

OpenManage Integration for VMware vCenter 5.0 版安裝指南

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。

章 1: 簡介	5
OpenManage Integration for VMware vCenter 授權.....	5
購買軟體授權.....	5
上傳授權後的選項.....	6
強制執行.....	6
重要的參考注意事項.....	6
硬體需求.....	7
設定部署模式.....	7
搭載 Lifecycle Controller 的 BIOS 和 iDRAC 版本.....	8
PowerEdge 伺服器上支援的功能.....	10
PowerEdge 機箱上支援的功能.....	11
已佈建的儲存所需的儲存空間.....	11
軟體需求.....	11
OpenManage Integration for VMware vCenter 需求.....	12
連接埠資訊.....	12
先決條件核對清單.....	14
章 2: 安裝及設定 OMIVV	15
下載 OpenManage Integration for VMware vCenter.....	15
使用 vSphere 用戶端 (HTML-5) 來部署 OMIVV OVF.....	16
設定 OMIVV 裝置.....	17
設定網路時間通訊協定伺服器.....	19
設定擁有兩張網路配接卡的 OMIVV 裝置.....	19
產生憑證簽章要求 (CSR).....	23
上傳 HTTPS 憑證.....	24
還原預設的 HTTPS 憑證.....	24
註冊 OpenManage Integration for VMware vCenter 並匯入授權檔案.....	24
以非管理員使用者身分註冊 vCenter 伺服器.....	26
非管理員使用者必須具備的權限.....	27
將 Dell 權限指派給現有角色.....	28
升級已註冊的 vCenter 版本後重新設定 OMIVV.....	28
驗證安裝.....	28
管理備份和還原.....	29
設定備份和還原.....	29
排程自動備份.....	29
執行立即備份.....	30
從備份還原 OMIVV 資料庫.....	30
重設備份和還原設定.....	30
更新 OMIVV 裝置和儲存庫位置.....	30
使用 RPM 升級 OMIVV 裝置.....	31
升級 VMware 工具.....	31
使用備份和還原來升級 OMIVV 裝置.....	31
取消註冊 OpenManage Integration for VMware vCenter.....	32
取消註冊後還原 OMIVV.....	33

取消註冊舊版 OMIVV 後還原 OMIVV.....	33
管理取消註冊與重新註冊.....	33
章 3: 設定 VMware vCenter 的裝置.....	34
使用初始組態精靈的組態工作.....	34
初始組態.....	34
建立主機認證設定檔.....	35
排程清查工作.....	36
排程保固擷取工作.....	36
設定事件與警報.....	37
「設定」頁面上的組態工作.....	37
設定保固到期通知.....	37
設定最新裝置版本通知.....	38
設定部署認證.....	38
覆寫狀況更新通知的重要性.....	38
章 4: 從 Dell EMC 支援網站存取文件.....	39
章 5: 相關說明文件.....	40

簡介

本指南提供搭配 PowerEdge 伺服器使用時，安裝與設定 OpenManage Integration for VMware vCenter (OMIVV) 的逐步指示。安裝 OMIVV 之後，如需瞭解清查管理、監控與警示、韌體更新、保固管理等各項系統管理層面的更多資訊，請參閱 *OpenManage Integration for VMware vCenter 使用者指南*，網址是：Dell.com/support/manuals。

主題：

- [OpenManage Integration for VMware vCenter 授權](#)
- [重要的參考注意事項](#)
- [硬體需求](#)
- [軟體需求](#)
- [連接埠資訊](#)
- [先決條件核對清單](#)

OpenManage Integration for VMware vCenter 授權

OpenManage Integration for VMware vCenter 有兩種類型的授權：

- **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 OpenManage Integration for VMware vCenter 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 設備更新。

OMIVV 最多可支援 15 個 vCenter。當您將評估授權升級為完整標準授權後，會收到一封確認訂購的電子郵件，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。

授權會提供下列資訊：

- **vCenter 連線授權數上限** — 最多允許註冊及同時使用 15 個 vCenter 連線。
- **主機連線授權上限** — 已購買的主機連線數目。
- **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。

i 註: 標準授權期間僅為三或五年，額外授權會附加至現有授權且無法覆寫。

i 註: 針對 OpenManage Integration for VMware vCenter 所購買的任何授權，若仍在期限內 (自購買後的 3 年或 5 年)，則可用於 5.x 版本。從現有 OMIVV 例項轉移備份的授權，或從 Digital Locker 重新下載的目前的授權，可套用至 5.x 例項。

當您購買授權後，請造訪 [Dell Digital Locker](#)，從 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 [訂單支援頁面](#)，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。

購買軟體授權

在升級到完整產品版本前，您執行的是試用版授權。按一下**購買授權**，瀏覽至 Dell 網站並購買授權。購買後，請使用**管理主控台**上傳授權。

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**。
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。

上傳授權至系統管理入口網站

您可以使用此選項來上傳 OMIVV 主機授權。

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**。
如果授權檔案經修改或編輯，OMIVV 裝置會將檔案視為損毀，授權檔案會無法運作。

上傳授權後的選項

新購買產品的授權檔案

當您下單購買新授權時，Dell 會透過電子郵件發出訂單確認信，接著您可以造訪 [Dell Digital Locker](#)，從 Dell Digital Locker 下載新的授權檔案。授權為 .xml 格式。如果授權是 .zip 格式，請先解壓縮 .zip 檔以取得 .xml 授權檔案，然後再上傳。

堆疊授權

OMIVV 可以堆疊多個標準授權，將支援的主機數目提高至所上傳授權中的主機總數。評估授權無法堆疊。依預設，OMIVV 最多可支援 15 個 vCenter。若要管理 15 個以上的 Vcenter，請使用多個裝置。

如果在現有的標準授權到期前即上傳新的標準授權，則授權會堆疊。如果授權已到期且新授權已上傳，則只有使用新授權的主機數量有受到支援。如果已上傳多個授權，則支援的主機數量會是最後一次上傳授權時，未過期授權中的主機總數。

過期授權

超出支援期限的授權 (通常是從購買日起算 3 或 5 年) 無法上傳。如果授權在上傳後過期，部分功能可能無法運作。也無法升級至新版本的 OMIVV。

更換授權

如果訂單有問題，您會收到 Dell 寄來的更換授權，內含與先前授權相同的權利 ID。當您上傳更換授權時，先前使用相同權利 ID 上傳的授權即會遭到更換。

強制執行

裝置更新

所有授權均已過期時，裝置不允許更新至較新的版本。請取得新的授權並上傳，再嘗試升級裝置。

評估授權

評估授權到期時，有幾個關鍵區域會停止運作，也會因此顯示錯誤訊息。

將主機新增到主機認證設定檔

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。

重要的參考注意事項

- 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)。
- 若要使用 DNS 伺服器，建議您採用以下作法：

- OMIVV 僅支援 IPv4 的 IP 位址。雖然靜態 IP 位址指派與 DHCP 指派皆受到支援，Dell EMC 建議您指派靜態 IP 位址。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 主機名稱項目出現在 DNS 伺服器的正向與反向查閱區域中。

如需更多有關 vSphere 之 DNS 需求的資訊，請參閱以下的 VMware 連結：

- [vSphere 6.5 與平台服務控制器裝置的 DNS 需求](#)
- [vSphere 6.7 與 Windows 上的平台服務控制器的 DNS 要求](#)
- 如果是 OMIVV 裝置模式，請務必根據您的虛擬化環境，採用適當的模式來部署 OMIVV。如需更多資訊，請參閱 [設定部署模式](#) 第頁的 7。
- 請配合連接埠需求來設定您的網路。如需更多資訊，請參閱 [連接埠資訊](#) 第頁的 12。
- Dell EMC 建議使用 Google Chrome 存取 OMIVV 功能。OMIVV 支援 Google Chrome 和 Mozilla Firefox。不支援 Microsoft Internet Explorer。

硬體需求

OMIVV 能夠為數代 Dell EMC 伺服器提供完整支援，對於搭載 iDRAC Express 或 Enterprise 的伺服器提供完整功能支援。若要確認您的主機伺服器符合資格，請參閱後續小節中的下列相關資訊：

- [支援的伺服器和 BIOS 下限](#)
- [支援 iDRAC 的版本 \(部署和管理\)](#)
- [OMIVV 支援的記憶體、CPU 和儲存空間](#)

主機板或網路子卡上必須具有 LAN，OMIVV 才能存取 iDRAC 和 CMC 兩者的管理網路，或是 OME-Modular 系統管理網路與 vCenter 管理網路。如需更多詳細資訊，請參閱 [設定 OMIVV 裝置](#) 第頁的 17 和 [設定擁有兩張網路配接卡的 OMIVV 裝置](#) 第頁的 19。

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 1. 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。

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**。系統會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，而且會發生下列一項或多項事件：
 - 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。

i 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。若要啟動 OMIVV 裝置，請關閉 OMIVV 裝置，將系統資源更新至現有的設定部署模式，並完成降級部署模式工作。

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。

搭載 Lifecycle Controller 的 BIOS 和 iDRAC 版本

需要搭載 Lifecycle Controller 的 BIOS 和 iDRAC 版本以啟用 OpenManage Integration for VMware vCenter 的功能。

Dell EMC 建議您使用以 Repository Manager 或 Lifecycle Controller 的平台建立的可開機 ISO 來更新伺服器至以下其中一個基底版本，然後再使用 OMIVV：

表 2. 適用於 PowerEdge 伺服器的受支援 BIOS 版本

伺服器	最低版本
T320	1.0.1 或更新版本
T420	1.0.1 或更新版本
T620	1.2.6 或更新版本
M420	1.2.4 或更新版本
M520	1.2.6 或更新版本
M620	1.2.6 或更新版本
M820	1.2.6 或更新版本
R220	1.0.3 或更新版本
R320	1.2.4 或更新版本
R420	1.2.4 或更新版本
R520	1.2.4 或更新版本
R620	1.2.6 或更新版本
R720	1.2.6 或更新版本
R720xd	1.2.6 或更新版本
R820	1.7.2 或更新版本
R920	1.1.0 或更新版本
R630	1.0.4 或更新版本
R730	1.0.4 或更新版本
R730xd	1.0.4 或更新版本
R430	1.0.4 或更新版本
R530	1.0.2 或更新版本
R830	1.0.2 或更新版本
R930	1.0.2 或更新版本
R230	1.0.2 或更新版本

表 2. 適用於 PowerEdge 伺服器的受支援 BIOS 版本

伺服器	最低版本
R330	1.0.2 或更新版本
T630	1.0.2 或更新版本
T130	1.0.2 或更新版本
T330	1.0.2 或更新版本
T430	1.0.2 或更新版本
M630	1.0.0 或更新版本
M830	1.0.0 或更新版本
FC430	1.0.0 或更新版本
FC630	1.0.0 或更新版本
FC830	1.0.0 或更新版本
R240	1.0.0 或更新版本
R340	1.0.0 或更新版本
R940	1.0.0 或更新版本
R940xa	1.0.0 或更新版本
R740	1.0.0 或更新版本
R740xd	1.0.0 或更新版本
R740xd2	1.0.0 或更新版本
R640	1.0.0 或更新版本
R840	1.0.0 或更新版本
R440	1.0.0 或更新版本
M640	1.0.0 或更新版本
T140	1.0.0 或更新版本
T340	1.0.0 或更新版本
T640	1.0.0 或更新版本
T440	1.0.0 或更新版本
R540	1.0.0 或更新版本
FC640	1.0.0 或更新版本
R6415	1.0.0 或更新版本
R7425	1.0.0 或更新版本
R7415	1.0.0 或更新版本
MX740C	1.0.0 或更新版本
MX840C	1.0.0 或更新版本
R6515	1.0.3 或更新版本
R7515	1.0.3 或更新版本
R6525	1.0.0 或更新版本

表 3. 適用於部署的受支援 iDRAC 和 Lifecycle Controller

表 3. 適用於部署的受支援 iDRAC 和 Lifecycle Controller

代	iDRAC 與 Lifecycle Controller
PowerEdge 第 12 代伺服器	2.50.50.50 或更新版本
PowerEdge 第 13 代伺服器	2.50.50.50 或更新版本
PowerEdge 第 14 代伺服器	3.00.00.00 和更新版本

表 4. 雲端伺服器的 BIOS 和 iDRAC 需求

Model	BIOS	iDRAC 與 Lifecycle Controller
C6320	1.0.2	2.50.50.50 或更新版本
C4130	1.0.2	2.50.50.50 或更新版本
C6420	1.0.0 或更新版本	3.00.00.00 或更新版本
C4140	1.0.0 或更新版本	3.00.00.00 或更新版本
C6525	1.0.0 或更新版本	3.42.42.42 或更新版本

PowerEdge 伺服器上支援的功能

由 OpenManage Integration for VMware vCenter 管理的主機支援下列功能：

表 5. PowerEdge 伺服器上支援的功能

功能	平台	
	12G 和 13G	14G
硬體清單	Y	Y
事件與警示	Y (SNMP v1 和 v2)	Y (SNMP v1 和 v2)
元件智慧健全狀況監控*	Y	Y
BIOS/韌體更新#	Y	Y
主動式 HA [§]	Y	Y
保固資訊	Y	Y
管理相容性	Y	Y
組態相容性	Y	Y
裸機伺服器的自動/手動探索	Y	Y
裸機相容性	Y	Y
硬體設定	Y	Y
作業系統部署	Y	Y
閃爍伺服器 LED	Y	Y
檢視/清除 SEL 記錄	Y	Y
連結並啟動 iDRAC	Y	Y
重設 iDRAC	Y	Y
系統鎖定模式	N	Y
系統設定檔	Y	Y
叢集設定檔	Y	Y
使用整合機箱 IP 來管理主機	N	Y [®]

表 5. PowerEdge 伺服器上支援的功能

功能	平台	
支援 OEM 伺服器	Y~	Y

* 使用型號 C6320 連接至雲端時，健全狀況監控不支援夾層卡。

使用型號 C6320 連接至雲端時，韌體更新不支援夾層卡。

\$ 主動式 HA 功能僅適用於備有 ESXi 6.0 或更新版本的 vCenter 6.5 或更新版本。此外，主動式 HA 功能在具有內嵌 PSU 及雲端伺服器機型的伺服器上不受支援。

@ 僅適用於 MX 機箱主機。清查、監控、主動式 HA 和韌體更新功能都有支援。

~ 僅支援機架式伺服器。

PowerEdge 機箱上支援的功能

本主題提供 PowerEdge 機箱上所支援之功能的相關資訊。

表 6. 模組化基礎架構上支援的功能

功能	M1000e	VRTX	FX2s	MX
SNMP 警示	Y	Y	Y	Y
硬體清單	Y	Y	Y	Y
連結並啟動 CMC 或管理模組	Y	Y	Y	Y
授權資訊	N/A	Y	Y	Y
保固資訊	Y	Y	Y	Y
健全狀況報告	Y	Y	Y	Y
多機箱管理群組關係資訊	N	N	N	Y
韌體更新	N	N	N	Y

已佈建的儲存所需的儲存空間

OMIVV 虛擬裝置至少需要 95 GB 的磁碟空間來佈建儲存。

預設虛擬應用裝置組態

OMIVV 虛擬應用裝置是以 8 GB 的 RAM 和兩個虛擬 CPU (小型部署模式) 加以佈建。

軟體需求

確認 vSphere 環境符合虛擬裝置系統要求、連接埠存取、時鐘同步，和聆聽連接埠的要求。

VMware vSphere 用戶端 (HTML-5) 的需求

vCenter 6.5 及更新版本

OpenManage Integration for VMware vCenter 需求

受管主機上安裝支援的 ESXi 版本

下表提供在受管理主機上支援之 ESXi 版本的相關資訊：

表 7. 支援的 ESXi 版本

ESXi 版本	伺服器世代		
	YX2X	YX3X	YX4X
6.0 U3	Y	Y	N
6.5	Y	Y	N
6.5 U1	Y	Y	Y
6.5 U2	Y	Y	Y
6.5 U3	Y	Y	Y
6、7	N	Y	Y
6.7 U1	N	Y	Y
6.7 U2	N	Y	Y
6.7 U3	N	Y	Y

i 註：PowerEdge MX 主機只有在與 ESXi 6.5 U2 和以上版本搭配使用時，才會受到支援。

OpenManage Integration for VMware vCenter 可支援下列任一 vCenter 伺服器版本：

表 8. 支援的 vCenter 伺服器版本

vCenter 版本	用戶端支援
6.5 U2	Y
6.5 U3	Y
6、7	Y
6.7 U1	Y
6.7 U2	Y
6.7 U3	Y

OpenManage Integration for VMware vCenter 5.0 版支援 VMware vRealize Operations Manager (vROPS) 2.0 版。

OMIVV 5.0 裝置支援 CentOS 7.6.1810。

連接埠資訊

本節列出設定虛擬裝置和受管節點的所有連接埠需求。

表 9. 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。

表 9. 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
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。
80	HTTP	TCP	無	輸入	ESXi 伺服器至 OMIVV 裝置	HTTP 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。
162	SNMP 代理程式	UDP	無	輸入	iDRAC/ESXi 至 OMIVV 裝置	SNMP 代理程式 (伺服器)	接收來自受管節點的 SNMP 陷阱。
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	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	SMB	TCP	128 位元	輸出	OMIVV 裝置至 CIFS	CIFS 通訊	與 Windows 共用通訊。
4433	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。
2049	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。
11620	SNMP 代理程式	UDP	無	輸入	iDRAC 至 OMIVV 裝置	SNMP 代理程式 (伺服器)	使用 UDP: 162 來接收標準 SNMP 警示的連接埠。會接收來自 iDRAC 和 CMC 或 OME-Modular 的資料，以便管理和監控受管節點。
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 10. 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
162,11620	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。

表 11. 受管節點 (iDRAC 或 CMC 或 OME-Modular)

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
443	WSMAN/HTTPS,	TCP	128 位元	輸入	OMIVV 裝置到 iDRAC 或	iDRAC 通訊	用來提供資訊給管理站，以及使用 REST 或 HTTPS 通訊協定與 MX 機箱通

表 11. 受管節點 (iDRAC 或 CMC 或 OME-Modular) (續)

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
	REST/ HTTPS				CMC 或 OME- Modular		訊。此連接埠必須從 iDRAC 和 CMC 或 OME-Modular 開啟。
4433	HTTPS	TCP	128 位元	輸出	iDRAC 至 OMIVV 裝置	自動探索	可自動探索管理站中的 iDRAC (受管節點)。
2049	NFS	UDP	無	輸入/輸出	iDRAC 至/從 OMIVV	公用共用	可讓 iDRAC 存取由 OMIVV 裝置公開的 NFS 公用共用。其用於作業系統部署和韌體更新。 用來從 OMIVV 存取 iDRAC 組態。用於部署流程。
4001 至 4004	NFS	UDP	無	輸入/輸出	iDRAC 至/從 OMIVV	公用共用	可讓 iDRAC 存取由 OMIVV 裝置公開的 NFS 公用共用。其用於作業系統部署和韌體更新。 用來從 OMIVV 存取 iDRAC 組態。用於部署流程。
69	TFTP	UDP	128 位元	輸入/輸出	iDRAC 至/從 OMIVV	簡單式檔案 傳輸	用於從管理站順利管理 iDRAC。

先決條件核對清單

開始安裝產品前，請先確定以下事項：

- 您擁有可讓 OMIVV 存取 vCenter 伺服器的使用者名稱和密碼。使用者可以擁有具備所有必要權限的管理員角色，或是具備必要權限的非管理員使用者。如需 OMIVV 作業所需權限清單的更多資訊，請參閱[非系統管理員使用者必要權限](#)。
- 您具有 ESXi 主機系統的根密碼，或是有主機系統管理權限的 Active Directory 認證。
- 您擁有與 iDRAC Express 或 Enterprise 相關的使用者名稱和密碼，且其在 iDRAC 上有系統管理權限。
- vCenter 伺服器正在執行中。
- 決定 OMIVV 安裝目錄的位置。
- OMIVV 和 vCenter 伺服器置於同個網路。
- 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。這只適用於 OMIVV 裝置未設定兩個網路配接卡的情況。
- VMware vSphere 環境符合虛擬裝置系統需求、連接埠存取、時鐘同步，和聆聽連接埠的要求。

i 註：虛擬應用裝置的作用和一般虛擬機器相同；凡是中斷或關機，都會影響虛擬應用裝置的整體功能。

i 註：當 OMIVV 部署在 ESXi 5.5 及更新版本上時，會顯示 VMware 工具在執行中 (過期)。如有需要，您可在成功部署 OMIVV 裝置後或稍後的任何時間升級 VMware 工具。

安裝及設定 OMIVV

請務必遵照硬體需求，並且執行所需的 VMware vCenter。

以下高階步驟大概就是 OMIVV 的整體安裝和設定程序：

1. 從 Dell 支援網站下載 *DellEMC_OpenManage_Integration_<version number>.<build number>.zip* 檔案 (網址為：Dell.com/support)。如需更多有關下載 OMIVV 的資訊，請參閱[下載 OpenManage Integration for VMware vCenter](#) 第頁的 15。
2. 瀏覽至您已下載檔案的位置，然後解壓縮其內容。
3. 使用 vSphere 用戶端 (HTML-5) 來部署包含 OMIVV 裝置的開放虛擬化格式 (OVF) 檔案。請參閱 [部署 OMIVV OVF](#)。
4. 部署 OVF 後，請設定時區、目前日期和時間。
5. 上傳授權檔案。如需更多有關授權的資訊，請參閱 [上傳授權至系統管理入口網站](#) 第頁的 5。
6. 視需求設定部署模式。如需更多資訊，請參閱[設定部署模式](#) 第頁的 7。
7. 用管理主控台向 vCenter 伺服器登錄 OMIVV 裝置。請參閱[登錄 OMIVV 與匯入授權檔案](#)。
8. 完成**初始組態精靈**來設定裝置。請參閱[透過組態精靈執行的組態工作](#)。

主題：

- [下載 OpenManage Integration for VMware vCenter](#)
- [使用 vSphere 用戶端 \(HTML-5\) 來部署 OMIVV OVF](#)
- [設定 OMIVV 裝置](#)
- [設定網路時間通訊協定伺服器](#)
- [設定擁有兩張網路配接卡的 OMIVV 裝置](#)
- [產生憑證簽章要求 \(CSR\)](#)
- [上傳 HTTPS 憑證](#)
- [註冊 OpenManage Integration for VMware vCenter 並匯入授權檔案](#)
- [以非管理員使用者身分註冊 vCenter 伺服器](#)
- [升級已註冊的 vCenter 版本後重新設定 OMIVV](#)
- [驗證安裝](#)
- [管理備份和還原](#)
- [更新 OMIVV 裝置和儲存庫位置](#)
- [使用 RPM 升級 OMIVV 裝置](#)
- [使用備份和還原來升級 OMIVV 裝置](#)
- [取消註冊 OpenManage Integration for VMware vCenter](#)
- [取消註冊後還原 OMIVV](#)

下載 OpenManage Integration for VMware vCenter

請妥善保管 Dell EMC PowerEdge 伺服器的服務標籤。建議您使用服務標籤來存取 Dell 支援網站上所有的支援。這樣可確保您下載適合您平台的軟體版本。

下載 OMIVV：

1. 前往 <https://www.dell.com/support>。
2. 執行下列其中一個動作：
 - 輸入 Dell EMC PowerEdge 伺服器的服務標籤，然後選取搜尋。
 - 選取**瀏覽所有產品 > 伺服器 > PowerEdge**。
3. 選取適當型號的 PowerEdge 伺服器。
4. 在伺服器的支援網頁上，選取 **驅動程式與下載**。
5. 從**作業系統**清單中，選取適當版本的 VMware ESXi。
6. 從**類別**清單中，選取**系統管理**。
隨後便會出現支援的 OMIVV 版本。

7. 按**下載**或**選取核取方塊**，將軟體加入您的下載清單中。

使用 vSphere 用戶端 (HTML-5) 來部署 OMIVV OVF

請務必先從支援網站下載並解壓縮產品 zip 檔案 *DellEMC_OpenManage_Integration_<version number>.<build number>.zip*。

註: 只有在使用 vSphere 用戶端 (HTML-5) 時，才會建議執行下列工作。如果您使用的是 Web 用戶端，則步驟可能有所不同。

1. 前往 OMIVV 的下載位置，然後按兩下 **DellEMC_OpenManage_Integration.exe** 來解壓縮檔案。
解壓縮和執行 exe 檔案所使用的支援用戶端作業系統版本是 Windows 7 SP1 及更新版本。
解壓縮和執行 exe 檔案所使用的支援伺服器作業系統版本是 Windows 2008 R2 及更新版本。

2. 接受 **EULA**，然後儲存 .ovf 檔案。
3. 將 .ovf 檔案複製或移動到 VMware vSphere 主機 (上傳裝置的目的地) 能夠存取的位置。
4. 啟動 **VMware vSphere 用戶端 (HTML-5)**。
5. 在 **VMware vSphere 用戶端** 選取主機，然後在主功能表中按一下 **動作 > 部署 OVF 範本**。
您也可以用滑鼠右鍵按一下 **主機**，然後選取 **部署 OVF 範本**。

部署 OVF 範本精靈隨即顯示。

6. 在 **選取 OVF 範本** 視窗中執行下列操作：

- a. 若要從網際網路下載 OVF 套件，請選取 **URL**。
- b. 如果要從本機系統選取 OVF 套件，請選取 **本機檔案**，然後按一下 **選擇檔案**。
- c. 按一下 **下一步**。
隨後便會出現 **選取名稱和資料夾** 視窗。

註: 如果 OVF 套件儲存在網路分享區，則安裝程序可能需要 10 到 30 分鐘。若要快速安裝，Dell EMC 建議您在本機磁碟控管 OVF。

7. 在 **選取名稱和資料夾** 視窗中，執行以下操作：

- a. 在 **虛擬機器名稱** 欄位中輸入範本名稱。名稱最多可包含 80 個字元。
- b. 從 **選取虛擬機器位置** 清單中，選取要部署範本的位置。
- c. 按一下 **下一步**。
隨即顯示 **選取運算資源** 視窗。

8. 從 **選取運算資源** 清單中選取目的地運算資源，然後按一下 **下一步**。
隨後便會出現 **檢閱詳細資料** 視窗，顯示以下資訊：

- **發行者**—發行者資料
- **下載大小**—OVF 範本的實際大小 (以 GB 為單位)
- **磁碟大小**—複雜與精簡佈建的相關資訊

9. 按一下 **下一步**。
選取儲存裝置 視窗隨即顯示。

10. 在 **選取儲存裝置** 視窗中執行以下操作：

- a. 從 **選取虛擬磁碟格式** 下拉式清單中，選取下列其中一種格式：
 - **Thick Provision (Lazy Zeroed)**
 - **Thick Provision (Eager zeroed)**
 - **Thin Provision**建議您選取 **Thick Provision (Eager Zeroed)**。

- b. 從 **虛擬機器儲存原則** 下拉式清單中選取一個原則。

- c. 按一下 **下一步**。
選取網路 視窗即會顯示來源和目的地網路的相關資訊。

11. 在 **選取網路** 視窗中選取每個來源網路的目的地網路，然後按一下 **下一步**。

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) 和頻外網路兩者的存取權 (iDRAC、CMC 和 Dell EMC OpenManage Enterprise Modular (OME-Modular))。

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。如果您能使用 vSphere 網路存取頻外網路，請勿為 OMIVV 裝置設定網路配接卡。如需設定兩張網路配接卡的更多資訊，請參閱 [設定擁有兩張網路配接卡的 OMIVV 裝置](#) 第 19 頁。

- 頻外網路—iDRAC、CMC 與 OME-Modular 所連接的管理網路。
 - vSphere 網路—ESXi 主機、vCenter 以及 PSC 所連接的管理網路。
12. 在**準備好完成**視窗中，檢查針對 OVF 部署工作選取的選項，然後按一下**完成**。部署工作即會執行並顯示完成狀態，供您追蹤該等工作的完成狀態。
 13. 開啟虛擬機器的電源。

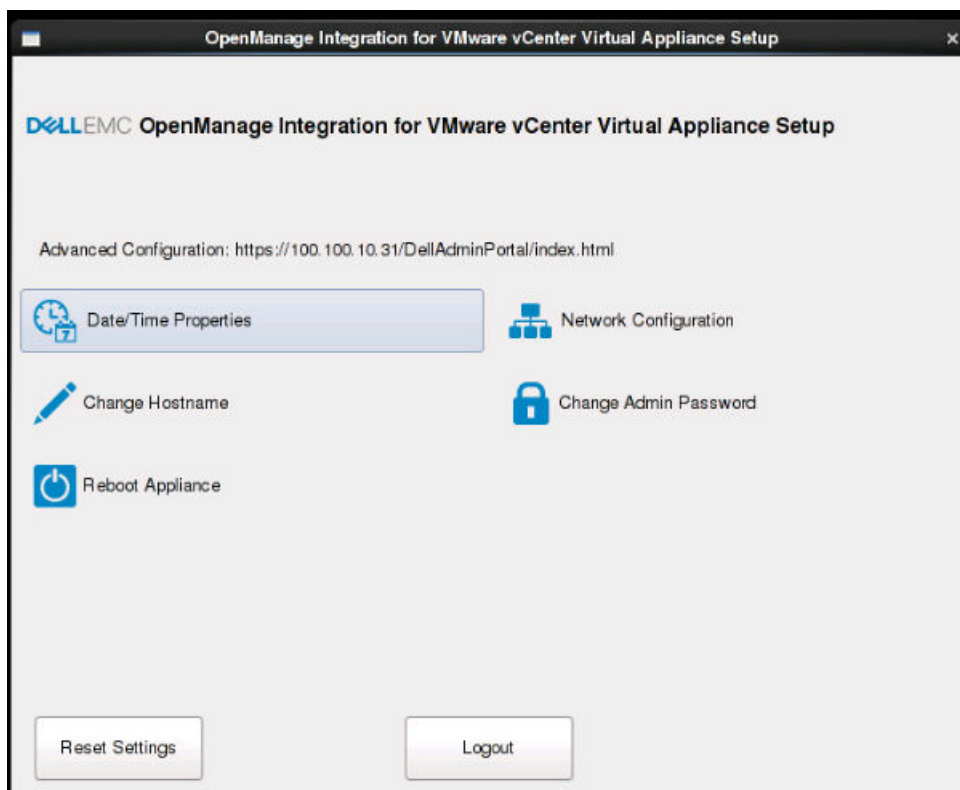
註：部署 OVF 後，您必須強制設定當前日期和時間才能註冊至 OMIVV。

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。

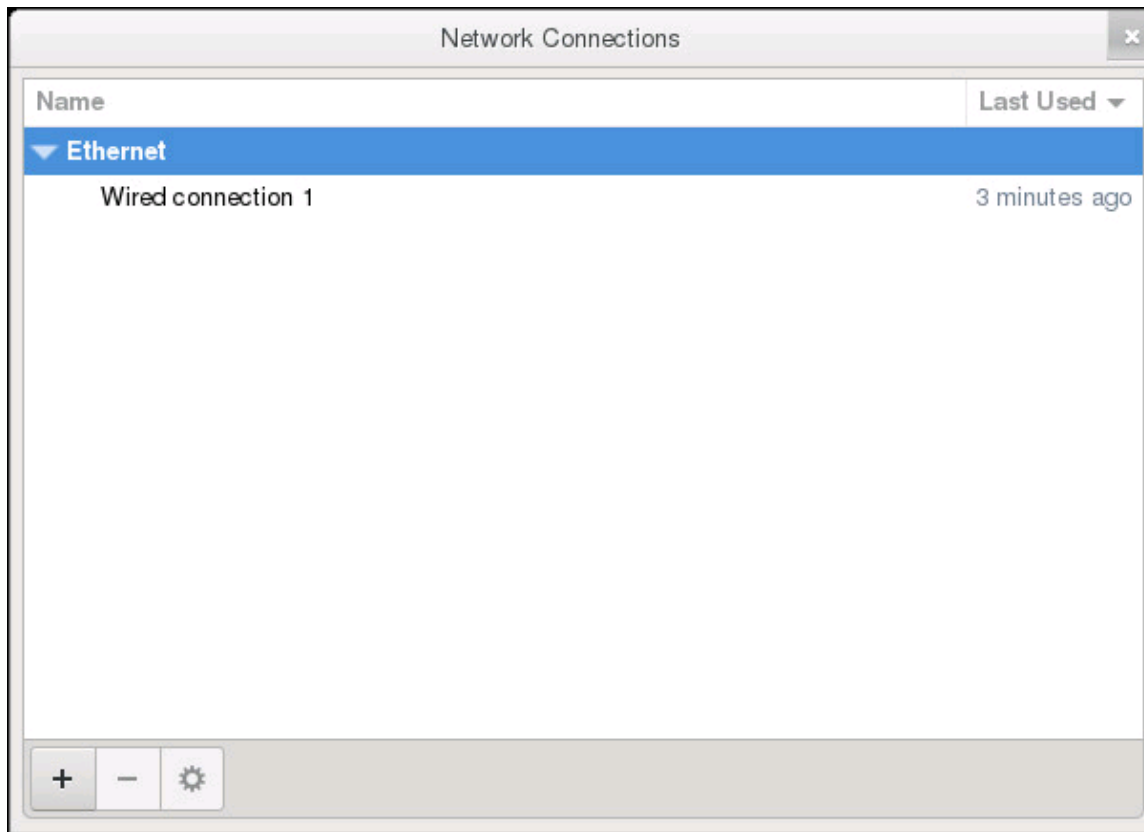
- a. 在**日期與時間**索引標籤上，選取**透過網路同步處理日期與時間**核取方塊。**透過網路同步處理日期與時間**核取方塊僅會於成功使用系統管理入口網站設定 NTP 後才會啟用。如需更多有關設定 NTP 的資訊，請參閱**設定網路時間通訊協定伺服器** 第頁的 19。
 - b. 按一下**時區**，選取適用的時區，然後按一下**確定**。
6. 如要設定 OMIVV 裝置的網路，按一下**網路組態**。


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。

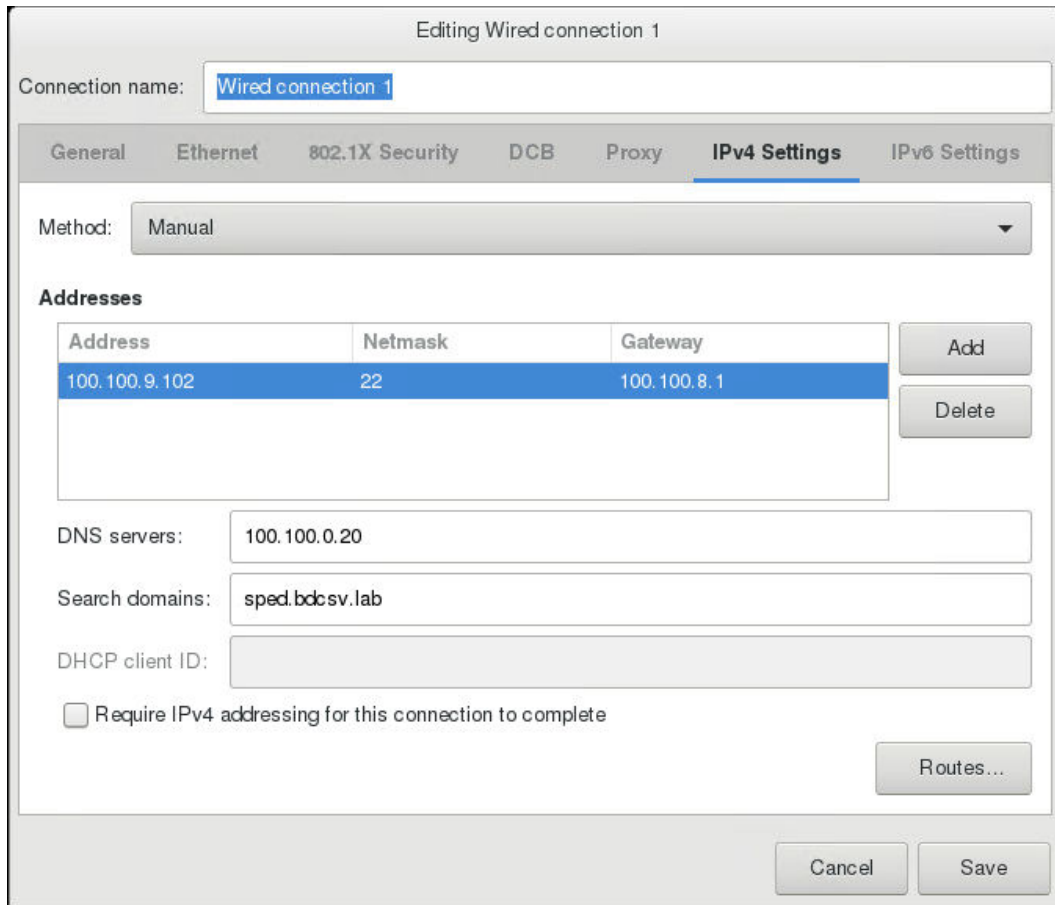
如果環境中的 vSphere 網路和頻外網路是獨立的隔離網路，OMIVV 便需要這兩個網路的存取權。在此情況下，OMIVV 裝置必須設定兩張網路配接卡。Dell EMC 建議將這兩個網路設定為初始組態的一部分。

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 [設定擁有兩張網路配接卡的 OMIVV 裝置](#) 第頁的 19。

7. 選取**有線連線 1**，然後按一下 。



- 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。
- 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。
- 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。
- 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 執行個體，然後再重新註冊。如需更多資訊，請參閱[管理取消註冊與重新註冊](#) 第頁的 33。

9. 重新啟動設備。

設定網路時間通訊協定伺服器

您可以使用網路時間通訊協定 (NTP) 來同步處理 OMIVV 裝置時鐘和 NTP 伺服器時鐘。

1. 在**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。

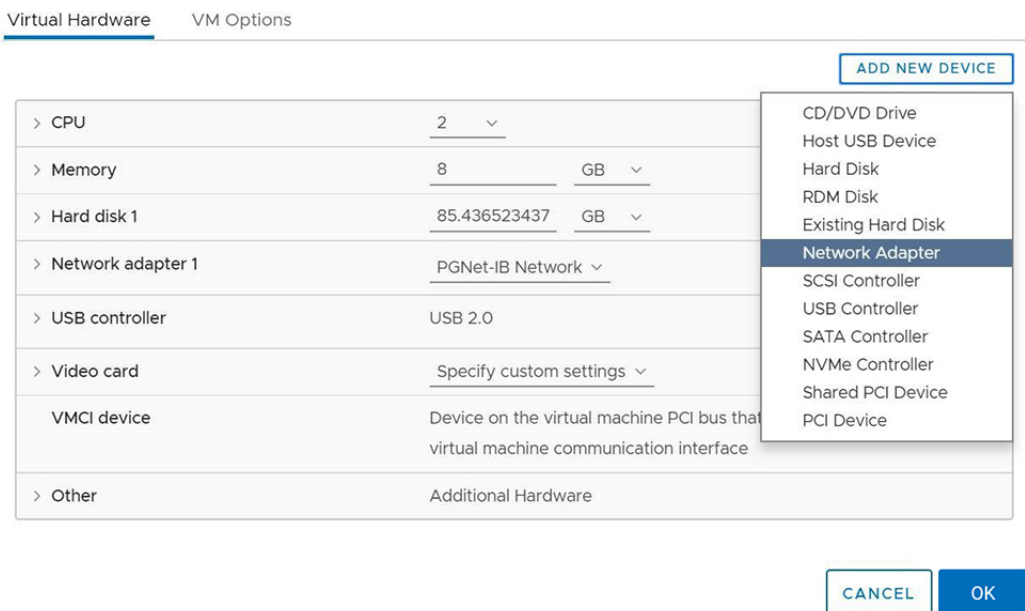
註: 可能需花費 10 分鐘，才可完成 OMIVV 時鐘與 NTP 伺服器同步化。

設定擁有兩張網路配接卡的 OMIVV 裝置

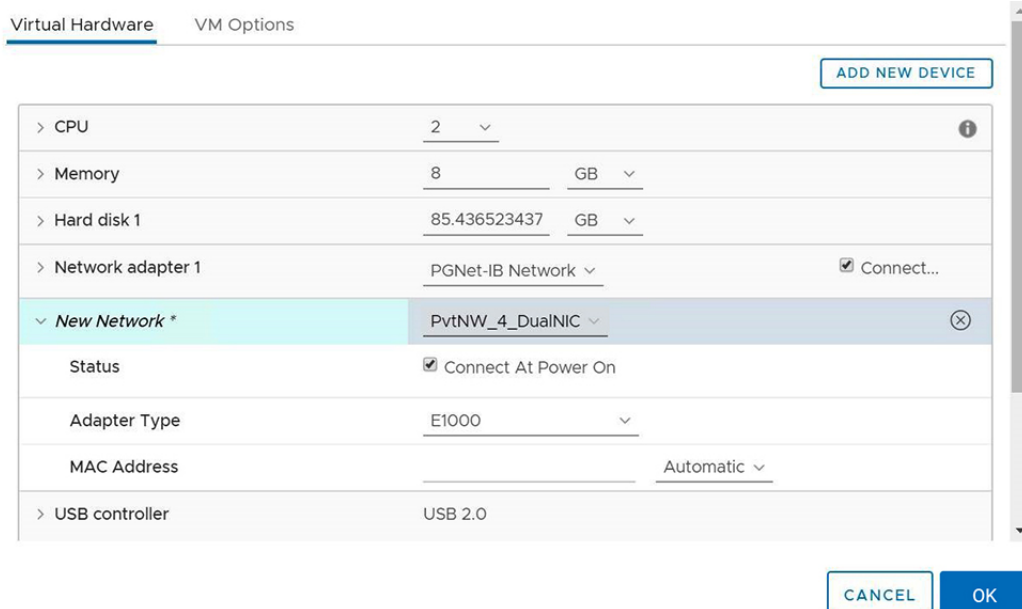
若要在 vSphere 環境中管理 Dell EMC 伺服器，OMIVV 需要 vSphere 網路 (vCenter 和 ESXi 管理網路) 和頻外網路 (iDRAC、CMC 和 OME-Modular) 兩者的存取權。如果環境中的 vSphere 網路和頻外網路是獨立的隔離網路，OMIVV 便需要這兩個網路的存取權。在此情況下，OMIVV 裝置必須設定兩張網路配接卡。若能使用 vSphere 網路存取頻外網路，請勿為 OMIVV 裝置設定兩張網路配接卡。

請確定您已為頻外網路及 vSphere 網路備妥下列資訊：

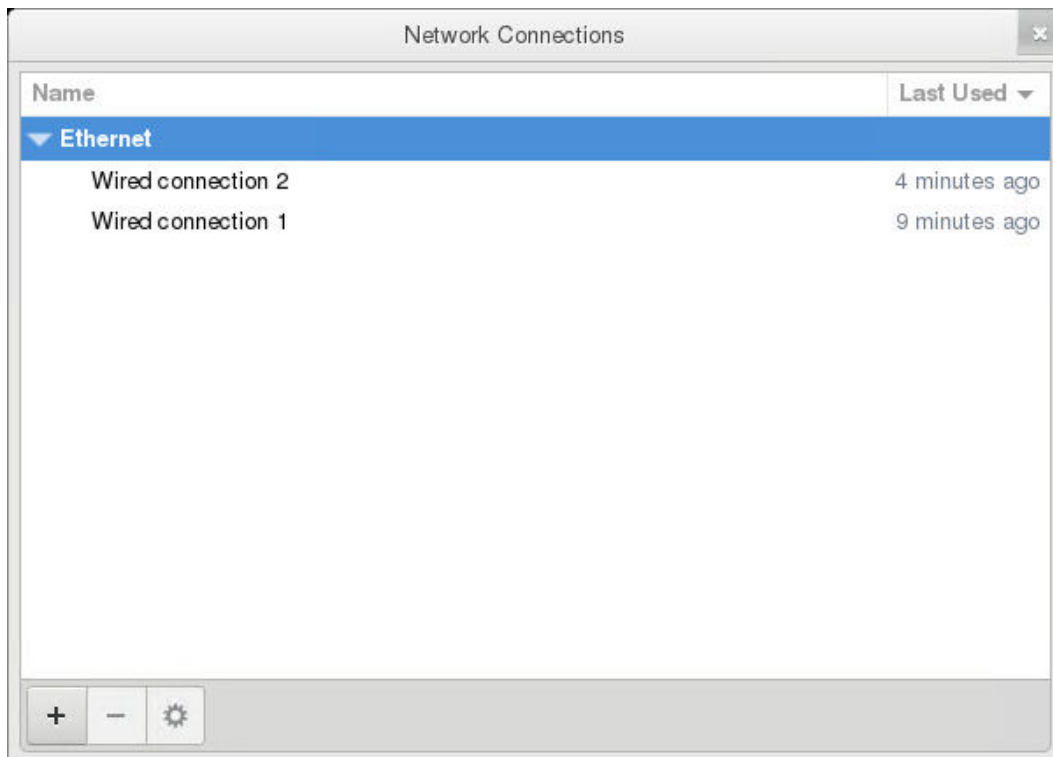
- IP 位址、網路遮罩 (CIDR 格式)，以及裝置的閘道 (若為靜態)
 - 預設閘道—必須將預設閘道設定為擁有網際網路連線的唯一網路。建議將 vSphere 網路作為預設閘道。
 - 路由要求 (網路 IP、網路遮罩和閘道)—對於無法直接連接或使用預設閘道連接的外部網路，設定靜態路由。
 - DNS 要求—OMIVV 僅針對單一網路支援 DNS 組態。如需更多 DNS 組態的相關資訊，請移至本主題的步驟 9 (b)。
1. 將 OMIVV 裝置關機。
 2. 使用 vSphere 用戶端 (HTML-5) 編輯虛擬機器設定，並新增額外的網路配接卡。若要編輯虛擬機器設定，以右鍵按一下虛擬機器，再按一下 **編輯設定**。
 3. 按一下 **新增裝置**，選取 **網路配接卡**。





- a. 為網路配接卡選取適當的網路，然後選取 **開機時連線** 核取方塊。
- b. 從下拉式功能表中選取 **E1000** 配接卡類型。OMIVV 僅支援 E1000 類型的網路配接卡。

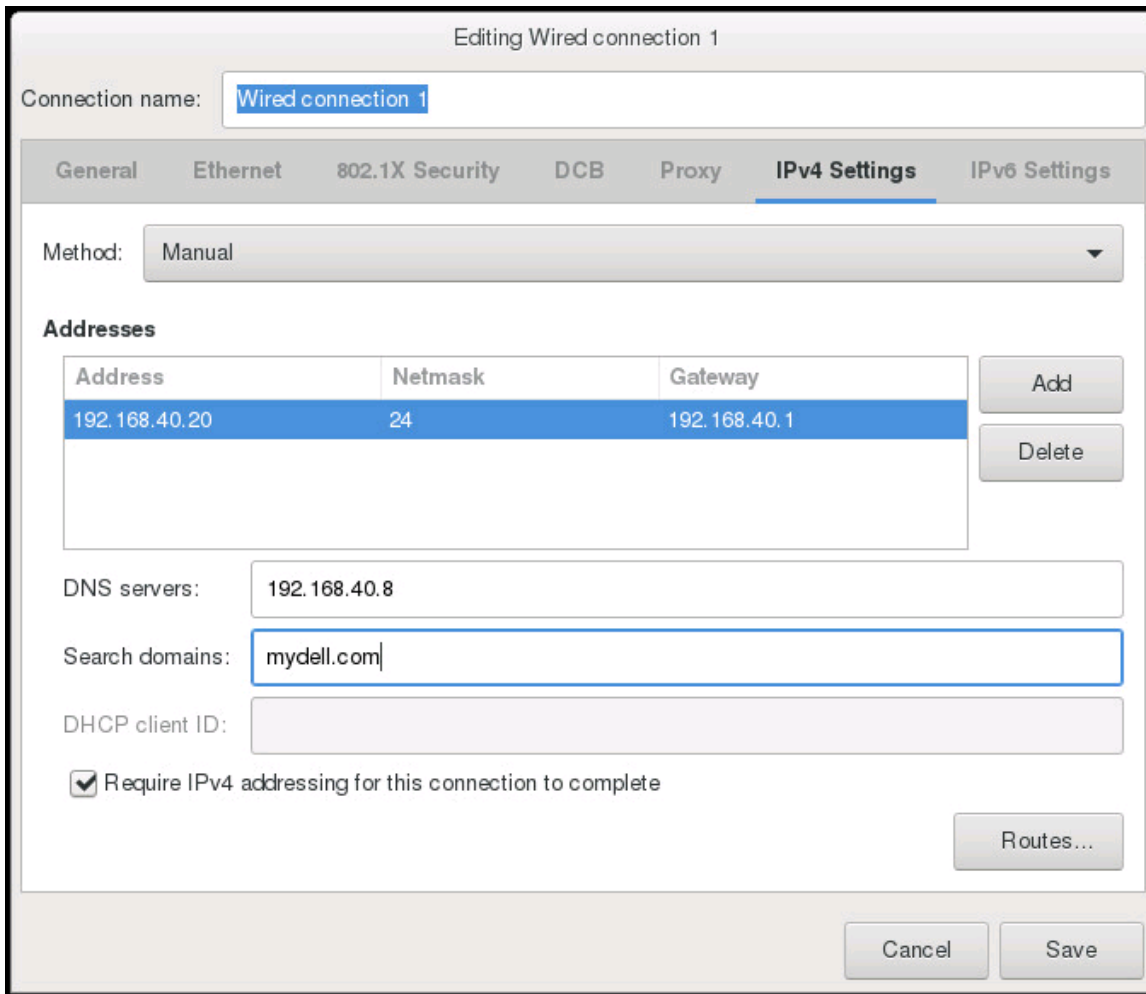


4. 開啟虛擬機器的電源。以系統管理員身分登入 (預設的使用者名稱為 Admin)，然後按下 **Enter**。
5. 在 **OpenManage Integration for VMware vCenter 虛擬裝置設定公用程式** 中，選取 **網路組態**。**網路連線** 頁面會顯示兩個 NIC。

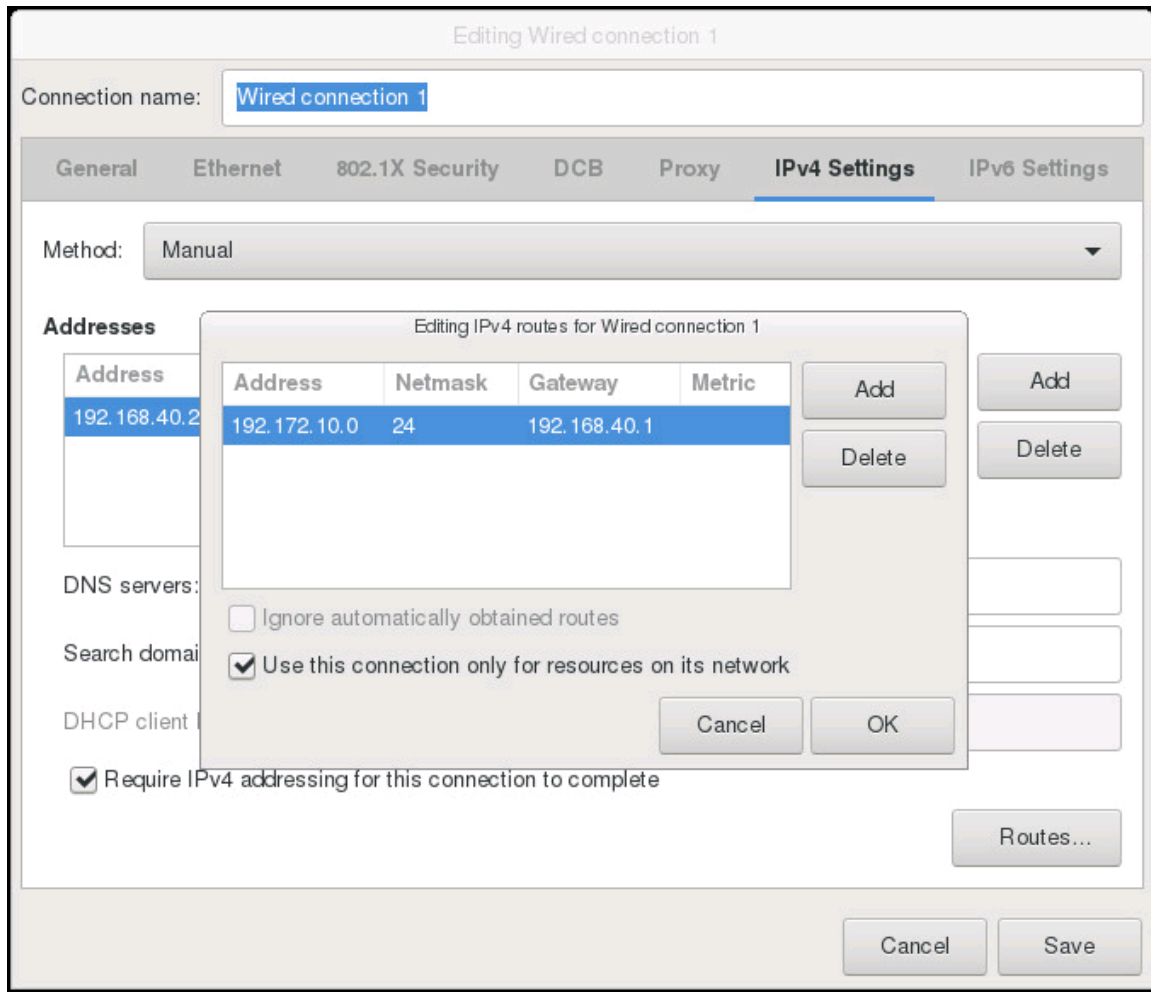


 **警告:** 請勿使用「+」來新增任何新的網路介面。務必使用 vSphere「編輯設定」來新增網路配接卡。

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，Dell EMC 建議您僅針對 vSphere 網路來設妥 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。



您已設定為預設開道的網路通常不需要任何手動路由組態，因為開道有能力提供連線。但是，若網路未設定預設開道（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。因為預設開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。

註:

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。

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**。

註: 如果要上傳自訂 CSR 至 OMIVV，請務必先上傳新憑證，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 (HTML-5) 上會顯示通訊錯誤。若要解決這個問題，請先取消註冊，然後向 vCenter 重新註冊裝置。如需更多資訊，請參閱[管理取消註冊與重新註冊](#) 第頁的 33。

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**。

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。

註冊 OpenManage Integration for VMware vCenter 並匯入授權檔案

請確定您的授權可從 [Dell Digital Locker](#) 下載。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。授權檔案為 .XML 格式。

註: 如果要上傳裝置的自訂憑證，請務必先上傳新憑證，再向 vCenter 註冊。如果在 vCenter 註冊後上傳新的自訂憑證，vSphere 用戶端 (HTML-5) 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。如需更多資訊，請參閱[管理取消註冊與重新註冊](#) 第頁的 33。

1. 由支援的瀏覽器開啟**管理主控台**。

若要開啟**系統管理主控台**，請啟動網頁瀏覽器，然後輸入 `https://<裝置 IP 或裝置主機名稱或 FQDN>`。

IP 位址是指裝置 VM 的 IP 位址，而不是 ESXi 主機 IP 位址。使用主控台上方顯示的 URL 即可存取 [Administration Console]。

例如：`Https://10.210.126.120` 或 `Https://myesxihost`

URL 沒有大小寫區分。

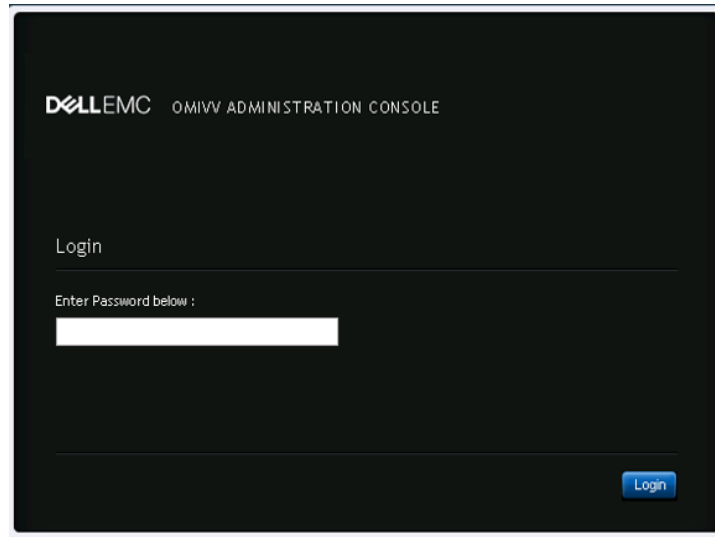


圖 1. 管理主控台

2. 在管理主控台登入視窗中輸入密碼，然後按一下**登入**。

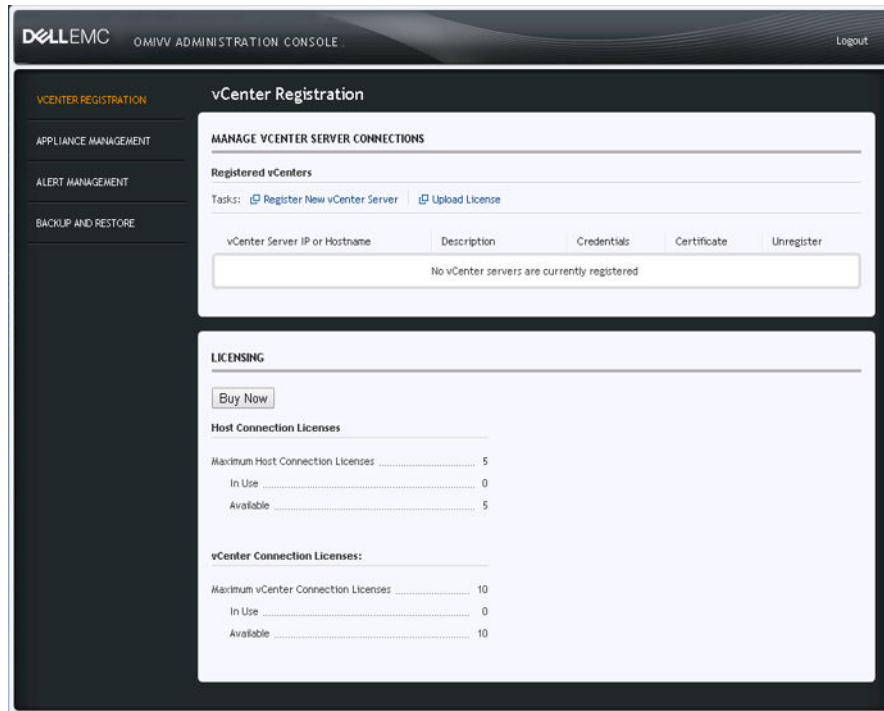


圖 2. 管理主控台的 vCenter 註冊視窗

3. 在 **vCenter** 註冊視窗中，按一下**註冊新的 vCenter 伺服器**。
4. 在註冊新的 **vCenter 伺服器**視窗中，執行以下子步驟：
 - a. 在 **vCenter** 名稱底下的 **vCenter 伺服器 IP 或主機名稱**文字方塊中，輸入伺服器 IP 或 FQDN，然後在**說明**文字方塊中輸入說明。說明是選填欄位。

註：建議使用完整網域名稱 (FQDN)，向 VMware vCenter 註冊 OpenManage Integration for VMware vCenter。如果是以 FQDN 為基礎的註冊，vCenter 的主機名稱必須經 DNS 伺服器正確解析。
 - b. 在 **vCenter 使用者帳戶**下方的 **vCenter 使用者名稱**中，輸入管理員的使用者名稱或具備必要權限的使用者名稱。請以下列格式輸入**使用者名稱**：網域\使用者或網域/使用者或使用者@網域。OMIVV 會使用管理員使用者帳戶，或具備必要權限的使用者帳戶來管理 vCenter。如需更多資訊，請參閱**以非管理員使用者身分註冊 vCenter 伺服器** 第頁的 26。
 - c. 在**密碼**中輸入密碼。

- d. 在**確認密碼**再次輸入密碼。
5. 按一下**註冊**。
 - 註:** 透過使用連結模式，OpenManage Integration for VMware vCenter 目前針對單一 vCenter 執行個體或多個 vCenter 伺服器的超大型部署模式，支援多達 2000 部主機。
6. 執行下列其中一個動作：
 - 如果您使用的是 OMIVV 試用版，您會看到 OMIVV 圖示。
 - 如果您使用的是完整產品版本，則可從 Dell Digital Locker ([Dell Digital Locker](#)) 下載授權檔案，並將此授權匯入您的虛擬裝置。若要匯入授權檔案，請按一下**上傳授權**。
7. 在**上傳授權**視窗中，按一下**瀏覽**以移至授權檔案，然後按一下**上傳**以匯入授權檔案。
 - 註:** 若您修改或編輯授權檔案，授權檔案 (.XML 檔案) 將失去作用，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，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。

OMIVV 註冊之後，OMIVV 圖示就會顯示在 vSphere 用戶端 (HTML-5) 首頁上。

若要確認安裝，請參閱[驗證安裝](#) 第頁的 28。

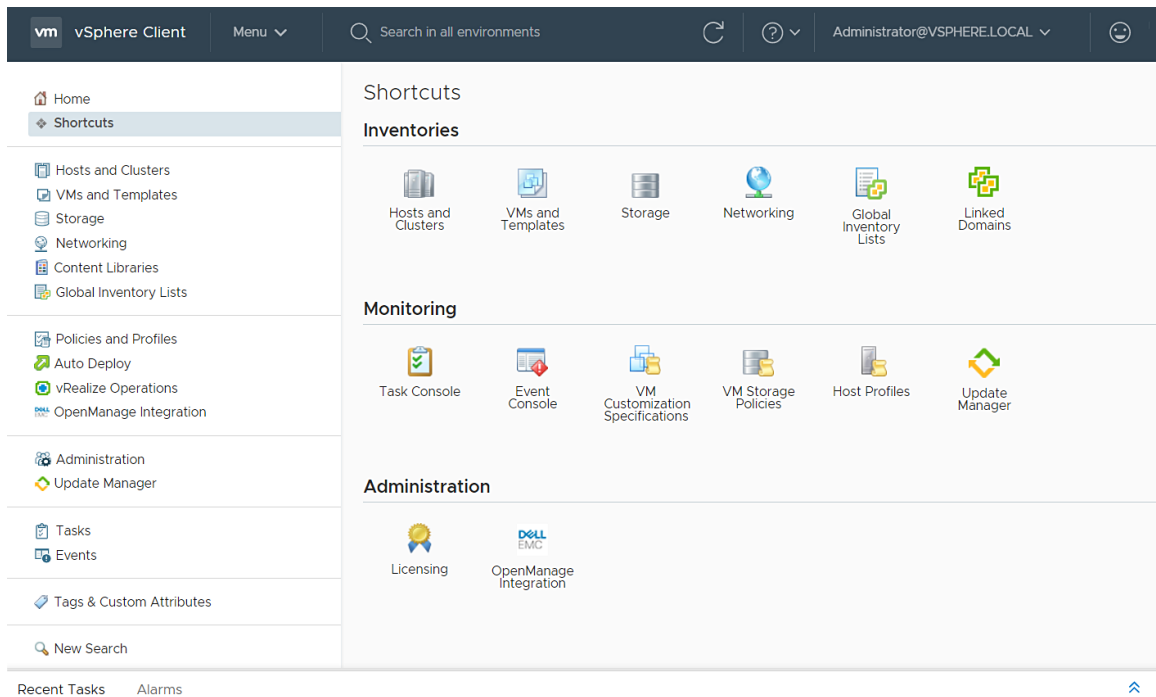


圖 3. OpenManage Integration for VMware vCenter 已順利加入 vCenter 中

針對所有 vCenter 作業，OMIVV 使用註冊使用者的權限，而非登入使用者的權限。

例如：使用者 X 具有必要權限並向 vCenter 註冊 OMIVV；使用者 Y 僅具有 Dell 權限。現在，使用者 Y 可以登入 vCenter 並可從 OMIVV 觸發韌體更新工作。執行韌體更新工作時，OMIVV 使用使用者 X 的權限，讓機器進入維護模式或重新啟動主機。

以非管理員使用者身分註冊 vCenter 伺服器

您必須具備 vCenter 系統管理員權限才能執行下列工作。

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 28。
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
- **i** 註：如果您使用的是 VMware vCenter 6.5 或升級至 vCenter 6.5 或更新版本，請指派下列健全狀況更新權限：
- 健全狀況更新提供者
 - 登錄
 - 取消登錄
 - 更新
- 主機
 - CIM
 - CIM 互動
 - 組態
 - 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
- **i** 註：如果您使用 vCenter 6.5 或升級至 vCenter 6.5 或更新版本，請確定指派修改叢集權限。
 - Host.Config
 - 進階設定
 - 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

i 註：如果您使用 vCenter 6.5 或升級至 vCenter 6.5 或更新版本，請確定指派修改叢集權限。


- 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
 - 建立工作
 - 更新工作

 **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 28。

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《使用者指南》中的〈安全性角色與權限〉主題。

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。

升級已註冊的 vCenter 版本後重新設定 OMIVV

升級已註冊的 vCenter 之後，請執行下列工作：

- 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 27。
例如，當您從 vCenter 6.0 升級至 vCenter 6.5 時，請指派額外的權限。
 2. 重新啟動已登錄的 OMIVV 裝置。
- 針對管理員使用者：
 1. 重新啟動已登錄的 OMIVV 裝置。

驗證安裝

下列步驟會驗證 OMIVV 安裝成功與否：

1. 關閉任何 vSphere 用戶端視窗，然後啟動新的 vSphere 用戶端 (HTML-5)。
2. 從 vCenter 伺服器嘗試傳送 PING 命令到虛擬裝置 IP 位址或主機名稱，以確保 vCenter 能夠與 OMIVV 通訊。

3. 在 vSphere 用戶端中展開 **功能表**，然後按一下**系統管理 > 解決方案 > 用戶端外掛程式**。
如需更多有關**外掛程式管理**或**用戶端外掛程式**頁面存取限制的資訊，請參閱 VMware 說明文件。
4. 在**用戶端外掛程式**頁面上驗證版本，並確認 OMIVV 已安裝並啟用。
如果未啟用 OMIVV，請等待一段時間，接著登出再登入 vCenter。
5. 若要確認 vSphere 用戶端 (HTML-5) 內有顯示 OMIVV 圖示，請在 vSphere 用戶端中展開**功能表**。
隨即顯示 OpenManage Integration 圖示。

管理備份和還原

您可以使用系統管理員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 30

在 OpenManage Integration for VMware vCenter 中執行下列步驟，透過管理主控台來存取**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。Dell EMC 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。密碼結尾不支援 % 符號。
 - 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 裸機伺服器。還原後僅保留 12G 與更新版本的伺服器。
- 不支援硬體設定檔與部署範本。Dell EMC 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 位元套件組合。
i 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 位元的韌體套件組合。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。

還原作業會導致 OMIVV 裝置在完成還原後重新啟動。

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**。
隨後裝置會重新開機。若要確認安裝，請參閱**驗證安裝** 第頁的 28。。
- 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**。
隨後裝置會重新開機。

更新 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 29。
 - 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《使用者指南》中的設定 HTTP Proxy 主題。
 - 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 執行個體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 第頁的 31。
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 31。
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。

使用 RPM 升級 OMIVV 裝置

請確保您要升級的裝置版本是比目前版本更新的版本。

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

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 外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](https://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/)取得的 RPM 進行升級，請確認[更新儲存庫路徑](https://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/)已設為以下路徑：

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](https://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/)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。

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。

 **註:** 在升級處理過程中，裝置會重新啟動一次或兩次。

 **註:** 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。如果您在叢集上已啟用主動式 HA，OMIVV 會取消登錄那些叢集的 Dell Inc 提供者，並在升級後重新登錄 Dell Inc 提供者。直到升級完成前，您將無法取得 Dell EMC 主機的健全狀況更新。

升級 VMware 工具

1. 以滑鼠右鍵按一下 OMIVV 裝置。

2. 將游標停留在**客體作業系統**，然後按一下**安裝/升級 VMware 工具**。

3. 在**安裝/升級 VMware 工具**對話方塊中，按一下**自動工具升級**，然後按一下**確定**。
您可以在**最近的工作區段**中檢視安裝狀態。

使用備份和還原來升級 OMIVV 裝置

Dell EMC 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 外掛程式。從 vCenter 取消註冊外掛程式，會移除由 OMIVV 外掛程式在 vCenter 上進行註冊之主動式 HA 叢集的 Dell 健全狀況更新提供者。

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。

i 註: Dell EMC 建議新的 OMIVV 裝置保留舊版 OMIVV 裝置的身分識別 (IP 或 FQDN)。

i 註: 如果新裝置的 IP 位址與舊版裝置的 IP 位址不同，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。

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 23 和 [上傳 HTTPS 憑證](#) 第頁的 24。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 [驗證安裝](#) 第頁的 28。
9. 升級後，Dell EMC 建議您在 OMIVV 外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。

i 註: 如果新的 Y 版 OMIVV 的身分識別 (IP 或 FQDN) 是從 X 版 OMIVV 變更而來，請將 SNMP 設陷的設陷目的地設定為指向新裝置。如果是 12G 及更新版本的伺服器，則可在這些主機上執行清查來修正身分識別變更。在 12G 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《使用者指南》中的〈管理相容性〉一節。

將舊版的 OMIVV 備份並還原至更新版本後，如果您發現系統顯示 200000 訊息，或未顯示 Dell EMC 標誌，或 OMIVV UI 在 vCenter UI 上無回應時，請執行下列步驟：

- 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-client/vc-packages/vsphere-client-serenity`。若為 Windows vCenter，請移至 vCenter 裝置中的下列資料夾，檢查是否有對應於舊版本的舊資料：vCenter 裝置的 `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity` 資料夾。
舊資料範例：`com.dell.plugin.OpenManage—com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.XXX`。
 - 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。

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**。

i 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**。

i 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。

取消註冊後還原 OMIVV

取消註冊舊版 OMIVV 後還原 OMIVV

如果您已在備份舊版資料庫後取消註冊 OMIVV 外掛程式，請先執行下列步驟，再繼續移轉：

註: 取消註冊外掛程式時，將會移除已註冊警報及 PHA 叢集的 Dell 健全狀況更新供應商上實作的所有自訂項目。下列步驟不會還源自訂。但會以警報的預設狀態重新註冊警報。

註: Dell EMC 建議新的 OMIVV 裝置保留舊版 OMIVV 裝置的身分識別 (IP 或 FQDN)。

註: 如果新裝置的 IP 位址與舊版裝置的 IP 位址不同，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 主機的叢集停用再啟用 PHA。

執行[使用備份和還原來升級 OMIVV 裝置](#) 第頁的 31 中列出的 3 至 9 項工作。

管理取消註冊與重新註冊

Dell EMC 建議您在取消註冊前先進行備份。

註: 取消註冊外掛程式時，將會移除已註冊警報及 PHA 叢集的 Dell 健全狀況更新供應商上實作的所有自訂項目。下列步驟不會還源自訂。但會以警報的預設狀態重新註冊警報。

1. 進行 OMIVV 的備份。
2. 取消註冊 OMIVV 上的 vCenter。
3. 執行任何已規劃的組態變更。例如變更主機名稱、變更新組態。
4. 重新啟動 OMIVV 裝置。
5. 還原備份檔案。如需更多資訊，請參閱[使用備份和還原來升級 OMIVV 裝置](#) 第頁的 31。

設定 VMware vCenter 的裝置

您可以使用下列任一方法設定 OMIVV 裝置：

- 使用**初始組態精靈**。

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

- 使用**設定標籤**。

i 註：這兩種方法的使用者介面很類似。

主題：

- [使用初始組態精靈的組態工作](#)
- [「設定」頁面上的組態工作](#)

使用初始組態精靈的組態工作

i 註：變更 DNS 設定之後，如果在執行 OMIVV 相關工作時發現 Web 通訊錯誤，請清除瀏覽器快取，並登出 vSphere 用戶端 (HTML-5)，然後再次登入。

您可以使用初始組態精靈來檢視和執行下列工作：

- 選取 vCenter
- 建立主機認證設定檔。如需更多資訊，請參閱[建立主機認證設定檔](#) 第頁的 35。
- 設定事件與警報。如需更多資訊，請參閱[設定事件與警報](#) 第頁的 37。
- 排程清查工作。如需更多資訊，請參閱[排程清查工作](#) 第頁的 36。
- 排程保固擷取工作。如需更多資訊，請參閱[排程保固擷取工作](#) 第頁的 36。

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**。
i 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 35。

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 設陷目的地。OMIVV 會為執行 ESXi 6.5 和更新版本的主機自動啟用 WBEM 服務。

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 設陷目的地失敗，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〈管理相容性〉一節 (使用者指南)。

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 36。
 - 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 36。

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**。

如果要修改保固擷取工作排程，請前往**設定 > 保固擷取 > 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 37。

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**。

Dell EMC 建議將您的 OMIVV 主機與組態基線建立關聯，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。

建立主機認證設定檔

如果新增的主機數目超過建立主機認證設定檔的授權限制，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**建立主機認證設定檔**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 執行個體。

i 註: 如果您在建立主機認證設定檔時，選擇**所有已註冊的 vCenter**，則所有執行停用 WBEM 服務之 ESXi 6.5 或更新版本的主機，其測試連線都會失敗。在此狀況下，Dell EMC 建議您完成主機認證設定檔精靈的動作，接著執行主機清查，然後再次測試主機認證設定檔。

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 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的建議字元的資訊，請參閱 dell.com/support 中的 *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。

i 註: iDRAC 帳戶需要系統管理員權限以更新韌體及部署作業系統。

- 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 AD 認證。

- 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。

d. 在**主機根**區域中，輸入主機的本機認證或 AD 認證。

- 若要輸入 ESXi 主機的本機認證，請執行下列作業：
 - 預設使用者名為 **root**。您不能編輯。
 - 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。
- 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。

註: 若為執行 ESXi 6.5 U2 或更新版本的主機，即使輸入不正確的主機認證，OMIVV 也能取得 iDRAC 資訊。

5. 按一下**下一步**。

選取主機頁面會隨即顯示。

註: 如果您嘗試在單一主機認證設定檔中管理所有 OMIVV 管理的主機，可能需要幾分鐘的時間來顯示 vCenter 中的 Dell 清查通知。當您首次將大量主機新增到主機認證設定檔時，可能會出現延遲。後續清查會正常執行。

6. 在**選取主機**頁面中，展開樹狀圖並選取主機，然後按一下**確定**。

● 按一下**新增主機**以便在**相關聯的主機**頁面上新增或移除主機。

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**。Dell EMC 建議您測試所有經設定的主機之連線。

註: 即使輸入有效認證，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。

註: 如果任一執行 ESXi 6.5 或更新版本的主機停用 WBEM 服務，那麼當您對該等主機執行測試連線或執行清查時，WBEM 便會自動啟用。

註: 使用不正確的密碼測試主機認證設定檔中 iDRAC 連線，將會鎖定對裝置的 iDRAC 存取，直到 iDRAC 中設定的處罰時間到了為止。iDRAC 的 IP 篩選和封鎖設定中所指定的處罰時間到了之後，以正確的密碼重新嘗試。

8. 按一下**完成**。

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。Dell EMC 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 > 保固擷取**。

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. 請確定已在主機和機箱上成功執行清查。

2. 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。

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 設陷目的地。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，Dell EMC 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。Dell EMC 建議選取「張貼所有事件」選項為事件張貼等級。
- **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標籤。

「設定」頁面上的組態工作

在**設定**頁面上，您可以執行下列工作：

- [設定保固到期通知](#)
- [設定最新裝置版本通知](#)
- [設定部署認證](#)
- [覆寫狀況更新通知的重要性](#)
- [初始組態](#)

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。Dell EMC 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 是作為佈建伺服器使用。部署認證可讓您與在自動探索程序中使用 OMIVV 外掛程式作為佈建伺服器的 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 認證加以佈建。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**。
請確定您只提供 iDRAC 支援的字元，以及 iDRAC 的本機認證。
3. 按一下**套用**。

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 > 裝置設定 > 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，並包括事件 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**。

從 Dell EMC 支援網站存取文件

您可以用下列連結存取所需文件：

- Dell EMC 企業系統管理文件 — www.dell.com/SoftwareSecurityManuals
- Dell EMC OpenManage 文件 — www.dell.com/OpenManageManuals
- Dell EMC 遠端企業系統管理文件 — www.dell.com/esmmanuals
- iDRAC 文件 — www.dell.com/idracmanuals
- Dell EMC OpenManage Connections 企業系統管理文件 — www.dell.com/OMConnectionsEnterpriseSystemsManagement
- Dell EMC 服務性工具文件 — www.dell.com/ServiceabilityTools
- 1. 前往 www.support.dell.com。
- 2. 按一下 **瀏覽所有產品**。
- 3. 從 **所有產品** 頁面，按一下 **軟體**，然後從以下按一下所需的連結：
 - 分析
 - 用戶端系統管理
 - 企業應用程式
 - 企業系統管理
 - 公共事業解決方案
 - 公用程式
 - 大型主機
 - 服務性工具
 - 虛擬化解決方案
 - 作業系統
 - 支援
- 4. 若要檢視文件，請按一下所需的產品，然後按一下所需的版本。
- 使用搜尋引擎：
 - 在搜尋方塊輸入文件名稱和版本。

相關說明文件

除了本指南外，您還可以在 www.dell.com/support/ 存取其他指南。按一下 **瀏覽所有產品**，然後按一下 **軟體 > 虛擬化解決方案**。按一下 **OpenManage Integration for VMware vCenter 5.0** 以存取下列文件：

- *OpenManage Integration for VMware vCenter 5.0 版使用者指南*
- *OpenManage Integration for VMware vCenter 5.0 版版本資訊*
- *OpenManage Integration for VMware vCenter 5.0 版相容性比較表*

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