OpenManage Integration for VMware vCenter 5.2 版

使用者指南

October 2020
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

1

簡介

IT 管理員把 VMware vCenter 用作主要主控台來管理和監控 VMware vSphere ESX/ESXi 主機。OpenManage Integration for VMware vCenter (OMIVV) 可透過精簡在 vSphere 環境中與管理及監控 Dell EMC 伺服器基礎結構相關聯的工作，協助您減少管理資料中心的複雜度。

此版本的新功能

此版本的 OpenManage Integration for VMware vCenter 5.2 提供下列功能：

- OMIVV RESTFul 應用程式發展介面簡介

  如需更多資訊，請參閱 *OpenManage Integration for VMware vCenter 5.2 版應用程式發展介面指南*，網址是：**https://www.dell.com/support/**。
- 支援 vSphere 7.0 U1
- 支援 XE2420 PowerEdge 伺服器
- 支援以 IPv4 範圍為基礎的裸機探索
- 安全性強化
- 已新增 **Dell EMC 機箱**和 **Dell EMC 主機**頁面上的篩選選項以根據健全狀況狀態篩選主機和機箱
- 針對有多項或不同保固的主機，提供保固報告方面的強化功能。

OpenManage Integration for VMware vCenter 功能

以下是 OpenManage Integration for VMware vCenter (OMIVV) 裝置的功能：

表 1. OMIVV 功能

功能	說明
清查	清查功能可提供下列項目： PowerEdge 伺服器詳細資料，例如記憶體 — 數量和類型、NIC、PSU、處理器和 Remote Access Controller (RAC) 伺服器、叢集和資料中心層級的保固資訊 機箱詳細資料，例如機箱管理控制器 (CMC) 或管理模組資訊、機箱電源供應器、KVM 狀態、風扇或散熱詳細資料、保固資訊、交換器、伺服器和儲存裝置詳細資料 支援在多機箱管理 (MCM) 組態中的 MX 機箱關聯性。 MX 機箱 MCM 組態的光纖資訊 MX 機箱的 QuickSync 硬體資訊
監視並傳送警示	監視與警示包含下列功能： 偵測重要硬體故障及執行虛擬化感知的動作。例如移轉工作負載，或讓主機進入維護模式。 提供清查、事件、警報等情報來診斷伺服器和機箱問題。 支援 VMware 主動式 HA 功能。
韌體更新	叢集感知伺服器的韌體更新包括以下各項： 將支援的伺服器更新為最新版的 BIOS 和韌體。

表 1. OMIVV 功能 (續)

功能	說明
	您也可以使用 OMIVV 搭配 vSphere Lifecycle Manager 來執行韌體更新 (適用於 vCenter 7.0 及更新版本)。
叢集的漂移偵測	叢集的韌體相容性 vSAN 叢集的驅動程式相容性 硬體相容性 **註:** 硬體相容性不支援使用機箱認證設定檔管理的主機。
驅動程式更新	vSAN 叢集的驅動程式更新。
部署	部署包括以下各項： 建立和部署系統設定檔。 在不使用 PXE 的情況下，使用 VMware vCenter 在裸機伺服器上遠端部署作業系統。
服務資訊	從 Dell 的保固資料庫擷取 Dell EMC 伺服器及其相關聯機箱的保固資訊，輕鬆進行線上保固升級。
安全性角色與權限	安全性角色與權限包含下列功能： 整合標準 vCenter 驗證、規則和權限。 在 iDRAC9 型伺服器支援 iDRAC 鎖定模式。如需 iDRAC9 型伺服器的清單，請參閱相容性比較表。
支援 OEM 伺服器	支援下列 OMIVV 功能： 清查 監視並傳送警示 韌體更新 部署 服務資訊 安全性角色與權限
MX 機箱韌體更新	提供選項以更新 MX 機箱的管理模組韌體。

註: 從 OMIVV 5.0 版開始，只支援 VMware vSphere 用戶端 (HTML-5)，而不支援 vSphere Web 用戶端 (FLEX)。

2

登入 Dell EMC OMIVV 系統管理主控台

您只要使用下列兩個系統管理入口網站之一，即可管理 OpenManage Integration for VMware vCenter 及其虛擬環境：

- Web 型管理主控台
- 個別伺服器的主控台檢視 (OMIVV 裝置的虛擬機器主控台)

1. 前往 https://<ApplianceIP/hostname/>。

   帳戶鎖定時間為一分鐘。

   帳戶鎖定時，您無法啟動新的工作階段。但是，舊的使用中工作階段仍會保持使用中的狀態。
2. 輸入密碼。

   輸入不正確的密碼會導致登入嘗試失敗。連續六次登入嘗試失敗將會導致帳戶鎖定。六次的登入嘗試失敗包括系統管理主控台或 REST 應用程式發展介面的登入嘗試，或使用不正確的權杖存取 REST 應用程式發展介面。

   帳戶鎖定時間為一分鐘。

   您無法在帳戶鎖定期間建立工作階段，但目前使用中的工作階段仍會保持使用中狀態。

   如果您是第一次登入，系統會提示您接受 EULA。
3. 請在 **Dell EMC 最終使用者授權合約**頁面上閱讀條款與條件，然後選取**我接受授權合約中的條款**核取方塊。

   如需更多有關遙測 EULA 的資訊，請按一下 **DELL EMC 遙測 EULA**。
4. 按一下**接受**。

註冊新的 vCenter 伺服器

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 12。

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：

1. 前往 https://<ApplianceIP/hostname/>。
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 登錄的 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。

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。

具有必要權限的使用者 X 使用 vCenter 註冊 OMIVV，而使用者 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。若要解決這個問題，請先取消註冊，然後向 vCenter 重新註冊裝置。

使用非系統管理帳戶註冊 vCenter 伺服器

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。

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：

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 13。

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 13。

將 Dell 權限指派給現有角色

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。

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，請參閱安全性角色與權限。
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。

更新已註冊之 vCenter 伺服器的憑證

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)。

OMIVV 產生的 CSR 會從受信任的憑證授權單位獲得數位簽署憑證。OMIVV 會使用數位憑證，在 Web 伺服器上啟用 HTTPS 以進行安全通訊。

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：

1. 前往 https://<ApplianceIP/hostname/>。
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**。

修改 vCenter 登入認證

您可以使用系統管理員權限或具有必要權限的非系統管理員使用者，修改 vCenter 登入認證。

如果已在叢集上啟用主動式 HA 功能，您不得變更與其相關聯的使用者。若以不同的 vCenter 使用者修改註冊，則會中斷主動式 HA 功能。如果認證需要修改，請取消註冊舊認證並使用新認證註冊。

1. 前往 https://<ApplianceIP/hostname/>。
2. 在**登入**對話方塊中輸入密碼，然後按一下**登入**。
3. 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。
4. 如已登錄 vCenter，若要開啟**憑證**下的**修改使用者帳戶**視窗，請按一下**修改**。
5. 如果輸入不正確的認證，則會顯示訊息。輸入有效的 vCenter 使用者名稱和密碼，然後重新輸入以確認密碼。
6. 若要變更密碼，請按一下**套用**。若要取消更新，請按一下**取消**。

取消註冊 OpenManage Integration for VMware vCenter

正在執行清查、保固或部署工作時，請務必不要從 vCenter 伺服器取消註冊 OMIVV。

如果您已在群集上啟用主動式 HA，請確定會在群集上停用主動式 HA。若要停用主動式 HA，請選取**設定** > **服務** > **vSphere 可用性**來存取叢集的**主動式 HA 故障與回應**畫面，然後按一下**編輯**。若要停用主動式 HA，請在**主動式 HA 故障與回應**畫面中，清除 **Dell Inc** 提供者旁的核取方塊。

若要移除 OpenManage Integration for VMware vCenter，請使用管理主控台，從 vCenter 伺服器解除登錄 OMIVV。

1. 前往 https://<ApplianceIP/hostname/>。
2. 在 **VCENTER 註冊**頁面上的 **vCenter 伺服器 IP 或主機名稱**表格中，按一下**取消註冊**。

   註: 確定您選取正確的 vCenter，因為 OMIVV 可能與超過一個以上的 vCenter 相關聯。

3. 若要確認所選的 vCenter 伺服器解除登錄，請在**取消註冊 VCENTER** 對話方塊中，按一下**取消註冊**。

   註: 取消註冊 OMIVV 後，先登出 vSphere 用戶端 (HTML-5)，然後再登入。如果仍會看見 OMIVV 圖示，請重新啟動 vSphere 用戶端 (HTML-5) 和 Web 用戶端 (FLEX) 兩者的用戶端服務。

上傳授權至 OMIVV 管理主控台

請確定您的授權可從 Dell Digital Locker 下載，網址：**https://www.dell.com/support**。如果您訂購多個授權，則授權可能會在不同時間分別寄送。您可以在「訂單狀態」中檢查其他授權項目的狀態，網址：**https://www.dell.com/support**。授權檔案為 .XML 格式。

1. 前往 https://<ApplianceIP/hostname/>。
2. 在**登入**對話方塊輸入密碼。
3. 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。
4. 按一下**上傳授權**。

5. 在**上傳授權**對話方塊中，按一下**瀏覽**以移至授權檔案，然後按一下**上傳**。

   註: 如果您修改或編輯授權檔案，授權檔案 (.XML 檔案) 將無法運作。您可以透過 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「聯絡技術支援部門」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。

管理 OMIVV 裝置

OMIVV 裝置管理可讓您管理 OpenManage Integration for VMware vCenter 網路、NTP 和 HTTPS 資訊，而且可讓管理員執行下列工作：

- 重新啟動 OMIVV 裝置。請參閱重新啟動 OMIVV 裝置 第頁的 15。
- 更新 OMIVV 裝置及設定更新儲存庫的位置。請參閱 升級 OMIVV 裝置和儲存庫位置 第頁的 15
- 使用 RPM 升級 OMIVV 裝置。請參閱使用 RPM 升級 OMIVV 裝置 (使用網際網路) 第頁的 16。
- 使用備份和還原來升級 OMIVV 裝置。請參閱使用備份和還原來升級 OMIVV 裝置 第頁的 17。
- 產生並下載故障診斷套裝。請參閱產生並下載故障診斷套裝 第頁的 19。
- 設定 HTTP 代理。請參閱設定 HTTP 代理 第頁的 19。
- 設定網路時間通訊協定伺服器。請參閱設定網路時間通訊協定 (NTP) 伺服器 第頁的 19。
- 設定部署模式。請參閱設定部署模式 第頁的 20。
- 如需瞭解延伸監控，請參閱延伸監控 第頁的 21。
- 產生憑證簽章要求 (CSR)。請參閱產生憑證簽章要求 (CSR) 第頁的 21。
- 上傳 HTTPS 憑證。請參閱上傳 HTTPS 憑證 第頁的 21。
- 設定全域警示。請參閱設定全域警示 第頁的 21。

存取裝置管理

在 OpenManage Integration for VMware vCenter 中，執行下列步驟以利用系統管理入口網站存取**裝置管理**頁面：

1. 前往 https://<ApplianceIP/hostname/>。
2. 在**登入**對話方塊中，輸入密碼。
3. 若要設定裝置管理區段，請在左窗格中按一下**裝置管理**。

重新啟動 OMIVV 裝置

1. 在**裝置管理**頁面上，按一下**虛擬裝置重新開機**。
2. 若要重新啟動 OMIVV 裝置，請在**重新啟動虛擬裝置**對話方塊中，按一下**套用**。

升級 OMIVV 裝置和儲存庫位置

- 為了確保所有資料都能受到保護，在更新 OMIVV 裝置之前，請先執行 OMIVV 資料庫備份。請參閱管理備份和還原 第頁的 18。
- OMIVV 裝置需具有網際網路連線，才能顯示可用的升級機制和執行 RPM 升級。請確認 OMIVV 裝置具有網際網路連線。如果您需要 Proxy 網路，請根據環境網路設定啟用 Proxy 設定，然後輸入 Proxy 資料。請參閱設定 HTTP Proxy。
- 請確認**更新儲存庫路徑**有效。
- 請務必先登出所有 vSphere 用戶端 (HTML-5) 工作階段，再登入已註冊的 vCenter 伺服器。
- 在登入任何已註冊的 vCenter 伺服器之前，請務必在同一個平台服務控制器 (PSC) 下同時更新所有裝置。否則，您可能會在 OMIVV 例項上看到不一致的資訊。

1. 在**裝置管理**頁面的**裝置更新**區段中，確認目前和可用的 OMIVV 版本。

   針對可用的 OMIVV 裝置版本，適用的 RPM 和 OVF OMIVV 裝置升級機制會以勾選標記顯示 [✔]。

   以下是您可能可用的升級機制選項，您可以針對升級機制執行任一工作：

選項	說明
1	如果勾選標記顯示於 RPM，您可以將 RPM 從現有版本升級為最新的可用版本。請參閱使用 RPM 升級 OMIVV 裝置 (使用網際網路) 第頁的 16。

選項	說明
2	如果勾選標記顯示於 OVF，您可以從現有版本備份 OMIVV 資料庫，並在最新的可用裝置版本中將其還原。請參閱使用備份和還原來升級 OMIVV 裝置 第頁的 17。
3	如果勾選標記同時顯示於 RPM 與 OVF，您可以執行上述任一選項來升級您的裝置。在這種情況下，建議選項是 RPM 升級。

2. 若要更新 OMIVV 裝置，請根據 OMIVV 的版本，執行適用的上述升級機制工作。

OMIVV 升級選項

備份及還原

您可以從 OMIVV 5.0 備份及還原至最新版本 (使用 vCenter 6.5 及更新版本)。

RPM 升級

您可以將 RPM 從 OMIVV 5.0 升級至最新版本。

使用 RPM 升級 OMIVV 裝置 (使用網際網路)

請確保您要升級的裝置版本是比目前版本更新的版本。

建議您先製作應用裝置快照，然後再升級 OMIVV 裝置。

1. 在**裝置管理**頁面上，請根據您的網路設定來啟用代理並輸入代理設定資料 (若有需要)。請參閱設定 HTTP 代理。

   針對可用的 OMIVV 裝置版本，適用的 RPM 和 OVF OMIVV 裝置升級機制會以勾選標記顯示 [✔]。

2. 若要將 OMIVV 附掛程式從現有版本升級至可用版本，請執行下列其中一個步驟：
   - 若要使用可在**更新儲存庫路徑**取得的 RPM 進行升級，請確認**更新儲存庫路徑**已設為以下路徑： https://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/

   如果路徑不同，請在**應用裝置管理**視窗的**應用裝置更新**區域中按一下**編輯**，將**更新儲存庫路徑**文字方塊中的路徑更新為 https://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/，然後按一下**套用**。

3. 比較可用的 OMIVV 裝置版本和目前的 OMIVV 裝置版本。
4. 若要套用更新至 OMIVV 裝置，請在**裝置設定**下方，按一下**更新虛擬裝置**。
5. 在**更新裝置**對話方塊中，按一下**更新**。
   按一下**更新**之後，就會登出**管理主控台**視窗。
6. 關閉網頁瀏覽器。

   在升級處理過程中，裝置會重新啟動一次或兩次。該裝置經過 RPM 升級後，請務必先清除瀏覽器快取，再登入 Dell 系統管理入口網站。

   RPM 升級完成之後，您就可以在 OMIVV 主控台檢視登入畫面。開啟瀏覽器，輸入 *https:\\< 裝置 IP|主機名稱>* 連結，並移至**裝置更新**區域。您可以確認可用的和目前的 OMIVV 裝置版本相同。

   RPM 升級後，在已註冊的 Dell 警報和適用於 PHA 叢集的 Dell 健全狀況更新提供者上的所有自訂內容都將還原為預設值。

使用 RPM 升級 OMIVV 裝置 (無網際網路)

建立 HTTP 或 HTTPS 共用。請確認 HTTP 或 HTTPS 共用支援包含 ++ 等特殊字元及空格的檔案名稱。

OMIVV 僅支援 HTTP 和 HTTPS 共用。

OMIVV 支援從 5.1 版升級至 5.2 版，無需網際網路連線。

1. 下載可從 **https://www.dell.com/support** 取得的 RPM .zip 套裝。
2. 解壓縮 RPM .zip 套裝，並從解壓縮位置將檔案和資料夾複製到 HTTP 或 HTTPS 共用。
3. 在**裝置管理**頁面中的**裝置更新**區域中，按一下**編輯**，然後在**更新儲存庫路徑**中輸入共用位置路徑。
4. 按一下**套用**。

5. 比較可用的 OMIVV 裝置版本和目前的 OMIVV 裝置版本。
6. 若要套用更新至 OMIVV 裝置，請在**裝置設定**下方，按一下**更新虛擬裝置**。
7. 在**更新裝置**對話方塊中，按一下**更新**。
   按一下**更新**之後，就會登出 **OMIVV 管理主控台**視窗。

   根據您的網路速度而定，完成更新可能需要大約 40 分鐘的時間。
8. 關閉網頁瀏覽器。
   當裝置升級完成後，請務必先清除瀏覽器快取，再登入 **OMIVV 管理主控台**。

使用備份和還原來升級 OMIVV 裝置

建議您在進行備份之後以及還原備份檔案之前，不要變更或移除由 OMIVV 管理的叢集或主機。如果已變更或移除由 OMIVV 管理的叢集或主機，請在還原後重新設定與這些叢集和主機相關聯的設定檔 (例如：主機認證設定檔、叢集設定檔)。

請勿從 vCenter 取消登錄 OMIVV 附掛程式。從 vCenter 取消註冊附掛程式，會移除由 OMIVV 附掛程式在 vCenter 上進行註冊之主動式 HA 叢集的 Dell 健全狀況更新提供者。

建議您先製作應用裝置快照，然後再升級 OMIVV 裝置。

若要將 OMIVV 裝置從較舊版本更新為目前版本，請執行下列步驟：

1. 備份先前版本的資料。
2. 從 vCenter 關閉舊 OMIVV 裝置。
3. 部署新的 OpenManage Integration 裝置 OVF。
4. 開啟 OpenManage Integration 新裝置的電源。
5. 設定新裝置的網路和時區。

   註: 建議新的 OMIVV 裝置保留舊版 OMIVV 裝置的身分識別 (IP 或 FQDN)。
6. OMIVV 裝置會隨附預設憑證。如果您希望您的裝置有自訂憑證，請以同樣方式更新。請參閱產生憑證簽章要求 (CSR) 第頁的 21和上傳 HTTPS 憑證 第頁的 21。否則，請跳過這個步驟。
7. 將資料庫還原到新的 OMIVV 裝置。請參閱從備份還原 OMIVV 資料庫。
8. 確認應用裝置。如需更多資訊，請參閱 。《安裝指南》中的〈驗證安裝〉主題
9. 升級後，建議您在 OMIVV 附掛程式管理的所有主機上再次執行清查。

   還原裝置後，事件與警報設定則為未啟用。您可以從**設定**標籤再次啟用事件與警報設定。

   如果您從舊版 OMIVV 升級為可用的版本，所有排定的工作都會繼續執行。

   執行備份和還原後，在已註冊的 Dell 警報和適用於 PHA 叢集的 Dell 健全狀況更新提供者上的所有自訂內容都將還原為預設值。

   從舊版的 OMIVV 版本備份和還原到較新的 OMIVV 版本後，如果遇到下列任何一種問題，請執行下列工作：

   - 200000 訊息
   - Dell EMC 標誌遺失
   - OMIVV UI 無回應
   - 未從 vCenter 移除 OMIVV 附掛程式
   - SSL 憑證無效

   解析度：

   - 在 vCenter 伺服器上重新啟動 vSphere 用戶端 (HTML-5) 和 vSphere Web 用戶端 (FLEX) 兩者的 vSphere 用戶端服務。
   - 如果問題仍然存在，請執行下列步驟：
     - 若為 VMware vCenter Server 裝置：請移至 `/etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity`。若為 Windows vCenter，請從 vCenter 裝置前往下列資料夾，檢查是否有與舊版相關聯的老舊資料 — 前往 vCenter 裝置的 `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\vc-packages\vsphere-client-serenity` 資料夾，查看是否有 com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.XXX 等老舊資料。
     - 手動刪除對應於舊版 OMIVV 的資料夾，並重新啟動 vSphere 用戶端 (HTML-5) 和 Web 用戶端 (FLEX) 兩者的 vSphere 用戶端服務。

   如果新裝置的 IP 位址與舊版裝置的 IP 位址不同，請執行下列步驟：

   - 主動式 HA 功能可能無法正常運作。在這種情況下，請為每個擁有 Dell EMC 主機的叢集停用再啟用主動式 HA。

- 設定 SNMP 設陷的陷阱目的地，以指向新裝置。身分識別變更可經由在這些主機上執行清查來修正。在主機上執行清查時，如果 SNMP 設陷不是指向新的 IP，那些主機會列為不相容。若要修正主機相容性問題，請參閱修正不相容的主機 第頁的 61。

管理備份和還原

您可以使用管理主控台來執行備份與還原相關工作。

- 設定備份和還原
- 排程自動備份
- 執行立即備份
- 從備份還原資料庫
- 重設備份和還原設定 第頁的 19

在 OMIVV 中執行下列步驟，使用管理主控台來存取**備份及還原設定**頁面：

1. 前往 `https:\\<裝置 IP|主機名稱>`。
2. 在**登入**對話方塊輸入密碼。
3. 在左窗格中，按一下**備份與還原**。

設定備份和還原

備份和還原功能會將 OMIVV 資料庫備份至遠端位置 (NFS 和 CIFS)，以供稍後還原。設定檔、組態及主機資訊皆存於備份。建議您排程自動備份，以防止資料遺失。

註: NTP 設定不會儲存及還原。

1. 在**備份及還原設定**頁面上，按一下**編輯**。
2. 在醒目提示的**設定與詳細資料**區域上，執行下列步驟：
   a. 在**備份位置**中，輸入備份檔案的路徑。
   b. 在**使用者名稱**中，輸入使用者名稱。
   c. 在**密碼**中輸入密碼。
   d. 在**輸入加密備份用的密碼**中，在方塊內輸入加密密碼。
      加密密碼可包含英數字元和特殊字元，例如「!、@、#、$、% 和 *」。
   e. 在**確認密碼**中，再次輸入加密密碼。
3. 若要儲存這些設定，請按一下**套用**。
4. 設定備份排程。請參閱 排程自動備份。

請在完成此程序後，設定備份排程。

排程自動備份

如需進一步瞭解設定備份位置和認證，請參閱設定備份和還原。

1. 在**備份及還原設定**頁面上，按一下**編輯自動排程備份**。
   相關欄位已啟用。
2. 若要啟用備份，請按一下**啟用**。
3. 請針對您一週哪幾天要執行備份工作，選取**備份天數**核取方塊。
4. 在**備份時間 (24 小時制，小時：分鐘)** 中，以小時：分鐘格式輸入時間。
   下次備份隨即填入下一次排程備份的日期與時間。
5. 按一下**套用**。

執行立即備份

1. 在**備份及還原設定**頁面上，按一下**立即備份**。
2. 若要從備份設定使用位置和加密密碼，請在**立即備份**對話方塊中選取**從備份設定使用位置和加密密碼**核取方塊。
3. 輸入**備份位置**、**使用者名稱**、**密碼**和**加密用的密碼**等值。

加密密碼可包含英數字元和特殊字元，例如「!、@、#、$、% 和 *」。密碼設定不受字元限制。

4. 按一下**備份**。

從備份還原 OMIVV 資料庫

從先前版本還原 OMIVV 之後：

- 不支援 11G 伺服器。還原後僅保留 12G 與較新的伺服器。
- 不支援硬體設定檔與部署範本。建議使用系統設定檔進行部署。
- 已取消在 11G 伺服器上排定的部署工作和/或使用硬體設定檔為基礎的部署範本。
- 已從認證設定檔移除所有 11G 伺服器，並捨棄已耗用的授權。
- 儲存庫設定檔只會使用 64 位元套裝。

  註: 若您執行備份並從 4.x 還原成 5.x，在叢集設定檔名稱旁會顯示警告符號，因為在 5.x 中 OMIVV 不支援 32 位元的韌體套裝。若要使用叢集設定檔的最新變更，請編輯叢集設定檔。
- 已取消在 11G 伺服器上排定的韌體更新工作。

在執行還原操作之前，請確定已設定正確的部署模式。如需設定部署模式的更多資訊，請參閱 設定部署模式 第頁的 20。

1. 在**備份及還原設定**頁面上，按一下**立即還原**。
2. 在**立即還原**對話方塊中，以 CIFS 或 NFS 格式輸入**檔案位置**和備份 .gz 檔案的路徑。
3. 輸入備份檔案的**使用者名稱**、**密碼**和**加密密碼**。
   加密密碼可包含英數字元和特殊字元，例如「!、@、#、$、% 和 *」。
4. 若要儲存變更，請按一下**套用**。
   還原作業會導致 OMIVV 裝置在完成還原後重新啟動。若要驗證安裝，請參閱安裝指南中的驗證安裝主題。

   還原完成後，請先關閉瀏覽器，然後清除瀏覽器快取，再登入系統管理員入口網站。

重設備份和還原設定

使用重設設定功能，您可將設定重設為未設定狀態。

1. 在**備份及還原設定**頁面上，按一下**重設設定**。
2. 在**重設設定**對話方塊中，按一下**套用**。

產生並下載故障診斷套裝

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。

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。

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**。

設定 HTTP 代理

1. 在**裝置管理**頁面上，向下捲動至 **HTTP 代理設定**，然後按一下**編輯**。
2. 選取**啟用**以使用 HTTP 代理設定。
3. 在**代理伺服器位址**中輸入代理伺服器位址。
4. 在**代理伺服器連接埠**中輸入代理伺服器連接埠。
5. 選取**是**以使用代理認證。
6. 如果使用代理認證，請在**使用者名稱**中輸入使用者名稱。
7. 在**密碼**中輸入密碼。
8. 按一下**套用**。

設定網路時間通訊協定 (NTP) 伺服器

您可以使用 NTP 來同步處理 OMIVV 裝置時鐘和 NTP 伺服器時鐘。

1. 在管理主控台的**裝置管理**頁面上，按一下 **NTP 設定**區域中的**編輯**。
2. 選取**啟用**。輸入偏好和次要 NTP 伺服器的主機名稱或 IP 位址，然後按一下**套用**。
3. 配置 NTP 後，啟動終端機主控台，並選取 **透過網路同步處理日期與時間**核取方塊。

註: 可能需要幾分鐘的時間，才可完成 OMIVV 時鐘與 NTP 伺服器同步化。

註: 如果 OMIVV 管理員入口網站花費很長的時間載入資訊，請確定 NTP 設定正確，而且 OMIVV 虛擬機器可連線至 NTP 伺服器。

設定部署模式

如果是上述任何部署模式，請務必使用保留區，保留足夠的記憶體資源給 OMIVV 裝置。有關保留記憶體資源的步驟，請參閱 vSphere 說明文件。

請確定將以下資源指派給具有 OMIVV 的虛擬機器，以滿足所需部署模式的系統需求：

表 2. 部署模式的系統需求

部署模式	主機數量	CPU 數量	記憶體 (GB)	最小儲存空間
小型	最多 250 個	2	8	95 GB
中型	最多 500 個	4	16	95 GB
大型	最多 1000 個	8	32	95 GB
X 大型模式	最多 2,000 個	12	32	95 GB

註: 僅於中型、大型和超大型部署模式上支援 MX 機箱韌體更新功能。

您可以選取適當的部署模式來調整 OMIVV，以符合環境中的節點數。

若要整合 OpenManage Mangement Pack for vRealize Operations (vROPS) 與 OMIVV，所需的部署模式必須至少是**中等**。

1. 在**裝置管理**頁面上，向下捲動至**部署模式**。
   隨即會顯示部署模式的組態值，例如**小型**、**中型**、**大型**和**超大型**。根據預設，模式設定為**小型**。
2. 若要根據環境編輯部署模式，請按一下**編輯**。
3. 在**編輯**模式中，請確定已滿足先決條件，然後選取所需的部署模式。
4. 按一下**套用**。
   已根據設定的部署模式所需的 CPU 和記憶體來確認所配置的 CPU 與記憶體。
   - 如果驗證失敗，會顯示錯誤訊息。
   - 如果驗證成功，OMIVV 裝置會重新啟動，而且部署模式會在您確認變更之後進行變更。
   - 如果已設定所需的部署模式，就會顯示訊息。
5. 如果變更了部署模式，請確認變更，然後重新啟動裝置以更新部署模式。

註: 在 OMIVV 裝置開機期間，會根據設定的部署模式來確認配置的系統資源。如果配置的系統資源少於設定的部署模式，則 OMIVV 裝置無法開機進入登入頁面。若要將 OMIVV 裝置開機，請關閉 OMIVV 裝置、將系統資源更新至現有的設定部署模式，然後開啟 OMIVV 裝置。

降級部署模式

1. 登入管理主控台。
2. 變更部署模式至必要的層級。
3. 關閉 OMIVV 裝置並變更系統資源至必要的層級。
4. 開啟 OMIVV 裝置。

升級部署模式

1. 先清除瀏覽器快取記憶體，再登入 Dell 系統管理員入口網站。
2. 開啟 OMIVV 裝置。

3. 登入管理主控台。
4. 變更部署模式至必要的層級。

延伸監控

確定啟用延伸監控，以支援適用於 vRealize Operations Manager 的 OpenManage 管理套件。建議透過「中型」部署模式來執行延伸監控。

確定啟用 SNMP 設陷監控，以支援適用於 OpenManage Management Pack for vRealize Operations Manager 的 SNMP 警示。這可讓使用者即時監控伺服器或機箱的健全狀況。

1. 前往 https://<ApplianceIP/hostname/>。
2. 在左窗格中，按一下**應用裝置管理**。
3. 在**裝置管理**頁面上，向下捲動至**延伸監控**。
4. 若要編輯延伸監控設定，請按一下**編輯**。
5. 在編輯模式中，啟用或停用延伸監控和 SNMP 設陷監控，然後按一下**套用**。

產生憑證簽章要求 (CSR)

在註冊 OMIVV 至 vCenter 前，請確認您已上傳 CSR。

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：

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. 如果您要繼續此要求，請在**產生憑證簽署要求**對話方塊中，輸入一般名稱、組織、位置、州名、國家/地區和電子郵件等資訊。
   按一下**繼續**。
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

請確定憑證使用 PEM 格式。

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。

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**。

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

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**。

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。

設定全域警示

警示管理可讓您針對如何為所有 vCenter 例項在 OMIVV 儲存警示進行全域設定。

1. 前往 https://<ApplianceIP/hostname/>。

2. 在**登入**對話方塊中，輸入密碼。
3. 在左方窗格中，按一下**警示設定**。若要輸入新的 vCenter 警示設定，請按一下**編輯**。
4. 在下列欄位中輸入數值：
   根據預設，系統會顯示目前警示數量。
   - **警示的數目上限**
   - **警示保留天數**
   - **重複警示的逾時 (秒)**
5. 若要儲存設定，請按一下**套用**。

關於 OMIVV 虛擬機器主控台

OMIVV 虛擬機器主控台可在虛擬機器上的 vSphere Client 內取得。主控台與系統管理主控台的合作關係非常密切。您可以使用主控台執行下列工作：

- 設定網路設定
- 變更 OMIVV 裝置密碼
- 設定 NTP 和設定當地時區
- OMIVV 裝置重新開機
- 將 OMIVV 裝置重設為原廠設定
- 使用唯讀角色登入
- 從主控台登出

開啟 OMIVV 虛擬機器主控台

若要開啟 OMIVV 虛擬機器主控台，請啟動 OMIVV 裝置的 Web 或遠端主控台。

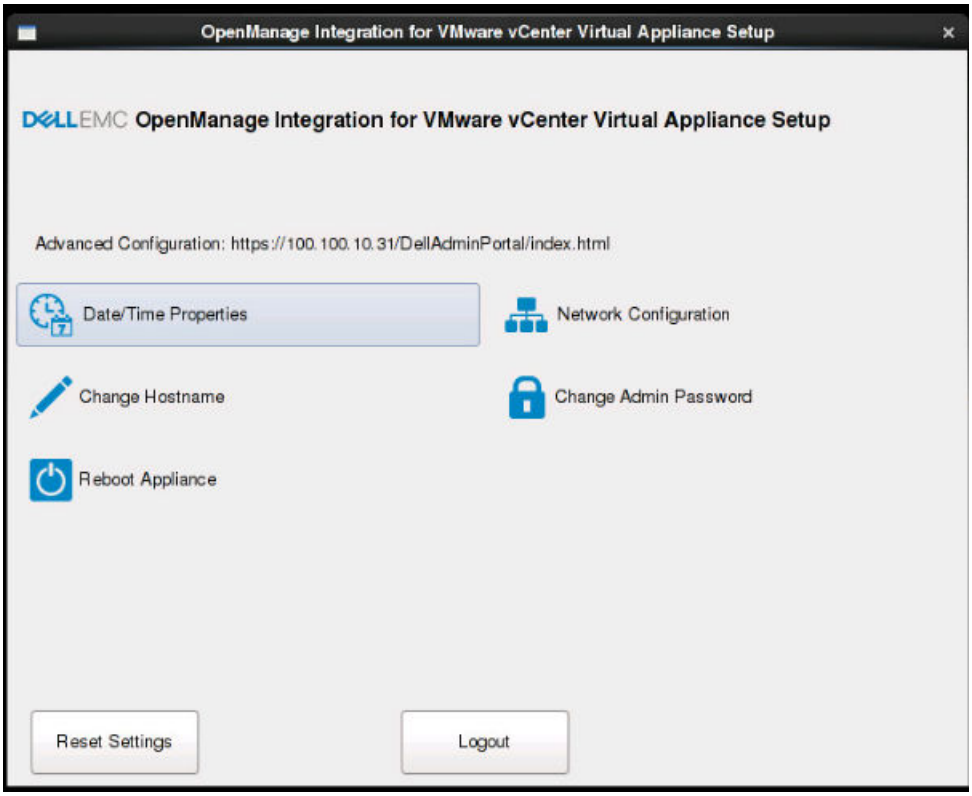
在開啟虛擬機器主控台並輸入認證 (使用者名稱：`admin`，密碼：您在部署裝置時設定的密碼) 之後，即可開始設定主控台。

設定 OMIVV 裝置

1. 開啟虛擬機器的電源。
2. 在右窗格中，按一下**啟動 Web 主控台**。
3. 以系統管理員身分登入 (預設使用者名稱是 `admin`)。
4. 如果您是第一次登入，請按照螢幕上的指示設定密碼 (Admin 和 ReadOnly 使用者)。

   註: 如果您忘記系統管理員密碼，則其無法從 OpenManage Integration for VMware vCenter 裝置中還原。

5. 若要設定 OMIVV 時區資訊，請按一下**日期/時間內容**。



註: 當 OMIVV 裝置無法從網路 (DHCP) 擷取 IP 位址時，0.0.0.0 會顯示為 IP 位址。若要解決此問題，您必須手動設定靜態 IP。

a. 在**日期與時間**索引標籤上，選取**透過網路同步處理日期與時間**核取方塊。**透過網路同步處理日期與時間**核取方塊僅會於成功使用系統管理入口網站設定 NTP 後才會啟用。如需更多有關設定 NTP 的資訊，請參閱設定網路時間通訊協定 (NTP) 伺服器 第頁的 19。

b. 按一下**時區**，選取適用的時區，然後按一下**確定**。

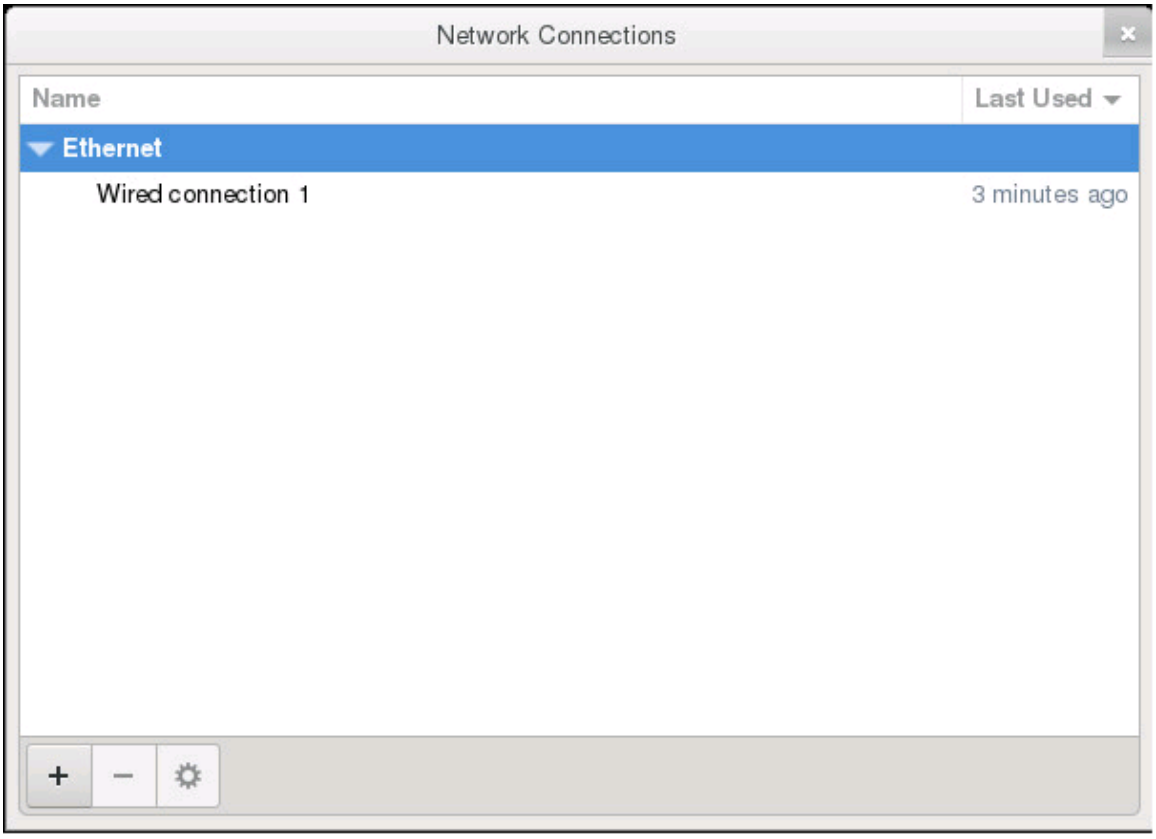
6. 如要設定 OMIVV 裝置的網路，按一下**網路組態**。

   若要在 vSphere 環境中管理 Dell EMC 伺服器，OMIVV 需要 vSphere 網路 (vCenter 和 ESXi 管理網路) 和頻外網路 (iDRAC、CMC 和 OME-Modular) 兩者的存取權。

   如果環境中的 vSphere 網路和頻外網路是獨立的隔離網路，OMIVV 便需要這兩個網路的存取權。在此情況下，OMIVV 裝置必須設定兩張網路配接卡。建議將這兩個網路設定為初始組態的一部分。

   如果您能使用 vSphere 網路存取頻外網路，請勿為 OMIVV 裝置設定兩張網路配接卡。如需設定次要 NIC 方面的更多資訊，請參閱設定有兩個網路介面控制器 (NIC) 的 OMIVV 裝置 第頁的 25。

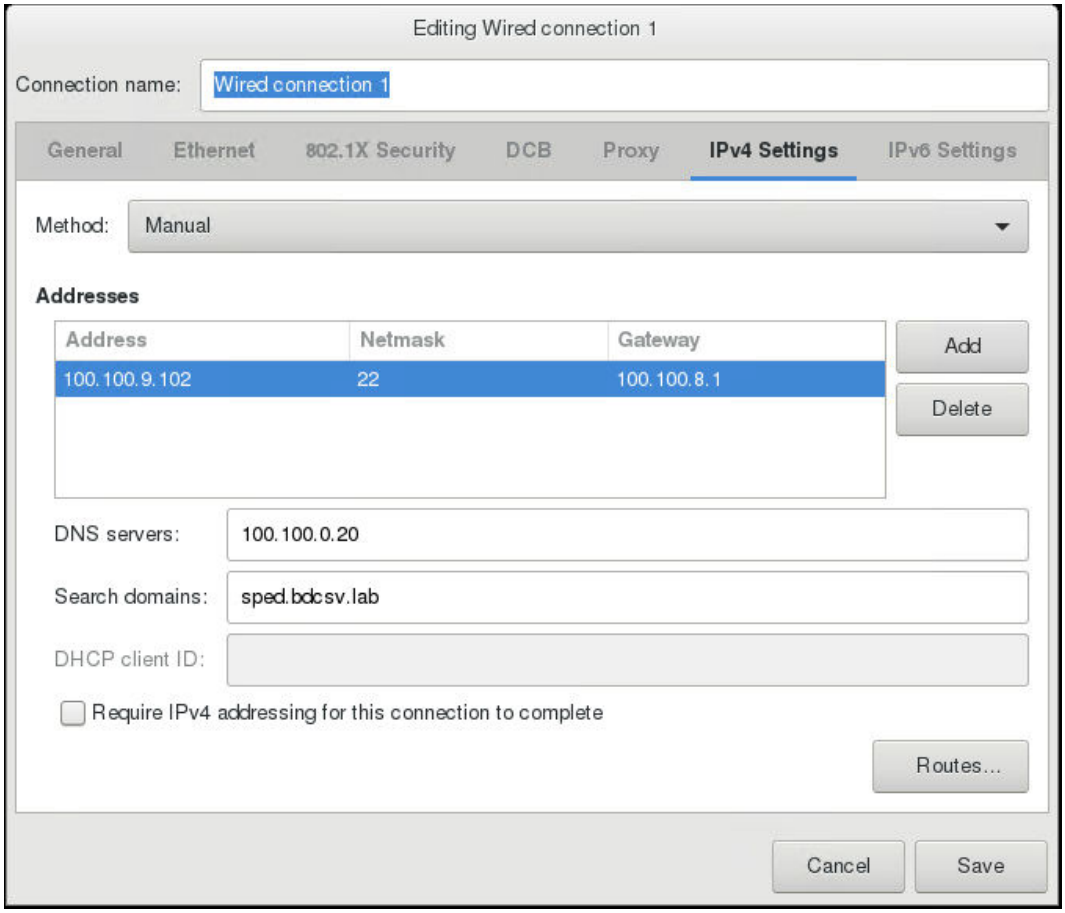
7. 選取**有線連線 1**，然後按一下  。



a. 按一下 **IPv4 設定**標籤，在**方法**下拉式清單中，選取**手動**，再按一下**新增**。

   註: 如果您選取自動 (DHCP)，請勿輸入任何 IP 位址，因為 OMIVV 裝置會在下一次重新開機時，自動收到來自 DHCP 伺服器的 IP。

b. 輸入有效的 IP、網路遮罩 (無類別網域間路由 (CIDR) 格式) 和閘道資訊。
   如果您在**遮罩**方塊中輸入 IP 位址，會自動轉換為對應的 CIDR 格式。
c. 在 **DNS 伺服器**和**搜尋網域**方塊中，分別輸入要個別搜尋的 DNS 伺服器 IP 與網域。
d. 選取**需要 IPv4 定址以完成此連線**核取方塊，然後按一下**儲存**。



註:

在您設定 OMIVV 裝置靜態 IP 後，OMIVV 終端公用程式頁面有時不會立即重新整理及顯示更新後的 IP。若要解決此問題，請退出 OMIVV 終端公用程式，然後再次登入。

8. 若要變更 OMIVV 裝置的主機名稱，請按一下**變更主機名稱**。
   a. 輸入有效的主機名稱，然後按一下**更新主機名稱**。

      註: 如果有任何 vCenter 伺服器已經在 OMIVV 裝置上註冊，請先取消註冊所有的 vCenter 例項，然後再重新註冊。如需更多資訊，請參閱《安裝指南》中的管理取消註冊與重新註冊主題。

9. 重新啟動裝置。

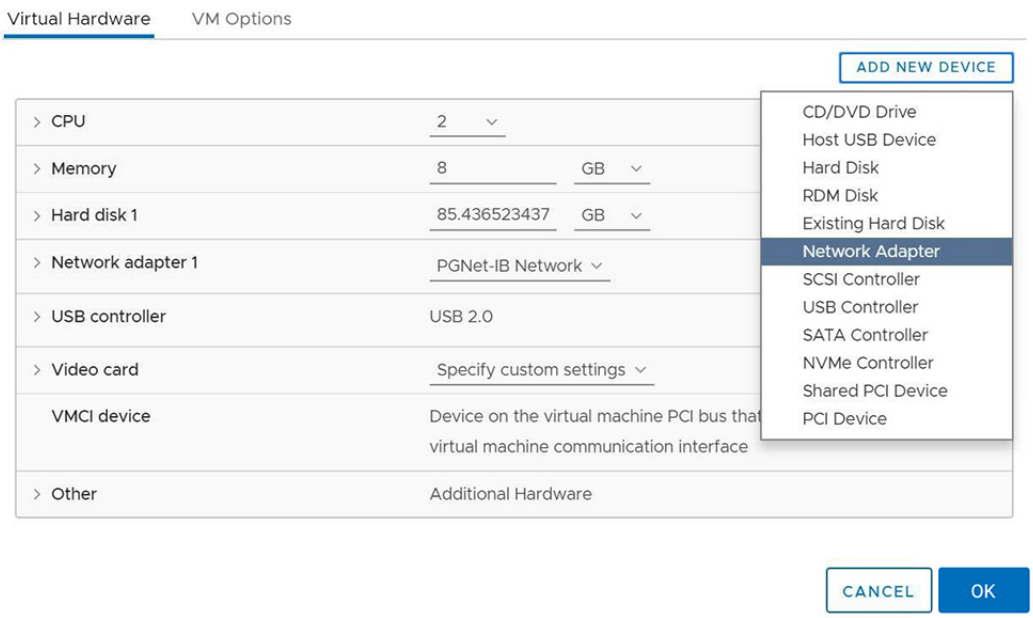
設定有兩個網路介面控制器 (NIC) 的 OMIVV 裝置

若要在 vSphere 環境中管理 Dell EMC 伺服器，OMIVV 需要 vSphere 網路 (vCenter 和 ESXi 管理網路) 和頻外網路 (iDRAC、CMC 和 OME-Modular) 兩者的存取權。如果環境中的 vSphere 網路和頻外網路是獨立的隔離網路，OMIVV 便需要這兩個網路的存取權。在此情況下，OMIVV 裝置必須設定兩個 NIC。若能使用 vSphere 網路存取頻外網路，請勿為 OMIVV 裝置設定兩個 NIC。

請確定您已為頻外網路及 vSphere 網路備妥下列資訊：

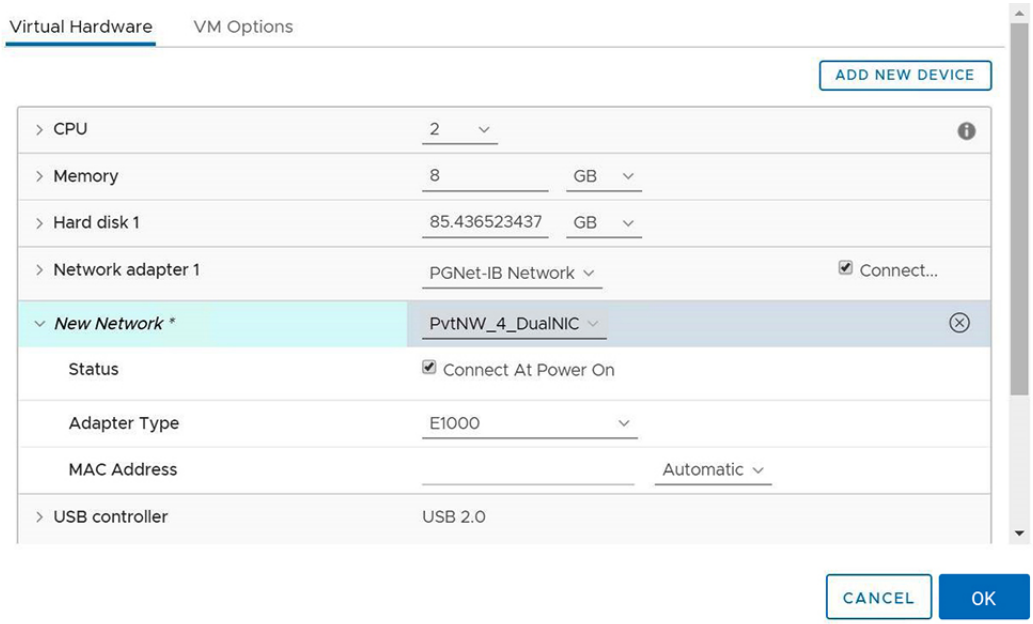
- IP 位址、網路遮罩 (CIDR 格式)，以及裝置的閘道 (若為靜態)
- 預設閘道—必須將預設閘道設定為擁有網際網路連線的唯一網路。建議將 vSphere 網路作為預設閘道。
- 路由要求 (網路 IP、網路遮罩和閘道)—對於無法直接連接或使用預設閘道連接的外部網路，設定靜態路由。
- DNS 要求— OMIVV 僅針對單一網路支援 DNS 組態。如需更多 DNS 組態的相關資訊，請移至本主題的步驟 9 (b)。

1. 關閉 OMIVV 裝置。
2. 使用 vSphere 用戶端 (HTML-5) 編輯虛擬機器設定，並新增額外的網路配接卡。若要編輯虛擬機器設定，以右鍵按一下虛擬機器，再按一下**編輯設定**。
3. 按一下**新增裝置**，選取**網路配接卡**。

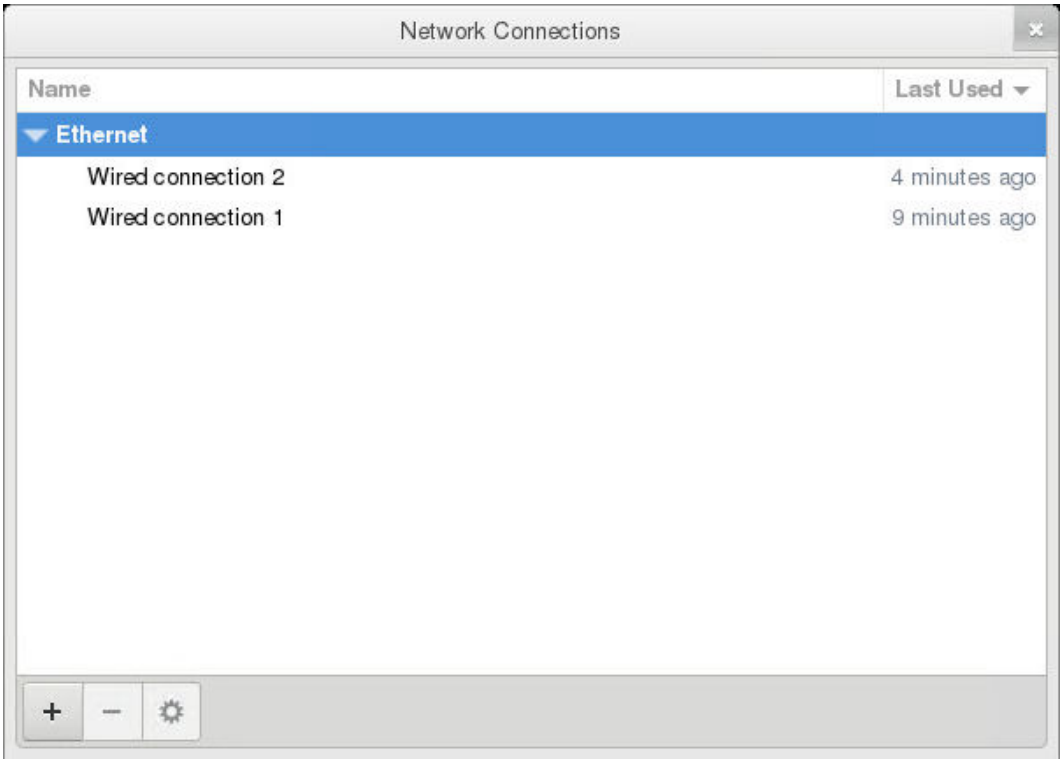


a. 為 NIC 選取適當的網路，然後選取**開機時連線**核取方塊。
b. 從下拉式功能表中選取 **VMXNET3** 配接卡類型。

註: OMIVV 支援 VMXNET3 類型的 NIC。

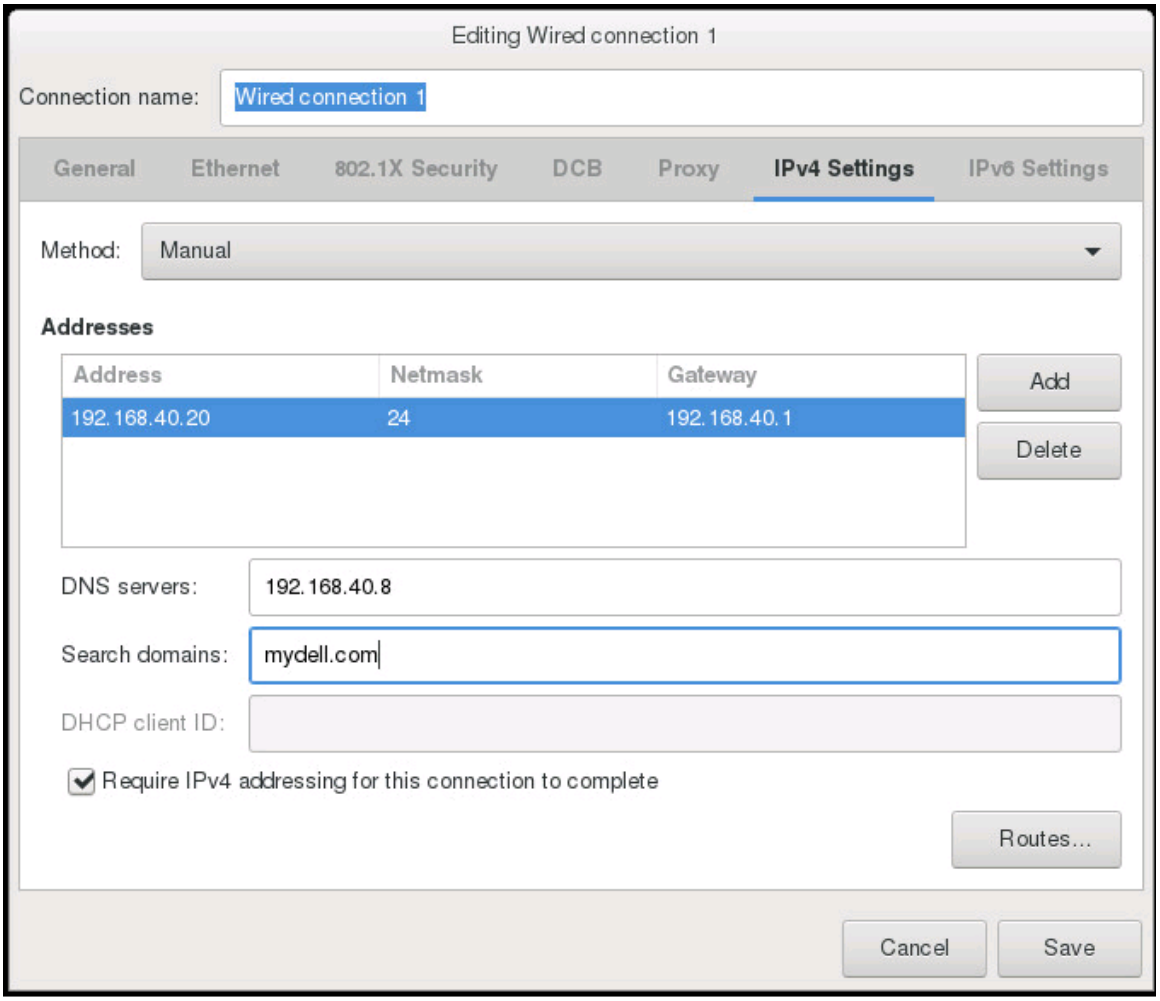


4. 開啟 OMIVV 裝置。以系統管理員身分登入 (預設的使用者名稱為 Admin)，然後按下 **Enter**。
5. 在 **OpenManage Integration for VMware vCenter 虛擬裝置設定**公用程式中，選取**網路組態**。
網路連線頁面會顯示兩個 NIC。



警告: 請勿使用「+」來新增任何新的網路介面。務必使用 vSphere「編輯設定」來新增 NIC。

6. 選取要設定的 NIC，然後按一下  。
7. 若要識別正確的 NIC，請使用顯示於**乙太網路**標籤上的 MAC ID，然後比對顯示在 vSphere 用戶端 (HTML-5) 的 MAC ID。確認您未變更列在**乙太網路**標籤中的預設 MAC 位址。
8. 按一下**一般**標籤，然後選取**此網路可用時，自動連線至該網路**核取方塊。
9. 按一下 **IPv4 設定**標籤，並執行下列操作：



a. 在**方法**下拉式清單中選擇**手動**或**自動 (DHCP)**。
b. 如果您選取**手動**方法，請按一下**新增**，然後輸入有效的 IP 位址、網路遮罩 (CIDR 格式) 和閘道的詳細資料。若您想要控制 DNS 伺服器 (主要和次要 DNS 項目) 的優先順序，建議使用靜態 IP。

   系統通常會使用主機名稱或 FQDN 來管理 vCenter 及 ESXi 主機等資料中心的 vSphere 元素。系統會使用 IP 位址來管理 iDRAC、CMC 和 OME-Modular。在此情況下，建議您僅針對 vSphere 網路來設定 DNS 設定。

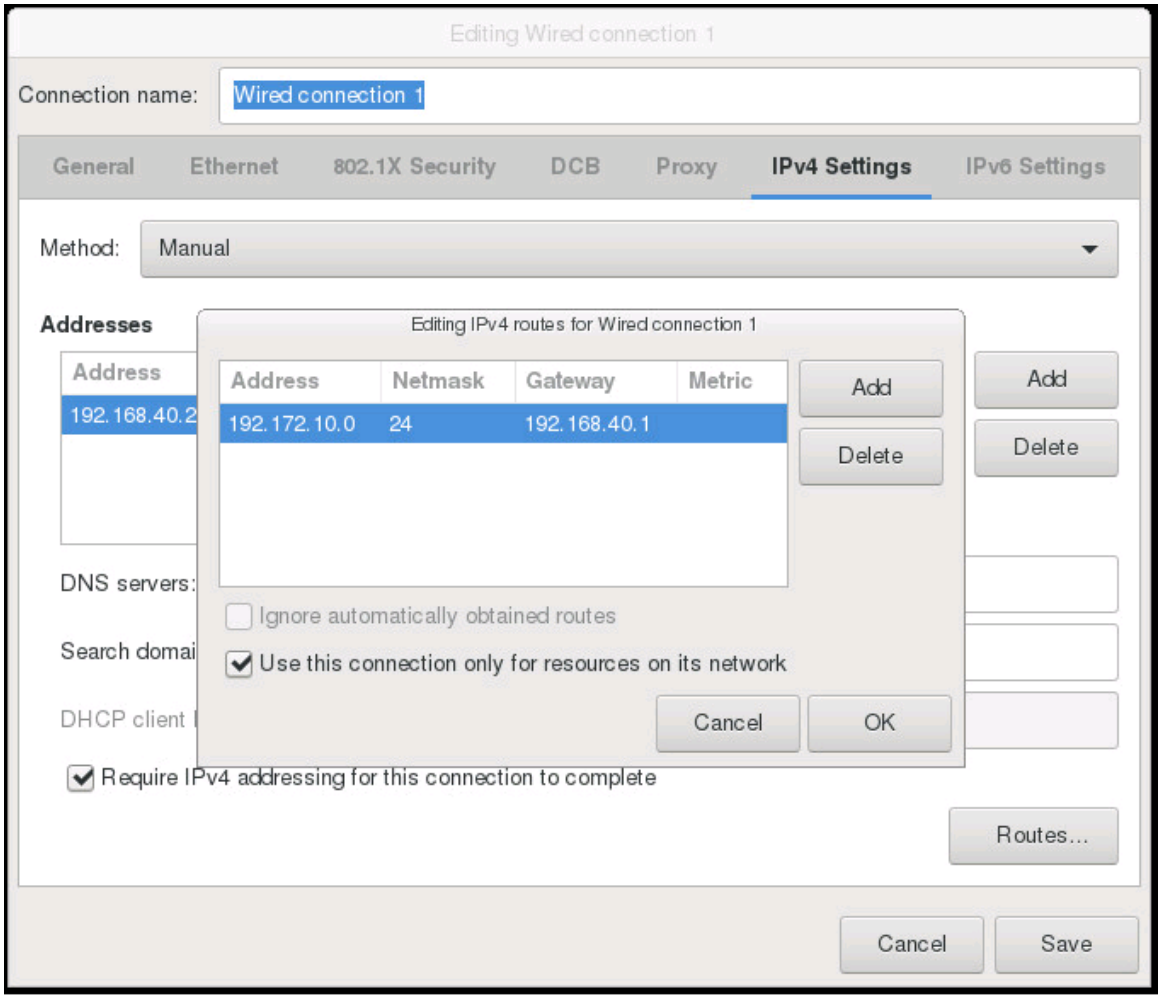
   如果使用主機名稱或 FQDN 來管理 vSphere 網路與 iDRAC 管理網路，則 DNS 伺服器必須設定成可以解析兩個網路上的主機名稱或 FQDN。如需更多資訊，請參閱 CentOS 說明文件。

   註: 無論 DNS 配置到哪個網路，最近一次設定的 DNS 伺服器會成為主要 DNS。

c. 在 **DNS 伺服器**和**搜尋網域**方塊中，分別輸入要搜尋的 DNS 伺服器 IP 與網域。
d. 選取**需要 IPv4 定址以完成此連線**核取方塊，然後按一下**儲存**。
e. 如果您不想使用此網路作為預設網路 (閘道)，按一下**路由**，然後選擇**僅將此連線用於其網路上的資源**核取方塊。

   註: 新增多個網路作為預設閘道可能會導致網路問題，OMIVV 功能可能因此受到影響。

f. 如果您要使用已知閘道連至任何外部網路，請在同一頁面上按一下**新增**，然後新增網路 IP 位址、網路遮罩 (CIDR 格式) 和閘道的詳細資料。



您已設定為預設閘道的網路通常不需要任何手動路由組態，因為閘道有能力提供連線。但是，若網路未設定預設閘道 (已選取**僅將此連線用於其網路上的資源**核取方塊者)，則可能需要手動路由組態。因為預設閘道未設定讓此網路連至外部網路，必須設定手動路由組態。

註: 不正確的路由組態可能會造成網路介面突然停止回應。請確定適當地設定路由項目。

g. 按一下**確定**。

10. 按一下**儲存**。若要設定其他 NIC，請重複工作步驟 6 到 10。
11. 前往 **OpenManage Integration for VMware vCenter 虛擬裝置設定**公用程式，按一下**裝置重新開機**。OMIVV 裝置要重新開機後才會完成網路組態。

    裝置重新開機成功後，NIC 即會開始依設定運作。若要檢視 NIC 的狀態，請以**唯讀**使用者的身分登入，並執行下列命令：`ifconfig`、`ping` 和 `route -n`。

變更 OMIVV 裝置密碼

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

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**。

設定網路時間通訊協定 (NTP) 並設定當地時區

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**日期/時間內容**。
   請確定在管理主控台中輸入 NTP 詳細資料。如需更多資訊，請參閱設定網路時間通訊協定 (NTP) 伺服器 第頁的 19。
3. 在**日期與時間**標籤上，選取**透過網路同步處理日期與時間**。
   NTP 伺服器視窗隨即顯示。
4. 若要新增另一個 NTP 伺服器 IP 或主機名稱 (如需要)，請按一下**新增**按鈕，然後按下 **TAB**。
5. 按一下**時區**，選取適用的時區，然後按一下**確定**。

變更 OMIVV 裝置的主機名稱

1. 在 **OpenManage Integration for VMware vCenter 虛擬裝置設定**公用程式上，按一下**變更主機名稱**。

   註: 如果有任何 vCenter 伺服器是在 OMIVV 裝置上註冊，請先取消註冊所有的 vCenter 例項，然後再重新註冊。

2. 輸入更新的主機名稱。
   以下列格式輸入網域名稱：*<hostname>*。
3. 按一下**更新主機名稱**。
   這會更新裝置主機名稱，並且顯示主功能表頁面。
4. 若要重新啟動裝置，請按一下**重新啟動裝置**。

註: 請務必先手動更新虛擬裝置整個環境的所有參照，例如 iDRAC 與 Dell EMC Repository Manager (DRM) 中的隨需分配伺服器。

重新啟動 OMIVV 裝置

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**裝置重新開機**。
3. 若要讓裝置重新開機，請按一下**是**。

將 OMIVV 裝置重設為原廠設定

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**重設設定**。
   螢幕上將顯示以下訊息：

```
All the settings in the appliance will be Reset to Factory Defaults and the appliance will be rebooted. Do you still wish to continue?
```

3. 若要重設裝置，請按一下**是**。
   如果您按一下**是**，OMIVV 裝置會重設為原廠預設設定，將刪除所有其他設定及現有的資料。

   完成原廠重設後，請再次將 vCenter 註冊到 OMIVV 裝置。

註: OMIVV 裝置重設為原廠預設設定時，對網路組態所做的任何更新都會保留。這些設定不會重設。

唯讀使用者角色

不具備所需權限的「唯讀」使用者，基於診斷目的具有殼層存取權。唯讀使用者僅具備執行少數命令的有限權限。

3

使用儀表板監控主機和機箱

儀表板會顯示以下資訊：

- 主機和機箱的健全狀態
- 主機和機箱的保固狀態
- 主機和 vCenter 的授權資訊
- 主機的組態相容性狀態
- 使用 OMIVV 排程的工作狀態
- 可供部署使用的裸機伺服器
- OMIVV 功能的快速參考

健全狀況

健全狀況區段會顯示所有 OMIVV 管理的主機和機箱健全狀況。此處顯示的所有主機皆使用相同的平台服務控制器 (PSC) 進行設定。

在完成定期健全狀況指標工作或來自主機和機箱的 SNMP 事件後 (觸發特定主機或機箱的健全狀況指標工作)，每個主機和機箱的狀態會重新整理。

依預設，健全狀況指標工作會在每小時後執行。顯示的資料用於在儀表板上監控伺服器和機箱的主動式 HA 健全狀況和健全狀況更新。記錄中會提供工作的詳細資料。

以下清單說明主機和機箱的不同狀態：

- **良好**—顯示處於良好狀態的主機和機箱計數。
- **警告**—顯示需要修正措施，但不會立即影響系統的主機和機箱計數。
- **嚴重**—顯示主機或機箱有一或多個元件存在嚴重問題，並須立即採取行動的主機和機箱計數。
- **未知**—顯示處於未知狀態的主機和機箱計數。無法連線到主機和機箱或健全狀況狀態未知時，主機和機箱會顯示未知狀態。

若要檢視更多主機相關聯資訊，請在**儀表板**頁面的**健全狀況**區段下，按一下**檢視主機**。

若要檢視更多機箱相關資訊，請在**儀表板**頁面的**健全狀況**區段下，按一下**檢視機箱**。

保固

在此保固類別下顯示的主機數量，指出使用 PSC 進行設定之 vCenter 伺服器的所屬主機。若要取得主機和機箱的保固資訊，請確定您已在**設定**頁面上啟用保固到期通知。

針對有多項或不同保固 (例如，次營業日 (NBD) 和僅零件保固 (POW) 的保固類型) 的主機，OMIVV 會根據剩餘最短保固天數的保固類型顯示狀態。

保固一節提供有關主機和機箱的下列資訊：

- **良好**—顯示其剩餘保固天數超過警告閾值的主機和機箱數量。
- **警告**—顯示其剩餘保固天數低於警告閾值的主機和機箱數量。
- **嚴重**—顯示其剩餘保固天數低於嚴重閾值的主機和機箱數量。
- **未知**—顯示其保固為未知的主機和機箱數量。

若要識別處於**健全**、**警告**、**嚴重**和**未知**狀態的主機，請執行下列步驟：

1. 前往**主機和叢集**。
2. 若要在叢集層級檢視主機的健全狀況狀態，請選取一個叢集，然後按一下**監控** > **OMIVV 叢集資訊** > **保固**。
3. 若要在資料中心層級檢視主機的健全狀況狀態，請選取一個資料中心，然後按一下**監控** > **OMIVV 資料中心資訊** > **保固**。

授權

授權區段會顯示下列資訊：

- 所有主機和 vCenter 授權計數
- 可用主機和 vCenter 授權計數
- 使用中主機和 vCenter 授權計數。

若要購買授權，請在**儀表板**頁面的**授權**區段下，按一下**購買授權**。

已準備好可進行部署

這將分離出僅使用 OMIVV 探索到的相容裸機伺服器。若要部署裸機伺服器，請按一下**部署**。

組態相容性

此區段會顯示叢集所屬的主機 (與叢集設定檔相關聯)。此處顯示的主機是使用相同的平台服務控制器 (PSC) 進行設定。

若要檢視主機的組態相容性狀態，請按一下**檢視相容性**。

工作

此區段會顯示使用 OMIVV 排程的工作。您只能檢視過去 7 天的工作詳細資料。

圓形圖會顯示**成功**、**進行中**、**失敗**、**排定**和**已取消**狀態的工作總數量。若要篩選圓形圖中的工作狀態，請按一下工作狀態。

您可以檢視處於**成功**、**進行中**、**失敗**、**已排定**和**已取消**等狀態的工作計數：

- 部署工作

  如需更多資訊，請參閱部署工作 第頁的 65。
- 主機韌體更新工作

  如需更多資訊，請參閱主機韌體更新工作 第頁的 67。
- 機箱韌體更新工作

  如需更多資訊，請參閱機箱韌體更新工作 第頁的 66。
- 系統鎖定工作

  如需更多資訊，請參閱系統鎖定模式工作 第頁的 67。

若要檢視所有工作的狀態，請按一下**檢視所有工作**。

快速參照

本節提供下列功能的快速參考：

- 啟動初始組態精靈

  如需更多資訊，請參閱 初始組態 第頁的 77
- 主機認證設定檔

  如需更多資訊，請參閱 主機認證設定檔 第頁的 34
- 管理相容性

  如需更多資訊，請參閱 管理相容性 第頁的 61
- 機箱認證設定檔

  如需更多資訊，請參閱 機箱認證設定檔 第頁的 38
- 叢集設定檔

  如需更多資訊，請參閱 叢集設定檔 第頁的 44

- 部署

  如需更多資訊，請參閱 部署檢查清單 第頁的 56

4

使用主機認證設定檔管理主機

主機認證設定檔

主機認證設定檔會儲存 OMIVV 用來與伺服器通訊的 iDRAC 和主機認證。OMIVV 管理與主機認證設定檔相關聯的主機。您可以讓單一主機認證設定檔與多個機箱相關聯。

PowerEdge MX 機箱主機可以使用單一整合機箱管理 IP 加以管理。在 PowerEdge MX 機箱中已停用 iDRAC IP 的主機，必須使用機箱認證設定檔進行管理。若要使用機箱認證設定檔管理 PowerEdge MX 機箱，請參閱建立機箱認證設定檔 第頁的 38。建議您使用主機認證設定檔來管理具有 iDRAC IP 的 PowerEdge MX 機箱主機，藉此取得完整的 OMIVV 功能。

建立主機認證設定檔

如果新增的主機數目超過授權限制，則無法建立主機認證設定檔。

搭配主機認證設定檔來使用 Active Directory (AD) 認證之前，請先確定以下事項：

- 使用者帳戶已存在於 AD 中。
- iDRAC 或主機有針對 AD 為基礎的驗證進行設定。

1. 在 OMIVV 首頁上，按一下**相容性與部署** > **主機認證設定檔**。
2. 在**主機認證設定檔**頁面上，按一下**建立新的設定檔**。
3. 閱讀精靈中**主機認證設定檔**頁面上的指示，然後按一下**開始使用**。
4. 在**名稱及認證**頁面上，執行下列步驟：
   a. 輸入設定檔名稱與說明。說明欄位是選填欄位。
   b. 從 **vCenter 名稱**清單中，選擇您想要建立主機認證設定檔的 vCenter 例項。
   c. 在 **IDRAC 認證**區域中，輸入 iDRAC 本機認證或 AD 認證。
      - 若要輸入 iDRAC 的本機認證，請執行下列作業:
        - 在**使用者名稱**方塊中輸入使用者名稱。使用者名稱上限為 16 個字元。

          如需定義使用者名稱的相關資訊，請參閱 **https://www.dell.com/support** 上的 *iDRAC 使用者指南*。
        - 輸入密碼。

          如需更多有關使用者名稱和密碼中建議字元的資訊，請參閱 **https://www.dell.com/support** 上的 *iDRAC 使用者指南*。
      - 若要下載並儲存 iDRAC 憑證，並在未來所有連線期間對其進行驗證，請選取**啟用憑證檢查**核取方塊。
      - 若要為已設定且啟用 AD 的 iDRAC 輸入認證，請選取**使用 Active Directory** 核取方塊。

        註: iDRAC 帳戶需要有系統管理員權限，才能更新韌體及部署作業系統 (OS)。
        - 在 **Active Directory 使用者名稱**方塊中輸入使用者名稱。

          請以下列其中一種格式輸入使用者名稱：`domain\username` 或 `username@domain`。使用者名稱上限為 256 個字元。請參閱 **Microsoft Active Directory 說明文件**，以取得使用者名稱限制的資訊。
        - 輸入密碼。

          iDRAC 與主機可以使用相同或個別的 AD 認證。

   d. 在**主機根**區域中，輸入本機主機認證或 AD 認證。

      預設使用者名稱為 root。
      - 若要輸入本機主機認證，請執行下列其中一項：
        - 輸入密碼。

僅有執行 ESXi 6.5 U3 及更舊版本的主機需要主機密碼。

若要為 ESXi 6.7 及更新版本略過此步驟，請確認已清除**使用主機認證**核取方塊。若為執行 ESXi 6.7 及更新版本的主機輸入密碼，則會忽略密碼。

對於執行 ESXi 6.7 及更新版本的主機，不需要輸入 ESXi 認證。OMIVV 可將 iDRAC 與其 ESXi 主機配對，即使輸入的主機認證不正確亦是如此。

- 若要為已設定且啟用 AD 的主機輸入認證，請選取**使用 Active Directory** 核取方塊。
  - 在 **Active Directory 使用者名稱**方塊中輸入使用者名稱。請以下列其中一種格式輸入使用者名稱：`domain\username` 或 `username@domain`。使用者名稱上限為 256 個字元。請參閱 **Microsoft Active Directory 說明文件**，以取得使用者名稱限制的資訊。
  - 輸入密碼。
- 若要下載並儲存主機憑證，並在未來所有連線期間對其進行驗證，請選取**啟用憑證檢查**核取方塊。

5. 按一下**下一步**。
   選取主機頁面會隨即顯示。
6. 在**選取主機**頁面中，展開樹狀檢視並選取主機，然後按一下**確定**。
   - 若要從**關聯主機**頁面新增或移除主機，請按一下**新增主機**

     註: 不要將已停用 iDRAC IPv4 的 PowerEdge MX 伺服器新增至主機認證設定檔。這些伺服器是使用機箱認證設定檔加以管理。

   選取的主機會顯示於**相關聯的主機**頁面。
7. 若要測試連線，請選取一個或多個主機，再按一下**開始測試**。
   建議您測試所有已設定主機的連線。
   在測試連線期間，OMIVV 會啟用 WBEM 服務，然後在為執行 ESXi 6.5 及更新版本的主機擷取 iDRAC IP 後停用。

   註: 輸入有效認證後，主機的測試連線作業也可能會失敗，並且顯示訊息表示輸入的認證無效。若 ESXi 封鎖存取，即會發生此問題。若多次試圖以不正確的認證連線至 ESXi，您的 ESXi 存取權將會被封鎖 15 分鐘。請等待 15 分鐘後，再重試該作業。

   - 若要停止測試連線程序，按一下**中止測試**。

   您可以在**測試結果**區段中檢視測試連線結果。
8. 按一下**完成**。

編輯主機認證設定檔

您一次可以編輯多個主機認證設定檔的認證。

1. 在**名稱及認證**頁面上，執行下列步驟：
   a. 編輯設定檔名稱與說明。
   b. 在 **IDRAC 認證**區域中，編輯 iDRAC 本機認證或 AD 認證。
      - 若要變更 iDRAC 的本機認證，請執行下列工作：
        - 在**使用者名稱**方塊中變更使用者名稱。使用者名稱上限為 16 個字元。

          如需定義使用者名稱的相關資訊，請參閱 **dell.com/support** 上的 *iDRAC 使用者指南*。
        - 變更密碼。
        - 若要下載並儲存 iDRAC 憑證，並在未來所有連線期間對其進行驗證，請選取**啟用憑證檢查**核取方塊。
      - 若要為已設定且啟用 AD 的 iDRAC 變更認證，請選取**使用 Active Directory** 核取方塊。

        註: iDRAC 帳戶需要有系統管理員權限，才能更新韌體及部署作業系統 (OS)。

        - 在 **Active Directory 使用者名稱**方塊中變更使用者名稱。

          請以下列其中一種格式輸入使用者名稱：`domain\username` 或 `username@domain`。使用者名稱上限為 256 個字元。如需更多定義使用者名稱的相關資訊，請參閱 *Microsoft Active Directory 說明文件*。
        - 輸入密碼。
        - 若要下載並儲存 iDRAC 憑證，並在未來所有連線期間對其進行驗證，請選取**啟用憑證檢查**核取方塊。

c. 在**主機根**區域中，編輯本機主機認證或 AD 認證。
   - 若要輸入本機主機認證，請執行下列其中一項：

     預設使用者名稱為 root。
     - 輸入密碼。

       僅有執行 ESXi 6.5 U3 及更舊版本的主機需要主機密碼。

       若要為 ESXi 6.7 及更新版本略過此步驟，請確認已清除**使用主機認證**核取方塊。若為執行 ESXi 6.7 及更新版本的主機輸入密碼，則會忽略密碼。

       對於執行 ESXi 6.7 及更新版本的主機，不需要輸入 ESXi 認證。OMIVV 可將 iDRAC 與其 ESXi 主機配對，即使輸入的主機認證不正確亦是如此。
   - 若要為已設定且啟用 AD 的主機變更認證，請選取**使用 Active Directory** 核取方塊。
     - 在 **Active Directory 使用者名稱**方塊中變更使用者名稱。

       請以下列其中一種格式輸入使用者名稱：`domain\username` 或 `username@domain`。使用者名稱上限為 256 個字元。請參閱
       Microsoft Active Directory 說明文件，以取得使用者名稱限制的資訊。
     - 變更密碼。
   - 若要下載並儲存主機憑證，並在未來所有連線期間對其進行驗證，請選取**啟用憑證檢查**核取方塊。

2. 按一下**下一步**。
   相關聯的主機頁面會隨即顯示。
3. 若要在相關聯的主機清單中新增或移除主機，請在**相關聯的主機**頁面上，按一下**新增主機**。

   註: 不要將已停用 iDRAC IPv4 的 PowerEdge MX 伺服器新增至主機認證設定檔。這些伺服器是使用機箱認證設定檔加以管理。

   選取的主機會顯示於**相關聯的主機**頁面。
4. 若要測試連線，請選取一個或多個主機，然後按一下**開始測試**。建議您測試所有已設定主機的連線。

   註: 輸入有效認證後，主機的測試連線作業也可能會失敗，並且顯示訊息表示輸入的認證無效。若 ESXi 封鎖存取，即會發生此問題。若多次試圖以不正確的認證連線至 ESXi，您的 ESXi 存取權將會被封鎖 15 分鐘。請等待 15 分鐘後，再重試該作業。

   - 若要停止測試連線，按一下**中止測試**。

   您可以在**測試結果**區段中檢視測試連線結果。

   在測試連線期間，OMIVV 會啟用 WBEM 服務，然後在為執行 ESXi 6.5 及更新版本的主機擷取 iDRAC IP 後停用。
5. 按一下**完成**。

   註:「修改日期」和「上次修改者」欄位中，包含您使用 vSphere 用戶端介面，針對主機認證設定檔所執行的變更。OMIVV 裝置在各自主機認證設定檔所執行的任何變更，都不會影響這兩個欄位。

檢視主機認證設定檔

1. 在 OMIVV 首頁上，按一下**相容性與部署** > **主機認證設定檔**。
   隨即會顯示包含所有主機認證設定檔與下列資訊的表格：
   - **設定檔名稱**—主機認證設定檔的名稱
   - **說明**—設定檔的說明 (如有提供)
   - **vCenter**—相關聯的 vCenter 之 FQDN 或主機名稱或 IP 位址
   - **相關聯的主機**—與主機認證設定檔相關聯的主機。如果出現一個以上相關聯的主機，使用展開圖示即可全部顯示。
   - **iDRAC 憑證檢查**—表示建立主機認證設定檔時是否已確認 iDRAC 憑證。
   - **主機根憑證檢查**—表示建立主機認證設定檔時是否已確認主機根憑證。
   - **建立日期**—建立主機認證設定檔的日期。
   - **修改日期**—修改主機認證設定檔的日期。
   - **上次修改者**—修改主機認證設定檔的使用者詳細資料。

註: 如果使用機箱認證設定檔來管理 PowerEdge MX 主機，OMIVV 會表示其與機箱認證設定檔建立關聯。如需更多資訊，請參閱 檢視機箱認證設定檔 第頁的 39。

2. 如果您要從精靈中移除或新增欄位名稱，請按一下 。
   依預設，不會選取**修改日期**及**上次修改**欄。若要選取這些欄，請按一下 。
3. 若要匯出主機認證設定檔資訊，請按一下 。

測試主機認證設定檔

使用測試認證設定檔功能，可以測試主機和 iDRAC 認證。建議選取所有主機。

1. 在 OMIVV 首頁上，選取與主機相關聯的主機認證設定檔，然後按一下**測試**。
   測試主機認證設定檔頁面會隨即顯示。
2. 選取所有相關聯的主機，然後按一下**開始測試**。
   a. 若要停止測試連線，按一下**中止測試**。
   隨即會顯示 iDRAC 與主機認證測試連線結果。

刪除主機認證設定檔

正在執行清查、保固或部署工作時，請務必不要刪除與主機具有關聯的主機認證設定檔。

OMIVV 不會管理屬於您已刪除之主機認證設定檔的所屬主機，除非您將這些主機新增到其他主機認證設定檔。

1. 在**主機認證設定檔**頁面上，選取一個設定檔，然後按一下**刪除**。
2. 提示您確認時，按一下**刪除**。
   所選的設定檔會從主機認證設定檔清單中移除。

5

使用機箱認證設定檔管理機箱

機箱認證設定檔

機箱認證設定檔儲存 OMIVV 用來與機箱通訊的機箱認證。OMIVV 管理及監控與機箱認證設定檔相關聯的機箱。您可以指派多個機箱到單一機箱認證設定檔。

PowerEdge MX 機箱主機可以使用單一整合機箱管理 IP 加以管理。在 PowerEdge MX 機箱中已停用 iDRAC IP 的主機，必須使用機箱認證設定檔進行管理。建議您使用主機認證設定檔來管理具有 iDRAC IP 的 PowerEdge MX 機箱主機，藉此取得完整的 OMIVV 功能。如需管理 MX 機箱的更多資訊，請參閱管理 PowerEdge MX 機箱 第頁的 97。

建立機箱認證設定檔

- 若要建立機箱認證設定檔，您必須具有下列權限：
  - M1000e、VRTX 和 FX2 機箱—讀取及設定 SNMP 陷阱目的地
  - PowerEdge MX 機箱—系統管理員
- 搭配主機認證設定檔來使用 Active Directory (AD) 認證之前，請先確定以下事項：
  - 使用者帳戶已存在於 AD 中。
  - CMC 或 OME-Modular 乃針對 AD 為基礎的驗證進行設定。
- 若為 PowerEdge MX 機箱，請確定您在已註冊的 vCenter 中至少有一個 MX 主機，才能成功測試連線。

1. 在 OMIVV 首頁上，按一下**相容性與部署** > **機箱認證設定檔** > **建立新設定檔**。
2. 閱讀精靈中**機箱認證設定檔**頁面上的指示，然後按一下**開始使用**。
3. 在**名稱及認證**頁面上，執行下列步驟：
   a. 輸入設定檔名稱與說明。說明是選填欄位。
   b. 在**使用者名稱**文字方塊中，輸入具有管理權限的使用者名稱 (通常用於登入機箱管理控制器 (CMC) 或 OpenManage Enterprise-Modular (OME-Modular))。
   c. 在**密碼**文字方塊中，輸入密碼。
   d. 在**確認密碼**文字方塊中，輸入您在**密碼**文字方塊中輸入的同一個密碼。密碼必須相符。
4. 在**選取機箱**頁面中，使用 **IP/主機名稱**欄旁的核取方塊選取個別機箱或多個機箱，然後按一下**確定**。
   選取的機箱會顯示於**相關聯的機箱**頁面。若要從相關聯的機箱清單中新增或移除機箱，請按一下**新增機箱**。

   如果選取的機箱已與機箱認證設定檔相關聯，則會顯示下列訊息：

   若選取目前與其他設定檔相關聯的機箱，會將此機箱由機箱認證設定檔中移除。沒有相關聯機箱的機箱認證設定檔將被刪除。

   例如，測試這個設定檔已經與機箱 A 有關聯。如果建立另一個設定檔測試 1，嘗試在機箱 A 與測試 1 之間建立關聯時，便會顯示警告訊息。

   所選機箱會自動執行測試連線。

   自動執行測試連線的時機：

   - 選取機箱後第一次執行。
   - 變更認證後
   - 重新選取機箱後

   測試結果區段中的測試結果會顯示為**通過**或**失敗**。若要手動測試機箱連線能力，請選取機箱，然後按一下**開始測試**。

   如果是以 MCM 群組設定的 PowerEdge MX 機箱，建議您使用主要機箱來管理所有主要機箱與成員機箱。成員機箱測試連線作業會失敗，且測試結果的狀態為**失敗**。隨即會顯示主要機箱的 IP 連結。按一下主要機箱的 IP 連結，探索完整的 MCM 群組。
5. 按一下**完成**。
   您必須至少要有一個驗證成功的機箱才能完成精靈中的工作。只有成功通過驗證的機箱可與機箱認證設定檔建立關聯。

若要新增 PowerEdge MX 機箱，請參閱新增 PowerEdge MX 機箱 第頁的 97。

編輯機箱認證設定檔

1. 在 OMIVV 首頁上，按一下**相容性與部署** > **機箱認證設定檔**。
2. 在**機箱認證設定檔**頁面上，按一下**編輯**。
3. 在**名稱及認證**頁面上，執行下列步驟：
   a. 編輯設定檔名稱與說明。說明是選填欄位。
   b. 在**使用者名稱**文字方塊中，變更為具有管理權限的使用者名稱 (通常用於登入機箱管理控制器 (CMC) 或 OpenManage Enterprise-Modular (OME-Modular))。
   c. 在**密碼**文字方塊中，輸入密碼。
      如果您將密碼欄位保留空白，OMIVV 會使用在建立工作流程期間所輸入的密碼。
   d. 在**確認密碼**文字方塊中，輸入您在**密碼**文字方塊中輸入的同一個密碼。密碼必須相符。
4. 在**選取機箱**頁面中，使用 **IP/主機名稱**欄旁的核取方塊選取或移除機箱，然後按一下**確定**。
   選取的機箱會顯示於**相關聯的機箱**頁面。若要從相關聯的機箱清單中新增或移除機箱，請按一下**新增機箱**。

   如果選取的機箱已與主機認證設定檔相關聯，則會顯示下列訊息：

   若選取目前與其他設定檔相關聯的機箱，會將此機箱由機箱認證設定檔中移除。沒有相關聯機箱的機箱認證設定檔將被刪除。

   例如，測試這個設定檔已經與機箱 A 有關聯。如果建立另一個設定檔測試 1，嘗試在機箱 A 與測試 1 之間建立關聯時，便會顯示警告訊息。

   所選機箱會自動執行測試連線。

   自動執行測試連線的時機：

   - 選取機箱後第一次執行。
   - 變更認證後
   - 重新選取機箱後

   測試結果區段中的測試結果會顯示為**通過**或**失敗**。若要手動測試機箱連線能力，請選取機箱，然後按一下**開始測試**。

   如果是以 MCM 群組設定的 PowerEdge MX 機箱，Dell EMC 建議您使用主要機箱來管理所有主要機箱與成員機箱。成員機箱測試連線作業會失敗，且測試結果的狀態為「失敗」。隨即會顯示主要機箱的 IP 連結。按一下主要機箱的 IP 連結，探索完整的 MCM 群組。

   註: 如果主機未出現在與 PowerEdge MX 機箱相關聯的已註冊 vCenter 中，則機箱的測試連線便會失敗。
5. 按一下**完成**。
   您必須至少要有一個驗證成功的機箱才能完成精靈中的工作。只有成功通過驗證的機箱可與機箱認證設定檔建立關聯。

   若要新增 PowerEdge MX 機箱，請參閱新增 PowerEdge MX 機箱 第頁的 97。

檢視機箱認證設定檔

在您建立一個或多個機箱認證設定檔後，您可以在機箱認證設定檔頁面上檢視機箱和相關聯的機箱。

1. 在 OMIVV 首頁上，按一下**相容性與部署** > **機箱認證設定檔**。

   隨即會顯示包含所有機箱認證設定檔與下列資訊的表格：

   - **設定檔名稱**—機箱認證設定檔的名稱
   - **說明**—設定檔的說明
   - **機箱 IP/主機名稱**—機箱 IP 或主機名稱連結。

     如為多機箱管理 (MCM) 群組，階層中會列出主要機箱 () 和成員機箱 ()。

     註: 針對 MCM 組態中的 PowerEdge MX 機箱，OMIVV 僅使用主要機箱管理所有主要和成員機箱。所有主要和成員都與主要機箱關聯的相同機箱認證設定檔相關聯。

     若為 MCM 群組中的成員機箱 (停用 IPv4)，會顯示主要機箱的 IPv4 位址。成員機箱的產品服務編號也會顯示在括號中。
   - **機箱產品服務編號**—指派給機箱的唯一識別符。

- **修改日期**—修改機箱認證設定檔的日期。

2. 下方格線會顯示關聯主機的下列資訊：
   - **設定檔名稱**
   - **關聯主機**
   - **產品服務編號**
   - **機箱 IP/主機名稱**
   - **機箱產品服務編號**
3. 若要匯出機箱認證設定檔資訊，請按一下 。

測試機箱認證設定檔

您可以使用機箱測試認證設定檔功能，測試與機箱認證設定檔相關聯的機箱認證。建議選取所有機箱。

1. 在 OMIVV 首頁上，按一下**相容性與部署** > **機箱認證設定檔**。
2. 選取機箱認證設定檔，然後按一下**測試**。
3. 在**測試機箱認證設定檔**頁面上，選取關聯的機箱，然後按一下**開始測試**。
   a. 若要停止測試連線，按一下**中止測試**。

   測試結果會顯示在**測試結果**欄中。

刪除機箱認證設定檔

在刪除機箱認證設定檔之前，請確定機箱例項不屬於 OMIVV 登錄的其他 vCenter。

如果已刪除機箱認證設定檔，OMIVV 便不會監視已刪除機箱認證設定檔中的機箱，直到您將機箱新增至其他機箱認證設定檔為止。

1. 在 OMIVV 首頁上，按一下**相容性與部署** > **機箱認證設定檔** > **刪除**。
2. 選取您要刪除的機箱認證設定檔。
3. 提示您確認時，按一下**刪除**。

   如果與機箱認證設定檔相關聯的所有機箱皆已移除，或移至不同的設定檔，則會顯示刪除確認訊息。此訊息表示機箱認證設定檔沒有任何相關聯的機箱，且已刪除。

   若要刪除機箱認證設定檔，請對刪除確認訊息按一下**確定**。

6

使用儲存庫設定檔管理韌體及驅動程式儲存庫

儲存庫設定檔

儲存庫設定檔可讓您建立和管理驅動程式或韌體儲存庫。

您可以使用韌體和驅動程式儲存庫設定檔來：

- 更新主機韌體
- 更新屬於 vSAN 叢集的主機驅動程式。
- 建立叢集設定檔和叢集基準。

預設的 OMIVV 韌體目錄為：

- **Dell EMC 預設目錄**：使用 Dell EMC 線上目錄取得最新韌體資訊的原廠建立韌體儲存庫設定檔。如果裝置沒有網際網路連線，請修改此儲存庫來指向本機 CIFS、NFS、HTTP 或 HTTPS 為基礎的共用區。如需此目錄修改方面的更多資訊，請參閱編輯或自訂 Dell 預設目錄 第頁的 42。

  您可以選取 Dell EMC 預設目錄做為預設目錄，以更新與任何叢集設定檔無關的 vSphere 主機的韌體。
- **已驗證的 MX 堆疊目錄**：使用 Dell EMC 線上目錄為 MX 機箱及其對應模組取得經驗證的韌體資訊之原廠建立韌體儲存庫設定檔。如需此目錄修改方面的更多資訊，請參閱編輯已驗證的 MX 堆疊目錄 第頁的 43。如需更多有關已驗證的 MX 堆疊目錄的資訊，請參閱 MX7000 韌體更新中提供的技術白皮書。

  註: 您無法使用 Dell EMC 預設目錄和已驗證的 MX 堆疊目錄儲存庫設定檔，為 vSAN 叢集建立基準。

建立儲存庫設定檔

1. 在 OMIVV 首頁上，按一下**相容性與部署** > **設定檔** > **儲存庫設定檔**。
2. 閱讀精靈中**儲存庫設定檔**頁面上的指示，然後按一下**開始使用**。
3. 在**設定檔名稱與說明**頁面上，輸入設定檔名稱與說明。說明欄位為選填，限制為 255 個字元。
4. 按一下**下一步**。
   設定檔設定頁面會隨即顯示。
5. 在**設定檔設定**頁面上，選取**韌體**或**驅動程式**。
   以下內容適用於驅動程式庫設定檔：
   - 驅動程式儲存庫設定檔最多可擁有 10 個驅動程式。如果出現更多檔案，驅動程式便會隨機選擇。
   - 僅使用離線驅動程式套裝 (.zip 檔案)。
   - 請下載與解壓縮離線驅動程式套裝 (.zip 檔案)，並提供共用位置的完整路徑以儲存到該共用位置。OMIVV 會自動建立 OMIVV 裝置內的目錄。驅動程式套裝可取自 https://my.vmware.com/web/vmware/downloads
   - OMIVV 需要 CIFS 或 NFS 的寫入存取權。
   - 子資料夾內的檔案會被忽略。
   - 大小超過 10 MB 的檔案會被忽略。
   - 驅動程式儲存庫僅適用於 vSAN 叢集。
6. 在**儲存庫共用位置**區域中，執行以下工作：
   a. 輸入儲存庫共用位置 (NFS 或 CIFS)。
   b. 如為 CIFS，則要輸入認證。
      OMIVV 只支援以 Server Message Block (SMB) 1.0 版和 SMB 2.0 版為基礎的 CIFS 共用。

      註: 若驅動程式儲存庫使用 SMB 1.0 共用，請在目錄路徑結尾新增檔分隔符號。
7. 若要確認目錄路徑與認證，請按一下**開始測試**。
   如要繼續建立儲存庫設定檔，您必須完成此驗證程序。

隨即會顯示測試連線結果。

8. 按一下**下一步**。
   與儲存庫位置同步頁面會隨即顯示。
9. 按一下**下一步**。
   提供儲存庫設定檔相關資訊的**摘要**頁面會隨即顯示。
10. 按一下**完成**。
    目錄建立後，會開始目錄下載與剖析，作業狀態會顯示在儲存庫設定檔的首頁上。

    在建立叢集設定檔及更新韌體時，有成功剖析的儲存庫設定檔可用。

編輯儲存庫設定檔

1. 在 OMIVV 首頁上，按一下**相容性與部署** > **儲存庫設定檔** > **編輯**。
2. 在**設定檔名稱與說明**頁面上，編輯設定檔名稱與說明，然後按一下**下一步**。
3. 在**設定檔設定**頁面上，選取**韌體**或**驅動程式**。
   以下內容適用於驅動程式庫設定檔：
   - 驅動程式儲存庫設定檔最多可擁有 10 個驅動程式。如果出現更多檔案，驅動程式便會隨機選擇。
   - 僅使用離線驅動程式套裝 (.zip 檔案)。
   - 請下載與解壓縮離線驅動程式套裝 (.zip 檔案)，並提供共用位置的完整路徑以儲存到該共用位置。OMIVV 會自動建立 OMIVV 裝置內的目錄。驅動程式套裝可取自 https://my.vmware.com/web/vmware/downloads
   - OMIVV 需要 CIFS 或 NFS 的寫入存取權。
   - 子資料夾內的檔案會被忽略。
   - 大小超過 10 MB 的檔案會被忽略。
   - 驅動程式儲存庫僅適用於 vSAN 叢集。
4. 在**儲存庫共用位置**區域中，執行以下工作：
   a. 輸入儲存庫共用位置 (NFS 或 CIFS)。
   b. 如為 CIFS，則要輸入認證。

      註: OMIVV 只支援以 Server Message Block (SMB) 1.0 版和 SMB 2.0 版為基礎的 CIFS 共用。
5. 若要確認目錄路徑與認證，請按一下**開始測試**。
   您必須先執行這項驗證，才能繼續進行。

   隨即會顯示測試連線結果。
6. 按一下**下一步**。
   與儲存庫位置同步頁面會隨即顯示。
7. 在**與儲存庫位置同步**頁面上，選取**與儲存庫位置同步**核取方塊，然後按一下**下一步**。
   若僅要更新設定檔名稱或檢閱資訊，請清除**與儲存庫位置同步**核取方塊，以便該目錄在 OMIVV 中保持不變。如需與儲存庫位置同步的更多資訊，請參閱與儲存庫位置同步 第頁的 43。
8. 檢閱**摘要**頁面上的設定檔資訊，然後按一下**完成**。

編輯或自訂 Dell 預設目錄

1. 在**儲存庫設定檔**頁面上，選取 **Dell 預設目錄**。
2. 在**設定檔名稱與說明**頁面上，編輯設定檔說明，然後按一下**下一步**。
3. 在**指定儲存庫位置**區段上，選擇下列任何一個儲存庫位置：
   - **Dell 線上預設**—儲存庫設定檔設定為 **Dell Online** (`https://downloads.dell.com/catalog/Catalog.gz`)。OMIVV 使用 Dell EMC Online 作為目錄和更新套件的來源。
   - **線上自訂**—OMIVV 使用**線上自訂** (HTTP 或 HTTPS 共用) 作為目錄和更新套件的來源。當您使用 Server Update Utility (SUU) 建立自訂儲存庫時，請確定目錄 (`catalog.xml.gz.sign`) 的簽名檔案存在於目錄檔案資料夾中。
   - **共用網路資料夾**—OMIVV 使用共用網路資料夾 (CIFS 或 NFS) 作為目錄和更新軟體套件的來源。

   a. 如果您選取**線上自訂**，請輸入目錄線上路徑。
   b. 如果您選取**共用網路資料夾**，請輸入目錄檔案位置 (NFS 或 CIFS)。
4. 若要確認目錄路徑與認證，請按一下**開始測試**。

隨即會顯示測試連線結果。

5. 在**與儲存庫位置同步**頁面上，選取**與儲存庫位置同步**核取方塊，然後按一下**下一步**。
   若僅要更新設定檔名稱或檢閱資訊，請清除**與儲存庫位置同步**核取方塊，以便該目錄在 OMIVV 中保持不變。如需與儲存庫位置同步的更多資訊，請參閱與儲存庫位置同步 第頁的 43。
6. 檢閱**摘要**頁面上的設定檔資訊，然後按一下**完成**。

編輯已驗證的 MX 堆疊目錄

1. 在**儲存庫設定檔**頁面上，選取**已驗證的 MX 堆疊目錄**，然後按一下**編輯**。
2. 僅可編輯下列項目：
   a. 目錄說明。
   b. 清除**與儲存庫位置同步**的核取方塊。
      若僅要更新設定檔名稱或檢閱資訊，請清除**與儲存庫位置同步**核取方塊，以便該目錄在 OMIVV 中保持不變。如需與儲存庫位置同步的更多資訊，請參閱與儲存庫位置同步 第頁的 43。

與儲存庫位置同步

Dell 預設目錄與已驗證的 MX 堆疊儲存庫設定檔會在每 24 小時之後或每次重新開機時，自動檢查變更及自動更新。

若要更新離線目錄，請完成下列步驟：

1. 使用 Dell EMC Repository Manager (DRM) 或 Server Update Utility (SUU) 更新離線位置 (CIFS 或 NFS) 中的目錄。如有驅動程式，請取代驅動程式套裝。
2. 編輯儲存庫設定檔，然後選擇**與儲存庫位置同步**核取方塊，以擷取變更供 OMIVV 參考。此程序需要數分鐘時間。
3. 若要在組態相容性基準中更新韌體，請確定要編輯相應的叢集設定檔並且儲存。

檢視儲存庫設定檔

1. 在 OMIVV 首頁上，按一下**相容性與部署** > **儲存庫設定檔**。
   隨即會顯示包含所有儲存庫設定檔與下列資訊的表格：
   - **設定檔名稱**—儲存庫設定檔的名稱
   - **說明**—設定檔的說明
   - **類型**—儲存庫的類型 (韌體或驅動程式)
   - **共用路徑**—NFS、CIFS、HTTP 或 HTTPS 路徑
   - **上次成功更新時間**—儲存庫設定檔更新的日期與時間。
   - **上次重新整理狀態**—目錄下載與剖析狀態
2. 如果您要從精靈中移除或新增欄位名稱，請按一下。
3. 若要匯出儲存庫設定檔資訊，按一下 。

刪除儲存庫設定檔

刪除儲存庫設定檔之前，請確定您已將該儲存庫設定檔與相關聯的叢集設定檔取消關聯。

1. 在**儲存庫設定檔**頁面上，選取一個儲存庫設定檔，然後按一下**刪除**。
2. 在刪除確認對話方塊中，按一下**刪除**。

7

使用叢集設定檔擷取基準組態

叢集設定檔

叢集設定檔可以讓您擷取組態基準 (硬體組態、韌體或驅動程式版本)，然後根據組態基準識別漂移以維持叢集的所需狀態。

若要建立叢集設定檔，請確保您有下列其中任何一個設定檔：系統設定檔、韌體儲存庫設定檔、驅動程式儲存庫設定檔，或其組合。建議針對基準叢集使用同質伺服器 (相同型號、相同硬體組態和相同韌體層級)。

- 建立叢集設定檔後，韌體和驅動程式儲存庫設定檔必須先剖析，才能用於建立叢集設定檔。
- 在建立叢集設定檔後，系統會建立相關聯韌體和驅動程式儲存庫的目前快照，以作為基準。如果原始儲存庫有所變更，叢集設定檔必須再次更新，以反映變更。否則，對原始儲存庫執行的任何更新將不會更新到叢集設定檔快照。
- 叢集設定檔建立之後，便會觸發漂移偵測工作。
- 叢集與叢集設定檔產生關聯時，它會覆寫該叢集先前的叢集設定檔關聯 (如果有)。
- 如果有多個獨立的 vCenter 在 OMIVV 註冊，則建議您針對每個 vCenter 建立不同的叢集設定檔。
- 只有在 vSAN 叢集上才支援驅動程式的基準。

  註: 不會考慮安裝在 OMIVV 外的驅動程式作為基準。

建立叢集設定檔

請確定：

- 您具有下列其中任何一個設定檔—系統設定檔、韌體儲存庫設定檔、驅動程式儲存庫設定檔，或其組合。
- vCenter 內會出現叢集。

1. 在 OMIVV 首頁上，**相容性與部署** > **設定檔** > **叢集設定檔** > **建立新的設定檔**。
2. 閱讀精靈中**叢集設定檔**頁面上的指示，然後按一下**開始使用**。
3. 在**設定檔名稱與說明**頁面上，輸入設定檔名稱與說明，然後按一下**下一步**。
   設定檔名稱最多可達 200 個字元，說明最多可達 400 個字元。
4. 在**相關聯的設定檔**頁面上，選擇下列任一設定檔或其組合：
   - 系統設定檔—選取系統設定檔會為叢集中的主機設定組態基準。針對基本和進階系統設定檔類型，系統設定檔名稱會以下列格式顯示：基本_<系統設定檔名稱>，進階_<系統設定檔名稱>
   - 韌體儲存庫設定檔—選取「韌體儲存庫」會為叢集中的主機建立韌體或 BIOS 基準。基準 vSAN 叢集不支援線上儲存庫。
   - 驅動程式儲存庫設定檔—選取「驅動程式儲存庫」會為叢集中的主機建立驅動程式基準。您一次最多可將 10 個驅動程式與基準相關聯。只有在 vSAN 叢集上才支援驅動程式的基準。
5. 按一下**下一步**。
   相關聯的叢集頁面隨即顯示。
6. 在**相關聯的叢集**頁面上，執行以下工作：
   a. 選取已註冊的 vCenter 伺服器之例項。
   b. 若要建立叢集關聯，按一下**瀏覽**。
   c. 選擇要建立基準的叢集。
   d. 按一下**確定**。
      選取的叢集會顯示於**相關聯的叢集**頁面。
   e. 按一下**下一步**。
7. 在**排程漂移偵測**頁面上，選取日期與時間，然後按一下**下一步**。
   摘要頁面隨即顯示提供叢集設定檔的相關資訊。
8. 按一下**完成**。
   漂移偵測工作會在叢集設定檔儲存後立即執行，且之後會在已排程的時間內執行。在工作頁面檢視工作完成狀態。

   註: 如果您在為叢集建立叢集設定檔後修改節點數目 (由 OMIVV 管理)，則集合大小會在後續的漂移偵測工作中自動更新。

編輯叢集設定檔

編輯叢集設定檔會變更基準，因而可能導致相容性等級被重新計算。

如果已變更相關聯的驅動程式儲存庫、或韌體儲存庫、或系統設定檔，且如果要對叢集設定檔使用最新變更，請選取叢集設定檔，按一下**編輯**，在精靈中按一下**下一步**，然後按一下**完成**。

1. 在 OMIVV 首頁上，按一下**相容性與部署** > **設定檔** > **叢集設定檔**。
2. 選取叢集設定檔，然後按一下**編輯**。
3. 在**設定檔名稱與說明**頁面上，編輯說明，然後按一下**下一步**。
4. 在**相關聯的設定檔**頁面上，您可以變更設定檔組合。
5. 在**相關聯的叢集**頁面上，您可以變更 vCenter 例項和相關聯的叢集。
6. 在**排程漂移偵測**頁面上，您可以變更漂移偵測排程。
7. 在**摘要**頁面上檢閱更新後的資訊，然後按一下**完成**。
   漂移偵測工作會在叢集設定檔儲存後立即執行，且之後會在已排程的時間內執行。

檢視叢集設定檔

1. 在 OMIVV 頁面上，按一下**相容性與部署** > **設定檔** > **叢集設定檔**。
   隨即會顯示包含所有叢集設定檔與下列資訊的表格：
   - **設定檔名稱** — 叢集設定檔的名稱
   - **說明**—設定檔的說明
   - **關聯的系統設定檔**—基本和進階系統組態檔案類型的相關系統設定檔名稱，系統設定檔名稱會以下列格式顯示：基本_<系統設定檔名稱>、進階_<系統設定檔名稱>
   - **相關聯的韌體儲存庫設定檔**—相關聯的韌體儲存庫設定檔名稱
   - **相關聯的驅動程式儲存庫設定檔**—相關聯的驅動程式儲存庫設定檔名稱

     註: 對於使用機箱認證設定檔管理的 PowerEdge MX 主機，不會計算組態漂移。
   - **vCenter**—與叢集設定檔關聯的 vCenter 例項
   - **上次成功更新時間**—叢集設定檔更新的日期與時間。

   註: 若關聯的儲存庫設定檔 (韌體或驅動程式) 或系統設定檔已修改，警告符號便會隨設定檔名稱一起顯示。在修改儲存庫或系統設定檔後，必須更新叢集設定檔，才能更新基線中的變更。如需更多更新叢集設定檔的相關資訊，請參閱 更新叢集設定檔 第頁的 45。
2. 如果您要從精靈中移除或新增欄名稱，請按一下。
3. 若要匯出叢集設定檔資訊，請按一下。

更新叢集設定檔

如果更新儲存庫設定檔 (韌體或驅動程式) 和系統設定檔，叢集設定檔頁面中的設定檔名稱旁會顯示警告符號。更新設定檔可能會影響叢集設定檔中相關聯叢集的組態相容性，以及 vSphere Lifecycle Manager 中的韌體相容性狀態。您可使用**更新設定檔**功能來更新叢集設定檔或重新建立基準。

1. 在 OMIVV 首頁上，按一下**相容性與部署** > **設定檔** > **叢集設定檔**。
2. 選取設定檔名稱旁有警告符號的叢集設定檔。
3. 按一下**更新設定檔**。
4. 若要將相關聯的設定檔更新為最新，請按一下**確定**。
   更新設定檔後，便無法還原基準。
   當叢集設定檔與更新的儲存庫設定檔或系統設定檔同步時，警告符號便會消失。

刪除叢集設定檔

1. 在 OMIVV 首頁上，按一下**相容性與部署** > **設定檔** > **叢集設定檔**。

2. 選取叢集設定檔，然後按一下**刪除**。
3. 在**刪除確認**對話方塊中，按一下**刪除**。
   如果叢集設定檔被刪除，則相應的漂移偵測工作也會被刪除。

8

管理裸機伺服器

檢視裸機伺服器

在**裸機伺服器**頁面上，您可以：

- 使用自動探索和手動探索來檢視探索到的裸機伺服器。

  隨即會顯示**產品服務編號**、**型號名稱**、**iDRAC IP**、**伺服器狀態**、**系統鎖定模式**、**法規遵循狀態**和 **iDRAC 授權狀態**等資訊。

  以下為裸機伺服器的不同狀態：

  - **未設定**—伺服器已新增至 OMIVV，並且正在等待設定。
  - **已設定**—伺服器已利用成功作業系統部署所需的所有硬體資訊完成設定。
  - **已隔離**—伺服器無法執行作業系統部署和韌體更新等工作，因為已從任何 OMIVV 動作中排除伺服器。
- 檢視裸機伺服器的法規遵循狀態。

  在下列情況下，裸機伺服器不相容：

  - 它不是支援的伺服器。
  - 它不具備支援的 iDRAC 授權 (最低要求是 iDRAC Express)。
  - 它未安裝支援的 iDRAC、BIOS 或 LC 版本。
  - LOM 或 NIC 不存在。
  - 系統鎖定模式已開啟。
- 如需檢視法規遵循問題的詳細資訊，在下方水平窗格中按一下**詳細資料**。

您也可以在**裸機伺服器**頁面上執行下列工作：

- 裸機伺服器的手動探索
- 移除裸機伺服器
- 系統設定檔與 ISO 設定檔部署
- 重新整理裸機伺服器
- 購買或更新 iDRAC 授權

裝置探索

探索是新增支援的裸機伺服器的程序。探索到伺服器之後，就可以將它用於系統設定檔和 iso 設定檔部署。如需進一步瞭解支援的伺服器清單，請參閱 *OpenManage Integration for VMware vCenter 相容性比較表*。

先決條件：

- 裸機伺服器的 iDRAC 和 OMIVV 虛擬機器之間必須有網路連線。
- 現有作業系統的主機不應探索加入 OMIVV，而應新增至 vCenter。將其新增至主機認證設定檔。
- 若要在 SD 卡上部署作業系統，並在 12G 和 13G PowerEdge 伺服器中使用系統設定檔功能，請確定已安裝 iDRAC 2.50.50.50 及更新版本。

自動探索

自動探索是新增裸機伺服器的程序。探索到伺服器後，請將它用於作業系統和硬體部署。自動探索是 iDRAC 功能，不需要使用 OMIVV 手動探索裸機伺服器。

自動探索先決條件

在嘗試探索 PowerEdge 裸機伺服器之前，請確認已安裝 OMIVV。使用 iDRAC Express 或 iDRAC Enterprise 的 PowerEdge 伺服器，可經探索進入裸機伺服器集區。請確認從 Dell EMC 裸機伺服器的 iDRAC 到 OMIVV 裝置之間有網路連線。

註: 具現有作業系統的主機不應使用 OMIVV 探索，而應將作業系統新增至主機認證設定檔。

您必須符合下列條件，才能進行自動探索：

- 電源 — 務必將伺服器連接到電源插座。伺服器不需要開啟電源。
- 網路連線—伺服器的 iDRAC 必須有網路連線功能，而且必須透過連接埠 4433 與隨需分配伺服器通訊。您可以用 DHCP 伺服器取得隨需分配伺服器的 IP 位址，也可以在 iDRAC 組態公用程式中，手動指定 IP 位址。
- 額外的網路設定—若要解析 DNS 名稱，請啟用 DHCP 設定中的「取得 DNS 伺服器位址」。
- 隨需分配服務位置—iDRAC 必須知道隨需分配服務伺服器的 IP 位址或主機名稱。請參閱隨需分配服務位置。
- 停用帳戶存取—如果有具備系統管理員權限的 iDRAC 帳戶，請先從 iDRAC Web 主控台將其停用。自動探索順利完成後，iDRAC 管理帳戶便會使用在**設定**頁面上輸入的部署認證重新啟用。如需更多有關部署認證的資訊，請參閱設定部署認證 第頁的 74。
- 自動探索啟用—伺服器的 iDRAC 必須啟用自動探索，自動探索程序才能開始。如需更多資訊，請參閱在 iDRAC 上啟用或停用管理帳戶 第頁的 48。

隨需分配服務位置

請使用下列選項，在自動探索時，依 iDRAC 取得隨需分配服務位置：

- 在 iDRAC 中手動指定 — 在 iDRAC 組態公用程式的「LAN 使用者組態」、「隨需分配伺服器」底下手動指定位置。
- DHCP 範圍選項 — 使用 DHCP 範圍選項來指定位置。
- DNS 服務記錄 — 使用 DNS 服務記錄來指定位置。
- DNS 已知名稱 — DNS 伺服器會指定具有已知名稱 DCIMCredentialServer 之伺服器的 IP 位址。

如果隨需分配服務值不是在 iDRAC 組態公用程式中手動指定，iDRAC 會嘗試使用 DHCP 範圍選項值。如果沒有 DHCP 範圍選項，則 iDRAC 會嘗試使用 DNS 的服務記錄值。

如需詳細瞭解設定 DHCP 範圍選項與 DNS 服務記錄的方式，請參閱「Dell 自動探索網路設定規格」，網址為：https://www.dell.com/support。

在 iDRAC 上啟用或停用管理帳戶

請先停用所有 iDRAC 帳戶 (其中一個沒有管理員存取權的帳戶除外)，才能設定自動探索。自動探索後，您即可啟用根帳戶以外的所有帳戶。

註: 停用管理員權限之前，建議您在 iDRAC 中建立非管理員使用者帳戶。

1. 在瀏覽器中，輸入 **iDRAC IP 位址**。
2. 登入 **Integrated Dell Remote Access Controller 圖形化使用者帳戶 (GUI)**。
3. 請執行下列其中一項動作：
   - 若為 iDRAC7：在左窗格中選取 **iDRAC 設定** > **使用者驗證** > **使用者**標籤。
   - 若為 iDRAC8：在左窗格中選取 **iDRAC 設定** > **使用者驗證** > **使用者**標籤。
   - 若為 iDRAC9：請前往 **iDRAC 設定** > **使用者** > **本機使用者**。
4. 在**本機使用者**標籤中，尋找根帳戶以外的任何管理帳戶。
5. 若要停用帳戶，請在使用者 ID 底下選取 **ID**。
6. 按一下**下一步**。
7. 在**使用者組態**頁面的**一般**底下，清除**啟用使用者**核取方塊。
8. 按一下**套用**。
9. 若要重新啟用每個管理帳戶，請在順利設定自動探索之後，重複步驟 1 至 8，但這次請選取**啟用使用者**核取方塊，然後按一下**套用**。

為自動探索手動設定 PowerEdge 伺服器

請確定具備 iDRAC 位址。

向 Dell EMC 訂購伺服器時，您可以在提供隨需分配伺服器 IP 位址後，要求在伺服器啟用自動探索功能。隨需分配伺服器 IP 位址是 OMIVV 的 IP 位址。若您從 Dell EMC 收到伺服器，並在掛接和連接 iDRAC 纜線後開啟伺服器電源，系統便會自動探索伺服器，並將伺服器列在**裸機伺服器**頁面上。

註: 對於自動探索到的伺服器，系統會將 **設定** > **裝置設定** > **部署認證**之下提供的認證設定為管理認證，並且作為日後與伺服器通訊之用，直到完成作業系統部署為止。完成作業系統部署之後，就會設定關聯主機認證設定檔中提供的 iDRAC 認證。

若要在目標機器上手動啟用自動探索，請對 12G 及更新版本的 PowerEdge 伺服器執行下列步驟：

1. 在目標系統上，在初始開機時按 F2。
2. 前往 **iDRAC 設定** > **使用者組態**，然後停用根使用者。請確定您在停用根使用者時，該 iDRAC 位址不能有其他具備作用中管理員權限的使用者。
3. 按一下**返回**，然後按一下**遠端啟用**。
4. 將**啟用自動探索**設定為**啟用**，並將**隨需分配伺服器**設定為 OMIVV 的 IP 位址。
5. 儲存設定。
   這樣下次啟動伺服器時，就會進行自動探索。順利執行自動探索後，就會自動啟用根使用者，並自動停用**啟用自動探索**旗標。

裸機伺服器的手動探索

請確定使用具有管理員權限的 iDRAC 使用者來探索。

OMIVV 可讓您根據 IPv4 的範圍手動探索伺服器。您可以使用 IPv4 範圍探索方法，來探索單一 IP 或一組 IP。

在新增裸機伺服器後，伺服器會顯示在**裸機伺服器**頁面的伺服器清單中。

1. 在 OMIVV 首頁上，按一下**相容性與部署** > **部署** > **探索**。
   隨即會顯示**探索裸機伺服器**頁面。
2. 在**探索裸機伺服器**頁面上執行下列作業：
   a. 在**探索工作名稱**欄位中，輸入工作的名稱。
   b. 輸入工作描述名稱 (選用)。
   c. 若要輸入 IP 範圍，請按一下**新增範圍資料**。

      每個探索工作中皆可提及多個範圍。最多支援 1024 個 IP。範圍內可設定的最大 IP 數目為 256。

      當您在一個範圍的排除清單中新增特定的 IP 集，然後在另一個範圍的包含清單中新增相同 IP 時，所包含的 IP 將具有較高的優先度。
   d. 輸入**開始 IP**。
      開始 IP 必須為 IPv4 位址格式。
   e. 輸入**結束 IP**。
      結束 IP 必須是 IP 的最後一個八位元組，且大於開始 IP。
   f. 輸入**排除清單**。
      排除清單是您要從清單中排除的 IP 清單。

      輸入**排除清單**的值必須介於**開始 IP** 和**結束 IP** 的範圍內。這些值必須以逗號分隔，每個值都可以是最後一個八位元組的值，或是以 - 分隔的最後一個八位元組範圍。

      例如：

      若要探索從 100.100.100.1 到 100.100.100.50 的所有 IP，請排除從 100.100.100.25 到 100.100.100.30 和從 100.100.100.40 到 100.100.100.45 的 IP，請在**開始 IP**、**結束 IP** 和**排除清單**中輸入下列各項。

      開始 IP：100.100.100.1

      結束 IP：50

      排除清單：25-30、40-45
   g. 若要使用在**部署認證**頁面上輸入的 iDRAC 認證，請選取**使用部署認證**核取方塊。
      如需更多有關部署認證的資訊，請參閱設定部署認證 第頁的 74。
   h. 如果未設定部署認證，請輸入使用者名稱和密碼。

依預設會設定部署認證。如果您想要使用部署憑證以外的其他認證，請輸入 iDRAC 使用者名稱和密碼。您可以為每個範圍使用不同的認證集。

使用者名稱必須介於 1 到 16 個字元之間。不支援特殊字元 /, \, ~, 和 '。

密碼最多可包含 42 個字元。

3. 選取下列任何選項：
   - **立即執行**—立刻執行工作，探索特定範圍內提及的所有 IP。
   - **稍後執行**—排程工作以稍後再執行，會探索指定範圍內的 IP。
4. 按一下**套用**。
   探索工作的狀態會顯示在**探索工作**頁面上。如需更多資訊，請參閱 探索工作 第頁的 66。

移除裸機伺服器

您可以手動移除自動探索或手動新增的伺服器。

1. 在 OMIVV 首頁上，按一下**相容性與部署** > **部署** > **刪除**。
2. 選取裸機伺服器，然後按一下**確定**。

重新整理裸機伺服器

透過連線至 iDRAC 和收集基本的清查資訊，重新整理操作可重新探索裸機伺服器。

註: 如果您在「已設定」裸機伺服器上執行重新整理作業，伺服器狀態會變更為「未設定」狀態，因為重新整理作業會重新探索伺服器。

1. 在 OMIVV 首頁上，按一下**相容性與部署** > **部署** > **重新整理**。
2. 在**重新整理裸機伺服器**頁面上選取伺服器，然後按一下**確定**。
   重新整理裸機伺服器資料可能需要幾分鐘的時間。在執行作業時，您可以關閉**重新整理裸機伺服器**頁面，重新探索程式會在背景繼續進行。重新探索到的伺服器會顯示**裸機伺服器**頁面上。

購買或更新 iDRAC 授權

當裸機伺服器沒有相容的 iDRAC 授權時，其狀態會顯示不相容。表格顯示的是 iDRAC 授權的狀態。選取不相容的裸機伺服器，以檢視 iDRAC 授權的詳細資訊。

1. 若要更新 iDRAC 授權，請在 OMIVV 首頁上，按一下**相容性與部署** > **部署**。
2. 選取 iDRAC 授權不相容的裸機伺服器，然後按一下**購買/更新 iDRAC 授權**。
3. 登入 Dell Digital Locker，並更新或購買新的 iDRAC 授權。
4. 安裝 iDRAC 授權之後，請按一下**重新整理**。

9

管理部署設定檔

系統設定檔

系統設定檔會擷取 iDRAC、BIOS、RAID、事件篩選器、FC 和 NIC 的元件層級設定與組態。可在裸機伺服器的作業系統部署期間，將這些組態套用至其他完全相同的伺服器。系統設定檔能用於叢集設定檔中，以維持組態基準。

先決條件

在建立或編輯系統設定檔之前，請先確定下列項目：

- 已啟用參考伺服器上的 CSIOR 功能。啟用 CSIOR 後，必須重新啟動參照伺服器，使 iDRAC 傳回的資料為最新。
- 由 vCenter 管理的每個參照主機皆已成功清查。
- 裸機伺服器已安裝最低要求的 BIOS 及韌體版本。如需更多資訊，請參閱支援網站上的 *OMIVV 相容性比較表*。
- 參照伺服器和目標伺服器為同質伺服器 (相同型號、相同硬體組態和相同韌體層級)。
- 硬體 (例如 FC、NIC 和 RAID 控制器) 存在於參照伺服器和目標伺服器相同的插槽中。
- 在預設選取中包含或排除任何屬性之前，請將游標移到屬性名稱上，以瞭解屬性的詳細資料。
- 當您在系統設定檔中設定 iDRAC 使用者時，會選取用於探索 iDRAC 的 iDRAC 使用者。

  註: 請勿清除與用來探索裸機的 iDRAC 使用者相連結的屬性，否則系統設定檔部署工作會失敗。
- 請勿變更用於探索 iDRAC 的 iDRAC 使用者名稱。如此會導致 iDRAC 連線問題，系統設定檔部署工作會失敗，且不會套用任何屬性。

在建立系統設定檔之前，建議您根據需要設定參照伺服器的屬性和值。將參照屬性和值套用到所有需要的目標主機上。

系統設定檔在套用設定檔時會搜尋確切的例項 (FQDD)，在完全相同的機架式伺服器上可成功運作，但在模組化伺服器中則有少數限制。例如在 FC640 中，從某個模組化伺服器建立的系統設定檔會因為 NIC 層級的限制，而無法套用至相同 FX 機箱中的其他模組化伺服器。在此情況下，建議您從機箱的每個插槽取得參照系統設定檔。請僅將這些系統設定檔套用到機箱的對應插槽。

註: 系統設定檔不支援開機選項的啟用和停用。

註:

- 使用系統設定檔時，若匯出具有 Enterprise 授權的系統設定檔，然後在具有 Express 授權的伺服器上匯入相同的系統設定檔會失敗。
- 您無法使用 iDRAC9 韌體 3.00.00.00 的 Express 授權匯入系統設定檔。您必須具備 Enterprise 授權。

建立系統設定檔

建議使用 Google Chrome 建立或編輯系統設定檔。

使用 Slimline 纜線連接 HBA、BOSS 和 PERC 的 PowerEdge R6515、R7515、R65125、R7525 和 C6515 伺服器。在 iDRAC 版本早於 4.30.30.30 的 OMIVV 建立的系統設定檔無法用於 iDRAC 4.30.30.30 和更新版本。使用 iDRAC 4.30.30.30 或更新版本建立新系統設定檔，並在需要時使用。

1. 在 OMIVV 首頁上，按一下**相容性與部署** > **設定檔** > **系統設定檔** > **建立新的設定檔**。
2. 閱讀精靈中**建立系統設定檔**頁面上的指示，然後按一下**開始使用**。
3. 在**名稱及認證**頁面上，執行下列步驟：
   a. 輸入設定檔名稱與說明。說明欄位是選填欄位。
   b. 選取下列任何系統設定檔類型：
      - **基本**—顯示 iDRAC、BIOS、RAID、NIC 和 FC 的最少屬性集。
      - **進階**—顯示 iDRAC、BIOS、RAID、NIC、FC 和 EventFilters 的所有屬性。
4. 在**參照伺服器**頁面中，若要選取任一主機或裸機為參照伺服器，請按一下**選取**。

由於以下任何原因，伺服器選取可能停用：

- 伺服器為不相容主機或不相容裸機伺服器
- 伺服器上已排定或正在執行部署工作。
- 該伺服器使用機箱認證設定檔進行管理。

隨即會顯示**擷取確認**對話方塊。

5. 若要從參照伺服器擷取系統組態，請按一下**確定**。
   從參照伺服器擷取系統組態可能需要幾分鐘的時間。
6. 檢閱參照伺服器的詳細資料，再按一下**下一步**。
   - 若要在**選取參照伺服器**頁面上變更參照伺服器，請按一下**瀏覽**。

     如果參照伺服器為裸機類型，只會顯示其 iDRAC IP。若參照伺服器本身即為主機伺服器，則會同時顯示 iDRAC 和主機 (FQDN) IP 位址。

   設定檔設定頁面會隨即顯示。
7. 在**設定檔設定**頁面上，您可以根據參照伺服器的組態檢視或修改元件的設定檔設定，例如 iDRAC、BIOS、RAID、NIC、CNA、FCoE 與 EvenFilters。
   依預設，系統不會列出平台專有屬性和唯讀屬性。如需更多關於平台專有屬性的資訊，請參閱系統專有屬性 第頁的 145。
   虛擬屬性不會顯示在系統設定檔中。如需更多資訊，請參閱伺服器組態 XML 檔案文件。
   在選取預設選取屬性以外的屬性之前，請檢查屬性的性質、相依性和其他詳細資料。
   如果您選取預設選取屬性以外的屬性，將會顯示下列訊息：
   這些屬性可能會影響其他相依屬性，或在性質上有破壞性，或溶解伺服器身分識別，或影響目標伺服器的安全性。

   註: 針對 12G 和 13G 的 PowerEdge 伺服器，部分屬性可能不會在 OMIVV 中正確地對應相依性。例如，除非系統設定檔在**系統 BIOS 設定**中設定為**自訂**，否則 BIOS 的記憶體操作電壓元件將會是唯讀。

   a. 展開每個元件以檢視設定選項，例如**例項**、**屬性名稱**、**值**、**破壞性**、**相依性**和**群組**。
      如果相依性文字無法使用，則會顯示空白欄位。
      註: 您可以使用**搜尋**欄位來篩選除了**值**以外的所有欄的特定資料。
   b. 必須為標有紅色驚嘆號的屬性設定值。此選項僅適用於已啟用 iDRAC 且具備有效使用者名稱的使用者。
8. 按一下**下一步**。
   摘要頁面顯示關於設定檔詳細資料和系統組態屬性統計資料的資訊。
   屬性總數、已啟用屬性總數，以及破壞性屬性總數會顯示於屬性統計資料下。
9. 按一下**完成**。
   已儲存的設定檔會顯示於**系統設定檔**頁面。
   系統設定檔的某些屬性會遭到覆寫，以使 OMIVV 能夠運作。如需更多有關自訂屬性的資訊，請參閱自訂屬性 第頁的 150。如需更多有關系統設定檔組態範本、屬性和工作流程的資訊，請參閱其他資訊 第頁的 149。

編輯系統設定檔

建議使用 Google Chrome 建立或編輯系統設定檔。

1. 在**建立系統設定檔**頁面上，選取一個系統設定檔，然後按一下**編輯**。
2. 在**名稱與說明**頁面上，變更設定檔名稱與說明。說明是選填欄位。

   註: 在建立基本或進階系統設定檔後，您無法修改設定檔。

3. 在**參照伺服器**頁面中，若要變更任一主機或裸機為參照伺服器，請按一下**選取**。
   由於以下任何原因，伺服器選取可能停用：
   - 伺服器為不相容主機或裸機伺服器。
   - 伺服器上已排定或正在執行部署工作。
   - 該伺服器使用機箱認證設定檔進行管理。

   隨即會顯示**擷取確認**對話方塊。

4. 若要從參照伺服器擷取系統組態，請按一下**確定**。
   從參照伺服器擷取系統組態可能需要幾分鐘的時間。
5. 檢閱參照伺服器的詳細資料，再按一下**下一步**。
   - 若要在**選取參照伺服器**頁面上變更參照伺服器，請按一下**瀏覽**。如果參照伺服器為裸機類型，只會顯示其 iDRAC IP。若參照伺服器本身即為主機伺服器，則會同時顯示 iDRAC 和主機 (FQDN) IP 位址。

   設定檔設定頁面會隨即顯示。
6. 在**設定檔設定**頁面上，您可以根據參照伺服器的組態檢視或修改元件的設定檔設定，例如 iDRAC、BIOS、RAID、NIC、CNA、FCoE 與 EvenFilters。

   依預設，系統不會列出平台專有屬性和唯讀屬性。如需更多關於平台專有屬性的資訊，請參閱系統專有屬性 第頁的 145。

   如果您嘗試修改少數屬性，系統會顯示下列警告訊息：

   這些屬性可能會影響其他相依屬性，或在性質上有破壞性，或溶解伺服器身分識別，或影響目標伺服器的安全性。

   註: 編輯系統設定檔後，如果修改用來探索裸機伺服器的 iDRAC 使用者密碼，則系統會忽略更新的密碼。更新的密碼會取代為用來探索裸機伺服器的密碼。

   a. 展開每個元件以檢視設定選項，例如例項、屬性名稱、值、破壞性、相依性和群組。
      如果相依性文字無法使用，則會顯示空白欄位。
   b. 必須為標有紅色驚嘆號的屬性設定值。此選項僅適用於已啟用 iDRAC 且具備有效使用者名稱的使用者。
7. 按一下**下一步**。
   摘要頁面顯示關於設定檔詳細資料和系統組態屬性統計資料的資訊。

   屬性總數、已啟用屬性總數，以及破壞性屬性總數會顯示於屬性統計資料下。
8. 按一下**完成**。
   已儲存的設定檔會顯示於**系統設定檔**頁面。

   系統設定檔的某些屬性會遭到覆寫，以使 OMIVV 能夠運作。如需更多有關自訂屬性的資訊，請參閱自訂屬性 第頁的 150。如需更多有關系統設定檔組態範本、屬性和工作流程的資訊，請參閱其他資訊 第頁的 149。

檢視系統設定檔

1. 在 OMIVV 首頁上，按一下**相容性與部署** > **系統設定檔**。
   隨即會顯示包含所有系統設定檔與下列資訊的表格：
   - **設定檔名稱**—系統設定檔的名稱
   - **說明**—設定檔的說明
   - **參照伺服器** — 從中解壓縮系統組態詳細資料的 iDRAC IP。
   - **伺服器機型**—參照伺服器的型號名稱
2. 如果您要從精靈中移除或新增欄名稱，請按一下。
3. 若要匯出系統設定檔資訊，請按一下  。

刪除系統設定檔

刪除的系統設定檔若為執行部署工作的一部份，可能會使刪除工作失敗。

1. 在**系統設定檔**頁面上，選取一個系統設定檔，然後按一下**刪除**。
2. 在刪除確認對話方塊中，按一下**刪除**。

ISO 設定檔

ISO 設定檔包含儲存在 NFS 或 CIFS 資料夾上 Dell EMC 自訂 ESXi ISO 映像檔案的資料夾路徑。於部署精靈中使用的 ISO 設定檔。

建立 ISO 設定檔

ISO 設定檔需要 NFS 或 CIFS 上，由 Dell EMC 自訂的 ISO 檔案位置。

1. 在 OMIVV 首頁上，按一下**相容性與部署** > **設定檔** > **ISO 設定檔** > **建立新的設定檔**。
2. 閱讀精靈中 **ISO 設定檔**頁面上的指示，然後按一下**開始使用**。
3. 在**設定檔名稱與說明**頁面上，輸入設定檔名稱與說明。說明是選填欄位。
4. 在**安裝來源 (ISO)** 方塊中，輸入 ISO 檔案位置 (NFS 或 CIFS)。
   OMIVV 只支援以 Server Message Block (SMB) 1.0 版和 SMB 2.0 版為基礎的 CIFS 共用。
   a. 如果您使用 CIFS，則要輸入認證。
5. 從 **ESXi 版本**下拉式清單中選取 ESXi 版本。
   選取正確的 ESXi 版本，以便使用適當的安裝開機指令檔。如果您選取不正確的 ESXi 版本，部署可能會失敗。
6. 若要確認 ISO 檔案路徑存取功能與認證，請按一下**開始測試**。
   隨即會顯示測試結果。
7. 按一下**完成**。

編輯 ISO 設定檔

1. 在 OMIVV 首頁上，按一下**相容性與部署** > **設定檔** > **ISO 設定檔**。
2. 選擇 ISO 設定檔，按一下**編輯**。
3. 在**設定檔名稱與說明**頁面上，編輯設定檔名稱與說明。說明是選填欄位。
4. 在**安裝來源 (ISO)** 方塊中，變更 ISO 檔案位置 (NFS 或 CIFS)。
   OMIVV 只支援以 Server Message Block (SMB) 1.0 版和 SMB 2.0 版為基礎的 CIFS 共用。
   a. 如果您使用 CIFS，則要輸入認證。
5. 從 **ESXi 版本**下拉式清單中選取 ESXi 版本。
   選取正確的 ESXi 版本，以便使用適當的安裝開機指令檔。如果您選取了不正確的 ESXi 版本，部署可能會失敗。
6. 若要確認 ISO 檔案路徑與驗證，請按一下**開始測試**。
   隨即會顯示測試結果。
7. 按一下**完成**。

檢視 ISO 設定檔

1. 在 OMIVV 首頁上，按一下**相容性與部署** > **ISO 設定檔**。
   隨即會顯示包含所有 ISO 設定檔與下列資訊的表格：
   - **設定檔名稱**—設定檔的名稱
   - **說明**—設定檔的說明
   - **安裝來源**—ISO 檔案位置 (NFS 或 CIFS)
   - **ESXi 基底版本**—ESXi 基底版本
2. 如果您要從精靈中移除或新增欄位名稱，請按一下 。
3. 若要匯出 ISO 設定檔資訊，按一下 。

刪除 ISO 設定檔

若您刪除的 ISO 設定檔為執行部署工作的一部份，部署工作將會失敗。

1. 在 OMIVV 首頁上，按一下**相容性與部署** > **設定檔** > **ISO 設定檔**。
2. 選擇 ISO 設定檔，按一下**刪除**。
3. 在確認對話方塊中，按一下**刪除**。

下載自訂的 Dell EMC ISO 映像

部署必須使用包含所有 Dell EMC 驅動程式的自訂 ESXi 映像。

1. 開啟瀏覽器，並前往 **support.dell.com**。
2. 按一下**瀏覽所有產品** > **伺服器** > **PowerEdge**。
3. 按一下 PowerEdge 伺服器機型。
4. 按一下該伺服器機型的**驅動程式與下載**頁面。
5. 從**作業系統**下拉式清單中選取 ESXi 版本。
6. 從**類別**下拉式清單中選取**企業解決方案**。
7. 在**企業解決方案**清單中，選取所需的 ISO 版本，然後按一下**下載**。

10

系統設定檔與 ISO 設定檔部署

若要部署系統設定檔和 ISO 設定檔，請確定您環境中的所有伺服器皆符合下列要求：

- 所有的伺服器皆會顯示於**系統設定檔和 ISO 設定檔部署**精靈內。
- *OpenManage Integration for VMware vCenter 相容性比較表*中提及的特定硬體支援資訊。
- 具有可用的 iDRAC 韌體和 BIOS 最低支援版本。

  如需特定韌體支援資訊，請參閱 *OpenManage Integration for VMware vCenter 相容性比較表*。
- 具有可用的 IDSDM 儲存裝置規格。

  若要瞭解 IDSDM 的儲存規格，請參閱 VMware 說明文件。
- 在以 OMIVV 部署作業系統之前，先從 BIOS 啟用 IDSDM。

  OMIVV 可讓您在 IDSDM、本機硬碟或 BOSS 卡上進行部署。
- 如果 vCenter、OMIVV 和 iDRAC 連線至不同的網路，那麼 vCenter、OMIVV 和 iDRAC 網路之間有路由。

  此要求只適用於 OMIVV 裝置未設定兩個網路介面控制器的情況。
- 已啟用「重新啟動時收集系統清查」(CSIOR)。
- 在開始自動或手動探索之前，為伺服器執行強制重新開機，以確保擷取到最新資料。
- 若要自動探索裸機伺服器，請訂購由原廠預先設定自動探索或交握選項的 Dell EMC 伺服器。如果伺服器沒有預先設定這些選項，您就必須手動輸入 OMIVV IP 位址，或是設定本機網路提供這項資訊。
- 如果 OMIVV 並未用於硬體組態，請在部署作業系統前，先確認是否符合下列條件：
  - 在 BIOS 啟用虛擬化技術 (VT) 旗標。
  - 虛擬驅動程式、IDSDM 和 BOSS 會設為第一個開機磁碟。
- 如果 OMIVV 有用於硬體組態，則即使 BIOS 組態並非系統設定檔的一部份，也請確認系統會自動啟用 VT 的 BIOS 設定。如果目標系統上沒有設定虛擬磁碟機，就需要使用 Express 或 Clone RAID 組態。
- 備好包含所有 Dell EMC 驅動程式的自訂 ESXi 映像，以進行部署。

  在 **support.dell.com** 的**驅動程式與下載**中，下載正確的映像。如需更多有關下載自訂 Dell EMC ISO 映像的相關資訊，請參閱 下載自訂的 Dell EMC ISO 映像 第頁的 55。
- 將自訂影像儲存到 OMIVV 可在部署期間存取的 CIFS 或 NFS 共用位置。

  如需此版本最新的支援 ESXi 版本清單，請參閱 *OpenManage Integration for VMware vCenter 相容性比較表*。

  以下內容適用於部署雙 NIC 的主機：

- 主機可以在同一個網路中或在兩個不同的網路中，採用 iDRAC 和 vCenter 管理 NIC。
- ISO 映像可儲存於任何網路中。
- 請確定選取的是正確的 vCenter 網路和 OMIVV 網路 (適用於環境)。作業系統部署精靈會顯示兩個 OMIVV 網路。

部署檢查清單

在部署系統設定檔和 ISO 設定檔之前，請先確定下列項目可用：

- 主機認證設定檔

  若要建立主機認證設定檔，請按一下**建立**。如需有關建立主機認證設定檔的更多資訊，請參閱建立主機認證設定檔 第頁的 34。
- 裸機伺服器

  若要探索裸機伺服器，請按一下**探索**。如需更多有關探索裸機伺服器的資訊，請參閱裸機伺服器的手動探索 第頁的 49。
- 系統設定檔

  若要建立系統設定檔，請按一下**建立**。如需有關建立系統設定檔的更多資訊，請參閱建立系統設定檔 第頁的 51。
- ISO 設定檔

若要建立 ISO 設定檔，請按一下**建立**。如需有關建立 ISO 設定檔的更多資訊，請參閱建立 ISO 設定檔 第頁的 54。

使用**系統設定檔和 ISO 設定檔部署**精靈，您可執行下列步驟：

- 系統設定檔部署

  如需更多資訊，請參閱部署系統設定檔 (硬體的組態) 第頁的 57。

- ISO 設定檔部署

  如需更多資訊，請參閱部署 ISO 設定檔 (ESXi 安裝) 第頁的 57。

- 系統設定檔與 ISO 設定檔部署

  如需更多資訊，請參閱部署系統設定檔和 ISO 設定檔 第頁的 59。

部署系統設定檔 (硬體的組態)

1. 若要啟動部署精靈，請前往**相容性與部署** > **部署** > **部署**。
2. 在部署精靈的**系統設定檔和 ISO 設定檔部署檢查清單**頁面上，確認部署檢查清單，然後按一下**開始使用**。
   您只能在相容的裸機伺服器上執行部署。如需更多資訊，請參閱 檢視裸機伺服器 第頁的 47。
3. 在**選取伺服器**頁面上，選取一或多個伺服器。
   選擇部署選項頁面隨即顯示。
4. 在**選取部署選項**頁面上，選取**系統設定檔 (硬體的組態)**。
5. 從**系統設定檔**下拉式功能表中，選取適當的系統設定檔，然後按一下**下一步**。
   針對基本和進階系統設定檔案類型，系統設定檔名稱會以下列格式顯示：基本_<系統設定檔名稱>，進階_<系統設定檔名稱>。
   組態預覽工作會嘗試比較或驗證所選系統設定檔與所選主機的相容性。
6. 若要在 iDRAC 上建立預覽工作，請在**組態預覽**頁面上，選取 iDRAC IP，然後按一下**預覽**。組態預覽為選用工作。
   系統設定檔預覽操作可能需要幾分鐘的時間才能完成。比較狀態會顯示在**結果**欄中。

   以下為比較結果：

   - **已完成**—預覽工作已順利執行。如需比較結果的詳細資訊，請按一下**詳細資料**欄中的**檢視詳細資料**。
   - **未完成**—預覽工作未在 iDRAC 上順利執行。請確定 iDRAC 可存取，且在需要時執行 iDRAC 重設。如需工作的詳細資訊，請參閱 OMIVV 記錄和在 iDRAC 主控台的記錄。
7. 在**排程部署工作**頁面上，執行下列步驟：
   a. 輸入部署工作名稱與說明。說明是選填欄位。
   b. 若要立即執行部署工作，請按一下**立即執行**。
   c. 若要將工作排程至稍後執行，請按一下**稍後排程**，然後選取日期和時間。
   d. 選取**提交工作後移至工作頁面**核取方塊。
   您可以在**工作**頁面上追蹤工作的狀態。如需更多資訊，請參閱 部署工作 第頁的 65。
8. 按一下**完成**。

部署 ISO 設定檔 (ESXi 安裝)

您只能在相容的裸機伺服器上執行部署。如需更多資訊，請參閱檢視裸機伺服器 第頁的 47。

1. 若要啟動部署精靈，請前往**相容性與部署** > **部署** > **部署**。
2. 在部署精靈的**系統設定檔和 ISO 設定檔部署檢查清單**頁面上，確認部署檢查清單，然後按一下**開始使用**。
3. 在**選取伺服器**頁面上，選取一或多個伺服器。
   選擇部署選項頁面隨即顯示。
4. 在**選取部署選項**頁面上，選取 **ISO 設定檔 (ESXi 安裝)**。
5. 從 **vCenter 名稱**下拉式功能表中，選取 vCenter 的例項。
6. 若要選取 vCenter 目的地容器，請按一下**瀏覽**，然後選取要部署作業系統的適當資料中心或叢集。
7. 從 **ISO 設定檔**下拉式功能表中，選取適當的 ISO 設定檔。
8. 在**安裝目標**下方，選取下列任何選項：

   - **第一個開機磁碟**—在硬碟機、固態硬碟 (SSD)，或是由 RAID 控制器建立的虛擬磁碟上部署作業系統。

- **內部雙 SD 模組 (IDSDM)**——在 IDSDM 上部署作業系統。如果 IDSDM 可在至少一部所選伺服器上使用，就會啟用 Internal Dual SD Module 選項。如果不可，則只會提供**第一個開機磁碟**選項。
  - 如果任一選取的伺服器未支援 IDSDM 或 BOSS 模組，或者未在部署期間於伺服器中安裝 IDSDM 或 BOSS，則會略過在這些伺服器上執行的部署作業。

    若要在伺服器的第一個開機磁碟上部署作業系統，請選取**將 Hypervisor 部署至沒有內部雙 SD 模組可用之伺服器的第一個開機磁碟**核取方塊。

  註: 第一個開機磁碟安裝目標不等於 BIOS 硬碟機順序或 UEFI 開機順序中的第一個項目。此選項可將作業系統部署至 ESXi 預先作業系統環境所辨識到的第一個磁碟上。當選取**第一個開機磁碟**選項時，請確定已啟用「硬碟容錯移轉」或「開機順序重試」選項。
- **BOSS**——在 BOSS 卡上部署作業系統。如果 BOSS 可在至少一部所選伺服器上使用，就會啟用 BOSS 選項。如果不可，則只會提供**第一個開機磁碟**選項。

  如果您使用 OMIVV 在 BOSS 控制器上部署作業系統，請確定已從參照伺服器擷取系統設定檔以及 BOSS VD 組態，且目標伺服器必須具有採用類似組態的 BOSS。如需更多有關建立 VD 的資訊，請參閱 *《Dell EMC 開機最佳化伺服器儲存-S1 使用者指南》*，網址是：www.dell.com/support。

9. 在**選取主機認證設定檔**設定頁面上，請執行下列作業：
   a. 若要對所有主機使用相同的主機認證設定檔，請按一下**是**，然後執行下列工作：
      i. 從下拉式功能表中選取主機認證設定檔。
      ii. 輸入密碼。

      下列項目適用於部署期間的 root 使用者：
      - 針對 ESXi 6.5 及更舊版本，會使用在主機認證設定檔中輸入的密碼。
      - 針對 ESXi 6.7 及更新版本，會使用在部署精靈中輸入的密碼。
      - 針對 ESXi 6.5 及更早版本，如果主機認證設定檔中未輸入密碼，就會使用在部署精靈中輸入的密碼。更新主機認證設定檔上的 ESXi 認證，以確保在作業系統部署後能順利執行清查。

   b. 若要為每個伺服器選取個別主機認證設定檔，請按一下**否**，然後執行下列工作：
      i. 從下拉式功能表中選取主機認證設定檔。
      ii. 輸入 root 密碼。若要檢視輸入的密碼，請按一下眼睛圖示。

      請確定您輸入正確的密碼，因為無法使用「確認密碼」選項。

   註: 若在主機認證設定檔中將 AD 認證用於 iDRAC 或 ESXi，則這些設定檔不會用於作業系統部署。

   註: 在主機認證設定檔中，建議您將用於探索裸機的使用者建立關聯，否則探索到的使用者會在作業系統部署後的 iDRAC 中停用。
10. 在**進行網路設定**頁面中，執行下列工作：
    a. 為伺服器輸入完整的主機名稱 (FQDN)。主機名稱的完整網域名稱是必要的。FQDN 不得使用 *localhost*。FQDN 是在您將主機新增至 vCenter 時使用。請建立一個使用 FQDN 來解析 IP 位址的 DNS 記錄。設定 DNS 伺服器，以支援反向對應要求。在安排執行部署工作之前，必須先備妥及驗證 DHCP 保留區和 DNS 主機名稱。

       註: 如果 vCenter 使用 FQDN 向 OMIVV 註冊，請確定 ESXi 主機可使用 DNS 解析來解決 FQDN。

    b. 選取用於管理網路的 NIC。請確定 NIC 處於連線狀態。

       註: 請確定您根據與 OMIVV 的網路連線來選取管理 NIC。**套用設定至所有伺服器**選項不適用於管理 NIC 選取。

    c. 選取可存取 vCenter 的 OMIVV 網路例項。如需更多資訊，請參閱 系統設定檔與 ISO 設定檔部署 第頁的 56。
    d. 選取下列任何網路選項：
       - 若為靜態，請輸入偏好的 DNS 伺服器、備用的 DNS 伺服器、IP 位址、子網路遮罩和預設閘道。
       - **使用 VLAN**——當您提供 VLAN ID 時，它會在進行部署時套用至作業系統的管理介面，並在所有流量標上 VLAN ID。伺服器識別會指派新的名稱和網路識別給已部署的伺服器。如需更多資訊，請參閱 VLAN 支援 第頁的 59。
       - **使用 DHCP**——將主機新增至 vCenter 時，會使用 DHCP 指派的 IP 位址。使用 DHCP 時，建議您為所選的 NIC MAC 位址使用 IP 保留區。
11. 在**排程部署工作**頁面上，執行下列步驟：
    a. 輸入部署工作名稱與說明。
    b. 若要立即執行部署工作，請按一下**立即執行**。

c. 若要將工作排程至稍後執行，請按一下**稍後排程**，然後選取日期和時間。
d. 選取**提交工作後移至工作頁面**核取方塊。
您可以在**工作**頁面上追蹤工作的狀態。如需更多資訊，請參閱部署工作 第頁的 65。

12. 按一下**完成**。

註: 在裸機伺服器上執行作業系統部署之後，OMIVV 會清除所有 iDRAC 工作。

在最新版本的 OMIVV 中，以舊版 OMIVV 排定的 ISO 設定檔部署工作將無效。取消排定的工作，並視需要建立部署工作。

如果排定的工作未取消，部署工作便會失敗。在這種情況下，請以裸機探索伺服器，然後建立 ISO 設定檔部署工作。

部署系統設定檔和 ISO 設定檔

您只能在相容的裸機伺服器上執行部署。如需更多資訊，請參閱檢視裸機伺服器 第頁的 47。

1. 若要啟動部署精靈，請前往**相容性與部署** > **部署** > **部署**。
2. 在部署精靈的**系統設定檔和 ISO 設定檔部署檢查清單**頁面上，確認部署檢查清單，然後按一下**開始使用**。
3. 在**選取伺服器**頁面上，選取一或多個伺服器。
選擇部署選項頁面隨即顯示。
4. 在**選取部署選項**頁面上，選取**系統設定檔 (硬體設定)** 和 **ISO 設定檔 (ESXi 安裝)**。
5. 從 **vCenter 名稱**下拉式功能表中，選取 vCenter 的例項。
6. 若要選取 vCenter 目的地容器，請按一下**瀏覽**，然後選取要部署作業系統的適當資料中心或叢集。
7. 若要使用與叢集設定檔 (與所選叢集相關聯) 相關聯的系統設定檔，請按一下**確認**。
   - 若要選取任何其他系統設定檔，請按一下**選取其他**。建議選取與叢集相關聯的系統設定檔，以避免組態相容性漂移。
8. 從 **ISO 設定檔**下拉式功能表中選取適當的 ISO 設定檔，然後按一下**下一步**。
9. 若要在 iDRAC 上建立預覽工作，請在**組態預覽**頁面上，選取 iDRAC IP，然後按一下**預覽**。組態預覽為選用工作。
系統設定檔預覽操作可能需要幾分鐘的時間才能完成。比較狀態會顯示在**結果**欄中。

   以下為比較結果：

   - **已完成**—預覽工作已順利執行。如需比較結果的詳細資訊，請按一下**詳細資料**欄中的**檢視詳細資料**。
   - **未完成**—預覽工作未在 iDRAC 上順利執行。請確定 iDRAC 可存取，且在需要時執行 iDRAC 重設。如需工作的詳細資訊，請參閱 OMIVV 記錄和在 iDRAC 主控台的記錄。

10. 完成部署 ISO 設定檔 (ESXi 安裝) 第頁的 57 主題中所列的工作 7–10。

VLAN 支援

OMIVV 支援在可路由的 VLAN 上部署作業系統，而且您可以在部署精靈中設定 VLAN 支援。在這個部份的部署精靈中，有一個選項可以使用 VLAN ID 指定 VLAN。當您提供 VLAN ID 時，它會在進行部署時套用至作業系統的管理介面，並在所有流量標上 VLAN ID。

請確保部署時所提供的 VLAN 能夠與 OMIVV 裝置和 vCenter Server 兩者通訊。如果 VLAN 的作業系統部署無法與其中一個或兩個目的地通訊，就會導致部署失敗。

如果您在單一部署工作中選取多個裸機伺服器，並希望將同一個 VLAN ID 套用至所有伺服器上，那麼在部署精靈的伺服器識別部份中，請使用**套用設定至所有伺服器**。這個選項可將同一個 VLAN ID 連同其他網路設定，套用到該部署工作中的所有伺服器。

註: 請確定您根據與 OMIVV 的網路連線來選取管理 NIC。**套用設定至所有伺服器**選項不適用於管理 NIC 選取。

部署工作時間

系統設定檔和 ISO 設定檔部署可能需要 30 分鐘到數小時才能完成，取決於多個因素而定。開始部署工作時，建議您根據提供的指南來規劃部署時間。完成系統設定檔和 ISO 設定檔部署所需的時間，會依部署類型、複雜度，以及同時執行的部署工作數目而有所不同。部署工作是以批次執行來改善整體部署工作的時間，上限為五部並行工作的伺服器。確切的並行工作數則要視可用資源而定。

下表顯示平均值，並可能會依伺服器組態、伺服器世代以及已排程部署的裸機伺服器數目等因素而異：

表 3. 單一伺服器的大約部署時間

部署類型	每個部署的約略時間
僅限 ISO 設定檔	介於 30-130
僅限系統設定檔	5–6 分鐘
系統設定檔和 ISO 設定檔	30 – 130 分鐘

部署順序內的伺服器狀態

在自動或手動探索期間探索到的伺服器會劃分為不同的狀態，來協助判斷伺服器對於資料中心是否為新的伺服器，或是有安排擱置中的部署工作。系統管理員可以使用這些狀態來檢查硬體組態狀態。

表 4. 部署順序內的伺服器狀態

伺服器狀態	說明
未設定	伺服器已新增至 OMIVV，並且正在等待設定。
已設定	伺服器已利用成功部署作業系統所需的所有硬體資訊完成設定。

11

相容性

管理相容性

若要在 OMIVV 中檢視和管理主機，每一個主機都必須符合特定準則。如果主機不符合相容性準則，OMIVV 將無法對其進行管理和監控。OMIVV 會詳細顯示不相容主機的詳細資訊，並且讓您修正不相容 (如果適用)。

若有下列情形，則主機即不相容：

- 主機未與主機認證設定檔建立關聯。
- 重新開機時收集系統清查 (CSIOR) 功能已停用或尚未執行，必須手動重新開機。

  註: 當主機使用機箱進行管理時，CSIOR 狀態未判定。
- 主機的 SNMP 陷阱目的地不是設為 OMIVV 裝置的 IP 位址。若 SNMP 陷阱目的地設定失敗，可能是主機認證設定檔中提供的 iDRAC 或主機認證無效。或者，iDRAC 中沒有可用插槽，或是 iDRAC 已開啟鎖定模式 (僅限 iDRAC9 型伺服器)。如需 iDRAC9 型伺服器的清單，請參閱相容性比較表。
- OMIVV 無法啟用在執行 ESXi 6.5 和更新版本的主機上的 WBEM 服務。
- iDRAC 韌體版本低於 2.50.50.50。只有在使用系統設定檔功能的情況下，才需要 iDRAC 版本 2.50.50.50 或更高版本。
- iDRAC 授權不相容 (iDRAC Express 為最低需求)。沒有相容 iDRAC 授權的伺服器無法用於監控和更新韌體。

警示: 即使不相容，相容性測試也不會顯示處於鎖定模式的主機。請務必手動檢查相容性等級。手動檢查時會顯示一則訊息。請忽略該訊息。因為它無法判斷其相容性狀態。請務必手動檢查這些系統的相容性。如果是這種情況，就會顯示警告。

在**管理相容性**頁面上，您可執行下列工作：

- 修正相容性。如需更多資訊，請參閱修正不相容的主機 第頁的 61。
- 執行清查。如果任何與主機認證設定檔相關聯之主機的 iDRAC 狀態是**不相容**或**不明**，則執行清查工作的連結會是作用中。
- 更新 iDRAC 授權。如需更多資訊，請參閱修正 iDRAC 授權相容性 第頁的 62。
- 新增 OEM 主機。如需新增 OEM 主機的更多資訊，請參閱新增 OEM 主機 第頁的 63。

檢視不相容的主機

1. 在 OMIVV 首頁上，按一下**相容性與部署** > **管理相容性**。

隨即會顯示所有不相容主機與下列資訊的表格：

- **主機** — 主機的 FQDN 或 IP 位址
- **機型**—伺服器的型號名稱
- **認證設定檔** — 主機認證設定檔名稱
- **CSIOR 狀態** — CSIOR 狀態 (**開啟**或**關閉**)。若為使用機箱管理的主機，CSIOR 狀態會顯示**未定**。
- **SNMP 設陷狀態** — SNMP 設陷狀態 (**已設定**或**未設定**)。
- **Hypervisor**—Hypervisor 的名稱與版本
- **WBEM 狀態** — WBEM 狀態 (**相容**或**不相容**)。若為使用機箱管理的主機，CSIOR 狀態會顯示**不適用**。
- **iDRAC 韌體版本**—iDRAC 的韌體版本
- **iDRAC 授權狀態** — iDRAC 授權狀態 (**相容**或**不相容**)。

  註: 當使用機箱認證設定檔來管理 PowerEdge MX 主機時，iDRAC 的韌體版本會在**管理相容性**頁面上顯示為**不適用**。這是因為 iDRAC 的韌體相容性不適用於 iDRAC9 型伺服器。如需 iDRAC9 型伺服器的清單，請參閱相容性比較表。

修正不相容的主機

若有下列情形，則主機即不相容：

- 主機未與主機認證設定檔建立關聯。

- 重新開機時收集系統清查 (CSIOR) 功能已停用或尚未執行，必須手動重新開機。

  註: 當主機使用機箱進行管理時，CSIOR 狀態未判定。
- 主機的 SNMP 陷阱目的地不是設為 OMIVV 裝置的 IP 位址。若 SNMP 陷阱目的地設定失敗，可能是主機認證設定檔中提供的 iDRAC 或主機認證無效。或者，iDRAC 中沒有可用插槽，或是 iDRAC 已開啟鎖定模式 (僅限 iDRAC9 型伺服器)。如需 iDRAC9 型伺服器的清單，請參閱相容性比較表。
- OMIVV 無法啟用在執行 ESXi 6.5 和更新版本的主機上的 WBEM 服務。
- iDRAC 韌體版本低於 2.50.50.50。只有在使用系統設定檔功能的情況下，才需要 iDRAC 版本 2.50.50.50 或更高版本。
- iDRAC 授權不相容 (iDRAC Express 為最低需求)。沒有相容 iDRAC 授權的伺服器無法用於監控和更新韌體。

1. 在 OMIVV 首頁上，按一下**相容性與部署** > **管理相容性**。
2. 選取不相容的主機，按一下**修正相容性**。
3. 閱讀精靈中歡迎頁面上的指示，然後按一下**開始使用**。
4. 在**選取主機**頁面上，選取一個或多個不相容主機，然後按一下**下一步**。
   - 如果主機未與主機認證設定檔建立關聯，將會顯示下列警告訊息：

     有未指派給認證設定檔的已選取主機。若要允許 OMIVV 執行相容性檢查，您必須將這些主機新增到主機認證設定檔

     若要排除未指派給主機認證設定檔的主機，請按一下**繼續**。

     若要將主機新增至主機認證設定檔頁面，請按一下**取消**，然後前往主機認證設定檔頁面。如需有關建立主機認證設定檔的更多資訊，請參閱建立主機認證設定檔 第頁的 34。

     在 MX 機箱中已停用 iDRAC IPv4 的主機，必須使用機箱認證設定檔進行管理。若要將這些主機與機箱認證設定檔建立關聯，您必須使用在 **Dell EMC 機箱**中的「新增 MX 機箱」來新增機箱，並建立機箱與機箱認證設定檔的關聯。

   若要更新 iDRAC 韌體與 BIOS 版本：

   a. 在 **更新 iDRAC 韌體與 BIOS 版本**頁面上，選取一個或多個您想要更新韌體版本的主機。
   b. 按一下**下一步**。
   c. 在**主機重新開機**頁面上，檢視必須重新開機的 ESXi 主機。
   d. 如果您要自動將主機置於維護模式，並且在必要時重新開機，請選取核取方塊，然後按一下**下一步**。
   e. 檢閱**摘要**頁面上的動作摘要，然後按一下**完成**。

   若要開啟 CSIOR：

   a. 在**選取主機**頁面上，選取一個或多個不相容主機，然後按一下**下一步**。
   b. 在**開啟 CSIOR** 頁面上，選取一個或多個您想要開啟 CSIOR 的主機，然後按一下**下一步**。
   c. 檢閱**摘要**頁面上的動作摘要，然後按一下**完成**。

   您在主機認證設定檔中提供有效資訊而修正 iDRAC 或主機認證後，或使 iDRAC 陷阱目的地中前四個插槽之一可用，或停用 iDRAC 中的系統鎖定模式，則精靈會將 SNMP 陷阱目的地狀態設定為**已設定**。

   註: 系統鎖定模式僅適用於 iDRAC9 型伺服器。

   如果有 WBEM 不相容的主機存在，請確認手動修正導致 WBEM 服務啟用失敗的主機狀況。您可在使用者記錄中查看錯誤狀況，以加以修正。在清查期間，啟用 OMIVV 以啟用這些主機的 WBEM 服務。

修正 iDRAC 授權相容性

相容的 iDRAC 授權是主機的相容性準則之一。如果主機沒有相容的 iDRAC 授權，則在**管理相容性**頁面上，這些主機將會列為不相容的主機。

您可以按一下不相容主機以查看詳細資料，例如 iDRAC 到期日、授權類型和授權說明。如果與主機認證設定檔相關聯之任何主機的 iDRAC 相容性狀態是**不相容**或**不明**，則**執行清查**會在作用中。

1. 若要修復 iDRAC 授權相容性，請在 OMIVV 首頁上，按一下**相容性和部署** > **相容性** > **管理相容性**。
2. 選取 iDRAC 授權不相容的主機，然後按一下**更新 IDRAC 授權**。
3. 登入 Dell Digital Locker，並更新或購買新的 iDRAC 授權。
   安裝 iDRAC 授權後，請針對主機執行清查工作，待清查工作順利完成後，再回到此頁面。

支援 OEM 伺服器

OEM 伺服器由 Dell EMC 合作夥伴提供，他們提供類似於 PowerEdge 伺服器的功能或產品組合。

- 從 OMIVV 4.3 起支援 OEM 的機架式伺服器。
- 透過**新增 OEM 主機**精靈新增 OEM 伺服器。如需新增 OEM 主機的更多資訊，請參閱新增 OEM 主機 第頁的 63。

  註: 如果已在 OEM 主機上啟用 WBEM 服務，並新增至 vCenter，OMIVV 依預設會將這些 OEM 伺服器新增至 OMIVV 管理清單中。建立主機與主機認證設定檔的關聯，以管理這些伺服器。如需建立主機認證設定檔的更多資訊，請參閱建立主機認證設定檔 第頁的 34。
- 在新增 OEM 伺服器後，所有主機管理程序將類似於 Dell EMC PowerEdge 伺服器的管理方式。
- 透過 iDRAC，也可在 OEM 伺服器上支援裸機和部署功能流程。

新增 OEM 主機

除了 Dell EMC PowerEdge 伺服器外，OMIVV 也支援經過品牌重塑以及解除品牌的伺服器。如需 OEM 的更多資訊，請參閱 https://www.dellemc.com。

如果已啟用 WBEM 服務，OMIVV 會判斷主機的 iDRAC 連線能力。如果有連線可用，OMIVV 會將該主機新增至受管理清單。

如果 OMIVV 無法作出判斷，您必須在**新增 OEM 主機**精靈中手動選取該主機，以便將其新增至 OMIVV 管理清單中。

如果 WBEM 服務已停用或 iDRAC 無法連線，請使用**新增 OEM 主機**精靈，以便將主機新增至 OMIVV 管理清單中。

1. 在 OMIVV 首頁上，按一下**相容性與部署** > **相容性** > **管理相容性** > **新增 OEM 主機**。
2. 在**新增 OEM 主機**視窗中，從 **vCenter 例項**下拉式清單中選取 vCenter 的例項。
3. 從**主機認證設定檔**下拉式清單中選取適當的主機認證設定檔。
4. 若要新增或移除相關聯的主機，請按一下**新增主機**。
   選取主機視窗隨即顯示。
5. 在**選取主機**視窗中，選取主機，然後按一下**是**。

   註: 只有不受 OMIVV 管理的主機會顯示在**選取主機**視窗中。

   OMIVV 會自動測試連線測試連線，且結果會顯示在**新增 OEM 主機**視窗中。

   iDRAC 測試與**主機測試**欄會顯示 **iDRAC 認證**與**主機認證**的測試連線結果。

   若要停止測試連線，按一下**中止測試**。
6. 按一下**確定**。
   所選的主機會新增至選取的主機認證設定檔，並觸發清查。

組態相容性

組態相容性頁面會根據與叢集設定檔相關聯之所有叢集的漂移偵測顯示相容性狀態。在有多個 vCenter 伺服器的 PSC 環境中，組態相容性頁面會列出屬於以相同裝置註冊的相同 PSC 的所有 vCenter 的所有叢集。

- 「硬體組態相容性」—顯示用於叢集設定檔之系統設定檔與屬於叢集一部份之關聯主機之間屬性的漂移。
- 「韌體相容性」—顯示用於叢集設定檔之韌體儲存庫設定檔與屬於叢集一部份之關聯主機之間的韌體版本漂移。
- 「驅動程式相容性」—顯示用於叢集設定檔之驅動程式儲存庫設定檔與屬於叢集設定檔一部份之關聯 vSAN 主機之間的驅動程式版本漂移。

檢視組態相容性

1. 在 OMIVV 首頁上，按一下**相容性與部署** > **相容性** > **組態相容性**。
   表格會顯示具有相關聯叢集設定檔、系統設定檔、韌體儲存庫設定檔和驅動程式儲存庫設定檔的叢集。

   針對基本和進階系統設定檔類型，系統設定檔名稱會以下列格式顯示：基本_<系統設定檔名稱>、進階_<系統設定檔名稱>。
2. 在**組態相容性**頁面上，選取一個叢集。
   會顯示組態相容性資訊和相容性狀態。

   組態相容性區段會顯示下列資訊：

   - **叢集名稱**—叢集的名稱
   - **相容性狀態**—表示相容的狀態 (相容或不相容)。如果叢集中任何主機不相容，狀態便會顯示為不相容。
   - **主機數量**—在叢集中存在的主機總數量

- **排程**—下一個排程漂移偵測工作的日期和時間。
- **上次漂移偵測時間**—上次漂移偵測工作完成的日期和時間。

相容性狀態區段會顯示硬體、韌體和驅動程式元件的相容性狀態。不同的相容性狀態為：

- **相容**—顯示相容於關聯的硬體、韌體和驅動程式元件的主機計數。
- **不相容**—顯示不相容於關聯的硬體、韌體和驅動程式元件的主機計數。
- **不適用**—顯示不適用的主機計數。

  硬體漂移不適用於透過機箱認證設定檔管理的主機。

  驅動程式漂移不適用於做為 vSphere 叢集一部分的主機。

  若使用線上目錄建立叢集設定檔，則韌體相容性不適用於 vSAN 叢集。

3. 若要檢視漂移詳細資料，請按一下**檢視漂移報告**。該連結僅為不相容的叢集而啟用。如需有關更多檢視漂移報告的資訊，請參閱檢視漂移報告 第頁的 64。

檢視漂移報告

組態相容性報告頁面會顯示硬體、韌體和驅動程式元件的漂移詳細資料。

漂移偵測工作狀態會顯示在**摘要**中。

硬體：

- 主機名稱或 IP—代表主機 IP 或主機名稱。
- 產品服務編號—代表主機的產品服務編號。
- 漂移狀態—代表漂移狀態 (不相容或失敗)。
- 例項 — 代表硬體元件名稱。
- 群組 — 代表屬性的群組名稱。
- 屬性名稱 — 代表屬性名稱。
- 目前值—代表主機中屬性目前的值。
- 基準值 — 代表基準值。
- 漂移類型/錯誤—表示不相容的原因。如需漂移類型的詳細資訊，請參閱元件與基準版本比較表 第頁的 151。

註: 只有當主機或 iDRAC 無法連線時，漂移偵測工作才會失敗。如果主機或 iDRAC 已成功清查，則漂移偵測工作會顯示成功。若要檢查任何其他漂移偵測工作失敗的原因，請參閱漂移報告中的**漂移類型/錯誤**欄位。

韌體和驅動程式：

- 主機名稱或 IP—代表主機 IP 或主機名稱。
- 產品服務編號—代表主機的產品服務編號。
- 漂移狀態—表示漂移狀態。
- 元件名稱 — 代表元件的名稱。
- 目前值—代表主機中屬性目前的值。
- 基準值 — 代表基準值。
- 漂移類型/錯誤—表示不相容的原因。如需漂移類型的詳細資訊，請參閱元件與基準版本比較表 第頁的 151。
- 嚴重性 (韌體)—代表更新所識別元件版本的重要性等級。
- 建議 (驅動程式)—表示驅動程式元件的更新建議。

註: 如果有一個以上的韌體版本可用，系統一律將最新的韌體版本用於相容性比較。

您可以使用篩選選項，根據漂移狀態來檢視漂移的詳細資料。

註: 在 5.x 中不支援 32 位元的韌體套裝。如果在 4.x 版本中，叢集設定檔與 32 位元的韌體套裝建立關聯，則當您執行備份並從 4.x 還原至 5.x 時，漂移狀態會顯示為失敗。使用有叢集設定檔的 64 位元韌體套裝，然後重新執行漂移偵測工作。

註: OMIVV 與 vSphere Lifecycle Manager 間的漂移報告可能會出現不相符的情況。這是因為 vSphere Lifecycle Manager 會一直顯示即時漂移報告，而 OMIVV 則會根據排定日期和時間顯示漂移報告。如果您在漂移報告中發現不相符的情況，請在**漂移偵測工作**頁面上，隨需執行漂移偵測工作。

12

管理 OMIVV 工作

工作頁面會顯示下列工作：

- 部署
- 探索
- 韌體更新
- 系統鎖定模式
- 漂移偵測
- 清查
- 保固

包括使用者建立的 (如部署工作) 和 OMIVV 建立的 (例如健全狀況指標收集工作) 工作，當工作總數達到 500 時，OMIVV 便會清除較舊的工作。如果工作總數超過 500，則會刪除較舊的 500 項工作。

部署工作

部署工作完成後，您可以在**部署工作**頁面上追蹤部署工作的狀態。

1. 在 OMIVV 首頁上，按一下**設定** > **部署工作**。
   隨即會顯示包含所有部署工作與下列資訊的表格：
   - **名稱**—部署工作的名稱
   - **說明**—工作說明
   - **排程時間**—排定工作的日期和時間。
   - **狀態**—部署工作的狀態
   - **集合大小**—部署工作中的伺服器數量
   - **進度摘要**—部署工作的工作進度詳細資料
2. 若要檢視更多有關部署工作中伺服器的資訊，請選取部署工作。
   以下資訊會顯示在下方窗格中：
   - **產品服務編號**
   - **iDRAC IP**
   - **狀態**
   - **警告**
   - **詳細資料**
   - **開始日期與時間**
   - **結束日期與時間**
   - **更多詳細資料**

   a. 若要查看更多有關部署工作的資訊，請選取工作，並將指標暫停在**詳細資料**欄處。
   b. 如需檢視更多關於系統設定檔工作失敗的資料，請按一下**更多詳細資料**。
      下列資訊隨即顯示：
      - 元件的 FQDD
      - 屬性的值
      - 舊值
      - 新值
      - 失敗相關訊息和訊息 ID (有幾種類型的錯誤不會顯示)

      少數顯示於**套用系統設定檔 - 失敗詳細資料**視窗的**屬性名稱**底下的屬性，與您按一下**更多詳細資料**時系統設定檔所顯示的屬性名稱不同。
3. 若要停止部署工作，請按一下**停止**。
4. 若要清除部署工作，請按一下**清除已完成**，選取**早於日期和工作狀態**，然後按一下**套用**。
   選定的工作隨後會從**部署工作**頁面中清除。

探索工作

探索任務建立後，您可以在**探索工作**頁面上追蹤工作狀態。

1. 在 OMIVV 首頁上，按一下**工作** > **探索工作**。
   隨即會顯示包含所有探索工作與下列資訊的表格：
   - **名稱**—探索工作的名稱
   - **說明**—工作說明
   - **排程時間**—排定工作的日期和時間。
   - **狀態**—探索工作的狀態。

     當成功探索到伺服器時，工作狀態便會顯示成功。

     如果工作失敗，則會顯示失敗的原因。
   - **集合大小**—探索工作中的伺服器數量
   - **進度摘要**—探索工作的工作進度詳細資料
2. 若要檢視更多資訊，請選取一項探索工作。
   以下資訊會顯示在下方窗格中：
   - **iDRAC IP**
   - **狀態**
   - **詳細資料**
   - **開始日期與時間**
   - **結束日期與時間**
3. 若要清除探索工作佇列，請按一下**清除已完成**。
   a. 選取日期。
      將刪除早於所選日期的工作。
   b. 選取工作的狀態。
   c. 按一下**套用**。

機箱韌體更新工作

機箱韌體更新工作完成後，您可以在**機箱韌體更新工作**頁面上檢視韌體更新工作的狀態。

1. 在 OMIVV 首頁上，按一下**工作** > **韌體更新** > **機箱韌體更新**。
2. 若要檢視最新記錄資訊，請按一下重新整理圖示。
   隨即會顯示包含所有主機認證設定檔與下列資訊的表格：
   - **狀態**—韌體更新工作的狀態
   - **排程時間**—排定的韌體更新工作時間
   - **名稱**—工作的名稱
   - **說明**—韌體更新工作的說明
   - **vCenter**—vCenter 名稱
   - **集合大小**—韌體更新工作中的機箱數量

     機箱總數僅包括主要和獨立機箱。成員機箱不含在內。
   - **進度摘要**—韌體更新工作的進度詳細資料
3. 若要檢視特定工作的更多詳細資訊，請選取工作。
   以下資訊會顯示在下方格線中：
   - **機箱產品服務編號**—機箱的產品服務編號
   - **狀態**—工作的狀態
   - **開始時間**—韌體更新工作的開始時間
   - **結束時間**—韌體更新工作的結束時間
4. 如果想要停止已排程但未執行的韌體更新，請選取您要停止的工作，然後按一下**停止**。
   警告: 如果您停止已經提交至 MX 機箱的韌體更新工作，則主機上的韌體仍可能會更新。OMIVV 會將工作報告為已取消。
5. 如果要清除更早的韌體更新工作或已安排好的韌體更新，請按一下**清除已完成**。

隨即顯示**清除韌體更新工作**對話方塊。您只能清除已取消、成功或已失敗的工作，無法清除已排程或進行中的工作。

6. 在**清除韌體更新作業**對話方塊中，選取**早於**，然後按一下**確定**。
   選定的工作隨後會從**機箱韌體更新**工作清單中清除。

主機韌體更新工作

機箱韌體更新工作完成後，您可以在**主機韌體更新工作**頁面中檢視韌體更新工作的狀態。

1. 在 OMIVV 首頁上，按一下**工作** > **韌體更新** > **主機韌體更新**。
2. 若要檢視最新記錄資訊，請按一下重新整理圖示。
   隨即會顯示包含所有主機韌體更新工作與下列資訊的表格：
   - **狀態**—韌體更新工作的狀態
   - **排程時間**—排定的韌體更新工作時間
   - **名稱**—工作的名稱
   - **說明**—韌體更新工作的說明
   - **vCenter**—vCenter 名稱
   - **集合大小**—韌體更新工作中的伺服器數量
   - **進度摘要**—韌體更新工作的進度詳細資料
3. 若要檢視特定工作的更多詳細資訊，請選取工作。
   以下資訊會顯示在下方格線中：
   - **主機名稱**—主機的產品服務編號
   - **狀態**—工作的狀態
   - **開始時間**—韌體更新工作的開始時間
   - **結束時間**—韌體更新工作的結束時間

   註: 如果韌體更新工作已使用多個 Dell Update Packages 排程，且 OMIVV 無法下載部分選取的更新套件，則 OMIVV 將繼續更新已成功下載的套件。工作頁面會顯示已成功下載套件的狀態。
4. 如果想要停止已排程但未執行的韌體更新，請選取您要停止的工作，然後按一下**停止**。

   警告: 如果您停止已經提交至 iDRAC 的韌體更新工作，則主機上的韌體仍可能會更新。OMIVV 會將工作報告為已取消。
5. 如果要清除更早的韌體更新工作或已安排好的韌體更新，請按一下**清除已完成**。
   隨即顯示**清除韌體更新工作**對話方塊。您只能清除已取消、成功或已失敗的工作，無法清除已排程或進行中的工作。
6. 在**清除韌體更新作業**對話方塊中，選取**早於**，然後按一下**確定**。
   選定的工作隨後會從**主機韌體更新**工作清單中清除。

系統鎖定模式工作

系統鎖定模式設定僅支援 iDRAC9 型伺服器。設定開啟時會鎖定系統組態，包括韌體更新。此設定是專門為了保護系統避免意外變更。您可以使用 OMIVV 裝置或從 iDRAC 主控台，為受管理之主機開啟或關閉系統鎖定模式。從 OMIVV 4.1 和更新版本開始，您可以設定和監控伺服器中 iDRAC 的鎖定模式。此外，iDRAC 必須有企業授權才能啟用鎖定模式。

註: 您無法變更使用機箱認證設定檔管理之主機的系統鎖定模式。

在完成系統鎖定組態之後，您可以檢視**系統鎖定模式工作**頁面中鎖定模式的更新狀態。

1. 在 OMIVV 首頁上，按一下**工作** > **系統鎖定模式**。
   隨即會顯示包含所有系統鎖定模式工作與下列資訊的表格：
   - **名稱**—系統鎖定模式工作名稱
   - **說明**—工作說明
   - **排程時間**—系統鎖定模式工作排定的日期和時間。
   - **vCenter**—vCenter 名稱
   - **狀態**—系統鎖定模式工作的狀態
   - **集合大小**—系統鎖定模式工作中的伺服器數量
   - **進度摘要**—系統鎖定模式工作的工作進度詳細資料
2. 若要檢視有關系統鎖定模式工作中伺服器的詳細資訊，請選取系統鎖定模式工作。
   以下資訊會顯示在下方格線中：

- **產品服務編號**
- **iDRAC IP**
- **主機名稱**
- **狀態**
- **詳細資料**
- **開始日期與時間**
- **結束日期與時間**

若要檢視有關系統鎖定模式工作的詳細資訊，請選取工作，並將指標暫停在**詳細資料**欄。

3. 若要清除系統鎖定模式工作，請按一下**清除已完成**，接著選取**早於日期和工作狀態**，然後按一下**套用**。
選定的工作隨後會從**系統鎖定模式**工作頁面中清除。

漂移偵測工作

執行漂移偵測工作的目的，是為了比較經驗證的基準及伺服器組態，其中包括硬體組態、韌體和驅動程式版本。

註: 只有當主機或 iDRAC 無法連線時，漂移偵測工作才會失敗。如果主機或 iDRAC 已順利清查，則漂移偵測工作將會順利執行，您可以在漂移報告中檢視漂移詳細資料。如需更多有關漂移報告的資訊，請參閱檢視漂移報告 第頁的 64。

1. 在 OMIVV 首頁上，按一下**工作** > **漂移偵測**。
隨即會顯示包含所有漂移偵測工作與下列資訊的表格：
   - **名稱**—漂移偵測工作的名稱
   - **上次執行**—上次漂移偵測工作執行的日期與時間。
   - **下次執行**—下次漂移偵測工作排定的日期和時間。
   - **狀態**—漂移偵測工作的狀態
   - **集合大小**—漂移偵測工作中的伺服器數量
   - **進度摘要**—漂移偵測工作的進度詳細資料
2. 若要檢視已更新的漂移偵測工作詳細資料，請按一下**重新整理**。
3. 若要檢視有關漂移偵測工作中伺服器的詳細資訊，請選取漂移偵測工作。下列資訊隨即顯示：
   - 產品服務編號
   - iDRAC IP
   - 主機名稱
   - 叢集
   - vCenter
   - 狀態
   - 開始日期與時間
   - 結束日期與時間
4. 若要隨需執行**漂移偵測**工作，請按一下**立即執行**。
在基準叢集中，將主機新增至主機認證設定檔或機箱認證設定檔之後，便會在新增的主機上自動執行漂移偵測工作。

檢視主機清查工作

主機清查頁面會針對與主機認證設定檔相關聯的主機，顯示在該主機上執行之最新清查工作的相關資訊。

1. 在 OMIVV 首頁上，按一下**工作** > **清查** > **主機清查**。
2. 選取 vCenter 來檢視所有相關聯的主機清查工作資訊。
   - **vCenter**—vCenter FQDN 或 IP 位址
   - **已通過主機**—清查成功的主機數量
   - **上次清查**—上一次執行清查的日期與時間
   - **下次清查**—下一次排定清查的日期與時間

   下窗格會顯示相關聯的主機詳細資料。
   - **主機**—主機的 FQDN 或 IP 位址
   - **狀態**—主機的清查狀態。選項包括：
     - **成功**

  - **Fail**
  - **進行中**
- **持續時間 (分:秒)**——以分和秒為格式的清查工作持續時間
- **開始日期和時間**——清查工作開始的日期和時間
- **結束日期和時間**——清查工作完成的日期和時間

執行清查工作

初始組態完成後，所有新增至主機認證設定檔的主機都會自動觸發清查。

1. 若要隨需執行清查，請按一下**工作** > **清查** > **主機清查**。
2. 按一下**立即執行**。
3. 若要查看清查工作的狀態，請按一下**重新整理**。
   清查工作完成後，您可以在 **OMIVV 主機資訊**頁面查看主機資訊。
4. 若要檢視 OMIVV 主機資訊，請展開**功能表**，然後選取**主機和叢集**
5. 在左窗格中，選取任何主機。
6. 在右窗格中，選取**監控**，然後展開 **OMIVV 主機資訊**。
   下列資訊隨即顯示：
   - 硬體清單
   - 儲存
   - 韌體
   - 電源監視
   - 保固
   - 系統事件記錄

   當主機是使用機箱認證設定檔進行管理時，韌體清查資料會顯示幾個額外元件，例如 Lifecycle Controller 和軟體 RAID。

   註: 清查工作會略過超過授權限制的主機，並標示為「失敗」。
7. 在**摘要**頁面的 **OMIVV 主機資訊**區段中，您也可以執行下列動作：
   - 啟動遠端存取主控台 (iDRAC)
   - 閃爍伺服器 LED 指示燈
   - 設定系統鎖定模式

     當主機使用機箱進行管理時，不支援設定系統鎖定模式。
   - 執行韌體精靈

修改主機清查工作

將主機關聯到主機認證設定檔後，必須定期排程清查，以確保主機的清查資訊為最新資訊。「清查工作」會顯示主機上所執行之清查工作的狀態。

您也可以從**設定** > **資料擷取排程** > **清查擷取**頁面修改清查排程。

1. 在**工作**頁面上，選取一個 vCenter 例項，然後按一下**編輯排程**。
   清查資料擷取對話方塊會隨即顯示。
2. 在**清查資料**區段下，執行下列步驟：
   a. 選取**啟用清查資料擷取 (建議)** 核取方塊。
   b. 選取清查資料擷取日期與時間，然後按一下**套用**。
   c. 若要重設設定值，按一下**清除**。
   d. 如要立即執行清查工作，在**工作**頁面上，按一下**立即執行**。

   註: 若為不具備 iDRAC Express 或 Enterprise 授權的伺服器，清查會因 iDRAC 需要升級授權而失敗。

   註: 執行模組化主機清查時，會自動探索對應的機箱。如果機箱為機箱認證設定檔的一部分，機箱清查會在主機清查後自動執行。

檢視機箱清查工作

機箱清查頁面會針對與機箱認證設定檔相關聯的機箱，顯示在該機箱上執行之最新清查工作的相關資訊。

1. 在 OMIVV 首頁上，按一下**工作** > **清查** > **機箱清查**。
2. 若要檢視機箱清查資訊，請選取機箱。
   - **機箱 IP/主機名稱**—機箱的 IP 位址
   - **產品服務編號**—機箱的產品服務編號。產品服務編號是製造商基於支援與維修用途所提供的唯一識別符。
   - **狀態**—機箱的狀態
   - **持續時間 (分:秒)**—以分和秒為格式的工作持續時間
   - **開始日期和時間**—清查工作開始的日期和時間。
   - **結束日期和時間**—清查工作完成的日期和時間

   在 MCM 群組中，清查只會在主要機箱上執行。清查資訊可同時提供主要機箱和成員機箱的相關資料。

   註: 下列 PowerEdge 伺服器不支援機箱清查工作：C6320P、C6320、C4130 和 C6420。

   註: MX 機箱刀鋒伺服器僅支援搭配 ESXi 6.5U2 及更高版本。如果這些主機是部署舊版 ESXi，OMIVV 中的清查工作便會失敗。

執行機箱清查工作

1. 在 OMIVV 首頁上，按一下**工作** > **機箱清查**。
2. 選取機箱，然後按一下**立即執行**。
   機箱清查完成後，您可以在**主機與機箱** > **機箱**頁面上，檢視機箱資訊。
3. 若要檢視機箱資訊，請在**機箱**頁面上選取一個機箱，然後按一下**檢視**。

   註: 在清查期間，OMIVV 會在 MCM 群組的主要機箱上設定陷阱目的地和警示原則。

   註: 當主機使用機箱進行管理時，執行機箱清查也會觸發主機的主機清查。此外，執行主機清查會觸發機箱清查。

檢視主機保固

保固工作是一項預先安排好的工作，可在所有系統上從 www.dell.com/support 取得保固資訊。請確認 OMIVV 裝置具有網際網路連線能力，才能擷取保固資訊。根據網路設定而定，OMIVV 可能需要代理資訊才能連上網際網路並擷取保固資訊。代理詳細資料可在管理主控台中更新。

1. 在 OMIVV 首頁上，按一下**工作** > **保固** > **主機保固**。
2. 選取 vCenter 來檢視相關聯的主機資訊。
   - **vCenter**—vCenter 清單
   - **已傳送的主機**—已傳送的 vCenter 主機數量
   - **上次保固**—上一次執行保固工作的日期與時間。
   - **下次保固**—下一次執行保固工作的日期與時間。

   下方窗格會顯示相關聯的主機資訊。
   - **主機**—主機 IP 位址
   - **狀態**—保固工作的狀態。選項包括：
     - 成功
     - Fail
     - 進行中
     - 已排程
   - **持續時間 (分:秒)**—以「分:秒」為格式的保固工作持續時間
   - **開始日期和時間**—保固工作開始的日期和時間
   - **結束日期和時間**—保固工作結束的時間

3. 若要隨需執行主機保固，請按一下**立即執行**。

修改主機保固工作

保固工作最初是在**初始組態精靈**中設定。您也可以從**設定** > **資料擷取排程** > **保固擷取**頁面上，修改保固工作排程。

1. 在**工作**頁面上，展開**保固**，然後選取**主機保固**。
2. 選取 vCenter，然後按一下**編輯排程**。
3. 在**保固資料**區段下方，執行下列步驟：
   a. 選取**啟用保固資料擷取 (建議)** 核取方塊。
   b. 選取保固資料擷取的日期與時間，然後按一下**套用**。
   c. 若要重設設定值，按一下**清除**。

檢視機箱保固

保固工作是一項預先安排好的工作，可在所有系統上從 support.dell.com 取得保固資訊。OMIVV 裝置必須具有網際網路連線能力，才能擷取保固資訊。請確認 OMIVV 裝置具有網際網路連線能力。根據網路設定而定，OMIVV 可能需要 Proxy 資訊才能連上網際網路並擷取保固資訊。Proxy 詳細資料可在管理主控台中更新。

1. 在 OMIVV 首頁上，按一下**工作** > **保固** > **機箱保固**。
   隨即會顯示所有機箱保固工作資訊的表格：
   - **機箱 IP/主機名稱**——主機 IP 位址
   - **產品服務編號**——機箱的產品服務編號
   - **狀態**—保固工作的狀態。選項包括：
     - 成功
     - Fail
     - 進行中
     - 已排程
   - **持續時間 (分:秒)**—以「分:秒」為格式的保固工作持續時間
   - **開始日期和時間**—保固工作開始的日期和時間。
   - **結束日期和時間**——保固工作結束的時間。
2. 若要隨需執行機箱保固工作，請按一下**立即執行**。

13

管理記錄

檢視記錄歷史記錄

1. 在 **OpenManage Integration for VMware vCenter** 頁面上，若要檢視所有的記錄，請按一下**記錄**。
   OMIVV 記錄擷取程序會從其資料庫中擷取所有記錄。這可能需要幾秒鐘，視記錄大小而定。

   - 若要匯出紀錄資料，請按一下 。
   - 若要排序格線中的資料，請按一下欄標題。
   - 若要在頁面間瀏覽，按一下「上一頁」和「下一頁」圖示。
   - 若要重新整理記錄，按一下左上角的「重新整理」圖示。

2. 按一下▼以根據下列類別及/或日期範圍篩選記錄：
   類別：

   - **所有類別**
   - **資訊**
   - **警告**
   - **錯誤**

   日期：

   - **上週**
   - **上個月**
   - **去年**
   - **自訂範圍**：如果您選取此選項，請按一下日曆圖示以指定開始與結束日期。

3. 選取需要的類別與日期後，按一下**套用**。
   您可以檢視與選取的類別及/或日期範圍相關的紀錄。記錄資料表格每次會在一頁中顯示 100 個記錄。
4. 如要清除篩選後的資料，請按一下**清除篩選**。

14

管理 OMIVV 裝置設定

在**設定**頁面上，您可以執行下列工作：

- 進行保固到期通知設定。如需更多資訊，請參閱設定保固到期通知 第頁的 73。
- 設定最新應用裝置版本通知。如需更多資訊，請參閱設定最新裝置版本通知 第頁的 73。
- 覆寫主動式 HA 警示的嚴重程度。如需更多資訊，請參閱覆寫狀況更新通知的重要性 第頁的 76。
- 初始組態。如需更多資訊，請參閱 初始組態 第頁的 77
- 設定與檢視事件和警報。如需更多資訊，請參閱設定事件與警報 第頁的 81。
- 排程或修改清查和保固的資料擷取排程。如需更多資訊，請參閱 排程清查工作 第頁的 89 和 排程保固擷取工作 第頁的 89。

管理多個裝置

如果多個 vCenter 例項共用相同的 PSC 且註冊 OMIVV 裝置一個以上的執行個體，便可使用此切換裝置精靈在不同的 OMIVV 執行個體間切換。

您可以在首頁上看到目前的 OMIVV 例項。

1. 在 **OMIVV** 首頁上，按一下**變更**。
   - **IP/名稱**—OMIVV 裝置的 FQDN 或 IP
   - **版本**—OMIVV 裝置的目前版本
   - **相容性狀態**—OMIVV 裝置依照其版本而呈現的狀態 (**相容**或**不相容**)
   - **可用性狀態**—根據 OMIVV 服務是否正在執行而呈現的 OMIVV 裝置可用狀態。顯示**良好**或**錯誤**以表示 OMIVV 的工作狀態。
   - **已註冊的 vCenter 伺服器**—已註冊之 vCenter 伺服器的 FQDN 或 IP
   - **動作**—動作名稱 (**選取**或**已選取**)
2. 在**切換 OMIVV 裝置**頁面上，按一下 **選取**。
3. 按一下**是**加以確認。
   您可在首頁檢視裝置 IP 位址中的變更。

設定保固到期通知

如果有任何主機的保固即將到期，請啟用保固到期通知以取得通知。

1. 在 OMIVV 首頁中，按一下**設定** > **通知** > **保固到期通知**。
2. 選取**為主機啟用保固過期通知**。
3. 選取在保固到期前要收到通知的天數。
4. 按一下**套用**。

設定最新裝置版本通知

若要取得有關 OMIVV 新版本可用性的通知，請選取**啟用最新版本通知 (建議)** 核取方塊。建議您每週檢查一次。若要使用 OMIVV 的最新裝置版本通知功能，您必須具備網際網路連線。如果您的環境需要 Proxy 才能連線至網際網路，請確定在系統管理員入口網站上設定 Proxy 設定。

若要接收提供最新版本 OMIVV (RPM、OVF、RPM/OVF) 的定期通知，請執行下列步驟來設定最新版本通知：

1. 在 OMIVV 首頁中，按一下**設定** > **裝置設定** > **通知** > **最新版本通知**。
2. 選取**啟用最新版本通知 (建議)** 核取方塊。
3. 若要接收最新的裝置版本通知，請選取日期和時間。
4. 按一下**套用**。

設定部署認證

OMIVV 是作為隨需分配伺服器使用。部署認證可讓您與在自動探索程序中使用 OMIVV 附掛程式作為隨需分配伺服器的 iDRAC 互相通訊。部署認證可讓您設定 iDRAC 認證，藉此與使用自動探索功能探索到的裸機伺服器進行安全通訊，直到作業系統部署完成。

作業系統部署程序順利完成之後，OMIVV 便會將 iDRAC 認證改為如主機認證設定檔所提供。如果您變更部署認證，則之後所有使用自動探索而新探索到的系統，都會以新的 iDRAC 認證加以隨需分配。但是，在變更部署認證之前所探索到的伺服器上的認證，則不受此變更的影響。

1. 在 OMIVV 首頁上，按一下**設定** > **裝置設定** > **部署認證**。
2. 輸入使用者名稱和密碼。預設的使用者名稱為 **root**，密碼為 **calvin**。
   請確定您輸入的密碼符合 iDRAC 中設定的 iDRAC 使用者密碼原則。此外，請務必使用 iDRAC 支援的字元。
3. 按一下**套用**。

硬體元件冗餘健全狀況 — 主動式 HA

主動式 HA 為可與 OMIVV 共同運作的 vCenter 功能。當您啟用主動式 HA 時，該功能會根據主機中支援元件的冗餘健全狀況降級主動採取措施，以保障您的工作負載。

在評估支援主機元件的冗餘健全狀況狀態後，OMIVV 裝置會向 vCenter 伺服器更新變更的健全狀況狀態。支援元件 (電源供應器、風扇與 IDSDM) 可用的冗餘健全狀況狀態為：

- 良好 (資訊) — 元件運作正常
- 警告 (中度降級) — 元件有非重大錯誤。中度降級狀態會在**事件**頁面的**類型**欄中顯示為 *警告*。
- 嚴重 (嚴重降級) — 元件有嚴重故障。

註: *未知*的健全狀況狀態代表無法從 Dell Inc 提供者取得任何主動式 HA 健全狀況更新。未知的健全狀況狀態可能在下列情況發生：

- 新增到主動式 HA 叢集的所有主機可能會保持在未知狀態幾分鐘，直到 OMIVV 使用其適當的狀態將其初始化。
- vCenter 伺服器的重新啟動可能導致主動式 HA 叢集中的主機變成未知狀態，直到 OMIVV 再次使用其適當的狀態將其初始化。

當 OMIVV 偵測到支援元件的冗餘健全狀況狀態有所變更時 (不論是透過陷阱或輪詢)，元件的健全狀況更新通知均會傳送到 vCenter 伺服器。輪詢每小時執行一次，可作為預防故障機制，以彌補陷阱遺失的可能性。

註:

- 設定事件時，建議選取「張貼所有事件」選項作為事件張貼等級。如需更多有關設定事件的資訊，請參閱設定事件與警報 第頁的 81。
- 主動式 HA 只能在有支援電源、風扇和 IDSDM 冗餘的平台上使用。
- 無法設定冗餘的 PSU (例如，接線式 PSU) 不支援主動式 HA 功能。

主動式 HA 事件

根據 VMware 主動式 HA 支援的元件，Dell Inc 提供者在向 vCenter 登錄期間，會登錄下列事件：

表 5. Dell 主動式 HA 事件

Dell Inc 提供者事件	元件類型	說明
DellFanRedundancy	風扇	風扇冗餘事件
DellPowerRedundancy	電源供應器 (PSU)	電源冗餘事件
DellIDSDMRedundancy	儲存	IDSDM 冗餘事件 **註:** 當主機新增至啟用主動式 HA 的叢集時，如果有 IDSDM 元件存在，請確定內部 SD 卡備援已在 iDRAC 設定中設定為**鏡像**。

對於啟用主動式 HA 的主機，OMIVV 會使用以下陷阱作為觸發程式，以判斷元件的冗餘健全狀況：

表 6. 主動式 HA 事件

事件名稱	說明	重要性
風扇資訊	風扇資訊	資訊
風扇警告	風扇警告	警告
風扇故障	風扇故障	嚴重
電源供應器正常	電源供應器恢復正常	資訊
電源供應器警告	電源供應器偵測到警告	警告
電源供應器故障	電源供應器偵測到故障	嚴重
缺少電源供應器	缺少電源供應器	嚴重
冗餘資訊	冗餘資訊	資訊
冗餘已降級	冗餘已降級	警告
冗餘遺失	冗餘遺失	嚴重
Integrated Dual SD Module 資訊	Integrated Dual SD Module (IDSDM) 資訊	資訊
Integrated Dual SD Module 警告	Integrated Dual SD Module 警告	警告
Integrated Dual SD Module 故障	Integrated Dual SD Module 故障	嚴重
缺少 Integrated Dual SD Module	缺少 Integrated Dual SD Module	嚴重
Integrated Dual SD Module 冗餘資訊	Integrated Dual SD Module 冗餘資訊	資訊
Integrated Dual SD Module 冗餘降級	Integrated Dual SD Module 冗餘降級	警告
Integrated Dual SD Module 冗餘遺失	遺失 Integrated Dual SD Module 冗餘	嚴重
機箱事件		
風扇資訊	風扇資訊	資訊
風扇警告	風扇警告	警告
風扇故障	風扇故障	嚴重
電源供應器正常	電源供應器恢復正常	資訊
電源供應器警告	電源供應器偵測到警告	警告
電源供應器故障	電源供應器偵測到故障	嚴重
冗餘資訊	冗餘資訊	資訊
冗餘已降級	冗餘已降級	警告
冗餘遺失	冗餘遺失	嚴重

為機架式和直立式伺服器設定主動式 HA

確定所有主機都已為所有三個支援的冗餘元件 (電源供應器、風扇以及 IDSDM) 設定冗餘。

1. 建立主機認證設定檔並將主機與主機認證設定檔建立關聯。請參閱建立主機認證設定檔 第頁的 34。
2. 確認已成功完成主機清查。請參閱檢視主機清查工作 第頁的 68。

3. 確認 iDRAC 中的 SNMP 陷阱目的地是設定為 OMIVV 裝置的 IP 位址。
   註: 請確定從記錄資料中為主動式 HA 叢集確認主機的可用性。
4. 在叢集上啟用主動式 HA。請參閱在叢集上啟用主動式 HA。

為模組化伺服器設定主動式 HA

為模組化伺服器設定主動式 HA 之前，請先確認符合下列條件：

- 所有主機都已為所有三個支援的冗餘元件 (電源供應器、風扇以及 IDSDM) 正確設定冗餘。
- 已成功完成主機和機箱清查。

註: 建議主動式 HA 叢集中的所有模組化主機不應該位於相同機箱內，因為機箱元件 (PSU 和風扇) 故障會影響其所有關聯的伺服器。

1. 建立主機認證設定檔並將主機與主機認證設定檔建立關聯。請參閱建立主機認證設定檔 第頁的 34。
2. 確認已成功完成主機清查。請參閱檢視主機清查工作 第頁的 68。
   註: 請確定從記錄資料中為主動式 HA 叢集確認主機的可用性。
3. 為相關聯的機箱建立機箱認證設定檔。請參閱建立機箱認證設定檔 第頁的 38。
4. 確認已成功完成機箱清查。請參閱檢視機箱清查工作 第頁的 70。
5. 啟動 CMC 或 OME 模組化，並確認機箱的陷阱目的地是設定為 OMIVV 裝置的 IP 位址。如需設定設陷的詳細資訊，請參閱由 **dell.com/support** 提供的「CMC 和 OME 模組化使用者指南」。
6. 在叢集上啟用主動式 HA。請參閱在叢集上啟用主動式 HA。

在叢集上啟用主動式 HA

在叢集上啟用主動式 HA 之前，請先確認符合下列條件：

- 已在 vCenter 主控台建立並設定啟用 DRS 的叢集。若要在叢集上啟用 DRS，請參閱 VMware 說明文件。
- 已包含在叢集中的所有主機應屬於主機認證設定檔並已順利清查。
- 若是模組化伺服器，必須將對應的機箱新增至機箱認證設定檔，並成功清查。

1. 在 vSphere 用戶端中展開**功能表**，然後選取**主機和叢集**。
   所有主機和叢集都會顯示在左窗格中。
2. 在右窗格中選取叢集，按一下 **vSphere DRS** > **編輯**。
3. 選取 **vSphere DRS** (如果未選取)。
4. 選取**設定** > **vSphere 可用性** > **主動式 HA** > **編輯**。
   隨即會顯示**編輯叢集設定**頁面。
5. 在**編輯叢集設定**頁面上，選取**主動式 HA**。
6. 在**故障 & 回應**區段中，從下拉式功能表選取**手動**或**自動**的自動層級。
7. 如果是**補救**，請根據嚴重程度狀態，選取隔離模式、維護模式，或隔離與維護模式的組合 (混合模式)。請參閱 VMware 說明文件，以獲得更多資訊。
8. 按一下**提供者**，然後選取 **Dell Inc** 當作叢集的提供者。
9. 按一下**儲存**。

在叢集上啟用主動式 HA 後，OMIVV 會初始化主動式 HA 健全狀況和冗餘狀態，並將其回報給 vCenter。根據來自 OMIVV 的健全狀況更新通知，vCenter 伺服器會執行您針對**補救**選取的手動或自動動作。

若要覆寫現有的嚴重程度，請參閱覆寫狀況更新通知的重要性 第頁的 76。

當 RPM 升級及備份和還原操作後，在已註冊的適用於 PHA 叢集的 Dell 健全狀況更新提供者上的所有自訂內容都將還原為預設值。

覆寫狀況更新通知的重要性

針對 Dell EMC 主機及其元件，您可以用自訂的嚴重程度設定覆寫現有 Dell 主動式 HA 事件的嚴重程度，以配合您的環境。

以下是套用到每個主動式 HA 事件的嚴重程度層級：

- **資訊**
- **稍微降低**

- **嚴重降低**

註: 您無法採用**資訊**嚴重程度層級來自訂主動式 HA 元件的嚴重程度。

1. 在 OpenManage Integration for VMware vCenter 中，按一下**設定** > **覆寫主動式 HA 的嚴重程度**。
   資料格會顯示所有支援的主動式 HA 事件。資料格欄包括事件 ID、事件說明、元件類型，預設嚴重程度以及覆寫嚴重程度等欄，以供自訂主機和其元件的嚴重程度。
2. 若要變更主機或其元件的嚴重程度，請在**覆寫嚴重程度**欄中，從下拉式清單選擇所需的狀態。
   此原則適用於在所有 vCenter 伺服器中已登錄 OMIVV 的所有主動式 HA 主機。
3. 請針對必須自訂的所有事件重複步驟 2。
4. 執行以下任何一個動作：
   a. 若要儲存自訂，請按一下**套用**。
   b. 若要取消覆寫嚴重等級設定，請按一下**取消**。

   若要將覆寫嚴重等級設定重設為預設，請按一下**重設為預設**。

初始組態

完成 OMIVV 基本安裝和 vCenter 註冊之後，當您第一次啟動 vCenter 中的 OMIVV 時，便會自動顯示初始組態精靈。

如果要稍後再啟動初始組態精靈，請前往：

- **設定** > **初始組態精靈** > **啟動初始組態精靈**
- **儀表板** > **快速參照** > **啟動初始設定精靈**

1. 閱讀**歡迎**頁面上的指示，然後按一下**開始使用**。
2. 在**選取 vCenter** 頁面上，從 **vCenter** 下拉式功能表中，選取特定 vCenter 或**所有已註冊的 vCenter**，然後按一下**下一步**。

   註: 如果您有多個 vCenter 伺服器屬於已註冊相同 OMIVV 裝置之相同 PSC 的一部分，而且如果您選擇設定單一 vCenter 伺服器，則請重複步驟 2，直到設定好每一個 vCenter 為止。
3. 在**建立主機認證設定檔**頁面上，按一下**建立主機認證設定檔**。
   如需建立主機認證設定檔的更多資訊，請參閱建立主機認證設定檔 第頁的 34。

   主機新增至主機認證設定檔後，OMIVV 的 IP 位址會自動設定為主機 iDRAC 的 SNMP 陷阱目的地。OMIVV 會啟用 WBEM 服務，然後在擷取執行 ESXi 6.5 和更新版本的主機 iDRAC IP 後停用。

   OMIVV 會利用 WBEM 服務，將 ESXi 主機和 iDRAC 關係妥善同步。如果對特定主機設定 SNMP 陷阱目的地失敗，及/或為特定主機啟用 WBEM 服務失敗，該等主機將被列為不相容。若要檢視並修正不相容性，請參閱修正不相容的主機 第頁的 61。
4. 在**配置其他設定**頁面中，執行下列步驟：
   a. 排程清查工作。如需排程清查工作的更多資訊，請參閱排程清查工作 第頁的 89。
   b. 排程保固擷取工作。如需排程保固擷取工作的更多資訊，請參閱排程保固擷取工作 第頁的 89。

      若要修改清查工作排程，請前往**設定** > **vCenter 設定** > **資料擷取排程** > **清查擷取**或**工作** > **清查** > **主機清查**。

      若要修改保固擷取工作排程，請前往**設定** > **vCenter 設定** > **資料擷取排程** > **保固擷取**或**工作** > **保固**。
   c. 設定事件與警報。如需設定事件與警報的相關資訊，請參閱設定事件與警報 第頁的 81。
   d. 若要套用個別設定，請個別按一下**套用**按鈕，然後按一下**下一步**。

      強烈建議啟用所有其他設定。如果任一其他設定未經套用，隨即會顯示訊息，指出套用所有其他設定是必要步驟。
5. 請閱讀**後續步驟**頁面上的指示，然後按一下**完成**。

   建議將您的 OMIVV 主機與組態基準建立關聯，因為這樣可以讓您密切監控主機與關聯叢集中發生的組態變更。當 OMIVV 成功管理主機之後，便可為任何叢集建立組態基準。若要建立組態基準，請執行下列步驟：

   - 為韌體與驅動程式建立儲存庫設定檔 - 這可以協助您定義基準韌體與驅動程式版本。
   - 建立系統設定檔 - 這可以協助您定義主機的基準硬體組態。
   - 建立叢集設定檔 - 若要建立成功的基準，請選取叢集並建立韌體、驅動程式與硬體組態的關聯。
   - PowerEdge MX 機箱內的主機 (iDRAC IPv4 是在停用狀態) 必須使用機箱認證設定檔加以管理。

檢視初始組態狀態

在「初始組態」精靈頁面上，您可以執行下列步驟：

- 檢視初始組態狀態

僅在所有 vCenter 都已設定主機認證設定檔、事件與警報、庫存與保固工作時才會完整顯示初始組態狀態。

- 啟動初始組態精靈

韌體更新設定

選取**清除 iDRAC 工作並重設 iDRAC** 核取方塊，會在更新主機韌體前，先清除**工作佇列**中存在的所有 iDRAC 工作，並接著重設 iDRAC。

清除 iDRAC 工作並重設 iDRAC 設定會在執行以下作業時使用：

- 透過 OMIVV 進行韌體更新

  使用 OMIVV 更新韌體時，可覆寫此設定。但是，覆寫設定不會影響在**韌體更新設定**頁面上所做的設定。

- 使用 vSphere Lifecycle Manager 的韌體補救

  執行韌體補救時，無法覆寫此設定。

1. 選取**清除 iDRAC 工作並重設 iDRAC** 核取方塊。
2. 按一下**套用**。

檢視授權資訊

上傳 OMIVV 授權時，這個標籤會顯示支援的主機和 vCenter 伺服器數量。

若要購買軟體授權，請按一下**軟體授權**旁的**購買授權**。如需更多資訊，請參閱 購買軟體授權 第頁的 79。

以下資訊會顯示在**授權**頁面上：

授權類型	說明
主機授權	• 可用授權 顯示可用的授權數 • 使用中的授權 顯示使用中的授權數
vCenter 授權	• 可用授權 顯示可用的授權數 • 使用中的授權 顯示使用中的授權數

授權管理區段會顯示以下項目的連結：

- 產品授權入口網站 (Digital Locker)
- 系統管理員主控台

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。

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。

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。

購買軟體授權

1. 前往**設定** > **授權** > **購買授權**，或**儀表板** > **購買授權**，或**管理入口網站** > **vCenter 註冊** > **授權** > **立即購買**。
   DellEMC 支援頁面隨即顯示。
2. 下載授權檔案，並將其儲存至已知位置。
   授權檔案可能會封裝在 .zip 檔案中。請確定您有解壓縮 .zip 檔案，並只有上傳 .xml 授權檔案。授權檔案可能會根據您的訂單號碼命名，例如 123456789.xml。

存取支援資訊

表 7. 支援頁面上的資訊

名稱	說明
說明文件支援	提供下列文件連結： • PowerEdge 伺服器 • OMIVV 手冊 • iDRAC 與 Lifecycle Controller
管理主控台	提供管理主控台的連結。
一般說明	提供 Dell EMC 支援網站的連結。
重設 iDRAC	提供重設 iDRAC 的連結，當 iDRAC 無回應時可使用。此重設會執行正常的 iDRAC 重新開機。如需更多有關重設 iDRAC 的資訊，請參閱重設 iDRAC 第頁的 80。
致電技術支援部門之前	就如何聯絡 Dell EMC Support 與正確轉接電話提供提示。
故障診斷套裝	提供建立和下載故障診斷套裝的連結。當您聯絡技術支援部門時，即可提供或檢視此套裝。如需更多資訊，請參閱建立並下載故障診斷套裝 第頁的 79。
Dell EMC 建議	提供 Dell EMC Repository Manager (DRM) 支援網站的連結。DRM 用於建立自訂目錄，可用於更新韌體和漂移偵測。

建立並下載故障診斷套裝

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。

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。

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**。

重設 iDRAC

重設 iDRAC 會執行正常的 iDRAC 重新開機。重設 iDRAC 後，iDRAC 通常會重新開機，而非主機。重設後，iDRAC 只能在幾分鐘後才能使用。僅在 OMIVV 裝置上的 iDRAC 無回應時才重設。

- 您只能將此重設動作套用在屬於主機認證設定檔的一部分，且已經清查至少一次的主機上。
- Dell EMC 建議您將主機切換至維護模式，然後重設 iDRAC。
- 重設 iDRAC 之後，如果 iDRAC 變成無法使用或停止回應，請硬重設 iDRAC。如需硬重設的相關資訊，請參閱《iDRAC 使用者指南》，網址為 https://www.dell.com/support/。

iDRAC 重新啟動時，您可能會發現：

- OMIVV 擷取主機健全狀態時發生通訊延遲。
- 目前對 iDRAC 開啟的所有工作階段已結束。
- iDRAC 的 DHCP 位址改變。如果 iDRAC 使用 DHCP 產生其 IP 位址，則 iDRAC IP 位址有可能會變更。此時，請重新執行主機清查工作，在清查資料中取得新的 iDRAC IP 位址。

1. 在**支援**頁面，按一下**重設 iDRAC**。
2. 在 **iDRAC 重設**頁面上，輸入主機名稱或 IP 位址。
3. 為確認您瞭解 iDRAC 重設程序，請選擇**我瞭解重設 iDRAC 的效果。繼續以重設所選主機上的 iDRAC** 核取方塊。
4. 按一下**重設 iDRAC**。

15

管理 vCenter 設定

關於事件與警報

在**設定**頁面上，您可以啟用主機與機箱的事件與警報、選取事件張貼等級，以及還原預設警報。您可以設定每個 vCenter 的事件與警報，或者為所有已登錄的 vCenter 設定事件與警報。對應至機箱的事件與警報與 vCenter 相關聯。

以下是四個事件張貼等級：

表 8. 事件張貼等級

事件	說明
請勿發佈任何事件	不允許 OMIVV 將任何事件或警示轉傳到與其相關的 vCenter。
張貼所有事件	將 OMIVV 從受管理的 Dell EMC 主機所收到的所有事件 (包括資訊事件) 張貼到相關的 vCenter。建議選取**張貼所有事件**選項為事件的張貼等級。
只張貼關鍵及警告事件	僅張貼嚴重或警告的事件到相關的 vCenter。
僅張貼虛擬化相關的嚴重事件與警告事件	將從主機收到的虛擬化相關事件張貼到相關的 vCenter。虛擬化相關事件是 Dell 所選擇對於執行虛擬機器的主機最重要的事件。

設定事件與警報時，嚴重的硬體警報會觸發 OMIVV 裝置，使主機系統進入維護模式。在某些情況下，系統會將虛擬機器移轉到另一個主機系統。OMIVV 會將從受管理的主機收到的事件轉送至 vCenter，並為這些事件建立警報。使用這些警報來觸發 vCenter 的動作，例如重新開機、維護模式或移轉。

例如，電源供應器故障並建立警報時，產生的動作會讓機器進入維護模式，而導致工作負載移轉至叢集中的其他主機。

叢集以外或者未啟用 VMware 分散資源排程 (DRS) 叢集中的所有主機，都會發現虛擬機器由於嚴重事件而關閉。Dell EMC 建議先啟用 DRS，然後再啟用 Dell 警報。如需更多資訊，請參閱 VMware 說明文件。

DRS 會持續監控跨資源池的使用量，並且根據業務需求，適當地在虛擬機器之間配置可用資源。若要確保虛擬機器在發生嚴重硬體事件時自動移轉，請使用具有 DRS 設定 Dell 警報的叢集。螢幕上的訊息詳細資料會列出可能受影響之 vCenter 例項上的叢集。請確認叢集受到影響，然後再啟用事件與警報。

若想要恢復預設的警報設定，請選取**還原警報**選項。此選項是方便的選項，不用解除安裝及重新安裝產品，即可還原預設的警報設定。如果安裝後有變更過任何 Dell EMC 警報組態，使用**還原警報**選項即可還原那些變更。

註: 若要接收 Dell 事件，請務必在 iDRAC、CMC 和「管理控制器」中啟用所需的事件。

註: OMIVV 會預先選取讓主機成功執行虛擬機器所需的虛擬化相關事件。依預設會停用 Dell 主機警報。如果啟用 Dell EMC 警報，則叢集應使用 DRS，確保傳送嚴重事件的虛擬機器得以自動移轉。

設定事件與警報

若要從伺服器接收事件，請務必在 iDRAC 中設定 SNMP 陷阱目的地。OMIVV 支援 SNMP v1 和 v2 警示。

1. 在 OMIVV 首頁上，按一下**設定** > **vCenter 設定** > **事件與警報**。
2. 若要為所有主機及其機箱啟用警報，按一下**針對所有主機與其機箱啟用警報**。
   啟用 Dell EMC 警報警告頁面會顯示啟用 Dell EMC 警報後，可能受到影響的叢集和非叢集主機。

   註: Dell EMC 主機的警報在啟用後，會以進入維護模式的方式來回應某些特定嚴重事件。您可以視需要修改警報。

   註: 在 vCenter 6.7 U1 和 6.7 U2 中，編輯選項會失敗。如需編輯警報定義，建議使用 Web 用戶端 (FLEX)。

   註: BMC 設陷沒有訊息 ID，因此 OMIVV 中的警示不會有這些詳細資料。

3. 若要接受變更，按一下**繼續**。
   所有主機及其機箱的警報均已啟用。
4. 選取下列任何一個事件張貼等級：
   - **不張貼任何事件**—不將任何事件或警示轉傳到其相關的 vCenter。
   - **張貼所有事件**—將所有事件 (包括資訊事件)，以及從受管理的主機和機箱所收到的事件，張貼到其相關的 vCenter。建議選取「張貼所有事件」選項為事件的張貼等級。
   - **只張貼關鍵及警告事件**—只將具有嚴重或警告程度的事件張貼到其相關的 vCenter。
   - **僅張貼虛擬相關的事件**—將從主機收到的虛擬化相關事件張貼到其相關的 vCenter。虛擬化相關事件是對執行虛擬機器的主機而言最嚴重的事件。
5. 若要儲存變更，請按一下**套用**。
   若要還原所有主機與其機箱的預設 vCenter 警報設定，請按一下**還原警報**。變更生效可能需時一分鐘。

   還原警報是個方便的選項，不用解除安裝及重新安裝產品，即可還原預設的警報設定。如果安裝後變更了任何 Dell EMC 警報組態，使用**還原警報**選項即可還原那些變更。

   註: 還原裝置後，事件與警報設定則為未啟用。您可以從設定標籤再次啟用事件與警報設定。

檢視機箱事件

1. 在 vSphere 用戶端中展開**功能表**，然後選取**主機和叢集**。
2. 在左窗格中，選取 vCenter 的例項。
3. 在右窗格中，按一下**監控** > **工作與事件** > **事件**。
4. 若要檢視更多資訊，請選取特定事件。

   註: 若是採用 MCM 組態的 PowerEdge MX 機箱，事件來源將會顯示為主要機箱，但是訊息詳細資料將會有成員機箱的產品服務編號以供識別之用。

檢視機箱警報

1. 在 vSphere 用戶端中展開**功能表**，然後選取**主機和叢集**。
2. 在左窗格中，選取 vCenter 的例項。
3. 在右窗格中，按一下**監視** > **問題與警報** > **觸發的警報**。
4. 在**觸發的警報**中按一下警報名稱以檢視警報定義。

檢視警報和事件設定

設定警報和事件後，即可檢視是否有啟用主機的 vCenter 警報，以及在「設定」標籤上選取了哪一個事件張貼等級。

1. 在 OMIVV 首頁上，按一下**設定** > **事件與警報**。
   隨後便會顯示以下詳細資料：
   - Dell EMC 主機的 vCenter 警報—顯示**已啟用**或**已停用**。
   - 事件張貼等級
2. 設定事件與警報。請參閱設定事件與警報 第頁的 81。

若要檢視事件張貼等級，請參閱關於事件與警報 第頁的 81。

虛擬化相關事件

下表包含與虛擬化有關的嚴重事件和警告事件，並包含事件名稱、說明、嚴重性層級和建議動作。

虛擬化相關事件會以下列格式顯示：

Dell-Message ID：<ID 號碼>，訊息：<訊息說明>。

機箱事件會以下列格式顯示：

Dell-Message：<訊息說明>，機箱名稱：<機箱名稱>，機箱產品服務編號：<機箱產品服務編號 >，機箱位置：<機箱位置>

表 9. 虛擬化事件

事件名稱	說明	重要性	建議動作
Dell-alertHWCAuditWarning	硬體組態警告	警告	無動作
Dell-alertHWCAuditInformation	硬體組態資訊	資訊	無動作
Dell-alertLiquidCoolingLeakInformational	已解決裝置先前偵測到的小規模洩漏狀況	資訊	無動作
Dell-alertLiquidCoolingLeakWarning	在裝置上偵測到小規模洩漏狀況	警告	無動作
Dell-alertLiquidCoolingLeakFailure	在裝置上偵測到大規模洩漏狀況	嚴重	中斷輸入電源，然後立即與您的服務提供者聯絡。
Dell-alertStorageSoftwareDefinedSubSystemFailure	軟體定義儲存子系統故障	嚴重	確認訊息中所識別的硬碟健全狀況狀態，然後重試此操作。若要檢查 iDRAC GUI 上的健全狀況狀態，請在 iDRAC 儀表板上按一下 **儲存** > **實體磁碟**。在命令行介面 (CLI) 執行下列 RACADM 命令：`racadm raid get pdisks -o -p status` 為儲存集區增加更多實體磁碟，然後重試該操作。
Dell-alertStorageSoftwareDefinedSubSystemWarning	軟體定義儲存子系統警告	警告	無動作
Dell-alertTemperatureProbeReadWarning	無法讀取溫度感應器	警告	無動作
Dell-alertTemperatureProbeChangeFailure	溫度增加錯誤	嚴重	檢查機箱事件記錄中是否發生風扇問題，並解決所有出現的問題。如果未偵測到風扇問題，請檢查機箱的環境溫度，並確定溫度在作業範圍內。若要檢查機箱的環境溫度，請執行下列 RACADM 命令：`racadm getsensorinfo`。
Dell 電流感應器偵測到警告值	指定系統中的電流感應器超過其警告閾值	警告	無動作
Dell 電流感應器偵測到故障值	指定系統中的電流感應器超過其故障閾值	錯誤	讓系統進入維護模式
Dell 電流感應器偵測到無法修復的值	特定系統中的電流感應器偵測到無法修復的錯誤	錯誤	無動作
重新獲得 Dell 冗餘	感應器回到正常值	資訊	無動作
Dell 冗餘降級	指定系統中的冗餘感應器偵測到備援裝置的其中一個元件故障，但該裝置仍為備援	警告	無動作
Dell - 冗餘遺失	指定系統中的冗餘感應器偵測到備援裝置中的其中一個元件已中斷連接、故障或不存在	錯誤	讓系統進入維護模式
Dell - 電源供應器恢復正常	感應器回到正常值	資訊	無動作

表 9. 虛擬化事件 (續)

事件名稱	說明	重要性	建議動作
Dell - 電源供應器偵測到警告	指定系統中的電源供應感應器讀數超過使用者定義的警告閾值	警告	無動作
Dell - 電源供應器偵測到故障	電源供應器已中斷連接或故障	錯誤	讓系統進入維護模式
Dell - 電源供應感應器偵測到無法修復的值	指定系統中的電源供應感應器偵測到無法修復的錯誤	錯誤	無動作
Dell - 記憶體裝置狀態警告	記憶體裝置修正率超過可接受的值	警告	無動作
Dell - 記憶體裝置錯誤	記憶體裝置修正率超過可接受的值，記憶體備用區已啟用，或發生多位元 ECC 錯誤	錯誤	讓系統進入維護模式
Dell - 風扇機櫃插入系統	感應器回到正常值	資訊	無動作
Dell - 系統已卸下風扇機櫃	指定系統已卸下風扇機櫃	警告	無動作
Dell - 系統長時間卸下風扇機櫃	指定系統已卸下風扇機櫃，且經過一段使用者定義的時間	錯誤	無動作
Dell - 風扇機櫃感應器偵測到無法修復的值	指定系統中的風扇機櫃感應器偵測到無法修復的錯誤	錯誤	無動作
Dell - 交流電源已恢復	感應器回到正常值	資訊	無動作
Dell - 交流電源已遺失警告	交流電源線已無法供電，但還有足夠的冗餘，可將此狀況歸類為警告	警告	無動作
Dell - 交流電源線電源中斷	交流電源線已無法供電，且沒有冗餘，必須將此狀況歸類為錯誤	錯誤	無動作
Dell - 處理器感應器回到正常值	感應器回到正常值	資訊	無動作
Dell - 處理器感應器偵測到警告值	指定系統中的處理器感應器處於節流狀態	警告	無動作
Dell - 處理器感應器偵測到故障值	指定系統中的處理器感應器已停用、發生組態錯誤或超出極限溫度	錯誤	無動作
Dell - 處理器感應器偵測到無法修復的值	特定系統中的處理器感應器故障。	錯誤	無動作
Dell - 裝置組態錯誤	指定系統中的隨插即用裝置偵測到組態錯誤	錯誤	無動作
Dell - 電池感應器回到正常值	感應器回到正常值	資訊	無動作
Dell - 電池感應器偵測到警告值	指定系統中的電池感應器偵測到電池處於可預測的故障狀態	警告	無動作

表 9. 虛擬化事件 (續)

事件名稱	說明	重要性	建議動作
Dell - 電池感應器偵測到故障值	指定系統中的電池感應器偵測到電池故障	錯誤	無動作
Dell - 電池感應器偵測到無法修復的值	指定系統中的電池感應器偵測到電池故障	錯誤	無動作
Dell - 熱感應關機保護已啟動	當系統設為因錯誤事件而熱感應關機時，就會產生這個訊息。如果溫度感應器讀數超過為系統設定的錯誤閾值，作業系統就會關閉，系統也會關機。長時間卸下部份系統的風扇機櫃也會產生此訊息	錯誤	無動作
Dell - 溫度感應器回到正常值	感應器回到正常值	資訊	無動作
Dell - 溫度感應器偵測到警告值	指定系統中背板、系統主機板、CPU 或磁碟機托架上的溫度感應器超出其警告閾值	警告	無動作
Dell - 溫度感應器偵測到故障值	指定系統中背板、系統主機板或磁碟機托架上的溫度感應器超出其故障閾值	錯誤	讓系統進入維護模式
Dell - 溫度感應器偵測到無法修復的值	指定系統中背板、系統主機板或磁碟機托架上的溫度感應器偵測到無法修復的錯誤	錯誤	無動作
Dell - 風扇感應器回到正常值	感應器回到正常值	資訊	無動作
Dell - 風扇感應器偵測到警告值	主機 <x> 的風扇感應器讀數超出警告閾值	警告	無動作
Dell - 風扇感應器偵測到故障值	指定系統中的風扇感應器偵測到一或多個風扇故障	錯誤	讓系統進入維護模式
Dell - 風扇感應器偵測到無法修復的值	風扇感應器偵測到無法修復的錯誤	錯誤	無動作
Dell - 電壓感應器回到正常值	感應器回到正常值	資訊	無動作
Dell - 電壓感應器偵測到警告值	特定系統中的電壓感應器超出其警告閾值	警告	無動作
Dell - 電壓感應器偵測到故障值	指定系統中的電壓感應器超出其故障閾值	錯誤	讓系統進入維護模式
Dell - 電壓感應器偵測到無法修復的值	指定系統中的電壓感應器偵測到無法修復的錯誤	錯誤	無動作
Dell - 電流感應器回到正常值	感應器回到正常值	資訊	無動作
Dell - 儲存裝置：儲存管理錯誤	儲存裝置管理偵測到裝置獨立的錯誤狀態	錯誤	讓系統進入維護模式
Dell - 儲存裝置：控制器警告	部分實體磁碟已經損壞	警告	無動作

表 9. 虛擬化事件 (續)

事件名稱	說明	重要性	建議動作
Dell - 儲存裝置：控制器故障	部分實體磁碟已經損壞	錯誤	讓系統進入維護模式
Dell - 儲存裝置：通道故障	通道故障	錯誤	讓系統進入維護模式
Dell - 儲存裝置：機櫃硬體資訊	機櫃硬體資訊	資訊	無動作
Dell - 儲存裝置：機櫃硬體警告	機櫃硬體警告	警告	無動作
Dell - 儲存裝置：機櫃硬體故障	機櫃硬體錯誤	錯誤	讓系統進入維護模式
Dell - 儲存裝置：陣列磁碟作業失敗	陣列磁碟作業失敗	錯誤	讓系統進入維護模式
Dell - 儲存裝置：EMM 故障	EMM 故障	錯誤	讓系統進入維護模式
Dell - 儲存裝置：電源供應器故障	電源供應器故障	錯誤	讓系統進入維護模式
Dell - 儲存裝置：溫度探針警告	實體磁碟溫度探針警告，過冷或過熱	警告	無動作
Dell - 儲存裝置：溫度探針故障	實體磁碟溫度探針錯誤，過冷或過熱。	錯誤	讓系統進入維護模式
Dell - 儲存裝置：風扇故障	風扇故障	錯誤	讓系統進入維護模式
Dell - 儲存裝置：電池警告	電池警告	警告	無動作
Dell - 儲存裝置：虛擬磁碟降級警告	虛擬磁碟降級警告	警告	無動作
Dell - 儲存裝置：虛擬磁碟降級故障	虛擬磁碟降級故障	錯誤	讓系統進入維護模式
Dell - 儲存裝置：溫度探針資訊	溫度探針資訊	資訊	無動作
Dell - 儲存裝置：陣列磁碟警告	陣列磁碟警告	警告	無動作
Dell - 儲存裝置：陣列磁碟資訊	陣列磁碟資訊	資訊	無動作
Dell - 儲存裝置：電源供應器警告	電源供應器警告	警告	無動作
Dell - 流體快取記憶體磁碟作業失敗	流體快取記憶體磁碟作業失敗	錯誤	讓系統進入維護模式
Dell - 纜線故障或嚴重事件	纜線故障或嚴重事件	錯誤	讓系統進入維護模式
Dell - 機箱管理控制器偵測到警告	機箱管理控制器偵測到警告	警告	無動作
Dell - 機箱管理控制器偵測到錯誤	機箱管理控制器偵測到錯誤	錯誤	讓系統進入維護模式
Dell - IO 虛擬化故障或嚴重事件	IO 虛擬化故障或嚴重事件	錯誤	讓系統進入維護模式
Dell - 連結狀態警告	連結狀態警告	警告	無動作
Dell - 連結狀態故障或嚴重事件	連結狀態故障或嚴重事件	錯誤	讓系統進入維護模式
Dell - 安全性警告	安全性警告	警告	無動作
Dell - 系統：軟體組態警告	系統：軟體組態警告	警告	無動作
Dell - 系統：軟體組態故障	系統：軟體組態故障	錯誤	讓系統進入維護模式
Dell - 儲存安全性警告	儲存安全性警告	警告	無動作
Dell - 儲存安全性故障或嚴重事件	儲存安全性故障或嚴重事件	錯誤	讓系統進入維護模式
Dell - 軟體變更更新警告	軟體變更更新警告	警告	無動作

表 9. 虛擬化事件 (續)

事件名稱	說明	重要性	建議動作
Dell - 機箱管理控制器稽核警告	機箱管理控制器稽核警告	警告	無動作
Dell - 機箱管理控制器稽核失敗或嚴重事件	機箱管理控制器稽核失敗或嚴重事件	錯誤	讓系統進入維護模式
Dell - PCI 裝置稽核警告	PCI 裝置稽核警告	警告	無動作
Dell 電源供應器稽核警告	電源供應器稽核警告	警告	無動作
Dell - 電源供應器稽核失敗或嚴重事件	電源供應器稽核失敗或嚴重事件	錯誤	讓系統進入維護模式
Dell - 電源使用方式稽核警告	電源使用方式稽核警告	警告	無動作
Dell - 電源使用方式稽核失敗或嚴重事件	電源使用方式稽核失敗或嚴重事件	錯誤	讓系統進入維護模式
Dell - 安全性組態警告	安全性組態警告	警告	無動作
Dell - 組態：軟體組態警告	組態：軟體組態警告	警告	無動作
Dell - 組態：軟體組態故障	組態：軟體組態故障	錯誤	讓系統進入維護模式
Dell - 虛擬磁碟分割區故障	虛擬磁碟分割區故障	錯誤	讓系統進入維護模式
Dell - 虛擬磁碟分割區警告	虛擬磁碟分割區警告	警告	無動作
iDRAC 事件 **註:** 對於已包含在叢集中的所有已啟用主動式 HA 的主機，下列虛擬化事件會對應至主動式 HA 事件 (「風扇沒有冗餘」事件和「電源供應器沒有冗餘」事件除外)。			
風扇有冗餘	無	資訊	無動作
遺失風扇冗餘	一或多個風扇已經故障或已卸下或組態已變更，此時需要其他風扇	嚴重	卸下並重新安裝故障的風扇或安裝其他風扇
風扇冗餘降級	一或多個風扇已經故障或已卸下或組態已變更，此時需要其他風扇	警告	卸下並重新安裝故障的風扇或安裝其他風扇
風扇沒有冗餘	一或多個風扇已經故障或已卸下或組態已變更，此時需要其他風扇	資訊	卸下並重新安裝故障的風扇或安裝其他風扇
風扇沒有冗餘。資源不足以維持正常運作	一或多個風扇已經故障或已卸下或組態已變更，此時需要其他風扇	嚴重	卸下並重新安裝故障的風扇或安裝其他風扇
電源供應器有冗餘	無	資訊	無動作
遺失電源供應器冗餘	因為電源供應器例外狀況、電源供應器清查變更，或系統電源清查變更，目前的電源運作模式為非冗餘。系統先前是在電源冗餘模式下運作	嚴重	檢查電源供應器故障的事件記錄。檢視系統組態與耗電量
電源供應器冗餘降級	因為電源供應器例外狀況、電源供應器清	警告	檢查電源供應器故障的事件記錄。檢視系統組態與耗電量

表 9. 虛擬化事件 (續)

事件名稱	說明	重要性	建議動作
	查變更，或系統電源清查變更，目前的電源運作模式為非冗餘。系統先前是在電源冗餘模式下運作		
電源供應器沒有冗餘	目前的電源供應器組態不符合啟用冗餘的平台需求。如果電源供應器故障，系統可能會關機。	資訊	如果誤用，請檢視系統組態與耗電量，並據此安裝電源供應器。請檢查電源供應器是否出現故障狀態
電源供應器沒有冗餘。資源不足以維持正常運作	系統可能會關閉電源或以效能降低的狀態操作	嚴重	檢查電源供應器故障的事件記錄。檢視系統組態與耗電量，並據此升級或安裝電源供應器
Internal Dual SD Module 有冗餘	無	資訊	無動作
遺失 Internal Dual SD Module 冗餘	其中一張 SD 卡或兩張 SD 卡無法正常運作	嚴重	更換故障的 SD 卡
Internal Dual SD Module 冗餘降級	其中一張 SD 卡或兩張 SD 卡無法正常運作	警告	更換故障的 SD 卡
Internal Dual SD Module 沒有冗餘	無	資訊	如果需要冗餘，請安裝其他 SD 卡，然後設定冗餘
機箱事件			
遺失電源供應器冗餘	因為電源供應器例外狀況、電源供應器清查變更，或系統電源清查變更，目前的電源運作模式為非冗餘。系統先前是在電源冗餘模式下運作	嚴重	檢查電源供應器故障的事件記錄。檢視系統組態與耗電量
電源供應器冗餘降級	因為電源供應器例外狀況、電源供應器清查變更，或系統電源清查變更，目前的電源運作模式為非冗餘。系統先前是在電源冗餘模式下運作	警告	檢查電源供應器故障的事件記錄。檢視系統組態與耗電量
電源供應器有冗餘	無	資訊	無動作
電源供應器沒有冗餘	目前的電源供應器組態不符合啟用冗餘的平台需求。如果電源供應器故障，系統可能會關機。	資訊	如果誤用，請檢視系統組態與耗電量，並據此安裝電源供應器。請檢查電源供應器是否出現故障狀態
電源供應器沒有冗餘。資源不足以維持正常運作	系統可能會關閉電源或以效能降低的狀態操作	嚴重	檢查電源供應器故障的事件記錄。檢視系統組態與耗電量，並據此升級或安裝電源供應器
遺失風扇冗餘	一或多個風扇已經故障或已卸下或組態已變更，此時需要其他風扇	嚴重	卸下並重新安裝故障的風扇或安裝其他風扇
風扇冗餘降級	一或多個風扇已經故障或已卸下或組態已	警告	卸下並重新安裝故障的風扇或安裝其他風扇

表 9. 虛擬化事件 (續)

事件名稱	說明	重要性	建議動作
	變更，此時需要其他風扇		
風扇有冗餘	無	資訊	無動作
風扇沒有冗餘	一或多個風扇已經故障或已卸下或組態已變更，此時需要其他風扇	資訊	卸下並重新安裝故障的風扇或安裝其他風扇
風扇沒有冗餘。資源不足以維持正常運作	一或多個風扇已經故障或已卸下或組態已變更，此時需要其他風扇	嚴重	卸下並重新安裝故障的風扇或安裝其他風扇

管理資料擷取排程

排程清查工作

如要在 OMIVV 檢視最新的清查資料，您必須定期排程清查，以確保主機或機箱的清查資訊是最新的。建議每週執行一次清查工作。

註: 機箱於 OMIVV 內容中進行管理。機箱管理中沒有 vCenter 的內容。排程的主機清查完成後會觸發機箱清查，以供所有使用 OMIVV 管理的機箱使用。

註: 每次叫用組態精靈時，就會將本頁中的設定重設為預設值。如果您先前已設定清查排程，請務必複製本頁中先前的排程，再完成精靈功能，這樣先前的排程就不會被預設設定覆寫。

1. 在 OMIVV 首頁上，按一下**設定** > **vCenter 設定** > **資料擷取排程** > **清查擷取**。
2. 選取**啟用清查資料擷取 (建議)** 核取方塊。

   在有多個 vCenter 伺服器的 PSC 環境中，如果個別 vCenter 的排程不同，且您選取**所有已註冊的 vCenter** 選項來更新清查排程，則清查排程設定頁面會顯示預設排程。
3. 選取清查資料擷取日期與時間，然後按一下**套用**。

   註: 在有多個 vCenter 伺服器的 PSC 環境中，若更新**所有已註冊的 vCenter** 的清查排程，更新會覆寫個別的 vCenter 清查排程設定。

排程保固擷取工作

1. 若要更新授權金鑰，請確定您有權存取索引目錄 (`https://downloads.dell.com/catalog/CatalogIndex.gz`)。
2. 若要取得保固報告，請確定您有權存取 `https://apigtwb2c.us.dell.com`。
3. 請確定已在主機和機箱上成功執行清查。
4. 若要使用 OMIVV 的保固功能，您必須具備網際網路連線。如果您的環境需要 Proxy 才能連接網際網路，請確定在系統管理員入口網站上設定 Proxy 設定。

硬體保固資訊可從 Dell 線上擷取，並由 OMIVV 顯示。Dell Online 只會傳送而不會儲存產品服務編號。

在具備多個 vCenter Server 的 PSC 環境中，只要一執行任何 vCenter 的保固，每個 vCenter 的機箱保固便會自動執行。但是，如果保固沒有新增至機箱認證設定檔，就不會自動執行。

註: 每次叫用組態精靈時，就會將本頁中的設定重設為預設值。如果您先前已設定一個保固擷取工作，請務必先在本頁中複製該排程保固擷取工作之後，再完成精靈功能，這樣先前的保固擷取就不會被預設設定覆寫。

1. 在 OMIVV 首頁上，按一下**設定** > **vCenter 設定** > **資料擷取排程** > **保固擷取**。
2. 選取**啟用保固資料擷取 (建議)** 核取方塊。

   有多個 vCenter 伺服器的 PSC 環境中，如果個別 vCenter 的排程不同，且您選取**所有已註冊的 vCenter** 選項來更新保固排程，則保固排程設定頁面會顯示預設排程。

3. 選取保固資料擷取的日期與時間，然後按一下**套用**。

   註: 在有多個 vCenter 伺服器的 PSC 環境中，若更新**所有已註冊的 vCenter** 的保固排程，更新會覆寫個別的 vCenter 保固排程設定。

16

機箱管理

檢視 Dell EMC 機箱資訊

您可使用 OMIVV 來檢視已探索到並清查的機箱資訊。Dell EMC 機箱會列出由 OMIVV 管理的所有機箱。

1. 在 OMIVV 首頁上，按一下**主機與機箱** > **機箱** > **機箱清單**。
   下列資訊隨即顯示：
   - **名稱**—顯示每個 Dell EMC 機箱的 IP 位址連結。
   - **健全狀況**—顯示機箱的健全狀況狀態。

     若要根據每個 Dell EMC 機箱的健全狀況狀態進行篩選，請按一下搜尋旁的篩選圖示。
   - **IP 位址/FQDN**—顯示 vCenter IP 位置或 FQDN。
   - **產品服務編號**—顯示機箱的產品服務編號。
   - **機箱 URL**—顯示機箱 URL。
   - **機型**—顯示機型名稱。
   - **角色**—僅適用於 MX 機箱。顯示機箱 (主要或成員) 的角色。
   - **上次清查**—顯示上次清查資訊。
   - **可用插槽**—顯示機箱中可用的插槽。
   - **設定檔名稱**—顯示與機箱建立關聯的機箱認證設定檔名稱。
   - **位置**—顯示機箱的位置。

   如果未執行清查，則不會顯示**名稱**、**上次清查**、**可用插槽**、**設定檔名稱**、**位置**和機箱清查資訊。

   註: 若是採用 MCM 組態的 PowerEdge MX 機箱，會使用主要機箱管理整個 MCM 基礎結構。如果成員機箱 IP 和 iDRAC IP 停用和/或機箱角色變更，Dell EMC 建議您先移除現有主要機箱並再次加入新的主要機箱 IP，然後與機箱認證設定檔建立關聯。
2. 選取機箱以檢視韌體、授權類型和與保固相關的資訊。
   如果未執行清查，則不會顯示**名稱**、**韌體**、**授權類型**和**保固**資訊。

檢視機箱清查資訊

1. 在 **Dell EMC 機箱**頁面上，選取一個機箱或按一下「產品服務編號」。
2. 在**機箱資訊**中，按一下**檢視**。
   概觀頁面會顯示機箱的健全狀況、作用中錯誤、機箱的元件層級健全狀況狀態、硬體概觀和機箱關係 (僅適用於 MX 機箱)。

   註: 如果是 M1000e 4.3 版及更早的版本，則不會顯示作用中的錯誤。

   主窗格會顯示機箱的整體狀況。有效的健全狀況指示燈為**良好**、**警告**、**嚴重**和**未知**。機箱狀況資料格檢視會顯示每個元件的狀況。機箱狀況參數適用於 VRTX 1.0 版 (含) 以後、M1000e 4.4 版 (含) 以後的機型。若為 4.3 以前的 M1000e 韌體版本，只會顯示兩個健全狀況指示燈：例如「良好」和「警告」或「嚴重」。

   整體健全狀況是根據健全狀況參數最差的機箱來表示狀況。例如，如果有五個良好符號和一個警告符號，整體健全狀況會顯示為警告。

檢視機箱的硬體清查資訊

您可以檢視所選機箱的硬體清查相關資訊。

1. 在 OMIVV 首頁上，按一下 **主機與機箱** > **機箱 s** > **機箱清單**。
   Dell EMC 機箱頁面隨即顯示。

2. 選取機箱，按一下產品服務編號連結。
隨即顯示**概觀**頁面。
3. 在**概觀**頁面上，按一下**硬體**。

表 10. 硬體清查資訊

硬體清查：元件	瀏覽 OMIVV	資訊

風扇	• 在 **Dell EMC 機箱**頁面上，按一下 **機箱** > **機箱清單**，然後按一下「產品服務編號」連結。
	• 在**概觀**頁面的左窗格中，選取**硬體**。
	• 在右窗格中，展開**風扇**。
	或
	• 在**概觀**頁面上，按一下**風扇**。
		風扇的相關資訊：
		• 名稱
		• 存在
		• 識別符 (僅適用於 MX 機箱)
		• 電源狀態
		• 讀數 (RPM)
		• 警告閾值 (不適用於 MX 機箱)
		• 嚴重閾值 (不適用於 MX 機箱)
		  ○ 最小值
		  ○ 最大值
		• 脈衝寬度調變 (僅適用於 MX 機箱)
		註: 在 PowerEdge MX 機箱中，會以「是」指示存在風扇，即使已將風扇從機箱移除亦是如此。但是，**摘要**頁面的風扇健全狀況會顯示為**嚴重**，並會顯示作用中錯誤。

電源	• 在 **Dell EMC 機箱**頁面上，按一下 **機箱** > **機箱清單**，然後按一下「產品服務編號」連結。 • 在**概觀**頁面的左窗格中，選取**硬體**。 • 在右窗格中，展開**電源供應器**。 **或** • 在**概觀**頁面上，按一下**電源供應器**。	電源供應器的相關資訊： • 名稱 • 容量 • 存在 • 電源狀態 • 輸入電壓 (僅適用於 PowerEdge MX 機箱)。

溫度感應器	• 在 **Dell EMC 機箱**頁面上，按一下**機箱** > **機箱清單**，然後按一下「產品服務編號」連結。
	• 在**概觀**頁面的左窗格中，選取**硬體**。
	• 在右窗格中，展開**溫度感應器**。
	或
	• 在**概觀**頁面上，按一下**溫度感應器**。
		溫度感應器的相關資訊：
		• 位置
		• 讀取中
		• 警告閾值
		  ○ 最大值
		  ○ 最小值
		• 嚴重閾值
		  ○ 最大值
		  ○ 最小值
		註: 針對 PowerEdge M1000e 機箱，將會顯示機箱溫度的相關資訊。如果是其他機箱，則會顯示機箱和關聯模組化伺服器的溫度感應器相關資訊。

I/O 模組	• 在 **Dell EMC 機箱**頁面上，按一下**機箱** > **機箱清單**，然後按一下「產品服務編號」連結。 • 在**概觀**頁面的左窗格中，選取**硬體**。 • 在右窗格中，展開 **I/O 模組**。 **或** • 在**概觀**頁面上，按一下 **I/O 模組**。	I/O 模組的相關資訊： • 插槽/位置 • 存在 • 名稱 • 光纖 • 產品服務編號 • 電源狀態 • 角色

表 10. 硬體清查資訊 (續)

硬體清查：元件	瀏覽 OMIVV	資訊
		• 韌體版本 • 硬體版本 • IP 位址 • 子網路遮罩 • 閘道 • MAC 位址 • DHCP 已啟用
光纖 (僅適用於 PowerEdge MX 機箱)	• 在 **Dell EMC 機箱**頁面上，按一下**機箱** > **機箱清單**，然後按一下「產品服務編號」連結。 • 在**概觀**頁面的左窗格中，選取**硬體**。 • 在右窗格中，展開**光纖**。 **或** • 在**概觀**頁面上，按一下**光纖**。	光纖元件相關資訊： • 健全狀況 • 光纖 • 說明 • 交換器計數 • 運算計數 • 上行鏈路計數 若要檢視與光纖相關聯的交換器，請選取光纖元件，下方格線便會顯示下列資訊： • 交換器 • 底架 • 插槽 • 機箱角色 • 交換器型號

PCIe	• 在 **Dell EMC 機箱**頁面上，按一下**機箱** > **機箱清單**，然後按一下「產品服務編號」連結。
	• 在**概觀**頁面的左窗格中，選取**硬體**。
	• 在右窗格中，展開 **PCIe**。
	或
	• 在**概觀**頁面上，按一下 **PCIe**。
		PCIe 的相關資訊：
		• PCIe 插槽
		  ○ 插槽
		  ○ 名稱
		  ○ 電源狀態
		  ○ 光纖
		• 伺服器插槽
		  ○ 名稱
		  ○ 編號
		• 插槽類型
		• 伺服器對應
		• 指派狀態
		• 已配置的插槽電源
		• PCI ID
		• 供應商 ID
		註: PCIe 資訊不適用於 M1000e 機箱。

iKVM — 僅適用於 PowerEdge M1000e	• 在 **Dell EMC 機箱**頁面上，按一下**機箱** > **機箱清單**，然後按一下「產品服務編號」連結。 • 在**概觀**頁面的左窗格中，選取**硬體**。在右窗格中，展開 **iKVM**。 **或** • 在**概觀**頁面上，按一下 **iKVM**。	iKVM 的相關資訊： • iKVM 名稱 • 存在 • 韌體版本 • 前面板 USB/視訊已啟用 • 允許存取 CMC CLI。 **註:** 機箱必須包含 iKVM 模組，iKVM 標籤才會顯示。

檢視韌體清查資訊

您可以檢視所選機箱的韌體相關資訊。

1. 在 OMIVV 首頁上，按一下**主機與機箱** > **機箱** > **機箱清單**。
   Dell EMC 機箱頁面隨即顯示。
2. 選取機箱，按一下產品服務編號連結。
   隨即顯示**概觀**頁面。
3. 在**概觀**頁面上，按一下**韌體**。
   隨後便會顯示韌體的下列相關資訊：
   - 元件
   - 目前版本

   在此頁面上，您也可以啟動 OpenManage Enterprise Modular 和 CMC。

檢視管理控制器資訊

您可以檢視所選機箱的管理控制器相關資訊。

1. 在 OMIVV 首頁上，按一下**主機與機箱** > **機箱** > **機箱清單**。
   Dell EMC 機箱頁面隨即顯示。
2. 選取機箱，按一下產品服務編號連結。
   隨即顯示**概觀**頁面。
3. 在**概觀**頁面上，按一下**管理控制器**。
   隨後便會顯示管理控制器的下列相關資訊：
   - 一般
     - 名稱
     - 韌體版本
     - 上次更新時間
     - 機箱位置
     - 硬體版本
   - 通用網路
     - DNS 網域名稱
     - DNS 使用 DHCP
     - MAC 位址
     - 冗餘模式
     - 硬體版本
   - IPv4 資訊
     - IPv4 已啟用
     - DHCP 已啟用
     - IP 位址
     - 子網路遮罩
     - 閘道
     - 慣用 DNS 伺服器
     - 備用 DNS 伺服器
   - IPv6 資訊
     - IPv6 已啟用
     - DHCP 已啟用
     - IP 位址
     - 連結本機位址
     - 閘道
     - 慣用 DNS 伺服器
     - 備用 DNS 伺服器
   - 本機存取組態

- 存在 Quick Sync 硬體
- 存在 LCD
- 存在 LED
- KVM 已啟用

註: 屬於 MCM 組態一部分的成員機箱，其網路相關資訊的幾個屬性不會顯示在**管理控制器**區段中。

檢視儲存裝置詳細目錄資訊

您可以檢視所選機箱的儲存裝置相關資訊。

1. 在 OMIVV 首頁上，按一下**主機與機箱** > **機箱** > **機箱清單**。
   Dell EMC 機箱頁面隨即顯示。
2. 選取機箱，按一下產品服務編號連結。
   隨即顯示**概觀**頁面。
3. 在**概觀**頁面上，按一下**儲存裝置**。

   隨後便會顯示儲存裝置的下列相關資訊：

   - 虛擬磁碟
   - 實體磁碟
   - 控制器
   - 機箱
   - 熱備援磁碟

   針對 MX 機箱，會顯示下列資訊：

   - 插槽編號
   - 插槽名稱
   - Model
   - 產品服務編號
   - 韌體版本
   - 資產標籤
   - 電源狀態
   - 指派模式

   對於 MX 機箱，如果您想要檢視磁碟機相關資訊，請按一下儲存運算模組。下方窗格會顯示以下磁碟機資訊：

   - 健全狀況
   - 狀態
   - 插槽
   - 插槽指派
   - 磁碟名稱
   - 容量
   - 匯流排通訊協定
   - 媒體

   如果 PowerEdge MX 機箱中的磁碟未指派，其插槽指派會顯示為 **NA**。

   若為 M1000e 機箱，如果有儲存裝置模組，就會在資料格檢視畫面顯示下列儲存裝置詳細資料 (不含任何其他資訊)：

   - 名稱
   - Model
   - 產品服務編號
   - IP 位址 (儲存裝置連結)
   - 光纖
   - 組群名稱
   - 群組 IP 位址 (儲存裝置群組的連結)。

   註: 按一下儲存底下反白顯示的連結，**檢視**表格便會顯示每個反白項目的詳細資料。在檢視表格中，如果按一下每行項目，就會顯示每個反白項目的其他資訊。

檢視保固資訊

您可檢視所選機箱的保固相關資訊。

1. 在 OMIVV 首頁上，按一下**主機與機箱** > **機箱** > **機箱清單**。
   Dell EMC 機箱頁面隨即顯示。
2. 選取機箱，按一下產品服務編號連結。
   隨即顯示**概觀**頁面。
3. 在**概觀**頁面上，按一下**保固**。

   保固的相關資訊：

   - 供應商
   - 說明
   - 狀態
   - 權利類型
   - 開始日期
   - 結束日期
   - 剩餘天數
   - 上次更新日期

   註: 若要檢視保固狀態，請務必執行保固工作。請參閱排程保固擷取工作 第頁的 89。

檢視機箱相關的主機

您可以檢視所選機箱相關主機的相關資訊。

1. 在 OMIVV 首頁上，按一下 **主機與機箱** > **機箱** > **機箱清單**。
   Dell EMC 機箱頁面隨即顯示。
2. 選取機箱，按一下產品服務編號連結。
   隨即顯示**概觀**頁面。
3. 在**概觀**頁面上，按一下**相關的主機**。

   關聯主機的下列相關資訊隨即顯示：

   - 主機名稱
   - 產品服務編號
   - Model
   - iDRAC IP
   - 位置
   - 插槽位置
   - 上一次清查

4. 若要檢視主機的詳細資訊，請選取主機。

檢視相關機箱資訊

機箱關係章節可顯示以 MCM 模式部署之 MX 機箱中各機箱之間的關係。

註: 相關機箱資訊僅適用於在 MCM 群組中設定的 PowerEdge MX 機箱。

1. 在 OMIVV 首頁上，按一下**主機與機箱** > **機箱** > **機箱清單**。
   Dell EMC 機箱頁面隨即顯示。
2. 選取機箱，按一下產品服務編號連結。
   隨即顯示**概觀**頁面。

   在**概觀**頁面上，其中**機箱關係**會顯示主要和成員機箱的所有相關機箱資訊。

管理 PowerEdge MX 機箱

MX7000X 機箱的管理方式與其他 Dell EMC 機箱 (例如 M1000e、VRTX 和 FX2) 的管理方式不同。

您可以在獨立模式中管理機箱並擁有管理模組公用 IP 和 iDRAC IP 的 MX 機箱。您也可以在多機箱管理 (MCM) 模式中設定擁有一個主要機箱和多個成員機箱的 MX 機箱。

Dell EMC OpenManage Enterprise-Modular 支援有線 MCM 群組。設為有線類型時，機箱會透過管理模組上的備援連接埠採用菊輪鍊或有線形式。您選取用來建立群組的機箱必須與至少一個機箱是菊輪鍊結。如需更多有關建立機箱群組的資訊，請參閱 *PowerEdge MX7000 機箱的 Dell EMC OpenManage Enterprise-Modular Edition 使用者指南*，網站為 dell.com/support。

您可以使用兩種方式管理 MX 機箱中的伺服器：

1. **使用主機認證設定檔管理伺服器**：當伺服器支援所有功能時，這是管理伺服器的標準和建議方式。在這種情況下，僅在完成 MX 主機清查後才探索機箱。如需建立主機認證設定檔的更多資訊，請參閱建立主機認證設定檔 第頁的 34。
2. **使用機箱認證設定檔管理伺服器**：如果您選擇使用機箱認證設定檔管理主機，則清查、監控、韌體及驅動程式更新等 OMIVV 功能會受到支援。如需有關使用機箱認證設定檔管理機箱和主機的更多資訊，請參閱建立機箱認證設定檔 第頁的 38。

註: OMIVV 不支援管理具有備份主要組態的 PowerEdge MX 機箱。

註: 如果停用 iDRAC 的 IPv4 位址，您可以選擇使用機箱認證設定檔來管理伺服器。如要使用機箱認證設定檔來管理伺服器，則無法支援下列 OMIVV 功能：

- iDRAC 鎖定模式
- 能夠使用此伺服器作為參照伺服器，以擷取系統設定檔
- 作業系統部署
- 取得或更新 CSIOR 狀態
- 伺服器組態相容性
- 與清查相關的部分資訊

註: 採用公用 IPv4 iDRAC IP 的主機也可以使用機箱認證設定檔予以管理。但因為這會不支援上述所列功能，因此不建議此方式。

機箱與主機管理使用整合機箱管理 IP

如果由主機認證設定檔管理的主機停用 iDRAC IPv4，主機清查會失敗且探索不到機箱。在這種情況下，必須手動新增機箱，且該機箱應與機箱認證設定檔建立關聯，如此才能管理該機箱及其關聯主機。

如果您選擇使用整合機箱管理 IP 管理您的主機，則會支援 OMIVV 功能，例如清查、監控、韌體及驅動程式更新。以下是使用整合機箱管理 IP 管理主機和機箱工作的概要說明：

1. 新增 MX 機箱。

   如需新增 MX 機箱的資訊，請參閱新增 PowerEdge MX 機箱 第頁的 97。

2. 建立機箱認證設定檔並為主機建立關聯。

   如需建立機箱認證設定檔的更多相關資訊，請參閱建立機箱認證設定檔 第頁的 38。

3. 檢視使用機箱認證設定檔管理的機箱與主機工作。
4. 檢視機箱與主機清查。

   如需有關主機和機箱清查的更多資訊，請參閱檢視主機清查工作 第頁的 68 和檢視機箱清查工作 第頁的 70。

5. 在使用機箱管理的主機上執行韌體更新。

   如需更多有關韌體更新的資訊，請參閱韌體更新 第頁的 111。

   註: 當主機使用機箱進行管理時，不支援裸機工作流程。

新增 PowerEdge MX 機箱

若主機具備有效的 IPv4 iDRAC IP，其便可新增至主機認證設定檔，並在主機清查期間，系統可自動探索到相關聯的 MX 機箱，然後顯示於 **Dell EMC 機箱**頁面上。

如果停用主機的 iDRAC IPv4，主機清查會失敗且探索不到機箱。在這種情況下，必須手動新增 MX 機箱，且該機箱應與機箱認證設定檔建立關聯，如此才能管理該機箱及其關聯主機。

若要手動新增 MX 機箱，請執行以下動作：

1. 在 **OMIVV** 首頁上，按一下**主機與機箱** > **機箱**。
2. 在 **Dell EMC 機箱**頁面上，按一下**新增 MX 機箱**。
3. 進入管理模組 IPv4 或 FQDN 或主機名稱，然後按一下**確定**。

   當您輸入 IP 時，若該 IP 是由 OMIVV 管理，其會經過驗證。

   註: 使用主機名稱或 FQDN 新增機箱前，請確定已在 DNS 中建立有效的正向與反向查閱項目。

   註: 若您輸入 FQDN，機箱 URL 會顯示該 FQDN。

   機箱新增至 **Dell EMC 機箱**頁面。
4. 透過建立機箱認證設定檔的方式，將主機與機箱認證設定檔建立關聯。如需建立機箱認證設定檔的更多相關資訊，請參閱建立機箱認證設定檔 第頁的 38。

註: 如果您是輸入 MX 機箱 IP 以外的其他 IP，測試連線會失敗，且無效的輸入內容會留在 **Dell EMC 機箱**頁面上。只有成功通過驗證的機箱會與機箱認證設定檔建立關聯。

註: 如果主機不在與新增的 MX 機箱建立關聯的已註冊 vCenter 中，測試連線會失敗。

註: 對於在 MCM 組態中設定的 PowerEdge MX 機箱，主要和成員必須要有相同的認證。

MX 機箱韌體更新

在排程韌體更新之前，請確定環境符合下列條件：

- 請確定 MX 機箱是機箱認證設定檔的一部分，並已成功清查。
- 如果有任何主機正在進行韌體更新，則無法更新機箱韌體。

註: 透過使用 MX 機箱的韌體更新功能，您僅能更新管理模組韌體。

1. 在 OMIVV 首頁上，按一下**主機與機箱** > **機箱** > **機箱清單** > **MX 機箱韌體更新**。
2. 閱讀精靈中**機箱韌體更新**頁面上的指示，然後按一下**開始使用**。
3. 從 **MX 機箱清單**中，選取一或多個 MX 機箱，然後按一下**下一步**。

   如果環境中未符合下列任何一個條件，機箱就不會顯示：

   - 機箱韌體更新正在從 OMIVV 進行。
   - 機箱認證設定檔不會為機箱建立。
   - 機箱清查未成功。

   針對具備 MCM 組態的 PowerEdge MX 機箱，您僅能選取主要機箱。系統會自動選取成員機箱。
4. 在**選取更新來源**頁面中，執行下列操作：
   a. 從下拉式功能表選擇適當的韌體儲存庫設定檔。
   b. 根據您選擇的機箱和韌體儲存庫設定檔，從已識別的系統類別中，選擇適當的套裝。
5. 在**選取韌體元件**頁面上，選取需要更新的韌體元件，然後按一下**下一步**。

   不能選取比目錄中可用版本更舊，或相同等級 (最新) 的元件。若要選取列為降級狀態元件，按一下**允許韌體降級**。

   在與 MCM 組態相關連的 PowerEdge MX 機箱中，即使未選取**允許韌體降級**核取方塊，也可降級韌體版本。

   無法僅選取要更新或降級的成員機箱。選取主要機箱會自動選取成員機箱。

   若要選取所有頁面上的所有韌體元件，請按一下。

   若要清除所有頁面上的所有韌體元件，請按一下。
6. 在**排程工作**頁面上，執行下列步驟：
   a. 輸入韌體更新工作名稱和說明。說明是選填欄位。

請務必填寫韌體更新工作的名稱，並確認未使用已被使用的名稱。如果您清除韌體更新工作的名稱，便可再次重複使用該工作名稱。

b. 選取適當的排定選項以套用更新。

7. 檢閱**檢閱摘要**頁面上的韌體更新詳細資料，然後按一下**完成**。

表 11. 每個部署模式的並行 MX 機箱韌體更新總數

部署模式	並行機箱韌體更新數量
小型	1
中型	1
大型	2
超大	2

17

主機管理

檢視 OMIVV 主機

您可以在 **OMIVV 主機**頁面上，檢視所有 OMIVV 管理的主機。

1. 在 OMIVV 首頁上，按一下**主機與機箱** > **主機**。
2. 在 **OMIVV 主機**標籤中，檢視下列資訊：
   - **主機名稱**—顯示主機的 IP 位址。若要檢視主機資訊，請選取主機。
   - **健全狀況**—顯示主機的健全狀況狀態。

     若要根據每個 Dell EMC 主機的健全狀況狀態進行篩選，請按一下搜尋旁的篩選圖示。
   - **vCenter**—顯示主機的 vCenter IP 位址。
   - **叢集** — 如果 Dell EMC 主機在叢集中，顯示叢集名稱。
   - **主機認證設定檔**—顯示主機認證設定檔的名稱。

監控單一主機

OMIVV 可讓您檢視單一主機的詳細資訊。您可以在**主機和叢集**頁面上檢視所有 OMIVV 主機。若要檢視更多資訊，請選取特定的 OMIVV 管理主機，然後前往**監視** > **OMIVV 主機資訊**。

檢視主機摘要資訊

您可以在**摘要**頁面上檢視個別主機的主機摘要詳細資料，該頁面會顯示各種 Portlet。兩個 portlet 適用於 OMIVV。這兩個 Portlet 是：

- **OMIVV 主機健全狀況**
- **OMIVV 主機資訊**

您可以將這兩個 Portlet 拖放到您要的位置，還可以依您的需求格式化及自訂，就像格式化及自訂其他 Portlet 一樣。檢視主機摘要詳細資料：

1. 在 OMIVV 首頁上，展開**功能表**，然後選取**主機和叢集**。
2. 在左窗格中，選取特定主機。
3. 在右窗格中，按一下**摘要**。
4. 向下捲動即可檢視 OMIVV 伺服器管理 Portlet。

   您可以在 **OMIVV 主機資訊**和 **OMIVV 主機健全狀況**區段中檢視下列資訊：

表 12. OMIVV 主機資訊

資訊	說明
產品服務編號	顯示伺服器的產品服務編號。請使用此 ID 撥打電話請求支援。
機型名稱	顯示伺服器型號名稱。
記憶體錯誤回復	顯示 BIOS 屬性的狀態。BIOS 屬性會在初始設定伺服器時於 BIOS 中啟用，並顯示伺服器的記憶體操作模式。變更記憶體操作模式值時，請重新啟動您的系統。這適用於支援記憶體錯誤回復 (FRM) 選項，以及執行 ESXi 5.5 或更新版本的 PowerEdge 伺服器。BIOS 屬性的四個不同值是：

表 12. OMIVV 主機資訊 (續)

資訊	說明
	• 已啟用及防護：這個值表示系統獲得支援，作業系統版本是 ESXi 5.5 或更新版本，而且在 BIOS 中將記憶體操作模式設定為 FRM。 • NUMA 已啟用並受到防護：這個值表示系統獲得支援，作業系統版本是 ESXi 5.5 以上，而且在 BIOS 將記憶體作業模式設定為 NUMA。 • 已啟用但未防護：這個值表示它支援搭載作業系統低於 ESXi5.5 的系統。 • 已停用：這個值表示它支援搭載任何作業系統版本的有效系統，而且 BIOS 中的記憶體操作模式不是設定為 FRM。 • 空白：如果 BIOS 不支援記憶體錯誤回復，就不會顯示 FRM 屬性。
系統鎖定模式	顯示 iDRAC 8 及更新版本伺服器的 iDRAC 鎖定模式的狀態。關閉的鎖代表 iDRAC 鎖定模式已開啟，而開啟的鎖代表 iDRAC 鎖定模式已關閉。
識別	顯示資訊如下： • 主機名稱 — 顯示受 OMIVV 管理的主機名稱 • 電源狀態 — 顯示電源為開啟或關閉。 • iDRAC IP — 顯示 iDRAC IP 位址 • 管理 IP — 顯示管理 IP 位址 • 主機認證設定檔 — 顯示此主機的主機認證設定檔名稱 • 型號 — 顯示 Dell EMC 伺服器型號 • 產品服務編號 — 顯示伺服器的產品服務編號。 • 資產標籤 — 顯示資產標籤 • 剩下的保固天數 — 顯示剩餘保固天數 • 上次清查掃描 — 顯示上次清查掃描的日期和時間
Hypervisor 與韌體	顯示資訊如下： • Hypervisor — 顯示 Hypervisor 版本 • BIOS 版本 — 顯示 BIOS 版本 • 遠端存取卡版本 — 顯示遠端存取卡版本
管理主控台	顯示啟動遠端存取主控台 (iDRAC) 的連結。
主機的動作	若要以不同的時間間隔閃爍，請將實體伺服器設定為以不同的時間間隔閃爍。請參閱設定閃爍指示燈 第頁的 126。

表 13. OMIVV 主機健全狀況

資訊	說明
OMIVV 主機健全狀況	元件的健全狀況是以圖形表示以下所有主要主機伺服器元件的狀態：伺服器全域狀態、伺服器、電源供應器、溫度、電壓、處理器、電池、侵入、硬體記錄、電源管理、電源及記憶體。機箱狀況參數適用於 VRTX 1.0 版 (含) 以後、M1000e 4.4 版 (含) 以後的機型。若為 4.3 以前的版本，只會顯示兩個健全狀況指示燈：良好和警告或嚴重 (裡面有橘色驚嘆號的倒三角形)。整體健全狀況是根據健全狀況參數最差的機箱來表示狀況。選項包括： • 良好 (綠色勾號) — 元件運作正常。 • 警告 (有驚嘆號的黃色三角形) — 元件有非重大錯誤。 • 嚴重 (紅色 X) — 元件有嚴重故障。 • 不明 (問號) — 狀態不明的元件。

例如，如果有五個良好符號和一個警告符號，整體健全狀況會顯示為警告。

註: 配備接線式 PSU 的主機或模組化伺服器將無法使用電源監控資訊。

檢視 OMIVV 主機資訊

您可在 **OMIVV 主機資訊**頁面上，檢視所有 OMIVV 管理之主機的硬體、儲存裝置、韌體、電源監控、保固和系統事件記錄資訊。

1. 在 OMIVV 首頁上，展開**功能表**，然後選取**主機和叢集**。
2. 在左窗格中，選取主機，然後按一下**監視** > **OMIVV 主機資訊**。

檢視主機的硬體資訊

表 14. 單一主機的硬體資訊

硬體：*元件*	資訊
FRU	• **零件名稱**—顯示 FRU 零件名稱。 • **零件編號**—顯示 FRU 零件編號。 • **製造廠商**—顯示製造廠商名稱。 • **序號**—顯示製造商的序號。 • **製造日期**—顯示製造日期。
處理器	• **插槽**—顯示插槽編號。 • **速度**—顯示目前的速度。 • **品牌**—顯示處理器品牌。 • **版本**—顯示處理器版本。 • **核心**—顯示此處理器中的核心數目。
電源	• **類型** — 顯示電源供應器的類型。電源供應器類型包括： ○ 不明 ○ 線性 ○ 切換中 ○ 電池 ○ UPS ○ 轉換器 ○ 穩壓器 ○ 交流電 ○ 直流電 ○ VRM • **位置**—顯示電源供應器的位置，例如插槽 1。 • **輸出 (瓦特)**—顯示功率 (瓦特)。
記憶體	• **記憶體插槽**—顯示已使用、總計及可用的記憶體計數。 • **記憶體容量**—顯示已安裝的記憶體、總記憶體容量及可用記憶體。 • **插槽**—顯示 DIMM 插槽。 • **大小**—顯示記憶體大小。 • **類型**—顯示記憶體類型。
NIC	• **總計**—顯示可用網路介面卡的總計數。 • **名稱**—顯示 NIC 名稱。 • **製造廠商**—只顯示製造廠商的名稱。 • **MAC 位址**—顯示 NIC 的 MAC 位址。
PCI 插槽	• **PCI 插槽**—顯示已使用、總計及可用的 PCI 插槽。 • **插槽**—顯示插槽。

表 14. 單一主機的硬體資訊 (續)

硬體：*元件*	資訊
	• **製造廠商**—顯示 PCI 插槽的製造廠商名稱。 • **說明**—顯示 PCI 裝置的說明。 • **類型**—顯示 PCI 插槽類型。 • **寬度**—顯示資料匯流排寬度 (如果可用)。
遠端存取卡	• **IP 位址**—顯示遠端存取卡的 IP 位址。 如果使用整合 IP 位址管理主機，本節將不會顯示 iDRAC IP。 • **MAC 位址**—顯示遠端存取卡的 MAC 位址。 • **RAC 類型**—顯示遠端存取卡的類型。 • **URL**—顯示與此主機關聯之 iDRAC 的即時 URL。

檢視主機的儲存裝置資訊

您可檢視虛擬磁碟、控制器、機櫃及關聯實體磁碟的計數，以及其通用熱備援磁碟與專用熱備援磁碟的計數。若要檢視每個儲存裝置元件的更多資訊，請從**檢視**下拉式功能表中，選取特定元件。

若主機使用機箱進行管理，則不會顯示控制器、機櫃、全域熱備援磁碟和專用熱備援磁碟完整的儲存裝置資訊。

註: 當使用機箱設定檔作為主機管理方式時，如果您按一下**儲存裝置**，然後從**檢視**下拉式功能表中選取以下項目：

- **機櫃** — 儲存裝置機櫃的控制器 ID 會顯示為 0，而非正確的控制器 ID。
- **實體磁碟** — HDD 的媒體類型會顯示為**磁碟機**，而非**硬碟機**。

表 15. 單一主機的儲存裝置詳細資料

資訊	說明
虛擬磁碟	• **名稱**—顯示虛擬磁碟的名稱。 • **裝置 FQDD**—顯示 FQDD。 • **實體磁碟**—顯示虛擬磁碟所在的實體磁碟。 • **容量**—顯示虛擬磁碟的容量。 • **配置**—顯示虛擬儲存裝置的配置類型，這代表為此虛擬磁碟設定的 RAID 類型。 • **媒體類型** — 顯示 SSD 或 HDD。 若要檢視等量大小、匯流排通訊協定和快取原則等資訊，請選取虛擬磁碟。 • **控制器 ID**—顯示控制器 ID。 • **裝置 ID**—顯示裝置 ID。 • **等量大小**—顯示等量大小，其為每個等量在單一磁碟上耗用的空間量。 • **匯流排通訊協定** — 顯示虛擬磁碟內的實體磁碟所使用的技術。可能的值如下： ○ SCSI ○ SAS ○ SATA • **預設讀取原則** — 顯示控制器支援的預設讀取原則。選項包括： ○ 預先讀取 ○ 未預先讀取 ○ 調整預先讀取 ○ 讀取快取已啟用 ○ 讀取快取已停用 • **預設寫入原則** — 顯示控制器支援的預設寫入原則。選項包括： ○ 回寫 ○ 強制回寫 ○ 回寫已啟用

表 15. 單一主機的儲存裝置詳細資料 (續)

資訊	說明
	○ 寫入 ○ 已保護啟用的寫入快取 ○ 寫入快取已停用 ● **快取原則**—啟用快取原則時顯示。
實體磁碟 當您從**檢視**下拉式功能表選取此選項時，會顯示**篩選**下拉式清單。 以下是篩選器中可以使用的選項： ● **所有實體磁碟** ● **通用熱備援磁碟** ● **專用熱備援磁碟** ● 最後一個選項會顯示虛擬磁碟的自訂名稱。	● **名稱**—顯示實體磁碟的名稱。 ● **裝置 FQDD**—顯示裝置 FQDD。 ● **容量**—顯示實體磁碟容量。 ● **磁碟狀態** — 顯示實體磁碟的狀態。選項包括： ○ 線上 ○ 就緒 ○ 受損 ○ 故障 ○ 離線 ○ 重建中 ○ 不相容 ○ 已移除 ○ 已清除 ○ 偵測到 SMART 警示 ○ 不明 ○ 外來 ○ 不支援 ● **已設定**—顯示是否已設定磁碟。 ● **熱備援類型** (不適用於 PCIe) — 顯示熱備援磁碟類型。選項包括： ○ 無—沒有熱備援磁碟。 ○ 通用 — 未使用的備份磁碟屬於磁碟群組 ○ 專用 — 未使用的備份磁碟指派給單一虛擬磁碟。虛擬磁碟內的實體磁碟故障時，熱備援磁碟隨即啟動，取代故障的實體磁碟，既不會中斷系統，也不需要人為介入。 ● **虛擬磁碟**—顯示虛擬磁碟名稱。 ● **匯流排通訊協定**—顯示匯流排通訊協定。 ● **控制器 ID**—顯示控制器 ID。 ● **媒體類型** — 顯示 SSD 或 HDD。 ● **剩餘已評等耐寫度** — 顯示 SSD 剩餘耐寫度。 ● **連接器 ID**—顯示連接器 ID。 ● **機櫃 ID**—顯示機櫃 ID。 ● **裝置 ID**—顯示裝置 ID。 ● **型號**—顯示實體儲存磁碟的型號。 ● **零件編號**—顯示儲存裝置零件編號。 ● **序號**—顯示儲存裝置序號。 ● **廠商**—顯示儲存裝置廠商名稱。
控制器	● **控制器 ID**—顯示控制器 ID。 ● **名稱**—顯示控制器名稱。 ● **裝置 FQDD**—顯示裝置的 FQDD。 ● **韌體版本**—顯示韌體版本。 ● **最低必要韌體** — 顯示最低要求的韌體。如果韌體過期且有較新版本可使用，就會填入此欄位。 ● **驅動程式版本**—顯示驅動程式版本。 ● **巡查讀取狀態**—顯示巡查讀取狀態。 ● **快取大小**—顯示快取大小。

表 15. 單一主機的儲存裝置詳細資料 (續)

資訊	說明
	註: 本節將顯示晶片組控制器資訊。這不會顯示在 iDRAC UI 的儲存控制器區段中，但您可以透過 iDRAC 的清查頁面檢視此資訊。
機箱	• **控制器 ID**——顯示控制器 ID。 • **連接器 ID**——顯示連接器 ID。 • **機櫃 ID**——顯示機櫃 ID。 • **名稱**——顯示機櫃名稱。 • **裝置 FQDD**——顯示裝置 FQDD。 • **產品服務編號**——顯示產品服務編號。

檢視單一主機的韌體資訊

下列與韌體相關的資訊隨即顯示：

- **名稱**——顯示此主機上所有韌體的名稱。
- **類型**——顯示韌體的類型。
- **版本**——顯示此主機上所有韌體的版本。
- **安裝日期**——顯示安裝日期。

註: 當主機是使用機箱認證設定檔進行管理時，韌體清查資料會顯示幾個額外的元件，例如 Lifecycle Controller 和軟體 RAID。

您可從此頁面啟動韌體更新和設定系統鎖定模式精靈。

檢視單一主機的電源監視資訊

您可以檢視一般資訊、閾值、保留功率容量和能源統計數字等資訊。

- **一般資訊**——顯示功率預算和目前的設定檔名稱。
- **閾值**——以瓦數顯示警告與故障閾值。
- **保留功率容量**——以瓦數顯示瞬間與尖峰保留功率容量。

能源統計數字

- **類型**——顯示能源統計資料類型。
- **測量開始時間 (主機時間)** — 顯示主機開始耗用能源的日期和時間。
- **測量完成時間 (主機時間)** — 顯示主機停止耗用能源的日期和時間。
- **註:** 主機時間 (如這裡使用的情況) 表示主機所在位置的當地時間。

  讀取——顯示一分鐘內的讀數平均值。
- **尖峰時間 (主機時間)**——顯示主機尖峰安培的日期和時間。
- **尖峰讀取**——顯示系統尖峰電源統計資料，即系統耗用的尖峰電源 (瓦數)。

註: 配備接線式 PSU 的主機或模組化伺服器將無法使用電源監控資訊。

註: 若為使用機箱管理的主機，將不會顯示完整的電源監視資訊。

檢視單一主機的保固資訊

若要檢視保固狀態，請務必執行保固工作。請參閱排程保固擷取工作 第頁的 89。**保固狀態**頁面可讓您監控保固到期日期。保固設定可控制從 Dell 線上擷取伺服器保固資訊的時間，方法是藉由啟用或停用保固排程，然後設定最少天數閾值警示。

- **提供者**——顯示保固提供者的名稱。
- **說明** — 顯示說明。
- **狀態** — 顯示主機的保固狀態。狀態選項包括：
  - 有效——主機在保固內，未超過任何閾值。
  - 警告——主機啟用中，但超出警告閾值。

- 嚴重 — 與警告相同，但屬於嚴重閾值
- 已過期—此主機的保固已過期。
- 未知 — OMIVV 未取得保固狀態，因為尚未執行保固工作、取得資料時發生錯誤，或是系統沒有保固。

- **權利類型**—顯示下列狀態：
  - 初始
  - 延伸
  - 過期
- **開始日期**—顯示保固的開始日期。
- **結束日期**—顯示保固的結束日期。
- **到期天數**—顯示保固的剩餘天數。
- **上次更新**—保固的最後一次更新。

檢視單一主機的系統事件記錄資訊

系統事件記錄 (SEL) 會針對 OMIVV 探索到的硬體提供狀態資訊，並顯示以下資訊：

- **狀態**—狀態圖示有好幾種，例如資訊 (藍色驚嘆號)、警告 (內含驚嘆號的黃色三角形)、錯誤 (紅色 X) 以及不明 (內含 ? 的方塊)。

  嚴重程度定義如下：
  - 資訊
  - 警告
  - 錯誤
- **時間 (伺服器時間)**—表示事件發生的時間與日期。

若要清除所有系統事件記錄，請按一下**清除記錄**。隨後便會顯示訊息，以表示在清除記錄後無法恢復記錄資料。

監控叢集與資料中心上的主機

OMIVV 可讓您檢視資料中心或叢集中所有主機的詳細資訊。

檢視 OMIVV 資料中心和叢集資訊

檢視資料中心和叢集的概觀

您可檢視資料中心或叢集資訊、系統鎖定模式、硬體資源和保固資訊等資訊。若要檢視此頁面的相關資訊，請確定清查已順利完成。OMIVV 資料中心和叢集檢視會直接報告 iDRAC 中的資料。

1. 在 OMIVV 首頁上，展開**功能表**，然後選取**主機和叢集**。
2. 在左窗格中，選取資料中心或叢集，然後按一下**監視** > **OMIVV 叢集或資料中心資訊**。
3. 若要檢視更多資訊，請選取特定主機。

   IDRAC IP、機箱 URL、CPU 和記憶體等資訊會顯示在頁面最下方的水平窗格中。

表 16. 資料中心和叢集的概觀

資訊	說明
資料中心/叢集資訊	顯示資訊如下： • 資料中心/叢集名稱 • 受管理主機的數目 • 能源消耗總量
系統鎖定模式	顯示 iDRAC 鎖定模式的狀態。主機總數的 iDRAC 鎖定模式狀態顯示如下： • 已開啟

表 16. 資料中心和叢集的概觀 (續)

資訊	說明
	• 已關閉 • 不適用 (僅適用於 iDRAC9 型伺服器) 如需 iDRAC9 型伺服器的清單，請參閱相容性比較表。
硬體資源	顯示資訊如下： • 總處理器 • 總記憶體 • 虛擬磁碟容量
保固摘要	顯示所選主機的保固狀態。狀態選項包括： • 過期的保固 • 作用中的保固 • 超過警告閾值 • 超過嚴重閾值 • 未知的保固 針對有多項或不同保固 (例如，ND 和 4DP 的服務等級準則) 的任何主機或機箱，OMIVV 會根據剩餘最短保固天數的保固類型考慮狀態。
主機	顯示主機名稱
產品服務編號	顯示主機產品服務編號
機型	顯示 PowerEdge 機型
資產標籤	顯示資產標籤 (如果已設定)
機箱產品服務編號	顯示機箱產品服務編號 (如果有)
作業系統版本	顯示 ESXi 作業系統版本
位置	僅限刀鋒：顯示插槽位置。若是其他，則會顯示「不適用」
系統鎖定模式	僅適用於 iDRAC9 型伺服器：顯示主機的 iDRAC 鎖定模式，包括已開啟、已關閉或不明。 對於 iDRAC9 型之前的所有 PowerEdge 伺服器，顯示的系統鎖定模式是**不適用**。如需 iDRAC9 型伺服器的清單，請參閱相容性比較表。
iDRAC IP	顯示 iDRAC IP 位址
服務主控台 IP	顯示服務主控台 IP
CMC 或管理模組 URL	顯示 CMC 或管理模組 URL (模組化伺服器的機箱 URL)，或顯示「不適用」
CPU 數目	顯示 CPU 數目
記憶體	顯示主機記憶體
電源狀態	主機有電源時會顯示。
上一次清查	顯示上次清查工作日期、星期幾與時間
主機認證設定檔	顯示主機認證設定檔的名稱
遠端存取卡版本	顯示遠端存取卡版本
BIOS 韌體版本	顯示 BIOS 韌體版本

檢視資料中心和叢集的硬體資訊

表 17. 資料中心和叢集的硬體資訊

硬體：*元件*	**資訊**
硬體：FRU	• **主機**—顯示主機名稱。 • **產品服務編號** — 顯示主機的產品服務編號。 • **零件名稱**—顯示 FRU 零件名稱。 • **零件編號**—顯示 FRU 零件編號。 • **製造廠商**—顯示製造廠商名稱。 • **序號**—顯示製造商的序號。 • **製造日期**—顯示製造日期。
硬體：處理器	• **主機**—顯示主機名稱。 • **產品服務編號** — 顯示主機的產品服務編號。 • **插槽**—顯示插槽編號。 • **速度**—顯示目前的速度。 • **品牌**—顯示處理器品牌。 • **版本**—顯示處理器版本。 • **核心**—顯示此處理器中的核心數目。

硬體：電源供應器	• **主機**—顯示主機名稱。
	• **產品服務編號** — 顯示主機的產品服務編號。
	• **類型** — 顯示電源供應器的類型。電源供應器類型包括：
	  ○ 不明
	  ○ 線性
	  ○ 切換中
	  ○ 電池
	  ○ UPS
	  ○ 轉換卡
	  ○ 穩壓器
	  ○ 交流電
	  ○ 直流電
	  ○ VRM
	• **位置**—顯示電源供應器的位置，例如插槽 1。
	• **輸出 (瓦特)**—顯示功率 (瓦特)。
	• **狀態** — 顯示電源供應器的狀態。狀態選項包括：
	  ○ 其他
	  ○ 不明
	  ○ 正常
	  ○ 嚴重
	  ○ 不嚴重
	  ○ 可復原
	  ○ 無法復原
	  ○ 高
	  ○ 低

硬體：記憶體	• **主機**—顯示主機名稱。 • **產品服務編號** — 顯示主機的產品服務編號。 • **插槽**—顯示 DIMM 插槽。 • **大小**—顯示記憶體大小。 • **類型**—顯示記憶體類型。
硬體：NIC	• **主機**—顯示主機名稱。 • **產品服務編號** — 顯示主機的產品服務編號。

表 17. 資料中心和叢集的硬體資訊 (續)

硬體：*元件*	資訊
	• **名稱**—顯示 NIC 名稱。 • **製造廠商**—只顯示製造廠商的名稱。 • **MAC 位址**—顯示 NIC 的 MAC 位址。
硬體：PCI 插槽	• **主機**—顯示主機名稱。 • **產品服務編號** — 顯示主機的產品服務編號。 • **插槽**—顯示插槽。 • **製造廠商**—顯示 PCI 插槽的製造廠商名稱。 • **說明**—顯示 PCI 裝置的說明。 • **類型**—顯示 PCI 插槽類型。 • **寬度**—顯示資料匯流排寬度 (如果可用)。
硬體：遠端存取卡	• **主機**—顯示主機名稱。 • **產品服務編號** — 顯示主機的產品服務編號。 • **IP 位址**—顯示遠端存取卡的 IP 位址。 • **MAC 位址**—顯示遠端存取卡的 MAC 位址。 • **RAC 類型**—顯示遠端存取卡的類型。 • **URL**—顯示與此主機關聯之 iDRAC 的即時 URL。

資料中心和叢集的儲存裝置資訊

表 18. 資料中心和叢集的儲存裝置詳細資料

儲存裝置：磁碟	說明

實體磁碟	• **主機**—顯示主機名稱。
	• **產品服務編號** — 顯示主機的產品服務編號。
	• **容量**—顯示實體磁碟容量。
	• **磁碟狀態** — 顯示實體磁碟的狀態。選項包括：
	  ○ 線上
	  ○ 就緒
	  ○ 受損
	  ○ 故障
	  ○ 離線
	  ○ 重新建置
	  ○ 不相容
	  ○ 已移除
	  ○ 已清除
	  ○ SMART 警示偵測
	  ○ 不明
	  ○ 外來
	  ○ 不支援
	  註: 如需這些警示所含意義的詳細資訊，請參閱 Dell EMC OpenManage Server Administrator 儲存管理使用者指南，網址是： `dell.com/support`
	• **型號**—顯示實體儲存磁碟的型號。
	• **上次清查**—顯示上次執行清查的日、月和時間。
	• **狀態**—顯示主機狀態。
	• **控制器 ID**—顯示控制器 ID。
	• **連接器 ID**—顯示連接器 ID。
	• **機櫃 ID**—顯示機櫃 ID。
	• **裝置 ID**—顯示裝置 ID。
	• **匯流排通訊協定**—顯示匯流排通訊協定。

表 18. 資料中心和叢集的儲存裝置詳細資料 (續)

儲存裝置：磁碟	說明
	• **剩餘已評等耐寫度** — 顯示固態硬碟剩餘耐寫度。 • **熱備援類型** (不適用於 PCIe) — 顯示熱備援磁碟類型。選項包括： ○ 無—沒有熱備援磁碟。 ○ 通用 — 未使用的備份磁碟屬於磁碟群組 ○ 專用 — 未使用的備份磁碟指派給單一虛擬磁碟機。虛擬磁碟機中的實體磁碟故障時，熱備援磁碟隨即啟動，取代故障的實體磁碟，既不會中斷系統，也不需要人為介入 • **零件編號**—顯示儲存裝置零件編號。 • **序號**—顯示儲存裝置序號。 • **廠商名稱**—顯示儲存裝置廠商名稱。
虛擬磁碟	• **主機**—顯示主機名稱。 • **產品服務編號** — 顯示主機的產品服務編號。 • **名稱**—顯示虛擬磁碟的名稱。 • **實體磁碟**—顯示虛擬磁碟所在的實體磁碟。 • **容量**—顯示虛擬磁碟的容量。 • **配置** — 顯示虛擬儲存裝置的配置類型。這代表為此虛擬磁碟機設定的 RAID 類型。 • **上次清查**—顯示上次執行清查是星期幾、日期和時間。 • **控制器 ID**—顯示控制器 ID。 • **裝置 ID**—顯示裝置 ID。 • **媒體類型** — 顯示固態硬碟或 HDD。 • **匯流排通訊協定** — 顯示虛擬磁碟內的實體磁碟所使用的技術。可能的值如下： ○ SCSI ○ SAS ○ SATA ○ PCIe • **Stripe 大小**—顯示 stripe 大小，其提供每個等量在單一磁碟上耗用的空間量。 • 預設讀取原則 — 顯示控制器支援的預設讀取原則。選項包括： ○ 預先讀取 ○ 未預先讀取 ○ 調整預先讀取 ○ 讀取快取已啟用 ○ 讀取快取已停用 • **預設寫入原則** — 顯示控制器支援的預設寫入原則。選項包括： ○ 回寫 ○ 強制回寫 ○ 回寫已啟用 ○ 寫入 ○ 已保護啟用的寫入快取 ○ 寫入快取已停用 • **磁碟快取原則**—顯示控制器支援的預設快取原則。選項包括： ○ 已啟用 — 快取 I/O ○ 已停用 — 直接 I/O

查看資料中心和叢集的韌體資訊

隨即顯示每一韌體元件的下列相關資訊：

- **主機**—顯示主機名稱。
- **產品服務編號** — 顯示主機的產品服務編號。
- **名稱**—顯示此主機上所有韌體的名稱。
- **版本**—顯示此主機上所有韌體的版本。

查看資料中心和叢集的電源監視資訊

- **主機**—顯示主機名稱。
- **產品服務編號** — 顯示主機的產品服務編號。
- **目前設定檔**—顯示電源設定檔，最佳化系統效能和節省能源。
- **能源耗用**—顯示主機的能源耗用。
- **尖峰保留容量**—顯示尖峰電源的保留容量。
- **功率預算**—顯示此主機的功率容量。
- **警告閾值**—顯示系統的溫度探針警告閾值組態最大值。
- **故障閾值**—顯示系統的溫度探針故障閾值組態最大值。
- **瞬間保留容量**—顯示主機即時空餘空間容量。
- **能源消耗開始日期** — 顯示主機開始耗用能源的日期和時間
- **能源消耗結束日期** — 顯示主機停止耗用能源的日期和時間
- **系統尖峰電源**—顯示主機尖峰電源。
- **系統尖峰電源開始日期** — 顯示主機尖峰電源開始的日期和時間
- **系統尖峰電源結束日期** — 顯示主機尖峰電源結束的日期和時間
- **系統尖峰安培**—顯示主機尖峰安培。
- **系統尖峰安培開始日期**—顯示主機尖峰安培的開始日期和時間。
- **系統尖峰安培結束日期**—顯示主機尖峰安培的結束日期與時間。

查看資料中心和叢集的保固資訊

若要檢視保固狀態，請務必執行保固工作。請參閱排程保固擷取工作 第頁的 89。**保固摘要**頁面可讓您監控保固到期日期。保固設定可控制從 Dell 線上擷取伺服器保固資訊的時間，方法是藉由啟用或停用保固排程，然後設定最少天數閾值警示。

- **保固摘要**—主機保固摘要會使用圖示來顯示，以視覺化方式顯示每個狀態類別中的主機數目。
- **主機**—顯示主機名稱。
- **產品服務編號** — 顯示主機的產品服務編號。
- **說明** — 顯示說明。
- **保固狀態** — 顯示主機的保固狀態。狀態選項包括：
  - 有效—主機在保固內，未超過任何閾值。
  - 警告—主機啟用中，但超出警告閾值。
  - 嚴重 — 與警告相同，但屬於嚴重閾值
  - 已過期—此主機的保固已過期。
  - 未知—OpenManage Integration for VMware vCenter 未取得保固狀態，因為尚未執行保固工作、取得資料時發生錯誤或是系統沒有保固。
- **剩下天數** — 顯示保固的剩餘天數。

韌體更新

OMIVV 可讓您在受管理的主機上，執行 BIOS 和韌體更新工作。您可以在多個叢集或非叢集主機上，執行並行韌體更新工作。但您不可以在同一叢集的兩部主機上，執行並行韌體更新。

註: 在多重裝置環境中，若要在叢集或主機上執行韌體更新，請確定已載入以目標 vCenter 註冊的裝置。

以下是執行韌體更新的兩種方法：

- 單一 DUP—藉由直接指向 DUP 位置 (CIFS 或 NFS) 來執行 iDRAC 和 BIOS 的韌體更新。單一 DUP 方法只能用於主機層級。
- 儲存庫設定檔—執行韌體和驅動程式更新。這種方法在主機層級和叢集層級兩者都適用。

  以下是用於韌體與驅動程式更新的儲存庫設定檔：

  - 韌體儲存庫—使用韌體目錄取得韌體資訊的儲存庫設定檔。

    以下是兩種類型的韌體儲存庫：

    - 使用者建立的韌體儲存庫
    - 原廠建立的韌體儲存庫：以下是原廠建立的兩種目錄：原廠建立的目錄不適用於 vSAN 叢集韌體更新和基準建立。

- Dell 預設目錄：使用 Dell EMC 線上目錄取得最新韌體資訊的原廠建立韌體儲存庫設定檔。如果裝置沒有網際網路連線，請修改此儲存庫來指向本機 CIFS 或 NFS 或 HTTP 或 HTTPS 為基礎的共用區。
- 已驗證的 MX 堆疊目錄：使用 Dell EMC 線上目錄為 MX 機箱及其對應模組取得經驗證的韌體資訊之原廠建立韌體儲存庫設定檔。

○ 驅動程式儲存庫——包含可用於更新 vSAN 叢集驅動程式的離線套件組合的儲存庫設定檔。

韌體更新精靈一律會檢查 iDRAC、BIOS 是否符合最低韌體層級，並會嘗試將它們更新為所需的最低版本。如需 iDRAC、BIOS 的最低韌體層級詳細資訊，請參閱 *OpenManage Integration for VMware vCenter 相容性比較表*。只要 iDRAC 和 BIOS 韌體版本符合最低需求，韌體更新程序便會容許所有韌體版本的更新，包括：iDRAC、RAID Controller、NIC、BIOS 等。

註: 若要更新 PowerEdge XR2 伺服器，OMIVV 會使用 Dell 線上目錄中的 R440 韌體元件。如果您要建立用於離線韌體儲存庫的自訂目錄 (使用 DRM) 來支援 PowerEdge XR2，請使用適用於 PowerEdge R440 伺服器的韌體元件。

更新 vSAN 主機上的韌體和驅動程式

在 vSAN 主機 (vSAN 啟用的叢集中的主機) 排程韌體更新之前，請確定環境符合下列條件：

- 請確定主機相容 (CSIOR 已啟用且主機必須支援 ESXi 版本)、與主機認證設定檔相關聯，且已成功清查。
- 排程韌體更新之前，會檢查下列先決條件：
  - DRS 已啟用。
  - 主機尚未處於維護模式。
  - vSAN 資料物件狀況良好。

  若要略過先決條件檢查，請清除**排定更新**頁面上的**檢查先決條件**核取方塊。
- 對於儲存裝置控制器、HDD 和 SSD 元件，所選儲存庫中的所選驅動程式與韌體版本符合 VMware vSAN 指南的規定 (依據 vSAN 版本)。
- 對於驅動程式，OMIVV 僅支援在 VMware 硬體相容性清單中所列出的離線套件組合。
- 叢集符合所選資料移轉選項的 vSAN 要求。如果 vSAN 叢集不符合所選資料遷移選項的需求，更新將會逾時。
- Dell EMC 建議選取基準 (叢集設定檔) 韌體或驅動程式儲存庫。
- 請確保在要更新的叢集下方所有主機都沒有可執行的韌體更新工作。
- 請確保對「進入維護模式」工作指定所需的逾時值。如果等候時間超過指定的時間，更新工作將會失敗。但是，在主機重新開機時，元件可能會自動更新。
- 啟用 vSAN 後，重新執行清查。

在進行韌體更新程序時，Dell EMC 建議您不要刪除或移動以下項目：

- 來自 vCenter 且韌體正在進行更新的主機。
- 正在進行韌體更新工作的主機認證設定檔。
- 這些儲存庫位於 CIFS 或 NFS。

OMIVV 會檢查主機的相容性，以及相同叢集的任何主機中是否有任何其他韌體更新工作正在進行。驗證完成後，韌體更新精靈隨即顯示。

1. 若要啟動韌體更新精靈，請在 OMIVV 首頁上，展開**功能表**，選取**主機和叢集**，然後執行下列其中一項動作：
   - 在主機上按一下滑鼠右鍵，選取 **OMIVV 主機動作** > **韌體更新**。
   - 選取主機，在右窗格中選取**監視** > **OMIVV 主機資訊** > **韌體** > **執行韌體精靈**。
   - 選取主機，在右窗格中選取**摘要**，然後前往 **OMIVV 主機資訊** > **主機動作 s** > **執行韌體精靈**。
2. 在**韌體更新核對清單**頁面上，請確保所有先決條件已驗證後再排程更新，然後按一下**開始使用**。
3. 在**更新來源**頁面上，選取下列其中一項：
   - **儲存庫設定檔**
   - **單一 DUP**
4. 若要從檔案載入單一韌體更新，請選取**單一 DUP**。
   a. 單一 DUP 可能位於可由 OMIVV 裝置存取的 CIFS 或 NFS 共用上：請以下列其中一種格式輸入檔案位置，然後前往步驟 9。
      - NFS——`<host>:/<share_path/FileName.exe`
      - CIFS——`\\<host accessible share path>\<FileName>.exe`

      註: 請確定單一元件 DUP 的檔案名沒有任何空白處。

若為 CIFS 共用，OMIVV 會提示您輸入可存取共用磁碟機的使用者名稱和密碼。

5. 如果選取**儲存庫設定檔**選項，請選取韌體和驅動程式儲存庫設定檔。

   若叢集設定檔與主機所在的叢集相關聯，則在預設下，會選取關聯的韌體和驅動程式儲存庫設定檔。

   如果您變更韌體或驅動程式儲存庫設定檔，則會顯示一則訊息，表示所選的儲存庫設定檔並未關聯至基準，而使用不同的儲存庫可能會影響基準比較。

   註: 如果您同時有與叢集設定檔相關聯的驅動程式和韌體儲存庫，則建議同時更新驅動程式和韌體。

   如果不想要更新韌體或驅動程式，或您的韌體或驅動程式已經是最新版本，請從下拉式功能表中選取**未選取儲存庫**。

   儲存庫設定檔選項中不會顯示預設韌體目錄 (Dell EMC 預設目錄和已驗證的 MX 堆疊目錄)。若要使用儲存庫設定檔，請在 OMIVV 中建立自訂儲存庫。

   請執行下列步驟以建立自訂儲存庫設定檔：

   a. 前往 Dell EMC Repository Manager (DRM) 並建立目錄。

      如需使用 DRM 建立目錄的更多資訊，請參閱使用 OMIVV 在 Dell EMC Repository Manager (DRM) 中建立目錄 第頁的 114。

   b. 下載目錄和對應的檔案。

   c. 使用下載的目錄在 OMIVV 中建立儲存庫設定檔。

      如需建立儲存庫設定檔的更多資訊，請參閱建立儲存庫設定檔 第頁的 41。

6. 根據您選取的韌體儲存庫設定檔，選取適當的套件組合，然後按一下**下一步**。僅支援 64 位元的套件組合。
7. 在**選取驅動程式元件**頁面上，選取需要更新的驅動程式元件，然後按一下**下一步**。當您選取要更新的驅動程式元件時，套件中的所有元件都會全部選取。

   您可以使用篩選選項，根據特定的欄名稱篩選資料。
8. 在**選取韌體元件**頁面上，選取需要更新的韌體元件，然後按一下**下一步**。

   會顯示以危險狀態 (例如緊急、建議、選用和降級) 為基礎的元件計數。

   不能選取比目錄中可用版本更舊，或相同等級 (最新) 或已排程更新的元件。若要選取比可用版本更舊的元件版本，請選取**允許韌體降級**核取方塊。

   若要選取所有頁面上的所有韌體元件，請按一下。

   若要清除所有頁面上的所有韌體元件，請按一下。
9. 在**排程更新**頁面上，輸入韌體更新工作名稱和說明。說明是選填欄位。

   韌體更新工作的名稱為必要。如果您清除韌體更新工作的名稱，便可再次重複使用該工作名稱。
10. 在**其他設定**區段中，執行下列步驟：

    a. 輸入維護模式逾時值 (60 至 1440 分鐘之間)。如果等候時間超過指定的時間，更新工作就會失敗，且輸入的維護工作會被取消或逾時。但是，在主機重新開機時，元件可能會自動更新。

    b. 從**進入維護模式選項**下拉式功能表中，選取適當的資料遷移選項。如需更多有關資料遷移選項的資訊，請參閱 VMware 文件。

       註: 如果叢集組態不支援完整資料遷移或儲存容量不足，進入維護模式的工作會失敗。

       在預設下，以下選項已選取：

       - **韌體更新完成後結束維護模式**—如果您停用此選項，主機會繼續留在維護模式。
       - **將已關閉電源及暫停的虛擬機器移到叢集中的其他主機**—停用此選項將會中斷虛擬機器的連線，直到主機裝置連線為止。

    c. 如果更新韌體時遇到問題，請選取**刪除工作佇列並重設 iDRAC** 核取方塊。這可能可以讓更新程序順利完成。這會增加完成工作需要的整體更新時間、取消 iDRAC 上已排定但擱置中的任何工作或活動，並重設 iDRAC。

       主機若使用機箱認證設定檔進行管理，則不支援刪除工作佇列。

       在預設下，**檢查先決條件**選項已選取。
11. 在**更新排程**區段中，選取下列任一選項：

    - **立即更新**
    - **排程更新**
    - **在下一次重新開機時套用更新**
12. 檢閱**檢閱摘要**頁面上的韌體更新資訊，然後按一下**完成**。

    視選取的元件和伺服器數量而定，韌體更新工作可能需要花費數小時的時間。您可在**工作**頁面中檢視工作狀態。

    韌體更新工作完成後，系統會根據**排程更新**頁面上選取的選項，於所選的主機上自動執行清查，且主機會自動結束維護模式。

使用 OMIVV 在 Dell EMC Repository Manager (DRM) 中建立目錄

本節說明在 DRM 3.0 版及更新版本中建立目錄的程序。

1. 前往下載 DRM 並下載 DRM。
2. 在 DRM 首頁上，按一下**新增儲存庫**。
   新增儲存庫視窗隨即顯示。
3. 在**新增儲存庫**視窗中，執行以下操作：
   a. 輸入**儲存庫名稱**與**說明**。
   b. 從**基本目錄**下拉式功能表中，選取一個目錄。
   c. 從**整合類型**下拉式功能表中，選取 **OpenManage Integration for VMware vCenter**。
4. 在 **OpenManage Integration for VMware vCenter** 視窗中，輸入**虛擬裝置 IP**、**vCenter Server IP**、**使用者名稱**與**密碼**，然後按一下**連線**。
   建立的目錄即會示在首頁。
5. 若要匯出目錄，請選取目錄，然後按一下**匯出**。

更新 vSAN 叢集上的韌體和驅動程式

在排程韌體更新之前，請確定環境符合下列條件：

- 請確定主機相容 (CSIOR 已啟用且主機必須支援 ESXi 版本)、與主機認證設定檔相關聯，且已成功清查。若主機未列出，請從 OMIVV 為主機執行管理相容性精靈，然後使用韌體更新精靈。
- 排程韌體更新之前，會檢查下列先決條件：
  - DRS 已啟用。
  - 主機尚未處於維護模式。
  - vSAN 資料物件狀況良好。
- 對於儲存裝置控制器、HDD 和 SSD 元件，請確保所選儲存庫中的所選驅動程式與韌體版本符合 VMware vSAN 指南的規定 (依據 vSAN 版本)。
- 對於驅動程式，OMIVV 僅支援在 VMware 硬體相容性清單中所列出的離線套件組合。
- 叢集符合所選資料移轉選項的 vSAN 要求。如果 vSAN 叢集不符合所選資料遷移選項的需求，更新將會逾時。
- Dell EMC 建議選取基準 (叢集設定檔) 韌體或驅動程式儲存庫。
- 請確保在要更新的叢集下方所有主機都沒有可執行的韌體更新工作。
- 請確保對「進入維護模式」工作指定所需的逾時值。如果等候時間超過指定的時間，更新工作將會失敗。但是，在主機重新開機時，元件可能會自動更新。
- 啟用 vSAN 後，請確保將會重新執行清查。

在進行韌體更新程序時，Dell EMC 建議您不要刪除或移動以下項目：

- 正在進行韌體更新工作的 vCenter 的叢集主機。
- 正在進行韌體更新工作的主機認證設定檔。
- 這些儲存庫位於 CIFS 或 NFS。

註: VMware 建議您用一模一樣的伺服器硬體來建立叢集。

OMIVV 會檢查主機的相容性，以及相同叢集的任何主機中是否有任何其他韌體更新工作正在進行。驗證完成後，韌體更新精靈隨即顯示。

1. 若要啟動韌體更新精靈，請在 OMIVV 首頁上，展開**功能表**，選取**主機和叢集**，然後執行下列其中一項動作：
   - 以滑鼠右鍵按一下叢集，選取 **OMIVV 叢集動作** > **韌體更新**。
   - 選取叢集，在右窗格中選取**監視** > **OMIVV 叢集資訊** > **韌體** > **執行韌體精靈**。
2. 在**韌體更新核對清單**頁面上，請確保所有先決條件已驗證後再排程更新，然後按一下**開始使用**。
3. 在**更新來源**頁面上，選取韌體和驅動程式儲存庫設定檔。
   若叢集設定檔與主機所在的叢集相關聯，則在預設下，會選取關聯的韌體和驅動程式儲存庫設定檔。
   如果您變更韌體或驅動程式儲存庫設定檔，則會顯示一則訊息，表示所選的儲存庫設定檔並未關聯至基準，而使用不同的儲存庫可能會影響基準比較。
   註: 如果您同時有與叢集設定檔相關聯的驅動程式和韌體儲存庫，則建議同時更新驅動程式和韌體。
   如果不想要更新韌體或驅動程式，或您的韌體或驅動程式已經是最新版本，請從下拉式功能表中選取**未選取儲存庫**。

儲存庫設定檔選項中不會顯示預設韌體目錄 (Dell EMC 預設目錄和已驗證的 MX 堆疊目錄)。若要使用儲存庫設定檔，請在 OMIVV 中建立自訂儲存庫。

請執行下列步驟以建立自訂儲存庫設定檔：

a. 前往 Dell EMC Repository Manager (DRM) 並建立目錄。

如需使用 DRM 建立目錄的更多資訊，請參閱使用 OMIVV 在 Dell EMC Repository Manager (DRM) 中建立目錄 第頁的 114。

b. 下載目錄和對應的檔案。

c. 使用下載的目錄在 OMIVV 中建立儲存庫設定檔。

如需建立儲存庫設定檔的更多資訊，請參閱建立儲存庫設定檔 第頁的 41。

4. 根據您選取的韌體儲存庫設定檔，選取適當的套件組合，然後按一下**下一步**。僅支援 64 位元的套件組合。

註: 即使是不同型號的 OEM (已解除品牌) 伺服器，也只能選取一個套件組合。即使套件組合不適用於一台或多台 OEM 伺服器，韌體更新精靈的元件頁面會列出每個 OEM 伺服器或韌體元件配對。如果指定的韌體元件配對的韌體更新失敗，請使用適用 OEM 伺服器顯示的備用套件組合，再試一次。

5. 在**選取驅動程式元件**頁面上，選取需要更新的驅動程式元件，然後按一下**下一步**。當您選取要更新的驅動程式元件時，套件中的所有元件都會全部選取。

您可以使用篩選選項，根據特定的欄名稱篩選資料。

6. 在**選取韌體元件**頁面上，選取需要更新的韌體元件，然後按一下**下一步**。

會顯示以危險狀態 (例如緊急、建議、選用和降級) 為基礎的元件計數。

您可以使用篩選選項，根據特定的欄名稱篩選資料。

不能選取比目錄中可用版本更舊，或相同等級 (最新) 或已排程更新的元件。若要選取比可用版本更舊的元件版本，請選取**允許韌體降級**核取方塊。

若要選取所有頁面上的所有韌體元件，請按一下。

若要清除所有頁面上的所有韌體元件，請按一下。

7. 在**排程更新**頁面上，輸入韌體更新工作名稱和說明。說明是選填欄位。

韌體更新工作的名稱為必要。如果您清除韌體更新工作的名稱，便可再次重複使用該工作名稱。

8. 在**其他設定**區段中，執行下列步驟：

a. 輸入維護模式逾時值 (60 至 1440 分鐘之間)。如果等候時間超過指定的時間，更新工作就會失敗，且輸入的維護工作會被取消或逾時。但是，在主機重新開機時，元件可能會自動更新。

b. 從**進入維護模式選項**下拉式功能表中，選取適當的資料遷移選項。如需更多有關資料遷移選項的資訊，請參閱 VMware 文件。

註: 如果叢集組態不支援完整資料遷移或儲存容量不足，進入維護模式的工作會失敗。

根據預設，會選取**將已關閉電源及暫停的虛擬機器移到叢集中的其他主機**選項。停用此選項將會中斷虛擬機器的連線，直到主機裝置連線為止。

c. 如果更新韌體時遇到問題，請選取**刪除工作佇列並重設 iDRAC** 核取方塊。這可能可以讓更新程序順利完成。這會增加完成工作需要的整體更新時間、取消 iDRAC 上已排定但擱置中的任何工作或活動，並重設 iDRAC。

主機若使用機箱認證設定檔進行管理，則不支援刪除工作佇列。

9. 在**更新排程**區段中，選取下列任一選項：

- **立即更新**
- **排程更新**

10. 檢閱**檢閱摘要**頁面上的韌體更新資訊，然後按一下**完成**。

視選取的元件和伺服器數量而定，韌體更新工作可能需要花費數小時的時間。您可在**工作**頁面中檢視工作狀態。

韌體更新工作完成後，系統會根據**排程更新**頁面上選取的選項，於所選的主機上自動執行清查，且主機會自動結束維護模式。

更新 vSphere 主機上的韌體

在 vSphere 主機 (僅 ESXi) 排程韌體更新之前，請確定環境符合下列條件：

- 請確定主機相容 (CSIOR 已啟用且主機必須支援 ESXi 版本)、與主機認證設定檔相關聯，且已成功清查。
- DRS 已啟用。

註: 若為獨立主機，則不適用 DRS 檢查。

若要略過先決條件檢查，請清除**排程更新**頁面上的**檢查先決條件**核取方塊。

註: 在 vSphere 叢集和主機上不支援驅動程式更新。

在進行韌體更新程序時，Dell EMC 建議您不要刪除或移動以下項目：

- 來自 vCenter 且韌體正在進行更新的主機。
- 正在進行韌體更新工作的主機認證設定檔。
- 這些儲存庫位於 CIFS 或 NFS。

OMIVV 會檢查主機的相容性，以及相同叢集的任何主機中是否有任何其他韌體更新工作正在進行。驗證完成後，韌體更新精靈隨即顯示。

1. 若要啟動韌體更新精靈，請在 OMIVV 首頁上，展開**功能表**，選取**主機和叢集**，然後執行下列其中一項動作：
   - 在主機上按一下滑鼠右鍵，選取 **OMIVV 主機動作** > **韌體更新**。
   - 選取主機，在右窗格中選取**監視** > **OMIVV 主機資訊** > **韌體** > **執行韌體精靈**。
   - 選取主機，在右窗格中選取**摘要**，然後前往 **OMIVV 主機資訊** > **主機動作** > **執行韌體精靈**。
2. 在**韌體更新核對清單**頁面上，請確保所有先決條件已驗證後再排程更新，然後按一下**開始使用**。
3. 在**更新來源**頁面上，選取下列其中一項：
   - **儲存庫設定檔**
   - **單一 DUP**
4. 若要從檔案載入單一韌體更新，請選取**單一 DUP**。
   a. 單一 DUP 可能位於可由 OMIVV 裝置存取的 CIFS 或 NFS 共用上。請使用下列格式之一輸入檔案位置，然後前往步驟 8。
      - NFS—`<host>:/<share_path/FileName.exe`
      - CIFS—`\\<host accessible share path>\<FileName>.exe`

      註: 請確定單一元件 DUP 的檔案名沒有任何空白處。

      若為 CIFS 共用，OMIVV 會提示您輸入可存取共用磁碟機的使用者名稱和密碼。
5. 如果您選取**儲存庫設定檔**選項，請選取韌體儲存庫設定檔。
   若叢集設定檔與主機所在的叢集相關聯，則在預設下，會選取關聯的韌體儲存庫。否則，將會選取 **Dell 預設目錄**。
   如果您變更韌體儲存庫設定檔，則會顯示一則訊息，表示所選的儲存庫設定檔並未關聯至基準，而使用不同的儲存庫可能會影響基準比較。
6. 根據您選取的韌體儲存庫設定檔，選取適當的套件組合，然後按一下**下一步**。僅支援 64 位元的套件組合。
7. 在**選取韌體元件**頁面上，選取需要更新的韌體元件，然後按一下**下一步**。
   會顯示以危險狀態 (例如緊急、建議、選用和降級) 為基礎的元件計數。
   您可以使用篩選選項，根據特定的欄名稱篩選資料。
   不能選取比目錄中可用版本更舊，或相同等級 (最新) 或已排程更新的元件。若要選取比可用版本低的元件版本，請選取**允許韌體降級**方塊。
   若要選取所有頁面上的所有韌體元件，請按一下。
   若要清除所有頁面上的所有韌體元件，請按一下。
8. 在**排程更新**頁面上，輸入韌體更新工作名稱和說明。說明是選填欄位。
   韌體更新工作的名稱為必要。如果您清除韌體更新工作的名稱，便可再次重複使用該工作名稱。
9. 在**其他設定**區段中，執行下列步驟：
   a. 輸入維護模式逾時值 (60 至 1440 分鐘之間)。如果等候時間超過指定的時間，更新工作就會失敗，且輸入的維護工作會被取消或逾時。但是，在主機重新開機時，元件可能會自動更新。
      在預設下，以下選項已選取：
      - **韌體更新完成後結束維護模式**—如果您停用此選項，主機會繼續留在維護模式。
      - **將已關閉電源及暫停的虛擬機器移到叢集中的其他主機**—停用此選項將會中斷虛擬機器的連線，直到主機裝置連線為止。

   b. 如果更新韌體時遇到問題，請選取**刪除工作佇列並重設 iDRAC** 核取方塊。這可能可以讓更新程序順利完成。這會增加完成工作需要的整體更新時間、取消 iDRAC 上已排定但擱置中的任何工作或活動，並重設 iDRAC。
      主機若使用機箱認證設定檔進行管理，則不支援刪除工作佇列。
      在預設下，**檢查先決條件**選項已選取。

10. 在**更新排程**區段中，選取下列任一選項：
    - **立即更新**
    - **排程更新**
    - **在下一次重新開機時套用更新**
    - **套用更新，然後強迫重新開機而不進入維護模式**
11. 檢閱**檢閱摘要**頁面上的韌體更新資訊，然後按一下**完成**。
    視選取的元件和伺服器數量而定，韌體更新工作可能需要花費數小時的時間。您可在**工作**頁面中檢視工作狀態。

    韌體更新工作完成後，系統會根據**排程更新**頁面上選取的選項，於所選的主機上自動執行清查，且主機會自動結束維護模式。

更新 vSphere 叢集上的韌體

在排程韌體更新之前，請確定環境符合下列條件：

- 請確定主機相容 (CSIOR 已啟用且主機必須支援 ESXi 版本)、與主機認證設定檔相關聯，且已成功清查。若主機未列出，請從 OMIVV 為主機執行管理相容性精靈，然後使用韌體更新精靈。
- DRS 已啟用。
- 請確保在要更新的叢集下方所有主機都沒有可執行的韌體更新工作。
- 請確保對「進入維護模式」工作指定所需的逾時值。如果等候時間超過指定的時間，更新工作將會失敗。但是，在主機重新開機時，元件可能會自動更新。

註: 在 vSphere 叢集和主機上不支援驅動程式更新。

在進行韌體更新程序時，Dell EMC 建議您不要刪除或移動以下項目：

- 正在進行韌體更新工作的 vCenter 的叢集主機。
- 正在進行韌體更新工作的主機認證設定檔。
- 這些儲存庫位於 CIFS 或 NFS

註: VMware 建議您用一模一樣的伺服器硬體來建立叢集。

OMIVV 會檢查主機的相容性，以及相同叢集的任何主機中是否有任何其他韌體更新工作正在進行。驗證完成後，韌體更新精靈隨即顯示。

1. 若要啟動韌體更新精靈，請在 OMIVV 首頁上，展開**功能表**，選取**主機和叢集**，然後執行下列其中一項動作：
    - 以滑鼠右鍵按一下叢集，選取 **OMIVV 叢集動作** > **韌體更新**。
    - 選取叢集，在右窗格中選取**監視** > **OMIVV 叢集資訊** > **韌體** > **執行韌體精靈**。
2. 在**韌體更新核對清單**頁面上，請確保所有先決條件已驗證後再排程更新，然後按一下**開始使用**。
3. 在**更新來源**頁面上，若叢集設定檔與主機所在的叢集相關聯，則在預設下，會選取關聯的韌體儲存庫。否則，將會選取 **Dell 預設目錄**。

    如果您變更韌體儲存庫設定檔，則會顯示一則訊息，表示所選的儲存庫設定檔並未關聯至基準，而使用不同的儲存庫可能會影響基準比較。
4. 根據您選取的韌體儲存庫設定檔，選取適當的套件組合，然後按一下**下一步**。僅支援 64 位元的套件組合。

    註: 即使是不同型號的 OEM (已解除品牌) 伺服器，也只能選取一個套件組合。即使套件組合不適用於一台或多台 OEM 伺服器，韌體更新精靈的元件頁面會列出每個 OEM 伺服器或韌體元件配對。如果指定的韌體元件配對的韌體更新失敗，請使用適用 OEM 伺服器顯示的備用套件組合，再試一次。
5. 在**選取韌體元件**頁面上，選取需要更新的韌體元件，然後按一下**下一步**。
    會顯示以危險狀態 (例如緊急、建議、選用和降級) 為基礎的元件計數。

    不能選取比目錄中可用版本更舊，或相同等級 (最新) 或已排程更新的元件。若要選取比可用版本更舊的元件版本，請選取**允許韌體降級**核取方塊。

    您可以使用篩選選項，根據特定的欄名稱篩選資料。

    若要選取所有頁面上的所有韌體元件，請按一下 。

    若要清除所有頁面上的所有韌體元件，請按一下 。
6. 在**排程更新**頁面上，輸入韌體更新工作名稱和說明。說明是選填欄位。
    韌體更新工作的名稱為必要。如果您清除韌體更新工作的名稱，便可再次重複使用該工作名稱。

7. 在**其他設定**區段中，執行下列步驟：
   a. 輸入維護模式逾時值 (60 至 1440 分鐘之間)。如果等候時間超過指定的時間，更新工作就會失敗，且輸入的維護工作會被取消或逾時。但是，在主機重新開機時，元件可能會自動更新。

      根據預設，會選取**將已關閉電源及暫停的虛擬機器移到叢集中的其他主機**選項。停用此選項將會中斷虛擬機器的連線，直到主機裝置連線為止。
   b. 如果更新韌體時遇到問題，請選取**刪除工作佇列並重設 iDRAC** 核取方塊。這可能可以讓更新程序順利完成。這會增加完成工作需要的整體更新時間、取消 iDRAC 上已排定但擱置中的任何工作或活動，並重設 iDRAC。

      主機若使用機箱認證設定檔進行管理，則不支援刪除工作佇列。
8. 在**更新排程**區段中，選取下列任一選項：
   - **立即更新**
   - **排程更新**
9. 檢閱**檢閱摘要**頁面上的韌體更新資訊，然後按一下**完成**。
   視選取的元件和伺服器數量而定，韌體更新工作可能需要花費數小時的時間。您可在**工作**頁面中檢視工作狀態。

   韌體更新工作完成後，系統會根據**排程更新**頁面上選取的選項，於所選的主機上自動執行清查，且主機會自動結束維護模式。

更新相同的韌體元件類型

以下是更新相同類型的韌體元件時需牢記的要點：

- 如果伺服器中有多個版本相同的同類型元件，則**選取韌體元件**頁面上只會顯示元件的一個版本。更新將套用至所有元件，而且元件僅有一個版本的漂移詳細資料會顯示。

  例如：

  表 19. 伺服器中存在相同類型的多個元件之範例

元件	目前版本	可用版本
HDD1	V1	V3
HDD2	V1	V3
HDD3	V1	V3

  在這種情況下，**選取韌體元件**頁面會顯示下列內容：

  表 20. 伺服器中存在相同版本的多個元件之範例

元件	目前版本	可用版本
HDD1	V1	V3

- 如果伺服器中有多個不同版本的相同類型元件，則會顯示每個唯一版本的單一元件。在這種情況下，如果選取任何一個元件，則會將更新套用至所有元件，不論其目前的韌體版本為何。所有元件的漂移詳細資料都會顯示，不論其目前的韌體版本為何。

  例如：

  表 21. 伺服器中存在不同版本的多個元件之範例

元件	目前版本	可用版本
HDD1	V1	V3
HDD2	V2	V3
HDD3	V2	V3

  在這種情況下，**選取韌體元件**頁面會顯示下列內容：

  表 22. 伺服器中存在不同版本的多個元件之範例

元件	目前版本	可用版本
HDD1	V1	V3
HDD2	V2	V3

- 如果目錄包含多個可用的版本，建議僅為元件類型選取其中一種可用版本。所選的韌體將會套用至所有適用的元件，不論其目前的版本為何。

  例如：

  表 23. 目錄中存在多個可用版本的範例

元件	目前版本	可用版本
HDD1	V1	V3
HDD2	V2	V3
HDD3	V2	V3
HDD1	V1	V4
HDD2	V2	V4
HDD3	V2	V4

  在這種情況下，**選取韌體元件**頁面會顯示下列內容：

  表 24. 目錄中存在多個可用版本的範例

元件	目前版本	可用版本
HDD1	V1	V3
HDD2	V2	V3
HDD1	V1	V4
HDD2	V2	V4

vSphere Lifecycle Manager 概觀

vSphere Lifecycle Manager 是一種在 vCenter 伺服器中執行的服務 (適用於 vCenter 7.0 及更新版本)。

vSphere Lifecycle Manager 可讓您建立由 ESXi 映像、韌體和驅動程式組成的基線映像。透過執行相容性檢查，確保叢集中的每台主機都能符合基線映像的需求。如果出現不相容狀態，系統會提供補救叢集的選項。

在 vSphere Lifecycle Manager 中，OMIVV 作為韌體附加元件提供者。如需更多有關 vSphere Lifecycle Manager 的資訊，請參閱 VMware 說明文件。

若要使用 vSphere Lifecycle Manager 搭配 OMIVV，vCenter 註冊是必要程序。如需註冊 vCenter 和 vSphere LifeCycle Manager 的詳細資訊，請參閱 註冊新的 vCenter 伺服器 第頁的 11。

在 vCenter 註冊期間，您可以在 Dell EMC 管理主控台註冊 vSphere Lifecycle Manage (適用於 vCenter 7.0 及更新版本)。vCenter 註冊成功之後，您可以在 Dell EMC 管理主控台的 **VCENTER 註冊**頁面修改 (註冊或取消註冊) vSphere Lifecycle Manager 的註冊狀態。如需更多資訊，請參閱 在 Dell EMC 管理主控台中註冊 vSphere Lifecycle Manager 第頁的 119 和 在 Dell EMC 管理主控台中取消註冊 vSphere Lifecycle Manager 第頁的 120。

在 Dell EMC 管理主控台中檢視 vSphere Lifecycle Manager 狀態

以下為可在 **vSphere Lifecycle Manager** 欄中檢視的 vSphere Lifecycle Manager 可能狀態：

- **註冊** (僅適用於 vCenter 7.0 及更新版本)—在 vSphere Lifecycle Manager 未註冊時顯示。
- **取消註冊** (僅適用於 vCenter 7.0 及更新版本)—在 vSphere Lifecycle Manager 已註冊時顯示。
- **不適用**—只在註冊的 vCenter 版本是 7.0 之前的版本時顯示。如果 vCenter 升級至 7.0，狀態會保持為 **NA**。若要反映狀態，請重新啟動 OMIVV 裝置。

在 Dell EMC 管理主控台中註冊 vSphere Lifecycle Manager

vCenter 必須為 7.0 及更新版本。

1. 前往 https://<AppliancelP/hostname/>。

2. 在 **VCENTER 註冊**頁面的 **vSphere Lifecycle Manager** 下，按一下**註冊**。
隨即會顯示**註冊 VSPHERE LIFECYCLE MANAGER** <vCenter 名稱> 對話方塊。
3. 按一下**註冊 vSphere Lifecycle Manager**。
即會顯示訊息，指出已成功註冊 vSphere Lifecycle Manager。

在 Dell EMC 管理主控台中取消註冊 vSphere Lifecycle Manager

vCenter 必須為 7.0 及更新版本。

1. 前往 https://<ApplianceIP/hostname/>。
2. 在 **VCENTER 註冊**頁面的 **vSphere Lifecycle Manager** 下，按一下**取消註冊**。
隨即會顯示**取消註冊 VSPHERE LIFECYCLE MANAGER** <vCenter 名稱> 對話方塊。
3. 按一下**取消註冊**。
即會顯示訊息，指出已成功取消註冊 vSphere Lifecycle Manager。即會從 vSphere Lifecycle Manager 中的**硬體支援管理員**清單移除 **DellEMC OMIVV**。不會影響 OMIVV 功能。

使用 vSphere Lifecycle Manager 管理叢集

先決條件：

在使用 vSphere Lifecycle Manager 管理叢集前，請先確定以下事項：

- Dell EMC 管理主控台中已啟用 vSphere Lifecycle Manager。如需詳細資訊，請參閱 在 Dell EMC 管理主控台中註冊 vSphere Lifecycle Manager 第頁的 119。
- 叢集中的主機具備管理相容性。如需詳細資訊，請參閱 管理相容性 第頁的 61。
- 會針對所選叢集建立叢集設定檔，且叢集設定檔與 OMIVV 中的韌體儲存庫相關聯。如需更多有關叢集設定檔的資訊，請參閱 建立叢集設定檔 第頁的 44。

您可以在 vSphere Lifecycle Manager 中使用使用者介面或 vSphere Automation API 來管理叢集。OMIVV 支援使用使用者介面和 vSphere Automation API 來管理叢集。

註: 您可以在 vSphere Lifecycle Manager 中使用 OMIVV 叢集動作 (例如系統鎖定和韌體更新)，但可能會影響基線報告。

使用 OMIVV 作為 vSphere Lifecycle Manager 中的韌體附加元件提供者—使用者介面

您可以使用 OMIVV 搭配 vSphere Lifecycle Manager 作為韌體附加元件提供者。

在 vSphere Lifecycle Manager 中，叢集設定檔稱為硬體支援套件 (HSP)。選取在 OMIVV 中建立的叢集設定檔作為 vSphere Lifecycle Manager 中的**韌體和驅動程式附加元件**。如需更多有關叢集設定檔的資訊，請參閱 叢集設定檔 第頁的 44。

若要設定所選叢集的映像並關聯 OMIVV 作為**韌體和驅動程式附加元件**，請執行下列工作：

1. 在 vSphere 用戶端中，按一下**主機與叢集**，然後選取您要使用映像管理的叢集。
2. 在**更新**頁面的左窗格中，展開**主機**，然後按一下**映像**。
3. 若要選取韌體和驅動程式附加元件，請按一下選取圖示。
即會顯示**選取韌體和驅動程式附加元件**頁面。
4. 在**選取硬體支援管理員**區段中，選取 **DellEMC OMIVV**。

   選取 **DellEMC OMIVV** 後，所有與韌體儲存庫關聯且連結至所選 vCenter 中叢集的叢集設定檔，將會列在**選取韌體和驅動程式附加元件**區段中。
5. 選取適用所選叢集的叢集設定檔，然後按一下**選取**。
   若要識別與所選叢集相關聯的叢集設定檔，請參閱叢集設定檔中顯示的說明。

   註: 如果您尚未在 OMIVV 中建立任何叢集設定檔，將會顯示空白清單。如需有關建立叢集設定檔的更多資訊，請參閱建立叢集設定檔 第頁的 44。

   - **附加元件版本**— 指出叢集設定檔的目前版本。如果叢集設定檔已修改或版本在 OMIVV 中增加，請務必在 vSphere Lifecycle Manager 中使用最新版本的叢集設定檔。

     註: 有時，vSphere Lifecycle Manager 會顯示不相容的韌體。但不相容的韌體不會列在 vSpphere Lifecycle Manager 中。若要解決此問題，請補救叢集。補救叢集不會造成 vSphere Lifecycle Manager 重新啟動。

- **支援的 ESXi 版本**—表示支援 OMIVV 的 ESXi 版本 (7.0.0)。

所選的叢集設定檔會在**更新**頁面上顯示為韌體附加元件。

6. 按一下**儲存**。
   vSphere Lifecycle Manager 會執行叢集相容性檢查。相容性檢查結果會顯示在 vSphere Lifecycle Manager 的**映像相容性**區段中。

   整體相容性包含軟體相容性與韌體相容性。OMIVV 管理 vSphere Lifecycle Manager 工作的韌體相容性部分。

檢視叢集相容性狀態

以下為每個主機可能的韌體相容性狀態：

- **相容**：安裝在主機上所有韌體元件的韌體版本，與 OMIVV 叢集設定檔中的韌體版本相同時，即會顯示此狀態。
- **不相容**：安裝在主機上的一個或多個韌體版本與 OMIVV 叢集設定檔中的韌體版本不同時，即會顯示此狀態。
  註: 升級 OMIVV 裝置後，以舊版 OMIVV 建立的 vSphere Lifecycle Manager 映像檢查相容性工作會失敗。若要解決此問題，請使用最新版本的硬體支援套件 (HSP) 來製作映像。
- **不相容**：在下列情況下會顯示此狀態：
  - 在 vCenter 中選取的叢集與所選的**韌體和驅動程式附加元件** (OMIVV 中的叢集設定檔) 沒有任何關聯。
  - 如果為所選叢集儲存 vSphere Lifecycle Manager 映像後，便會更新叢集設定檔中的韌體儲存庫。
- **未知**：如果未在 OMIVV 中成功清查主機，即會顯示此狀態。如需更多資訊，請參閱主機認證設定檔 第頁的 34。

註: OMIVV 與 vSphere Lifecycle Manager 間的漂移報告可能會出現不相符的情況。這是因為 vSphere Lifecycle Manager 會一直顯示即時漂移報告，而 OMIVV 則會根據排定日期和時間顯示漂移報告。如果您在漂移報告中發現不相符的情況，請在 OMIVV 的**漂移偵測工作**頁面上，隨需執行漂移偵測工作。

修正叢集相容性問題

1. 如果主機狀態為**相容**，則無需對該主機執行進一步動作。
2. 如果主機狀態為**不相容**，請繼續進行補救。如需詳細資訊，請參閱在 vSphere Lifecycle Manager 中補救叢集 第頁的 122。
3. 如果主機狀態為**不相容**：
   a. 請確定 vCenter 中選取的叢集與叢集設定檔相關聯。選取與 vSphere Lifecycle Manager 中**韌體和驅動程式附加元件**相同的叢集設定檔。
   b. 編輯 vSphere Lifecycle Manager 映像，然後重新選擇更新的叢集設定檔 (韌體和驅動程式附加元件)，然後儲存映像。
4. 如果主機狀態為**未知**，請確定主機已新增至 OMIVV 中的主機認證設定檔，且成功執行清查。

硬體相容性檢查

執行韌體補救之前，vSphere Lifecycle Manager 提供 vSAN 叢集硬體相容性檢查的執行選項。硬體相容性檢查會將映像中的韌體和驅動程式，與 vSAN 硬體相容性清單 (HCL) 中列出的硬體和支援的驅動程式進行比較。vSphere Lifecycle Manager 只會針對儲存裝置控制器 (PCIe 裝置) 執行硬體相容性檢查。如需支援的韌體清單，請在 vSphere 用戶端中移至**顯示器** > **vSAN** > **Skyline 健全狀況**。

若要執行硬體相容性檢查，請在**映像相容性**區段中，按一下**檢查相容性**。

執行硬體相容性檢查時，OMIVV 會傳回叢集設定檔中的韌體版本。

如果韌體版本與硬體相容性清單 (HCL) 列出的韌體相容，則 vSphere Lifecycle Manager 的相容性狀態會顯示為**相容**。如需相容性狀態的相關資訊，請參閱 Vmware 說明文件。

硬體相容性檢查結果會顯示在**硬體相容性**頁面。

執行補救前置檢查

前置檢查作業會針對叢集中的每一台主機執行各種檢查，以確保叢集已準備好進行韌體補救。

前置檢查為可在主機或叢集層級執行的選用工作。

您可以略過前置檢查作業，vSphere Lifecycle Manager 會在補救作業期間執行前置檢查。

在前置檢查過程中，OMIVV 會執行下列先決條件檢查：

- iDRAC 可連線性

- iDRAC 鎖定模式
- 針對所選叢集的任何主機從 OMIVV 觸發的韌體更新工作 (若有) 狀態
- 啟用「重新啟動時收集系統清查」(CSIOR)
- 與韌體儲存庫和所需韌體元件的連線。

若要確認韌體補救的先決條件，請按一下**執行前置檢查**。
前置檢查工作狀態和結果會顯示在**映像相容性**區段中。

如果任何主機的前置檢查失敗，請修正問題，然後重新執行前置檢查或繼續進行補救工作。

在 vSphere Lifecycle Manager 中補救叢集

在**映像相容性**區段，您可以一次補救叢集中的一台主機或所有主機。

a. 若要執行個別主機的補救工作，請在**映像相容性**區段中按一下主機旁的垂直刪節號圖示，然後選取**補救**。
b. 若要執行叢集中所有主機的補救工作，請在**映像相容性**區段中，按一下**補救全部**。

   建議您在執行韌體更新之前，先執行 iDRAC 重設。執行 iDRAC 重設可降低故障可能性。

   若要在每個主機上以 vSphere Lifecycle Manager 於韌體更新前自動重設 iDRAC，請在 OMIVV 中啟用**清除 iDRAC 工作並重設 iDRAC** 核取方塊。如需詳細資訊，請參閱 韌體更新設定 第頁的 78。

若要檢視補救工作狀態，請按一下**更新**頁面上的**顯示更多**。

您可以在 OMIVV 的**記錄**頁面上檢視與 OMIVV 相關的記錄。

使用 OMIVV 作為 vSphere Lifecycle Manager 中的韌體附加元件提供者—vSphere Automation API

使用 vSphere Automation API 管理叢集之前，請先確定您已使用 vSphere Lifecycle Manager 使用者介面完成下列工作：

- 選取 DellEMC OMIVV 的硬體支援管理員。
- 選取適用於所選叢集的叢集設定檔，然後儲存映像。

掃描韌體相容性

命令：POST https://{VC IP/FQDN}/api/esx/settings/clusters/{cluster ID}/software?vmw-task=true&action=scan

```
{
    "spec" : {
      "message": "test commit"
    }
}
```

說明：根據叢集所需狀態掃描叢集中所有主機。您可以呼叫 `cis/tasks/{task-id}` 來查詢此作業的結果，其中 task-id 是此作業的回應。

HTTP 回應代碼：200。如需所有回應代碼的清單，請參閱 回應代碼 第頁的 152。

範例回應：

```
{task ID}
```

取得相容性工作狀態

命令：GET https://{VC IP/FQDN}/rest/cis/tasks/{task ID}

說明：傳回工作的相關資訊。

HTTP 回應代碼：200。如需所有回應代碼的清單，請參閱 回應代碼 第頁的 152。

範例回應：以下範例僅包含不相容的韌體。


```
"result":
[
{
 "value":
[
{
"value":
{
"hardware_modules":
[
{
 "value":
 {
 "current":
 {
 "version": "25.5.6.0009"
 },
 "details":
 {
 "component_class": "PCI_DEVICE",
 "description": "PERC H730 Mini"
 } "notifications":
 {
  "info":
 [
 {
 "id": "Different versions.",
 "time": "2020-02-04T10:47:54.422Z",
 "message":
 {
 "args": [],
 "default_message": "Different versions.",
 "id": "Different versions."
  }
  }
 ]
 },
 "status": "NON_COMPLIANT",
 "target": {
 "version": "25.5.5.0005"
  }
  }
 "key": ""
  }
  ],
 "notifications":
 {
 "info":
 [
 {
 "id": "[vCenter:<vCenter IP/FQDN>][Cluster: <Cluster name>][Host: <host IP/
FQDN>]              The host is non-compliant",
 "time": "2020-02-04T10:47:54.423Z",
 "message":
 {
 "args": [],
 "default_message": "[vCenter:<vCenter IP/FQDN>][Cluster: <Cluster name>][Host: <host IP/
FQDN>] The host is non-compliant",
 "id": "[vCenter:<vCenter IP/FQDN>][Cluster: <Cluster name>][Host: <host IP/FQDN>] The host
is non-compliant"
 }
 }]
 },
"status": "NON_COMPLIANT",
"target": {
"pkg": "<cluster profile name>",
 "version": "0.0.0-0"
 }
 },
 "key": "com.dell.plugin.OpenManager_HWSupportManager"
```

```
 }
 ],
```

執行補救前置檢查

命令：POST https://{VC IP/FQDN}/api/esx/settings/clusters/{cluster ID}/software?vmw-task=true&action=check

說明：在叢集的所有主機上套用所需狀態前，請先於叢集上執行檢查。檢查叢集中所有主機是否處於良好狀態，好以所需狀態進行更新。

HTTP 回應代碼：200。如需所有回應代碼的清單，請參閱 回應代碼 第頁的 152。

範例回應：

```
{task-id}
```

取得補救前置檢查工作狀態

命令：GET https://{VC IP/FQDN}/rest/cis/tasks/{task ID}

說明：傳回工作的相關資訊。

HTTP 回應代碼：200。如需所有回應代碼的清單，請參閱 回應代碼 第頁的 152。

範例回應：

```
{
 "value":
{
"parent": "",
"cancelable": true,
"end_time": "2020-02-12T18:03:59.391Z",
"description":
{
 "args": [],
 "default_message": "Task created by VMware vSphere Lifecycle Manager",
 "id": "com.vmware.vcIntegrity.lifecycle.Task.Description"
  },
 "target":
{
"id": "domain-c8",
 "type": "ClusterComputeResource"
 },
 "result":
{
"start_time": "2020-02-12T17:52:09.264Z",
"commit": "",
"end_time": "2020-02-12T18:03:59.386Z",
 "entity_results":
[
{
"host": "host-47",
"type": "HOST",
"check_statuses": [],
"status": "OK"
 }
 {
"host": "host-41",
"type": "HOST",
"check_statuses": [],
"status": "OK"
 },
 {
 "host": "host-22",
 "type": "HOST",
 "check_statuses": [],
 "status": "OK"
  },
{
```

```
  "host": "host-16",
  "type": "HOST",
  "check_statuses": [
{
  "check":
 {
   "name":
  {
  "args": [],
  "default_message": "Host Hardware support check.",
  "id": "com.vmware.vcIntegrity.lifecycle.ClusterHealthCheckTask.HwSupportCheck.Name"
   },
  "description":
 {
  "args": [],
  "default_message": "Checks if the hardware update can be performed.",
  "id": "com.vmware.vcIntegrity.lifecycle.ClusterHealthCheckTask.HwSupportCheck.Description"
  },
  "check": "com.vmware.vcIntegrity.lifecycle.ClusterHealthCheckTask.HwSupportCheck"
  },
 "issues": [
 {
 "args": [],
 "default_message": "[vCenter: jpvc7dot0d5-2.sped.bdcsv.lab][Cluster:
R6415_vSAN_AllFlash_ESXi7.0RC+][Host: 100.100.10.154][Update PreCheck Task] System Lockdown
Mode is turned On for iDRAC IP, 172.20.5.5; hence Firmware update cannot continue.",
"id": "[vCenter: jpvc7dot0d5-2.sped.bdcsv.lab][Cluster: R6415_vSAN_AllFlash_ESXi7.0RC+][Host:
100.100.10.154][Update PreCheck Task] System Lockdown Mode is turned On for iDRAC IP,
172.20.5.5; hence Firmware update cannot continue."
 }
],
"status": "ERROR"
 }
 ],
"status": "ERROR"
 },
 {
 "host": "host-19",
 "type": "HOST",
 "check_statuses": [],
 "status": "OK"
 },
 {
"host": "host-13",
 "type": "HOST",

 "check_statuses": [],
 "status": "OK"
  },
```


補救叢集

命令：POST https://{{VC IP/FQDN}/}}/api/esx/settings/clusters/{cluster ID}/software?vmw-task=true&action=apply

```
{
 "accept_eula" : true
}
```

說明：將與給定叢集相關聯的所需狀態套用至叢集內主機。

HTTP 回應代碼：200。如需所有回應代碼的清單，請參閱 回應代碼 第頁的 152。

範例回應：

```
{task-id}
```

設定閃爍指示燈

您可以將前指示燈設定為閃爍一段設定時間，以協助在大型資料中心環境找到實體伺服器。

1. 若要啟動**閃爍伺服器 LED 指示燈**精靈，請執行下列其中一項動作：
   a. 在 OMIVV 首頁上，展開**功能表**，選取**主機與叢集**，在主機或叢集上按一下滑鼠右鍵，然後前往 **摘要** > **OMIVV 主機資訊** > **主機動作** > **閃爍伺服器 LED 指示燈**。
   b. 在主機上按一下滑鼠右鍵，前往 **OMIVV 主機動作** > **閃爍伺服器 LED 指示燈**。
2. 在右窗格中，按一下「摘要」，然後前往 **OMIVV 主機資訊** > **主機動作** > **閃爍伺服器 LED 指示燈**。
   閃爍伺服器 LED 指示燈對話方塊隨即顯示。
3. 選取下列其中一項：
   a. 若要開啟伺服器 LED 指示燈並設定時段，請按一下**開啟**。
   b. 若要關閉伺服器 LED 指示燈，請按一下**關閉**。

設定系統鎖定模式

系統鎖定模式僅支援經企業授權的 iDRAC9 型伺服器。當您開啟系統鎖定模式時，請鎖定包括韌體更新在內的系統組態。啟系統鎖定模式設定是專門為了保護系統避免意外變更。您可以使用 OMIVV 裝置或從 iDRAC 主控台，為受管理之主機開啟或關閉系統鎖定模式。從 OMIVV 4.1 和更新版本開始，您可以設定和監控伺服器中 iDRAC 的鎖定模式。此外，iDRAC 必須有企業授權才能啟用鎖定模式。

註: 您無法變更使用機箱認證設定檔管理之主機的系統鎖定模式。

您可以鎖定或解除鎖定在主機或叢集等級的主機或叢集，以設定系統鎖定模式。當系統鎖定模式開啟時，下列功能有限制：

- 所有的組態工作，例如韌體更新、作業系統部署、清除系統事件記錄、重設 iDRAC，及設定 iDRAC 設阱目的地。

1. 若要啟動「設定系統鎖定模式精靈」，請執行下列動作之一：
   a. 在 OMIVV 首頁上，展開**功能表**，選取**主機與叢集**，在主機或叢集上按一下滑鼠右鍵，然後前往**摘要** > **OMIVV 主機資訊** > **主機動作** > **設定系統鎖定模式**。
   b. 在主機或叢集上按一下滑鼠右鍵，前往 **OMIVV 主機動作** > **設定系統鎖定模式**。
   c. 選取主機或叢集，前往 **監視** > **OMIVV 主機或叢集資訊** > **韌體** > **設定系統鎖定模式**。
2. 針對叢集層級，輸入系統鎖定模式工作名稱和說明。說明是選填欄位。
3. 若要啟用系統鎖定模式，按一下**開啟**。此選項會限制系統中的系統組態變更 (包含韌體和 BIOS 版本)。
4. 若要停用系統鎖定模式，按一下**關閉**。此選項允許系統中的系統組態變更 (包含韌體和 BIOS 版本)。
   如果您嘗試為 13G 或更舊的 PowerEdge 伺服器設定系統鎖定模式，則系統會提示訊息，表示此平台不支援此功能。
5. 按一下**確定**。
   已為設定系統鎖定模式成功建立工作。若要檢查工作狀態，前往**工作** > **系統鎖定模式**。如需更多有關系統鎖定模式工作的資訊，請參閱系統鎖定模式工作 第頁的 67。

18

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. 以該使用者登錄 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。

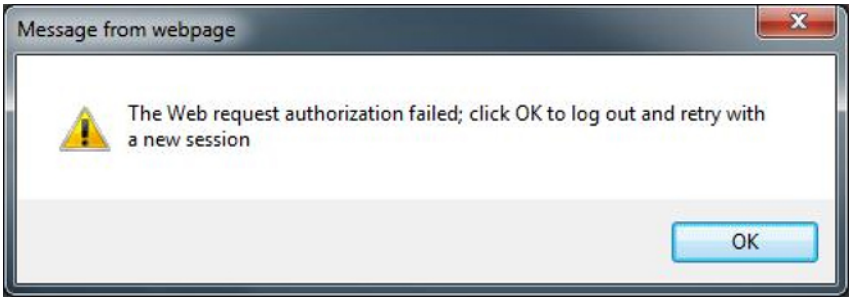


圖 1. 安全性錯誤訊息

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 25. 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

表 25. 權限群組 (續)

組群名稱	說明
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

19

常見問題集 - FAQ

您可以使用本節尋找疑難排解問題的答案。本節包括：

- 常見問題集 (FAQ)
- 裸機部署問題 第頁的 144

常見問題集 - FAQ

本節包含一些常見問題和解決方式。

不相容的 vSphere 主機會顯示不正確的 iDRAC 授權類型和說明

如果 CSIOR 被停用或尚未執行時，主機是不相容的，那麼即使有有效的 iDRAC 授權可以使用，還是會顯示不正確的 iDRAC 授權資訊。因此，雖然您可以在 vSphere 主機清單中檢視該主機，當您按一下該主機想要查看詳細資料時，**iDRAC 授權類型**中並不會顯示任何資訊，而 **iDRAC 授權說明**中會顯示「您的授權需要升級」。

解決方法：若要解決這個問題，請在參照伺服器上啟用 CSIOR。

受影響的版本：4.0 及更新版本

Dell 供應商並未顯示為健康狀況更新供應商

當您在 OMIVV 註冊 vCenter Server，然後升級 vCenter Server 版本 (例如，從 vCenter 6.0 升級為 vCenter 6.5) 時，Dell 供應商並未顯示在**主動式 HA 供應商**清單中。

解決方法：您可以針對非系統管理員使用者或系統管理員使用者，升級已註冊的 vCenter。若要升級至最新版本的 vCenter Server，請先參閱 VMware 說明文件，再執行以下任何一個選項 (如果適用)：

- 針對非管理員使用者：
  1. 如有必要，請指派額外的權限給非系統管理員使用者。請參閱非管理員使用者必須具備的權限 第頁的 12。
  2. 重新啟動已登錄的 OMIVV 裝置。
  3. 登出 vSphere 用戶端，然後再次登入。
- 針對管理員使用者：
  1. 重新啟動已登錄的 OMIVV 裝置。
  2. 登出 vSphere 用戶端，然後再次登入。

這次 Dell 供應商就會列在**主動式 HA 供應商**清單中了。

受影響的版本：4.0 及更新版本

由於無效或未知的 iDRAC IP，導致主機清查或測試連線失敗。

由於無效或未知的 iDRAC IP，導致主機清查或測試連線失敗，接著您會收到「網路延遲或無法連線主機」、「連線遭拒」、「作業逾時」、「WSMAN」、「無法路由至主機」和「IP 位址：Null」等訊息。

1. 開啟 iDRAC 虛擬主控台。
2. 按下 F2 並移至**疑難排解選項**。
3. 在**疑難排解選項**中，移至**重新啟動管理代理程式**。
4. 若要重新啟動管理代理程式，請按下 F11。

現在可為您提供有效的 iDRAC IP。

註: OMIVV 無法啟用在執行 ESXi 6.5 的主機上的 WBEM 服務時，主機清查也可能會失敗。請參閱 建立主機認證設定檔 第頁的 34，以獲得 WBEM 服務的詳細資訊。

在執行修復不相容 vSphere 主機精靈時，某個特定主機的狀態會顯示為「不明」

當您執行修復不相容的 vSphere 主機精靈來修復不相容的主機時，特定主機的狀態會顯示為「未知」。當無法連線到 iDRAC 時，就會顯示該未知狀態。

解決方法：驗證主機的 iDRAC 連線，並且務必順利執行清查。

受影響的版本：4.0

在登錄 OMIVV 應用裝置時所獲指派的 Dell 權限，不會在取消登錄 OMIVV 後移除

在 OMIVV 裝置註冊 vCenter 之後，vCenter 權限清單中會新增數個 Dell 權限。但是從 OMIVV 裝置取消註冊 vCenter 時，Dell 權限並不會移除。

註: 雖然這些 Dell 權限未移除，但不會對所有 OMIVV 作業產生任何影響。

受影響的版本：3.1 及更新版本

我該如何解決因 VMware 憑證發行單位 (VMCA) 所導致的錯誤代碼 2000000

當您執行 vSphere 憑證管理員，並將 vCenter 伺服器或平台控制器服務 (PSC) 憑證替換為新的 CA 憑證和 vCenter 6.0 金鑰時，OMIVV 便會顯示錯誤代碼 2000000，並擲回例外。

解決方法：若要解決這個例外狀況，應該更新服務的 ssl Anchor。您可以在 PSC 上執行 `ls_update_certs.py` 指令碼來更新 ssl Anchor。這個指令碼會將舊的憑證指紋視為輸入引數，而將新的憑證視為已安裝。舊憑證是替換之前的憑證，而新憑證是替換之後的憑證。如需更多詳細資訊，請參閱 https://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121701 和 https://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121689。

受影響的版本：3.0 及更新版本、vCenter 6.0 及更新版本

替換 vCenter Windows 安裝上的憑證

如需更多資訊，請參閱 https://kb.vmware.com/s/article/2121689。

替換 vCenter 伺服器應用裝置上的憑證

如需更多資訊，請參閱 https://kb.vmware.com/s/article/2121689。

從受管物件瀏覽器 (MOB) 擷取舊憑證

如需更多資訊，請參閱 https://kb.vmware.com/s/article/2121701。

從舊憑證擷取指紋

如需更多資訊，請參閱 https://kb.vmware.com/s/article/2121701。

我已將應用裝置重設為原廠設定，但是在系統管理主控台中，更新儲存庫路徑卻沒有設定為預設路徑

請在重設應用裝置之後，前往**系統管理主控台**，然後在左窗格中按一下**應用裝置管理**。**應用裝置設定**頁面上的**更新儲存庫路徑**並未改為預設路徑。

解決方案：在**系統管理主控台**中，將**預設更新儲存庫**欄位中的路徑，手動複製到**更新儲存庫路徑**欄位。

如果在 OMIVV 變更 DNS 設定後，vCenter HTML-5 Client 出現 Web 通訊錯誤，我該怎麼做

如果您在變更 DNS 設定後，進行任何 OMIVV 相關工作時，vCenter HTML-5 Client 上出現任何種類的 Web 通訊錯誤，請執行下列其中一項：

- 清除瀏覽器快取記憶體。
- 登出後再登入 vSphere 用戶端。

韌體頁面上有些韌體的安裝日期顯示為 1969 年 12 月 31 日

在 vSphere 用戶端中，主機韌體頁面上有些韌體項目的安裝日期會顯示為 12/31/1969。如果沒有韌體安裝日期，就會顯示舊的日期。

解決方式：凡是有韌體元件顯示這個老舊的日期，就表示它沒有安裝日期可用。

受影響的版本：2.2 以後的版本

即使在 vCenter 成功註冊外掛程式，我在 HTML-5 用戶端上還是看不到 OpenManage Integration 圖示

除非 vSphere Client 服務重新啟動，否則 OpenManage Integration 圖示不會顯示在 vSphere Client 上。當您註冊 OpenManage Integration for VMware vCenter 裝置時，該裝置會同時在 vSphere Client 上註冊。如果您取消註冊裝置，然後再重新註冊相同版本，或是註冊該裝置的新版本，系統會成功註冊，但是 vSphere Client 中可能不會顯示 OMIVV 圖示。這是 VMware 的快取問題所導致。若要解決這個問題，請務必在 vCenter Server 上重新啟動 vSphere Client 服務。這樣外掛程式便會顯示在 UI 中。

解決方案：在 vCenter Server 上重新啟動 vSphere Client 服務。

受影響的版本：2.2 以後的版本

如果應用裝置 IP 和 DNS 設定被覆寫為 DHCP 值，則應用裝置重新開機之後，DNS 組態設定會還原為原始設定，為什麼？

以靜態方式指派的 DNS 設定，會被來自 DHCP 的值取代，這是目前已知的個問題。當 DHCP 被用來取得 IP 設定，且 DNS 值是以靜態方式指派時，就會發生這種情形。當 DHCP 租賃續約，或應用裝置重新啟動時，以靜態方式指派的 DNS 設定就會遭到移除。

解決方案：DNS 伺服器設定與 DHCP 不同時，請以靜態方式指派 IP 設定。

受影響的版本：全部

執行韌體更新可能會顯示錯誤訊息：韌體儲存庫檔案不存在或無效。

執行韌體更新精靈時，在叢集層級上可能會顯示錯誤訊息：**韌體儲存庫檔案不存在或無效**。這可能是因為每日背景程序無法從儲存庫下載和快取目錄檔案。如果在背景程序執行時無法連線到目錄檔案，就會發生這種情況。

解決方案：解決可能存在的任何目錄連線問題後，您可以變更韌體儲存庫位置，然後將它設回原來的位置，以重新初始化背景程序。完成背景程序需要大約五分鐘的時間。請確定提供給 CIFS 的認證中沒有存在 @ 字元。此外，請確定 DUP 檔案存在於共用位置。

受影響的版本：全部

不支援使用 OMIVV 來更新搭載 13.5.2 版韌體的 Intel 網路卡

Dell PowerEdge 伺服器和部分搭載 13.5.2 版韌體的 Intel 網路卡具有已知問題。當韌體更新是使用 iDRAC 和 Lifecycle Controller 加以套用，則搭載此版本韌體之部分型號的 Intel 網路卡便無法順利更新。本版韌體的客戶，必須使用作業系統來更新網路驅動程式軟體。如果 Intel 網路卡所搭載的韌體不是 13.5.2 版， 您就可以使用 OMIVV 來進行更新。如需更多資訊，請參閱 http://en.community.dell.com/techcenter/b/techcenter/archive/2013/03/20/intel-network-controller-card-with-v13-5-2-firmware-cannot-be-upgraded-using-lifecycle-controller-to-v13-5-6.aspx

註: 使用一對多韌體更新時，請避免選取搭載 13.5.2 版的 Intel 網路介面卡，因為更新會失敗，繼而使更新工作停止更新其餘的伺服器。

由於 DUP 的分段需求，而無法使用 OMIVV 將 Intel 網路卡從 14.5 或 15.0 更新至 16.x

這是 NIC 14.5 和 15.0 的已知問題。您必須先使用自訂目錄將韌體更新至 15.5.0 之後，才能將韌體更新至 16.x。

受影響的版本：全部

為什麼系統管理入口網站顯示無法連線的更新儲存庫位置

如果您提供一個無法連上的更新儲存庫路徑，「裝置更新」檢視的頂端會顯示「失敗：連線至 URL....時發生錯誤」的錯誤訊息。但是，更新儲存庫路徑並不會被清除為更新之前的值。

解決方法：從這一頁移到另一頁，並且務必重新整理頁面。

受影響的版本：全部

為什麼執行一對多韌體更新時，系統沒有進入維護模式

有些韌體更新不需要重新啟動主機。在這種情況下更新韌體時，就不需要讓主機進入維護模式。

有些電源供應器狀態已變成「嚴重」，機箱全域健全狀況卻仍然顯示為「健全」

有關電源供應器的機箱全域健全狀況，是以備援原則，以及仍在線上且正常運作的 PSU 是否滿足機箱電源需求為依據。所以即使有部分 PSU 已經沒電了，仍然符合機箱的整體電源需求。因此機箱全域健全狀況仍是「健全」。如需深入瞭解電源供應器和電源管理，請查看 Dell EMC PowerEdge M1000e 機箱管理控制器韌體文件的使用者指南。

在系統概觀頁面的處理器檢視中，處理器版本顯示為「不適用」

在 12G 及更新版本的伺服器中，處理器版本位於「品牌」欄。而在較低世代的伺服器中，處理器版本是顯示在**版本**欄。

OMIVV 在連結模式中是否支援 vCenter

可以，OMIVV 可以採用連結模式或未連結模式支援多達 10 個 vCenter Server。

OMIVV 有哪些必要的連接埠設定

使用下列適用於 OMIVV 的連接埠設定：

表 26. 虛擬裝置

連接埠號碼	通訊協定	連接埠類型	最大的加密層級	方向	目的地	使用	說明
53	DNS	TCP	無	輸出	OMIVV 裝置至 DNS 伺服器	DNS 用戶端	連線至 DNS 伺服器或解析主機名稱。
68	DHCP	UDP	無	輸入	DHCP 伺服器至 OMIVV 裝置	動態網路組態	用以取得網路詳細資料，例如 IP、閘道、網路遮罩和 DNS。
69	TFTP	UDP	128 位元	輸出	OMIVV 至 iDRAC	簡單式檔案傳輸	用於將裸機伺服器更新至最低受支援的韌體版本。
123	NTP	UDP	無	輸入	NTP 至 OMIVV 裝置	時間同步處理	與特定時區同步。
162	SNMP 代理程式	UDP	無	輸入	iDRAC 或 CMC，或 OME-Modular 至 OMIVV 裝置	SNMP 代理程式 (伺服器)	接收來自受管節點的 SNMP 陷阱。
80/443	HTTP/HTTPS	TCP	無	輸出	OMIVV 裝置至網際網路	Dell 線上資料存取	連線至線上 (網際網路) 保固、韌體與最新的 RPM 資訊。
443	HTTPS	TCP	128 位元	輸入	OMIVV UI 至 OMIVV 裝置	HTTPS 伺服器	OMIVV 提供的 Web 服務。這些 Web 服務是由 vSphere 用戶端和 Dell 系統管理員入口網站所用。
443	HTTPS	TCP	128 位元	輸入	ESXi 伺服器至 OMIVV 裝置	HTTPS 伺服器	用於作業系統部署流程，讓安裝後指令碼能與 OMIVV 應用裝置通訊。
443	HTTPS	TCP	128 位元	輸入	iDRAC 至 OMIVV 裝置	自動探索	用於自動探索受管節點的佈健伺服器。
443	WSMAN	TCP	128 位元	輸入/輸出	OMIVV 裝置至/來自 iDRAC	iDRAC 通訊	iDRAC 和 CMC 或 OME-Modular 通訊，用來管理和監控受管節點。
445/139	SMB	TCP	128 位元	輸出	OMIVV 裝置至 CIFS	CIFS 通訊	與 Windows 共用通訊。
2049/111	NFS	UDP/TCP	無	輸入/輸出	OMIVV 裝置至 NFS	公用共用	由 OMIVV 應用裝置公開給受管節點的 NFS 公用共用，用於韌體更新和作業系統部署流程。
4001 至 4004	NFS	UDP/TCP	無	輸入/輸出	OMIVV 裝置至 NFS	公用共用	這些連接埠必須保持開啟狀態，才能執行 statd、quotd、lockd 以及由 NFS 伺服器之 V2 和 V3 通訊協定裝載的服務。
使用者定義	任何	UDP/TCP	無	輸出	OMIVV 裝置至 Proxy 伺服器	Proxy	與 Proxy 伺服器通訊。

表 27. 受管節點 (ESXi)

連接埠號碼	通訊協定	連接埠類型	最大的加密層級	方向	目的地	使用	說明
162	SNMP	UDP	無	輸出	ESXi 至 OMIVV 裝置	硬體事件	從 ESXi 傳送的非同步 SNMP 陷阱。此連接埠必須從 ESXi 開啟。
443	WSMAN	TCP	128 位元	輸入	OMIVV 裝置至 ESXi	iDRAC 通訊	用來提供資訊給管理站。此連接埠必須從 ESXi 開啟。
443	HTTPS	TCP	128 位元	輸入	OMIVV 裝置至 ESXi	HTTPS 伺服器	用來提供資訊給管理站。此連接埠必須從 ESXi 開啟。

如需 iDRAC 和 CMC 連接埠資訊的詳細資訊，請參閱 **https://www.dell.com/support** 上的 *Integrated Dell Remote Access Controller 使用者指南*和 *Dell 機箱管理控制器使用者指南*。

如需 OME-Modular 連接埠資訊的詳細資訊，請參閱 **https://www.dell.com/support** 上的 *Dell EMC OME-Modular 使用者指南*。

註: 如為 iDRAC9 型伺服器，iDRAC 是透過連接埠 2049 的 TCP 來安裝 NFS。如需 iDRAC9 型伺服器的清單，請參閱相容性比較表。

成功套用系統設定檔 (相同使用者在 iDRAC 使用者清單有變更的新認證)後，用於裸機探索的使用者密碼沒有變更

如果僅選取系統設定檔 (硬體的組態) 以進行部署，則用於探索的使用者密碼不會變更為新認證。我們刻意設計成這樣，如此一來外掛程式才能在日後需要部署時與 iDRAC 通訊。

看不到列在 vCenter 主機與叢集頁面上的新 iDRAC 版本詳細資料

解決方法：在 vSphere W eb 用戶端順利完成韌體更新工作後，請重新整理**韌體更新**頁面，並驗證韌體版本。如果頁面顯示的是舊版本，請前往 OpenManage Integration for VMware vCenter 的**主機相容性**頁面，檢查該主機的 CSIOR 狀態。如果 CSIOR 沒有啟用，請啟用 CSIOR，然後重新啟動主機。如果 CSIOR 已經啟用，請登入 iDRAC 主控台重設 iDRAC，等過了幾分鐘後，再重新整理**韌體更新**頁面。

OMIVV 是否能在已啟用鎖定模式的情況下支援 ESXi

可以。這個版本的鎖定模式支援 ESXi 6.0 以上的主機。

我試圖使用鎖定模式卻失敗

當我以鎖定模式將主機新增至主機認證設定檔時，清查啟動後卻失敗，並指出「找不到遠端存取控制器，或是此主機不支援清查」。

如果您讓主機處於鎖定模式，或是從鎖定模式移除主機，則必須先等待 30 分鐘後，才能在 OMIVV 中執行下一個作業。

嘗試在伺服器上部署 ESXi 時失敗

1. 請確定 **ISO 位置 (NFS 路徑)** 和暫置**資料夾路徑**皆正確無誤。
2. 請確定虛擬裝置可存取指派伺服器身分時所選取的 **NIC**。
3. 請確定您根據與 OMIVV 的網路連線來選取管理 NIC。
4. 如果使用**靜態 IP 位址**，請確定提供的網路資訊 (包括子網路遮罩和預設閘道) 正確無誤。同時，請確定 IP 位址尚未指派到網路。
5. 確定系統至少找到 1 個虛擬磁碟、IDSDM 或 BOSS。

部署精靈在顯示自動探索到的系統時，沒有顯示機型資訊

這通常代表系統所安裝的韌體版本不符合建議的最低需求。有時候可能是韌體更新尚未在系統上註冊。

解決方法：將系統冷開機或重新接插刀鋒，即可解決這個問題。您必須停用 iDRAC 上新啟用的帳戶，然後重新起始自動探索，才能提供型號資訊和 NIC 資訊給 OMIVV。

NFS 共用是使用 ESXi ISO 加以設定，但是部署卻失敗，而且出現共用位置裝載錯誤

若要尋找解決方式：

1. 確認 iDRAC 能夠 Ping 到裝置。
2. 確認網路執行速度不是太慢。
3. 確認連接埠：2049、4001-4004 已開啟，且防火牆相應設定正確。

我要如何從 vCenter 強制移除 OMIVV 裝置

1. 移至 vSphere 用戶端，然後針對所有已啟用主動式 HA 的叢集，清除 Dell 提供者的核取方塊。
2. 前往 **https://<vcenter_serverIPAddress>/mob**
3. 輸入 VMware vCenter 管理員認證。
4. 按一下**首頁** > **內容** > **HealthUpdateManager**。
5. 按一下 **QueryProviderList** > **叫用方式**。
6. 複製提供者 ID 字串值，然後關閉視窗。
7. 按一下 **UnregisterHealthUpdateProvider**，然後輸入複製的提供者 ID 字串值。
8. 按一下**叫用方式**。
9. 前往**首頁** > **內容**
10. 按一下 **ExtensionManager** 。
11. 按一下 **UnregisterExtension**。
12. 輸入擴充碼，取消登錄 com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient，然後按一下**叫用方式**。
13. 在 vSphere Client 中關閉 OMIVV，並加以刪除。取消登錄機碼必須用於 vSphere Client。
14. 在 vCenter 中清除 serenity 項目，然後重新啟動 vCenter 服務。

在立即備份畫面輸入密碼時收到錯誤訊息

如果您使用的是低解析度的顯示器，則在「立即備份」視窗中不會看到「加密密碼」欄位。向下捲動頁面，才能輸入加密密碼。

韌體更新失敗時該怎麼辦

檢查 OMIVV 裝置記錄，看看工作是否已經逾時。如果是，則必須透過正常關機再開機來重設 iDRAC。系統啟動並執行後，請執行清查或使用**韌體**標籤，看看是否有順利更新。

vCenter 登錄失敗時該怎麼辦

vCenter 註冊可能會因為通訊問題而失敗，因此發生這類問題時，解決方法之一就是使用靜態 IP 位址。若要使用靜態 IP 位址，請在 OpenManage Integration for VMware vCenter 的「主控台」標籤中選取**設定網路** > **編輯裝置**，然後輸入正確的**閘道**和 **FQDN** (完整網域名稱)。接著在「編輯 DNS 組態」底下，輸入 DNS 伺服器名稱。

註: 請確認虛擬裝置可以解析您所輸入的 DNS 伺服器。

主機認證設定檔測試認證時，效能緩慢或沒有回應

伺服器上的 iDRAC 只有一個使用者 (例如，只有*根使用者*)，而該使用者處於停用狀態，或所有使用者都處於停用狀態。與處於停用狀態的伺服器通訊會導致延遲。若要解決這個問題，您可以修正伺服器的停用狀態，或重設伺服器上的 iDRAC，將根使用者重新啟用到預設設定。

若要修正停用狀態的伺服器：

1. 打開「機箱管理控制器」主控台，選取停用的伺服器。
2. 若要自動開啟 iDRAC 主控台，請按一下**啟動 iDRAC 圖形化使用者介面 (GUI)**。
3. 導覽至 iDRAC 主控台中的使用者清單，然後按以下其中一項：
   - iDRAC7：選取 **iDRAC 設定** >「**使用者**」**標籤**。
   - iDRAC8：選取 **iDRAC 設定** >「**使用者**」**標籤**。
   - iDRAC9：選取 **iDRAC 設定** > **使用者標籤**。

   若為 iDRAC 7 和 8：

   a. 若要編輯設定，在使用者 ID 欄位中，按一下管理 (根) 使用者的連結。
   b. 按一下**設定使用者**，然後按一下**下一步**。
   c. 在所選使用者的**使用者組態**頁面中，選取「啟用使用者」旁的核取方塊，然後按一下**套用**。

若為 iDRAC9：

a. 選取**根**使用者，然後按一下**啟用**。

OMIVV 是否支援 VMware vCenter Server 應用裝置

支援，OMIVV 自 v2.1 開始便支援 VMware vCenter Server 應用裝置。

伺服器可能會顯示為不相容於 CSIOR 狀態，「未知」

解決方案：未知的 CSIOR 狀態表示主機上的 iDRAC 無回應。在主機上手動重設 iDRAC 可解決此問題。

受影響的版本：全部

我已使用「下次重新開機時套用」選項執行韌體更新，且系統已重新開機，但韌體層級卻沒有更新

若要更新韌體，請在主機重新開機之後，在主機上執行清查。有時候，如果重新開機事件沒有到達應用裝置，就不會自動觸發清查。在這種情況下，您必須手動重新執行清查，才能更新韌體版本。

主機已從 vCenter 樹狀結構移除，卻仍然顯示在機箱下

機箱底下的主機，被視為是機箱清查的一部分。待機箱清查順利完成之後，就會更新機箱底下的主機清單。即使主機已從 vCenter 樹狀結構中移除，該主機仍會顯示在機箱底下，直到下次執行機箱清查為止。

在備份及還原 OMIVV 後，警報設定沒有還原

還原 OMIVV 裝置的備份並不會還原所有的警報設定。不過在 OpenManage Integration for VMware GUI 中，**警報與事件**欄位會顯示已還原的設定。

解決方案：在 OMIVV GUI 的**設定**標籤中，手動變更**事件與警報**設定。

NPAR 若是在目標節點上啟用但在系統設定檔上停用，作業系統部署會失敗

在目標機器上套用的系統設定檔若停用 NIC 分割 (NPAR)，作業系統部署會失敗。此處的目標節點上已啟用 NPAR，而且在透過部署精靈進行部署的過程中，僅會選取一個分割 NIC (分割區 1 除外) 作為管理工作的 NIC。

解決方案：如果您要在進行部署時利用系統設定檔變更 NPAR 狀態，請確定在部署精靈的管理網路中，僅選取第一個分割區。

受影響的版本：4.1 及更新版本

當可用版本比目前版本更舊，可用的 OMIVV 裝置版本會顯示錯誤資訊

在 OMIVV 管理主控台的**裝置管理**下方，**可用的虛擬裝置版本**會將 RPM 與 OVF 模式顯示為可用。

註: 建議您將更新儲存庫路徑設定為最新版本，且不支援虛擬設備版本降級。

新增 12G 與更新的裸機伺服器時，會發生 267027 例外狀況

在裸機探索時，如果輸入錯誤的認證，使用者帳戶會自動鎖定幾分鐘。在這段期間、iDRAC 將無法回應，並需要花費幾分鐘的時間回復正常。

解決方法：等待幾分鐘，然後重新輸入使用者認證。

在部署期間，系統設定檔會因 iDRAC 錯誤而套用失敗

在部署期間，OMIVV 會嘗試在 iDRAC 中建立組態更新工作。但是，工作建立有時會失敗，並顯示訊息指出組態工作已建立。

解決方案：請清除過時項目，然後重試部署。登入 iDRAC 以清除工作。

當 Proxy 設定有網域使用者驗證時，OMIVV RPM 升級會失敗

如果 OMIVV 裝置已設定使用 Proxy 連線至網際網路，而且 Proxy 已使用 NTLM 驗證通過驗證，那麼 RPM 更新會因基礎 YUM 工具的問題而失敗。

受影響的版本: OMIVV 4.0 及更新版本

解決方法/因應措施：請備份並還原，以更新 OMIVV 應用裝置。

無法套用 FX 機箱中有 PCIe 卡的系統設定檔

如果來源伺服器使用 FX 機箱時有 PCIe 卡資訊，目標伺服器上的 OS 部署會失敗。系統設定檔的 `fc.chassislot ID` 在來源伺服器和目標伺服器上會不一樣。OMIVV 嘗試在目標伺服器上部署相同的 `fc.chassislot ID`，但卻失敗。系統設定檔在套用設定檔時，會搜尋確切的執行個體 (FQDD)，這點在完全相同的機架式伺服器上可以成功運作，但在模組化伺服器中則有少數限制。例如在 FC640 中，從模組化伺服器建立的系統設定檔會因為 NIC 層級的限制，而無法套用至相同 FX 機箱中的其他模組化伺服器。

受影響的版本：4.1 及更新版本。

解決方案：從 FX2 機箱插槽 1 的 FC640 伺服器取得的系統設定檔，只能套用到存在於另一個 FX2 機箱插槽 1 的另一個 FC640 伺服器。

漂移偵測針對 FX 機箱裝有 PCIe 卡的模組化伺服器顯示為不合規

系統設定檔在與基準進行比對時，會搜尋確切的執行個體 (FQDD)，這點在完全相同的機架式伺服器上可以成功運作，但在模組化伺服器中則有少數限制。例如在 FC640 中，從一個模組化伺服器建立的系統設定檔 (基準) 會因為 FQDD 比對不符，而顯示相同 FX 機箱中的其他模組化伺服器有偏移現象。

受影響的版本：4.1 及更新版本。

解決方法：在建立系統設定檔時，清除未與其他伺服器通用的 FQDD。

當 iDRAC 未填入所選 NIC 的 MAC 位址時，無法在 PowerEdge 伺服器上部署作業系統

當 iDRAC 未填入所選 NIC 連接埠的 MAC 位址時，PowerEdge 伺服器上的作業系統部署會失敗。

解決方法：將各自的 NIC 韌體和 iDRAC 韌體更新至最新版本，並確定在 NIC 連接埠上填入 MAC 位址。

受影響的版本：4.3 及更新版本

為具備 ESXi 6.5U1 的主機建立主機認證設定檔時，「選取主機」頁面上不會顯示該主機的產品服務編號

當 OMIVV 向 vCenter 查詢 ESXi 的產品服務編號時，vCenter 無法傳回產品服務編號，因為產品服務編號值為 Null。

解決方案：將 ESXi 版本更新至 ESXi 6.5U2 或 ESXi 6.7 U1。

受影響的版本：4.3 及更新版本

在備份並從舊版 OMIVV 還原至較新 OMIVV 版本後，並未顯示 Dell EMC 圖示

在備份並從舊版 OMIVV 還原至較新 OMIVV 版本後，出現以下問題：

- Dell EMC 標誌未顯示在 vCenter 中。
- 2000000 錯誤
- 3001 錯誤

  解析度：

  - 在 vCenter 伺服器上重新啟動 vSphere 用戶端。
  - 如果問題仍然存在，請執行下列步驟：
    - 如果是 VMware vCenter Server 裝置，請前往 `/etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity`，如果是 Windows vCenter，請前往 vCenter 裝置中的 `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\vc-packages\vsphere-client-serenity` 資料夾，看看是否有舊資料存在，例如：com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.XXX。
    - 手動刪除對應舊版 OMIVV 的資料夾。

使用 OMIVV 進行部分 iDRAC 韌體版本的升級或降級時，即使韌體更新成功，OMIVV 仍可能指出工作失敗。

韌體更新期間，當您進行 iDRAC 版本 (例如 3.20.20.20、3.21.21.21 和 3.21.21.22) 的降級或升級時，即使工作已順利執行，但狀態卻顯示為失敗。

解決方法：在工作失敗後重新整理清查，然後為其他元件重新執行工作。

受影響的版本：4.3

在叢集層級設定系統鎖定模式時，有時會出現「未成功清查叢集下的任何主機」訊息

在叢集層級設定系統鎖定模式時，有時會顯示「未成功清查叢集下的任何主機」訊息。即使叢集已成功清查由 OMIVV 管理的 iDRAC9 型伺服器，依然會顯示此訊息。如需 iDRAC9 型伺服器的清單，請參閱相容性比較表。

解決方法：重新啟動 vCenter。

若要重新啟動 vCenter，請執行下列步驟：

1. 使用 vCenter 單一登入系統管理員帳戶登入 vSphere 用戶端。
2. 前往**管理** > **部署** > **部署** > **系統組態**。
3. 按一下**節點**，選取 vCenter Server 裝置節點，再按一下**相關的物件**標籤。
4. 重新啟動 vCenter 節點。

有時在 OMIVV 設備的 RPM 升級之後，在 vCenter 最近的工作中檢視記錄時會看到多個項目。

有時在 RPM 升級之後，在 vCenter 最近的工作中檢視記錄時會發現有多個項目。

解決方法：重新啟動 vCenter 服務。

受影響的版本：4.3

註冊 vCenter 後，OMIVV 的 Dell EMC 標誌不會顯示在 VMware 的首頁上

說明：OMIVV 的 Dell EMC 標誌可能不會顯示在 VMware 的**首頁**上，因為註冊完成後不久，VMware vCenter 將會驗證外掛程式。

解決方案：執行下列步驟：

1. 重新整理瀏覽器或清除瀏覽器快取，或為 vSphere Client (HTML-5) 重新啟動用戶端服務。
2. 登出 vSphere 用戶端，然後再次登入。

受影響的版本：5.0

在備份和還原後，不相容的 11G PowerEdge 伺服器會保留在 OMIVV 清查中

在 OMIVV 中執行備份和還原操作之後，不相容且未清查的 11G 主機仍會與主機認證設定檔相關聯。但是，如果您嘗試修正組態相容性並執行全新清查，則工作在不支援的 11G 伺服器上會失敗。

解決方案：OMIVV 5.0 不支援 11G 伺服器。從主機認證設定檔中，手動移除不支援的 11G 主機。

受影響的版本：5.0

升級 OMIVV 裝置後，無法從 Flex 用戶端啟動 vCenter

解決方案：如需解決方案，請參閱以下 KB 文章：https://kb.vmware.com/s/article/54751。

受影響的版本：5.0

在 OMIVV 上新增或移除網路配接卡時，現有的 NIC 會從 OMIVV 主控台消失

有時，當您使用 vSphere 用戶端在 OMIVV 應用裝置中新增或移除網路配接卡時，現有的 NIC 會從 OMIVV 主控台消失。

因應措施：執行下列任一工作：

1. a. 從終端主控台公用程式移除所有工作配接卡。
   b. 將裝置關機
   c. 從裝置移除網路配接卡。
   d. 重新啟動 OMIVV 裝置。
   e. 將裝置關機
   f. 新增必要的網路配接卡，並完成網路配接卡組態。
   g. 重新啟動裝置。
2. a. 從系統管理員入口網站備份 OMIVV
   b. 建立 OMIVV 裝置。
   c. 將裝置關機
   d. 新增必要的網路配接卡，並完成網路配接卡組態。
   e. 重新啟動裝置。
   f. 還原最新的備份資料。

受影響的版本：OMIVV 5.0

新增或卸下第二個 NIC 後，網路組態頁面會顯示三個 NIC

在您使用 vSphere 用戶端從 OMIVV 裝置中新增或移除 NIC 之後，一旦將 OMIVV 裝置開機並登入 OMIVV 終端主控台，有時**網路組態**頁面會顯示不一致的 NIC 數量。

解決方案：使用 MAC 位址來比較並設定正確的 NIC，然後使用 **–** 按鈕移除額外的 NIC。

受影響的版本：5.0

在備份並還原至最新 OMIVV 版本後，舊版中狀態未知的伺服器未列在裸機伺服器頁面上

從舊版還原備份後，不受支援的伺服器 (11G 及更早世代) 會從裸機伺服器清查中移除。而備份之前未被舊版確定其世代的伺服器也會一併移除。

解決方案：重新探索伺服器。如果遺失的伺服器受到支援，則會列在裸機伺服器清查中。

受影響的版本：5.0

在部署作業系統後，OMIVV 無法將 ESXi 主機新增至 vCenter 或無法新增主機設定檔，或是主機無法進入維護模式

在部署作業系統後，OMIVV 會查詢 vCenter 以執行主機動作 (新增主機、新增主機設定檔，或進入維護模式)。如果查詢未在兩分鐘內收到回應，vCenter 上的特定動作會逾時，而且工作歷程記錄會顯示訊息，表示通訊失敗。但是，vCenter 查詢作業有時會成功。

解決方案：從工作歷程記錄中取得主機 IP，然後手動新增。

無法連線到 iDRAC IP 時，管理相容性頁面上的 iDRAC 授權狀態會顯示為相容

執行定期清查後若無法連線到 iDRAC，管理相容性頁面上的 iDRAC 授權狀態會顯示為相容。

解決方案：請確定可連線到 iDRAC，並再次執行清查以取得正確的 iDRAC 授權詳細資料。

在使用 OMIVV 成功部署作業系統後，ESXi 主機會中斷連線或處於未回應狀態。

ESXi 主機無法將活動訊號封包傳送到 vCenter，因為其 DNS 未正確設定為查閱 vCenter 的 FQDN。

解決方案：執行下列工作：

1. 從 vCenter 清查中移除 ESXi 主機。
2. 使用**新增主機**精靈，將主機新增至 vCenter。
3. 建立主機認證設定檔，並執行清查。

OMIVV 的網路介面卡 (NIC) 未連線至 ESXi 主機網路時，部署工作會逾時

作業系統部署依存於所選的 NIC。如果未選取正確的 NIC，則 OSD 工作會逾時。

解決方案：在部署精靈的「配置主機設定」頁面中，選取適當的「連線至主機的裝置 NIC」。在作業系統安裝過程中，OMIVV 需要使用此功能來連線到 ESXi 網路。

特定主機的保固工作未執行

在有多個 vCenter 的 PSC 環境中，如果您將使用 FQDN 的主機新增到一個 vCenter，並將 IP 新增至另一個 vCenter，則系統只會執行一個主機執行個體的保固工作。

解決方案：從主機認證設定檔中移除中斷連線的主機執行個體，然後執行清查和保固工作。

受影響的版本：5.0

執行備份和還原後不會發生主動式 HA 初始化

當您從已在 vSphere Client 上註冊的舊版還原 OMIVV 時，對於主動式 HA 叢集，Dell 提供者已中斷連線。

解決方案：停用並啟用叢集的主動式 HA。

受影響的版本：5.0

OMIVV 頁面會在 Firefox 瀏覽器中顯示無效的工作階段、逾時例外，或是 2 百萬個錯誤

如果 OMIVV 頁面閒置了一段時間 (5–10 分鐘)，則會顯示無效的工作階段、逾時例外，或是 2 百萬個錯誤。

解決方案：重新整理瀏覽器。如果問題仍然存在，請從 `vCenter` 登出並再次登入。

若要在 OMIVV 中看到正確的資料，請確定您已完成解決方案中所列的工作。

受影響的版本：5.0

在 vCenter 中，「最近的工作」窗格不會顯示某些 OMIVV 工作通知的詳細資料欄

解決方案：若要查看工作通知，請在 vCenter 中，前往 vCenter 的**工作主控台**。

受影響的版本：5.0

使用 vCenter 6.5 U2 時，可能會在 OMIVV 的所有頁面顯示 2000002 錯誤

解決方案：使用 VMware for 6.5 U2 提供的最新修補程式，或遷移至 6.5 U3 版及更新版本。

受影響的版本：5.1

執行 RPM 升級或備份並從舊版的 OMIVV 還原到新版的 OMIVV 後，會在 OMIVV 的所有頁面中顯示 2000002 錯誤

註冊目前的版本之前，如果您在 vCenter 伺服器中有舊版的 OMIVV，則 SSL 交握異常會導致無法連接新版的 OMIVV，直到 vCenter 重新整理新的外掛程式資料為止 。 因為 vCenter 包含舊版 OMIVV 的資料，而舊版本會以不同方式處理 SSL 流量。

解析度：

- 在 vCenter 伺服器上重新啟動 vSphere 用戶端。
- 如果問題仍然存在，請執行下列步驟：
  - 若為 VMware vCenter Server 裝置，請前往 `/etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity`，若為 Windows vCenter，請前往 vCenter 裝置中的 `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\vc-packages\vsphere-client-serenity` 資料夾，查看舊資料是否存在，例如：com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.XXX。
  - 手動刪除對應舊版 OMIVV 的資料夾。
  - 重新啟動適用於 vSphere 用戶端的 vSphere 用戶端服務 (HTML5)

受影響的版本：5.0 及更新版本

有時，OMIVV 需要很長的時間才能完成 vCenter 取消註冊

若您取消註冊的 vCenter 含有大量主機 (超過 300 台)，則 OMIVV 會有很長的時間維持正在載入狀態。

解決方案：重新整理瀏覽器。

如果 vCenter 取消註冊不成功，請重新取消註冊 vCenter。

受影響的版本：5.1

更新 OMIVV 憑證後，顯示「連線 OMIVV 裝置失敗。SSL 憑證無效」錯誤訊息

解決方法：重新啟動 vCenter 用戶端服務。

受影響的版本：全部

OMIVV 中的部署工作失敗

部署工作失敗，因為 LifeCycle Controller 正忙於完成待處理工作或正在執行其他工作。

解決方案：執行下列步驟：

1. 在 iDRAC 中清除 iDRAC 工作佇列 [選用]
2. 重設 iDRAC
3. 再次執行部署工作

受影響的版本：全部

變更 vCenter 密碼後，在 OMIVV 中的測試連線和清查失敗

在 ESXi 6.7 及更新版本中，OMIVV 會使用智慧平臺管理介面 (IPMI) 通訊協定擷取 ESXi 主機的 iDRAC IP，此操作不需要依賴 WBEM。

但如果 OMIVV 因任何原因而無法擷取 iDRAC IP，OMIVV 便會嘗試使用共用資訊模型 (CIM) 通訊協定 (作為回復)，此方法取決於 WBEM 的狀態。如果用於註冊的 vCenter 使用者密碼已變更，在執行測試連線與清查時，您可能會遭遇與 WBEM 相關的問題。

解決方法：在變更 vCenter 密碼後，請先修改 OMIVV 系統管理主控台中的 vCenter 認證，再在 vCenter 中執行任何操作。如需更多有關修改認證的資訊，請參閱 修改 vCenter 登入認證 第頁的 14。

受影響的版本：全部

在將 OMIVV 裝置重設為原廠設定後，不會從 vCenter 移除 OMIVV 例項

當您將裝置重設為原廠設定時，便會發生此問題。OMIVV 裝置的項目仍會保留在 vCenter 的 `vsphere-client-serenity` 資料夾中，可避免在原廠重設後進行 vCenter 註冊。

解決方法：從 vCenter 中移除 OMIVV 項目。如需更多資訊，請參閱 我要如何從 vCenter 強制移除 OMIVV 裝置 第頁的 136。

受影響的版本：全部

在系統設定檔的「設定檔設定」頁面上，OMIVV 僅會顯示 BIOS 和 iDRAC 屬性

解決方法：將 Google Chrome 升級至最新版本。

受影響的版本：5.2

作業系統部署已完成，但發生未知錯誤

當您使用探索伺服器的使用者以外的其他使用者執行作業系統部署時，就會發生這個問題。OMIVV **記錄**頁面上的錯誤訊息會顯示找不到類別的錯誤。

解決方法：NA，此問題不會影響 OMIVV 功能的功能性。

受影響的版本：5.2

FX2 機箱內的機箱管理控制器 (CMC) 韌體更新失敗

OMIVV 可讓您透過伺服器 iDRAC 更新 FX2 機箱的 CMC 韌體。如果在 iDRAC 中停用了**允許透過作業系統和 Lifecycle Controller 更新 CMC** 選項，則 CMC 韌體更新會失敗。

解決方式：在 iDRAC 內執行下列步驟：

1. 前往**設定** > **更新和復原**。
2. 將**允許透過作業系統和 Lifecycle Controller 更新 CMC** 設定為**啟用**。

受影響的版本：5.2

OMIVV 中的 ISO 設定檔部署失敗

在最新版本的 OMIVV 中，以舊版 OMIVV 排定的 ISO 設定檔部署工作將無效。

解決方法：取消排定的工作，並視需要建立部署工作。

如果排定的工作未取消，部署工作便會失敗。在這種情況下，請以裸機探索伺服器，然後建立 ISO 設定檔部署工作。

受影響的版本：5.2

裸機部署問題

本節處理部署過程所發生的問題。

自動探索與交握必要條件

- 執行自動探索與交握之前，請先確認 iDRAC 和 Lifecycle Controller 韌體及 BIOS 版本皆符合基本建議。
- 您必須在系統或 iDRAC 至少執行一次 CSIOR。

硬體組態失敗

- 在起始部署工作之前，請先確認系統已完成 CSIOR，而且不是正在進行重新開機。
- BIOS 組態最好能夠以複製模式執行，這樣參照伺服器的系統才會一模一樣。
- 有些控制器不允許使用一部磁碟機建立 RAID 0 陣列。只有高階控制器才支援這項功能，且應用這類硬體設定檔可能導致失敗。

在新購買的系統上啟用自動探索

主機系統的自動探索功能預設是不會啟用的；您必須在購買時要求啟用。如果您在購買時要求啟用了自動探索，則 iDRAC 上的 DHCP 會啟用，而系統管理帳戶則會停用。您不需要設定 iDRAC 的靜態 IP 位址。它會從網路上的 DHCP 伺服器取得一個。若要使用自動探索功能，必須將 DHCP 伺服器或 DNS 伺服器 (或兩者) 設定為支援探索程序。CSIOR 應該已在進行原廠程序過程中執行過了。

如果您沒有在購買時要求自動探索，可以用下列方式啟用：

1. 在開機程序中，按下 **Ctrl+E**。
2. 在 iDRAC 設定視窗啟用 NIC (僅適用刀鋒伺服器)。
3. 啟用自動探索。
4. 啟用 DHCP。
5. 停用管理員帳戶。
6. 啟用**從 DHCP 取得 DNS 伺服器位址**。
7. 啟用**從 DHCP 取得 DNS 網域名稱**。
8. 在**佈建伺服器**欄位輸入：

```
<OpenManage Integration virtual appliance IPaddress>:4433
```

A

系統專有屬性

iDRAC

表 28. 系統專有屬性 iDRAC

屬性名稱	顯示屬性名稱	群組顯示名稱
DNS RAC 名稱	DNS RAC 名稱	NIC 資訊
DataCenterName	資料中心名稱	伺服器拓撲
通道名稱	通道名稱	伺服器拓撲
機架名稱	機架名稱	伺服器拓撲
機架插槽	機架插槽	伺服器拓撲
RacName	Active Directory RAC 名稱	Active Directory
地址	IPv4 位址	IPv4 靜態資訊
網路遮罩	網路遮罩	IPv4 靜態資訊
閘道	閘道	IPv4 靜態資訊
DNS2	DNS 伺服器 2	IPv4 靜態資訊
位址 1	IPv6 位址 1	IPv6 靜態資訊
閘道	IPv6 閘道	IPv6 靜態資訊
前置詞長度	IPV6 連結本機前置詞長度	IPv6 靜態資訊
DNS1	IPV6 DNS 伺服器 1	IPv6 靜態資訊
DNS2	IPv6 DNS 伺服器 2	IPv6 靜態資訊
DNSFromDHCP6	來自 DHCP6 的 DNS 伺服器	IPv6 靜態資訊
HostName	伺服器主機名稱	伺服器作業系統
RoomName	RoomName	伺服器拓撲
NodeID	系統節點 ID	伺服器資訊

BIOS

表 29. BIOS 的系統專有屬性

屬性名稱	顯示屬性名稱	群組顯示名稱
AssetTag	資產標籤	雜項設定
IscsiDev1Con1Gateway	啟動器閘道	連線 1 設定
IscsiDev1Con1Ip	啟動器 IP 位址	連線 1 設定
IscsiDev1Con1Mask	啟動器子網路遮罩	連線 1 設定
IscsiDev1Con1TargetIp	目標 IP 位址	連線 1 設定

表 29. BIOS 的系統專有屬性 (續)

屬性名稱	顯示屬性名稱	群組顯示名稱
IscsiDev1Con1TargetName	目標名稱	連線 1 設定
IscsiDev1Con2Gateway	啟動器閘道	連線 1 設定
IscsiDev1Con2Ip	啟動器 IP 位址	連線 1 設定
IscsiDev1Con2Mask	啟動器子網路遮罩	連線 1 設定
IscsiDev1Con2TargetIp	目標 IP 位址	連線 1 設定
IscsiDev1Con2TargetName	目標名稱	連線 1 設定
IscsiInitiatorName	iSCSI Initiator 名稱	網路設定
Ndc1PcieLink1	整合式網路卡 1 PCIe Link1	整合式裝置
Ndc1PcieLink2	整合式網路卡 1 PCIe Link2	整合式裝置
Ndc1PcieLink3	整合式網路卡 1 PCIe Link3	整合式裝置
UefiBootSeq	UEFI 開機順序	UEFI 開機設定

RAID

表 30. RAID 的系統專有屬性

屬性名稱	顯示屬性名稱	群組顯示名稱
機櫃要求的組態模式	NA	NA
機櫃目前的組態模式	NA	NA

CNA

表 31. CNA 的系統專有屬性

屬性名稱	顯示屬性名稱	群組顯示名稱
ChapMutualAuth	CHAP 相互驗證	iSCSI 一般參數
ConnectFirstTgt	連線	iSCSI 第一目標參數
ConnectSecondTgt	連線	iSCSI 第二目標參數
FirstFCoEBootTargetLUN	開機 LUN	FCoE 組態
FirstFCoEWWPNTarget	全球連接埠名稱目標	FCoE 組態
FirstTgtBootLun	開機 LUN	iSCSI 第一目標參數
FirstTgtChapId	CHAP ID	iSCSI 第一目標參數
FirstTgtChapPwd	CHAP 密碼	iSCSI 第一目標參數
FirstTgtIpAddress	IP 位址	iSCSI 第一目標參數
FirstTgtIscsiName	iSCSI 名稱	iSCSI 第一目標參數
FirstTgtTcpPort	TCP 連接埠	iSCSI 第一目標參數
IP 自動設定	IpAutoConfig	iSCSI 一般參數
IscsiInitiatorChapId	CHAP ID	iSCSI 啟動器參數
IscsiInitiatorChapPwd	CHAP 密碼	iSCSI 啟動器參數
IscsiInitiatorGateway	預設閘道	iSCSI 啟動器參數

表 31. CNA 的系統專有屬性 (續)

屬性名稱	顯示屬性名稱	群組顯示名稱
IscsiInitiatorIpAddr	IP 位址	iSCSI 啟動器參數
IscsiInitiatorIpv4Addr	IPv4 位址	iSCSI 啟動器參數
IscsiInitiatorIpv4Gateway	IPv4 預設閘道	iSCSI 啟動器參數
IscsiInitiatorIpv4PrimDns	IPv4 主要 DNS	iSCSI 啟動器參數
IscsiInitiatorIpv4SecDns	IPv4 次要 DNS	iSCSI 啟動器參數
IscsiInitiatorIpv6Addr	IPv6 位址	iSCSI 啟動器參數
IscsiInitiatorIpv6Gateway	IPv6 預設閘道	iSCSI 啟動器參數
IscsiInitiatorIpv6PrimDns	IPv6 主要 DNS	iSCSI 啟動器參數
IscsiInitiatorIpv6SecDns	IPv6 次要 DNS	iSCSI 啟動器參數
IscsiInitiatorName	iSCSI 名稱	iSCSI 啟動器參數
IscsiInitiatorPrimDns	主要 DNS	iSCSI 啟動器參數
IscsiInitiatorSecDns	次要 DNS	iSCSI 啟動器參數
IscsiInitiatorSubnet	子網路遮罩	iSCSI 啟動器參數
IscsiInitiatorSubnetPrefix	子網路遮罩前置詞	iSCSI 啟動器參數
SecondaryDeviceMacAddr	次要裝置 MAC 位址	iSCSI 次要裝置參數
SecondTgtBootLun	開機 LUN	iSCSI 第二目標參數
SecondTgtChapPwd	CHAP 密碼	iSCSI 第二目標參數
SecondTgtIpAddress	IP 位址	iSCSI 第二目標參數
SecondTgtIscsiName	iSCSI 名稱	iSCSI 第二目標參數
SecondTgtTcpPort	TCP 連接埠	iSCSI 第二目標參數
UseIndTgtName	使用獨立的目標名稱	iSCSI 次要裝置參數
UseIndTgtPortal	使用獨立的目標入口網站	iSCSI 次要裝置參數
VirtFIPMacAddr	虛擬 FIP MAC 位址	主要組態頁面
VirtIscsiMacAddr	虛擬 iSCSI 卸載 MAC 位址	主要組態頁面
VirtMacAddr	虛擬 MAC 位址	主要組態頁面
VirtMacAddr[Partition:n]	虛擬 MAC 位址	分割區 n 組態
VirtWWN	虛擬全球節點名稱	主要組態頁面
VirtWWN[Partition:n]	虛擬全球節點名稱	分割區 n 組態
VirtWWPN	虛擬全球連接埠名稱	主要組態頁面
VirtWWPN[Partition:n]	虛擬全球連接埠名稱	分割區 n 組態
全球節點名稱	WWN	主要組態頁面
全球節點名稱	WWN[Partition:n]	分割區 n 組態

FC

表 32. FC 的系統專有屬性

屬性名稱	顯示屬性名稱	群組顯示名稱
VirtualWWN	虛擬全球節點名稱	連接埠組態頁面
VirtualWWPN	虛擬全球連接埠名稱	連接埠組態頁面

B

其他資訊

下列 Dell 技術白皮書可提供更多有關系統設定檔組態範本、屬性和工作流程的資訊，網址是 **delltechcenter.com**：

- *使用伺服器組態設定檔進行伺服器複製*
- *伺服器組態 XML 檔案*
- *組態 XML 工作流程*
- *組態 XML 工作流程指令碼 133*
- *XML 組態檔範例*

C

自訂屬性

表 33. 自訂屬性

FQDD	屬性	OMIVV 自訂
BIOS	Virtualization Technology	一律啟用
iDRAC	重新啟動時收集系統清查資訊	一律啟用
RAID	IncludedPhysicalDiskID	如果 IncludedPhysicalDiskID 值為「自動選取」，則我們會移除該值
RAID	RAIDPDState	已移除
iDRAC	使用者管理員密碼 密碼	只有已啟用 iDRAC 的使用者具備可輸入密碼的「密碼」連結。
PCIeSSD	PCIeSSDSecureErase	永遠停用

D

元件與基準版本比較表

表 34. 元件與基準版本比較表

漂移類型				
硬體	**相關的基準**	**目標元件**	**案例**	**相容性狀態**
	可用	可用	硬體元件符合相關聯的基準。	相容
	可用	可用	元件的硬體屬性不符合相關的基準。	不相容
	無法使用	可用	比較狀態並未計算，予以略過。	相容
	可用	無法使用	相關基準有提供硬體元件，但主機未提供元件或屬性。	不相容
	無法使用	無法使用	比較狀態並未計算，予以略過。	相容
韌體	**相關的基準**	**目標元件**	**案例**	**相容性狀態**
	可用	可用	韌體元件版本符合相關的基準。	相容
	可用	可用	韌體元件版本不符合相關的基準。	不相容
	不可用	可用	相關基準未提供韌體元件版本，但主機有提供元件。 比較狀態並未計算，予以略過。	相容
	可用	無法使用	比較狀態並未計算，予以略過。	相容
	無法使用	無法使用	比較狀態並未計算，予以略過。	相容
驅動程式	**相關的基準**	**目標元件**	**案例**	**相容性狀態**
	可用	可用	驅動程式元件版本符合相關的基準。	相容
	可用	可用	驅動程式元件版本不符合相關的基準。	不相容
	無法使用	可用	比較狀態並未計算，予以略過。	相容
	可用	無法使用	相關基準有提供驅動程式元件版本，但主機有提供元件。	不相容
	無法使用	無法使用	比較狀態並未計算，予以略過。	相容

E

回應代碼

表 35. 回應代碼

回應代碼	說明
200	成功產生/傳回工作資訊或工作清單。
202	成功啟動任何工作。
400	錯誤要求
401	未經授權的要求
404	找不到
409	衝突
500	內部伺服器錯誤
503	服務不可用