


OpenManage Integration for VMware vCenter 4.3 版

Web 用戶端安裝指南

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
主機和 vCenter 伺服器的授權要求.....	5
購買並上傳軟體授權.....	5
上傳授權後的選項.....	6
強制執行.....	6
重要的參考注意事項.....	7
硬體需求.....	7
設定部署模式.....	7
BIOS、iDRAC、Lifecycle Controller 版本.....	8
PowerEdge 伺服器上支援的功能.....	10
PowerEdge 機箱上支援的功能.....	11
佈建儲存所需的空間.....	12
軟體需求.....	12
OpenManage Integration for VMware vCenter 需求.....	12
連接埠資訊.....	13
先決條件核對清單.....	15
安裝、設定與升級 OMIVV.....	15
下載 OpenManage Integration for VMware vCenter.....	16
使用 vSphere Web 用戶端來部署 OMIVV OVF.....	16
產生憑證簽署要求.....	17
上傳 HTTPS 憑證.....	17
以非系統管理員使用者身分註冊 vCenter Server.....	18
註冊 OpenManage Integration for VMware vCenter 與匯入授權檔案.....	20
升級已登錄的 vCenter.....	23
驗證安裝.....	23
更新虛擬裝置儲存庫位置和虛擬裝置.....	23
將 OMIVV 從現有版本升級至最新版本.....	23
透過備份與還原更新裝置.....	24
取消註冊舊版 OMIVV 後復原 OMIVV.....	25
章 2: VMware vCenter 的裝置組態.....	26
透過組態精靈執行的組態工作.....	26
檢視組態精靈歡迎對話方塊.....	26
選取 vCenter.....	26
建立連線設定檔.....	27
排程清查工作.....	28
執行保固擷取工作.....	29
設定事件與警報.....	29
設定 SNMP 設陷社群字串.....	30
透過「設定」標籤進行的設定工作.....	30
裝置設定.....	30
vCenter 設定.....	32
建立機箱設定檔.....	34

章 3: 從 Dell EMC 支援網站存取文件.....	35
章 4: 相關說明文件.....	36

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，如需瞭解所有包括清查管理、監控與警示、韌體更新，及保固管理在內等管理層面的相關資訊，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](#)
- [安裝、設定與升級 OMIVV](#)

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** — 完整產品版本包含最多 10 個 vCenter Server 的標準授權，您可以購買不限數量、由 OMIVV 管理的主機連線。

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 10 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，此數字代表已探索與清查到的主機 (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。

 **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。

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](#)，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。


主機和 vCenter 伺服器的授權要求

以下是主機與 vCenter 的授權要求：

- 您可以購買可支援由 OMIVV 管理之 Dell EMC 伺服器數量的授權。只有將主機新增至連線設定檔之後，才會用到授權。授權並未與特定伺服器具有關聯。
- 一個 OMIVV 例項最多可支援 10 個 vCenter 伺服器例項。vCenter 伺服器數目並未有個別的授權。

購買並上傳軟體授權

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

 **註：** 只有在使用試用版授權時，才會出現**購買授權**選項。

1. 在 OpenManage Integration for VMware vCenter 中，執行下列其中一個工作：

- 在**授權**標籤中的**軟體授權**旁，按一下**購買授權**。
 - 在**入門**標籤的**基本工作**底下，按一下**購買授權**。
2. 將您從 Dell Digital Locker 下載的授權檔案儲存到一個已知位置。
 3. 在 Web 瀏覽器中，輸入管理主控台的 URL。
使用此格式：`https://<ApplianceIPAddress>`
 4. 在**管理主控台** 登入視窗中輸入密碼，然後按一下**登入**。
 5. 按一下**上傳授權**。
 6. 在**上傳授權**視窗中，若要瀏覽至授權檔案，請按一下**瀏覽**。
 7. 選取授權檔案，然後按一下**上傳**。

i 註：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

從 OMIVV 2.1 版開始，OMIVV 可以堆疊多個標準授權，以將支援的主機數量提高為上傳授權的主機總數。評估授權無法堆疊。支援的 vCenter Server 無法藉由堆疊增加數量，必須使用多台應用裝置。

堆疊授權有某些功能上的限制。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。如果授權在上傳之後才過期，則您可以繼續使用現有主機的功能，但無法升級到新版 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

當所有授權都過期時，裝置就不會允許更新至更新的版本。因此在升級裝置之前，請先取得並上傳新授權。

評估授權

評估授權到期時，有幾個關鍵區域會停止運作，並顯示錯誤訊息。

新增主機至連線設定檔

當您在連線設定檔新增主機時，如果授權第 11 代或更新版本主機的數目，超過授權的數目，就無法額外新增主機。

重要的參考注意事項

- 從 OMIVV 4.0 版開始，只支援 VMware vSphere Web 用戶端，而不支援 vSphere Desktop 用戶端。
- 若為 vCenter 6.5 及更新版本，OMIVV 裝置只提供 Flash 版本，而不提供 HTML5 版本。
- 使用 DNS 伺服器時，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，但建議您指派靜態 IP 位址。當您部署具有有效 DNS 登錄的 OMIVV 產品時，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 5.5 的 DNS 需求](#)
- [vSphere 6.0 的 DNS 需求](#)
- [vSphere 6.5 與平台服務控制器裝置的 DNS 需求](#)
- 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 7 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 13 頁的 13。

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。您可以在《OpenManage Integration for VMware vCenter Release Notes》(OpenManage Integration for VMware vCenter 版本資訊) 找到關於平台需求的全方位資訊，網址是：Dell.com/support/manuals。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)
- OMSA 支援第 11 代和舊版伺服器，以及 ESXi 版本支援 (包括部署及管理)
- 支援 OMIVV 的記憶體和空間

motherboard/網路子卡上必須具有 LAN，OMIVV 才能存取 iDRAC 和 CMC 或管理模組系統管理網路與 vCenter 管理網路。

設定部署模式

請確定符合所需部署模式的下列系統需求：

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 (以 GB 為單位)	最小儲存空間
小型	最多 250 個	2	8	44 GB
中型	最多 500 個	4	16	44 GB
大型	最多 1000 個	8	32	44 GB

註: 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 虛擬應用裝置。有關保留記憶體資源的步驟，請參閱 vSphere 說明文件。

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** 或 **大型**，而部署模式預設設定為 **小型**。
2. 如果您要根據環境來更新部署模式，請按一下 **編輯**。
3. 在 **編輯** 模式中，確定符合先決條件之後，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，而且發生下列任一情況：
 - 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. 如果變更部署模式，請確認變更，然後繼續重新啟動 OMIVV 裝置，讓部署模式進行更新。

註: 在 OMIVV 裝置啟動期間，會根據設定的部署模式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，OMIVV 裝置無法啟動至登入畫面。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，並進行降級部署模式工作。

降級部署模式

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

BIOS、iDRAC、Lifecycle Controller 版本

本節中列出啟用 OpenManage Integration for VMware vCenter 功能所需的 BIOS、iDRAC 及 Lifecycle Controller 版本。

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：

註: 建議您將 Dell EMC OpenManage Enterprise-Modular Edition 1.00.01 版搭配 OMIVV 4.3 使用。

表 2. 適用於 PowerEdge 第 11 代伺服器的 BIOS

伺服器	最低版本
PowerEdge R210	1.8.2 或更新版本
PowerEdge R210II	1.3.1 或更新版本
PowerEdge R310	1.8.2 或更新版本
PowerEdge R410	1.9.0 或更新版本
PowerEdge R415	1.8.6 或更新版本
PowerEdge R510	1.9.0 或更新版本
PowerEdge R515	1.8.6 或更新版本
PowerEdge R610	6.1.0 或更新版本
PowerEdge R710	6.1.0 或更新版本
PowerEdge R710	6.1.0 或更新版本
PowerEdge R715	3.0.0 或更新版本
PowerEdge R810	2.5.0 或更新版本
PowerEdge R815	3.0.0 或更新版本
PowerEdge R910	2.5.0 或更新版本
PowerEdge M610	6.1.0 或更新版本
PowerEdge M610x	6.1.0 或更新版本
PowerEdge M710HD	5.0.1 或更新版本
PowerEdge M910	2.5.0 或更新版本
PowerEdge M915	2.6.0 或更新版本
PowerEdge T110 II	1.8.2 或更新版本
PowerEdge T310	1.8.2 或更新版本

表 2. 適用於 PowerEdge 第 11 代伺服器的 BIOS

伺服器	最低版本
PowerEdge T410	1.9.0 或更新版本
PowerEdge T610	6.1.0 或更新版本
PowerEdge T710	6.1.0 或更新版本

表 3. 適用於 PowerEdge 第 12 代伺服器的 BIOS

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

表 4. 適用於 PowerEdge 第 13 代伺服器的 BIOS

伺服器	最低版本
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
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

表 4. 適用於 PowerEdge 第 13 代伺服器的 BIOS

伺服器	最低版本
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

表 5. 適用於 PowerEdge 第 14 代伺服器的 BIOS

伺服器	最低版本
R940	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
R640	1.0.0 或更新版本
M640	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

表 6. 適用於部署的 iDRAC 和 Lifecycle Controller

代	版本	
	iDRAC	Lifecycle Controller
PowerEdge 第 11 代伺服器	3.35 的模組化, 1.85 的機架或直立型	1.5.2 或更新版本
PowerEdge 第 12 代伺服器	2.30.30.30 或更新版本	2.30.30.30 或更新版本
PowerEdge 第 13 代伺服器	2.30.30.30 或更新版本	2.30.30.30 或更新版本
PowerEdge 第 14 代伺服器	3.00.00.00 和更新版本	3.00.00.00 和更新版本

表 7. 雲端伺服器的 BIOS 和 iDRAC 需求

Model	BIOS	iDRAC 與 Lifecycle Controller
C6320	1.0.2	2.30.30.30 或更新版本
C4130	1.0.2	2.30.30.30 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

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 8. PowerEdge 伺服器上支援的功能

功能	平台		
	第 11 代	第 12 和 13 代	第 14 代
硬體清單	Y	Y	Y
事件與警示	Y (僅限 SNMP v1)	Y (SNMP v1 和 v2)	Y (SNMP v1 和 v2)
元件智慧健全狀況監控*	Y	Y	Y
BIOS/韌體更新#	Y	Y	Y
主動式 HA\$	N	Y	Y
保固資訊	Y	Y	Y
主機相容性	Y	Y	Y
裸機伺服器的自動/手動探索	Y	Y	Y
裸機相容性	Y	Y	Y
硬體設定	Y	Y	Y
裸機 Hypervisor 部署	Y	Y	Y
閃爍伺服器 LED	Y	Y	Y
檢視/清除 SEL 記錄	Y	Y	Y
連結並啟動 iDRAC	Y	Y	Y
重設 iDRAC	Y	Y	Y
系統鎖定模式	N	N	Y
系統設定檔	N	N	Y
叢集設定檔	N	Y ^	Y
使用整合機箱 IP 來管理主機	N	N	Y@
支援 OEM 伺服器	N	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。

^ 在叢集設定檔中，不支援組態漂移。

@ 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。

~ 僅支援第 13 代伺服器。

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 9. 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

表 9. 模組化基礎架構上支援的功能

功能	M1000e	VRTX	FX2s	MX
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

佈建儲存所需的空間

OMIVV 虛擬裝置至少需要 44GB 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 2 個虛擬 CPU (小型部署模式) 加以佈建。

軟體需求

vSphere 環境必須符合虛擬裝置、連接埠存取，和接聽連接埠的需求。

VMware vSphere Web 用戶端的需求

- 支援 vCenter 6.0 及更新版本
- 您必須從 vCenter 安裝 Web 用戶端服務 (vSphere Desktop 用戶端不支援)

如需特定軟體需求，亦可參閱《OpenManage Integration for VMware vCenter Compatibility Matrix》(OpenManage Integration for VMware vCenter 相容性比較表)，網址是：Dell.com/support/manuals。

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 10. 支援的 ESXi 版本

ESXi 版本支援	伺服器世代			
	11G	12G	13G	14G
5.1 版	Y	Y	N	N
5.1 版 U1	Y	Y	N	N
5.1 版 U2	Y	Y	Y	N
5.1 版 U3	Y	Y	Y (M830、FC830 及 FC430 除外)	N
5.5 版	Y	Y	N	N
5.5 版 U1	Y	Y	N	N
5.5 版 U2	Y	Y	Y	N
5.5 版 U3	Y	Y	Y	N
6.0 版	Y	Y	Y	N
6.0 版 U1	Y	Y	Y	N

表 10. 支援的 ESXi 版本

ESXi 版本支援	伺服器世代			
	11G	12G	13G	14G
6.0 版 U2	Y	Y	Y	N
6.0 版 U3	Y	Y	Y	Y
6.5 版	N	Y	Y	N
6.5 版 U1	N	Y	Y	Y
6.5 版 U2	N	Y	Y	Y
6.7 版	N	Y	Y	Y
6.7 版 U1	N	Y	Y	Y

i 註: 只有搭配使用 ESXi 6.5 U2 和更新版本時，才支援 MX 主機。

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

表 11. 支援的 vCenter 伺服器版本

vCenter 版本	Web 用戶端支援
6.0 版 U2	Y
6.0 版 U3	Y
6.5 版	Y
6.5 版 U1	Y
6.5 版 U2	Y
6.7 版	Y
6.7 版 U1	Y

i 註: 如需有關登錄 vCenter Server 的詳細資訊，請參閱 *OpenManage Integration for VMware vCenter Version 4.3 Web Client Install Guide* (OpenManage Integration for VMware vCenter 4.3 版 Web 用戶端安裝指南)，網址是：Dell.com/support/manuals。

OpenManage Integration for VMware vCenter 4.3 版支援 VMware vRealize Operations Manager (vROPS) 1.1 版和 1.2 版。

連接埠資訊

虛擬裝置與受管節點

在 OMIVV 中，當您使用修復不相容的 vSphere 主機精靈中的修復不相容的主機連結，來部署 OMSA 代理程式時，OMIVV 會執行以下動作：

- 啟動 HTTP 用戶端服務
- 啟用連接埠 8080
- 讓 ESXi 5.0 或更新版本可使用連接埠下載並安裝 OMSA VIB

OMSA VIB 安裝完成後，服務會自動停止，且連接埠會關閉。

表 12. 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。
69	TFTP	UDP	無	輸出	OMIVV 裝置至 TFTP 伺服器	TFTP 用戶端	在有舊韌體的 11G 伺服器上用於韌體更新。

表 12. 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 vCenter Web 用戶端和 Dell 管理員入口網站使用。
443	WSMAN	TCP	128 位元	輸入/輸出	OMIVV 裝置至/從 iDRAC/OMSA	iDRAC/OMSA 通訊	iDRAC、OMSA 和 CMC 或管理模組通訊，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、OMSA 和 CMC 或管理模組的資料，來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 13. 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(OMSA)	iDRAC/OMSA 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。
8080	HTTP	TCP	128 位元	輸出	ESXi 至 OMIVV 裝置	HTTP 伺服器；可下載 OMSA VIB 並修正不相容的 vSphere 主機。	可協助 ESXi 下載 OMSA/驅動程式 VIB。

表 14. 受管節點 (iDRAC 或 CMC 或管理模組)

表 14. 受管節點 (iDRAC 或 CMC 或管理模組)

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, REST/HTTPS	TCP	128 位元	輸入	OMIVV 應用裝置到 iDRAC 或 CMC 或管理模組	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 機箱通訊。此連接埠必須從 iDRAC 和 CMC 或管理模組開啟。
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

啟動產品安裝前的核對清單：

- 確認您擁有可讓 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。如需更多有關 OMIVV 作業所需的權限清單，請參閱 [非管理員使用者必須具備的權限](#)。
- 檢查您具有 ESXi 主機系統的根密碼，或是有主機管理權限的 Active Directory 認證。
- 檢查您是否擁有與 iDRAC Express 或在 iDRAC 上有管理權限的 Enterprise 相關聯的使用者名稱和密碼。
- 檢查 vCenter 伺服器是否正在執行中。
- 確認 OMIVV 安裝目錄的位置。
- 檢查以確保 VMware vSphere 環境符合虛擬裝置、連接埠存取以及接聽連接埠的需求。此外，如有必要請在用戶端系統上安裝 Adobe Flash Player。如需進一步瞭解支援的 Flash Player 版本，請參閱 *《OpenManage Integration for VMware vCenter Compatibility Matrix》* (OpenManage Integration for VMware vCenter 相容性比較表)。

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。

i 註: 建議將 OMIVV 和 vCenter 伺服器置於同個網路。

i 註: OMIVV 裝置網路應該具備 iDRAC、主機和 vCenter 的存取權。

安裝、設定與升級 OMIVV

請務必符合硬體需求，並且執行所需的 VMware vCenter 軟體。

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 16。
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 網路用戶端，部署包含 OMIVV 裝置的「開放虛擬格式」(OVF) 檔案。請參閱 [部署 OMIVV OVF](#)。
4. 上傳授權檔案。如需更多有關授權的資訊，請參閱 [上傳授權](#)。
5. 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](#)。
6. 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](#)。

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 Web 用戶端來部署 OMIVV OVF

請務必先從 Dell 網站下載並解壓縮產品 zip 檔案 *Dell_OpenManage_Integration_<version number>.<build number>.zip*。

1. 找到您下載並解壓縮的 OMIVV 虛擬磁碟，然後執行 **Dell_OpenManage_Integration.exe**。
解壓縮和執行 exe 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 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 Web 用戶端**。
5. 從 **VMware vSphere Web 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**選取來源**視窗中，執行以下子工作：
 - a. 如果您要從網際網路下載 OVF 套件，請選取 **URL**。
 - b. 如果您要從本機系統選取 OVF 套件，請選取**本機檔案**，然後按一下**瀏覽**。

 **註:** 如果 OVF 套件位於網路共用上，安裝程序可能需要 10 到 30 分鐘。若要快速安裝，建議您在本機磁碟控管 OVF。
7. 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：
 - **產品** — 顯示 OVF 範本名稱。
 - **版本** — 顯示 OVF 範本的版本。
 - **廠商** — 顯示廠商名稱。
 - **發行者** — 顯示發行者詳細資料。
 - **下載大小** — 顯示 OVF 範本的實際大小 (以 GB 為單位)。
 - **磁碟上大小** — 顯示複雜與精簡佈建詳細資訊的詳細資訊。
 - **說明** — 註解會顯示在這裡。
8. 按一下**下一步**。

隨後便會出現**選取名稱和資料夾**視窗。

9. 在**選取名稱和資料夾**視窗中，執行以下子步驟：
 - a. 在**名稱**中輸入範本名稱。名稱最多可包含 80 個字元。
 - b. 在**選取資料夾或資料中心**清單中，選取要部署範本的位置。
10. 按一下**下一步**。
選取儲存裝置視窗隨即顯示。
11. 在**選取儲存裝置**視窗中，執行以下子步驟：
 - a. 在**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. 在**虛擬機器儲存原則**下拉式清單中選取一個原則。
12. 按一下**下一步**。
隨後便會出現**設定網路**視窗，顯示來源和目的網路的詳細資料。
13. 在**設定網路**視窗中，按一下**下一步**。
 **註:** 建議您將 OMIVV 裝置和 vCenter 伺服器放在同一個網路。
14. 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**。
部署工作會隨即執行，並提供完成狀態視窗，讓您追蹤工作進度。

產生憑證簽署要求

在 vCenter 登錄 OMIVV 之前，請務必先上傳憑證。


產生新的憑證簽署要求 (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，請按一下**繼續**；若要取消，則按一下**取消**。
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，針對此要求輸入**一般名稱、組織名稱、組織單位、位置、州名、國家/地區和電子郵件**。按一下**繼續**。
3. 按一下**下載**，然後將產生的憑證要求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，在虛擬裝置與主機系統之間進行安全通訊。若要設定這類安全通訊，必須將 CSR 傳送至憑證授權單位，然後使用管理主控台上傳產生的憑證。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。

 **註:** 您可以使用 Microsoft Internet Explorer、Firefox、Chrome 來上傳憑證。

1. 在**裝置管理**頁面中，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. 若要選取欲上傳的憑證，先按一下**瀏覽**，然後按一下**上傳**。
4. 如果您想要取消上傳，請按一下「取消」。
 **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 登錄。如果向 vCenter 註冊後才上傳新的自訂憑證，Web 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。

還原預設的 HTTPS 憑證

1. 在**裝置管理**頁面中，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**。

以非系統管理員使用者身分註冊 vCenter Server

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系統管理員使用者註冊 vCenter Server，請執行以下步驟：

1. 若要變更為某個角色選取的權限，請新增該角色，然後為該角色選取必要的權限，或修改現有的角色。
請參閱 VMware vSphere 說明文件，瞭解建立或修改角色的必要步驟，然後在 vSphere Web 用戶端中選取權限。若要為角色選取所有必要的權限，請參閱[非管理員使用者必須具備的權限](#)。

i 註: vCenter 管理員應新增或修改角色。

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。
如需在 vSphere Web 用戶端中指派權限的詳細資訊，請參閱 VMware vSphere 說明文件。

i 註: vCenter 管理員應在 vSphere Client 中指定權限。

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 Server。
4. 請將 Dell 權限指定給在步驟 1 中建立或修改的角色。請參閱在[vSphere Web 用戶端中將 Dell 權限指派給角色](#)。

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

非管理員使用者若要以 vCenter 登錄 OMIVV，必須具備以下權限：

i 註: 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，便會顯示錯誤訊息：

- 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
 - 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: 如果您使用的是 VMware vCenter 6.5 或升級至 vCenter 6.5 或更新版本，請指派下列權限：

- 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: 如果您使用的是 vCenter 6.5 或升級至 vCenter 6.5 或更新版本, 請確定您有指派修改叢集權限。

● 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

i 註: 如果非系統管理員使用者嘗試註冊 vCenter Server, 則必須為現有角色新增 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 19。


以具必要權限的非管理員使用者身分登錄 vCenter 伺服器

您可使用具所需權限的非系統管理員使用者身分, 為 OMIVV 產品登錄 vCenter 伺服器。請參閱註冊 **OpenManage Integration for VMware vCenter 與匯入授權檔案** 主題的步驟 5 至步驟 9。 , 取得以非系統管理員使用者或系統管理員身分註冊 vCenter Server 的資訊。

將 Dell 權限指派給現有角色

您可編輯現有的角色, 以指定 Dell 權限。

i 註: 請確定您以具管理員權限的使用者身分登入。

1. 以具系統管理權限的使用者身分登入 vSphere Web 用戶端。
2. 在 vSphere Web 用戶端中, 於左窗格中按一下 **「管理」** → **「角色」**。
3. 從**角色提供者**下拉式清單中選取 vCenter 伺服器系統。
4. 從**角色**清單選取角色, 然後按一下 。
5. 按一下 **「權限」**、展開 **「Dell」**, 然後針對所選角色選取下列 Dell 權限, 然後按一下 **「確定」** :
 - 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 《OpenManage Integration for VMware vCenter User's Guide》 (OpenManage Integration for VMware vCenter 使用者指南) 中的 安全性角色與權限, 網址為: Dell.com/support/manuals。

權限和角色的變更會立即生效。具必要權限的使用者現已可執行 OpenManage Integration for VMware vCenter 作業。

i 註: 針對所有 vCenter 作業, OMIVV 使用登錄使用者的權限, 而非登入使用者的權限。

i 註: 如果不具有指定 Dell 權限的登入使用者存取 OMIVV 的特定頁面, 將會顯示 2000000 錯誤。

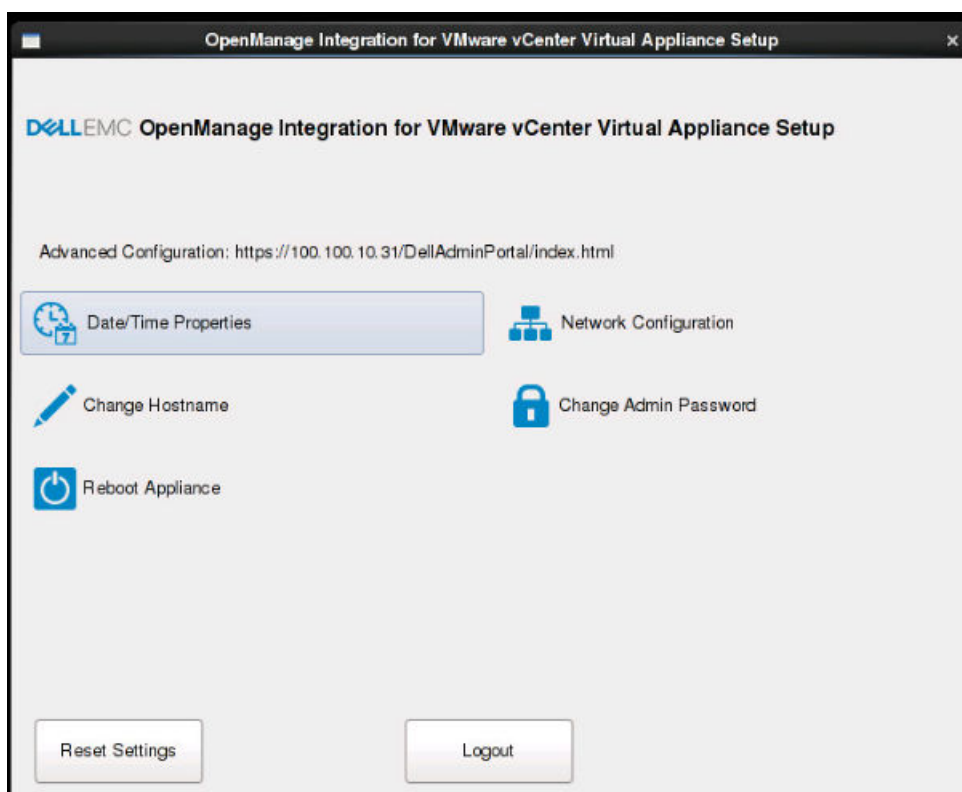
註冊 OpenManage Integration for VMware vCenter 與匯入授權檔案

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。

i 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。如果向 vCenter 註冊後才上傳新的自訂憑證，Web 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。

1. 從 vSphere Web 用戶端，按一下 **首頁 > 主機與叢集**，然後在左面板找到剛部署的 OMIVV，再按一下 **開啟虛擬機器電源**。部署時，如果選取 **部署後開啟電源**，部署完成後虛擬機器會自動啟動。
2. 若要執行 **管理主控台**，請按一下 **VMware vCenter** 主視窗中的 **主控台** 標籤。
3. 允許 OMIVV 完成開機，然後輸入使用者名稱 **Admin** (預設為 Admin)，然後按 **Enter** 鍵。
4. 輸入新的管理員密碼。確定管理員密碼符合介面上所顯示的密碼複雜度規則。按 **Enter** 鍵。
5. 重新輸入之前提供的密碼，然後按 **Enter** 鍵。
若要在 OMIVV 裝置中設定網路與時區資訊，請按 **Enter** 鍵。
6. 若要設定 OMIVV 時區資訊，請按一下 **日期/時間** 內容。

圖 1. 主控台索引標籤



7. 在 **日期與時間** 索引標籤，選取 **透過網路同步處理日期與時間**。隨後便會顯示 **NTP 伺服器** 方塊。
8. 將有效的 NTP 伺服器詳細資料新增至與其同步處理的 vCenter。
9. 按一下 **時區**，選取適用的時區，然後按一下 **確定**。
10. 若要將靜態 IP 設定至 OMIVV 裝置，請按一下 **網路設定**，或跳到步驟 17。
11. 選取 **自動 eth0**，然後按一下 **編輯**。
12. 選取 **IPv4 設定** 標籤，然後在 **方法** 下拉式清單中選取 **手動**。
13. 按一下 **新增**，然後新增有效的 IP 網路遮罩和閘道資訊。
14. 在 **DNS 伺服器** 欄位中，提供 DNS 伺服器的詳細資料。
15. 按一下 **套用**。
16. 若要變更 OMIVV 裝置的主機名稱，請按一下 **變更主機名稱**。
17. 輸入有效的主機名稱，然後按一下 **更新主機名稱**。

註: 主機名稱與 NTP 變更之後，請務必將系統重新開機。

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 執行個體，然後再重新註冊。

在開啟管理主控台之前，請務必先手動更新所有該裝置的參照，例如，iDRAC、DRM 中的佈建伺服器。

18. 由支援的瀏覽器開啟**管理主控台**。

若要開啟**管理主控台**，請在 OpenManage Integration for VMware vCenter 的**說明與支援**標籤中，按一下**管理主控台**底下的連結，或啟動 Web 瀏覽器並提供 URL：`https://<ApplianceIP 或 Appliance hostname>`。

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。

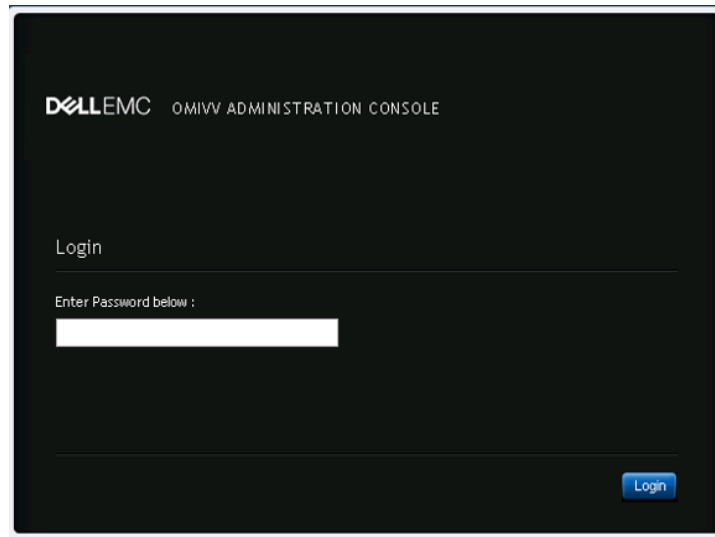


圖 2. 管理主控台

19. 在**管理主控台**登入視窗中輸入密碼，然後按一下**登入**。

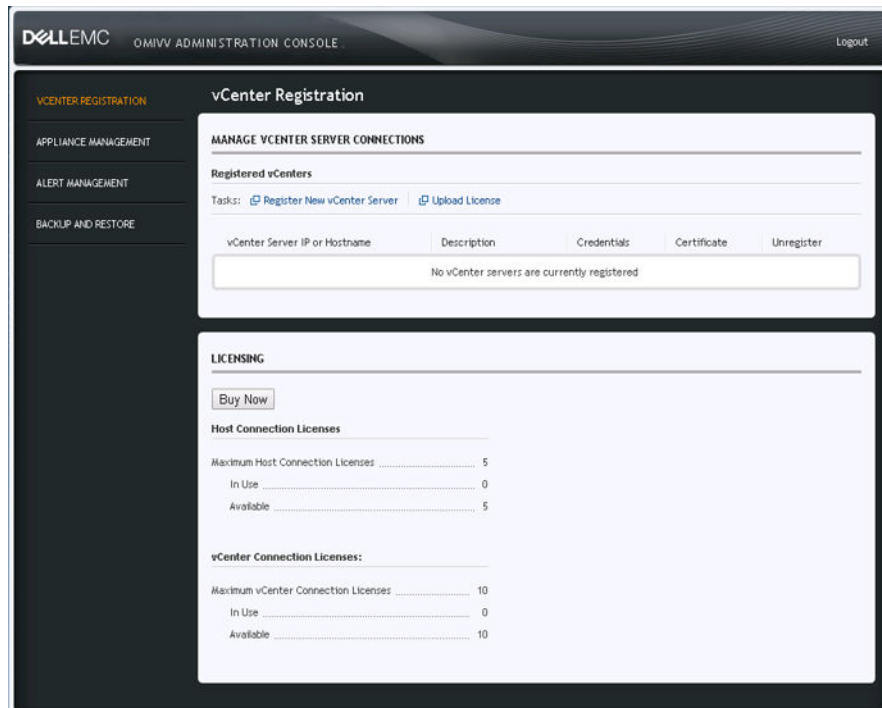


圖 3. 管理主控台的 vCenter 註冊視窗

20. 在 **vCenter 註冊視窗** 中，按一下 **註冊新的 vCenter 伺服器**。

21. 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 或主機名稱，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 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。

- c. 在 **密碼** 中輸入密碼。

- d. 在 **確認密碼** 再次輸入密碼。

22. 按一下 **登錄**。

註: OpenManage Integration for VMware vCenter 目前透過使用連結模式，針對單一 vCenter 執行個體或多個 vCenter 伺服器的大型部署模式，支援多達 1000 部主機。

23. 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**。

24. 在 **上傳授權視窗** 中，按一下 **瀏覽** 以瀏覽至授權檔案，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 Web 用戶端首頁的 **管理類別** 底下。

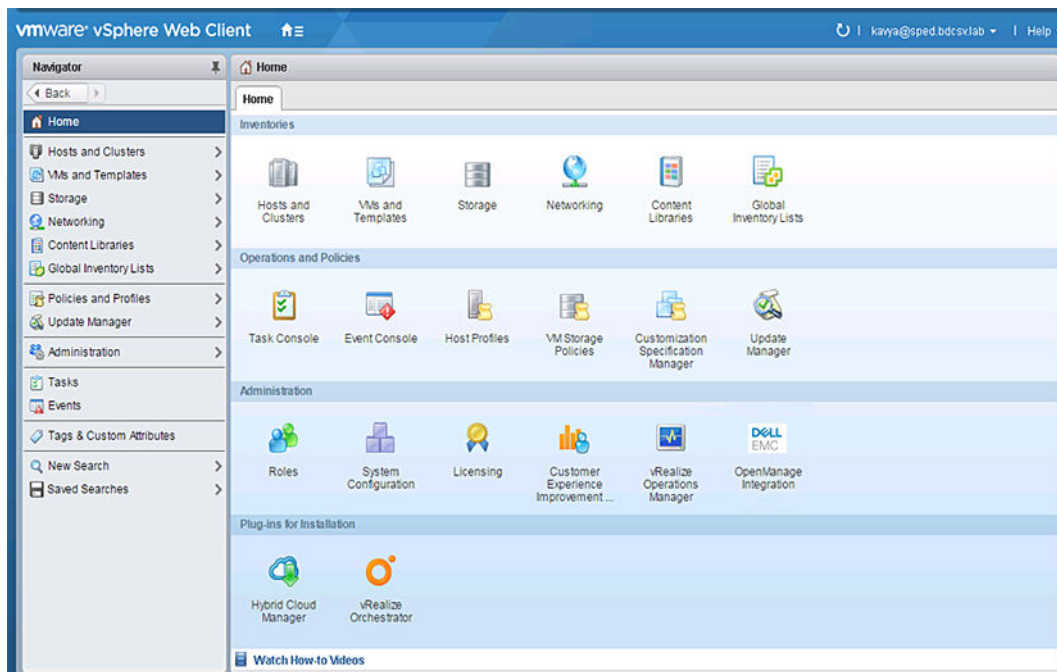


圖 4. OpenManage Integration for VMware vCenter 已順利加入 vCenter 中

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。

升級已登錄的 vCenter

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 18。
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 Web 用戶端。
2. 確認 vSphere Web 用戶端內有顯示 OMIVV 圖示。
3. 從 vCenter 伺服器嘗試傳送 PING 命令到虛擬應用裝置 IP 位址或主機名稱，以確保 vCenter 能夠與 OMIVV 通訊。
4. 在 vSphere Web 用戶端，請按一下 **首頁 > 管理 > 解決方案**，然後按一下 **外掛程式管理** (較舊的 vCenter 的版本) 或 **用戶端外掛程式** (新版)。
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。
5. 在**外掛程式管理員**或**用戶端外掛程式**視窗中，驗證是否已安裝和啟用 OMIVV。

更新虛擬裝置儲存庫位置和虛擬裝置

為了確保所有資料都能受到保護，在更新虛擬裝置之前，請先執行 OMIVV 資料庫備份。請參閱[管理備份和還原](#)主題 (位於《使用者指南》中)。

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

i 註：OMIVV 裝置需具有網際網路連線能力，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能力。根據網路設定，如果網路需要 Proxy，請啟用 Proxy 並提供 Proxy 設定。請參閱[設定 HTTP Proxy](#) 主題 (位於《使用者指南》中)。

i 註：請確認**更新儲存庫路徑**有效。

針對可用的虛擬裝置版本，適用的 RPM 和 OVF 虛擬裝置升級機制會以勾選符號顯示。以下是可能的升級機制選項，您可以針對升級機制執行任一工作：

- 如果勾選符號顯示於 RPM，您可以將 RPM 從現有版本升級為最新的可用版本。請參閱[從現有版本升級為最新版本](#)。
- 如果勾選符號顯示於 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[透過備份與還原更新裝置](#)。
- 如果勾選符號同時顯示於 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. 若要更新虛擬裝置，請根據 OMIVV 的版本，執行適用的上述升級機制工作。

i 註：請務必先登出所有 Web 用戶端工作階段，再登入已登錄的 vCenter 伺服器。

i 註：在登入任何已登錄的 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。

3. 按一下**裝置管理**，並確認升級機制。

將 OMIVV 從現有版本升級至最新版本

1. 在**裝置管理**頁面上，根據您的網路設定而定，如果您的網路需要代理，則啟用代理並提供代理設定。請參閱 [使用者指南](#)中的[設定 HTTP Proxy](#) 主題。
2. 若要將 OpenManage Integration 外掛程式從現有版本升級至最新版本，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，請務必將**更新儲存庫路徑**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**。

- 若要使用最新下載的 RPM 資料夾或檔案進行升級，但沒有網際網路連線能力，請從 <https://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/> 路徑下載所有的檔案與資料夾，並將其複製到 HTTP 共用區。

在**裝置管理**視窗中的**裝置更新**區段內，按一下**編輯**，然後在**更新儲存庫路徑**文字方塊中，加入連至離線 HTTP 共用區的路徑，然後按一下**套用**。

3. 比較可用的虛擬裝置版本和目前的虛擬裝置版本，並確認可用的虛擬裝置版本高於目前的虛擬裝置版本。
4. 若要套用更新至虛擬裝置，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。

i 註：在升級處理過程中，裝置會重新啟動一次或兩次。

i 註：該裝置經過 RPM 升級後，請確定您執行下列動作：

- 先清除瀏覽器快取記憶體，再登入 Dell 系統管理員入口網站。
- 重新安裝 VMware 工具。

若要重新安裝 VMware 工具：

1. 以滑鼠右鍵按一下 OMIVV 裝置。
2. 將游標停留在**來賓**，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**最近的工作中**檢視安裝狀態。

i 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，提供 <https://<AppliancePI>/hostname> 連結，並導覽至**裝置更新**區域。您可以確認可用虛擬裝置和目前虛擬裝置的版本是相同的。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。因此，直到升級完成前，您將無法取得 Dell EMC 主機的健全狀況更新。

透過備份與還原更新裝置

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. 備份較舊版本的資料庫。
2. 從 vCenter 關閉舊 OMIVV 裝置。

i 註：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 OMIVV 外掛程式在 vCenter 上註冊的所有警報，以及在警報上執行的所有自訂化作業，例如動作等。

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、時區等。

i 註：確定新 OpenManage Integration 裝置的 IP 位址與舊裝置一模一樣。

i 註：如果新裝置與舊裝置的 IP 位址不同，OMIVV 外掛程式可能無法正常運作。在此情況下，請先取消登錄，然後再重新登錄所有 vCenter 執行個體。

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**產生憑證簽署要求** 第頁的 17 和**上傳 HTTPS 憑證** 第頁的 17。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**使用者指南**中的**從備份還原 OMIVV 資料庫**主題。
8. 確認應用裝置。請參閱 *OpenManage Integration for VMware vCenter 安裝指南* 中的安裝驗證，網址是：Dell.com/support/manuals。
9. 在所有已登錄的 vCenter 伺服器上執行**清查**。

i 註：Dell EMC 建議您在升級之後，於外掛程式管理的所有主機上再執行一次清查。若要隨選執行清查，請參閱**排程清查工作**。

i 註: 如果新 y 版 OMIVV 的 IP 位址是變更自 x 版 OMIVV，請將 SNMP 陷阱的陷阱目的地，設定為將游標暫留在新應用裝置上方。如果是第 12 代及更新一代的伺服器，則可在這些主機上執行清查來修正 IP 變更。在第 12 代主機上執行清查時，如果 SNMP 陷阱沒有暫留在新 IP 上方，那些主機會列為不相容。如果是第 12 代之前與舊版相容的主機，IP 變更會顯示為不相容，您必須設定 Dell EMC OpenManage Server Administrator (OMSA)。若要修正 vSphere 主機相容性問題，請參閱 *使用者指南* 中的 **執行修正不相容 vSphere 主機精靈** 主題。

i 註: 從較舊版的 OMIVV 備份和恢復到較新版的 OMIVV 之後，如果您觀察到 2 百萬個錯誤或 Dell EMC 標誌沒有顯示在 vCenter，請執行下列步驟：

- 在 vCenter Server 上重新啟動 vSphere Web 用戶端。
- 如果問題仍然存在，請執行下列步驟：
 - 如果是 VMware vCenter Server 應用裝置，請前往 `/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity`，如果是 Windows vCenter，請前往 vCenter 應用裝置中的 `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\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。

取消註冊舊版 OMIVV 後復原 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：

i 註: 取消註冊外掛程式時，會移除由外掛程式對已註冊警報實作的所有自訂。下列步驟不會還原自訂。但會以警報的預設狀態重新註冊警報。

1. 執行 [透過備份與還原更新裝置](#) 第頁的 24 的步驟 3 至步驟 5。
2. 將外掛程式註冊到註冊舊外掛程式的同一個 vCenter。
3. 若要完成移轉，請執行 [透過備份與還原更新裝置](#) 第頁的 24 中的步驟 6 到步驟 9。

VMware vCenter 的裝置組態

完成 OMIVV 基本安裝和 vCenter 註冊之後，再按一下 OMIVV 圖示，便會顯示**初始組態精靈**。您可以使用以下其中一種方法來設定應用裝置：

- 使用**初始組態精靈**設定裝置。
- 使用 OMIVV 中的**設定**標籤設定裝置。

您可以在第一次啟動時，使用**初始組態精靈**來進行 OMIVV 應用裝置設定。後續的執行個體，則使用**設定**標籤。

i 註：這兩種方法的使用者介面很類似。

主題：

- [透過組態精靈執行的組態工作](#)
- [透過「設定」標籤進行的設定工作](#)
- [建立機箱設定檔](#)

透過組態精靈執行的組態工作

i 註：如果您在變更 DNS 設定之後執行 OMIVV 相關工作時，發現 Web 通訊錯誤，請清除瀏覽器快取記憶體，並登出 Web 用戶端，然後再次登入。

您可以使用組態精靈來檢視和執行下列工作：

- 檢視組態精靈歡迎頁面
- 選取 vCenter。請參閱[選取 vCenter](#)。
- 建立連線設定檔。請參閱[建立連線設定檔](#)。
- 建立機箱設定檔。MX 機箱內的主機 (iDRAC IPv4 是在停用狀態) 必須使用機箱設定檔加以管理。請參閱[建立機箱設定檔](#) 第頁的 34。
- 設定事件與警報。請參閱[設定事件與警報](#)。
- 排程清查工作。請參閱[排程清查工作](#)。
- 執行保固擷取工作。請參閱[執行保固擷取工作](#)。

檢視組態精靈歡迎對話方塊

若要在安裝及註冊 vCenter 之後設定 OMIVV，請執行下列步驟來檢視**初始組態精靈**：

1. 在 vSphere Web 用戶端中，按一下**首頁**，然後按一下 **OpenManage Integration** 圖示。
您可以執行以下任何一個選項來存取初始組態精靈：
 - 第一次按一下 **OpenManage Integration** 圖示時，就會自動顯示**初始組態精靈**。
 - 從 **OpenManage Integration > 開始使用**，按一下**啟動初始組態精靈**。
2. 在**歡迎對話方塊**中檢閱步驟，然後按下一步。

選取 vCenter

您可以在 **vCenter 選擇**對話方塊中，設定以下 vCenter：

- 特定 vCenter
- 所有登錄的 vCenter

存取 **vCenter 選擇**對話方塊：

1. 在**初始組態精靈**的**歡迎對話方塊**中，按下一步。
2. 從 **vCenter** 下拉式清單中，選取一個 vCenter 或所有登錄的 vCenter。

選取尚未設定的 vCenter，或者如果您已在環境中新增了 vCenter。vCenter 選取頁面可讓您選取一或多個 vCenter 以進行設定。

3. 若要繼續連線設定檔說明對話方塊，請按下一步。

i 註: 如果您有多個屬於相同單一登入 (SSO) 的 vCenter 伺服器登錄了相同的 OMIVV 裝置，而且如果您選擇設定單一 vCenter 伺服器，則請重複步驟 1 至 3，直到設定好每一個 vCenter 為止。

建立連線設定檔

使用連線設定檔並搭配 Active Directory 認證之前，請先確定以下事項：

- Active Directory 使用者的帳戶存在於 Active Directory。
- iDRAC 和主機有針對 Active Directory 為基礎的驗證進行設定。

連線設定檔會儲存 OMIVV 用來與 Dell EMC 伺服器通訊的 iDRAC 和主機認證。每個 Dell EMC 伺服器均必須與連線設定檔建立關聯，OMIVV 才能加以管理。您可將多個伺服器指定至單一連線設定檔。您可以使用組態精靈或從 **OpenManage Integration for VMware vCenter > 設定標籤** 建立連線設定檔。您可以使用 Active Directory 認證登入 iDRAC 和主機。

i 註: iDRAC 與主機可以使用相同或個別的 Active Directory 認證。

i 註: 如果新增的主機數量超過建立連線設定檔的授權限制，則無法建立連線設定檔。

i 註: MX 機箱主機可以使用單一整合機箱管理 IP 加以管理。若要使用機箱設定檔來管理 MX 機箱，請參閱 [建立機箱設定檔](#)。Dell EMC 建議您使用 iDRAC IP 取得完整的 OMIVV 功能來管理 MX 機箱主機。

1. 在連線設定檔說明對話方塊中，按下一步。

2. 在連線設定檔名稱和認證對話方塊中，輸入連線設定檔名稱及選填的連線設定檔說明。

3. 在連線設定檔名稱和認證對話方塊的 **iDRAC 認證** 底下，根據是否利用 Active Directory 設定 iDRAC 來執行下列任一動作：

i 註: iDRAC 帳戶需要管理權限來更新韌體、套用硬體設定檔、在第 14 代伺服器中套用系統設定檔，以及部署 Hypervisor。

- 已經為 Active Directory 設定與啟用 iDRAC IP，而且您要在其中使用 Active Directory 時，請選取 **使用 Active Directory**；否則請向下捲動以設定 iDRAC 認證。
 - a. 在 Active Directory 的 **使用者名稱** 中，輸入使用者名稱。請以下列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。
 - b. 在 Active Directory **密碼** 中輸入密碼。密碼上限為 127 個字元。
 - c. 在 **確認密碼** 再次輸入密碼。
 - d. 請依需求執行下列其中一個動作：
 - 若要在所有未來連線時下載、儲存並驗證 iDRAC 憑證，請選取 **啟用憑證檢查**。
 - 若不在所有未來連線時儲存及進行 iDRAC 憑證檢驗，請清除 **啟用憑證檢查**。
- 若不用 Active Directory 設定 iDRAC 認證，請執行下列作業：
 - a. 在 **使用者名稱** 中，輸入使用者名稱。使用者名稱上限為 16 個字元。有關所用 iDRAC 版本的使用者名稱限制，請參閱 iDRAC 說明文件。
 - b. 在 **密碼** 中輸入密碼。密碼上限為 20 個字元。
 - c. 在 **確認密碼** 再次輸入密碼。
 - d. 執行下列其中一個動作：
 - 若要在所有未來連線時下載、儲存並驗證 iDRAC 憑證，請選取 **啟用憑證檢查**。
 - 若不在所有未來連線時儲存及進行 iDRAC 憑證檢驗，請清除 **啟用憑證檢查**。

4. 在 **主機根** 中執行下列其中一個步驟：

- 在您要使用 Active Directory 並已針對 Active Directory 完成設定及啟用的主機上，請選取 **使用 Active Directory** 並執行下列步驟；否則請設定您的主機認證：

i 註: 有關主機使用者名稱與網域的限制，請參閱以下資訊：

主機使用者名稱的需求：

- 長度介於 1 到 64 個字元
- 沒有不可列印字元

主機網域需求：

- 長度介於 1 到 64 個字元

- 第一個字元必須是字母。
- 不能包含空格。
- b. 在 Active Directory **密碼** 中輸入密碼。密碼上限為 127 個字元。
- c. 在**確認密碼**再次輸入密碼。
- d. 執行下列其中一個動作：
 - 若要在所有未來連線時下載、儲存並驗證主機憑證，請選取**啟用憑證檢查**。
 - 若不在所有未來連線時儲存及進行 iDRAC 憑證檢驗，請清除**啟用憑證檢查**。
- 若不用 Active Directory 設定主機認證，請執行下列作業：
 - a. 在**使用者名稱**中，使用者名稱為 **root**，這是預設的使用者名稱，您無法變更。然而，如果已設定 Active Directory，您可以選擇任何 Active Directory 使用者，而不只是 root。
 - b. 在**密碼**中輸入密碼。密碼上限為 127 個字元。
i 註: OMSA 認證與 ESXi 主機所使用的認證相同。
 - c. 在**確認密碼**再次輸入密碼。
 - d. 執行下列其中一個動作：
 - 若要在所有未來連線時下載、儲存並驗證主機憑證，請選取**啟用憑證檢查**。
 - 若不在所有未來連線時儲存及進行主機憑證檢驗，請清除**啟用憑證檢查**。
- 5. 按一下**下一步**。
- 6. 在**連線設定檔相關主機**對話方塊中，選取連線設定檔的主機，然後按一下**確定**。
i 註: 如果 OEM 主機沒有顯示在「選取主機」視窗中，請使用「新增 OEM 主機」精靈來新增 OEM 主機，請參閱 *使用者指南* 中的**新增 OEM 主機**主題。
- 7. 若要測試連線設定檔，請選取一或多個主機，然後按一下**測試連線**。
i 註: 這是自行選用的步驟，可檢查主機和 iDRAC 認證。雖然這並非必要步驟，Dell EMC 仍建議您測試連線設定檔。
i 註: 如果所有執行 ESXi 6.5 或更新版本的主機都停用 WBEM 服務，那麼當您對這些主機執行測試連線及清查時，WBEM 會自動啟用。
i 註: 如果您在建立連線設定檔時，選擇**所有註冊的 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。遇到這種情況時，建議您完成連線設定檔精靈動作、執行主機清查，然後再次測試連線設定檔。
i 註: 主機的測試連線可能會失敗，即使輸入有效認證，測試結果仍會指出輸入的認證無效。這可能是因為 ESXi 封鎖存取之故。請等候 15 分鐘後，再重試測試連線。
- 8. 若要完成設定檔建立，請按**下一步**。
 按一下「**下一步**」後，系統即會儲存您在此精靈中提供的所有詳細資訊，而您將無法從精靈修改此詳細資料。從組態精靈完成組態設定之後，您可以針對這項 vCenter 詳細資料，從**管理設定檔連線設定檔**頁面修改或建立更多連線設定檔。請參閱 *OpenManage Integration for VMware vCenter User's Guide* (OpenManage Integration for VMware vCenter 使用者指南) 中的**修改連線設定檔** (Dell.com/support/manuals)。

i 註: 若為不具備 iDRAC Express 或 Enterprise 卡的伺服器，iDRAC 測試連線結果不適用於此系統。

主機新增至連線設定檔之後，OMIVV 的 IP 位址會自動設定為主機 iDRAC 的 SNMP 陷阱目的地，而 OMIVV 會針對執行 ESXi 6.5 及更新版本的主機，自動啟用 Web 架構企業管理 (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 陷阱目的地失敗，及/或為特定主機啟用 WBEM 服務失敗，則那些主機列為不相容。若要檢視需要重新設定 SNMP 陷阱目的地及/或啟用 WBEM 服務的不相容主機，請參閱 *OpenManage Integration for VMware vCenter User's Guide* (OpenManage Integration for VMware vCenter 使用者指南) 中的**報告與修復 vSphere 主機的相容性**主題，網址為：Dell.com/support/manuals。

排程清查工作

您可以使用組態精靈或 OpenManage Integration，在 **OpenManage Integration > 管理 > 設定標籤** 之下設定清查排程。

i 註: 建議您排程定期清查工作，以確保 OMIVV 持續顯示最新資訊。清查工作僅耗用最少的資源，不會降低主機效能。

i 註: 在執行所有主機的清查後，即會自動探索機箱。如果機箱已新增至機箱設定檔，即會自動執行機箱清查。在具備多個 vCenter 伺服器的 SSO 環境中，只要有任何 vCenter 的清查在排定的時間執行，就會自動執行每個 vCenter 的機箱清查。

i 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**初始組態精靈**中，請從**清查時程**對話方塊選取**啟用清查資料擷取** (如果尚未啟用)。預設已啟用**啟用清查資料擷取**。
2. 請在**清查資料擷取排程**底下，執行下列步驟：
 - a. 針對想要執行庫存的當週內任何一天，選取旁邊的核取方塊。
預設選取**所有日期**。
 - b. 在**資料擷取時間**中，以小時:分鐘格式輸入時間。
您輸入的時間是您的當地時間。因此，如果想在虛擬設備時區執行清查，請計算當地和虛擬設備時區之間的時間差，然後相應輸入時間。
 - c. 若要套用變更並繼續進行，請按**下一步**。
按一下「**下一步**」後，系統即會儲存您在此精靈中提供的所有詳細資訊，而您將無法從此精靈修改此詳細資料。從組態精靈完成設定後，您可以從**管理 > 設定**標籤修改主機的清查查排程詳細資料。請參閱《*OpenManage Integration for VMware vCenter User's Guide*》(OpenManage Integration for VMware vCenter 使用者指南) 中的**修改清查工作排程**，網址是：Dell.com/support/manuals。

執行保固擷取工作

保固擷取工作組態可自 OMIVV 中的「**設定**」標籤取得。此外，您也可以從**工作佇列 > 保固**執行或排程保固擷取工作。排定的工作會列在工作佇列中。在具備多個 vCenter Server 的 SSO 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**保固排程**對話方塊中，選取**啟用保固資料擷取**。
2. 在**保固資料擷取排程**中執行下列步驟：
 - a. 選取您要執行保固那幾天旁的核取方塊。
 - b. 以小時:分鐘格式輸入時間。
您輸入的時間是您的當地時間。因此，如果想在虛擬設備時區執行清查，請計算當地和虛擬設備時區之間的時間差，然後相應輸入時間。
3. 若要套用變更並繼續，請按**下一步**，然後繼續進行**事件與警報**設定。
按「**下一步**」之後，所有您在此精靈中提供的詳細資訊就會儲存起來，而且您無法從精靈修改這些詳細資料。在組態精靈完成設定之後，您就可以從**設定**標籤修改保固工作排程。請參閱《*OpenManage Integration for VMware vCenter User's Guide*》(OpenManage Integration for VMware vCenter 使用者指南) 中的**修改保固工作排程**，網址是：Dell.com/support/manuals。

設定事件與警報

您可以使用**初始組態精靈**，或從事件和警報的**設定**標籤來設定事件和警報。若要從伺服器接收事件，請將 OMIVV 設定為陷阱目的地。若為第 12 代及更新版本主機，必須在 iDRAC 中設定 SNMP 陷阱目的地。若為第 12 代以前的主機，則必須在 OMSA 中設定陷阱目的地。


註：對於第 12 代主機及更新版本主機，OMIVV 支援 SNMP v1 和 v2 警報，對於第 12 代以前的主機，則僅支援 SNMP v1 警報。


1. 在**初始組態精靈的事件張貼等級**，選取下列其中之一：
 - 不張貼任何事件 — 封鎖硬體事件
 - 張貼所有事件 — 張貼所有的硬體事件
 - 只張貼嚴重事件和警告事件 — 只張貼嚴重或警告等級的硬體事件
 - 只張貼與虛擬化有關的嚴重事件和警告事件 — 只張貼與虛擬化有關的嚴重事件和警告事件，這是預設的事件張貼等級
2. 若要啟用所有硬體警報和事件，請選取**啟用所有 Dell EMC 主機的警報**。
註：已啟用警報的 Dell EMC 主機會以進入維護模式的方式回應某些特定嚴重事件，您可以視需要修改警報。
啟用 **Dell EMC 警示警告**對話方塊隨即顯示。
3. 若要接受變更，請按一下**繼續**，若要取消變更，則按一下**取消**。
註：請務必只在您選取**啟用所有 Dell EMC 主機的警報**時才完成這個步驟。
4. 若要還原所有受管 Dell EMC 伺服器的預設 vCenter 警報設定，請按一下**還原預設警報**。
變更生效可能需時一分鐘。
註：還原裝置後，不會啟用事件與警報設定 (即使 GUI 顯示為已啟用)。您可以從**設定**標籤再次啟用**事件與警報**標籤。

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

5. 按一下**套用**。

設定 SNMP 設陷社群字串

1. 在 **OpenManage Integration for VMware vCenter** 頁面的**管理 > 設定**標籤上，於**裝置設定**下，針對 **OMSA SNMP 設陷社群字串** 按一下 。
OMSA SNMP 設陷社群字串設定對話方塊隨即顯示。根據預設，**public** 會顯示在 SNMP 設陷社群字串中。
2. 將 **public** 文字自訂為任何字串，然後按一下**套用**。

 **註:** 第 11 代 PowerEdge 伺服器的 SNMP 設陷社群字串於透過 OMIVV 安裝或升級 OMSA 時設定。

透過「設定」標籤進行的設定工作

您可以使用「設定」標籤檢視並執行下列組態工作：


- 啟用 OMSA 連結。請參閱 [啟用 OMSA 連結](#)。
- 進行保固到期通知設定。請參閱 [進行保固到期通知設定](#)。
- 設定韌體更新儲存庫。請參閱 [設定韌體更新儲存庫](#)。
- 設定最新應用裝置版本通知。請參閱 [設定最新應用裝置版本通知](#)。
- 設定與檢視事件和警報。請參閱 [設定事件與警報](#)。
- 檢視清查和保固的資料擷取排程。請參閱 [檢視清查和保固的資料擷取排程](#)。

裝置設定

在本節中會設定 OMIVV 裝置的下列項目：


- 保固到期通知
- 韌體更新儲存庫
- 最新裝置版本通知
- 部署認證

進行保固到期通知設定

1. 在 **OpenManage Integration for VMware vCenter** 的**管理 > 設定**標籤上，按一下**裝置設定**下的**保固過期通知**。
2. 展開**保固過期通知**即可檢視下列項目：
 - **保固過期通知** — 無論設定是啟用還是停用
 - **警告** — 第一個警告設定的天數
 - **嚴重** — 嚴重警告設定的天數
3. 若要設定保固到期相關警告的保固到期閾值，請按一下**保固過期通知**右側的  圖示。
4. 請在**保固過期通知**對話方塊中執行下列步驟：
 - a. 如果您要啟用這項設定，請選取**對於主機啟用保固過期通知**。
選取此核取方塊可啟用保固到期通知。
 - b. 在**最少天數閾值**警示下，執行下列步驟：
 - i. 在**警告**下拉式清單中，選取發出保固過期前警告的天數。
 - ii. 在**嚴重**下拉式清單中，選取發出保固過期前警告的天數。
5. 按一下**套用**。

設定韌體更新儲存庫

您可以在 OMIVV **設定**標籤上設定韌體更新儲存庫。

 **註:** 您可以使用此儲存庫，只為非 vSAN 主機與叢集的韌體更新。

1. 在 OpenManage Integration for VMware vCenter 的 **管理 > 設定標籤的裝置設定** 下方，按一下 **韌體更新儲存庫** 右側的  圖示。
2. 在 **韌體更新儲存庫** 對話方塊中，選取下列其中一個選項：
 - **Dell Online** — 韌體更新預設儲存庫是設定為 Dell Online (<https://downloads.dell.com>)。OMIVV 會從 Dell 儲存庫下載所選的韌體更新，並更新管理的主機。
 - **Dell 線上自訂** — OMIVV 會從「Dell 線上自訂」下載所選的韌體更新，並視需要套用到管理的主機上。
 -  **註:** 如果網路需要 Proxy，請根據網路設定來啟用 Proxy 設定。
 - **共用網路資料夾** — 您可以在 CIFS 型或 NFS 型網路共用具有本機韌體儲存庫。此儲存庫可以是 Dell 定期推出的伺服器更新公用程式 (SUU) 傾印，或是使用 DRM 的自訂儲存庫。此網路共用應供 OMIVV 存取。
 -  **註:** 如果您使用 CIFS 共用，儲存庫的密碼不能超過 31 個字元。
 -  **註:** 請確定您使用最新的 Dell EMC Repository Manager (DRM) 版本 (3.0) 及更新版本。
 - a. 如果選取 **Dell 線上自訂**，請使用以下格式輸入目錄線上路徑：
 - `http://share/filename.xml.gz`
 - `http://share/filename.gz`
 - `https://share/filename.xml.gz`
 - `https://share/filename.gz`
 - b. 如果選取 **共用網路資料夾**，請使用以下格式輸入目錄檔案位置：
 - .XML 檔案的 NFS 共用 — `host:/share/filename.xml`
 - .gz 檔案的 NFS 共用 — `host:/share/filename.gz`
 - .XML 檔案的 CIFS 共用 — `\\host\share\filename.xml`
 - .gz 檔案的 CIFS 共用 — `\\host\share\filename.gz`
 -  **註:** OMIVV 只支援以伺服器訊息區塊 (SMB) 1.0 版和 SMB 2.0 版為基礎的 CIFS 共用。Dell EMC 建議使用 SMB 2.0 版為基礎的 CIFS 共用。
 -  **註:** 如果您使用的是 CIFS 共用，OMIVV 會提示您輸入使用者名稱和密碼。
 - c. 若要驗證指定的目錄檔案位置，請按一下 **開始測試**。您必須先執行這項驗證，才能繼續進行。
 -  — 代表測試連線已順利完成。
 -  — 代表測試連線以失敗告終。
3. 按一下 **套用**。
 -  **註:** 要從來源讀取目錄並更新 OMIVV 資料庫，可能需要最多 10 分鐘的時間。


使用 OMIVV 在 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. 在「首頁」中，按一下 **新增儲存庫**。
新增儲存庫 視窗隨即顯示。
2. 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**。
3. 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。
4. 若要匯出目錄，請選取目錄，然後按一下 **匯出**。


設定最新裝置版本通知


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 OpenManage Integration for VMware vCenter 的**管理** → **「設定」** 標籤上，於**應用裝置設定**底下的**最新版本通知**右側，按一下圖示。
預設停用最新版本通知。
2. 在**最新版本通知與擷取排程**對話方塊中，執行下列動作：
 - a. 如果您要啟用最新版本通知，請選取**啟用最新版本通知**核取方塊。
 - b. 在**最新版本擷取排程**之下，選取一週哪幾天要工作。
 - c. 在**最新版本擷取時間**中，指定所需的當地時間。
您提供的時間是您的當地時間。請務必計算所有時差，好讓 OMIVV 裝置能夠在適當的時間執行這項工作。
3. 若要儲存設定，請按一下**套用**，若要重設這些設定，請按一下**清除**，若要中止作業，請按一下**取消**。

設定部署認證

部署認證可讓您設定認證，藉此與使用自動探索功能探索到的裸機系統進行安全通訊，直到作業系統部署完成。為了與 iDRAC 進行安全通訊，OMIVV 從開始探索到部署程序結束為止，都會使用部署認證。作業系統部署程序順利完成之後，OMIVV 便會將 iDRAC 認證改為如連線設定檔所提供。如果您變更部署認證，則之後所有新探索到的系統，都會以新認證加以佈建。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。

 **註：** 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。

1. 在 OpenManage Integration for VMware vCenter 中，**管理** > **設定** 標籤的**應用裝置設定**底下，**部署認證**的右方，按一下圖示。
2. 在**裸機伺服器部署的認證**的**認證**底下，輸入下列各項的值：
 - 在**使用者名稱**文字方塊中，輸入使用者名稱。
使用者名稱請勿超過 16 個字元 (僅限使用 ASCII 可列印字元)。
 - 在**密碼**文字方塊中，輸入密碼。
密碼請勿超過 20 個字元 (僅限使用 ASCII 可列印字元)。
 - 在**確認密碼**文字方塊中，再次輸入密碼。
請確定密碼相符。
3. 若要儲存指定的認證，請按一下**套用**。

vCenter 設定


在本節中，設定下列 vCenter 設定：

- 啟用 OMSA 連結。請參閱[啟用 OMSA 連結](#)。
- 設定事件與警報。請參閱[設定事件與警報](#)。
- 設定清查與保固的資料擷取排程。請參閱[檢視清查和保固的資料擷取排程](#)。

啟用 OMSA 連結

在啟用 OMSA 連結前，先安裝和設定 OMSA Web 伺服器。請參閱使用中 OMSA 版本的《OpenManage Server Administrator Installation Guide》(OpenManage Server Administrator 安裝指南)，以取得安裝和設定 OMSA Web 伺服器的指示。

 **註：** 只有 PowerEdge 第 11 代伺服器才需要 OMSA。

1. 在 OpenManage Integration for VMware vCenter 中，**管理** > **設定** 標籤的**vCenter 設定**底下，於 OMSA Web 伺服器 URL 的右方按一下圖示。
2. 在**OMSA Web 伺服器 URL** 對話方塊中輸入 URL。
請務必輸入完整的 URL，以及 HTTPS 和連接埠號碼 1311。
`https://<OMSA 伺服器 IP 或 fqdn>:1311`

3. 若要將 OMSA URL 套用至所有的 vCenter 伺服器，請選取將這些設定套用到所有 vCenter。

i 註: 如果沒有選取這個核取方塊，OMSA URL 只會套用到一個 vCenter。

4. 若要確認您提供的 OMSA URL 連結有效，請瀏覽至主機の摘要標籤，並檢查 OMSA 主控台連結是否在 **OMIVV 主機資訊** 區段中。

設定事件與警報


事件與警報對話方塊可啟用或停用所有的硬體警報。目前的警報狀態會顯示於 vCenter 警報標籤上。嚴重事件表示實際或即將發生的資料遺失或系統故障。警告事件未必重大，但表示未來可能會有問題。

此外還可以使用 VMware 警報管理員來啟用事件與警報。事件會顯示在主機與叢集檢視中的 vCenter 工作和事件標籤上。若要從伺服器接收事件，要將 OMIVV 設定為 SNMP 陷阱目的地。針對第 12 代之前的主機，SNMP 陷阱目的地是在 iDRAC 中設定。針對第 12 代之前的主機，陷阱目的地則是在 OMSA 中設定。您可以在**管理 > 設定**標籤內，使用 OpenManage Integration for VMware vCenter 來設定事件與警報。在 vCenter **設定**之下，展開**事件與警報**標題來顯示 Dell 主機の vCenter 警報 (啟用或停用) 以及事件張貼等級。

i 註: 若為第 12 代及之後的主機，OMIVV 支援 SNMP v1 和 v2 警示。若為第 12 代之前的主機，則 OMIVV 支援 SNMP v1 警示。

i 註: 若要接收 Dell 事件，必須啟用警報和事件。

1. 在 OpenManage Integration for VMware vCenter 中，**管理 > 設定**標籤的 **vCenter 設定** 底下，展開**事件與警報**。顯示目前 **Dell EMC 主機の vCenter 警報** (啟用或停用) 或所有 vCenter 警報和事件張貼等級。

2. 按一下**事件與警報**右側的  圖示。

3. 若要啟用所有硬體警報和事件，請選取**啟用所有 Dell EMC 主機の警報**。

i 註: 已啟用警報的 Dell EMC 主機會以進入維護模式的方式回應嚴重事件，您可以視需要修改警報。

4. 若要還原所有受管 Dell 伺服器の預設 vCenter 警報設定，請按一下**還原預設警示**。
此步驟可能需一分鐘才能讓變更生效，而且只有在選取**啟用 Dell EMC 主機の警報**時才能使用。

5. 在**事件張貼等級**中，選取「不張貼任何事件」、「張貼所有事件」、「只張貼關鍵及警告事件」或「僅張貼虛擬相關的關鍵事件與警告事件」。如需詳細資訊，請參閱《OpenManage Integration for VMware vCenter User's Guide》(OpenManage Integration for VMware vCenter 使用者指南) 中的**事件、警報及健全狀況監控**一節。

6. 如果您要將這些設定套用到所有 vCenter，請選取將這些設定套用到所有 vCenter。

i 註: 選取此選項會覆寫所有 vCenter 的現有設定。

i 註: 如果您已從**設定**標籤上的下拉式清單選取**所有已註冊的 vCenter**，則此選項無法使用。

7. 若要儲存，按一下**套用**。

檢視清查和保固的資料擷取排程

1. 在 OpenManage Integration for VMware vCenter 的**管理 > 設定**標籤上，按一下 **vCenter 設定** 下的**資料擷取排程**。按一下之後，便會展開資料擷取排程，顯示清查與保固的編輯選項。

2. 針對**清查擷取**或**保固擷取**，按一下  圖示。
在**清查/保固資料擷取**對話方塊中，您可以檢視清查或保固擷取的以下資訊：

- 清查及/或保固擷取選項已啟用或停用？
- 星期幾啟用。
- 幾點啟用。

3. 若要編輯資料擷取排程，請執行下列步驟：

a. 在**清查/保固資料**底下，選取**啟用清查/保固資料擷取**核取方塊。

b. 在**清查/保固資料擷取排程**底下，選取一週哪幾天要工作。

c. 在**清查/保固資料擷取時間**文字方塊中，輸入此工作的當地時間。

您可能必須考慮工作設定和工作實作之間的時間差。

d. 若要儲存設定，請按一下**套用**，若要重設這些設定，請按一下**清除**，若要中止作業，請按一下**取消**。

4. 再次按一下**資料擷取排程**，將清查與保固排程縮成單一列。

建立機箱設定檔

要監控機箱，必須有機箱設定檔。您可以使用一或多個機箱來建立機箱認證設定檔，並與設定檔建立關聯。

您可以使用 Active Directory 認證登入 iDRAC 和主機。

1. 在 OpenManage Integration for VMware vCenter 中按一下**管理**。
2. 按一下**設定檔**，然後按一下**認證設定檔**。
3. 展開**認證設定檔**，然後按一下**機箱設定檔**標籤。

4. 在**機箱設定檔**頁面按一下  圖示，以建立新機箱設定檔。


5. 在**機箱設定檔精靈**頁面上，請執行下列動作：


在**機箱設定檔**底下的**名稱及認證**區段中：


- a. 在**設定檔名稱**文字方塊中，輸入設定檔名稱。
- b. 在**說明**文字方塊中輸入說明 (選填)。

在**認證**區段底下：

- a. 在**使用者名稱**文字方塊中，輸入有管理權限的使用者名稱 (通常用於登入機箱管理控制器)。
- b. 在**密碼**文字方塊中，輸入相對應使用者名稱的密碼。
- c. 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。

 **註:** 認證可以是本機認證或 Active Directory 認證。如果要搭配機箱設定檔使用 Active Directory 認證，Active Directory 中必須先有 Active Directory 使用者帳戶，而且必須先針對 Active Directory 型驗證設定機箱管理控制器。

6. 按一下  在機箱與機箱設定檔之間建立關聯。

 **註:** 使用**新增 MX 機箱**接受探索、有效提供，以及手動新增的機箱，其下任何模組化主機成功執行清查後，該機箱才能與機箱設定檔建立關聯。

7. 若要選取個別機箱或多個機箱，請選取 **IP/ 主機名稱**欄旁相對應的核取方塊。

如果所選的機箱已屬於另一個設定檔，便會出現警告訊息，指出所選的機箱已與某個設定檔相關聯。

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。


8. 按一下**確定**。


關聯機箱頁面隨即顯示。


9. 所選機箱必須進行測試連線，且會自動執行。


自動執行測試連線的時機：

- 選取機箱後會第一次執行
- 變更認證後
- 重新選取機箱後

 **註:** 如果是 MCM 群組設定的 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**。按一下主要機箱的 IP 連結，探索完整的 MCM 群組。

測試結果欄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 。

 **註:** 如果註冊的 vCenter 中沒有任何主機與新增的 MX 機箱相關聯，則各自的機箱測試連線便會失敗。

 **註:** 只有成功通過驗證的機箱會與機箱設定檔建立關聯。

10. 若要完成設定檔，請按一下**完成**。

 **註:** 您必須至少有一個驗證成功的機箱才能完成精靈。

若要新增 MX 機箱管理模組 IP，請參閱 *使用者指南*中的**新增 MX 機箱 IP 或 FQDN**主題。

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 和 Dell EMC Lifecycle Controller 文件 — www.dell.com/idracmanuals
- Dell EMC OpenManage Connections 企業系統管理文件 — www.dell.com/OMConnectionsEnterpriseSystemsManagement
- Dell EMC 檢修性工具文件 — www.dell.com/ServiceabilityTools
- 1. 造訪 www.dell.com/Support/Home。
- 2. 按一下**從所有產品選擇**。
- 3. 從**所有產品**區段中，按一下**軟體和安全性**，然後按一下以下所需的連結：
 - **企業系統管理**
 - **遠端企業系統管理**
 - **檢修性工具**
 - **Dell 用戶端命令套件**
 - **Connections 用戶端系統管理**
- 4. 若要檢視文件，按一下所需的產品版本。
- 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 [Dell.com/support](https://www.dell.com/support) 存取其他指南。按一下**從所有產品中選擇**，然後按一下**軟體和安全性 > 虛擬化解決方案**。按一下 **OpenManage Integration for VMware vCenter 4.3** 以存取下列文件：

- *OpenManage Integration for VMware vCenter Version 4.3 Web Client User's Guide (OpenManage Integration for VMware vCenter 4.3 版 Web 用戶端使用者指南)*
- *OpenManage Integration for VMware vCenter Version 4.3 Release Notes (OpenManage Integration for VMware vCenter 4.3 版本資訊)*
- *OpenManage Integration for VMware vCenter Version 4.3 Compatibility Matrix (OpenManage Integration for VMware vCenter 4.3 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。