一步**：
    - Dell.Configuration
    - Dell.Deploy-Provisioning
    - Dell.Inventory
    - Dell.Monitoring
    - Dell.Reporting

如需 vCenter 內可用 OMIVV 角色的詳細資訊，請參閱。

7. 編輯角色名稱，如有需要，另針對所選的角色輸入說明。
8. 按一下**完成**。
   登出後再登入 vCenter。具必要權限的使用者現已可執行 OMIVV 作業。

vCenter 使用者安全性

安全性角色與權限

OpenManage Integration for VMware vCenter 會以加密格式儲存使用者認證。為了防止任何不當的要求，它不會提供任何密碼給用戶端應用程式。備份資料庫是使用自訂安全性短語完全加密，因此資料不會遭到濫用。

根據預設，「系統管理員」群組中的使用者具備所有權限。系統管理員可以使用 VMware vSphere Web 用戶端中 OpenManage Integration for VMware vCenter 的所有功能。如果您希望由一位具備必要權限的使用者來管理產品，請執行下列步驟：

1. 建立一個具備必要權限的角色。
2. 以該使用者註冊 vCenter Server。
3. 同時加入 Dell 操作角色和 Dell 基礎結構部署角色。

資料完整性

OpenManage Integration for VMware vCenter、管理主控台和 vCenter 之間的通訊，是透過 HTTPS 完成。OpenManage Integration for VMware vCenter 會產生 vCenter 與應用裝置之間進行信任通訊用的憑證，還會在通訊與 OpenManage Integration for VMware vCenter 註冊之前，驗證並信任 vCenter Server 的憑證。

安全管理主控台工作階段會在閒置 15 分鐘後逾時，而且工作階段只在目前瀏覽器視窗及/或標籤中才有效。如果您嘗試在新視窗或標籤中開啟工作階段，系統就會提示安全性錯誤，要求有效的工作階段。這個動作也可以防止使用者按到任何惡意的 URL，而攻擊管理主控台工作階段。

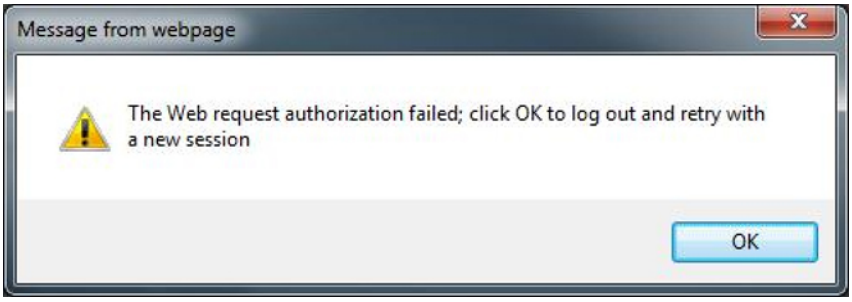

圖 2. 安全性錯誤訊息

存取控制驗證、授權與角色

為了執行 vCenter 作業，OpenManage Integration for VMware vCenter 使用了 vSphere 用戶端的目前使用者工作階段，以及針對 OpenManage Integration 儲存的系統管理認證。OpenManage Integration for VMware vCenter 使用 vCenter Server 的內建角色與權限模型，授權在 OpenManage Integration 和 vCenter 受管物件 (主機與叢集) 執行使用者動作。

Dell 操作角色

此角色包含完成裝置和 vCenter 伺服器工作 (包括韌體更新、硬體清查、重新啟動主機、將主機設為維護模式，或是建立 vCenter 伺服器工作) 的權限/群組。

這個角色包含下列權限群組：

表 3. 權限群組

表 3. 權限群組

組群名稱	說明
權限群組 — Dell.Configuration	執行主機相關工作、執行 vCenter 相關工作、設定 SelLog、設定 ConnectionProfile、設定 ClearLed、韌體更新
權限群組 — Dell.Inventory	設定清查、設定保固擷取、設定唯讀
權限群組 — Dell.Monitoring	設定監視、監視
權限群組 — Dell.Reporting (未使用)	建立報告、執行報告

Dell 基礎結構部署角色

此角色包含與 Hypervisor 部署功能相關的權限。

此角色所提供的權限為「設定主機認證設定檔」、「指定識別」和「部署」。

權限群組 — Dell.Deploy-Provisioning

設定主機認證設定檔、指定識別、部署。

關於權限

OpenManage Integration for VMware vCenter 所執行的每個動作都有相關聯的權限。下列各節將列出可用動作及其關聯權限：

- Dell.Configuration.Perform vCenter-related tasks
  - 結束並進入維護模式
  - 讓 vCenter 使用者群組查詢權限
  - 登錄並設定警報，例如在事件設定頁面啟用/停用警報
  - 將事件/警示發佈到 vCenter
  - 在事件設定頁面上進行事件設定
  - 在事件設定頁面還原預設警示
  - 在進行警示/事件設定時，檢查叢集上的 DRS 狀態
  - 執行更新或任何其他組態動作後，重新啟動主機
  - 監視 vCenter 工作狀態/進度
  - 建立 vCenter 工作，例如韌體更新工作、主機組態工作和清查工作
  - 更新 vCenter 工作狀態/進度
  - 取得主機設定檔
  - 新增主機至資料中心
  - 新增主機至叢集
  - 在主機套用設定檔
  - 取得 CIM 憑證
  - 設定主機以符合相容性
  - 取得相容性工作狀態
- Dell.Inventory.Configure ReadOnly
  - 在設定連線設定檔時，讓所有 vCenter 主機建構 vCenter 樹狀結構
  - 在選取索引標籤時，檢查主機是否為 Dell 伺服器
  - 取得 vCenter 的位址/IP
  - 取得主機 IP/位址
  - 根據 vSphere 用戶端工作階段 ID，取得目前的 vCenter 工作階段
  - 取得 vCenter 清查樹狀目錄，在樹狀結構顯示 vCenter 清查。
- Dell.Monitoring.Monitor
  - 取得主機名稱，以便發佈事件
  - 執行事件記錄作業，例如取得事件計數，或是變更事件記錄設定
  - 登錄、解除登錄及設定事件/警示 — 接收 SNMP 設陷及張貼事件
- Dell.Configuration.Firmware Update
  - 執行韌體更新
  - 在韌體更新精靈頁面載入韌體儲存庫和 DUP 檔案資訊
  - 查詢韌體清查

- 進行韌體儲存庫設定
- 使用暫置功能來設定暫置資料夾及執行更新
- 測試網路與儲存庫連線

- Dell.Deploy-Provisioning.Create Template
  - 設定硬體組態設定檔
  - 設定 Hypervisor 部署設定檔
  - 設定連線設定檔
  - 指定識別
  - 部署
- Dell.Configuration.Perform host-related tasks
  - 閃爍 LED、清除 LED
  - 啟動 iDRAC 主控台
  - 顯示與清除 SEL 記錄
- Dell.Inventory.Configure Inventory
  - 在 Dell 伺服器管理索引標籤顯示系統清查
  - 取得儲存裝置詳細資料
  - 取得電源監視詳細資料
  - 在連線設定檔頁面建立、顯示、編輯、刪除及測試連線設定檔
  - 排程、更新及刪除清查排程
  - 在主機執行清查

使用者與認證管理

預先載入的帳戶

下表說明預先載入的 OMIVV 帳戶：

表 4. 預先載入的帳戶

使用者帳戶	說明
OpenManage Integration for VMware vCenter 系統管理員	OMIVV Web 應用程式管理的預設使用者。
唯讀使用者。	OMIVV 提供單一的預設本機唯讀使用者帳戶。 系統管理員僅能使用 VM 遠端主控台登入 OMIVV。 此帳戶可在故障診斷期間使用，以檢視重要的裝置狀態和記錄。
Linux 作業系統 root	無法存取 root 作業系統帳戶。技術支援小組會使用 root 帳戶為欄位問題除錯。

預設認證

下表說明預先載入 OMIVV 帳戶的預設認證。

表 5. 預設認證

帳戶	使用者	密碼
OpenManage Integration for VMware vCenter 系統管理員	管理員	在部署完成後的初次開機時設定。如需變更系統管理員密碼的詳細資訊，請參閱 變更 OMIVV 裝置密碼 第頁的 18。
唯讀使用者	唯讀	在部署完成後的初次開機時設定。您可以在以唯讀使用者的身分登入後，使用標準 Linux 密碼變更命令來變更唯讀使用者密碼。

表 5. 預設認證

帳戶	使用者	密碼
Linux 作業系統 root	Root	作業系統的 root 密碼是在部署 OMIVV 時設定。

管理認證

如果您是第一次登入 Dell EMC 管理主控台，請以系統管理員身分登入 (預設使用者名稱是 admin)。

註: 如果您忘記系統管理員密碼，則其無法從 OMIVV 裝置中還原。

變更 OMIVV 裝置密碼

關於此工作

您可以在 vSphere Client 中使用主控台變更 OMIVV 裝置密碼。

步驟

1. 開啟 OMIVV Web 主控台。
2. 在 **OpenManage Integration for VMware vCenter 虛擬裝置設定**公用程式中，按一下**變更管理員密碼**。
   完成螢幕上的指示以設定密碼。
3. 在**目前密碼**文字方塊中，輸入目前管理員密碼。
4. 在**新密碼**文字方塊中輸入新密碼。
5. 在**確認新密碼**文字方塊中再次輸入新密碼。
6. 按一下**變更系統管理員密碼**。

認證

OMIVV 裝置支援單一系統管理員使用者。

登入 OMIVV 後，系統管理員只能存取 OMIVV 裝置的組態功能，例如：

- 註冊新的 vCenter 伺服器
- 設定裝置
- 使用 RPM 及備份和還原來升級 OMIVV 裝置
- 設定網路時間通訊協定伺服器
- 設定部署模式
- 產生憑證簽章要求 (CSR)
- 上傳 HTTPS 憑證
- 設定全域警示
- 產生並下載故障診斷套裝

網路安全性

OMIVV 裝置使用預先設定的防火牆，將輸入和連出的網路流量限制至 TCP 和 UDP 埠，以提高安全性。本區段中的表格列出 OMIVV 使用的輸入和連出連接埠。

網路暴露

在與遠端系統通訊時，OpenManage Integration for VMware vCenter 會使用輸入與連出連接埠。

連出連接埠

連線至遠端系統時，OMIVV 可使用連出連接埠。

下表列出的連接埠為 OMIVV 連出連接埠。

表 6. 連出連接埠

連接埠號碼	第 4 層通訊協定	服務
7	TCP, UDP	ECHO
22	TCP	SSH
25	TCP	SMTP
53	UDP, TCP	DNS
67.68	TCP	DHCP
80	TCP	HTTP
88	TCP, UDP	Kerberos
111	TCP, UDP	ONC RPC
123	TCP, UDP	NTP
161-163	TCP, UDP	SNMP
389	TCP, UDP	LDAP
443	TCP	HTTPS
448	TCP	Data Protection Search 系統管理員 REST 應用程式發展介面
464	TCP, UDP	Kerberos
514	TCP, UDP	rsh
587	TCP	SMTP
636	TCP, UDP	LDAPS
902	TCP	VMware ESXi
2049	TCP, UDP	NFS
2052	TCP, UDP	mountd, clearvisn
3009	TCP	Data Domain REST 應用程式發展介面
5672	TCP	RabbitMQ over amqp
8443	TCP	MCSDK 8443 是 443 的替代方案
9002	TCP	Data Protection Advisor REST 應用程式發展介面
9443	TCP	Avamar 管理主控台 Web 服務

輸入連接埠

連線至 OMIVV 時，遠端系統可使用的輸入連接埠。

下表列出的連接埠為 OMIVV 輸入連接埠。

表 7. 輸入連接埠

連接埠號碼	第 4 層通訊協定	服務
22	TCP	SSH

表 7. 輸入連接埠

連接埠號碼	第 4 層通訊協定	服務
80	TCP	HTTP
443	TCP	HTTPS
5671	TCP	RabbitMQ over amqp

資料安全性

OMIVV 所維護的資料會儲存在裝置的內部資料庫中，並受到安全保護，無法從外部存取。

透過 OMIVV 傳輸的資料會受到安全通訊通道保護。

註: 建議 RESTful 應用程式發展介面使用者按照您的環境限制安全地儲存認證和擷取的資料。

密碼編譯

OMIVV 為下列元件使用密碼編譯：

- 存取控制
- 認證
- 數位簽章

管理認證

OMIVV 使用認證進行安全 HTTP 存取 (HTTPS)。

根據預設，OMIVV 會為 HTTPS 安全交易安裝並使用自我簽署認證。

為獲得更強固的安全性，建議使用經過認證機構 (CA) 簽署或自訂的認證。

自我簽署認證足以在網頁瀏覽器和伺服器之間建立加密通道。自我簽署認證無法用於認證。

您可以使用下列類型的認證進行 OMIVV 認證：

- 自我簽署認證

  當裝置的主機名稱變更時，OMIVV 便會產生自我簽署認證。
- 由受信任的認證機構 (CA) 廠商簽署的認證。

註: 建立認證時，請考慮公司政策。

更新已註冊之 vCenter 伺服器的憑證

關於此工作

OpenManage Integration for VMware vCenter 透過具備 2048 位元金鑰長度的 RSA 加密標準，使用 OpenSSL 應用程式發展介面建立憑證簽章要求 (CSR)。

如果 vCenter 伺服器上的憑證已變更，請使用下列工作匯入 OMIVV 的新憑證：

步驟

1. 前往 https://<裝置 IP 或主機名稱>。
2. 在左窗格中，按一下 **VCENTER 註冊**。
   已註冊的 vCenter 伺服器會顯示在工作窗格中。
3. 若要更新 vCenter 伺服器 IP 的憑證或主機名稱，請按一下**更新**。

產生憑證簽章要求 (CSR)

事前準備作業

依預設，OMIVV 具有自我簽署憑證。如果您需要 OMIVV 的自訂認證機構 (CA) 簽署的憑證，建議您在 vCenter 註冊之前上傳新憑證。

關於此工作

產生新的 CSR 時，那些使用先前產生的 CSR 而建立的憑證就無法上傳到裝置。若要產生 CSR，請執行下列步驟：

步驟

1. 在**裝置管理**頁面上，按一下 **HTTPS 憑證**區域中的**產生憑證簽署要求**。
   隨後便會顯示一則訊息，表明如果產生新要求，則使用先前 CSR 所建立的憑證就無法再上傳到該裝置。若要繼續此要求，按一下**繼續**。
2. 如果您繼續此要求，請在**產生憑證簽署要求**對話方塊中，輸入一般名稱、組織名稱、位置、州名、國家/地區、電子郵件和主旨替代名稱 (SAN)，然後按一下**繼續**。

   註: OMIVV 不支援 SAN 的多個值。

3. 按一下**下載**，然後將產生的 CSR 儲存至可存取的位置。

上傳 HTTPS 憑證

事前準備作業

請確定憑證使用 PEM 格式。

關於此工作

您可以使用 HTTPS 憑證，在 OMIVV 裝置與主機系統或 vCenter 之間進行安全通訊。如要設定這種類型的安全通訊，請傳送 CSR 憑證至簽章授權單位，然後使用管理主控台上傳所產生的 CSR。另外還有自動簽署的預設憑證可供安全通訊使用，每次安裝都會有一個這樣的專屬憑證。

步驟

1. 在**裝置管理**頁面上，按一下 **HTTPS 憑證**區域中的**上傳憑證**。
2. 按一下**上傳憑證**對話方塊中的**確定**。
3. 若要上傳憑證，先按一下**瀏覽**，然後按一下**上傳**。
   若要檢查狀態，請前往已註冊 vCenter 的 vSphere 用戶端的**事件主控台**。

結果

上傳憑證時，OMIVV 管理主控台會長達 3 分鐘無回應。在上傳 HTTP 憑證工作完成後，請關閉瀏覽器工作階段，並在新的瀏覽器工作階段中存取系統管理員入口網站。

還原預設的 HTTPS 憑證

步驟

1. 在**裝置管理**頁面上，按一下 **HTTPS 憑證**區域中的**還原預設憑證**。
2. 在**還原預設憑證**對話方塊中，按一下**套用**。

結果

還原憑證時，OMIVV 管理主控台會長達 3 分鐘無回應。在還原預設的 HTTP 憑證工作完成後，請關閉瀏覽器工作階段，並在新的瀏覽器工作階段中存取系統管理員入口網站。

稽核和紀錄

系統管理員使用者可以使用 OMIVV 系統管理主控台，針對所有相關記錄檔產生故障診斷套裝。

如需更多資訊，請參閱建立並下載故障診斷套裝 第頁的 22。

唯讀帳戶可讓使用者讀取裝置在執行階段的各種參數，協助對應用裝置進行故障診斷。如需進階的故障診斷，技術支援可提供針對特定參數的檢查指南。

註: 只有 OMIVV 系統管理員使用者可以在裝置上執行寫入作業。OMIVV 記錄中無法使用使用者稽核。如需瞭解從 vCenter 附掛程式執行之 vCenter 作業的詳細資訊，請參閱 vCenter 稽核記錄。若為 RESTful 應用程式發展介面，用戶端必須能夠處理稽核記錄。

建立並下載故障診斷套裝

關於此工作

故障診斷套裝包含 OMIVV 裝置記錄資訊，此資訊可以用來協助解決問題或將問題傳送到技術支援部門。OMIVV 不會記錄任何的使用者敏感性資料。

步驟

1. 在**支援**頁面上，按一下**建立並下載故障診斷套裝**。
   隨即會顯示**故障診斷套裝**對話方塊。
2. 在**故障診斷套裝**對話方塊中，按一下**建立**。
   視記錄檔的大小而定，建立套裝可能需要一些時間。
3. 若要儲存檔案，按一下**下載**。
   Dell EMC OMIVV 管理主控台登入頁面隨即顯示。
4. 登入 Dell EMC OMIVV 管理主控台。
5. 下載故障診斷套裝。如需更多資訊，請參閱產生並下載故障診斷套裝 第頁的 22。

產生並下載故障診斷套裝

事前準備作業

若要產生故障診斷套裝，請確定您已登入系統管理入口網站。

關於此工作

故障診斷套裝包含 OMIVV 的記錄資訊，此資訊可以用來協助解決問題或將問題傳送到技術支援部門。

步驟

1. 在**裝置管理**頁面上，按一下**產生故障診斷套裝**。
2. 按一下**下載故障診斷套裝**。

檢修性

支援網站 **https://www.dell.com/support** 可讓您存取授權資訊、產品說明文件、諮詢、下載及故障診斷資訊。此資訊可協助您在聯絡支援小組，先解決產品問題。

OMIVV 服務人員不需要特殊登入。如果故障診斷套裝不足，人員可啟用 root 使用者，以收集更多資訊。

請確定您已安裝可用的安全性修補程式和其他更新，包括 OMIVV vCenter 作業系統更新。

安全性修補程式

定期 OMIVV 更新包含安全性更新，以及根據需要的必要安全性更新。

更新會逕行累積，並發佈在「支援」上，OMIVV 使用者會在 vCenter 收到相同的通知。

OMIVV 作業系統更新

我們會定期為 OMIVV 作業系統發佈安全性修補程式和修正程式。

這些修正程式必須透過 RPM 更新套件，安裝在 OMIVV 的現有 OVF 部署上。當可用時，強烈建議您透過 RPM 更新，在 OMIVV 伺服器上安裝這些安全性修補程式和修正程式。

產品代碼完整性

OMIVV 軟體安裝程式已由 Dell 簽署。建議您確認 OMIVV 安裝程式簽名的真實性。

5

其他組態與管理

主題：

OpenManage Integration for VMware vCenter (OMIVV) 授權

OMIVV 的授權有以下兩種類型：

- 評估授權 — OMIVV 應用裝置第一次開機時，評估授權會自動安裝。試用版內含由 OMIVV 所管理之五部主機 (伺服器) 的評估授權。這個 90 天試用版是隨貨附送的預設授權。
- 標準授權—您可以購買由 OMIVV 管理的任何數量的主機授權。授權包含產品支援與 OMIVV 裝置更新。標準授權適用於三年或五年的期間。購買的任何額外授權都會延長現有授權的期間。標準授權會覆寫評估授權。

單一 XML 金鑰的授權持續時間是以原始訂單的銷售日期為基礎。一旦 90 天的寬限期結束，就任何之前即將到期的授權所上傳的任何新授權，均按此計數反映。

OMIVV 最多可支援 15 個 vCenter 例項。當您將評估授權升級為完整標準授權後，會收到一封關於訂單確認的電子郵件，之後即可從 Dell Digital Locker 下載授權檔案。請將 .XML 授權檔案儲存到本機系統，然後使用**管理主控台**上傳新的授權檔案。

購買授權時，請造訪 https://www.dell.com/support，透過 Dell Digital Locker 下載 .XML 檔案 (授權金鑰)。如果您無法下載授權金鑰，請前往**聯絡訂單支援部門**頁面，網址：https://www.dell.com/support，以尋找您產品適用的當地 Dell 支援服務電話號碼，然後與 Dell 支援部門聯絡。

授權會在 OMIVV 管理主控台中提供下列資訊：

- vCenter 連線授權數上限—最多允許註冊及同時使用 15 個 vCenter 連線。
- 主機連線授權數上限—已購買的主機連線數 (一個 OMIVV 例項支援最多 2000 個主機)。
- 使用中 — 使用中的 vCenter 連線或主機連線授權數目。若為主機連線，此數字代表已清查到的主機 (或伺服器) 數目。
- 可用 — 可供日後使用的 vCenter 連線數目或主機連線授權數目。

當您嘗試在主機認證設定檔新增主機時，如果授權主機的數目超過授權的數目，就無法額外新增主機。OMIVV 不支援管理超過可用主機授權數量的主機。

使用 OMIVV RESTful 應用程式發展介面取得更多有關授權的資訊。如需更多資訊，請參閱 *OpenManage Integration for VMware 應用程式發展介面指南*，網址是：https://www.dell.com/support。

註: 任何使用中授權均可用於 OMIVV 5.x 版本。從先前的 OMIVV 例項備份的授權，或從 Digital Locker 再次下載的授權，可用於目前的 OMIVV 例項。

保護真實性與完整性

為了確保產品的完整性，OMIVV 安裝和更新元件已經過簽署。

為確保通訊的完整性，建議使用經過 CA 簽署的憑證。

在 OMIVV 中管理備份和還原

為了在災害情況下保護 OMIVV，建議您執行 OMIVV 備份。需要時，您可以從這些備份還原 OMIVV。如需備份及還原的詳細資訊，請參閱 **https://www.dell.com/support** 上的 OMIVV 使用者指南。