

OpenManage Integration for VMware vCenter 4.2 版

Web 用戶端使用者指南

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	9
此版本的新功能.....	9
OpenManage Integration for VMware vCenter 功能.....	9
章 2: 關於管理主控台	11
使用管理入口網站.....	11
以非管理員使用者的身分登錄 vCenter Server.....	11
登錄 vCenter Server.....	13
上傳授權至管理入口網站.....	14
管理虛擬裝置.....	15
設定全域警示.....	19
管理備份和還原.....	19
關於 vSphere 用戶端主控台.....	20
章 3: 管理多個裝置	23
章 4: 從 Web 用戶端存取 OpenManage Integration	24
在 VMware vCenter Web 用戶端中瀏覽.....	24
Web 用戶端中的圖示.....	24
尋找軟體版本.....	25
重新整理畫面內容.....	25
檢視 Dell EMC 主機.....	25
檢視 OpenManage Integration for VMware vCenter 授權標籤.....	26
存取說明與支援.....	26
下載疑難排解套件組合.....	27
重設 iDRAC.....	27
開啟線上說明.....	27
啟動管理主控台.....	28
檢視記錄歷史記錄.....	28
檢視記錄.....	29
匯出記錄檔.....	29
章 5: OpenManage Integration for VMware vCenter 授權	30
購買並上傳軟體授權.....	30
章 6: VMware vCenter 的裝置組態	31
透過組態精靈執行的組態工作.....	31
檢視組態精靈歡迎對話方塊.....	31
選取 vCenter.....	31
建立連線設定檔.....	32
排程清查工作.....	33
執行保固擷取工作.....	34
設定事件與警報.....	34
透過「設定」標籤進行的設定工作.....	34

裝置設定.....	35
vCenter 設定.....	36
章 7: 使用「基準」標籤.....	39
儲存庫設定檔.....	39
建立儲存庫設定檔.....	40
編輯儲存庫設定檔.....	40
刪除儲存庫設定檔.....	41
叢集設定檔.....	41
建立叢集設定檔.....	41
編輯叢集設定檔.....	42
刪除叢集設定檔.....	42
章 8: 設定檔.....	43
關於連線設定檔.....	43
檢視連線設定檔.....	43
建立連線設定檔.....	44
修改連線設定檔.....	45
刪除連線設定檔.....	46
測試連線設定檔.....	47
關於機箱設定檔.....	47
檢視機箱設定檔.....	47
建立機箱設定檔.....	47
編輯機箱設定檔.....	48
刪除機箱設定檔.....	48
測試機箱設定檔.....	49
章 9: 清查和保固管理.....	50
清查工作.....	50
檢視主機清查.....	50
檢視機箱清查.....	51
修改清查工作排程.....	52
執行清查工作.....	52
立即執行機箱清查工作.....	52
保固工作.....	53
檢視保固歷史記錄.....	53
檢視機箱保固.....	54
修改保固工作排程.....	54
立即執行主機保固工作.....	54
立即執行機箱保固工作.....	55
監控單一主機.....	55
檢視主機摘要詳細資料.....	55
檢視單一主機的硬體詳細資料.....	57
檢視單一主機的儲存裝置詳細資料.....	58
關於 Web 用戶端中的系統事件記錄.....	60
檢視單一主機的其他硬體詳細資料.....	61
監控叢集與資料中心上的主機.....	61
檢視資料中心和叢集的概觀.....	62
檢視資料中心和叢集的硬體詳細資料.....	63

檢視資料中心和叢集的儲存裝置詳細資料.....	64
檢視資料中心和叢集的其他硬體詳細資料.....	66
設定實體伺服器閃爍指示燈.....	67
設定系統鎖定模式.....	67
章 10: 事件、警報及健全狀況監控.....	69
關於主機的事件與警報.....	69
關於機箱的事件與警報.....	70
檢視機箱事件.....	70
檢視機箱警報.....	70
虛擬化相關事件.....	70
主動式 HA 事件.....	75
檢視警報和事件設定.....	76
檢視事件.....	77
硬體元件冗餘健全狀況 — 主動式 HA.....	77
為機架式和直立式伺服器設定主動式 HA.....	77
在叢集上啟用主動式 HA.....	78
覆寫狀況更新通知的重要性.....	78
啟動管理主控台.....	79
啟動遠端存取主控台.....	79
啟動 OMSA 主控台.....	79
啟動機箱管理控制器主控台.....	79
章 11: 關於韌體更新.....	81
執行非 vSAN 主機的韌體更新.....	81
為 vSAN 主機執行韌體更新精靈.....	83
執行非 vSAN 叢集的韌體更新精靈.....	84
執行 vSAN 叢集的韌體更新精靈.....	85
章 12: 機箱管理.....	88
檢視機箱摘要詳細資料.....	88
檢視機箱的硬體清查資訊.....	89
檢視機箱的其他硬體組態.....	90
檢視機箱的關聯主機.....	92
章 13: 部署 Hypervisor.....	93
裝置探索.....	94
手動探索.....	94
OpenManage Integration for VMware vCenter 中的自動探索.....	94
移除裸機伺服器.....	97
佈建.....	97
系統設定檔.....	97
建立系統設定檔.....	98
管理系統設定檔.....	99
設定硬體設定檔.....	99
在參照伺服器上啟用 CSIOR.....	100
建立或自訂硬體設定檔.....	100
建立或複製硬體設定檔.....	102
管理硬體設定檔.....	102

建立 Hypervisor 設定檔.....	102
管理 Hypervisor 設定檔.....	103
建立部署範本.....	103
管理部署範本.....	104
關於部署精靈.....	104
VLAN 支援.....	104
執行部署精靈.....	105
使用工作佇列來管理部署工作.....	107
管理韌體更新工作.....	108
部署工作時間.....	109
下載自訂的 Dell EMC ISO 映像.....	110
章 14: 關於主機、裸機和 iDRAC 相容性.....	111
報告與修復 vSphere 主機的相容性.....	111
修復 vSphere 主機的 iDRAC 授權相容性.....	112
檢視基準相容性.....	112
使用 OMSA 搭配第 11 代伺服器.....	113
在 ESXi 系統上部署 OMSA 代理程式.....	113
設定 OMSA 設陷目的地.....	114
報告及修正裸機伺服器的相容性.....	114
修正裸機伺服器的 iDRAC 授權相容性.....	115
重新整理裸機伺服器.....	115
章 15: 安全性角色與權限.....	116
資料完整性.....	116
存取控制驗證、授權與角色.....	116
Dell 操作角色.....	116
Dell 基礎結構部署角色.....	117
關於權限.....	117
章 16: 常見問題集 - FAQ.....	119
常見問題集 - FAQ.....	119
在 Google Chrome 中，「全部匯出」按鈕無法匯出為 .CSV 檔案.....	119
不相容的 vSphere 主機會顯示不正確的 iDRAC 授權類型和說明.....	119
從舊版 OMIVV 取消登錄 vCenter，接著使用較新 OMIVV 版本登錄相同的 vCenter 後，Dell EMC 圖 示沒有顯示.....	119
Dell 供應商並未顯示為健康狀況更新供應商.....	120
在 ESXi 5.x 主機上執行韌體更新工作時，清查工作會失敗.....	120
由於無效或未知的 iDRAC IP，導致主機清查或測試連線失敗。.....	120
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」.....	120
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.....	120
在嘗試以嚴重性類別篩選時，OMIVV 並未顯示所有相關記錄.....	121
我該如何解決因 VMware 憑證發行單位 (VMCA) 所導致的錯誤代碼 2000000.....	121
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.....	124
從「工作佇列」頁面選取時，保固和清查排程未套用到所有的 vCenter.....	124
如果在 OMIVV 變更 DNS 設定後，vCenter Web 用戶端出現 Web 通訊錯誤，我該如何做.....	125
若瀏覽到其他頁面再返回「設定」頁面，「設定」頁面就無法載入.....	125
在初始組態精靈的「清查排程與保固排程」頁面上，出現「不能將工作排程在過去的時間」錯誤.....	125
韌體頁面上有些韌體的安裝日期顯示為 1969 年 12 月 31 日.....	125

連續全域重新整理會在最近的工作視窗中擲出例外。.....	125
使用 IE 10 時，為什麼有些 Dell 畫面的 Web 用戶端 UI 會扭曲.....	125
我已向 vCenter 成功登錄外掛程式，但在 Web 用戶端上看不到 OpenManage Integration 圖示.....	126
即使儲存庫中有所選第 11 代系統的套件組合，韌體更新卻顯示沒有套件組合可供韌體更新使用.....	126
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？.....	126
不支援使用 OMIVV 來更新搭載 13.5.2 版韌體的 Intel 網路卡.....	126
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.....	126
使用無效的 DUP 來更新韌體時，雖然 LC 內的工作狀態顯示為「失敗」，但是 vCenter 主控台上的硬體更新工作狀態卻不是失敗，也不是逾時數小時。為什麼會這樣.....	127
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.....	127
為什麼執行一對多韌體更新時，系統沒有進入維護模式.....	127
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」.....	127
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」.....	127
OMIVV 在連結模式中是否支援 vCenter.....	127
OMIVV 有哪些必要的連接埠設定.....	127
成功套用硬體設定檔或系統設定檔 (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.....	129
看不到列在 vCenter 主機與叢集頁面上的新 iDRAC 版本詳細資料.....	129
如何使用 OMSA 模擬溫度硬體故障，來測試事件設定.....	129
我明明已將 OMSA 代理程式安裝在 OMIVV 主機系統上了，卻還是收到錯誤訊息，說 OMSA 尚未安裝。.....	130
OMIVV 是否能在已啟用鎖定模式的情況下支援 ESXi.....	130
我試圖使用鎖定模式卻失敗.....	130
使用參照伺服器時無法建立硬體設定檔.....	130
嘗試在伺服器上部署 ESXi 時失敗.....	130
Hypervisor 無法部署在 Dell PowerEdge R210 II 機器上.....	130
部署精靈在顯示自動探索到的系統時，沒有顯示機型資訊.....	130
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.....	131
我要如何從 vCenter 強制移除虛擬應用裝置.....	131
在立即備份畫面輸入密碼時收到錯誤訊息.....	131
在 vSphere Web 用戶端按一下「Dell 伺服器管理 Portlet」或 Dell 圖示，結果傳回 404 錯誤.....	131
韌體更新失敗時該怎麼辦.....	131
vCenter 登錄失敗時該怎麼辦.....	131
連線設定檔測試認證時效能緩慢或沒有回應.....	131
OMIVV 是否支援 VMware vCenter Server 應用裝置.....	132
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.....	132
主機已從 vCenter 樹狀結構移除，卻仍然顯示在機箱下.....	132
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.....	132
在備份及還原 OMIVV 後，警報設定沒有還原.....	132
NPAR 若是在目標節點上啟用但在系統設定檔上停用，Hypervisor 部署會失敗.....	132
當可用版本比目前版本舊時，可用的虛擬裝置版本會顯示錯誤的資訊.....	133
當新增具有 Express 授權的第 12 代裸機伺服器時，會擲出 267027 例外狀況.....	133
在第 14 代上部署 OS 期間，硬體設定檔會因 iDRAC 錯誤而套用失敗.....	133
當 Proxy 設定有網域使用者驗證時，OMIVV RPM 升級會失敗.....	133
無法套用 FX 機箱中有 PCIe 卡的系統設定檔.....	133
裸機部署問題.....	133
在新購買的系統上啟用自動探索.....	134

章 17: 相關說明文件.....135

從 Dell EMC 支援網站存取文件.....	135
附錄 A：系統專有屬性.....	136
附錄 B：自訂屬性.....	140
附錄 C：其他資訊.....	141
附錄 D：元件與基準版本比較表.....	142

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) 可提供強化的部署、管理、監控和升級等功能，讓您從 VMware 用戶端更有效地管理 Dell 主機。

主題：

- [此版本的新功能](#)
- [OpenManage Integration for VMware vCenter 功能](#)

此版本的新功能

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

- 現有的叢集感知更新已增強，可支援 vSAN 叢集。支援驅動程式和韌體更新。
- 能夠針對驅動程式、韌體及硬體的組態與漂移偵測設定 vSAN 叢集基準
- 能夠包含/排除系統設定檔屬性
- 支援第 14 代平台
- 支援 SMB2 CIFS 共用
- 支援 OMSA 9.1
- 支援 vSphere 6.7

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： <ul style="list-style-type: none"> • PowerEdge 伺服器詳細資料，例如記憶體（數量和類型）、NIC、PSU、處理器、RAC、保固資訊、伺服器、叢集，以及資料中心層級檢視 • 機箱詳細資料，例如機箱管理控制器資訊、機箱電源供應器、KVM 狀態、風扇/散熱詳細資料、保固資訊、空的交換器/伺服器詳細資料。
監視並傳送警示	監視與警示包含下列功能： <ul style="list-style-type: none"> • 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問題。 • 支援 VMware 主動式 HA 功能。
韌體更新	韌體更新包括以下各項： <ul style="list-style-type: none"> • 將 Dell EMC 硬體更新為最新版的 BIOS 和韌體。 • 目前的叢集感知更新功能已增強，可在啟用 DRS 選項時支援 vSAN 叢集。增強功能亦支援更新 vSAN 叢集的驅動程式和韌體。
部署與佈建	使用 VMware vCenter（而不使用 PXE），在裸機 PowerEdge 伺服器上建立硬體設定檔（第 11 代到第 13 代 PowerEdge 伺服器）、系統設定檔（第 14 代伺服器）、Hypervisor 設定檔，以及遠端部署 OS。

表 1. OMIVV 功能 (續)

功能	說明
服務資訊	從 Dell 的保固資料庫擷取 Dell EMC 伺服器及其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： <ul style="list-style-type: none">● 整合標準 vCenter 驗證、規則和權限。● 在第 14 代伺服器支援 iDRAC 鎖定模式。

 註: 從 OMIVV 4.0 版開始，OMIVV 只支援 VMware vSphere Web 用戶端，而不支援 vSphere Desktop 用戶端。

 註: 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。

關於管理主控台

您只要善用以下兩個管理入口網站，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)

主題：

- [使用管理入口網站](#)

使用管理入口網站

您可以使用管理入口網站執行下列工作：


- 登錄 vCenter 伺服器。請參閱[登錄 vCenter 伺服器](#)。
- 修改 vCenter 登入認證。請參閱[修改 vCenter 登入認證](#)。
- 更新 SSL 憑證。請參閱[更新已登錄 vCenter 伺服器的 SSL 憑證](#)。
- 上傳或購買授權。如果您是使用評估版授權，則會顯示[購買軟體連結](#)。您可以按一下此連結，購買完整版授權以管理多部主機。請參閱[上傳授權至管理入口網站](#)。
- 更新 OMIVV。請參閱[更新虛擬裝置儲存庫位置和虛擬裝置](#) 第頁的 15。
- 產生疑難排解配套。請參閱[下載疑難排解套件組合](#) 第頁的 27。
- 重新啟動 OMIVV。請參閱[重新啟動虛擬裝置](#) 第頁的 15。
- 執行備份與還原。請參閱[透過備份與還原更新裝置](#) 第頁的 16。
- 設定警示。請參閱[設定全域警示](#) 第頁的 19。
- 設定部署模式，請參閱[設定部署模式](#) 第頁的 17。

以非管理員使用者的身分登錄 vCenter Server


您可以使用 vCenter 管理員認證，或是有 Dell 權限的非管理員使用者身分，為 OMIVV 應用裝置登錄 vCenter Server。

若要為非系統管理員使用者啟用必要權限，使其能登錄 vCenter Server，請執行下列步驟：

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](#)。

 **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。

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


有必要權限的 vCenter Server 非管理員使用者現在可以登錄及/或取消登錄 vCenter、修改認證或更新認證。




3. 以具必要權限的非管理員使用者身分登錄 vCenter Server。請參閱[以具必要權限的非管理員使用者身分登錄 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](#)。


具備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：

-  **註：** 非管理員使用者以 OMIVV 登錄 vCenter 伺服器時，如果沒有指派以下權限，就會顯示錯誤訊息：

- 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
-  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
 -  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
-  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

 註: 如果非管理員使用者嘗試註冊 vCenter Server, 即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 13。


以具備必要權限的非管理員使用者身分登錄 vCenter 伺服器

您可使用具備必要權限的非管理員使用者身分，為 OMIVV 裝置登錄 vCenter 伺服器。請參閱註冊 **OpenManage Integration for VMware vCenter** 並匯入授權檔案主題登錄 vCenter Server 第頁的 13，以取得透過非管理員使用者身分或管理員身分登錄 vCenter 伺服器的相關資訊。

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](#)。

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。

登錄 vCenter Server

您可以在安裝 OpenManage Integration for VMware vCenter 後，登錄 OMIVV 裝置。OpenManage Integration for VMware vCenter 會使用管理員使用者帳戶，或具備必要 vCenter 操作權限的非管理員使用者帳戶。單一 OMIVV 裝置執行個體可支援總共 10 個 vCenter 伺服器和最多 1000 個 ESXi 主機。

若要登錄新 vCenter 伺服器，請執行下列步驟：

1. 由支援的瀏覽器開啟**管理入口網站**。
若要開啟管理入口網站，請在 OpenManage Integration for VMware vCenter 的「說明與支援」索引標籤中，按一下「管理主控台」下方的連結，或開啟網頁瀏覽器並輸入：`https://<裝置 IP>主機名稱`。
2. 在左窗格按一下 **VCENTER 註冊**，然後按一下 **登錄新 vCenter 伺服器**。
3. 請在**登錄新的 vCenter** 對話方塊的 **vCenter 名稱** 底下，執行下列步驟：
 - a. 在 **vCenter 伺服器 IP 或主機名稱** 文字方塊，輸入 vCenter IP 位址或主機的 FQDN。
i 註: Dell 建議您使用完整網域名稱 (FQDN)，向 VMware vCenter 登錄 OMIVV。無論是何種登錄，DNS 伺服器應可正確解析 vCenter 的主機名稱。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 主機名稱項目出現在 DNS 伺服器的正向與反向查閱區域中。
 - b. 在 **說明** 文字方塊中輸入說明 (選填)。
4. 在 **vCenter 使用者帳戶** 底下，執行下列步驟：
 - a. 請在 **vCenter 使用者名稱** 文字方塊中，輸入系統管理員的使用者名稱，或具所需權限之非系統管理員的使用者名稱。
 - b. 在 **密碼** 文字方塊中，輸入密碼。
 - c. 在 **確認密碼** 文字方塊中，再次輸入密碼。
5. 按一下 **登錄**。

登錄 vCenter 伺服器之後，OMIVV 可登錄為 vCenter 外掛程式，「Dell EMC OpenManage Integration」圖示會顯示在 vSphere Web 用戶端中，您可以從其中存取 OMIVV 功能。

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。

具有必要權限的使用者 X 使用 vCenter 登錄 OMIVV，而使用者 Y 僅具有 Dell 權限。則使用者 Y 現在可以登入 vCenter 並可由 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。

修改 vCenter 登入認證

具備管理權限的使用者或具備必要權限的非管理員使用者，均可修改 vCenter 登入認證。

- 若要開啟管理入口網站，請在 OpenManage Integration for VMware vCenter 的說明與支援索引標籤中，按一下**管理主控台**下方的連結，或啟動 Web 瀏覽器並提供 URL：`https://<ApplianceIP|hostname>`。
- 在**登入**對話方塊中輸入密碼，然後按一下**登入**。
- 在左窗格中，按一下 **VCENTER 註冊**。
登錄的 vCenter 伺服器會顯示於**管理 VCENTER 伺服器連線**右側窗格的視窗中。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**。
- 輸入 vCenter **使用者名稱、密碼和確認密碼**；密碼必須相符。
- 若要變更密碼，請按一下**套用**，或者若要取消變更，則按一下**取消**。

註：如果提供的使用者認證沒有必要權限，就會顯示錯誤訊息。

更新已登錄之 vCenter 伺服器的 SSL 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 API 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。OpenManage Integration for VMware vCenter 會使用數位憑證，在 Web 伺服器上啟用 SSL 以進行安全通訊。

如果 vCenter 伺服器上的 SSL 憑證已變更，請使用下列步驟匯入 OpenManage Integration for VMware vCenter 的新憑證：

- 若要開啟管理入口網站，請在 OpenManage Integration for VMware vCenter 的說明與支援索引標籤中，按一下**管理主控台**下方的連結，或開啟網頁瀏覽器並在位址列輸入 URL：`https://<裝置 IP|裝置主機名稱>`。
- 在左窗格中，按一下 **VCENTER 註冊**。
已登錄的 vCenter 伺服器會顯示在右窗格中。
- 若要更新 vCenter 伺服器 IP 的憑證或主機名稱，請按一下**更新**。

解除安裝 OpenManage Integration for VMware vCenter

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。

註：清查、保固或部署工作正在執行時，請確定您未從 vCenter 伺服器取消註冊 OMIVV。

- 若要開啟管理入口網站，請在 OpenManage Integration for VMware vCenter 的說明與支援索引標籤中，按一下**管理主控台**下方的連結，或啟動 Web 瀏覽器並提供 URL：`https://<ApplianceIP|hostname>`。
- 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：由於 vCenter 可能不只一個，因此請務必選取正確的 vCenter。

- 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：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**，然後按一下**編輯**，以存取叢集的**主動式 HA 故障與回應**畫面。要停用主動式 HA：

在**主動式 HA 故障與回應**畫面中，清除 **Dell Inc** 提供者的核取方塊。

上傳授權至管理入口網站

您可以上傳 OMIVV 授權來變更以下二者的數目：支援的並行登錄 vCenter 執行個體和受管理的主機。如果需要增加更多主機，也可以執行下列步驟來新增授權：

1. 若要開啟管理入口網站，請在 OpenManage Integration for VMware vCenter 的說明與支援索引標籤中，按一下**管理主控台**下方的連結，或開啟網頁瀏覽器並在位址列輸入 URL：`https://<裝置 IP>|<裝置主機名稱>`。
2. 在**登入**對話方塊輸入密碼。
3. 在左窗格中，按一下 **VCENTER 註冊**。
已登錄的 vCenter 伺服器會顯示在右窗格中。
4. 按一下**上傳授權**。
5. 在**上傳授權**對話方塊中，按一下**瀏覽**以瀏覽至授權檔案，然後按一下**上傳**。

i 註：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。

管理虛擬裝置

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

- 重新啟動虛擬設備。請參閱[重新啟動虛擬裝置](#)。
- 更新虛擬設備及設定更新儲存庫的位置。請參閱[更新虛擬裝置儲存庫位置和虛擬裝置](#)。
- 設定 NTP 伺服器。請參閱[設定網路時間通訊協定伺服器](#)。
- 上傳 HTTPS 憑證。請參閱[上傳 HTTPS 憑證](#)。

在 OpenManage Integration for VMware vCenter 中，執行下列步驟以透過管理入口網站存取**裝置管理**頁面：

1. 若要開啟管理入口網站，請在 OpenManage Integration for VMware vCenter 的說明與支援索引標籤中，按一下**管理主控台**下方的連結，或開啟網頁瀏覽器並在位址列輸入 URL：`https://<裝置 IP>|<裝置主機名稱>`。
2. 在**登入**對話方塊輸入密碼。
3. 若要設定裝置管理區段，請在左窗格中按一下**裝置管理**。

重新啟動虛擬裝置

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

變更虛擬裝置的主機名稱

執行下列步驟：

1. 在「裝置管理」頁面上，按一下「變更主機名稱」。
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**。
裝置的主機名稱隨即更新，您也會返回主功能表。
4. 若要重新啟動裝置，請按一下**重新啟動裝置**。

i 註：如果您已將裝置註冊於任何 vCenter 伺服器，請先取消註冊所有 vCenter 執行個體，然後再重新註冊。

i 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、DRM 中的佈建伺服器。

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](#) 第頁的 19。

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](#)。

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[設定 HTTP 代理](#)。
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，請確認**更新儲存庫路徑**已設為以下路徑：<http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/>。如果路徑不同，請在**裝置管理**視窗的**裝置更新**區域中按一下**編輯**，即可在**更新儲存庫路徑**文字方塊中，將路徑更新為 <http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/>。若要儲存，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 <http://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 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 取消登錄外掛程式會移除 OMIVV 外掛程式在 vCenter 上登錄的所有警報，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 18 和 [上傳 HTTPS 憑證](#) 第頁的 18。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。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: 如果從 x 版 OMIVV 變更為新 y 版 OMIVV 的 IP 位址, 請將 SNMP 陷阱的陷阱目的地設定為指向新裝置。對於第 12 代及更新一代的伺服器, 可藉由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 陷阱不是指向新的 IP, 那些主機列為不相容。對於第 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 [執行修正不相容 vSphere 主機精靈](#)。

下載疑難排解配套

1. 在 **裝置管理** 頁面上, 按一下 **產生疑難排解配套**。
2. 按一下 **下載疑難排解配套** 連結。
3. 按一下 **關閉**。

設定 HTTP 代理

1. 在 **裝置管理** 頁面, 向下捲動至 **HTTP 代理設定**, 然後按一下 **編輯**。
2. 請以編輯模式執行下列步驟:
 - a. 選取 **啟用** 以使用 HTTP 代理設定。
 - b. 在 **代理伺服器位址** 中輸入代理伺服器位址。
 - c. 在 **代理伺服器連接埠** 中輸入代理伺服器連接埠。
 - d. 選取 **是** 以使用代理認證。
 - e. 如果使用代理認證, 請在 **使用者名稱** 中輸入使用者名稱。
 - f. 在 **密碼** 中輸入密碼。
 - g. 按一下 **套用**。

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), 來同步處理虛擬裝置時鐘和 NTP 伺服器時鐘。

1. 在 **裝置管理** 頁面中, 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**。

i 註: 可能需花費 10 分鐘, 才可完成虛擬設備時鐘與 NTP 伺服器同步化。

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 2. 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。

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」。

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 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**。

設定全域警示

警示管理可讓您針對如何儲存所有 vCenter 執行個體的警示，進行全域設定。

1. 若要開啟管理入口網站，請在 OpenManage Integration for VMware vCenter 的**說明與支援**索引標籤中，按一下**管理主控台**下方的連結，或開啟網頁瀏覽器並在位址列輸入 URL：`https://<裝置 IP|裝置主機名稱>`。
2. 在**登入**對話方塊輸入密碼。
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. 輸入下列欄位的數值：
 - **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**，或者若要取消，請按一下**取消**。

管理備份和還原

您可以從管理主控台管理備份和還原。此頁面的工作包括：

- 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

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. 若要開啟管理入口網站，請在 OpenManage Integration for VMware vCenter 的**說明與支援**索引標籤中，按一下**管理主控台**下方的連結，或啟動 Web 瀏覽器並提供 URL：`https://<ApplianceIP|hostname>`。
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，以供稍後還原。備份中包含設定檔、範本及主機資訊。Dell 建議您排程自動備份，以防止資料遺失。

i 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. 在反白顯示的**設定與詳細資料**區域中，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，在文字方塊輸入加密密碼。
加密密碼可包含字母數字字元和特殊字元，例如「!**@#%***」。
 - 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**頁面中，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. 針對您在當週幾天要執行備份，選取**備份天數**核取方塊。
4. 在**備份時間 (24 小時制, HH: mm)** 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**立即備份**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。
加密密碼可包含字母數字字元和特殊字元，例如「!、@、#、\$、%、*」。長度沒有限制。
4. 按一下**備份**。

從備份還原 OMIVV 資料庫

還原作業會導致虛擬裝置在完成還原後重新啟動。

1. 開啟**備份及還原設定**頁面。請參閱[管理備份及還原](#)。
2. 在**備份及還原設定**頁面中，按一下**立即還原**。
3. 在**立即還原**對話方塊中，以 CIFS/NFS 格式輸入**檔案位置**和備份 .gz 檔案的路徑。
4. 輸入備份檔案的**使用者名稱**、**密碼**和**加密密碼**。
加密密碼可包含字母數字字元和特殊字元，例如「!、@、#、\$、%、*」。長度不受限制。
5. 若要儲存變更，請按一下**套用**。
隨後裝置會重新開機。

 **註:** 如果 OMIVV 裝置重設為原廠設定，請確定您再次註冊該裝置。

關於 vSphere 用戶端主控台

vSphere Client 主控台是在虛擬機器的 vSphere Client 內。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：

- 進行網路設定
- 變更虛擬裝置密碼
- 設定 NTP 和設定當地時區
- 重新啟動虛擬裝置
- 將虛擬裝置重設為原廠設定
- 從主控台登出
- 使用唯讀使用者角色

開啟 OMIVV 虛擬機器主控台

1. 從 vSphere Web 用戶端的**首頁**按一下**vCenter**。
2. 在**清查清單**中，按一下**虛擬機器**，然後選取 OMIVV 虛擬裝置。
3. 執行下列其中一個步驟：
 - 在**物件標籤**上，選取**動作** → **開啟主控台**。
 - 在您選取的虛擬設備按一下滑鼠右鍵，然後選取**開啟主控台**。

在開啟虛擬機器主控台並提供認證 (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。

進行網路設定

您可以在 vSphere 用戶端主控台中變更網路設定。

1. 開啟虛擬機器主控台。請參閱[開啟 vSphere Client 主控台](#)。
2. 在**主控台**視窗中 , 選取**設定網路** , 然後按下 **ENTER**。
3. 在**編輯裝置**或**編輯 DNS** 底下輸入所需的網路設定 , 然後按一下**儲存並結束**。若要中止任何變更 , 請按一下**結束**。

變更虛擬裝置密碼

您可以在 vSphere Web 用戶端中使用主控台變更虛擬裝置密碼。

1. 開啟 OMIVV 虛擬機器主控台 OMIVV DLCL_UG 開啟 vSphere 用戶端主控台
2. 在**主控台**視窗中 , 使用方向鍵選取**變更管理員密碼** , 然後按下 **ENTER**。
3. 在**目前管理員密碼**中輸入值 , 然後按下 **ENTER**。
管理員密碼至少要有八個字母 , 其中包含一個特殊字元、一個數字、一個大寫字母和一個小寫字母。
4. 在**輸入新的管理員密碼**輸入新密碼 , 然後按 **ENTER** 鍵。
5. 在**請確認管理員密碼**中再次輸入新密碼 , 然後按下 **Enter**。

設定 NTP 和設定當地時區

1. 開啟虛擬機器主控台。請參閱[開啟 vSphere Client 主控台](#)。
2. 若要設定 OMIVV 時區資訊 , 請按一下**日期/時間內容**。
3. 在**日期與時間**標籤中 , 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 NTP 伺服器 IP 或主機名稱 , 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**。

重新啟動虛擬裝置


1. 開啟 OMIVV 虛擬機器主控台 OMIVV DLCL_UG 開啟 vSphere 用戶端主控台
2. 按一下**重新啟動裝置**。
3. 若要重新啟動裝置 , 請按一下**是**。若要取消 , 請按一下**否**。

將虛擬裝置重設為原廠設定

1. 開啟 OMIVV 虛擬機器主控台 OMIVV DLCL_UG 開啟 vSphere 用戶端主控台
2. 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** , 若要取消 , 請按一下**否**。
如果您按一下「是」, OMIVV 裝置會重設為原廠設定 , 所有其他設定及現有的資料將會遺失。

 **註:** 虛擬裝置重設為原廠設定時 , 對網路組態所做的任何更新都會保留 ; 這些設定不會重設。

從 vSphere 主控台登出

若要從 vSphere 主控台登出 , 請按一下**登出**。

唯讀使用者角色

有一種使用者角色僅具備唯讀權限，卻具備診斷用途的 Shell 存取權。唯讀使用者僅具備執行掛載的有限權限。唯讀使用者的密碼是設定為 **readonly**。使用者的唯讀使用者角色密碼，與舊版 OMIVV (OMIVV 1.0 版到 2.3.1 版) 中的系統管理員密碼相同，而且為了安全起見，自 OMIVV 3.0 版起就變更了。

管理多個裝置

您可以管理和監控已向 vCenter Server 登錄，且屬於相同或不同平台服務控制器 (PSC) 的多個 OMIVV 應用裝置。Dell EMC 建議使用類似的 vCenter 版本。

如果頁面已快取，Dell EMC 建議您執行全域重新整理。

1. 在 VMware vCenter 首頁上，按一下 **OpenManage Integration** 圖示。
2. 在導覽的 **Dell EMC** 群組底下，按一下 **OMIVV 裝置**。
3. 在 **OMIVV 裝置** 標籤中，檢視以下資訊並監控裝置：

i 註: 在 Dell 裝置標籤中，裝置出現在清單中的優先順序是預先決定的，而反白顯示的裝置則是作用中的裝置。

- **名稱** — 顯示使用每一個 OMIVV 裝置的 IP 位址或 FQDN 的連結。若要檢視和監控裝置特有的資訊，請按一下特定裝置的名稱連結。按一下裝置名稱連結後，您會移至該 OMIVV 裝置的主要內容窗格。您可以管理 OMIVV 作業，並監控特定裝置的主機、資料中心和叢集。

i 註: 若您使用多個裝置，則按一下**名稱**後會顯示一個訊息方塊，提示您在快取的頁面上執行全域重新整理。

若要知道您是在哪一個裝置上管理 OMIVV 作業，請執行以下動作：

- a. 在 OpenManage Integration for VMware vCenter 中，按一下**說明與支援**標籤。
 - b. 在「管理主控台」底下，檢視特定的 OMIVV 裝置 IP。
- **版本** — 顯示每一個 OMIVV 裝置的版本。
 - **相容性狀態** — 指出應用裝置是否相容於載入的外掛程式。
 - i 註:** 當 OMIVV 應用裝置不相容於外掛程式，且**名稱**連結為停用狀態時，該應用裝置的相容性狀態會顯示為**不相容**。
 - **可用性狀態** — 顯示的狀態會指出您是否可以從外掛程式連線到該應用裝置，且該 OMIVV 應用裝置是否正在執行所需的 Web 服務。
 - i 註:** 當裝置的相容性狀態為**相容**，且裝置的可用性狀態為**正常**時，即可選擇該裝置。
 - **登錄的 vCenter 伺服器** — 顯示裝置所登錄且您存取後可進入已登入之工作階段的所有 vCenter。如果一個裝置登錄了多個 vCenter，這些 vCenter 會顯示為可展開和摺疊的清單。按一下 vCenter 連結會將您帶往 **vCenter 伺服器** 頁面，該頁面的導覽窗格上會列出所有的 vCenter。

從 Web 用戶端存取 OpenManage Integration

安裝 OMIV 之後當您登入 VMware vCenter 時，**首頁**標籤底下的 **OpenManage Integration** 圖示會位於**管理**群組底下的主內容區域。您可以使用 **OpenManage Integration** 圖示瀏覽至 **OpenManage Integration for VMware vCenter** 頁面。**Dell EMC** 群組會顯示在**導覽**窗格中。

VMware vCenter 配置有下列三個主要窗格：

表 3. OpenManage Integration for VMware vCenter 窗格

窗格	說明
導覽	在主控台存取不同檢視。OpenManage Integration for VMware vCenter 在 vCenter 功能表下有一個特殊群組，作為 OpenManage Integration for VMware vCenter 的主要存取點。
主內容	顯示在「導覽」窗格中選取的檢視。主內容窗格是顯示大部分內容的區域。
通知	顯示 vCenter 警報、工作和進行中的工作。OpenManage Integration for VMware vCenter 在 vCenter 整合警報、事件和工作系統，以在「通知」窗格顯示資訊。

主題：

- 在 VMware vCenter Web 用戶端中瀏覽
- Web 用戶端中的圖示
- 尋找軟體版本
- 重新整理畫面內容
- 檢視 Dell EMC 主機
- 檢視 OpenManage Integration for VMware vCenter 授權標籤
- 存取說明與支援
- 檢視記錄歷史記錄

在 VMware vCenter Web 用戶端中瀏覽

OpenManage Integration for VMware vCenter 位於 VMware vCenter 的一個特殊 **Dell EMC** 群組中。

1. 登入 VMware vCenter。
2. 在 VMware vCenter 首頁上，按一下 **OpenManage Integration** 圖示。














您可以在這裡執行以下動作：

- 管理 OpenManage Integration for VMware vCenter 連線設定檔、產品設定、檢視摘要頁面，並執行主要內容窗格各標籤中的其他工作。
- 從導覽窗格的 **vCenter** 清查清單底下，監視主機、資料中心和叢集。請選取您要調查的主機、資料中心或叢集，然後在物件標籤上，按一下您選擇監視的物件。

Web 用戶端中的圖示

產品使用者介面使用許多圖示型動作按鈕，代表您採取的動作。

表 4. 已定義的圖示按鈕

圖示按鈕	定義
	新增或新建項目
	在連線設定檔、資料中心和叢集新增伺服器
	中止工作
	折疊清單
	展開清單
	刪除物件
	變更排程
	編輯
	清除工作
	匯出檔案
	檢視系統設定檔
	篩選
	立即執行

尋找軟體版本

在 OpenManage Integration for VMware vCenter 的**開始使用**標籤可以找到軟體版本。

1. 在 VMware vCenter 首頁上，按一下 **OpenManage Integration** 圖示。
2. 在 OpenManage Integration for VMware vCenter 的**開始使用**標籤上，按一下**版本資訊**。
3. 在**版本資訊**對話方塊中，檢視版本資訊。
4. 若要關閉對話方塊，按一下**確定**。

重新整理畫面內容

使用 VMware vCenter **重新整理**圖示重新整理畫面。

1. 選取您要重新整理的頁面。
2. 在 VMware vCenter 標題列中，按一下**重新整理 (Ctrl+Alt+R)** 圖示。
重新整理圖示位於「搜尋」區域的右側，看起來像是順時針方向的箭頭。

檢視 Dell EMC 主機

如果您想要只快速檢視 Dell EMC 主機，請在 OpenManage Integration for VMware vCenter 的「導覽」窗格中，選取 **Dell EMC 主機**。

1. 在 VMware vCenter 首頁上，按一下 **OpenManage Integration** 圖示。
2. 在導覽的 **OpenManage Integration** 之下，按一下 **Dell EMC 主機**。
3. 在 **Dell EMC 主機**標籤中，檢視下列資訊：
 - **主機名稱** — 顯示使用每個 Dell 主機之 IP 位址的連結。若要檢視 Dell 主機資訊，請按一下特定主機連結。
 - **VCenter** — 顯示此 Dell EMC 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。
- **連線設定檔** — 顯示連線設定檔名稱。

檢視 OpenManage Integration for VMware vCenter 授權標籤

安裝 OpenManage Integration for VMware vCenter 授權時，這個標籤會顯示支援的主機和 vCenter 伺服器數量。在頁面頂端還可以檢視 OpenManage Integration for VMware vCenter 的版本。

在授權下的頁面會顯示**購買授權**連結。

授權管理區段會顯示：

- **產品授權入口網站 (數位購物服務區)**
- **iDRAC 授權入口網站**
- **管理主控台**

OpenManage Integration for VMware vCenter 的**授權**標籤會顯示下列資訊：

授權標籤資訊	說明
主機授權	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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

存取說明與支援

為了提供您需要的產品相關資訊，OpenManage Integration for VMware vCenter 提供了**說明與支援**標籤。您可以在此標籤中找到以下資訊：

表 5. 「說明與支援」標籤中的資訊

名稱	說明
產品說明	提供下列連結： <ul style="list-style-type: none"> ● OpenManage Integration for VMware vCenter 說明 — 提供產品說明的連結 (位於產品內)。使用目錄或搜尋功能來尋找您需要的資訊。 ● 關於 - 此連結會顯示版本資訊對話方塊。您可以在此處檢視產品版本。
Dell EMC 手冊	提供下列即時連結： <ul style="list-style-type: none"> ● 伺服器手冊 ● OpenManage Integration for VMware vCenter 手冊
管理主控台	提供管理主控台的連結。
其他說明與支援	提供下列即時連結： <ul style="list-style-type: none"> ● iDRAC with Lifecycle Controller 手冊 ● Dell VMware 說明文件 ● OpenManage Integration for VMware vCenter 產品頁面 ● Dell 說明與支援首頁

表 5. 「說明與支援」標籤中的資訊 (續)

名稱	說明
	<ul style="list-style-type: none"> ● Dell TechCenter
支援電話提示	就如何聯絡 Dell Support 與正確轉接電話提供提示。
故障排除配套	提供建立和下載故障排除配套的連結。當您聯絡技術支援部門時，即可提供或檢視此配套。如需更多資訊，請參閱 下載故障排除配套 。
Dell EMC 建議	提供 Dell Repository Manager (DRM) 的連結。使用 DRM 來尋找並下載所有可供系統使用的韌體更新。
iDRAC 重設	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。

下載疑難排解套件組合

註: 若要產生疑難排解套件組合，請確定您使用在 OMIVV 上具有寫入權限之使用者的身分登入 vSphere Web 用戶端。

您可以使用疑難排解套件組合資訊來協助進行疑難排解，或傳送資訊給技術支援部門。若要取得疑難排解資訊，請執行下列步驟：

1. 在 OpenManage Integration for VMware vCenter 中，按一下**說明與支援**標籤。
2. 在**故障排除配套**之下，按一下**建立並下載疑難排解套件組合**。
3. 按一下**建立**按鈕。
4. 若要儲存檔案，按一下**下載**。
5. 在**檔案下載**對話方塊中，按一下**儲存**。
6. 在**另存新檔**對話方塊中，瀏覽到您想要儲存檔案的位置，然後按一下**儲存**。
7. 按一下**關閉**即可結束。

重設 iDRAC

您可以在**說明與支援**標籤上找到重設 iDRAC 連結。重設 iDRAC 會執行正常的 iDRAC 重新開機。iDRAC 重新開機不會重新啟動主機。執行重設後，返回可用狀態最多需要 2 分鐘。當 iDRAC 在 OpenManage Integration for VMware vCenter 中沒有回應時，才使用重設功能。

註: 建議先將主機設在維護模式再重設 iDRAC。您可以在主機上套用重設動作，該主機是連線設定檔的一部分，並已至少清查一次。重設動作可能不會讓 iDRAC 返回至可用狀態。在這種情況下，必須進行硬重設。若要深入瞭解硬重設，請參閱 iDRAC 文件。

在 iDRAC 重新啟動時，您可以檢視下列項目：

- 在 OpenManage Integration for VMware vCenter 取得其健全狀況狀態時，發生通訊輕微延遲錯誤。
- iDRAC 所有開啟的工作階段關閉。
- iDRAC 的 DHCP 位址可能會改變。

如果 iDRAC 使用 DHCP 作為其 IP 位址，則 IP 位址有可能會變更。如果 IP 位址變更，請重新執行主機清查工作，在清查資料中擷取新的 iDRAC IP 位址。

1. 在 OpenManage Integration for VMware vCenter 中，按一下**說明與支援**標籤。
2. 在 iDRAC 重設，請按一下 **Reset iDRAC (重設 iDRAC)**。
3. 在 **iDRAC 重設**對話方塊的「iDRAC 重設」之下，輸入主機 IP 位址/名稱。
4. 為確認您瞭解 iDRAC 重設程序，請選擇**我瞭解 iDRAC 重設。繼續 iDRAC 重設**。
5. 按一下 **Reset iDRAC (重設 iDRAC)**。

開啟線上說明

您可以在**說明與支援**標籤上開啟線上說明。如要瞭解某項主題或程序，可以搜尋文件以取得說明。

1. 在 OpenManage Integration for VMware vCenter 中，按一下**說明與支援**中**產品說明**下方的 **OpenManage Integration for VMware vCenter 說明**。
線上說明內容會顯示在瀏覽器視窗中。
2. 使用左窗格目錄或搜尋，找到您選擇的主題。
3. 若要關閉線上說明，請按一下瀏覽器視窗右上角的 **X**。

啟動管理主控台

您可以從 VMware vCenter Web 用戶端內部啟動 OpenManage Integration for VMware vCenter，並從**說明與支援**標籤開啟管理主控台。

1. 在 OpenManage Integration for VMware vCenter 中，按一下**說明與支援**標籤中**管理主控台**之下的主控台連結。
2. 在**管理主控台**登入對話方塊中，使用系統管理員密碼登入。

您可以在管理主控台中執行下列作業：

- 登錄或取消登錄 vCenter、修改認證或更新憑證。
- 上傳授權。
- 檢視已登錄和可用 vCenter 數目，以及使用中與可用的主機授權上限的相關摘要。
- 重新啟動虛擬設備。
- 更新或升級至最新版本。
- 顯示網路設定 (唯讀模式)。
- 完成連接至 Dell EMC 伺服器的 HTTP 代理設定，以將裝置升級或連線至 <http://downloads.dell.com/published/Pages/index.html>。
- 完成 NTP 設定，可讓您啟用或停用 NTP 伺服器，然後設定偏好的和次要的 NTP 伺服器。
- 產生憑證簽章要求 (CSR)、上傳憑證，或還原 HTTPS 憑證的預設憑證。
- 進行全域設定，決定如何替所有的 vCenter 執行個體儲存警示。您可以設定儲存的警示上限、警示保留天數，以及重複警示的逾時。
- 進行全域設定，決定如何替所有的 vCenter 執行個體儲存警示。
- 啟動備份或還原。
- 將備份位置設定為網路共用，同時為備份檔案設定加密密碼 (以及測試網路連線)。
- 排定週期性備份。

檢視記錄歷史記錄

記錄頁面可讓您檢視 OMIVV 所產生的記錄。

您可以使用兩個下拉式清單來篩選和排序此頁面上的內容。第一個下拉式清單可讓您根據下列記錄類型，來篩選和檢視記錄的詳細資料：

- 所有類別
- 資訊
- 警告
- 錯誤

第二個下拉式清單可協助您根據以下日期與時間頻率來排序記錄詳細資料：

- 上週
- 上個月
- 去年
- 自訂範圍
 - 如果您選取**自訂範圍**，則可以根據您要篩選的內容來指定開始和結束日期，然後按一下**套用**。

資料格表格會顯示下列資訊：

- 類別 — 顯示記錄類別的類型
- 日期與時間 — 顯示使用者動作的日期和時間
- 說明 — 顯示使用者動作的說明

您可以按一下欄標題，以遞增或遞減順序排序資料格欄。使用**篩選**文字方塊在內容中進行搜尋。頁面格線底部會顯示下列資訊：

表 6. 記錄歷史記錄


記錄資訊	說明
項目總計	顯示所有記錄項目的總數
每個畫面上的項目	在顯示的頁面上顯示記錄項目數。使用下拉式方塊可設定每頁的項目數。
頁面	在您檢視記錄資訊時，顯示目前所在的頁面。您還可以在文字方塊中輸入頁碼，或使用上一頁與下一頁按鈕，前往您想要的頁面。
上一頁或下一頁按鈕	引導您至下一頁或上一頁
全部匯出圖示	匯出記錄內容至 CSV 檔案

檢視記錄

1. 在 OpenManage Integration for VMware vCenter 中，按一下**監視**標籤。
2. 在**記錄**標籤中，檢視 OpenManage Integration for VMware vCenter 的使用者動作記錄。如需進一步瞭解顯示的記錄，請參閱[記錄歷史記錄](#)。
3. 若要排序格線中的資料，請按一下欄標題。
4. 若要使用類別或時間區塊排序，請使用資料格前方的下拉式清單。
5. 若要在記錄項目的頁面之間瀏覽，請使用**上一頁**與**下一頁**按鈕。

匯出記錄檔

OpenManage Integration for VMware vCenter 使用逗號分隔值 (CSV) 檔案格式匯出資料表格中的資訊。

1. 在 OpenManage Integration for VMware vCenter 中，按一下**監視**標籤。
2. 若要匯出紀錄內容至 CSV 檔案，在畫面右下角按一下  圖示。
3. 在**選取下載位置**對話方塊中，瀏覽至要儲存記錄資訊的位置。
4. 在**檔案名稱**文字方塊中，接受 `ExportList.csv` 這個預設名稱，或自行輸入具 .CSV 副檔名的檔案名稱。
5. 按一下**儲存**。

OpenManage Integration for VMware vCenter 授權

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

- 評估授權 — 第一次開啟 OMIVV 4.x 版裝置的電源時，系統會自動安裝評估授權。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。此授權僅適用於第 11 代與更新世代的 Dell EMC 伺服器，且是預設的授權，有 90 天試用期。
- 標準授權 — 完整產品版本包含最多 10 個 vCenter 伺服器的標準授權，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 授權檔案儲存至您的本機系統，然後使用 [Administration Console] 上傳新的授權檔案。

授權會提供下列資訊：

- vCenter 連線授權上限 — 最多允許登錄及使用 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。

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。

當您購買授權後，請造訪 <http://www.dell.com/support/licensing>，從 Dell Digital Locker 下載 .XML 檔案 (授權金鑰)。如果您無法下載授權金鑰，請前往下列網址連絡 Dell 支援服務：www.dell.com/support/incidentsonline/in/en/indhs1/email/order-support，以尋找您產品適用的當地 Dell 支援服務電話號碼。

主題：

- [購買並上傳軟體授權](#)

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。

i 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。

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**

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並執行下列工作：

- 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**。
- 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

若要在安裝及登錄 vCenter 之後設定 OMIVV，請執行下列步驟以檢視**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**。

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。

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

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。

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：

註: iDRAC 帳戶需要管理權限以更新韌體、套用系統設定檔於第 14 代伺服器及部署 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 **使用者名稱** 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：網域\使用者名稱或使用者名稱@網域。使用者名稱上限為 256 個字元。
 - 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。請參閱 iDRAC 說明文件，以取得所使用之 iDRAC 版本的使用者名稱限制資訊。
 - 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：
 - a. 在 Active Directory **使用者名稱** 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：網域\使用者名稱或使用者名稱@網域。使用者名稱上限為 256 個字元。

註: 如需主機使用者名稱與網域限制，請參閱下列資訊：

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
- 沒有無效字元，例如 " / \ [] ; | = , + * ? < > @

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。
- 沒有無效字元，例如 " / \ [] ; | = , + * ? < > @

- 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，您無法加以變更。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。
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**。
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：這是選擇性步驟，可檢查主機和 iDRAC 認證。雖然這並非必要步驟，但仍建議您測試連線設定檔。

i 註：所有執行 ESXi 6.5 及 / 或更新版本且停用 WBEM 服務的主機測試連線皆失敗。對這類主機而言，WBEM 服務會在您執行這些主機的清查時自動啟用。雖然測試連線失敗，但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。

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。請參閱本指南中的**修改連線設定檔**主題。

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 會自動啟用 ESXi 6.5 主機的 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 使用者指南* 中的**報告與修復 vSphere 主機的相容性** 第頁的 111。

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，只要有任意 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排程詳細資料。請參閱**修改清查工作排程** 第頁的 52

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。

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** 第頁的 54。

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。

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

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**。

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**。

i 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**還原預設警示**。
變更生效可能需時一分鐘。

i 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。

i 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**。

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 **保固到期通知**。
2. 展開 **保固到期通知** 即可檢視下列項目：
 - **保固到期通知** — 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 **保固到期通知** 右側的  圖示。
4. 請在 **保固到期通知** 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 **對於主機啟用保固到期通知**。
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。

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 線上** — 您可以存取使用 Dell 韌體更新儲存庫的位置 (Ftp.dell.com)。OpenManage Integration for VMware vCenter 從 Dell 儲存庫下載選取的韌體更新並更新管理的主機。
 -  **註:** 如果網路需要 Proxy，請根據網路設定啟用 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。
3. 如果選取 **共用網路資料夾**，請使用下列格式輸入 **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。
 -  **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。共用網路資料夾的使用者名稱或密碼不支援使用 @、% 和 , 字元。
4. 下載完成之後按一下 **套用**。
 -  **註:** 要從來源讀取目錄並更新 OMIVV 資料庫，最多可能需要 60 到 90 分鐘。


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 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 代伺服器或更早版本才需要 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，請瀏覽至主機的摘要標籤，並檢查 OMSA 主控台連結是否在 **Dell EMC 主機資訊** 區段中。


設定事件與警報

Dell EMC 管理中心事件與警報對話方塊可啟用或停用所有硬體警報。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 主機的 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 警報。若為第 12 代之前的主機，則 OMIVV 支援 SNMP v1 警報。

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** 的 **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 主機的警報**。

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 伺服器的預設 vCenter 警報設定，請按一下 **還原預設警報**。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 主機的警報** 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 **事件、警報及健全狀況監控**。

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，請參閱 **修改清查工作排程** 或 **修改保固工作排程**。


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。

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。

使用「基準」標籤

您可以使用「基準」標籤來建立儲存庫設定檔和叢集設定檔。

主題：

- 儲存庫設定檔
- 建立儲存庫設定檔
- 編輯儲存庫設定檔
- 刪除儲存庫設定檔
- 叢集設定檔
- 建立叢集設定檔
- 編輯叢集設定檔
- 刪除叢集設定檔

儲存庫設定檔


儲存庫設定檔可讓您建立或維護多個驅動程式，或韌體儲存庫設定檔。這些驅動程式或韌體儲存庫設定檔可用於：

- 識別 vSAN 叢集漂移的基準設定檔。
- 更新 vSAN 叢集或 vSAN 叢集節點的驅動程式或韌體。



註：

- 使用專門為您的 vSAN 環境建立的自訂韌體目錄。
- 驅動程式儲存庫設定檔最多可擁有 10 個驅動程式。
 - ① 註：您的離線套件組合 (.zip 檔案) 不能超過 10 個。如果檔案超量，驅動程式便會隨機選擇。
- 若為驅動程式儲存庫設定檔，則只會使用來自離線套件組合的 VIB 格式非同步驅動程式 (.zip 檔案)。
 - ① 註：只有必要的非同步 VIB 驅動程式會根據 vSAN 需求加以驗證。如需更多資訊，請參閱「VMware 硬體相容性對照表」。
- 若為驅動程式儲存庫設定檔，OMIVV 會需要 CIFS 或 NFS 共用的寫入存取權。
- 若為驅動程式儲存庫設定檔，檔案內的子資料夾或大小超過 10 MB 的檔案將會被忽略。
- 在成功剖析後，儲存庫設定檔才可用於「基準設定檔」，或是用於執行 vSAN 驅動程式或韌體更新工作。
- 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。




若要啟動儲存庫設定檔頁面，請執行下列步驟：

1. 在 **OpenManage Integration for VMware vCenter** 頁面上，按一下 **管理 > 基準** 標籤，展開 **基準資訊**，然後按一下 **儲存庫設定檔**。
 - a. 在 **儲存庫設定檔** 頁面上，檢視您已建立的儲存庫設定檔清單。
表格隨即顯示，其中列出儲存庫設定檔，內容包含 **設定檔名稱**、**說明**、**類型**、**共用路徑**、**上次成功更新時間** 和 **上次重新整理狀態**。
 - b. 若要進一步檢視儲存庫設定檔的詳細資料，請選取所需的儲存庫設定檔。
檢視儲存庫設定檔所顯示的資訊，例如 **設定檔名稱**、**共用路徑**、**建立日期**、**修改日期** 和 **上次修改者**。
 - c. 若要在資料格中交換欄，請在資料格內拖曳欄。
 - d. 若要篩選或搜尋資料格的內容，請在 **篩選** 欄位中鍵入篩選準則。
 - e. 若要匯出儲存庫設定檔資訊至 .CSV 檔案，請選取儲存庫設定檔，然後在資料格的右上角內，按一下  圖示。

建立儲存庫設定檔

1. 在 **OpenManage Integration for VMware vCenter** 頁面上，按一下 **管理 > 基準**，展開 **基準資訊**，然後按一下 **儲存庫設定檔**。
 2. 按一下 **+**。
 3. 在 **歡迎** 頁面上，閱讀指示並按一下 **下一步** 以新增更多詳細資料：
 - a. 在 **設定檔名稱** 方塊中，鍵入儲存庫設定檔名稱。
 - b. 在 **設定檔說明** 欄位中，鍵入說明 (選填)。
 - c. 按一下 **下一步**。
 4. 在 **設定檔設定對話方塊** 中，選取下列其中一個儲存庫類型：
 - 韌體 (預設會選取此選項)
 - 驅動程式
 - a. 在 **儲存庫共用位置** 欄位中，輸入儲存庫共用位置 (CIFS 或 NFS)。
 - b. 若為 CIFS 共用，請鍵入使用者名稱和密碼。密碼不接受以下字元：&、!、@、% 和 <。
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。
 - c. 若要驗證特定儲存庫的路徑存取，並驗證韌體和驅動程式儲存庫的目錄檔案是否存在，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。
 - d. 按一下 **下一步**。
註: 若為驅動程式儲存庫，請下載離線驅動程式 .zip 檔，並儲存到共用位置，然後提供共用位置的完整路徑。OMIVV 會自動建立 OMIVV 裝置內的目錄。VIB 驅動程式套件組合可在 <https://my.vmware.com/web/vmware/downloads> 取得。
5. 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。
 6. 按一下 **完成**。
目錄建立後，目錄下載與剖析將會啟動，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 vSAN 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 **OpenManage Integration for VMware vCenter** 頁面上，按一下 **管理 > 基準**，展開 **基準資訊**，然後按一下 **儲存庫設定檔**。
2. 選取您要編輯的儲存庫設定檔，並按一下 。
3. 在 **儲存庫設定檔精靈** 中，您可以編輯 **設定檔名稱** 和 **說明** (選填)，然後按一下 **下一步**。
4. 請在 **設定檔設定對話方塊** 中，執行下列步驟：
 - a. 您可以編輯 CIFS 認證。
 - b. 若要驗證特定儲存庫的路徑存取，並驗證韌體和驅動程式儲存庫的目錄檔案是否存在，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。
 - c. 若要將指定位置的儲存庫重新整理為最新內容，請按一下 **與儲存庫位置同步**。
註: **與儲存庫位置同步** 選項的預設為已選取。若您想要從最新的驅動程式或韌體目錄 (共用位置) 中重新建立目錄，請確保已選取此選項。
5. 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。
6. 按一下 **完成**。

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連結。

1. 在 **OpenManage Integration for VMware vCenter** 頁面上，按一下**管理 > 基準**，展開**基準資訊**，然後按一下**儲存庫設定檔**。
2. 選取您要刪除的儲存庫設定檔，然後按一下 **X**。
3. 若要移除設定檔，請在確認對話方塊中按一下**是**，若要取消則按一下**否**。

叢集設定檔

叢集設定檔可讓您擷取基準組態，例如硬體組態（僅適用於第 14 代伺服器）、韌體或驅動程式版本，並可根據基準識別出漂移，讓 vSAN 叢集保持在所需狀態。

i 註：


- 韌體和驅動程式儲存庫設定檔在建立後必須先剖析，才能用於建立叢集設定檔。
- 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。

若要啟動叢集設定檔頁面，請執行下列步驟：

1. 在 **OpenManage Integration for VMware vCenter** 頁面上，按一下**管理 > 基準標籤**，展開**基準資訊**，然後按一下**叢集設定檔**。
 - a. 在**叢集設定檔**頁面上，檢視您已建立的叢集設定檔清單。

表格隨即顯示列出叢集設定檔，內容包含**設定檔名稱**、**說明**、**相關聯的系統設定檔**、**相關聯的韌體儲存庫設定檔**、**相關聯的驅動程式儲存庫設定檔**、**上次成功更新時間**。

i 註：如果現有的叢集設定檔有任何最新版的儲存庫設定檔可以使用，則相關的韌體或驅動程式設定檔會顯示警告符號。
 - b. 若要進一步檢視叢集設定檔的詳細資料，請選取所需的叢集設定檔。

檢視叢集設定檔所顯示的詳細資訊，例如**設定檔名稱**、**建立日期**、**修改日期**和**上次修改者**。
 - c. 若要在資料格中交換欄，請在資料格內拖曳欄。
 - d. 若要篩選或搜尋資料格的內容，請按一下**篩選**。
 - e. 若要匯出儲存庫設定檔資訊至 .CSV 檔案，請選取儲存庫設定檔，然後在資料格的右上角內，按一下 。

建立叢集設定檔


1. 系統設定檔、韌體和驅動程式的儲存庫設定檔、叢集的同質性伺服器機型。
2. vCenter 內必須有 vSAN 叢集。
3. 必須為 vSAN 叢集內至少一台主機建立連線設定檔，且清查作業應成功執行。


i 註：如果有多個獨立的 vCenter 在 OMIVV 註冊，那麼建議您為每一個 vCenter 各建立不同的叢集設定檔。

i 註：在建立叢集設定檔時，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。如果儲存庫有變更，叢集設定檔就需要再次更新，以反映變更。否則，對儲存庫進行的任何更新將不會更新到原始的叢集設定檔快照。


1. 在 **OpenManage Integration for VMware vCenter** 頁面上，按一下**管理 > 基準**，展開**基準資訊**，然後按一下**叢集設定檔**。
2. 按一下 **+**。
3. 在**歡迎**頁面上，閱讀指示並按一下**下一步**以新增更多詳細資料：
 - a. 在**設定檔名稱**欄位中，鍵入叢集設定檔名稱。
 - b. 在**設定檔說明**欄位中，鍵入該叢集設定檔的說明。設定檔說明為選填欄位。
 - c. 按一下**下一步**。
4. 請在**設定檔設定**對話方塊中，執行下列步驟：
 - a. 選取系統設定檔或儲存庫設定檔（韌體儲存庫設定檔或驅動程式儲存庫設定檔），或其組合。




i 註：系統設定檔僅適用於第 14 代伺服器。

 **註:** Dell EMC 建議您以系統設定檔、韌體和驅動程式儲存庫建立基準。


- b. 按一下**下一步**。
 5. 在**設定檔關聯**對話方塊中，執行下列步驟：
 - a. 從下拉式清單中選取已登錄的 vCenter 伺服器。
 - b. 按一下**瀏覽**來和所需的 vSAN 叢集建立關聯。
 - c. 按一下**下一步**。
 6. 在**漂移偵測排程**對話方塊中選擇日期和時間，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。
 7. 按一下**完成**。
叢集設定檔便會自動儲存，並顯示在**叢集設定檔**頁面上。
-  **註:** 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。

編輯叢集設定檔

 **註:** 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。

1. 在 **OpenManage Integration for VMware vCenter** 頁面上，按一下**管理 > 基準**，展開**基準資訊**，然後按一下**叢集設定檔**。
 2. 選取您要編輯的叢集設定檔，並按一下。
 3. 在**叢集設定檔精靈**中，您可以編輯**說明** (選填)，然後按一下**下一步**。
-  **註:** 您無法編輯設定檔名稱。
4. 在**設定檔設定**對話方塊中，您可以變更設定檔組合。
 5. 在**設定檔關聯**對話方塊中，您可以變更叢集設定檔內所需的關聯與組態。
 6. 在**設定檔組態**對話方塊中，您可以編輯**漂移偵測排程**，然後按一下**下一步**。
摘要頁面隨即顯示提供叢集設定檔已更新的相關資訊。
 7. 按一下**完成**。
已更新的叢集設定檔會自動儲存，並顯示在叢集設定檔視窗中。
-  **註:** 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。

刪除叢集設定檔

1. 在 **OpenManage Integration for VMware vCenter** 頁面上，按一下**管理 > 基準**，展開**基準資訊**，然後按一下**叢集設定檔**。
2. 選取您要刪除的叢集設定檔，再按一下.
3. 若要移除設定檔，請在確認對話方塊中按一下**是**，若要取消則按一下**否**。
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。

設定檔

認證設定檔可讓您管理與設定連線設定檔和機箱設定檔，而部署範本可讓您管理與設定硬體和 Hypervisor 設定檔。

主題：

- [關於連線設定檔](#)
- [關於機箱設定檔](#)

關於連線設定檔

連線設定檔標籤可讓您管理與設定連線設定檔，其中包含虛擬裝置正用來與 Dell EMC 伺服器進行通訊的認證。請只用一個連線設定檔與每個 Dell EMC 伺服器建立關聯，以便接受 OpenManage Integration for VMware vCenter 的管理。您可以指派多個伺服器到單一連線設定檔。在您執行**初始組態精靈**之後，可以執行下列工作，從 OpenManage Integration for VMware vCenter 管理連線設定檔：

- [檢視連線設定檔](#)
- [建立連線設定檔](#)
- [修改連線設定檔](#)
- [刪除連線設定檔](#)
- [測試連線設定檔](#)

檢視連線設定檔

連線設定檔必須先建立和/或存在才能檢視。建立一或多個連線設定檔之後，可以在**連線設定檔**頁面加以檢視。OpenManage Integration for VMware vCenter 使用設定檔中提供的認證和 Dell EMC 主機進行通訊。

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**連線設定檔**標籤。

您可以檢視已建立的所有連線設定檔。

表 7. 連線設定檔資訊

連線設定檔欄位	說明
設定檔名稱	顯示連線設定檔名稱
說明	顯示說明 (如果提供)
vCenter	視內容而定會顯示 FQDN 或主機名稱或 vCenter IP 位址
關聯主機	顯示與連線設定檔關聯的主機。如果有一個以上，使用展開圖示即可全部顯示。
iDRAC 憑證檢查	顯示 iDRAC 憑證檢查是啟用還是停用
主機根憑證檢查	顯示主機根憑證檢查是啟用還是停用
建立日期	顯示建立連線設定檔的日期
修改日期	顯示修改連線設定檔的日期
上次修改者	顯示修改連線設定檔的使用者詳細資料

建立連線設定檔

您可以將多個主機與單一連線設定檔建立關聯。若要建立連線設定檔，請執行以下步驟：

i 註：在進行此程序時所列出的 VCenter 主機，是使用相同的單一登入 (SSO) 所驗證。如果您沒有看到 vCenter 主機，則該主機可能不在不同的 SSO 上，或是您所用的 VMware vCenter 是 5.5 以前的版本。

1. 在 OpenManage Integration for VMware vCenter 的 **管理** → **設定檔** → **認證設定檔** → **連線設定檔** 標籤中，按一下 **+**。
2. 閱讀歡迎頁面上的指示，然後按下一步。
3. 在 **連線設定檔** 頁面輸入以下詳細資料：
 - a. 在 **設定檔** 底下，輸入 **設定檔名稱** 和選填的 **說明**。
 - b. 在 **vCenter** 底下的下拉式清單中，選擇 vCenter 伺服器來建立設定檔。
此選項可讓您為每一個 vCenter 建立一個連線設定檔。
 - c. 在 **iDRAC 認證** 區域中，執行下列其中一項作業：

i 註：iDRAC 帳戶需要系統管理員權限以進行更新韌體、套用硬體設定檔及部署 Hypervisor。


- 如果是您要使用 Active Directory、而且已經設定並允許使用 Active Directory 的 iDRAC，請選取 **使用 Active Directory**；否則請跳到下一個選項。
 - 在 **Active Directory 使用者名稱** 文字方塊中，輸入使用者名稱。請以下列其中一種格式輸入使用者名稱：網域\使用者名稱或使用者名稱@網域。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。
 - 在 **Active Directory 密碼** 文字方塊中，輸入密碼。密碼上限為 127 個字元。
 - 在 **確認密碼** 文字方塊中，再次輸入密碼。
 - 若要驗證 iDRAC 憑證，請選取下列一項：
 - 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**。
 - 若不執行任何驗證，也不儲存憑證，請清除 **啟用憑證檢查**。
- 若不用 Active Directory 設定 iDRAC 認證，請執行下列動作：
 - 在 **使用者名稱** 文字方塊中，輸入使用者名稱。使用者名稱上限為 16 個字元。請參閱 iDRAC 說明文件，以取得您 iDRAC 版本的使用者名稱限制資訊。


i 註：本機 iDRAC 帳戶需要系統管理員權限以進行更新韌體、套用硬體設定檔及部署 Hypervisor。
 - 在 **密碼** 文字方塊中，輸入密碼。密碼上限為 20 個字元。
 - 在 **確認密碼** 文字方塊中，再次輸入密碼。
 - 若要驗證 iDRAC 憑證，請選取下列一項：
 - 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**。
 - 若不執行任何驗證，也不儲存憑證，請勿選取 **啟用憑證檢查**。
- d. 在 **主機根** 區域，請執行下列方法之一：
 - 若為要使用 Active Directory，而且已經針對 Active Directory 完成設定及啟用的主機，請選取 **使用 Active Directory** 核取方塊，否則請跳過這一步，直接設定主機認證。
 - 在 **Active Directory 使用者名稱** 文字方塊中，輸入使用者名稱。請以下列任何一種格式輸入使用者名稱：網域\使用者名稱或使用者名稱@網域。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。
 - 在 **Active Directory 密碼** 文字方塊中，輸入密碼。密碼上限為 127 個字元。
 - 在 **確認密碼** 文字方塊中，再次輸入密碼。
 - 若要執行憑證檢查，請選擇下列其中一項：
 - 如果未來連線時一律要下載、儲存並驗證主機憑證，請選取 **啟用憑證檢查**。
 - 若不執行任何檢查且不儲存主機憑證，請勿選取 **啟用憑證檢查**。
 - 若不用 Active Directory 設定主機認證，請執行下列動作：
 - 在 **使用者名稱** 文字方塊中，使用者名稱是根。
根使用者名稱是預設的使用者名稱，無法變更。


i 註：如果有設定 Active Directory，您就可以選擇任何 Active Directory 使用者名稱，而不只是根。
 - 在 **密碼** 文字方塊中，輸入密碼。密碼上限為 127 個字元。
 - 在 **確認密碼** 文字方塊中，再次輸入密碼。
 - 若要執行憑證檢查，請選擇下列其中一項：
 - 如果未來連線時一律要下載、儲存並驗證主機憑證，請選取 **啟用憑證檢查**。
 - 若不執行任何檢查且不儲存主機憑證，請勿選取 **啟用憑證檢查**。


 **註:** OMSA 認證與 ESXi 主機所使用的認證相同。

4. 按一下**下一步**。
5. 在**選取主機**對話方塊中，選取此連線設定檔的主機，然後按一下**確定**。
6. 必要時可在**關聯主機**頁面上，為連線設定檔新增一或多個主機。

若要新增主機，請按一下、選取主機，然後按一下**確定**。

7. 若要測試連線設定檔，請選取一或多個主機，然後按一下.

 **註:** 這是選擇性步驟，可驗證主機和 iDRAC 認證是否正確。雖然這並非必要步驟，但仍建議您測試連線設定檔。


 **註:** 所有執行 ESXi 6.5 及 / 或更新版本且停用 WBEM 服務的主機測試連線皆失敗。對這類主機而言，WBEM 服務會在您執行這些主機的清查時自動啟用。雖然測試連線失敗，但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。


8. 若要完成設定檔建立，請按**下一步**。
如果是不具備 iDRAC Express 或 Enterprise 卡的伺服器，則 iDRAC 測試連線結果會顯示此系統**不適用**。


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 會自動啟用 ESXi 6.5 主機的 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**執行修正不相容 vSphere 主機精靈**。


修改連線設定檔

建立連線設定檔後，您可以編輯設定檔名稱、說明、關聯主機和 iDRAC，以及主機認證。

 **註:** 在進行此程序時所列出的 **vCenter**，是使用相同的單一登入 (SSO) 所驗證。如果您無法檢視 vCenter 主機，則該主機可能在不同的 SSO 上，或是您所用的 VMware vCenter 是 5.5 以前的版本。

 **註:** 清查、保固或部署工作正在執行時，請確定您未更新連線設定檔。

 **註:** 清查、保固或部署工作正在執行時，請確定您未將與連線設定檔具有關聯的主機移至其他連線設定檔，或從連線設定檔移除主機。

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**連線設定檔**。
4. 選取設定檔，然後按一下.
5. 在**連線設定檔**視窗的歡迎標籤中閱讀資訊，然後按**下一步**。
6. 在**名稱及認證**標籤中，執行下列步驟：
 - a. 在**設定檔**底下，輸入**設定檔名稱**和選填的**說明**。
 - b. 在 **vCenter** 底下，檢視這個連線設定檔的關聯主機。關於主機顯示於此的原因，請參閱上方的注意事項。
 - c. 在 **iDRAC 認證** 底下，執行以下其中一個步驟：
 - 如果您要使用 Active Directory，而且已經設定並啟用 Active Directory 的 iDRAC 帳戶，請選取**使用 Active Directory**。
 - 在 **Active Directory 使用者名稱**文字方塊中，輸入使用者名稱。請以下列其中一種格式輸入使用者名稱：網域\使用者名稱或網域/使用者名稱，或使用者名稱@網域。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。
 - 在 **Active Directory 密碼**文字方塊中，輸入密碼。密碼上限為 127 個字元。
 - 在 **確認密碼**文字方塊中，再次輸入密碼。
 - 若要執行憑證檢查，請選擇下列其中一項：
 - 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**。
 - 若不執行任何檢查，且不儲存憑證，請勿選取**啟用憑證檢查**。
 - 如果不要透過 Active Directory 來設定 iDRAC 認證，請輸入以下資訊：
 - **使用者名稱** — 請以下列其中一種格式輸入使用者名稱：網域\使用者名稱或網域@使用者名稱。
使用者名稱接受以下字元：/ (正斜線)、& (& 符號)、\ (反斜線)、. (英文句點)、" (英文引號)、@ (小老鼠符號)、% (百分比符號) (上限為 127 個字元)。

網域可包含英數字元，例如- (破折號) 和 . (英文句點) (上限為 254 個字元)。網域的第一個和最後一個字元必須為英數字元。

- **密碼** — 請輸入密碼。

密碼不接受以下字元：/ (正斜線)、& (& 符號)、\ (反斜線)、. (英文句點)、" (英文引號)。

- **確認密碼** — 請再次輸入您的密碼。
- **啟用憑證檢查** — 依預設，核取方塊已清除。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**。若不執行憑證檢查且不儲存憑證，請勿選取**啟用憑證檢查**核取方塊。

 **註:** 如果您使用 Active Directory，請選取**啟用憑證檢查**。

d. 在**主機根**底下，執行下列作業：

- 若要存取所有與 Active Directory 相關聯的主控台，請選取**使用 Active Directory** 核取方塊。
- **使用者名稱** — 預設使用者名稱是根，無法修改。如果您選取了**使用 Active Directory**，就可以使用任何 Active Directory 使用者名稱。

 **註:** **使用者名稱**是根，如果您沒有選取**使用 Active Directory**，就不能修改這一項。iDRAC 使用者不一定非用根認證不可，如果已設定 Active Directory，就可以使用任何系統管理員權限。


- **密碼** — 請輸入密碼。

密碼不接受以下字元：/ (正斜線)、& (& 符號)、\ (反斜線)、. (英文句點)、" (英文引號)。

- **確認密碼** — 請再次輸入您的密碼。
- **啟用憑證檢查** — 依預設，核取方塊已清除。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**。若不執行任何檢查，且不儲存憑證，請清除**啟用憑證檢查**核取方塊。

 **註:** 如果您使用 Active Directory，請選取**啟用憑證檢查**。

 **註:** OMSA 認證與 ESXi 主機所使用的認證相同。

 **註:** 如果是不具備 iDRAC Express 或 Enterprise 卡的主機，則 iDRAC 測試連線結果會顯示此系統**不適用**。

7. 按一下**下一步**。

8. 在**選取主機**對話方塊中，選取此連線設定檔的主機。

9. 按一下**確定**。


關聯主機對話方塊可讓您在所選的伺服器上測試 iDRAC 與主機認證。

10. 執行下列其中一個步驟：

- 如果不要透過測試認證的方式來建立連線設定檔，請按一下**完成**。
- 若要開始測試，請選取主機加以檢查，然後按一下




。其他選項皆為非使用中。


 **註:** 所有執行 ESXi 6.5 及 / 或更新版本且停用 WBEM 服務的主機測試連線皆失敗。對這類主機而言，WBEM 服務會在您執行這些主機的清查時自動啟用。雖然測試連線失敗，但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。


測試完成之後，請按一下**完成**。


- 若要停止測試，請按一下**中止所有測試**。然後在**終止測試**對話方塊中，按一下**確定**，然後按一下**完成**。


 **註:** **修改日期**和**上次修改者**欄位中，包含您透過 Web 用戶端介面，針對連線設定檔執行的變更。OMiV 裝置在各自連線設定檔所執行的任何變更，都不會影響這兩個欄位的詳細資料。

刪除連線設定檔


 **註:** 清查、保固或部署工作正在執行時，請確定您未刪除與主機具有關聯的連線設定檔。

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**，再按一下**連線設定檔**標籤，然後選取您要刪除的設定檔。
4. 按一下 。
5. 若要移除設定檔，請在刪除確認訊息按一下**是**，若要取消刪除動作，則按一下**否**。

 **註:** OMIVV 不會管理屬於您已刪除之連線設定檔的主機，除非您將這些主機新增到其他連線設定檔。

 **註:** 在刪除連線設定檔前，請務必先刪除排定的韌體更新工作。

測試連線設定檔

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**，按一下**連線設定檔**標籤，然後選取連線設定檔。
4. 在**測試連線設定檔**對話方塊中，選取您要測試的主機，然後按一下  圖示。
如果您未選取連線設定檔，執行測試連線可能會花費一些時間。
5. 若要停止所有選取的測試並取消測試，請按一下**終止所有測試**。在**終止測試**對話方塊中，按一下**確定**。
6. 按一下**取消**即可結束。

關於機箱設定檔

OMIVV 可以監控與 Dell 伺服器相關聯的所有 Dell EMC 機箱。要監控機箱，必須有機箱設定檔。您可以藉由執行下列工作來管理機箱設定檔：

- 檢視機箱設定檔。請參閱[檢視機箱設定檔](#)。
- 建立機箱設定檔。請參閱[建立機箱設定檔](#)。
- 編輯機箱設定檔。請參閱[編輯機箱設定檔](#)。
- 刪除機箱設定檔。請參閱[刪除機箱設定檔](#)。
- 測試機箱設定檔。請參閱[測試機箱設定檔](#)。

檢視機箱設定檔

在檢視之前，請務必先建立機箱設定檔，或是確保有機箱設定檔可讓您檢視。

建立一或多個機箱設定檔之後，您就可以在機箱設定檔頁面上加以檢視了。


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。
隨後便會顯示機箱設定檔。
4. 如果該機箱設定檔與多個機箱相關聯，若要顯示所有關聯機箱，請按一下  圖示。
5. 在**機箱設定檔**頁面上，檢視機箱資訊。


表 8. 機箱設定檔資訊


機箱欄位	說明
設定檔名稱	顯示機箱設定檔的名稱
說明	顯示說明 (如果提供)
機箱 IP/主機名稱	顯示機箱或主機名稱的 IP 位址
機箱服務標籤	顯示指派給機箱的專屬識別碼
修改日期	顯示機箱設定檔修改的日期



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**下一步**。
隨後便會顯示**選取機箱**頁面，顯示所有可用的機箱。

 **註:** 該機箱下任何模組化主機成功執行清查後，機箱方能接受探索，且可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設定檔有關聯。
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. 若要測試機箱連線能力，請選取機箱，然後按一下  圖示以開始驗證認證，其結果會在**測試結果**欄顯示為**通過**或**失敗**。
10. 若要完成設定檔，請按一下**完成**。


編輯機箱設定檔

建立機箱設定檔後，您可以編輯設定檔名稱、說明、關聯的機箱和認證。


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**，按一下**機箱設定檔**標籤，然後選取機箱設定檔。
4. 按一下  圖示 (位於主功能表上)。
Edit Chassis Profile (編輯機箱設定檔) 視窗隨即顯示。
5. 在**機箱設定檔**中，您可以編輯**設定檔名稱**和選填的**說明**。
6. 在**認證**區域中，您可以編輯**使用者名稱**、**密碼**和**確認密碼**。
您在**確認密碼**中輸入的密碼必須和您在**密碼**欄位中輸入的密碼相同。輸入的認證必須具有機箱上的系統管理員權限。
7. 若要儲存變更，請按一下**套用**。
關聯機箱標籤可讓您測試機箱和所選機箱上的認證。執行下列其中一個步驟：
 - 若要開始測試，請選取一個或多個機箱加以檢查，然後按一下  圖示。**測試結果**欄會顯示測試連線是否成功。
 - 您可以在機箱設定檔新增或刪除一或多個機箱。


 **註:** 如果沒有清查機箱，只會顯示 IP/主機名稱和服務標籤。清查機箱之後，就會顯示**機箱名稱**和**型號**這兩個欄位。


刪除機箱設定檔

 **註:** 在刪除機箱設定檔之前，請確定機箱執行個體不屬於 OMIVV 登錄的其他 vCenter。


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. 選取您要刪除的機箱設定檔，然後按一下 。
隨即顯示警告訊息。
5. 若要繼續刪除，請按一下**是**，或者若要取消刪除，請按一下**否**。
如果和機箱設定檔相關聯的所有機箱皆已清除或移到其他設定檔，則會顯示刪除確認訊息，表示機箱設定檔沒有任何相關聯的機箱，並且已經刪除。若要刪除機箱設定檔，請對刪除確認訊息按一下**確定**。

 **註:** OMIVV 不會監控與您已刪除之機箱設定檔相關聯的機箱，除非這些機箱新增至其他機箱設定檔。

 **註:** 如果機箱設定檔被刪除，其相關的保固歷史記錄資料也不會從保固歷史記錄刪除。

測試機箱設定檔

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**，按一下**機箱設定檔**標籤，然後選取單一或多個機箱設定檔來測試。
這個動作可能需要幾分鐘的時間完成。
4. 在**測試機箱設定檔**對話方塊中，選取您要測試的機箱，然後按一下 。
5. 若要中止所有選取的測試並取消測試，請按一下**中止所有測試**。在**終止測試**對話方塊中，按一下**確定**。
6. 按一下**取消**即可結束。

清查和保固管理

設定 OMIVV 之後，您就可以在**監視**標籤底下，監視清查、保固工作、管理部署工作，以及管理韌體更新工作。清查與保固都是在**初始組態精靈**或**設定**標籤中設定。

「工作佇列」頁面管理下列工作：

- 顯示提交的伺服器部署或韌體更新工作。
- 重新整理韌體更新或部署工作，或清查/保固歷史記錄佇列。
- 排程清查或保固工作。
- 清除韌體更新或部署工作佇列項目。

i 註：為確保清查/保固含有最新資訊，請安排一週至少執行一次清查/保固工作。

您可以在本頁面執行的工作包括：

- [管理部署工作](#)
- [管理韌體更新工作](#)
- [管理清查工作](#)
- [管理保固工作](#)

i 註：對於所有提及的工作，如果裝置時間變更為未來日期後又再還原，請確定再次排程這些工作。

i 註：若要進行基本健全狀況監視，請務必將 OMIVV 裝置重新開機。若要進行長時間健全狀況監視，請務必停用**長時間監視**，然後再從 OMIVV 系統管理主控台啟用它。

主題：

- [清查工作](#)
- [保固工作](#)
- [監控單一主機](#)
- [監控叢集與資料中心上的主機](#)
- [設定實體伺服器閃爍指示燈](#)
- [設定系統鎖定模式](#)

清查工作

清查工作是使用**設定**標籤或**初始組態精靈**加以設定。使用**清查歷史記錄**標籤可以檢視所有的清查工作。以下是您可以在本標籤執行的工作：

- [檢視主機或機箱清查](#)
- [修改清查工作排程](#)
- [立即執行機箱清查工作](#)

檢視主機清查

要收集資料必須先順利完成清查。完成清查之後，您就可以檢視整個資料中心或個別主機系統的清查結果。您可以用遞增及/或遞減順序來排序清查檢視的欄。

i 註：以下是無法擷取和顯示主機資料的幾個可能原因：

- 主機未與連線設定檔建立關聯，因此您無法執行清查工作。
- 尚未在主機執行清查工作以收集資料，因此沒有資料可以顯示。
- 超過主機授權數，您必須有額外的授權可用，清查工作才能完成。
- 主機沒有第 12 代以後 PowerEdge 伺服器所需的正確 iDRAC 授權，因此，請購買正確的 iDRAC 授權。
- 認證可能不對。

- 主機可能無法連線。

檢視主機清查詳細資料：

1. 在 OpenManage Integration for VMware vCenter 中，按一下**監視**標籤。
2. 按一下**工作佇列**、展開**清查歷史記錄**，然後按一下**主機清查**。
vCenter 資訊會顯示在上方格線中。
3. 若要檢視所選 vCenter 的主機資訊，請選取 vCenter 以顯示所有相關聯的主機詳細資料。
4. 檢視主機清查資訊。

表 9. vCenter、主機資訊

vCenter	
vCenter	顯示 vCenter 位址
已通過主機	顯示任何已通過的主機
上一次清查	顯示上一次執行清查排程的日期與時間
下一次清查	顯示下一次執行清查排程的日期與時間
主機	
主機	顯示主機位址。
狀態	顯示狀態。選項包括： <ul style="list-style-type: none"> • 成功 • 故障 • 進行中 • 已排程
持續時間 (分: 秒)	以分和秒格式顯示工作的持續時間
開始日期與時間	顯示清查排程開始時的日期和時間
結束日期與時間	顯示清查排程結束的時間


檢視機箱清查

要收集資料必須先順利完成清查。您可以用遞增及/或遞減順序來排序清查檢視的欄。

1. 在 OpenManage Integration for VMware vCenter 中，按一下**監視**標籤。
2. 按一下**工作佇列**，展開**清查歷史記錄**，然後按一下**機箱清查**。
3. 檢視機箱清查資訊。

表 10. 機箱資訊

機箱庫存	
機箱 IP	顯示機箱 IP 位址
服務標籤	顯示機箱的服務標籤。服務標籤是製造商提供的唯一識別碼，用於支援與維護
狀態	顯示機箱的狀態
持續時間 (分: 秒)	以分和秒格式顯示工作的持續時間
開始日期與時間	顯示清查排程開始時的日期和時間
結束日期與時間	顯示清查排程結束的時間

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



修改清查工作排程


若要確定有最新的主機資訊，請安排每週至少執行基本次數的清查工作。清查工作僅耗用最少的資源，不會降低主機效能。您可以從**初始組態精靈**或**監視**標籤變更清查工作排程。

清查工作排程會設定執行清查工作的時間或日期，例如：

- 每週特定時間和選取的日子
- 在設定的時間間隔

若要在主機系統上執行清查，請建立提供通訊和驗證資訊的連線設定檔。

1. 在 OpenManage Integration for VMware vCenter 按一下**監視**標籤。
2. 按一下**工作佇列**、**清查歷史記錄**，然後按一下**主機清查**。
3. 選取 vCenter，然後按一下.
4. 請在**清查資料擷取**對話方塊中執行下列步驟：
 - a. 在**清查資料**下，選取**啟用清查資料擷取**核取方塊。
 - b. 在**清查資料擷取排程**下，選取一週哪幾天要工作。
 - c. 在**清查資料擷取時間**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。
5. 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**。
6. 若要立即執行工作，請從 OpenManage Integration for VMware vCenter 的**監視** > **工作佇列**標籤上，按一下**清查歷史記錄** > **主機清查**。
7. 按一下，然後在**成功**對話方塊中按一下**關閉**。


 **註:** 執行模組化主機清查時，會自動探索對應的機箱。如果機箱已是機箱設定檔的一部分，則執行主機清查後，就會自動執行機箱清查。

立即排程清查工作之後，清查工作目前在佇列中。您無法執行單一主機的清查。清查工作的範圍涵蓋所有主機。

執行清查工作

1. **組態精靈**完成後，所有新增至連線設定檔的主機都會自動觸發清查。後續若要隨選執行清查，請按一下**工作佇列** > **清查** > **立刻執行**，即可執行清查工作。
2. 若要查看清查工作的狀態，請按一下**重新整理**。
3. 導覽至**主機與叢集**檢視、按一下任何 **Dell 主機**，然後按一下 **OpenManage Integration** 標籤。隨後應該就會顯示以下資訊：

- 概觀頁面
- 系統事件記錄
- 硬體清單
- 存放時
- 韌體
- 電源監視

 **註:** 清查工作會略過超過授權限制的主機，並標示為故障。

OpenManage Integration 索引標籤可以使用下列主機命令：

- 閃爍指示燈
- 執行韌體更新精靈
- 啟動遠端存取
- 啟動 OMSA
- 啟動 CMC
- 設定系統鎖定模式


立即執行機箱清查工作

您可以在**機箱清單**索引標籤檢視和執行機箱清查工作。

1. 在 OpenManage Integration for VMware vCenter 按一下**監視**標籤。
2. 按一下**工作佇列**、**清查歷史記錄**，然後按一下**機箱清查**。

顯示機箱清單及其最後清查工作的狀態。

註: 執行排程機箱清查的時間和排程的主機清查時間相同。

- 按一下 。
- 更新的已清查機箱清單隨即顯示，而且以**成功**或**失敗**的方式說明每個機箱的狀態。

保固工作

硬體保固資訊可從 Dell 線上擷取，並由 OMIVV 顯示。伺服器的服務標籤可用來收集伺服器的相關保固資訊。保固資料擷取工作可使用**初始組態精靈**加以設定。

您可以在本標籤執行的工作包括：

- 檢視保固歷史記錄
- 修改保固工作排程
- 立即執行主機保固工作
- 立即執行機箱保固工作

檢視保固歷史記錄

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。您可以用遞增及/或遞減順序來排序清查檢視的欄。

註: 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。請參閱 [設定 HTTP 代理](#) 第頁的 17。

- 在 OpenManage Integration for VMware vCenter 按一下 **監視** 標籤。
- 按一下 **工作佇列**，然後按一下 **保固歷史記錄**。
- 展開 **保固歷史記錄** 以顯示 **主機保固** 和 **機箱保固**。
- 若要檢視對應的保固工作歷史記錄資訊，請選取 **主機保固**，然後選取 vCenter 以顯示所有相關聯的主機詳細資料。

表 11. VCenter、主機歷史記錄資訊

vCenter 歷史記錄	
vCenter	顯示 vCenter 清單
已通過主機	顯示已傳送的 vCenter 主機數目
上一個保固	顯示上一次執行保固工作的日期與時間
下一個保固	顯示下一次執行保固工作的日期與時間
主機歷史記錄	
主機	顯示主機位址
狀態	顯示狀態。選項包括： <ul style="list-style-type: none">成功故障進行中已排程
持續時間 (分:秒)	以分:秒格式顯示保固工作的持續時間
開始日期與時間	顯示保固工作開始時的日期和時間
結束日期與時間	顯示保固工作結束的時間

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。您可以用遞增及/或遞減順序來排序清查檢視的欄。


1. 在 OpenManage Integration for VMware vCenter 按一下 **監視** 標籤。
2. 按一下 **工作佇列**，然後按一下 **保固歷史記錄**。
3. 展開 **保固歷史記錄** 以顯示 **主機保固** 和 **機箱保固**。
4. 按一下 **機箱保固**。
5. 檢視機箱保固詳細資料。

表 12. 機箱資訊

機箱歷史記錄	
機箱 IP	顯示機箱 IP 位址
服務標籤	顯示機箱的服務標籤。服務標籤是製造商提供的唯一識別碼，用於支援與維護
狀態	顯示機箱的狀態
持續時間 (分: 秒)	以分:秒格式顯示保固工作的持續時間
開始日期與時間	顯示保固工作開始時的日期和時間
結束日期與時間	顯示保固工作結束的時間


修改保固工作排程


保固工作最初是在 **初始組態精靈** 中設定。您可以從 **設定** 標籤修改保固工作排程。

1. 在 OpenManage Integration for VMware vCenter 按一下 **監視** 標籤。
2. 按一下 **工作佇列**，然後按一下 **保固歷史記錄**。
3. 展開 **保固歷史記錄** 以顯示 **主機保固** 和 **機箱保固**。
4. 若要檢視您的對應保固工作歷史記錄資訊，請選取 **主機保固** 或 **機箱保固**。
5. 按一下 。
6. 在 **保固資料擷取** 對話方塊中，執行下列步驟：
 - a. 在 **保固資料** 底下，選取 **啟用保固資料擷取** 核取方塊。
 - b. 在 **保固資料擷取排程** 底下，選取一週哪幾天要進行保固工作。
 - c. 在 **保固資料擷取時間** 文字方塊中，輸入此工作的當地時間。
您可能必須計算在適當時間執行此工作所需的時間差。
7. 按一下 **套用**。

立即執行主機保固工作


每週至少執行一次保固工作。

1. 在 OpenManage Integration for VMware vCenter 按一下 **監視** 標籤。
2. 按一下 **工作佇列**，然後按一下 **保固歷史記錄**。
3. 展開 **保固歷史記錄** 以顯示 **主機保固** 和 **機箱保固**。
4. 若要檢視您的對應保固工作歷史記錄資訊，請選取 **主機保固** 或 **機箱保固**。
5. 選取您要執行的保固工作，然後按一下 .
6. 在 **成功** 對話方塊中，按一下 **關閉**。
保固工作目前佇列中。

 **註:** 主機保固一執行，所有機箱的機箱保固便會自動執行。在具備多個 vCenter 的 SSO 環境中，只要任何 vCenter 的保固是以手動方式執行，每個 vCenter 的機箱保固便會自動執行。

立即執行機箱保固工作

每週至少執行一次保固工作。

1. 在 OpenManage Integration for VMware vCenter 中，瀏覽至**監視 > 工作佇列**標籤。
2. 若要選取您要執行的保固工作，請按一下**保固歷史記錄**，然後按一下**機箱保固**。
3. 按一下 。
4. 在**成功**對話方塊中，按一下**關閉**。
保固工作目前佇列中。

監控單一主機

OpenManage Integration for VMware vCenter 可讓您檢視單一主機的詳細資訊。您可以從「**導覽**」窗格 (可顯示所有廠商的所有主機) 的 VMware vCenter 中存取主機。若要尋找更詳細的資訊，請按一下特定的 Dell EMC 主機。若要檢視 Dell EMC 主機的清單，請在 OpenManage Integration for VMware vCenter 的「**導覽**」窗格中，按一下 **Dell EMC 主機**。

檢視主機摘要詳細資料

您可以在**主機摘要**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。其中的兩個 Portlet 可用於 OpenManage Integration for VMware vCenter。這兩個 Portlet 是：

- Dell EMC 主機健全狀況
- Dell EMC 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 OpenManage Integration for VMware vCenter 的「**瀏覽**」窗格中，按一下**主機**。
2. 在**物件**標籤上，選取您想要檢視的特定主機。
3. 按一下**摘要**索引標籤。
4. 檢視主機摘要的詳細資料：

表 13. 主機摘要資訊

資訊	說明
備用系統	在狀態區域下方與 Portlet 前方的黃色方塊中顯示 OpenManage Integration for VMware vCenter 的警示。
通知區域	在右側面板區域中顯示 Dell 產品整合資訊，您可在其中找到下列相關資訊： <ul style="list-style-type: none">● 最近的工作● 進行中的工作● 警示 Dell 警報資訊顯示在通知區域 Portlet。

5. 向下捲動即可檢視 Dell EMC Server Management Portlet。

表 14. Dell EMC 伺服器管理 Portlet

資訊	說明
服務標籤	顯示 PowerEdge 伺服器的服務標籤。請使用此 ID 撥打電話請求支援。
機型名稱	顯示伺服器的機型名稱。
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 或更新版本的第 12 代及更新版本的 PowerEdge 伺服器。BIOS 屬性的四個不同值是：

表 14. Dell EMC 伺服器管理 Portlet (續)

資訊	說明
	<ul style="list-style-type: none"> ● 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	顯示第 14 代 PowerEdge 伺服器 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	<p>顯示資訊如下：</p> <ul style="list-style-type: none"> ● 主機名稱 — 顯示 Dell EMC 主機的名稱 ● 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 ● 連線設定檔 — 顯示此主機的連線設定檔名稱 ● 型號 — 顯示 Dell EMC 伺服器型號 ● 服務標籤 — 顯示伺服器的服務標籤 ● 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	<p>顯示資訊如下：</p> <ul style="list-style-type: none"> ● 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	<p>管理主控台用於啟動外接式系統管理主控台，例如：</p> <ul style="list-style-type: none"> ● 啟動遠端存取主控台 (iDRAC) — 啟動整合式 Dell 遠端存取控制器 (iDRAC) Web 使用者介面。 ● 啟動 OMSA 主控台 — 啟動 OMSA 主控台以存取 OpenManage 伺服器管理員使用者介面。
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 閃爍指示燈 。

6. 檢視 Dell EMC 主機健全狀況 Portlet：

表 15. Dell EMC 主機健全狀況

資訊	說明
Dell EMC 主機健全狀況	<p>元件的健全狀況是以圖形表示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：健康和警告或嚴重 (裡面有橘色驚嘆號的倒三角形)。整體狀況是根據狀況參數最差的機箱顯示狀況。選項包括：</p> <ul style="list-style-type: none"> ● 健康 (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。

表 15. Dell EMC 主機健全狀況

資訊	說明
	<ul style="list-style-type: none"> 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，如果有五個健康符號和一個警告符號，整體健全狀況會顯示為警告。

i 註: 若為接線式 PSU，則無法在 OMIVV 使用電源監控。

檢視單一主機的硬體詳細資料

您可以在 **Dell EMC 主機資訊** 標籤上檢視單一主機的硬體詳細資料。若要在此頁面上顯示資訊，請執行清查工作。硬體檢視可以直接報告 OMSA 與 iDRAC 的資料。請參閱 [執行清查工作](#)。

1. 在 OpenManage Integration for VMware vCenter 的「瀏覽」窗格中，按一下**主機**。
2. 在**主機**標籤上，選取您想要檢視硬體：<Component Name> 詳細資料的特定主機。
3. 在**監視**標籤中，選取 **Dell EMC 主機資訊** 標籤。

i 註: 如果系統鎖定模式已為第 14 代主機開啟，最上方會顯示具有鎖定圖示的黃色帶。

在硬體：<Component Name> 子標籤上，檢視每個元件的下列資訊。

表 16. 單一主機的硬體資訊

硬體：元件	資訊
硬體：FRU	<ul style="list-style-type: none"> 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 — 顯示製造廠商序號 製造日期 — 顯示製造日期
硬體：處理器	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 類型 — 顯示電源供應器的類型。電源供應器類型包括： <ul style="list-style-type: none"> 不明 線性 切換中 電池 UPS 轉換器 穩壓器 AC 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)
硬體：記憶體	<ul style="list-style-type: none"> 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
硬體：NIC	<ul style="list-style-type: none"> 總計 — 顯示可用網路介面卡的總計數

表 16. 單一主機的硬體資訊 (續)

硬體：元件	資訊
	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> PCI 插槽 — 顯示已使用、總計及可用的 PCI 插槽 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	<ul style="list-style-type: none"> 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

檢視單一主機的儲存裝置詳細資料

您可以在 **Dell EMC 主機資訊** 標籤上檢視單一主機的儲存裝置詳細資料。若要在此頁面上顯示資訊，請執行清查工作。硬體會直接報告來自 OMSA 和 iDRAC 的資料。請參閱 [執行清查工作](#)。頁面會根據 **檢視** 下拉式清單中所選取的內容，來顯示不同的選項。如果您選取 **實體磁碟**，則會出現其他下拉式清單。下一個下拉式清單稱為「篩選」，可讓您篩選實體磁碟選項。若要檢視儲存裝置詳細資料：

1. 在 OpenManage Integration for VMware vCenter 的「瀏覽」窗格中，按一下 **主機**。
2. 在 **物件** 標籤中，選取您想要檢視「儲存裝置：實體磁碟」詳細資料的主機。
3. 在 **監視** 標籤中，選取 **Dell EMC 主機資訊** 標籤。

在 **儲存裝置** 子標籤上，檢視下列項目：

表 17. 單一主機的儲存裝置詳細資料

元件	資訊
儲存	顯示虛擬磁碟、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。從「檢視」下拉式清單選取時，選取的選項會反白顯示。
檢視	顯示您要檢視此主機的選項： <ul style="list-style-type: none"> ● 虛擬磁碟 ● 實體磁碟 ● 控制器 ● 機箱

檢視「檢視」選項的儲存裝置詳細資訊

主機儲存裝置頁面上的儲存裝置選項，取決於您從 **檢視** 下拉式清單選取的選項。

從「檢視」下拉式清單選取任一上述選項，並檢視下列項目：

表 18. 單一主機的儲存裝置詳細資料

資訊	說明
虛擬磁碟	<ul style="list-style-type: none"> ● 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

表 18. 單一主機的儲存裝置詳細資料 (續)

資訊	說明
	<ul style="list-style-type: none"> ● 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 ● 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 — 顯示虛擬磁碟所包括之實體磁碟所使用的技術。可能的值如下： <ul style="list-style-type: none"> ○ 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： <ul style="list-style-type: none"> ○ 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： <ul style="list-style-type: none"> ○ 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 ● 快取原則 — 啟用快取原則時顯示
<p>實體磁碟 — 當您選取此選項時，將顯示篩選下拉式清單。</p> <p>您可根據下列選項篩選實體磁碟：</p> <ul style="list-style-type: none"> ● 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自訂名稱的虛擬磁碟 	<ul style="list-style-type: none"> ● 名稱 — 顯示實體磁碟的名稱 ● 裝置 FGDD — 顯示裝置 FGDD ● 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： <ul style="list-style-type: none"> ○ 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 ● 熱備援磁碟類型 — 顯示熱備援磁碟類型。選項包括： <ul style="list-style-type: none"> ○ 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 ● 連接器 ID — 顯示連接器 ID ● 機櫃 ID — 顯示機櫃 ID

表 18. 單一主機的儲存裝置詳細資料 (續)

資訊	說明
	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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
機箱	<ul style="list-style-type: none"> ● 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 ● 服務標籤 — 顯示服務標籤

關於 Web 用戶端中的系統事件記錄

系統事件記錄 (SEL) 會針對 OMIVV 探索到的硬體提供狀態資訊，並根據以下準則顯示資訊：

狀態 狀態圖示有以下幾種：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)。

時間 (伺服器時間) 表示事件發生的時間與日期。

搜尋此頁面 顯示特定訊息、伺服器名稱、組態設定等。

嚴重程度定義如下：

資訊 OMIVV 作業已順利完成。

警告 OMIVV 作業部分失敗，部分成功。

錯誤 OMIVV 作業失敗。

您可以將記錄儲存為外部 CSV 檔案。請參閱[顯示個別主機的系統事件記錄](#)。


顯示單一主機的事件記錄

若要顯示事件，請執行下列步驟：

1. 若要存取**監視標籤**，並開啟**系統事件記錄**子標籤，請執行以下任一步驟：

選項	說明
從 OMIVV	在本選項執行以下步驟： <ol style="list-style-type: none"> a. 在 OpenManage Integration for VMware vCenter 的「瀏覽」窗格中，按一下主機。 b. 在物件標籤上，按兩下您要檢視 SEL 記錄的特定主機。
從首頁	在首頁上，按一下 主機與叢集 。

2. 在**監視標籤**中，選取 **Dell EMC 主機資訊 > 系統事件記錄**。
最近的系統記錄項目會提供 10 筆最近的系統事件記錄項目。
3. 若要更新**系統事件記錄**，請執行全域重新整理。

4. 若要限制 (篩選) 事件記錄項目的數目，請選擇以下一個選項：
 - 若要在搜尋篩選文字方塊中動態篩選記錄項目，請輸入文字字串。
 - 若要清除篩選文字方塊，請按一下 **X**，所有事件記錄項目便會全部顯示出來。
5. 若要清除所有事件記錄項目，請按一下 **清除記錄檔**。
隨後便會出現一則訊息，表明所有記錄項目一經清除後就會刪除，而且您可以選擇以下其中一個選項：
 - 若同意清除記錄項目，請按一下 **清除記錄檔**。
 - 若要取消，請按一下 **取消**。
6. 若要將事件記錄匯出成 .CSV 檔案，請按一下 。
7. 若要瀏覽到該位置，並儲存系統事件記錄，請按一下 **儲存**。



檢視單一主機的其他硬體詳細資料

您可以在 **Dell 主機資訊** 標籤上檢視單一主機的韌體、電源監控、保固狀態等詳細資料。若要在此頁面上顯示資訊，請執行清查工作。硬體檢視會直接報告 OMSA 和 iDRAC 的資料。請參閱 [立即執行機箱清查工作](#)。

1. 在 OpenManage Integration for VMware vCenter 的「瀏覽」窗格中，按一下 **主機**。
2. 在 **物件** 標籤上，選取您想要檢視 <Component Name> 詳細資料的特定主機。
3. 在 **監視** 標籤中，選取 **Dell EMC 主機資訊** 標籤。

在硬體：<Component Name> 子標籤上，檢視每個元件的下列資訊：

表 19. 單一主機資訊

元件	資訊
韌體 主機頁面可讓您使用搜尋、篩選並匯出韌體資訊的 CSV 檔案	<ul style="list-style-type: none"> ● 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
電源監視  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。	<ul style="list-style-type: none"> ● 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 <ul style="list-style-type: none"> ● 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。 ● 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 — 顯示系統尖峰電源耗用時的系統尖峰電源統計資料 (瓦數)
保固  註： 若要檢視保固狀態，請務必執行保固工作。請參閱 執行保固擷取工作 。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。	<ul style="list-style-type: none"> ● 提供者 — 顯示保固提供者的名稱 ● 說明 — 顯示說明 ● 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 ● 剩下天數 — 顯示保固的剩餘天數 ● 上次更新 — 保固的最後一次更新

監控叢集與資料中心上的主機

OpenManage Integration for VMware vCenter 可讓您檢視資料中心或叢集所含之所有主機的詳細資訊。您可以按一下資料格列標題來排序資料。資料中心和叢集頁面可讓您將資訊匯出成 CSV 檔案，並在資料格上提供篩選或搜尋功能。

檢視資料中心和叢集的概觀

在 [Dell EMC 資料中心/叢集資訊] 標籤上，檢視資料中心或叢集的主機詳細資料。若要在此頁面上顯示資訊，請執行清查工作。您看到的資料取決於存取資料使用的檢視畫面。硬體檢視會直接報告 OMSA 和 iDRAC 的資料。請參閱 [執行清查工作](#)。

i 註：資料中心與叢集頁面可讓您將資訊匯出成 .CSV 檔案，並在資料格提供篩選或搜尋功能。

1. 在 OpenManage Integration for VMware vCenter 的 [瀏覽] 窗格中，按一下 **vCenter**。
2. 按一下 **資料中心或叢集**。
3. 在物件標籤中，選取您想要檢視主機詳細資料的特定資料中心或叢集。
4. 在監視標籤中，選取 **Dell EMC 資料中心/叢集資訊 > 概觀** 標籤，然後檢視詳細資料。

i 註：若要顯示詳細資料的完整清單，從資料格線選取特定主機。

表 20. 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： <ul style="list-style-type: none"> ● 資料中心/叢集名稱 ● Dell 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： <ul style="list-style-type: none"> ● 已開啟 ● 已關閉 ● 不適用 (僅適用於第 14 代伺服器)
硬體資源	顯示資訊如下： <ul style="list-style-type: none"> ● 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： <ul style="list-style-type: none"> ● 過期的保固 ● 作用中的保固 ● 未知的保固
主機	顯示主機名稱
服務標籤	顯示主機服務標籤
機型	顯示 PowerEdge 機型
資產標籤	顯示資產標籤 (如果已設定)
機箱服務標籤	顯示機箱服務標籤 (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	僅適用於第 14 代 PowerEdge 伺服器：顯示主機的 iDRAC 鎖定模式，包括已開啟、已關閉或不明。 對於第 14 代之前的所有 PowerEdge 伺服器，顯示的系統鎖定模式是 [不適用]。
iDRAC IP	顯示 iDRAC IP 位址
服務主控台 IP	顯示服務主控台 IP
CMC URL	顯示 CMC URL (刀鋒伺服器的機箱 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

表 20. 資料中心和叢集的概觀 (續)

資訊	說明
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
連線設定檔	顯示連線設定檔名稱
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詳細資料

您可以在 **Dell EMC 資料中心/叢集資訊** 標籤上，檢視單一主機的硬體詳細資料。若要在此頁面上顯示資訊，請執行清查工作。資料中心和叢集頁面可讓您將資訊匯出成 CSV 檔案，並在資料格上提供篩選或搜尋功能。您會看到哪些資料，要視您在哪一個檢視處理資料而定。硬體檢視可以直接報告 OMSA 與 iDRAC 的資料。請參閱 [執行清查工作](#)。

1. 在 OpenManage Integration for VMware vCenter 的「導覽」窗格中，按一下 **vCenter 清查清單**。
2. 按一下 **資料中心或叢集**。
3. 在物件標籤上，選取您要檢視元件專屬詳細資料的特定資料中心或叢集。
4. 在監視標籤中，選取 **Dell EMC 資料中心/叢集資訊** 標籤。

在硬體：<Component Name> 子標籤上，檢視每個元件的下列資訊。

表 21. 資料中心和叢集的硬體資訊

硬體：元件	資訊
硬體：FRU	<ul style="list-style-type: none"> ● 主機 — 顯示主機名稱 ● 服務標籤 — 顯示主機的服務標籤 ● 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 — 顯示製造廠商序號 ● 製造日期 — 顯示製造日期
硬體：處理器	<ul style="list-style-type: none"> ● 主機 — 顯示主機名稱 ● 服務標籤 — 顯示主機的服務標籤 ● 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	<ul style="list-style-type: none"> ● 主機 — 顯示主機名稱 ● 服務標籤 — 顯示主機的服務標籤 ● 類型 — 顯示電源供應器的類型。電源供應器類型包括： <ul style="list-style-type: none"> ○ 不明 ○ 線性 ○ 切換中 ○ 電池 ○ UPS ○ 轉換器 ○ 穩壓器 ○ AC ○ 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)

表 21. 資料中心和叢集的硬體資訊 (續)

硬體：元件	資訊
	<ul style="list-style-type: none"> ● 狀態 — 顯示電源供應器的狀態。狀態選項包括： <ul style="list-style-type: none"> ○ 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	<ul style="list-style-type: none"> ● 主機 — 顯示主機名稱 ● 服務標籤 — 顯示主機的服務標籤 ● 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	<ul style="list-style-type: none"> ● 主機 — 顯示主機名稱 ● 服務標籤 — 顯示主機的服務標籤 ● 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	<ul style="list-style-type: none"> ● 主機 — 顯示主機名稱 ● 服務標籤 — 顯示主機的服務標籤 ● 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	<ul style="list-style-type: none"> ● 主機 — 顯示主機名稱 ● 服務標籤 — 顯示主機的服務標籤 ● 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

檢視資料中心和叢集的儲存裝置詳細資料

您可以在**資料中心/叢集資訊**標籤上，檢視資料中心或叢集的實體儲存裝置詳細資料。若要在此頁面上顯示資訊，請執行清查工作。資料中心和叢集頁面可讓您將資訊匯出成 CSV 檔案，並在資料格上提供篩選/搜尋功能。硬體檢視可以直接報告 OMSA 與 iDRAC 的資料。請參閱[執行清查工作](#)。

1. 在 OpenManage Integration for VMware vCenter 的「導覽」窗格中，按一下 **vCenter 清查清單**。
2. 按一下**資料中心或叢集**。
3. 在**物件**標籤中，選取特定的資料中心或叢集。
4. 在**監視**標籤中，選取 **Dell EMC 資料中心/叢集資訊**標籤，然後瀏覽至**儲存 > 實體磁碟/虛擬磁碟**。
若要顯示詳細資料的完整清單，從資料格線選取特定主機。

表 22. 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	<ul style="list-style-type: none"> ● 主機 — 顯示主機名稱 ● 服務標籤 — 顯示主機的服務標籤

表 22. 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
	<ul style="list-style-type: none"> ● 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： <ul style="list-style-type: none"> ○ 線上 ○ 就緒 ○ 受損 ○ 故障 ○ 離線 ○ 重建中 ○ 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.com/support 中的 Dell EMC OpenManage Server Administrator 儲存管理使用者指南 ● 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 ● 熱備援磁碟類型 — 顯示熱備援磁碟類型。選項包括： <ul style="list-style-type: none"> ○ 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 ● 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
<p>虛擬磁碟</p>	<ul style="list-style-type: none"> ● 主機 — 顯示主機名稱 ● 服務標籤 — 顯示主機的服務標籤 ● 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 SSD 或 HDD ● 匯流排通訊協定 — 顯示虛擬磁碟所包括之實體磁碟所使用的技術。可能的值如下： <ul style="list-style-type: none"> ○ SCSI ○ SAS ○ SATA ● 等量大小 — 顯示等量大小，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： <ul style="list-style-type: none"> ○ 預先讀取 (Read-Ahead) ○ 未預先讀取

表 22. 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
	<ul style="list-style-type: none"> ○ 調整預先讀取 (Adaptive Read Ahead) ○ 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： <ul style="list-style-type: none"> ○ 回寫 (Write-Back) ○ 強制回寫 ○ 回寫已啟用 ○ 寫入 (Write-Through) ○ 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： <ul style="list-style-type: none"> ○ 已啟用 — 快取 I/O ○ 已停用 — 直接 I/O

檢視資料中心和叢集的其他硬體詳細資料

您可以在 **Dell EMC 資料中心/叢集資訊** 標籤上檢視資料中心和叢集的韌體、電源監控、保固狀態等詳細資料。若要在此頁面上顯示資訊，請執行清查工作。資料中心和叢集頁面可讓您將資訊匯出成 CSV 檔案，並在資料格上提供篩選/搜尋功能。硬體檢視會直接報告 OMSA 和 iDRAC 的資料。請參閱 [立即執行清查工作](#)。

1. 在 OpenManage Integration for VMware vCenter 的「瀏覽」窗格中，按一下 **vCenter**。
2. 按一下 **資料中心或叢集**。
3. 在物件標籤中，選取您想要檢視主機元件詳細資料的特定資料中心或叢集。
4. 在監視標籤中，選取 **Dell EMC 資料中心/叢集資訊** 標籤。

在 <Component Name> 子標籤上，檢視每個元件的下列資訊：

表 23. 單一主機資訊


元件	資訊
韌體	<ul style="list-style-type: none"> ● 主機 — 顯示主機名稱 ● 服務標籤 — 顯示主機的服務標籤 ● 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
電源監視  註： 若要顯示詳細資料的完整清單，從資料格線選取特定主機。	<ul style="list-style-type: none"> ● 主機 — 顯示主機名稱 ● 服務標籤 — 顯示主機的服務標籤 ● 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

表 23. 單一主機資訊 (續)

元件	資訊
	<ul style="list-style-type: none"> ● 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
保固摘要 ⓘ 註: 若要檢視保固狀態，請務必執行保固工作。請參閱 執行保固擷取工作 。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。	<ul style="list-style-type: none"> ● 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 ● 服務標籤 — 顯示主機的服務標籤。 ● 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： <ul style="list-style-type: none"> ○ 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

設定實體伺服器閃爍指示燈

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. 在 OpenManage Integration for VMware vCenter 中，按一下「導覽」區域中清查清單下的主機。
2. 在物件標籤中，連按兩下您想要的主機。
3. 在摘要標籤中，向下捲動至 Dell EMC 伺服器管理 Portlet。
4. 在主機動作選取閃爍指示燈。
5. 請選擇下列其中一個選項：
 - 若要開啟閃爍並設定時段，在指示燈對話方塊中，按一下閃爍開啟，然後使用逾時下拉式清單選取逾時增加大小，然後按一下確定。
 - 若要關閉閃爍，在指示燈對話方塊中，按一下閃爍關閉，然後按一下確定。

設定系統鎖定模式

系統鎖定模式設定可用在第 14 代 PowerEdge 伺服器的 iDRAC 中。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，開啟或關閉受管理之主機的系統鎖定模式。

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。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 設目的地。

若要設定在主機或叢集等級的主機或叢集的系統鎖定模式，請執行下列步驟：

1. 若要啟動「設定系統鎖定模式精靈」，請執行下列子步驟之一：
 - a. 在導覽窗格中，按一下主機與叢集，選取並以滑鼠右鍵按一下主機或叢集，接著按一下動作下拉式清單，然後選取所有 **OpenManage Integration 動作 > 設定系統鎖定模式**。
 - b. 在 OpenManage Integration 中，按一下主機或叢集頁面，選取並以滑鼠右鍵按一下主機或叢集，或選取主機或叢集，然後按一下動作下拉式清單，然後選取所有 **OpenManage Integration 動作 > 設定系統鎖定模式**。
 - c. 在導覽窗格中，選取主機，然後依序按一下摘要 > Dell EMC 主機資訊 > 設定系統鎖定模式。
 - d. 在導覽窗格中，選取主機或叢集，然後按一下監控 > Dell EMC 主機資訊 > 韌體 > 設定系統鎖定模式。
2. 若要啟用系統鎖定模式，請選擇開啟選項，或停用鎖定模式，請選取關閉。
3. 按一下套用。

如果您嘗試為第 11 至第 13 代 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。

在系統鎖定組態完成後，您可以檢視**工作佇列**頁面中鎖定模式的更新狀態。鎖定模式的工作佇列資訊僅在叢集等級有效。若要存取工作佇列頁面，請在 OpenManage Integration 中，選取**監視 > 工作佇列 > 系統鎖定模式工作**。請參閱 iDRAC 文件，以獲得更多關於系統鎖定模式的資訊。

事件、警報及健全狀況監控

硬體管理的目標為提供系統狀況狀態和最新的基礎結構資訊，系統管理員需要這些內容來回應嚴重硬體事件，而不必離開 OMIVV 外掛程式或 vCenter。

資料中心與主機系統監控會在 vCenter 的**工作與事件**標籤上，顯示硬體 (伺服器及儲存裝置) 與虛擬化相關事件，讓管理員監控基礎結構的健全狀況。此外，嚴重硬體警示可以觸發 OpenManage Integration for VMware vCenter 警報，而一些針對 Dell 虛擬化相關事件定義的警報能讓受管理的主機系統進入維護模式。

若要從伺服器接收事件，請將 OMIVV 設定為所有受監控裝置上的陷阱目的地，各個目的地如下所示：

- 針對第 12 代及之後的主機，SNMP 陷阱目的地是在 iDRAC 中設定。
- 針對第 12 代以前的主機，陷阱目的地是在 OMSA 中設定。
- 針對機箱，陷阱目的地是在 CMC 中設定。

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 代以前主機，OMIVV 僅支援 SNMP v1 警示。

若要監控，請執行下列步驟：

- 進行**事件與警報**設定。
- 必要時，設定 SNMP OMSA 陷阱目的地。
- 使用 vCenter 中的**工作與事件**標籤檢查事件資訊。

主題：

- [關於主機的事件與警報](#)
- [關於機箱的事件與警報](#)
- [虛擬化相關事件](#)
- [主動式 HA 事件](#)
- [檢視警報和事件設定](#)
- [檢視事件](#)
- [硬體元件冗餘健全狀況 — 主動式 HA](#)
- [啟動管理主控台](#)

關於主機的事件與警報

您可以從**管理 > 設定**標籤內的 OpenManage Integration for VMware vCenter 編輯事件與警報。在這裡，您可以選取事件張貼等級、啟用 Dell EMC 主機的警報，或還原預設警報。您可以為每個 vCenter，或一次為所有已登錄的 vCenter 設定事件與警報。

以下是四個事件張貼等級：

表 24. 事件張貼等級

事件	說明
請勿發佈任何事件	不讓 OpenManage Integration for VMware vCenter 轉寄任何事件或警示到相關的 vCenter。
張貼所有事件	發佈所有事件，包括非正式事件，OpenManage Integration for VMware vCenter 從受管 Dell EMC 主機接收後會轉寄到相關的 vCenter。
只張貼關鍵及警告事件	僅張貼嚴重性屬於嚴重或警告的事件到相關的 vCenter。
僅張貼虛擬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。

您設定事件與警報時，可以啟用它們。當啟用時，嚴重硬體警報會觸發 OMIVV 設備，使主機系統進入維護模式，並在某些情況下，會移轉虛擬機器到另一個主機系統。OpenManage Integration for VMware vCenter 會轉送從管理型 Dell EMC 主機收到的事件，並為那些事件建立警報。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，雙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。DRS 會持續監控跨資源集區的使用量，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 執行個體上的叢集。請確認叢集受到影響，然後再啟用事件與警報。

如果必須還原預設警報設定，可以使用**重設預設的警報**按鈕。此按鈕是方便的選項，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 警報組態，使用這個按鈕即可還原那些變更。

註：若要接收 Dell 事件，請務必啟用事件。

註：OpenManage Integration for VMware vCenter 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 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。

關於機箱的事件與警報

對應至機箱的事件與警報只會在 vCenter 層級顯示。在每個 vCenter 中，主機的事件與警報設定也適用於機箱層級。您可以在 OpenManage Integration for VMware vCenter 的**管理 > 設定**標籤內，編輯事件與警報設定。您可以在此選取事件張貼等級、啟用 Dell EMC 主機和機箱的警報，或還原預設警報。您可以設定每個 vCenter 的事件與警報，或者一次為所有已登錄的 vCenter 設定事件與警報。

檢視機箱事件

1. 在左窗格中選取 vCenter，然後按一下 vCenter 伺服器。
2. 按一下特定 vCenter。
3. 按一下**監視 > 事件**標籤。
4. 若要檢視更多事件的詳細資料，請選取特定事件。

檢視機箱警報

1. 在左窗格中選取 vCenter，然後按一下 vCenter 伺服器。
2. 按一下特定 vCenter。
隨即顯示警報。僅會顯示前四個警報。
3. 若要檢視完整清單，請按一下**全部顯示**以檢視監視標籤中**所有問題**的詳細清單。
4. 在**觸發的警報**中按一下**警報**以檢視警報定義。

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 25. 虛擬化事件

事件名稱	說明	重要性	建議動作
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

表 25. 虛擬化事件 (續)

事件名稱	說明	重要性	建議動作
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	指定系統中的備援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	指定系統中的備援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
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，但還有足夠的備援，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，且沒有備援，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知故障狀態	警告	無動作

表 25. 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、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、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、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
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：陣列磁碟故障	陣列磁碟故障	錯誤	讓系統進入維護模式

表 25. 虛擬化事件 (續)

事件名稱	說明	重要性	建議動作
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故障	流體快取記憶體磁碟故障	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
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

表 25. 虛擬化事件 (續)


事件名稱	說明	重要性	建議動作
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。檢視系統組態與電源消耗
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。檢視系統組態與電源消耗
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，請檢視系統組態與電源消耗，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。檢視系統組態與電源消耗，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

表 25. 虛擬化事件 (續)

事件名稱	說明	重要性	建議動作
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。檢視系統組態與電源消耗
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。檢視系統組態與電源消耗
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，請檢視系統組態與電源消耗，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。檢視系統組態與電源消耗，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

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：


 註：支援元件的主動式 HA 健全狀況狀態可以為正常 (綠色)、警告 (黃色)、嚴重 (紅色) 或未知 (灰色) 狀態。

表 26. 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

對於啟用主動式 HA 的主機，OMIVV 會使用以下設阱作為觸發程式，以判斷元件的冗餘健全狀況：根據冗餘的健全狀況資訊，系統可能會將主動式 HA 健全狀況更新傳送至該主機的 vCenter。系統不會直接轉送這些設阱至主動式 HA 主機的 vCenter。

表 27. 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
電源設備故障	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
電源設備故障	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

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 OpenManage Integration for VMware vCenter 的**管理 > 設定**標籤中，展開 **vCenter 設定** 底下的**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**。

若要檢視事件張貼等級，請參閱**關於事件與警報**。

檢視事件

請務必先設定事件，之後才能在事件標籤中看到它們。請參閱[設定事件與警報](#)。

在「事件」標籤上檢視主機、叢集或資料中心的事件。

1. 在 OpenManage Integration for VMware vCenter 導覽中，按一下 **主機**、**資料中心** 或 **叢集**。
2. 在 **物件** 標籤上，選取您要檢視事件的特定主機、資料中心或叢集。
3. 在 **監視** 標籤上，按一下 **事件**。
4. 若要檢視事件的詳細資料，請選取特定事件。

硬體元件冗餘健全狀況 — 主動式 HA

i 註: 只有支援受支援元件 (電源供應器、風扇與 iDSDM) 之冗餘健全狀況狀態的伺服器可以使用主動式 HA。

i 註: 透過 OMIVV 設定全域警示時，在主動式 HA 叢集上所設定的主動式 HA 原則可能會受到影響。

i 註: 主動式 HA 只能在有支援電源、風扇和 iDSDM 冗餘的平台上使用。

i 註: 無法設定備援的 PSU (例如，接線式 PSU) 不支援主動式 HA 功能。

主動式 HA 是能與 OMIVV 共同運作的 vCenter (vCenter 6.5 及更新版本) 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。

i 註: 來自 PowerEdge 第 12 代及之後的所有主機，以及屬於連線設定檔並已順利清查的 ESXi 版本 v6.0 及更新版本都能使用主動式 HA。

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：

- 健康 (資訊) — 元件運作正常。
- 警告 (中度降級) — 元件有非重大錯誤。
- 嚴重 (嚴重降級) — 元件有嚴重故障。

i 註: 中度降級與嚴重降級狀態會在事件頁面的 **類型** 欄中顯示為 **警告**。

i 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。

為機架式和直立式伺服器設定主動式 HA

若要為機架式和直立式伺服器進行設定，請執行下列步驟：

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) 正確設定冗餘。

1. 建立連線設定檔並將其與主機建立關聯。請參閱[建立連線設定檔](#)。
2. 確認已成功完成主機清查。請參閱[檢視主機清查](#)。
3. 確認 iDRAC 中的 SNMP 陷阱目的地是設定為 OMIVV 裝置的 IP 位址。

i 註: 請確定在 **OpenManage Integration > 監視 > 記錄** 標籤中，使用者動作記錄確認有可供主動式 HA 叢集使用的主機。

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

若要為模組化伺服器進行設定，請執行下列步驟：

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。

i 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，因為機箱故障會影響其所有刀鋒伺服器。

1. 建立連線設定檔並將其與主機建立關聯。請參閱[建立連線設定檔](#)。
2. 確認已成功完成主機清查。請參閱[檢視主機清查](#)。
 - i** 註：請確定在 **OpenManage Integration > 監視 > 記錄** 標籤中，使用者動作記錄確認有可供主動式 HA 叢集使用的主機。
3. 為相關聯的機箱建立機箱設定檔。請參閱[建立機箱設定檔](#)。
4. 確認已成功完成機箱清查。請參閱[檢視機箱清查](#)。
5. 啟動 CMC，並確認機箱的陷阱目的地是設定為 OMIVV 裝置的 IP 位址。
6. 在**機箱管理控制器**中，前往**設定 > 一般**。
7. 在**一般機箱設定**頁面上，選取**啟用增強機箱記錄與事件**。
8. 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連線設定檔的一部分並已順利清查，而在適用的情況下，機箱都應該具備機箱設定檔。
1. 在 OpenManage Integration 中，按一下**叢集**。
 2. 在**叢集**底下，按一下其中一個叢集，然後選取**設定 > vSphere 可用性**，再按一下**編輯**。隨後便會顯示**編輯叢集設定精靈**。
 3. 按一下**vSphere DRS**，然後選取**開啟 vSphere DRS** (如果沒有選取)。
 4. 按一下**vSphere 可用性**，然後選取**開啟主動式 HA** (如果沒有選取)。
 5. 在左窗格的**vSphere 可用性**底下，按一下**主動式 HA 故障與回應**。隨後便會顯示**主動式 HA 故障與回應**畫面。
 6. 在**主動式 HA 故障與回應**畫面上，展開**自動層級**。
 7. 如果是**自動層級**，請選取**手動或自動**。
 8. 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。
 9. 如果是**主動式 HA 提供者**，請使用核取方塊選取叢集的 Dell 提供者。
 10. 針對所選的 Dell 提供者，按一下**編輯**。隨後便會顯示**主動式 HA 提供者的編輯封鎖的故障情況**對話方塊。
 11. 若要封鎖故障情況，不讓它張貼事件，請使用核取方塊，從**故障情況**表中選取事件 (透過陷阱或輪詢加以產生)。您可以使用**篩選欄位**，篩選故障情況資料格的內容，或在故障情況資料格內拖放欄。故障情況可以在叢集層級或主機層級中套用。
 12. 若要套用在叢集中所有目前和未來的**主機**，請選取**叢集層級**核取方塊。
 13. 若要套用變更，請在**編輯封鎖的故障情況**按一下**確定**，若要取消，則按一下**取消**。
 14. 若要儲存變更，請在**編輯叢集設定精靈**中按一下**確定**，若要取消，則按一下**取消**。

在叢集上啟用主動式 HA 後，OMIVV 會掃描叢集內的所有主機，並初始化所有受支援之主機伺服器元件的主動式 HA 健全狀況狀態。OMIVV 現在可以傳送支援元件的健全狀況更新通知至 vCenter 伺服器。根據來自 OMIVV 的健全狀況更新通知，vCenter 伺服器會採取您針對**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 78。

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 的**管理標籤**中，按一下**主動式 HA 組態 > 主動式 HA 事件**。
2. 按一下以檢視支援事件清單的相關資訊。
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。
3. 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。
4. 請針對必須自訂的所有事件重複步驟 3。
5. 執行以下任何一個動作：
 - a. 若要儲存自訂，按一下**套用變更**。
 - b. 若要在選擇重要性層級後回復覆寫的重要性，按一下**取消**。
 - c. 若要將預設嚴重程度套用至覆寫的嚴重程度，請按一下**重設為預設值**。

啟動管理主控台

您可以從 Dell EMC 伺服器管理 Portlet 啟動三個管理主控台。這些主控台包括：

- 若要存取 iDRAC 使用者介面，請啟動遠端存取主控台。請參閱**啟動遠端存取主控台 (iDRAC)**。
 - 若要存取 OpenManage 伺服器管理員使用者介面，請啟動 OMSA 主控台。啟動 OMSA 主控台之前，應在 Open Management Integration for VMware vCenter 中設定 OMSA URL。請參閱**啟動 OMSA 主控台**。
 - 若要存取機箱使用者介面，請按一下「刀鋒機箱主控台」。請參閱**啟動機箱管理控制器主控台 (CMC)**。
- 註：**如果您使用的是刀鋒系統，請啟動 CMC 主控台，以啟動機箱管理控制器使用者介面。如果您使用的不是刀鋒系統，就不會顯示機箱管理控制器使用者介面。

啟動遠端存取主控台

您可以從 Dell EMC 伺服器管理 Portlet 啟動 iDRAC 使用者介面。

1. 在 OpenManage Integration for VMware vCenter 中，按一下「**導覽**」區域中清查清單下的**主機**。
2. 在**物件標籤**上，按兩下您想要的主機。
3. 在**摘要標籤**中，向下捲動至 Dell EMC 伺服器管理 Portlet。
4. 按一下**管理主控台 > 遠端存取主控台 (iDRAC)**。

啟動 OMSA 主控台

請務必先設定 OMSA URL，並安裝與設定 OMSA Web 伺服器之後，再啟動 OMSA 主控台。您可以從**設定標籤**設定 OMSA URL。

註：使用 OpenManage Integration for VMware vCenter 安裝 OMSA，才能監控與管理 PowerEdge 第 11 代伺服器。

1. 在 OpenManage Integration for VMware vCenter 中，按一下「**導覽**」區域中清查清單下的**主機**。
2. 在**物件標籤**中，連按兩下您想要的主機。
3. 在**摘要標籤**中，向下捲動至 **Dell EMC 主機資訊**。
4. 在 **Dell EMC 主機資訊**區段中，按一下 **OMSA 主控台**。

啟動機箱管理控制器主控台

您可以從 Dell EMC 伺服器管理 Portlet 啟動機箱使用者介面。

1. 在 OpenManage Integration for VMware vCenter 中，按一下「**導覽**」區域中清查清單下的**主機**。
2. 在**物件標籤**中，連按兩下您想要的刀鋒伺服器。
3. 在**摘要標籤**中，向下捲動至 Dell EMC 伺服器管理 Portlet。

4. 按一下**管理主控台** > **機箱管理控制器主控台 (CMC)**。

關於韌體更新

OMIVV 裝置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。但您不可在同一叢集的兩部主機上，執行並行韌體更新。

下表列出您能以各種部署模式同時執行的韌體更新工作的數量 (不過您也可以安排任何數量的韌體更新工作)：

表 28. 以各種部署模式執行的韌體更新工作

小型部署模式	中型部署模式	大型部署模式
5	10	15

以下為您可以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 共用) 來執行 iDRAC、BIOS 或 LC 的韌體更新。單一 DUP 方法只能用於主機層級。

儲存庫 — 可執行 BIOS 和所有支援的韌體更新。這種方法在主機層級和叢集層級兩者都適用。以下是儲存庫的兩個位置：

- Dell Online — 此位置會使用 Dell 的韌體更新儲存庫 (Ftp.dell.com)。OpenManage Integration for VMware vCenter 從 Dell 儲存庫下載選取的韌體更新並更新管理的主機。
- 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。

i 註：如果網路需要代理，請根據網路設定啟用代理設定。

i 註：如果您使用 CIFS 共用，儲存庫的密碼不能超過 31 個字元。請勿在密碼中使用 @、&、%、!、"、'、(逗號)、<、> 等字元。

i 註：請務必使用最新的 DRM 版本 (3.x) 及更新版本。

有關設定韌體更新儲存庫的詳細資訊，請參閱 [設定韌體更新儲存庫](#) 第頁的 35。

韌體更新精靈一律會檢查 iDRAC、BIOS 和 Lifecycle Controller 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 和 Lifecycle Controller 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、Lifecycle Controller 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、Lifecycle Controller、RAID、NIC/LOM、電源供應器、BIOS 等。

主題：

- [執行非 vSAN 主機的韌體更新](#)
- [為 vSAN 主機執行韌體更新精靈](#)
- [執行非 vSAN 叢集的韌體更新精靈](#)
- [執行 vSAN 叢集的韌體更新精靈](#)

執行非 vSAN 主機的韌體更新

i 註：在韌體更新程序期間，確保您不會刪除以下項目：

- 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連線設定檔。

若要執行非 vSAN 主機的韌體更新，請執行下列步驟：

1. 若要存取韌體更新精靈，請在 OpenManage Integration 中按一下 **主機**，並執行下列其中一個動作：
 - 以滑鼠右鍵按一下主機，選取所有 **OpenManage Integration 動作 > 韌體更新**。
 - 在「主機」頁面中，按一下主機，然後選取所有 **OpenManage Integration 動作 > 韌體更新**。
 - 在導覽窗格中選取主機，然後按一下 **摘要 > Dell EMC 主機資訊 > 執行韌體精靈**。
 - 在導覽窗格中選取主機，然後按一下 **監視 > Dell EMC 主機資訊 > 韌體 > 執行韌體精靈**。

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。

i 註: 如果您從舊版的 OMIVV 升級為可用的版本，而且已經排程韌體更新工作，就可以在備份 OMIVV 資料庫並將其還原至可用版本後，於相同主機上啟動韌體更新精靈。

2. 閱讀「歡迎」頁面上的指示，然後按「下一步」。
隨即顯示「選擇更新來源」頁面。

3. 在**選取更新來源**頁面上，選取下列其中一項：

- a. 畫面上會顯示**目前儲存庫位置**，並從**選取更新套件組合**下拉式清單中，選取韌體更新套件組合。

i 註: 搭載 iDRAC 版本 1.51 和較舊版本的第 12 代主機不支援 64 位元配套。

i 註: 搭載任何 iDRAC 版本的第 11 代主機不支援 64 位元配套。

i 註: OMIVV 支援 32 位元和 64 位元的更新韌體套件組合。除了上述的套件組合之外，如果目錄中具有相同版本 ID 的機型有 32 位元和 64 位元的套件組合可用，OMIVV 也會建立混合式套件組合。

- b. 若要從檔案載入單一韌體更新，請選取**單一 DUP**。如果您選取「單一 DUP」，請前往步驟 6。
單一 DUP 可能位於可由虛擬裝置存取的 CIFS 或 NFS 共用上。請使用下列格式之一輸入**檔案位置**：

- NFS 共用 — <host>:/<share_path/>FileName.exe
- CIFS 共用 — \\<host accessible share path>\<FileName>.exe

若為 CIFS 共用，OMIVV 會提示您可以存取共用磁碟機的網域格式輸入使用者名稱和密碼。

i 註: 共用網路資料夾的使用者名稱或密碼不支援使用 @、% 和，字元。

i 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。

4. 按一下**下一步**。

「選取元件」頁面隨即顯示。


5. 使用這些核取方塊，從清單選取至少一個韌體元件，然後按「下一步」。

屬於降級或目前排定要更新的元件則無法選取。您可以選取**允許降級**選項，選取列出要降級的元件。

隨後會顯示「排程韌體更新」頁面。

i 註: 當您從舊版的 OMIVV 升級成可用的版本時，所有元件的必須重新開機欄位會顯示「否」，除非您重新整理韌體更新儲存庫。

若要從資料格的各種元件內容篩選以逗號分隔的值，請使用**篩選**。

您也可以在元件資料格內拖曳欄。如果您要從精靈匯出，請按一下 。

i 註: 如果您選取必須重新開機的元件，請確定 vCenter 環境的設定方式可以移轉工作負載。

6. 在「排程韌體更新」頁面上，執行以下操作：

- a. 在**韌體更新作業名稱**欄位指定工作名稱，在**韌體更新說明**欄位指定說明，這個是選填欄位。

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，便可再次重複使用該工作名稱。

- b. 輸入**維護模式逾時值** (以分鐘為單位)。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。

i 註: 最小維護模式逾時值為 60 分鐘。

i 註: 最大維護模式逾時值為一天。

- c. 選取下列任何一個選項：

- 選取**立即更新**，馬上開始韌體更新工作。

*韌體更新完成後結束維護模式*選項預設會選取。

*將已關閉電源及暫停的虛擬機器移到叢集中的其他主機*選項預設會選取。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。

- 若要稍後再執行韌體更新工作，請選取**排程更新**。您可以將韌體更新工作安排在目前時間的 30 分鐘後。

- 在行事曆方塊中，選取月份和日期。

- 在「時間」文字方塊內，以「小時:分鐘」格式輸入時間。此時間為 OMIVV 裝置時間。

- 為避免服務中斷，請選取在下次重新開機時套用更新。
- 若要在主機不是維護模式時套用更新並重新開機，請選取套用更新，然後強迫重新開機而不進入維護模式。不建議使用這個方法。

7. 按一下下一步。

摘要頁面隨即顯示，提供韌體更新之所有元件的相關詳細資料。

8. 按一下完成。

韌體更新工作需要數分鐘才能完成，確切時間會根據韌體更新工作所包含的元件數目而異。您可以在「工作佇列」頁面中檢視韌體更新工作的狀態。若要存取工作佇列頁面，請在 OpenManage Integration 中，選取監視 > 工作佇列 > 韌體更新。韌體更新工作完成後，系統會根據排程韌體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。

為 vSAN 主機執行韌體更新精靈

排定更新之前，請先確定已符合下列先決條件：

- DRS 已啟用。
- 主機未處於維護模式。
- vSAN 資料物件狀況良好。

若要略過上述檢查，請清除「排程韌體更新」頁面中的「檢查先決條件」核取方塊。

- 依照 VMware vSAN 準則，確定選取相容的驅動程式和韌體版本。進行韌體更新之前，會安裝已選取的驅動程式。
- 叢集符合所選資料移轉選項的 vSAN 要求。
- 啟用 vSAN 後，重新執行清查。

i 註：在進行韌體更新程序時，Dell EMC 建議您不要刪除以下項目：

- 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連線設定檔。

若要執行單一主機韌體更新，請執行下列步驟：

1. 若要存取韌體更新精靈，請在 OpenManage Integration 中按一下主機，並執行下列其中一個動作：

- 以滑鼠右鍵按一下主機，選取所有 OpenManage Integration 動作 > 韌體更新。
- 在「主機」頁面中，按一下主機，然後選取所有 OpenManage Integration 動作 > 韌體更新。
- 在導覽窗格中選取主機，然後按一下摘要 > Dell EMC 主機資訊 > 執行韌體精靈。
- 在導覽窗格中選取主機，然後按一下監視 > Dell EMC 主機資訊 > 韌體 > 執行韌體精靈。

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。

i 註：如果您從舊版的 OMIVV 升級為可用的版本，而且已經排程韌體更新工作，就可以在備份 OMIVV 資料庫並將其還原至可用版本後，於相同主機上啟動韌體更新精靈。

2. 閱讀「歡迎」頁面上的指示，然後按「下一步」。

隨即顯示「選擇更新來源」頁面。

3. 在「選取更新來源」頁面中，執行下列操作：

a. 從下拉式清單中，選取驅動程式儲存庫設定檔或韌體儲存庫設定檔，或是兩者的組合。

如果基準儲存庫在叢集設定檔中是相關聯的，則相關聯的韌體和驅動程式儲存庫都會自動選取。

b. 從「選取更新套件組合」下拉式功能表中，選擇適當的套件組合。

如果選取的是驅動程式儲存庫，則會顯示選取驅動程式頁面。該頁面會顯示驅動程式元件的詳細資料，例如主機名稱、服務標籤、元件名稱、廠商、套件名稱、目前、可用、更新適用、必須重新開機。

c. 在選取驅動程式頁面上，選取您需要更新的驅動程式元件，然後按下一步。

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。


如果選取的是韌體儲存庫，則會顯示「選取元件」頁面。該頁面會顯示元件的詳細資料，例如主機名稱、服務標籤、機型名稱、元件、目前、可用、嚴重性、需要重新開機。

d. 使用這些核取方塊，從清單選取至少一個韌體元件，然後按「下一步」。

屬於降級或目前排定要更新的元件則無法選取。您可以選取允許降級選項，選取列出要降級的元件。

隨後便會顯示「排程韌體更新」頁面。

若要從資料格的各種元件內容篩選以逗號分隔的值，請使用篩選。

您也可以將元件資料格內拖曳欄。如果您要從精靈匯出，請按一下 。

i 註: 如果您選取需要重新開機的元件, 請確定 vCenter 環境的設定方式可以移轉工作負載。

4. 在「排程韌體更新」頁面上, 執行以下操作:

a. 在**韌體更新作業名稱**欄位指定工作名稱, 在**韌體更新說明**欄位指定說明, 這個是選填欄位。

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。

i 註: 檢查先決條件核取方塊預設會選取。在以下情況中, 韌體更新工作會停止:

- DRS 未啟用。
- 叢集中的某些主機已啟用維護模式。
- vSAN 物件的健全狀況不良。

b. 輸入維護模式逾時值 (以分鐘為單位)。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。

i 註: 最小維護模式逾時值為 60 分鐘。

i 註: 最大維護模式逾時值為一天。

c. 選取下列任何一個選項:

• 選取**立即更新**, 馬上開始韌體更新工作。

韌體更新完成後結束維護模式選項預設會選取。

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。

- 若要稍後再執行韌體更新工作, 請選取**排程更新**。您可以將韌體更新工作安排在目前時間的 30 分鐘後。
 - 在行事曆方塊中, 選取月份和日期。
 - 在「時間」文字方塊內, 以「小時:分鐘」格式輸入時間。此時間為 OMIVV 裝置時間。
- 為避免服務中斷, 請選取**在下次重新開機時套用更新**。
- 若要在主機不是維護模式時套用更新並重新開機, 請選取**套用更新, 然後強迫重新開機而不進入維護模式**。不建議使用這個方法。

5. 按一下**下一步**。

摘要頁面隨即顯示, 提供韌體更新之所有元件的相關詳細資料。

6. 按一下**完成**。

韌體更新工作需要數分鐘才能完成, 確切時間會根據韌體更新工作所包含的元件數目而異。您可以在「工作佇列」頁面中檢視韌體更新工作的狀態。若要存取工作佇列頁面, 請在 OpenManage Integration 中, 選取**監視 > 工作佇列 > 韌體更新**。韌體更新工作完成後, 系統會根據**排程韌體更新**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。

執行非 vSAN 叢集的韌體更新精靈

OMIVV 可讓您在叢集的所有主機上, 執行 BIOS 和韌體更新。精靈只會更新以下主機: 已包含在連線設定檔中, 且在韌體、CSIOR 狀態、Hypervisor 及 OMSA 狀態方面皆相容 (僅限第 11 代伺服器)。如果在叢集上啟用了分散資源排程 (DRS), 則 OMIVV 會在主機進入或離開維護模式時移轉工作負載, 藉此執行叢集感知韌體更新。

在執行韌體更新精靈之前, 請確認符合下列條件:

- 已設定韌體更新儲存庫。如需設定韌體更新儲存庫的相關資訊, 請參閱**設定韌體更新儲存庫**。
- 在您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。
- 叢集中的主機已經新增至連線設定檔, 且順利執行清查。
- DRS 已啟用。

i 註: VMware 建議您用一模一樣的伺服器硬體來建立叢集。

i 註: 在進行韌體更新程序時, Dell EMC 建議您不要刪除以下項目:

- 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叢集主機的連線設定檔。


1. 若要啟動韌體更新精靈, 請在 OpenManage Integration 中按一下**叢集**, 並執行下列任一子步驟:

- 按一下**叢集**, 選擇**動作 > 所有 OpenManage Integration 動作 > 韌體更新**。
- 在**物件**索引標籤中, 選取**動作 > 所有 OpenManage Integration 動作 > 韌體更新**。

- 按一下叢集，選取**監視 > Dell EMC 叢集資訊 > 韌體**。在**韌體**畫面上，按一下**執行韌體精靈**連結。
- 以滑鼠右鍵按一下叢集，選取**動作 > 所有 OpenManage Integration 動作 > 韌體更新**。

OMIVV 會檢查主機的可兼容性，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」頁面隨即顯示。

2. 閱讀歡迎頁面上的指示，然後按**下一步**。
隨後便會顯示「選擇伺服器」頁面。
3. 在「選擇伺服器」頁面的「名稱」樹狀圖中，使用核取方塊來選擇主機。
4. 按一下**下一步**。
「選取更新來源」頁面隨即顯示，您可以在其中選取套件組合。另外還會顯示儲存庫位置。
5. 在「選取更新來源」頁面上，選定主機的各個機型在機型名稱旁都有一個下拉式清單，您可以在其中選取所需的套件組合。請為韌體更新選取所需的套件組合。
 - i 註:** OMIVV 支援 32 位元和 64 位元的更新韌體套件組合。除了這些套件組合之外，如果目錄中具有相同版本 ID 的機型有 32 位元和 64 位元的套件組合可用，OMIVV 也會建立混合式套件組合。
 - i 註:** 搭載 iDRAC 版本 1.51 和較舊版本的第 12 代主機不支援 64 位元配套。
 - i 註:** 搭載任何 iDRAC 版本的第 11 代主機不支援 64 位元配套。
6. 按一下**下一步**。
「選取元件」頁面隨即顯示。該頁面會顯示元件的詳細資料，例如**主機名稱、服務標籤、機型名稱、元件、目前、可用、嚴重性、必須重新開機**。
7. 在**選取元件**頁面上，使用核取方塊從清單中選擇至少一個元件，然後按**下一步**繼續進行。
屬於降級或目前排定要更新的元件則無法選取。您可以選取**允許降級**選項，選取列出要降級的元件。
若要從資料格的各種元件內容篩選以逗號分隔的值，請使用**篩選**。

您也可以將元件資料格內拖曳欄。如果您要從精靈匯出，請按一下。

8. 在「韌體更新資訊」頁面中，檢視所有的韌體更新詳細資料。
9. 按一下**下一步**。
隨後便會顯示「排程韌體更新」頁面。
 - a. 在**韌體更新作業名稱**欄位中，輸入韌體更新工作的名稱。
韌體更新工作名稱為必填，而且不會使用已在使用中的名稱。如果您清除韌體更新工作名稱，便可再次重複使用它。
 - b. 在「韌體更新說明」欄位中輸入韌體更新說明。這個欄位為選填。
 - c. 輸入維護模式逾時值 (以分鐘為單位)。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。
 - i 註:** 最小維護模式逾時值為 60 分鐘。
 - i 註:** 最大維護模式逾時值為一天。
 - d. 在**排程韌體更新**底下，選擇以下一個選項：
 - 若要立即執行更新工作，請按一下**立即更新**。
 - 若要稍後再執行更新工作，請按一下**排程更新**，然後執行以下子工作：
 - i. 在**行事曆**方塊中，選取月份和日期。
 - ii. 在**時間**文字方塊內，以小時:分鐘格式輸入時間。
10. 按一下**下一步**。
隨即顯示**摘要**頁面。
11. 在**摘要**頁面上，按一下**完成**，隨後便會顯示已順利建立韌體更新工作訊息。

韌體更新工作需要數分鐘的時間完成，時間長短視乎選取的主機數量以及每個主機中的元件數量而定。您可以在**工作佇列**頁面中檢視韌體更新工作的狀態。若要存取工作佇列頁面，請在 OpenManage Integration 中，選取**監視 > 工作佇列 > 韌體更新**。韌體更新工作完成後，選定主機會自動執行清查，而主機會自動離開維護模式。

執行 vSAN 叢集的韌體更新精靈

在執行韌體更新精靈之前，請確認符合下列條件：

- DRS 已啟用。

- 主機未處於維護模式。
- vSAN 資料物件狀況良好。如果第一個主機的 vSAN 物件健全狀況不良，韌體更新工作就會失敗。對於其他主機，它會等待 60 分鐘，讓 vSAN 物件的健全狀況再次好轉。
- 依照 VMware vSAN 準則，確定選取相容的驅動程式和韌體。進行韌體更新之前，會安裝已選取的驅動程式。
- 叢集符合所選資料移轉選項的 vSAN 要求。強烈建議您選取基準（叢集設定檔）韌體或驅動程式儲存庫。
- 您必須先建立驅動程式儲存庫設定檔和韌體儲存庫設定檔，才能開始更新韌體。有關建立驅動程式儲存庫與韌體儲存庫的資訊，請參閱 [建立儲存庫設定檔](#) 第頁的 40。
- 在您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。
- 叢集中的主機已經新增至連線設定檔，且順利執行清查。
- 啟用 vSAN 後，重新執行清查。

i 註: VMware 建議您用一模一樣的伺服器硬體來建立叢集。

i 註: 在進行韌體更新程序時，Dell EMC 建議您不要刪除以下項目：

- 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叢集主機的連線設定檔。
- 位於 CIFS 或 NFS 的儲存庫。

1. 若要啟動韌體更新精靈，請在 **OpenManage Integration** 中按一下 **叢集**，並執行以下任一子步驟：

- 按一下 **叢集**，選擇 **動作 > 所有 OpenManage Integration 動作 > 韌體更新**。
- 在 **物件** 索引標籤中，選取 **動作 > 所有 OpenManage Integration 動作 > 韌體更新**。
- 按一下 **叢集**，選取 **監視 > Dell EMC 叢集資訊 > 韌體**。在 **韌體** 畫面上，按一下 **執行韌體精靈** 連結。
- 以滑鼠右鍵按一下 **叢集**，選取 **動作 > 所有 OpenManage Integration 動作 > 韌體更新**。

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**」頁面隨即顯示。

2. 閱讀歡迎頁面上的指示，然後按下一步。

隨後便會顯示「**選擇伺服器**」頁面。

3. 在「**選擇伺服器**」頁面的「**名稱**」樹狀圖中，使用核取方塊來選擇主機。

4. 按一下下一步。

隨即顯示「**選擇更新來源**」頁面。

5. 在「**選擇更新來源**」頁面中，執行下列操作：

a. 從下拉式清單中，選取驅動程式儲存庫設定檔或韌體儲存庫設定檔，或是兩者的組合。

如果基準儲存庫在叢集設定檔中是相關聯的，則相關聯的韌體和驅動程式儲存庫都會自動選取。

根據預設，**選取套件組合**區域中會選取主機的機型名稱。

b. 如果選取的是韌體儲存庫，則選定主機的各個機型在機型名稱旁都有一個下拉式清單，您可以在其中選取韌體更新所需的套件組合。從下拉式清單中選取所需的套件組合，然後按下一步。

如果選取的是驅動程式儲存庫，則會顯示**選取驅動程式**頁面。該頁面會顯示驅動程式元件的詳細資料，例如**主機名稱、服務標籤、元件名稱、廠商、套件名稱、目前、可用、更新適用、必須重新開機**。

i 註: OMIVV 支援 32 位元和 64 位元的更新韌體套件組合。除了這些套件組合之外，如果目錄中相同版本 ID 有多個套件組合時，OMIVV 也會建立混合式套件組合。

i 註: 搭載 iDRAC 版本 1.51 和較舊版本的第 12 代主機不支援 64 位元配套。


6. 在**選取驅動程式**頁面上，選取您更新所需的驅動程式元件，然後按下一步。

如果選取的是韌體儲存庫，則會顯示「**選取元件**」頁面。該頁面會顯示元件的詳細資料，例如**主機名稱、服務標籤、機型名稱、元件、目前、可用、嚴重性、必須重新開機**。

7. 在**選取元件**頁面上，選取您更新韌體所需的元件，然後按下一步。

屬於降級或目前排定要更新的元件則無法選取。您可以選取**允許降級**選項，選取列出要降級的元件。

若要從資料格的各種元件內容篩選以逗號分隔的值，請使用**篩選**。

您也可以將元件資料格內拖曳欄。如果您要從精靈匯出，請按一下 。

8. 在**韌體更新資訊**頁面上，檢視所有的韌體更新詳細資料，然後按下一步。

隨後便會顯示「**排程韌體更新**」頁面。

9. 在「**排程韌體更新**」頁面上，執行以下操作：

a. 在**韌體更新作業名稱**欄位中，輸入韌體更新工作的名稱。

i 註: 韌體更新工作名稱為必填，而且不會使用已在使用中的名稱。如果您清除韌體更新工作名稱，便可再次重複使用它。

- b. 在「韌體更新說明」欄位中輸入韌體更新說明。這個欄位為選填。
- c. 輸入維護模式逾時值 (以分鐘為單位)。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。

i 註: 最小維護模式逾時值為 60 分鐘。

i 註: 最大維護模式逾時值為一天。

- d. 若要立即執行更新工作，請按一下**立即更新**。
- e. 從**虛擬 vSAN 資料移轉**下拉式清單中，選取適當的選項。根據預設，會選取**確保存取功能**。

i 註: 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。

- f. 若要稍後再執行更新工作，請按一下**排程更新**，然後執行以下工作：

- i. 在**行事曆**方塊中，選取月份和日期。
- ii. 在**時間**文字方塊內，以小時:分鐘格式輸入時間。
- iii. 從**虛擬 vSAN 資料移轉**下拉式清單中，選取適當的選項。根據預設，會選取**確保存取功能**。

i 註: 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。

- 10. 按一下**下一步**。
隨即顯示**摘要**頁面。

- 11. 在**摘要**頁面上，按一下**完成**，隨後便會顯示已順利建立韌體更新工作訊息。

韌體更新工作需要數分鐘的時間完成，時間長短視選取的主機數量以及每個主機中的元件數量而定。您可以在**工作佇列**頁面中檢視韌體更新工作的狀態。若要存取工作佇列頁面，請在 OpenManage Integration 中，選取**監視 > 工作佇列 > 韌體更新**。韌體更新工作完成後，會在所選的主機上自動執行清查，且主機會自動結束維護模式。

機箱管理

OMIVV 可讓您檢視與模組化伺服器相關聯之機箱的其他資訊。您可以在「機箱資訊」索引標籤中檢視以下資訊：個別機箱的機箱概觀詳細資料，硬體清查、韌體與管理控制器的相關資訊，個別機箱元件的健全狀況，以及機箱保固資訊。系統會針對每個機箱顯示下列三個索引標籤，並針對某些機箱視型號而異：

- 「摘要」索引標籤
- 「監視」索引標籤
- 「管理」索引標籤

註：若要檢視所有資訊，該機箱必須與某個機箱設定檔相關聯，且必須已順利完成機箱清查。如需詳細資訊，請參閱[關於機箱設定檔](#)。

主題：

- [檢視機箱摘要詳細資料](#)
- [檢視機箱的硬體清查資訊](#)
- [檢視機箱的其他硬體組態](#)
- [檢視機箱的關聯主機](#)

檢視機箱摘要詳細資料

您可以在[機箱摘要](#)頁面上，檢視個別機箱的機箱摘要詳細資料。

1. 在[首頁](#)上，按一下 **vCenter**。
2. 在左窗格的 **OpenManage Integration** 下方，按一下 **Dell EMC 機箱**。
3. 在左窗格中，選取相對應的機箱 IP。
4. 按一下 **摘要**索引標籤。

隨後便會顯示所選機箱的下列相關資訊：

- 名稱
- Model
- 韌體版本
- 服務標籤
- CMC

註：按一下 CMC 連結，就會顯示[機箱管理控制器](#)頁面。

註：如果您沒有執行機箱的清查工作，就只能看見服務標籤和 CMC IP 位址。

5. 檢視與所選機箱相關聯之裝置的狀況。
主窗格會顯示機箱的整體狀況。有效的狀況指示燈為**健康**、**警告**、**嚴重**、**不存在**。**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 以前的版本，只會顯示兩個健全狀況指示燈：例如**健康**和**警告**或**嚴重**(裡面有橘色驚嘆號的倒三角形)。

註：整體狀況是根據狀況參數最差的機箱顯示狀況。例如，如果有 5 個健康符號和 1 個警告符號，整體健全狀況會顯示為**警告**。

6. 用機箱的授權類型和到期日來檢視 **CMC Enterprise** 或 **Express**。

上述詳細資料不適用於 M1000e 機箱。

7. 按一下**保固**圖示，並檢視剩餘天數和用於主機的天數。
如果您有多個保固，則最後一個保固的最後一天是用來計算保固的剩餘日數。
8. 檢視**作用中錯誤**表格所列的機箱錯誤(顯示在**機箱狀況**頁面上)。

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。

檢視機箱的硬體清查資訊

您可以檢視所選機箱內硬體清查的相關資訊。若要檢視此頁面上的資訊，請務必執行清查工作，並匯出含有元件資訊的 CSV 檔案。

1. 在**首頁**上，按一下 **vCenter**。
2. 在左窗格的 **OpenManage Integration** 下方，按一下 **Dell EMC 機箱**。
3. 在左窗格中，選取相對應的機箱 IP。
4. 按一下 **監視索引** 標籤。

若要檢視相關元件資訊，請瀏覽 OMIVV：

表 29. 硬體清查資訊

硬體清查：元件	瀏覽 OMIVV	資訊
風扇	請使用以下任一方法： <ul style="list-style-type: none"> ● 在概觀索引標籤中，按一下 風扇。 ● 在監視標籤展開左窗格，按一下 硬體清查，然後按一下 風扇。 	風扇的相關資訊： <ul style="list-style-type: none"> ● 名稱 ● 存在 ● 電源狀態 ● 讀取中 ● 警告閾值 ● 嚴重閾值 <ul style="list-style-type: none"> ○ 最小值 ○ 最大值
電源供應器	請使用以下任一方法： <ul style="list-style-type: none"> ● 在概觀索引標籤中，按一下 電源供應器。 ● 在監視索引標籤展開左窗格，按一下 硬體清查，然後按一下 電源供應器。 	電源供應器的相關資訊： <ul style="list-style-type: none"> ● 名稱 ● 容量 ● 存在 ● 電源狀態
溫度感測器	請使用以下任一方法： <ul style="list-style-type: none"> ● 在概觀索引標籤中，按一下 溫度感測器。 ● 在監視索引標籤展開左窗格，按一下 硬體清查，然後按一下 溫度感測器。 	溫度感應器的相關資訊： <ul style="list-style-type: none"> ● 位置 ● 讀取中 ● 警告閾值 <ul style="list-style-type: none"> ○ 最大值 ○ 最小值 ● 嚴重閾值 <ul style="list-style-type: none"> ○ 最大值 ○ 最小值 <p>註： 如果是 PowerEdge M1000e 機箱，則只會顯示關於機箱的溫度感應器資訊。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。</p>
I/O 模組	請使用以下任一方法： <ul style="list-style-type: none"> ● 在概觀標籤中，按一下 I/O 模組。 ● 在監視標籤中，展開左窗格，按一下 硬體清查，然後按一下 I/O 模組。 	I/O 模組的相關資訊： <ul style="list-style-type: none"> ● 插槽/位置 ● 存在 ● 名稱 ● 光纖 ● 服務標籤 ● 電源狀態 <p>若要檢視其他資訊，請選取對應的 I/O 模組，下列資訊隨即顯示：</p> <ul style="list-style-type: none"> ● 角色 ● 韌體版本 ● 硬體版本 ● IP 位址

表 29. 硬體清查資訊 (續)

硬體清查：元件	瀏覽 OMIVV	資訊
		<ul style="list-style-type: none"> 子網路遮罩 閘道 MAC 位址 DHCP 已啟用
PCIe	<p>請使用以下任一方法：</p> <ul style="list-style-type: none"> 在概觀索引標籤中，按一下 PCIe。 在監視索引標籤展開左窗格，按一下 硬體清查，然後按一下 PCIe。 	<p>PCIe 的相關資訊：</p> <ul style="list-style-type: none"> PCIe 插槽 <ul style="list-style-type: none"> 插槽 名稱 電源狀態 光纖 伺服器插槽 <ul style="list-style-type: none"> 名稱 號碼 <p>若要檢視其他資訊，請選取對應的 PCIe，下列資訊隨即顯示：</p> <ul style="list-style-type: none"> 插槽類型 伺服器對應 指派狀態 已配置的插槽電源 PCI ID 廠商 ID <p>註： PCIe 資訊不適用於 M1000e 機箱。</p>
iKVM	<p>請使用以下任一方法：</p> <ul style="list-style-type: none"> 在概觀索引標籤中，按一下 iKVM。 在監視標籤中，展開左窗格，按一下 硬體清查，然後按一下 iKVM。 	<p>iKVM 的相關資訊：</p> <ul style="list-style-type: none"> iKVM 名稱 存在 韌體版本 前面板 USB/視訊已啟用 允許存取 CMC CLI <p>註： 您只能檢視 PowerEdge M1000e 機箱的 iKVM 相關資訊</p> <p>註： 機箱必須包含 iKVM 模組，iKVM 標籤才會顯示。</p>

檢視機箱的其他硬體組態

您可以檢視所選機箱有關保固、儲存、韌體、管理控制器的詳細資訊。若要檢視此頁面上的資訊，請務必執行清查工作，並匯出含有元件資訊的 .CSV 檔案。

若要檢視機箱的保固、儲存、韌體、管理控制器詳細資訊，請執行下列步驟：

1. 在首頁上，按一下 **vCenter**。
2. 在左窗格的 **OpenManage Integration** 下方，按一下 **Dell EMC 機箱**。
3. 在左窗格中，選取相對應的機箱 IP。
4. 按一下 **監視索引標籤**。

若要查看保固、儲存、韌體和管理控制器的相關資訊，請瀏覽 OMIVV。

表 30. 韌體詳細資料

硬體設定	瀏覽 OMIVV	資訊
韌體	a. 在監視標籤中，按一下雙箭頭標記並展開左窗格，然後按一下 韌體 。	韌體的相關資訊：

表 30. 韌體詳細資料

硬體設定	瀏覽 OMIVV	資訊
	b. 在 監視 標籤中，如果您按一下 啟動 CMC ，就會顯示 機箱管理控制器 頁面。	<ul style="list-style-type: none"> • 元件 • 目前版本

表 31. 管理控制器詳細資訊

硬體設定	瀏覽 OMIVV	資訊
管理控制器	<p>a. 在監視標籤中，按一下雙箭頭標記並展開左窗格，然後按一下管理控制器。</p> <p>b. 在管理控制器頁面中，若要檢視其他資訊，請按一下箭頭標記並展開左欄。</p>	<p>管理控制器的相關資訊：</p> <ul style="list-style-type: none"> • 一般 <ul style="list-style-type: none"> ○ 名稱 ○ 韌體版本 ○ 上次更新時間 ○ CMC 位置 ○ 硬體版本 • 通用網路 <ul style="list-style-type: none"> ○ DNS 網域名稱 ○ DNS 使用 DHCP ○ MAC 位址 ○ 備援模式 • CMC IPV4 資訊 <ul style="list-style-type: none"> ○ IPv4 啟用 ○ DHCP 啟用 ○ IP 位址 ○ 子網路遮罩 ○ 閘道 ○ 慣用 DNS 伺服器 ○ 備用 DNS 伺服器

表 32. 儲存資訊

硬體設定	瀏覽 OMIVV	資訊
存放時	在 監視 標籤中，按一下 儲存 。	<p>儲存的相關資訊：</p> <ul style="list-style-type: none"> • 虛擬磁碟 • 控制器 • 機箱 • 實體磁碟 • 熱備援磁碟 <p>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。</p> <p>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)：</p> <ul style="list-style-type: none"> • 名稱 • 機型 • 服務標籤 • IP 位址 (儲存裝置連結) • 光纖 • 組群名稱 • 群組 IP 位址 (儲存裝置群組連結)

表 33. 保固資訊

硬體設定	瀏覽 OMIVV	資訊
保固	在 監視 標籤中，按一下 保固 。	保固的相關資訊： <ul style="list-style-type: none"> ● 供應商 ● 說明 ● 狀態 ● 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 執行保固擷取工作 。

檢視機箱的關聯主機

您可以在**管理**標籤上，檢視關於所選機箱關聯主機的相關資訊。

1. 在**首頁**上，按一下 **vCenter**。
2. 在左窗格的 **OpenManage Integration** 下方，按一下 **Dell EMC 機箱**。
3. 在左窗格中，選取相對應的機箱 IP。
4. 按一下**管理索引**標籤。

關聯主機的下列相關資訊隨即顯示：

- 主機名稱 (如果按一下所選的主機 IP，主機相關詳細資料隨即顯示。)
- 服務標籤
- 機型
- iDRAC IP
- 插槽位置
- 上一次清查

部署 Hypervisor

OMIVV 可讓您在支援的裸機伺服器中設定下列元件，以及部署 Hypervisor 並將它新增到 vCenter 中的指定資料中心和叢集：

- 開機順序設定
- RAID 組態
- BIOS 設定
- iDRAC 組態

您可以使用 VMware vCenter (而不使用 PXE)，在裸機 PowerEdge 伺服器上建立硬體設定檔、系統設定檔和 Hypervisor 設定檔。

註： 部署 Hypervisor 時，針對第 14 代以後的伺服器建議您使用系統設定檔。

若要佈建硬體並且執行部署，請先確認實體伺服器有顯示在部署精靈上。同時確認所有實體伺服器都符合以下需求：

- 符合 *OpenManage Integration for VMware vCenter 相容性比較表* 中的特定硬體支援資訊。
- 符合最低支援版本的 iDRAC 韌體、Lifecycle Controller 和 BIOS。有關特定的韌體支援資訊，請參閱 *OpenManage Integration for VMware vCenter 相容性比較表*。
- 部署之後，請在 PCI 插槽中手動設定 NIC。如果您使用的是附加 NIC，則系統必須啟用主機板網路功能 (LOM) 或網路子卡 (NDC) 功能，並連線至網路。OMIVV 支援僅使用內嵌或整合式 LOM 的部署。
- 符合 iSDM 的儲存規格。若要瞭解 iSDM 的儲存規格，請參閱 VMware 說明文件。請務必先從 BIOS 啟用 iSDM，再以 OMIVV 部署 Hypervisor。OMIVV 可讓您在 iSDM 或本機硬碟機上進行部署。
- 如果 vCenter 和 iDRAC 連線到不同的網路，請確定這兩個網路之間必須具備路由。
- 請務必啟用「重新啟動時收集系統清查」(CSIOR)。另外，在啟動自動/手動探索之前，請確認所擷取的資料是最新的，做法是完全關閉系統電源，然後再開啟系統，即強制重新開機。
- 按一下來訂購由原廠預先設定自動探索和信號交換選項的 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，請在起始 Hypervisor 部署前，先確認是否符合下列條件：
 - 在 BIOS 啟用虛擬化技術 (VT) 旗標。
 - 針對作業系統安裝，將系統的開機順序設定為可開機的虛擬磁碟或 iSDM。
- 如果 OMIVV 有用於硬體組態，則即使 BIOS 組態並非硬體設定檔的一部份，也請確認系統仍會自動啟用 VT 的 BIOS 設定。如果目標系統上沒有顯示虛擬磁碟，就需要使用 Express/Clone RAID 組態。
- 在進行部署時，確認有準備好包含所有 Dell 驅動程式的自訂 ESXi 映像。您可以在 support.dell.com 找到正確的映像，做法是瀏覽到 **Dell 驅動程式與下載** 頁面，將自訂映像儲存到 OMIVV 可在部署過程中存取的 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*。若要使用正確的映像，請參閱 [下載自訂的 Dell ISO 映像](#)。
- 請確認在參照硬體設定檔中選取 BIOS 模式後，再套用 Hypervisor 設定檔，因為 OMIVV 只支援 BIOS 模式在目標伺服器上自動部署 Hypervisor。如果沒有選取任何硬體設定檔，請務必手動將開機模式設定為 BIOS 並重新啟動伺服器，然後再套用 Hypervisor 設定檔。

如果伺服器是來自 PowerEdge 第 12 代伺服器之前的版本，則部署程序會執行下列工作：

- 將 OMSA 套件安裝到目標系統上。
- 在 OMSA 自動將 SNMP 設陷目的地設定為指向 OMIVV。

主題：

- [裝置探索](#)
- [佈建](#)
- [系統設定檔](#)
- [管理系統設定檔](#)
- [設定硬體設定檔](#)
- [建立 Hypervisor 設定檔](#)
- [建立部署範本](#)
- [關於部署精靈](#)
- [部署工作時間](#)
- [下載自訂的 Dell EMC ISO 映像](#)


裝置探索

探索是新增支援的 PowerEdge 裸機伺服器的程序。探索到伺服器之後，就可以將它用於 Hypervisor 和硬體部署。有關部署所需的 PowerEdge 伺服器清單，請參閱 *OpenManage Integration for VMware vCenter 相容性比較表*。Dell EMC 裸機伺服器的 iDRAC 和 OMIVV 虛擬機器之間必須有網路連線。

- ① **註:** 已有 Hypervisor 的主機不應探索加入 OMIVV，反而應該將它們新增至 vCenter。請將它們新增至連線設定檔，再使用主機相容性精靈，讓它們與 OpenManage Integration for VMware vCenter 趨於一致。
- ① **註:** 如果探索到的是 OMIVV 4.0 以前的裸機伺服器，請確定您已將機器從裸機伺服器清單中移除並重新探索。
- ① **註:** 若要針對第 12 代裸機 PowerEdge 伺服器在 SD 卡上執行作業系統部署，請確認已安裝 iDRAC 2.30.30.30 和更新版本。

手動探索

您可以手動新增一個不是由探索程序新增的裸機伺服器。新增之後，伺服器就會顯示在部署精靈的伺服器清單中。

1. 在 OpenManage Integration for VMware vCenter 的**管理 > 部署**標籤上，按一下  圖示。隨後便會顯示**新增伺服器**對話方塊。
2. 在**新增伺服器**對話方塊中，執行下列步驟：
 - a. 在 **iDRAC IP 位址** 文字方塊中，輸入 iDRAC IP 位址。
 - b. 在 **使用者名稱** 文字方塊中，輸入使用者名稱。
 - c. 在 **密碼** 文字方塊中輸入密碼
3. 按一下**新增伺服器**。
新增伺服器的工作可能需要數分鐘才能完成。

OpenManage Integration for VMware vCenter 中的自動探索

自動探索是新增 PowerEdge 裸機伺服器的程序。探索到伺服器之後，請將它用於 Hypervisor 和硬體部署。自動探索是 iDRAC 功能，不需要從 OMIVV 手動探索裸機伺服器。

自動探索事前準備作業

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。

- ① **註:** 已有 Hypervisor 的主機不應探索加入 OMIVV，反而應該將 Hypervisor 新增至連線設定檔，然後使用主機相容性精靈，讓 Hypervisor 與 OMIVV 趨於一致。

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 與佈建伺服器通訊。您可以用 DHCP 伺服器取得 IP 位址，也可以在 iDRAC 組態公用程式中，手動指定 IP 位址。
- 其他網路設定 — 如果使用的是 DHCP，請務必啟用「從 DHCP 取得 DNS 伺服器位址」設定，這樣才能進行 DNS 名稱解析。
- 佈建服務位置 — iDRAC 必須知道佈建服務伺服器的 IP 位址或主機名稱。請參閱 [佈建服務位置](#)。
- 停用帳戶存取 — 請務必啟用管理帳戶對 iDRAC 的存取權限，凡是具備管理員權限的 iDRAC 帳戶，請先從 iDRAC Web 主控台予以停用。自動探索順利完成後，管理 iDRAC 帳戶便會重新啟用。
- 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。

佈建服務位置

請使用下列選項，在自動探索時，依 iDRAC 取得佈建服務位置：

- 在 iDRAC 中手動指定 — 在 iDRAC 組態公用程式的「LAN 使用者組態」、「佈建伺服器」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。

如果佈建服務值不是在 iDRAC 主控台中手動指定，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：http://en.community.dell.com/techcenter/extras/m/white_papers/20178466。

在 iDRAC 上啟用或停用管理帳戶

在設定自動探索前，請停用 root 以外的所有管理帳戶。在自動探索程序進行期間，root 帳戶應停用。成功設定自動探索後，請回到 iDRAC GUI，並重新啟用 root 以外的所有已關閉管理帳戶。

註： 為防止自動探索失敗，您可以在 iDRAC 上啟用非管理帳戶。自動探索失敗時，非管理帳戶可讓您遠端存取。

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 iDRAC6：在左窗格中選取 **iDRAC 設定 > 網路/安全性 > 使用者標籤**。
 - 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**。
4. 在**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 第 11 代伺服器

請確定具備 iDRAC 和主機 IP 位址。

如果您尚未命令裸機裝置使用原廠提供的自動探索功能，可以手動設定。

順利自動探索到裸機伺服器之後，就會建立新的系統管理員帳戶，或是以交握服務傳回的認證來啟用現有帳戶。但是在自動探索前停用的所有其他系統管理員帳戶，則不會啟用。請務必在自動探索成功後，重新啟用這些系統管理員帳戶。請參閱在 [iDRAC 上啟用或停用系統管理帳戶](#)。

註： 如果自動探索因故未能順利完成，就無法以遠端方式連線 iDRAC。遠端連線會要求您在 iDRAC 上啟用非系統管理員帳戶。如果 iDRAC 上沒有啟用非系統管理員帳戶，您就只能在本機登入方塊，並在 iDRAC 啟用帳戶，才能存取 iDRAC。

1. 在瀏覽器輸入 **iDRAC IP 位址**。
2. 登入 **iDRAC Enterprise 圖形化使用者介面 (GUI)**。
3. 在 **Integrated Dell Remote Access Controller 6 — Enterprise > 系統摘要** 標籤的虛擬主控台預覽中，按一下**啟動**。
4. 在**警告 — 安全性**對話方塊中，按一下**是**。
5. 在 iDRAC 公用程式主控台中，按下 **F12** 一次或兩次。隨後便會顯示**需要驗證**對話方塊。
6. 在**需要驗證**對話方塊中，檢視所顯示的名稱，然後按 **Enter** 鍵。
7. 輸入密碼。
8. 按 **Enter** 鍵。
9. 當**關機/重新啟動**對話方塊出現時，請按下 **F11**。
10. 主機會重新啟動，同時畫面會顯示載入記憶體的相关資訊，再來是 RAID，接著當它顯示 iDRAC 並提示您按下 CTRL + E 時，請立即按下 **CTRL + E**。
如果您看到以下對話方塊，就表示動作成功，否則，請前往「電源」功能表，關閉電源後再次開啟電源，然後再重複這個步驟。

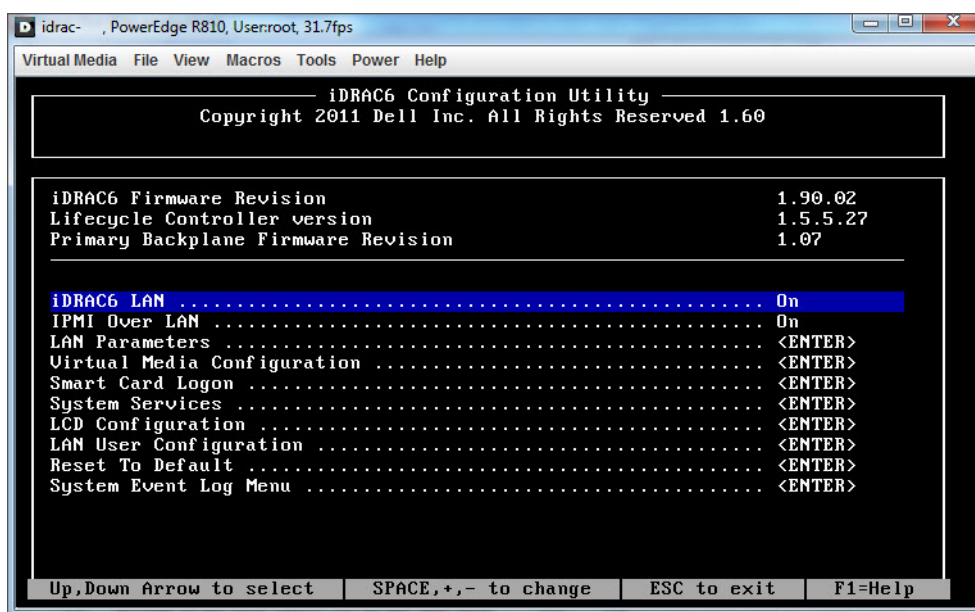


圖 1. iDRAC 組態公用程式

11. 在 iDRAC6 組態公用程式，用方向鍵選取 **LAN** 參數。
12. 按下 **Enter**。
13. 如果這是刀鋒主機，若要設定 NIC，請使用空白鍵將選項切換為啟用。
14. 如果您使用的是 DHCP，請使用方向鍵選取 **DHCP** 的網域名稱。
15. 使用空白鍵將選項切換為開啟。
16. 如果您使用的是 DHCP，請使用方向鍵瀏覽至 IPV4 設定，然後選取 **DHCP** 的 DNS 伺服器。
17. 使用空白鍵將選項切換為開啟。
18. 若要結束，請在鍵盤按下 **ESC**。
19. 請使用方向鍵選取 **LAN 使用者組態**。
20. 使用方向鍵選取佈建伺服器。
21. 按 **Enter** 鍵。
22. 輸入主機的 IP 位址。
23. 按下 **ESC**。
24. 使用方向鍵選取帳戶存取。
25. 使用空白鍵將選項切換為停用。
26. 使用方向鍵選取自動探索。
27. 使用空白鍵將選項切換為啟用。
28. 從鍵盤按下 **Esc**。
29. 再按一下 **ESC**。

為自動探索手動設定 PowerEdge 第 12 代以後的伺服器

請確定具備 iDRAC 位址。

向 Dell EMC 訂購伺服器時，您可以在提供佈建伺服器 IP 位址後，要求在伺服器啟用自動探索功能。佈建伺服器 IP 位址是 OMIVV 的 IP 位址。因此，若您從 Dell EMC 收到伺服器，並在安裝和連接 iDRAC 纜線後開啟伺服器電源，系統便會自動探索伺服器，並將伺服器列在部署精靈的第一頁。

註：對於自動探索到的伺服器，系統會把在**管理 > 設定 > 部署憑證**底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。順利完成作業系統部署之後，就會設定關聯連線設定檔中提供的 iDRAC 認證。

若要在目標機器上手動啟用自動探索，請對第 12 代以後世代的伺服器執行下列步驟：

1. 若要前往系統設定，請將目標系統開機/重新開機，然後在初始開機時按 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**佈建伺服器**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。

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 OpenManage Integration for VMware vCenter 中，按一下**管理 > 部署**標籤。
2. 在**裸機伺服器**頁面上選取伺服器，然後按一下 **✖**。

佈建

所有自動/手動探索到的相容裸機系統，都可以由 OMIVV 用於硬體佈建和 Hypervisor 部署。若要準備佈建和部署，請執行下列步驟：

表 34. 準備部署

步驟	說明
建立系統設定檔	包含從設定新伺服器所用的第 14 代參照伺服器收集來的系統組態設定。
建立硬體設定檔	包含從部署新伺服器所用的參照伺服器收集來的硬體設定。請參閱 建立或自訂硬體設定檔 第頁的 100。 註: 針對第 13 代與較舊的伺服器，建議您使用硬體設定檔。
建立 Hypervisor 設定檔	包含部署 ESXi 所需的 Hypervisor 安裝資訊。請參閱 建立 Hypervisor 設定檔 第頁的 102。
建立部署範本	部署範本包含系統設定檔、硬體設定檔、Hypervisor 設定檔，系統設定檔與 Hypervisor 設定檔的組合，或硬體設定檔與 Hypervisor 設定檔的組合。您可以根據需要，針對所有可用的資料中心伺服器來儲存及重複使用這些設定檔。

部署範本建立之後，請使用部署精靈來收集建立排程工作所需的資訊，該排程工作是在 vCenter 佈建伺服器硬體及部署新主機。如需執行部署精靈的相關資訊，請參閱[執行部署精靈](#) 第頁的 105。最後，請透過工作佇列來檢視工作狀態，並變更擱置中的部署工作。

系統設定檔

在 iDRAC 中，對於支援設定 CNA、FCoE (包括對於開機順序的組態支援)、RAID、BIOS 和 iDRAC 的 PowerEdge 伺服器，系統設定檔功能可供使用。OMIVV 以「系統設定檔」支援第 14 代 iDRAC 系統設定檔。OMIVV 透過支援伺服器組態設定檔，可讓您匯出第 14 代 Dell EMC 伺服器的整個組態，並匯入到目標伺服器。

將 FX2 機箱中已安裝之模組化伺服器的系統設定檔套用到另一個 FX2 機箱中安裝的類似伺服器時，兩個伺服器的插槽編號必須相同。

例如，從 FX2 機箱插槽 1 的 FC640 伺服器取得的系統設定檔，只能套用到另一個 FX2 機箱插槽 1 的另一個 FC640 伺服器。


- 註:** 系統設定檔不支援以下組態：
 - 開機選項的啟用和停用
 - BOSS 相關組態
- 註:** 使用系統設定檔時，若使用 Enterprise 授權匯出系統設定檔，而在具有 Express 授權的伺服器上匯入相同的系統設定檔會失敗，反之則會成功。
- 註:** 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。
- 註:** 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，而無法套用到相同 FX 機箱中的其他模組化伺服器。在這個情況下，建議從機箱每個插槽取得參考系統設定檔，並僅將這些系統設定檔套用到機箱的對應插槽。

使用系統設定檔的典型工作包括：

- 建立或從參考伺服器擷取系統設定檔資訊。請參閱[建立系統設定檔](#) 第頁的 98。
- 使用部署範本，將設定檔套用到選定的伺服器上。請參閱[建立部署範本](#) 第頁的 103。

i 註：針對第 14 代以後的伺服器，建議您使用系統設定檔。

若要啟動系統設定檔頁面，請執行下列步驟：

1. 在 OpenManage Integration for VMware vCenter 的**管理 > 部署**標籤上，選取**部署範本 > 系統設定檔**。
 - a. 在**系統設定檔**頁面上，檢視您已建立的系統設定檔清單。
畫面會出現一個表格，列出系統設定檔與設定檔名稱、說明、伺服器機型及參考伺服器資訊。
 - b. 若要深入檢視系統設定檔主機的詳細資料，請選取系統設定檔。
檢閱系統設定檔資訊，其中顯示詳細資料，例如設定檔名稱、iDRAC IP、iDRAC 類型、服務標籤、主機名稱、伺服器機型、建立日期、修改日期和修改者。
 - c. 若要在資料格中交換欄，請在資料格內拖放欄。
 - d. 若要篩選或搜尋資料格的內容，請按一下**篩選**欄位。
 - e. 若要匯出系統設定檔資訊至 .CSV 檔案，請選取系統設定檔，然後在資料格的右上角內，按一下 圖示。

建立系統設定檔

在建立系統設定檔之前，請確認符合下列條件：

- 參照伺服器是在 OMIVV 外部依據需求來設定。目前版本不支援修改任何屬性的任何值 (iDRAC 使用者密碼除外)。
- 參照伺服器上已啟用「重新啟動時收集系統詳細目錄 (CSIOR)」，且參照伺服器已重新啟動，以確保從 iDRAC 傳回的資料為最新資料。
- OpenManage Integration 已為每一個 vCenter 管理的主機成功執行清查。
- 裸機伺服器已安裝最低要求 BIOS 及韌體版本。如需 iDRAC、BIOS 和 Lifecycle Controller 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](#)。

您可以只使用第 14 代參照伺服器以建立系統設定檔。

1. 在 OpenManage Integration for VMware vCenter 的**管理 > 部署**標籤上，選取**部署範本 > 系統設定檔**。
2. 按一下 **+**。
3. 閱讀歡迎頁面上的指示，然後按**下一步**。
 - 在**設定檔名稱**文字方塊中，輸入設定檔名稱。
 - 在**設定檔說明**文字方塊中，輸入說明。說明值是選填欄位。
4. 按一下**下一步**。
隨後便會顯示**參照伺服器**對話方塊。選取第 14 代參照伺服器的方式有兩種，一種是直接從對話方塊選取，另一種是透過設定檔來源頁面中的**瀏覽**按鈕選取。
5. 執行以下任一子步驟來選取第 14 代參照伺服器：

i 註：從第 11 至第 14 代的所有主機都會顯示在對話方塊中，而且選取連結僅為第 14 代相容裸機伺服器和主機而啟用，其中僅顯示第 14 代裸機伺服器，而且選取連結僅為相容的裸機伺服器而啟用。

- a. 在**參照伺服器**對話方塊中，按一下正確的第 14 代參照伺服器，然後對著該參照伺服器按一下**選取連結**。
i 註：選取連結僅為相容主機而啟用。
- b. 在**參照伺服器**頁面中，按一下**瀏覽**，選取一個由 OMIVV 管理及順利清查的相容第 14 代主機參照伺服器，或者選取一個相容第 14 代裸機伺服器。

隨後便會顯示指明擷取設定的**擷取確認**對話方塊。若要從參照伺服器擷取硬體組態，請在**擷取確認**對話方塊中，按一下**是**，過幾分鐘後就會完成擷取。

隨後所選的伺服器名稱、參照伺服器類型、iDRAC IP 位址、型號及服務標籤就會顯示在**設定檔來源**頁面上。

i 註：如果**參照伺服器類型**是裸機伺服器，只顯示 iDRAC IP 位址；然而，如果**參照伺服器類型**為主機，就會顯示 iDRAC IP 和主機 IP/FQDN。

6. 按一下**下一步**。
7. 在**設定檔設定**頁面上，展開 iDRAC 以檢視系統設定檔屬性。您可以使用遞增或遞減順序來排序資料格欄。按一下資料篩選圖示即可篩選資料。
 - a. 若要快速檢視值欄中的「設定密碼」連結，請按一下 **▼**、在**值包含**中輸入「密碼」，然後針對已啟用的使用者輸入密碼。

註: Dell EMC 建議您提供在新增裸機伺服器期間所用的相同認證。如果您在部署範本中變更密碼，根使用者不會看到這項變更。部署作業系統期間，如果 Hypervisor 設定檔與部署範本具有關聯，則部署會使用連線設定檔 (iDRAC 及 ESXi) 密碼。

註: 設定密碼選項僅適用於已啟用 iDRAC 且具備有效使用者名稱的使用者。

此外，您可以根據 Dell 參照伺服器的組態檢視元件的設定檔設定，例如 iDRAC、BIOS、RAID、NIC、CNA、FCoE 和 EvenFilters。

b. 展開每個元件以顯示設定選項，例如執行個體、屬性名稱、值、破壞性、相依性和群組。

當您將游標停留在屬性上方時，便會顯示更多該屬性的相關資訊。

下列幾種屬性，例如唯讀、系統專有和破壞性屬性均預設為無法選取。

如果相依性文字無法使用，則相依性文字為空白。

註: 執行 RPM 升級或備份與還原時，下列事項適用於所有移轉的設定檔：

- 當您將滑鼠停留在屬性上方時，便會顯示屬性名稱。
- 只會選取非系統專有屬性。
- 相依性文字不會顯示。
- 已啟用的屬性會顯示已選取屬性的總數。

8. 按一下下一步。

顯示摘要頁面，其中提供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、平台專有屬性總數，以及破壞性屬性總數會顯示於屬性統計資料下。

9. 在摘要頁面中，按一下完成。

設定檔便會自動儲存，並顯示在系統設定檔視窗中。

目前版本不支援所有系統專有屬性。如需更多關於系統專有屬性的資訊，請參閱系統專有屬性 第頁的 136。

系統設定檔的少數屬性會遭到覆寫，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 140。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 141。

管理系統設定檔

系統設定檔會使用參照伺服器定義伺服器的系統組態。在 OpenManage Integration for VMware vCenter 上，有幾個管理動作可在現有的系統設定檔上執行，包括：

- 檢視系統設定檔
- 刪除系統設定檔

註: 目前版本不支援從 OMIVV 修改系統設定檔。您必須在 OMIVV 外部設定您的機器，然後將其當作系統設定檔的參照伺服器使用。

設定硬體設定檔

若要設定伺服器硬體設定，請建立硬體設定檔。硬體設定檔這個組態範本可以套用到新探索到的基礎結構元件，需要的資訊如下：

表 35. 建立硬體設定檔的需求

需求	說明
開機順序	開機順序是指開機裝置順序和硬碟機順序，開機模式設為 BIOS 時才能夠編輯。
BIOS 設定	BIOS 設定包括記憶體、處理器、SATA、整合式裝置、序列通訊、內嵌伺服器管理、電源管理、系統安全性及其他設定。 註: 無論參考伺服器上的設定為何，OpenManage Integration for VMware vCenter 都可在所有部署的伺服器上，支援 BIOS [處理器] 群組底下的特定 BIOS 設定。在使用參照伺服器建立硬體設定檔之前，參照伺服器必須先啟用 CSIOR 設定之後再重新開機，才能提供準確的清查與組態資訊。
iDRAC 設定	iDRAC 設定包括網路、使用者清單和使用者組態。
RAID 組態	RAID 組態會在解壓縮硬體設定檔時，顯示參考伺服器上目前的 RAID 拓撲。

表 35. 建立硬體設定檔的需求 (續)

需求	說明
	<p>註: 硬體設定檔設定了兩個 RAID 組態選項：</p> <ol style="list-style-type: none"> 1. 套用 RAID1+ 建立專用熱備援 (如果適用) — 如果您要將預設的 RAID 組態設定套用到目標伺服器，請使用這個選項。 2. 從參照伺服器複製 RAID 組態 — 如果您要複製參照伺服器設定，請使用這個選項。請參閱 自訂參照伺服器以建立硬體設定檔。

建立硬體設定檔的工作包括：

- 在參照伺服器上啟用 CSIOR
- 自訂參照伺服器以建立硬體設定檔
- 複製硬體設定檔

在參照伺服器上啟用 CSIOR

在使用參照伺服器建立硬體設定檔前，先啟用「重新啟動時收集系統清查」(CSIOR) 設定，並重新啟動伺服器，才能提供準確的清查與組態資訊。

啟用 CSIOR 的方法有兩種：


表 36. 啟用 CSIOR 的方法

方法	說明
本機	採用使用 Dell Lifecycle Controller United Server Configurator (USC) 使用者介面的個別主機。
遠端	使用 WS-Man 指令碼。如需進一步瞭解如何以指令碼處理此功能，請參閱 <i>Dell TechCenter</i> 和 <i>DCIM Lifecycle Controller 管理設定檔</i> 。

若要在參考伺服器以本機方式啟用 CSIOR：

1. 開啟系統電源，並在進行 POST 過程中按下 **F2** 來啟動 USC。
2. 選取**硬體組態 > 零件更換組態**。
3. 啟用在**重新啟動時收集系統清查**設定，結束 USC。

建立或自訂硬體設定檔

1. 在 OpenManage Integration for VMware vCenter 的**管理 > 部署**標籤上，選取**部署範本 > 硬體設定檔**。
2. 按一下  圖示。
3. 在**硬體設定檔精靈**中的歡迎頁面上按**下一步**，然後執行下列動作：
 - 在**設定檔名稱**文字方塊中，輸入設定檔名稱。
 - 在**說明**文字方塊中，輸入說明。說明是選填欄位。
4. 按**下一步**。
隨後便會顯示**參照伺服器**對話方塊。選取參照伺服器的方式有兩種，一種是直接從對話方塊選取，一種是透過參照伺服器視窗中的瀏覽按鈕選取。
5. 執行以下任一子步驟來選取參照伺服器：
 - 在**參照伺服器**對話方塊中，選擇正確的參照伺服器，然後對著該參照伺服器按一下**選取連結**。
隨後便會顯示指明擷取設定的**擷取確認**對話方塊。若要從參照伺服器擷取硬體組態，請在**擷取確認**對話方塊中，按一下**是**，接著再過幾分鐘後就會完成擷取。
 - 在**參照伺服器**頁面中，按一下**瀏覽**，選取一個由 OMIVV 管理及順利清查的相容參照伺服器，或者選取一個相容裸機伺服器。
若要從參照伺服器擷取硬體組態，請在**擷取確認**對話方塊中，按一下**是**。

隨後所選的伺服器名稱、iDRAC IP 位址、型號以及服務標籤就會顯示在**參照伺服器**頁面上。
6. 在**參照伺服器**頁面上，若要自訂參照伺服器設定，請按一下**自訂參照伺服器設定**，然後選擇下列可以選擇性加入及自訂的設定：
 - **RAID 設定**

- BIOS 設定
- 開機順序
- iDRAC Settings
 - 網路設定
 - 使用者清單

7. 在 RAID 組態視窗中，選取下列其中一項，然後按下一步：

- 套用 RAID1+ 建立專用熱備援 (如果適用) — 如果您要將預設的 RAID 組態設定套用到目標伺服器，請使用這個選項。在支援 RAID1 之整合式控制器的前兩個磁碟機上，RAID 組態工作預設為 RAID1。此外，如果有符合 RAID 條件的候選磁碟機，也會針對 RAID1 陣列建立專用熱備援。
- 如下所示從參照伺服器複製 RAID 組態 — 如果您要複製參照伺服器設定，請使用這個選項。

8. 在 BIOS 設定頁面上，如果您希望設定檔中包含 BIOS 設定資訊，請展開類別以顯示設定選項，然後按一下編輯，更新下列其中一項：

- 系統資訊
- 記憶體設定
- 處理器設定
- SATA 設定
- Boot 設定
- 一次性 Boot
- 整合裝置
- 停用插槽
- 序列通訊
- 系統檔案設定
- 系統安全
- 各式設定

待某類別的所有更新完成之後，若要儲存變更，請按下一步，若要取消變更，則按一下取消。

i 註：如需詳細的 BIOS 資訊 (包括設定選項與說明)，請參閱所選伺服器的 *硬體擁有者手冊*。

9. 在開機順序頁面執行下列步驟，然後按下一步：

- a. 若要顯示開機順序選項，請展開開機順序，然後按一下編輯，進行以下更新：
 - i. 在開機模式清單中，選取 BIOS 或 UEFI。
 - ii. 若要變更顯示的開機裝置順序，請在檢視清單的開機裝置順序底下選取裝置，然後按一下上移或下移。
 - iii. 選取啟用開機順序重試，好讓伺服器自動重試開機順序。
 - iv. 若要套用變更，請按一下確定，若要取消變更，則按一下取消。
- b. 若要顯示硬碟機順序選項，請展開硬碟機順序，按一下編輯。更新下列項目：
 - i. 若要變更顯示的硬碟機順序，請選取裝置，然後按一下上移或下移。
 - ii. 若要套用變更，請按一下確定，若要取消變更，則按一下取消。

i 註：針對第 13 代以前的伺服器，UEFI 和 BIOS 模式皆會顯示；而對於第 13 代或更新世代的伺服器，會顯示 BIOS 或 UEFI 模式。

10. 在 iDRAC 設定頁面中，執行下列步驟：

- a. 展開類別以顯示設定選項，然後按一下編輯：

請更新下列其中一項：

 - 網路設定
 - 網路
 - 虛擬媒體
- b. 在 iDRAC 本機使用者清單底下，執行下列其中一項：
 - 新增使用者 — 手動輸入 iDRAC 使用者和必填資訊。完成後，若要套用變更，請按一下套用，若要取消，則按一下取消
 - 刪除使用者 — 刪除所選的使用者。若要選取使用者，請使用滑鼠，然後按一下刪除。若要確認刪除，請按一下是。
 - 編輯使用者 — 手動編輯 iDRAC 使用者的資訊。完成後，若要套用設定，請按一下套用，若要取消，則按一下取消。

待某類別的所有更新完成之後，若要儲存變更，請按下一步，若要取消變更，則按一下取消。

i 註：如需詳細的 iDRAC 資訊 (包括設定選項與說明)，請參閱所選伺服器的 *iDRAC 使用者指南*。

11. 按一下下一步。

12. 在摘要頁面中，按一下**完成**。

設定檔便會自動儲存，並顯示在**硬體設定檔**視窗中。

建立或複製硬體設定檔

1. 在 OpenManage Integration for VMware vCenter 的**管理 > 部署**標籤上，選取**部署範本 > 硬體設定檔**。
2. 按一下 **+**。
3. 在**硬體設定檔精靈**中的歡迎頁面上，按**下一步**，然後執行下列動作：
 - 在**設定檔名稱**文字方塊中，輸入設定檔名稱。
 - 在**說明**文字方塊中，輸入**說明**。說明是選填欄位。
4. 按一下**下一步**。
5. 若要選取相容、受 vCenter 管理，並經過 Dell EMC OpenManage 外掛程式順利清查的參照伺服器，請在**參照伺服器**頁面上，按一下**瀏覽**。
6. 若要從參照伺服器擷取所有硬體設定，請按一下**複製參照伺服器設定**選項。
7. 按一下**下一步**。
解壓縮設定可能需要幾分鐘的時間完成。
8. 按一下**下一步**。
隨後便會填入設定，且所選伺服器的名稱、iDRAC IP 位址和服務標籤，會顯示在參照伺服器視窗中。


設定檔會儲存，然後顯示在**硬體設定檔**視窗的**可用設定檔**底下。

管理硬體設定檔


硬體設定檔會使用參照伺服器來定義伺服器的硬體組態。在 OpenManage Integration for VMware vCenter 上，有好幾個管理動作可在現有的硬體設定檔上執行，包括：

- 檢視或編輯硬體設定檔
- 刪除硬體設定檔

檢視或編輯硬體設定檔

1. 在 OpenManage Integration for VMware vCenter 的**管理 > 部署**標籤上，選取**部署範本 > 硬體設定檔**。
隨後便會顯示硬體設定檔。
2. 若要編輯設定檔，請選取一個設定檔，然後按一下 。
3. 在**硬體設定檔精靈**中，若要以不同的值進行設定，請按一下**編輯**。
4. 若要套用變更，請按一下**儲存**，若要取消，則按一下**取消**。

刪除硬體設定檔

 **註**: 刪除的硬體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 OpenManage Integration for VMware vCenter 的**管理 > 部署**標籤上，選取**部署範本 > 硬體設定檔**。
2. 選取設定檔，然後按一下 **X**。
3. 若要移除設定檔，請在確認對話方塊中按一下**是**，若要取消則按一下**否**。

建立 Hypervisor 設定檔

若要在伺服器上部署及設定 ESXi，請建立 Hypervisor 設定檔。Hypervisor 設定檔所需的資訊如下：

- NFS 或 CIFS 共用上，Dell 自訂的 ISO 軟體媒體的位置
- 負責管理部署主機 vCenter 執行個體，以及可選用的主機設定檔
- 外掛程式在 vCenter 部署伺服器的目的地叢集或資料中心

1. 在 OpenManage Integration for VMware vCenter 的**管理 > 部署**標籤上，選取**部署範本 > Hypervisor 設定檔**。

2. 在 **Hypervisor 設定檔** 頁面上，按一下 **+**。
3. 在 **Hypervisor 設定檔** 對話方塊中，執行下列子工作：
 - 在 **設定檔名稱** 文字方塊中，輸入設定檔名稱。
 - 在 **說明** 文字方塊中輸入說明 (選填)。
4. 在 **選擇參照 ISO 路徑及版本** 底下的 **安裝來源 (ISO)** 文字方塊中，輸入通往 Hypervisor 共用位置的路徑。Hypervisor 映像複本即會修改為允許以指令檔執行安裝。參照 ISO 位置的格式為下列其中一種：
 - NFS 格式：`host:/share/hypervisor.iso`
 - CIFS 格式：`\\host\share\hypervisor.iso`

i 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。

如果使用的是 CIFS 共用，請輸入**使用者名稱**、**密碼**和**確認密碼**。請確定密碼相符。


5. 在 **選取版本** 清單中，選取 ESXi 版本。
所有使用此 Hypervisor 設定檔部署的伺服器都有此映像，而且如果伺服器是第 12 代之前的版本，也會安裝最新建議版本的 OMSA。
6. 若要確認路徑和驗證，請按一下 **測試設定** 底下的 **開始測試**。
7. 按一下 **套用**。

管理 Hypervisor 設定檔

有好幾個管理動作可在現有的 Hypervisor 設定檔上執行，包括：


- 檢視或編輯 Hypervisor 設定檔
- 刪除 Hypervisor 設定檔

檢視或編輯 Hypervisor 設定檔

1. 在 OpenManage Integration for VMware vCenter 的 **管理 > 部署標籤** 上，選取 **部署範本 > Hypervisor 設定檔**。隨後便會顯示 Hypervisor 設定檔。
2. 選取設定檔，然後按一下 。
3. 在 **Hypervisor 設定檔** 對話方塊中，提供更新的值。
4. 若要套用變更，請按一下 **儲存**，若要取消，則按一下 **取消**。

刪除 Hypervisor 設定檔

i 註: 刪除的 Hypervisor 設定檔若為執行部署工作的一部份，可能導致工作失敗。

1. 在 OpenManage Integration for VMware vCenter 的 **管理 > 部署標籤** 上，選取 **部署範本 > Hypervisor 設定檔**。
2. 選取設定檔，然後按一下 。
3. 在確認對話方塊中，若要移除設定檔，請按一下 **刪除**，若要取消，則按一下 **取消**。

建立部署範本

部署範本包含系統設定檔、硬體設定檔、Hypervisor 設定檔，系統設定檔與 Hypervisor 設定檔的組合，或硬體設定檔與 Hypervisor 設定檔的組合。**部署精靈**會使用此範本在 vCenter 內佈建伺服器硬體並部署主機。

1. 在 OpenManage Integration for VMware vCenter 的 **管理 > 部署標籤** 中，選取 **部署範本**。
2. 按一下 **+**。
3. 在 **部署範本** 對話方塊中，輸入範本的名稱。
4. 輸入部署範本的 **說明** (選填)。
5. 按一下 **系統設定檔** 或 **硬體設定檔**，然後從下拉式功能表中選取適當的設定檔。

i 註: 第 14 代伺服器建議使用系統設定檔，而第 13 代與較舊的伺服器則建議使用硬體設定檔。

6. 從下拉式功能表選擇 **Hypervisor 設定檔**。
7. 若要套用設定檔選項並儲存變更，請按一下**儲存**。若要取消，請按一下**取消**。

管理部署範本

在 OpenManage Integration 上，有好幾個管理動作可在現有的部署範本上執行，包括：

- 檢視或編輯部署範本
- 刪除部署範本

檢視或編輯部署範本

1. 在 OpenManage Integration for VMware vCenter 的**管理 > 部署**標籤中，選取**部署範本**。隨後便會顯示部署範本設定檔。
2. 在**部署範本**對話方塊中，鍵入新的範本名稱和說明。
確認範本名稱是專屬名稱。
3. 從下拉式功能表變更**硬體設定檔**或**系統設定檔**。
4. 從下拉式功能表變更 **Hypervisor 設定檔**，然後按一下**儲存**。

刪除部署範本

1. 在 OpenManage Integration for VMware vCenter 的**管理 > 部署**標籤中，選取**部署範本**。
2. 在**部署範本**頁面上，選取範本並按一下 **X**。
3. 若要確認範本刪除，請在訊息方塊上按一下**刪除**，若要取消，則按一下**取消**。

關於部署精靈

部署精靈會說明部署程序，如下所示：

- 選取相容的裸機伺服器。
 - ① **註:** 若您選取第 14 代伺服器進行部署，則部署範本清單會包含硬體設定檔，或系統設定檔，或 Hypervisor 設定檔，或硬體和 Hypervisor 設定檔的組合，或系統與 Hypervisor 設定檔的組合。
 - ① **註:** 若您選取非第 14 代伺服器，或第 14 代和非 14 代伺服器的組合，則部署範本清單會包含硬體設定檔或 Hypervisor 設定檔，或是硬體設定檔與 Hypervisor 設定檔的組合。
- 選取部署範本，其中包括硬體和 Hypervisor 設定檔。
- 選取安裝目標 (硬碟或 IDSDM)。

部署 Hypervisor 時，您可以部署到 Internal Dual SD Module。您應該先從 BIOS 啟用 Internal Dual SD Module 之後，再以 OMIVV 部署 Hypervisor。

- 選取與主機相關聯的連線設定檔。
- 為每一個主機指派網路詳細資料。
- 選取 vCenter、目的地資料中心或叢集，以及可自行選用的主機設定檔。
- 排程要執行的伺服器部署工作。

① **註:** 如果您只部署硬體設定檔，則伺服器識別、連線設定檔、部署精靈的網路詳細資料選項均會略過，您會直接前往**排程部署**頁面。

① **註:** 如果是試用/評估授權，只要授權未過期，您都可以使用部署精靈。

VLAN 支援

OMIVV 支援在可路由的 VLAN 上部署 Hypervisor，而且您可以在部署精靈上設定 VLAN 支援。在這個部份的部署精靈中，有一個選項可以指定使用 VLAN 以及指定 VLAN ID。當您提供 VLAN ID 時，它會在進行部署時套用到 Hypervisor 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，能夠與虛擬裝置和 vCenter Server 兩者通訊。如果 Hypervisor 部署到的 VLAN，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選了多個裸機伺服器，並希望將同一個 VLAN ID 套用到所有伺服器上，那麼在部署精靈的伺服器識別部份中，請使用**套用設定至所有已選的伺服器**。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: OMIVV 不支援多重主目錄組態。如果您將第二個網路介面新增至應用裝置，希望能與第二個網路通訊，就會導致 Hypervisor 部署、伺服器相容性和韌體更新方面的工作流程發生問題。

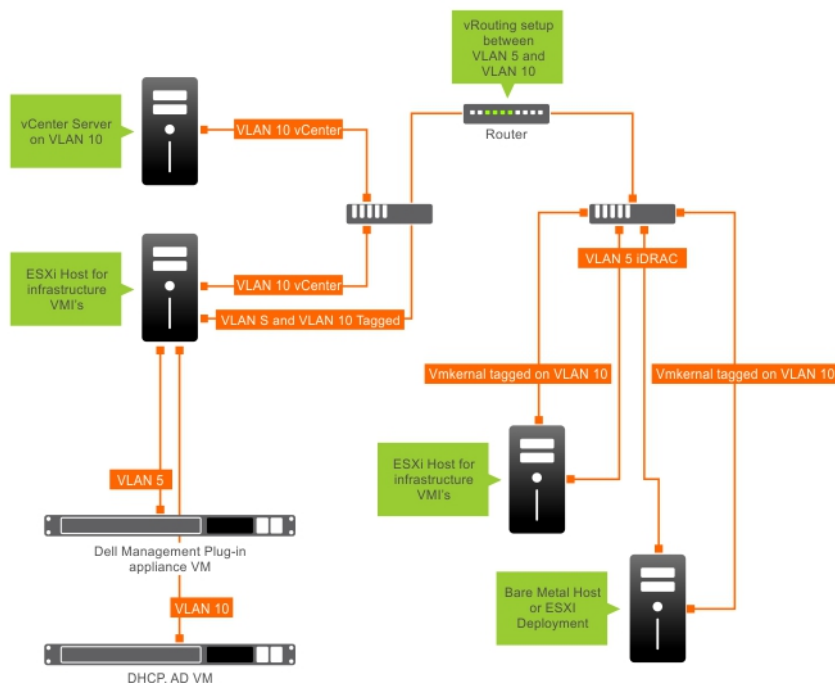


圖 2. VLAN 網路。

在這個範例網路中，OMIVV 裝置位於 VLAN 5，而 vCenter 和 ESXi 主機的 VMkernel 則是部署在 VLAN 10。由於 OMIVV 不支援多重 VLAN 定址，所以 VLAN 5 必須路由至 VLAN 10，所有系統之間才能正確通訊。如果這些 VLAN 之間沒有啟用路由，部署就會失敗。

執行部署精靈

在執行部署精靈之前，請務必先以適合 vCenter 的硬體設定檔、系統設定檔和 Hypervisor 設定檔以及連線設定檔來建立部署範本。

執行部署精靈：

1. 在 OpenManage Integration for VMware vCenter 中，選取**管理 > 部署**標籤。
2. 在**裸機伺服器**視窗中，按一下**執行部署精靈連結**。隨後便會顯示部署精靈的**歡迎**頁面。
3. 檢視**歡迎**頁面中的資訊，然後按**下一步**。
4. 在**選擇要部署的伺服器**頁面上，若要把指派相容裸機伺服器給部署工作，請按一下伺服器清單旁的核取方塊。
5. 按一下**下一步**。
6. 在**選擇範本/設定檔**頁面上，執行以下子步驟：
 - a. 在**部署範本**底下，若要把部署範本指派給所選的伺服器，請在**選擇部署範本**中，選取現有的部署範本。

註: 只有當您在**選擇要部署的伺服器**頁面上選取第 14 代伺服器時，才會顯示以系統設定檔為基礎的範本。

您可以從下拉式清單中，選取下列其中一個部署範本：

- 如果您選取只設定伺服器硬體的硬體設定檔專用或系統設定檔專用部署範本，請跳到步驟 10。
- 如果您選取部署 Hypervisor 的 Hypervisor 設定檔部署範本，請從步驟 6 (b) 繼續進行。

註: 如果您選取硬體設定檔或系統設定檔專用部署，系統會自動提示您加入**排程部署**頁面的資訊。

- b. 在**Hypervisor 安裝**底下，選取以下任一選項：

- **第一個開機磁碟**— 在硬碟機 (HDD)、固態磁碟機 (SSD)，或是由 RAID 控制器建立的虛擬磁碟上部署 Hypervisor。
 - **Internal Dual SD Module**— 可將 Hypervisor 部署在 IDSDM。
- i 註:** 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 **硬碟機** 選項。

若有任何所選的伺服器不支援 IDSDM，或是部署時 IDSDM 未出現，請執行下列其中一個動作：

i 註: 確保在作業系統部署過程中，**HardDiskFailOver** 是啟用狀態。

- 如果您要將 Hypervisor 部署在伺服器的第一個開機磁碟上，請選取將 **Hypervisor 部署至那些沒有內部雙 SD 模組可用的伺服器上的第一個開機磁碟** 核取方塊。

△ 警告: 如果選取此選項，並將 Hypervisor 部署在伺服器的第一個開機磁碟上，則開機磁碟中的資料將會全數清除。

- 如果不要部署在所選的伺服器上，而是繼續將 Hypervisor 部署在下一個伺服器，請清除將 **Hypervisor 部署至那些無可用內部雙 SD 模組之伺服器上的第一個開機磁碟**。

c. 在 **認證設定檔** 底下，執行以下任一動作：

- 選取 **所有伺服器皆使用此認證設定檔** 選項按鈕，若要將所有伺服器指派給同一個現有的設定檔，請從下拉式清單中選取連線設定檔。
- 按一下 **替每個伺服器選擇一個連線設定檔** 選項按鈕，然後從下拉式清單中，為每一部伺服器選取個別的連線設定檔。

7. 按一下 **下一步**。

隨後會顯示 **伺服器識別** 頁面。


提供伺服器識別的方法有兩種：

- 輸入網路資訊 (IP 位址、子網路遮罩和閘道) — 主機名稱必須是完整的網域名稱。FQDN 不得使用 *localhost*。FQDN 是在您將主機新增至 vCenter 時使用。
- 使用動態主機組態通訊協定 (DHCP) 來設定 IP 位址、子網路遮罩、閘道 IP、主機名稱及偏好的/替代的 DNS 伺服器 — 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。

i 註: 請使用完整網域名稱 (FQDN) (而非 localhost) 作為主機名稱。自 ESXi 5.1 開始，localhost 的值就會阻礙 OMIVV 外掛程式處理主機傳來的事件。請建立一個使用 FQDN 來解析 IP 位址的 DNS 記錄。若要正確識別 ESXi 5.1 傳來的 SNMP 警示，請將 DNS 伺服器設定為支援反向對應要求。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。

8. 在 **伺服器識別** 頁面上，執行下列步驟：

本頁可提供用於指定 VLAN ID 的選項。當您提供 VLAN ID 時，它會在進行部署時套用到 Hypervisor 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。請參閱 [VLAN 支援](#)。

- 若要展開並檢視個別伺服器資訊，請在所選伺服器底下，按一下 。
- 在 **主機名稱和 NIC** 中，輸入伺服器的完整主機名稱。
- 在 **用於管理工作的 NIC** 下拉式清單中，選取管理伺服器用的 NIC。
- 輸入 IP 位址、子網路遮罩、預設閘道和 DNS 詳細資料，或選擇 **使用 DHCP 取得** 核取方塊。
- 如果是部署到需要 VLAN ID 的網路，請先選取 **VLAN** 核取方塊，然後輸入 **VLAN ID**。
VLAN ID 請使用數字 1 到 4094。VLAN ID 0 保留用於標記訊框優先順序。
- 對所有要部署的伺服器重複步驟 a 到 h，或選取 **套用設定至所有已選的伺服器** 核取方塊。
如果您選取 **套用設定至所有已選的伺服器**，請輸入其他伺服器的 FQDN 名稱和 IP 位址。

i 註: 在指定伺服器的 FQDN 名稱時，請務必為每個伺服器提供專屬的主機名稱。

9. 按一下 **下一步**。

10. 在 **排程部署** 頁面上，執行下列動作：

- 輸入 **工作名稱** 和 **工作說明**。
- 如果是 **vCenter 設定**，請輸入以下命令：
 - 在 **vCenter 執行個體** 中，選取部署後管理主機的服務器執行個體。
 - 在 **vCenter 目的地容器** 中，按一下 **瀏覽**，搜尋 vCenter 目的地。
 - 在 **vCenter 主機設定檔** 中，選取封裝主機組態並協助管理主機組態的設定檔，不過這並非必要選項。
- 選取一個工作排程，決定執行部署工作的時機：
 - 選取 **排程部署工作**
 - 用日曆控制項選取日期。
 - 輸入時間。
 - 若要立即開始工作，請選取 **立即執行部署工作**。

若要在部署工作開始後前往工作佇列，請選取 **提交工作後移至工作佇列**。

11. 按一下**完成**。

部署精靈工作完成後，您可以使用**工作佇列**來管理部署工作。。

使用工作佇列來管理部署工作

1. 在 OpenManage Integration for VMware vCenter 的**監視 > 工作佇列**標籤上，按一下**部署工作**。

以下有關部署工作的詳細資料，會顯示在上方格線中：

- 名稱
- 說明
- 排定的時間
- 狀態
- 集合大小
- 進度摘要

2. 若要更新部署工作詳細資料，請按一下**重新整理**圖示。

3. 若要顯示部署工作詳細資料 (包含部署工作所含之伺服器的詳細資訊)，請在上方格線中選取一個部署工作。

以下詳細資料會顯示在下方格線中：


- 服務標籤
- iDRAC IP 位址
- 工作狀態
- 警告
- 部署工作詳細資料 (將滑鼠游標停留在上方可取得更多資訊)。
- 開始時間和結束時間
- 更多詳細資料


您可以選取工作，並將游標移到部署工作的**詳細資料**欄上方，即可在快顯文字中檢視部署工作的所有相關資訊。

如需更多關於系統設定檔工作失敗的詳細資料，請按一下**更多詳細資料**。**更多詳細資料**頁面會顯示下列資訊：

- 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。

若要將詳細資料匯出至 .CSV 檔案，請在右側角落的資料格，按一下 。

4. 若要中止部署工作，請按一下  圖示。

5. 當訊息出現時，請按一下**中止作業**加以中止，或者按一下**請勿中止作業**加以取消。

6. 要顯示**清除部署工作佇列**視窗，按一下 。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佇列中清除。

系統鎖定模式工作

1. 在 OpenManage Integration for VMware vCenter 頁面上，按一下**監視 > 工作佇列**標籤，然後按一下**系統鎖定模式工作**。

以下有關系統鎖定模式工作的資訊，會顯示在上方格線中：


- 名稱
- 說明
- 排定的時間
- vCenter
- 狀態
- 集合大小
- 進度摘要

2. 若要更新系統鎖定模式工作詳細資料，請按一下**重新整理**圖示。

- 若要顯示系統鎖定模式工作詳細資料 (包含系統鎖定模式工作所含之伺服器的詳細資訊)，請在上方格線中選取一個系統鎖定模式工作。

以下詳細資料會顯示在下方格線中：

- 服務標籤
- iDRAC IP
- 主機名稱
- 狀態
- 詳細資料

 **註:** 如果狀態欄顯示成功，詳細資料欄會是空的。

如果狀態欄顯示失敗，故障原因便會顯示在詳細資料欄中。

- 開始日期與時間
- 結束日期與時間

您可以選取工作，並將游標移到系統鎖定模式工作的詳細資料欄上方，即可在快顯文字中檢視系統鎖定模式工作的所有相關資訊。

- 若要清除系統鎖定模式工作，請按一下 。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工作佇列中清除。

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。

- 在 **OpenManage Integration for VMware vCenter** 頁面上，按一下 **監視 > 工作佇列** 標籤，然後按一下 **漂移偵測工作**。

下列有關漂移偵測工作的資訊，會顯示在上方格線中：


- 名稱
- 上次執行時間
- 下次執行時間
- 狀態
- 集合大小
- 進度摘要

- 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**。
- 若要顯示漂移偵測工作詳細資料 (包含漂移偵測工作所含之伺服器的詳細資訊)，請在上方格線中選取一個漂移偵測工作。

以下詳細資料會顯示在下方格線中：

- 維修標籤
- 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

- 若要隨需執行漂移偵測工作，請按一下 。

 **註:** 在基準叢集中將主機裝置新增至連線設定檔之後，便會在新增的主機裝置上，自動執行漂移偵測工作。



管理韌體更新工作

若要檢視本頁面中的資訊，請為叢集執行韌體更新工作。請參閱 [為叢集執行韌體更新精靈](#)。

頁面會顯示所有韌體更新工作。在此頁面中，您可以檢視、重新整理、清除或中止您的韌體更新工作。

- 從 OpenManage Integration 選取 **監視 > 工作佇列 > 韌體更新**。
- 若要顯示最新資訊，請按一下 **重新整理** 圖示。
- 檢視 DataGrid 中的狀態。

此資料格會提供韌體更新工作的下列相關資訊：

- 狀態
 - 排定的時間
 - 名稱
 - 說明
 - vCenter
 - 集合大小 (韌體清查工作上的伺服器數量)
 - 進度摘要 (韌體更新的進度詳細資料)
4. 如需特定工作的更多詳細資料，請在特定工作的資料格中選取工作。
您可以在這裡找到下列詳細資料：
- 主機名稱
 - 狀態
 - 開始時間
 - 結束時間
5. 如果想要中止已排程但未執行的韌體更新，請選取您要中止的工作，然後按一下 。
- i** 註: 如果您中止的韌體更新工作已經提交給 iDRAC，則主機上的韌體仍可能會更新，但是 OMIVV 會將工作呈報為已取消。
6. 如果要清除較早的韌體更新工作或排程的韌體更新，請按一下 。
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。
7. 在清除韌體更新作業對話方塊中，選取早於，然後按一下套用。
選定的工作隨後會從佇列中清除。

部署工作時間

佈建和部署裸機伺服器可能需要 30 分鐘到數小時才能完成，端視幾項因素而定。開始部署工作時，建議您根據提供的指南來規劃部署時間。完成佈建與部署所需的時間，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。下表列出部署工作可能花費的約略時間：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。

表 37. 大約部署時間

部署類型	每個部署的約略時間
僅限 Hypervisor	30 到 130 分鐘
Hypervisor 與硬體設定檔	1-4 小時
僅限系統設定檔	5-6 分鐘
系統設定檔和 Hypervisor 設定檔	30-40 分鐘

部署順序內的伺服器狀態

當清查工作執行時，自動/手動探索到的裸機系統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。管理員可以使用這些狀態來判斷伺服器是否應包含在部署工作中。狀態如下：

表 38. 部署順序內的伺服器狀態

伺服器狀態	說明
未設定	伺服器已連上 OMIVV，並且正在等待設定。
已設定	伺服器已用順利部署 Hypervisor 所需的所有硬體資訊完成設定了。

下載自訂的 Dell EMC ISO 映像

部署必須使用包含所有 Dell 驅動程式的自訂 ESXi 映像。

1. 導覽至 support.dell.com。
2. 按一下**從所有產品中選擇** > **伺服器、儲存裝置與網路**。
3. 在**選取產品**中，按一下 **PowerEdge**。
4. 按一下 PowerEdge 伺服器機型。
5. 按一下該伺服器機型的**驅動程式與下載**頁面。
6. 按一下**變更作業系統**連結，然後選取您要的 ESXi 系統。
7. 按一下**企業解決方案**。
8. 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**。

關於主機、裸機和 iDRAC 相容性

若要以 OMIVV 管理主機和裸機伺服器，每一項都必須符合特定的基本準則。如果不相容，OMIVV 就無法妥善管理它們。OMIVV 會詳細顯示裸機或主機的不相容資訊，並且允許您修正不相容 (如果適用)。

您可以針對每一項執行下列其中一個動作，來檢視和修正相容性問題：

- 若要檢視和修復 vSphere 主機相容性問題，請參閱[執行修正不相容 vSphere 主機精靈](#)。
- 若要檢視和修復有相容性問題的裸機伺服器，請參閱[執行修正不相容裸機伺服器精靈](#)。


主題：

- [報告與修復 vSphere 主機的相容性](#)
- [檢視基準相容性](#)
- [使用 OMSA 搭配第 11 代伺服器](#)
- [報告及修正裸機伺服器的相容性](#)

報告與修復 vSphere 主機的相容性

在下列情況下，主機不相容：

- 主機未指派給連線設定檔。
- 重新啟動時收集系統清查 (CSIOR) 已停用或尚未執行，必須手動重新啟動。
- OMSA 代理程式未安裝、已過期或設定不正確。如果有針對第 11 代伺服器安裝或更新 OMSA，就必須重新啟動 ESXi 主機。
- 主機的 SNMP 陷阱目的地不是設為 OMIVV 裝置的 IP 位址。SNMP 陷阱目的地設定中的失敗可能是當連線設定檔中提供的 iDRAC 或主機認證無效、iDRAC 沒有可用插槽，或 iDRAC 鎖定模式已開啟 (只有在第 14 代主機中)。
- OMIVV 無法啟用在執行 ESXi 6.5 的主機上的 WBEM 服務。

 **警告:** 即使處於鎖定模式的主機不相容，也不會出現在相容性檢查中，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。

您可以執行修復不相容的 vSphere 主機精靈，來修復不相容的主機。有些不相容的 ESXi 主機需要重新啟動。如果 OMSA 必須安裝或更新，就必須重新啟動 ESXi 主機。此外，凡是未曾執行過 CSIOR 的主機，一律要重新開機。如果您選擇自動重新啟動 ESXi 主機，會發生下列動作：

- 若為 CSIOR 狀態修正：
 - 如果主機未曾執行過 CSIOR，則主機上的 CSIOR 會設定為開，然後主機會設定為維護模式並重新啟動。
- 如果主機沒有安裝 OMSA，或者執行的是不支援的 OMSA 版本：
 - 在主機安裝 OMSA。
 - 將主機設定為維護模式並重新啟動。
 - 重新啟動完成後會設定 OMSA，變更才會生效。
 - 主機離開維護模式。
 - 執行清查，重新整理資料。
- 針對 OMSA 狀態修正，其中已安裝受支援的 OMSA 版本，但必須加以設定：
 - 在主機設定 OMSA。
 - 執行清查，重新整理資料。

檢視和修復不相容的主機：

1. 在 OpenManage Integration for VMware vCenter 中，從管理標籤按一下 **相容性 > vSphere 主機**。
 - a. 在 **vSphere 主機** 頁面上，檢視不相容主機的清單。
 - 畫面會出現一個表格，列出不相容的主機，以及主機 IP 或主機名稱、型號、連線設定檔、CSIOR 狀態、OMSA 狀態、WBEM 狀態、SNMP 陷阱狀態、Hypervisor 和 iDRAC 授權狀態。
 - b. 若要深入檢視不相容主機的詳細資料，請選取一個不相容的主機。
 - c. 若要在表格中交換欄，請在資料格內拖放欄。
2. 若要修復不相容的主機，請按一下 **修復不相容的 vSphere 主機**。
 - 隨後便會啟動 **修復不相容的 vSphere 主機精靈**。這是動態精靈，且只會顯示與所選不相容主機有關的頁面。

如果所有選取的不相容主機都與 CSIOR 相容，您可以檢視精靈中的開啟 **CSIOR** 頁面。

3. 在**修復不相容的 vSphere 主機**精靈中，按一下**歡迎**頁面上的**下一步**。
4. 在**選取 vSphere 主機來修復相容性精靈**頁面中，選取您要修復之主機的核取方塊。
5. 按一下**下一步**。
隨後便會顯示警告訊息，如果有選取的主機未指派給連線設定檔，系統會提示您繼續相容性精靈，或取消修復相容性精靈。若要修復連線設定檔的不相容，請執行下列其中一項：
 - 若要從相容性精靈排除沒有指派給連線設定檔的主機，請按一下**繼續相容性精靈**。
 - 若要結束精靈，並在**連線設定檔**頁面上修復系統，請按一下**取消**。請參閱**建立連線設定檔** 第頁的 32。您可以在連線設定檔建立之後再回到精靈。
6. 如果您針對警告訊息按一下**繼續相容性精靈**，請在開啟 **CSIOR** 視窗中選取核取方塊，針對所選的主機開啟 **CSIOR**。
7. 按一下**下一步**。
8. 在**修復 OMSA** 視窗選取核取方塊，針對所選的主機修復 **OMSA**。
9. 按一下**下一步**。
10. 在**重新啟動主機**視窗中，檢視必須重新啟動的 ESXi 主機。
如果有安裝或更新 OMSA，就必須重新啟動 ESXi 主機。此外，凡是未曾執行過 CSIOR 的主機，一律要重新開機。請執行下列其中一項動作：
 - 如果希望在必要時讓主機自動進入維護模式，並重新啟動，請選取**必要時讓主機自動進入維護模式並重新啟動核取方塊**。
 - 如果您要手動重新開機，請在安裝 OMSA 後重新啟動主機；手動設定 OMSA，或在主機開始執行後以及 OMSA 沒有設定時透過相容性精靈設定，然後再次執行清查。請參閱**執行清查工作**。
11. 按一下**下一步**。
12. 在**摘要**視窗中，檢查不相容主機上發生的動作。
您必須手動重新開機，才能讓摘要頁面中的動作生效。
13. 按一下**完成**。

您在連線設定檔中提供有效資訊而修正 iDRAC 或主機認證後，或使 iDRAC 設陷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 設陷目的地狀態設定為**已設定**。

i 註：系統鎖定模式僅適用於第 14 代伺服器。

如果有不相容 WBEM 的主機存在，請確認手動修正那些主機的狀況，那些主機會使 WBEM 服務的啟用失敗。您可以在使用者記錄中檢視它們，然後允許 OMIVV 在清查時為那些主機啟用 WBEM 服務。

修復 vSphere 主機的 iDRAC 授權相容性

列在 vSphere 主機相容性頁面上的 vSphere 主機都是不相容的，因為它們沒有相容的 iDRAC 授權。表格顯示的是 iDRAC 授權的狀態。您可以按其中一個不相容的主機，檢視更多詳細資料 (例如 iDRAC 授權還剩幾天)，然後視需要加以更新。如果任何與連線設定檔相關聯之主機的 iDRAC 相容性狀態是「不相容」或「不明」，則**執行清查工作**連結會在作用中。

1. 在 OpenManage Integration for VMware vCenter 中，從**管理**標籤按一下**相容性 > vSphere 主機**。
2. 選取 **iDRAC 授權狀態不相容**的主機。
3. 如果授權已過期，請按一下**購買/更新 iDRAC 授權**連結。
4. 登入 **Dell 授權管理**頁面，並更新或購買新的 iDRAC 授權。
請使用此頁面上的資訊來識別及更新 iDRAC。
5. 安裝 iDRAC 授權後，請針對 vSphere 主機執行清查工作，待清查工作順利完成後，再回到此頁面，主機才能相容。

檢視基準相容性

基準相容性頁面會針對與叢集設定檔相關聯之所有受 OMIVV 管理的 vSAN 主機，依漂移偵測顯示基準相容性狀態。

- **組態相容性** — 顯示叢集設定檔所用的系統設定檔，與相關 vSAN 主機之間的屬性漂移。
- **韌體及驅動程式相容性** — 顯示叢集設定檔所用的韌體及/或驅動程式儲存庫設定檔，與相關 vSAN 主機之間的韌體與驅動程式版本漂移。

1. 在 **OpenManage Integration for VMware vCenter** 頁面上，按一下**管理 > 相容性 > 基準相容性**。
隨後便會顯示一個表格，列出與基準相關聯的不相容主機，以及主機 IP 或 FQDN、vCenter IP 或 FQDN、叢集名稱、叢集設定檔名稱、組態相容性狀態、韌體相容性狀態，和驅動程式相容性狀態。

i 註：只有不相容主機會顯示在**基準相容性**頁面上。

相容性類別如下：

- **相容** — 代表主機中的元件，與基準中的關聯設定檔相容。
- **不相容** — 代表主機中的元件，與基準中的關聯設定檔不相容。
- **不適用** — 代表韌體或驅動程式或系統設定檔與叢集設定檔並不相關。

a. 若要深入檢視主機的詳細資料，請選取一個您所要的主機。

您可以檢視底部窗格中的**主機名稱**和**上次漂移偵測時間**。

b. 若要在表格中交換欄，請在資料格內拖曳欄。

c. 若要篩選資料格的內容，請使用**篩選**。

i **註:** 您可以檢視以下有關**基準相容性**頁面的資訊：

- 不相容主機的總數
- 不相容叢集的總數
- 與基準相關聯的主機和叢集總數
- 漂移類型的不相容主機分配的總數

2. 本表列出漂移偵測工作順利完成後，與基準相關聯的主機。若要檢視漂移詳細資料，請選擇您所要的主機，然後按一下**顯示漂移詳細資料**。

隨後會顯示**漂移詳細資料**對話方塊。

3. 您可以在**漂移詳細資料**對話方塊中，檢視以下內容：

- 如果相容性漂移偵測工作失敗，相容性狀態會顯示為「不相容」，另外還會顯示失敗原因。請使用所指出的原因來解決問題。
- 如果漂移偵測工作順利完成，則相容性狀態會顯示為「不相容」，且**漂移詳細資料**頁面上會顯示以下詳細資料：

硬體：

- 執行個體 — 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 — 代表主機值。
- 基準值 — 代表基準值。
- 漂移類型 — 指出不相容的原因。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 142。

韌體和驅動程式：

- 元件名稱 — 代表元件的名稱。
- 目前值 — 代表主機值。
- 基準值 — 代表基準值。
- 漂移類型 — 指出不相容的原因。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 142。
- 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) — 代表更新所識別元件版本的重要性等級。
- 必須重新開機 — 代表裝置是否需要重新開機。

i **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。

4. 按一下**完成**。

使用 OMSA 搭配第 11 代伺服器

若要管理 PowerEdge 第 11 代伺服器，OMIVV 規定必須在伺服器上執行 OMSA。如果是透過 OMIVV 部署的第 11 代主機，就會自動安裝 OMSA。如果是手動方式部署的第 11 代主機，則可以選擇下列其中一項：

- 使用 OMIVV 安裝和設定 OMSA。請參閱[設定 OMSA 設陷目的地](#) 第頁的 114。
- 手動安裝和設定 OMSA。請參閱在 [ESXi 系統上部署 OMSA 代理程式](#) 第頁的 113。

i **註:** 使用 OMIVV 部署 OMSA 代理程式時，OMIVV 會啟動 HttpClient 服務，並在 ESXi 5.0 以後的版本啟用連接埠 8080，以下載並安裝 OMSA VIB。OMSA 安裝完成後，服務便會自動停止，連接埠也會關閉。

i **註:** 除了前述選項之外，您還可以使用 Web 用戶端主機相容性來安裝並設定 OMSA 代理程式。

在 ESXi 系統上部署 OMSA 代理程式

在 ESXi 系統上安裝 OMSA VIB，從系統收集清查與警示資訊。

註: Dell PowerEdge 第 12 代伺服器之前的 Dell 主機上，必須有 OpenManage 代理程式。請使用 OpenManage Integration for VMware vCenter 來安裝 OMSA，或先手動將 OMSA 安裝到主機上，再安裝 OpenManage Integration for VMware vCenter。若要詳細瞭解手動安裝 OMSA 代理程式，請參閱 <http://en.community.dell.com/techcenter/systems-management/w/wiki/1760.openmanage-server-administrator-omsa.aspx>

1. 如果沒有安裝 OMSA，請從 **www.vmware.com** 安裝 vSphere 命令列工具 (vSphere CLI)。
2. 輸入下列指令：

```
Vihostupdate.pl -server <IP Address of ESXi host> -i -b <OMSA version X.X>
```

註: OMSA 安裝可能需要幾分鐘的時間進行。此命令完成後，必須重新啟動主機。

註: SNMP 社群字串可以從 **管理 > 設定 > 設備設定 > OMSA SNMP 設陷社群字串** 設定。如需更多有關 SNMP 設陷社群字串的資訊，請參閱 **設定 SNMP 設陷社群字串**。

設定 OMSA 設陷目的地

所有第 11 代主機皆必須設定 OMSA。

註: 只有第 12 代 PowerEdge 伺服器以前的 Dell EMC 伺服器才需要 OMSA。

若要設定 OMSA 陷阱目的地：

1. 提供 `https://<HostIP>:1311/` 做為其 URL，以從 Web 瀏覽器導覽至 OMSA 代理程式。
2. 登入介面，然後選取 **警示管理** 標籤。
3. 選取 **警示動作**，並且確認凡是要監視的事件都已設定 **廣播訊息** 選項，這樣才會張貼事件。
4. 在索引標籤最上方選取 **平台事件**。
5. 按一下灰色的 **設定目的地** 按鈕，然後按一下 **目的地** 連結。
6. 選取 **啟用目的地** 核取方塊。
7. 在 **目的地 IP 位址** 欄位中，輸入 OMIVV 裝置的 IP 位址。
8. 按一下 **套用變更**。
9. 重複步驟 1 至 8，設定其他事件。


註: SNMP 社群字串可以從 **管理 > 設定 > 設備設定 > OMSA SNMP 設陷社群字串** 設定。如需更多有關 SNMP 設陷社群字串的資訊，請參閱 **設定 SNMP 設陷社群字串**。

報告及修正裸機伺服器的相容性

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)。
- 它不具備支援的 iDRAC、BIOS 或 LC 版本。
- LOM 或 rNDC 不存在。
- 系統鎖定模式已開啟。

檢視和修復不相容裸機伺服器的清單：

1. 在 OpenManage Integration for VMware vCenter 中，選取 **管理 > 部署** 標籤。
 - a. 在 **裸機伺服器** 頁面上，檢視不相容伺服器的清單。
畫面會出現一個表格，列出不相容的伺服器，以及產品服務編號、型號、iDRAC IP、伺服器狀態、系統鎖定模式、相容性狀態和 iDRAC 授權狀態。
 - b. 若要深入檢視伺服器的詳細資料，請選取一個不相容的伺服器。
 - c. 若要將伺服器的不相容資訊匯出至 .CSV 檔案，請在表格右側按一下 。
 - d. 若要篩選資料格的內容，請按一下 **篩選** 欄位。
 - e. 若要在表格中交換欄，請在資料格內拖放欄。
2. 若要修正不相容的伺服器，請按一下 **修正不相容的伺服器**。

i 註: 修正不相容的伺服器連結僅為第 11 代不相容的伺服器而啟用。

3. 在修正裸機相容性精靈中，按歡迎頁面上的下一步。
4. 在修正相容性頁面上，選取您要修正之伺服器的核取方塊。
隨後會列出不相容的伺服器，並顯示不相容的韌體元件。列出的不相容伺服器至少必須更新以下一個韌體元件：
 - iDRAC IP
i 註: 您無法從 OMIVV 修正 iDRAC 授權不相容的裸機伺服器。請確定將支援的 iDRAC 授權上傳到 OMIVV 以外的伺服器，然後按一下 [重新整理裸機伺服器](#)。請參閱 [重新整理裸機伺服器](#) 第頁的 115。
 - BIOS
 - LC
 - 系統鎖定模式
i 註: 若要從相應的 iDRAC 檢視不相容裸機伺服器的最新詳細資料，請按一下 [重新整理裸機詳細資料](#)。如果系統鎖定模式已開啟，則伺服器不相容，反之則相容。
5. 若要檢視相容性問題的詳細資訊，請按一下 [相容性問題](#)。
i 註: 如果裸機伺服器由於系統鎖定模式開啟而不相容，請確定您從 iDRAC 主控台手動設定伺服器的系統鎖定模式。
6. 按一下下一步。
7. 在摘要視窗中，檢查不相容裸機伺服器的韌體元件上發生的動作。
8. 按一下完成。

修正裸機伺服器的 iDRAC 授權相容性

裸機伺服器頁面所列的裸機伺服器都是不相容的，因為它們沒有相容的 iDRAC 授權。表格顯示的是 iDRAC 授權的狀態。您可以按其中一個不相容的裸機伺服器，檢視更多詳細資料 (例如 iDRAC 授權還剩幾天)，然後視需要加以更新。如果裸機伺服器頁面上的 [重新整理裸機伺服器](#) 連結是在啟用狀態，就表示有因為 iDRAC 授權而不相容的裸機伺服器。

1. 在 OpenManage Integration for VMware vCenter 中，選取 [管理 > 部署](#) 標籤。
在 [裸機伺服器](#) 頁面上，檢視表格所顯示的不相容伺服器清單。
2. 選取 **iDRAC 授權狀態不相容或不明的** 裸機伺服器。
3. 如果授權已過期，請按一下 [購買/更新 iDRAC 授權](#) 連結。
4. 登入 [Dell 授權管理](#) 頁面，並更新或購買新的 iDRAC 授權。
請使用此頁面上的資訊來識別及更新 iDRAC。
5. 安裝 iDRAC 授權之後，請按一下 [重新整理裸機伺服器](#)。

重新整理裸機伺服器

1. 在 [OpenManage Integration for VMware vCenter](#) 頁面上，按一下 [管理 > 部署 > 裸機伺服器](#)，然後按一下 [重新整理裸機伺服器](#)。
2. 在 [重新整理裸機伺服器](#) 視窗中，選取要重新整理資料的伺服器，然後按一下 [重新整理選取的伺服器](#)。

重新整理裸機伺服器資料可能需要幾分鐘的時間。

所有選取的裸機伺服器資料皆會在 [裸機伺服器](#) 頁面中重新整理。

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 角色、Dell 操作角色和 Dell 基礎結構部署角色。

主題：

- 資料完整性
- 存取控制驗證、授權與角色
- Dell 操作角色
- Dell 基礎結構部署角色
- 關於權限

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 SSL/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 SSL 憑證，還會在通訊與 OpenManage Integration for VMware vCenter 註冊之前，驗證與信任 vCenter Server 的憑證。OpenManage Integration for VMware vCenter 的主控台標籤會使用安全性程序，以防止金鑰在管理主控台和後端服務來回傳送時的不當要求。這類安全性會使跨網站要求偽造失敗。

安全管理主控台工作階段會在閒置 5 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。

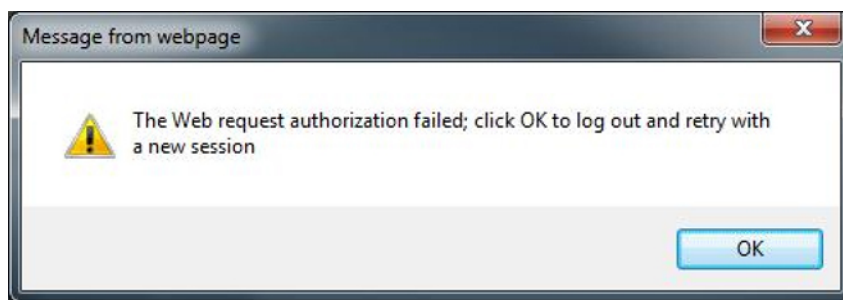


圖 3. 安全性錯誤訊息

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 Web 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 39. 權限群組

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

Dell 基礎結構部署角色

此角色包含與 Hypervisor 部署功能相關的權限。

這個角色提供的權限為建立範本、設定硬體組態設定檔、設定 Hypervisor 部署設定檔、設定連線設定檔、指派身份以及部署。

權限群組 — Dell.Deploy - 佈建

建立範本、設定硬體組態設定檔、設定 Hypervisor 部署設定檔、設定連線設定檔、指派身份、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
 - 登錄並設定警示，例如在事件設定頁面啟用/停用警示
 - 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
 - 從 Dell 伺服器管理索引標籤的閃爍 LED、清除 LED、設定 OMSA URL
 - 啟動 OMSA 主控台
 - 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

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 133

主題：

- [常見問題集 - FAQ](#)
- [裸機部署問題](#)

常見問題集 - FAQ

本節包含一些常見問題和解決方式。

在 Google Chrome 中，「全部匯出」按鈕無法匯出為 .CSV 檔案

註冊 vCenter Server 之後，如果您新增一個主機，並建立連線設定檔，然後檢視該主機的清查詳細資料，那麼**全部匯出**按鈕便會傳回失敗。**全部匯出**按鈕不會將資訊匯出至 .CSV 檔案。

 註：

在所有版本的 Google Chrome 瀏覽器中，**全部匯出**按鈕都不會以**無痕模式**將資訊匯出至 .CSV 檔案。

解決方法：若要在 Google Chrome 中，使用**全部匯出**按鈕將資訊匯出至 .CSV 檔案，請在 Chrome 瀏覽器中停用**無痕模式**。

受影響的版本：4.0

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，雖然您在 vSphere 主機清單中看得到該主機，但是當您按一下該主機想要查看其詳細資料時，**iDRAC 授權類型**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

從舊版 OMIVV 取消登錄 vCenter，接著使用較新 OMIVV 版本登錄相同的 vCenter 後，Dell EMC 圖示沒有顯示

如果您從舊版 OMIVV 取消登錄 vCenter 伺服器，然後以相同 vCenter 伺服器登錄較新版本的 OMIVV，在 [vsphere-client-serenity] 資料夾下便會出現舊版 OMIVV 的舊有資料項目。由於在 vCenter 裝置上存在舊版 OMIVV 專屬的舊有資料，因此即使在較新版本的 OMIVV 登錄後，亦不會顯示 Dell 圖示。

解決方式：執行下列步驟：

1. 若為 VMware vCenter，請移至 /etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity，若為 Windows vCenter，請移至 vCenter 裝置中的 C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity 資料夾，您會看見如下的舊資料：
 - com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-3.0.0.197
2. 手動刪除對應舊版 OMIVV 的資料夾。
3. 在 vCenter 伺服器重新啟動 vSphere Web 用戶端服務。

受影響的版本：全部

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 11。
 2. 重新啟動已登錄的 OMIVV 裝置。
 3. 登出 Web 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 Web 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

在 ESXi 5.x 主機上執行韌體更新工作時，清查工作會失敗

註冊 vCenter Server 之後，如果您在 ESXi 5.x 主機上執行韌體更新工作，並在**選取元件**畫面上選取 iDRAC 作為元件，主機中的 ESXi 便無法與新的 iDRAC IP 同步處理，而提供給 OMIVV 的 iDRAC IP 也因此失效。這也是您無法在該主機上順利執行清查的原因。

解決方法：若要解決這個問題，請在 ESXi 主機上重新啟動 sfcd 精靈。如需更多相關資訊，請參閱 https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2077693。


受影響的版本：4.0

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「network latencies or unreachable host (網路延遲或無法連線主機)」、「connection refused (連線遭拒)」、「operation has timed out (作業逾時)」、「WSMAN」、「no route to host (無法通往主機)」和「IP address: null (IP 位址：null)」等訊息。

1. 開啟 iDRAC 虛擬主控台。
2. 按下 F2 並瀏覽至**故障診斷**選項。
3. 在**故障診斷**選項中瀏覽至**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 [建立連線設定檔](#) 第頁的 44，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 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「不明」。當 iDRAC 無法連線時，就會顯示不明狀態。

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。

i 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

在嘗試以嚴重性類別篩選時，OMIVV 並未顯示所有相關記錄

當您從下拉式清單選擇**所有類別**，並從中選擇以嚴重性類別來篩選記錄資料時，所有屬於特定類別的記錄都會正確顯示。如果您是從篩選下拉式清單中選擇**資訊**加以篩選，就不會顯示韌體更新記錄，只會顯示工作初始化記錄。

解決方法：若要在 OMIVV 中檢視所有記錄，請從「篩選」下拉式清單中選取**所有類別**。

受影響的版本：3.1

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。如需更多相關資訊，請造訪 http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121701 和 http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121689。

在 Windows vSphere 6.0 中更新 ssl Anchor

1. 從 http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121701 下載 `lstoolutil.py.zip` 檔案。
2. 將 `lstoolutil.py` 檔案複製到 `%VMWARE_CIS_HOME%\VMware Identity Services\lstool\scripts\` 資料夾。
i 註：若您使用 vSphere 6.0 Update 1，請勿替換 `lstoolutil.py` 檔案。

您可以使用下列相關程序來更新 ssl Anchor：

- 為安裝於 Windows 作業系統上的 vCenter 更新 ssl Anchor：使用 vSphere 憑證管理員公用程式，替換 vCenter Windows 安裝上的憑證。請參閱 [替換 vCenter Windows 安裝上的憑證](#) 第頁的 121。
- 為 vCenter Server 應用裝置更新 ssl Anchor：使用 vSphere 憑證管理員公用程式，替換 vCenter Server 應用裝置上的憑證。請參閱 [替換 vCenter 伺服器應用裝置上的憑證](#) 第頁的 122。

上述程序所得到的輸出，應該會分別顯示 `Updated 24 service (s)` 和 `Updated 26 service (s)`。如果顯示的輸出是 `Updated 0 service (s)`，則表示舊的憑證指紋不正確。您可以執行下列步驟，擷取舊的憑證指紋。此外，若沒有使用 **vCenter 憑證管理員** 來替換憑證，請使用以下程序來擷取舊的憑證指紋：

i 註：使用所取得的舊指紋來執行 `ls_update_certs.py`。

1. 從受管物件瀏覽器 (MOB) 擷取舊憑證。請參閱 [從受管物件瀏覽器 \(MOB\) 擷取舊憑證](#) 第頁的 122。
2. 從舊憑證擷取指紋。請參閱 [從舊憑證擷取指紋](#) 第頁的 123。

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

若使用 vSphere 憑證管理員公用程式替換 vCenter Windows 安裝上的憑證，請執行下列步驟：

1. 透過遠端桌面連線連接至外部平台服務控制器。
2. 以系統管理員模式開啟命令提示字元。
3. 使用以下命令來建立 `c:\certificates` 資料夾：`mkdir c:\certificates`
4. 使用以下命令來擷取舊憑證：`"%VMWARE_CIS_HOME%\vmafdd\vecs-cli entry getcert --store BACKUP_STORE --alias bkp__MACHINE_CERT --output c:\certificates\old_machine.crt`
5. 使用以下命令來擷取舊憑證指紋：`"%VMWARE_OPENSSL_BIN%" x509 -in C:\certificates\old_machine.crt -noout -sha1 -fingerprint`

i 註: 所擷取的憑證指紋，其格式如下：SHA1

```
Fingerprint=13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88
```

指紋是一串數字和字母，如下所示：13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88

6. 使用以下命令來擷取新憑證：`%VMWARE_CIS_HOME%\vmafdd\vecs-cli entry getcert --store MACHINE_SSL_CERT --alias __MACHINE_CERT --output c:\certificates\new_machine.crt`

7. 執行下列步驟：

- a. 使用以下命令來執行 `ls_update_certs.py`。`%VMWARE_PYTHON_BIN% ls_update_certs.py --url`
- b. 使用以下命令，將 `psc.vmware.com` by `Lookup_Service_FQDN_of_Platform_Services_Controller` 和 `13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88` 指紋換成在步驟 5 所取得的指紋：`https://psc.vmware.com/lookupservice/sdk --fingerprint 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 --certfile c:\certificates\new_machine.crt --user Administrator@vsphere.local --password Password`

i 註: 確定提供有效的憑證。

8. 在所有服務成功更新後，登出並再次登入 vCenter Web 用戶端。

OMIVV 現在可成功啟動。

替換 vCenter 伺服器應用裝置上的憑證

若使用「vSphere 憑證管理員」公用程式替換 vCenter 伺服器應用裝置上的憑證，請執行下列步驟：

1. 透過主控台或 Secure Shell (SSH) 工作階段登入外部平台服務控制器應用裝置。
2. 執行以下命令來存取 Bash shell：`shell.set --enabled true`
3. 輸入 `shell` 並按下 **Enter** 鍵。
4. 使用以下命令來建立資料夾或憑證：`mkdir /certificates`
5. 使用以下命令來擷取舊憑證：`/usr/lib/vmware-vmafd/bin/vecs-cli entry getcert --store BACKUP_STORE --alias bkp__MACHINE_CERT --output /certificates/old_machine.crt`
6. 使用以下命令來擷取舊憑證指紋：`openssl x509 -in /certificates/old_machine.crt -noout -sha1 -fingerprint`

i 註: 所擷取的憑證指紋，其格式如下：SHA1

```
Fingerprint=13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88
```

指紋是一串數字和字母，如下所示：13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88

7. 使用以下命令來擷取新憑證：`/usr/lib/vmware-vmafd/bin/vecs-cli entry getcert --store MACHINE_SSL_CERT --alias __MACHINE_CERT --output /certificates/new_machine.crt`

8. 執行以下命令來變更目錄：`cd /usr/lib/vmidentity/tools/scripts/`

9. 執行下列步驟：

- a. 使用以下命令來執行 `ls_update_certs.py`。`python ls_update_certs.py --url`
- b. 使用以下命令，將 `psc.vmware.com` by `Lookup_Service_FQDN_of_Platform_Services_Controller` 和 `13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88` 指紋換成在步驟 6 所取得的指紋：`https://psc.vmware.com/lookupservice/sdk --fingerprint 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 --certfile /certificates/new_machine.crt --user Administrator@vsphere.local --password "Password"`

i 註: 確定提供有效的憑證。

10. 在所有服務成功更新後，登出並再次登入 vCenter Web 用戶端。

OMIVV 現在可成功啟動。

從受管物件瀏覽器 (MOB) 擷取舊憑證

您可以使用受管物件瀏覽器 (MOB) 連線至平台控制器服務 (PSC)，為 vCenter 伺服器系統擷取舊憑證。

若要擷取舊的憑證，您應可以透過執行下列步驟，找到 `ArrayOfLookupServiceRegistrationInfo` 受管物件的 `sslTrust` 欄位：

i 註: 在本指南中，`C:\certificates\` 資料夾位置是用於儲存所有憑證。

1. 使用以下命令，在 PSC 上建立 C:\certificates\ 資料夾：mkdir C:\certificates\.
2. 在瀏覽器中開啟以下連結：<https://<vCenter FQDN|IP address>/lookupservice/mob?moid=ServiceRegistration&method=List>
3. 系統出現提示時，以 administrator@vsphere.local 使用者名稱登入，並提供密碼。
 (i) 註：如果您在 vCenter 單一登入 (SSO) 網域使用自訂名稱，請使用該使用者名稱和密碼。
4. 在 **filterCriteria** 中修改值欄位以僅顯示標籤 **<filtercriteria></filtercriteria>**，並按一下叫用方式。
5. 根據您要更換的憑證，搜尋下列主機名稱：

表 40. 搜尋準則資訊

信賴起點	搜尋準則
vCenter 伺服器	使用 Ctrl+F 在頁面上搜尋 vc_hostname_or_IP.example.com
平台服務控制器	使用 Ctrl+F 在頁面上搜尋 psc_hostname_or_IP.example.com

6. 找到對應 sslTrust 欄位的值。sslTrust 欄位的值，是舊憑證的 Base64 編碼字串。
7. 在更新平台服務控制器或 vCenter 伺服器的信賴起點時，請使用下列範例。

(i) 註：為了改善可讀性，實際的字串會大幅縮短。

- 針對 vCenter 伺服器

表 41. vCenter 伺服器範例

名稱	類型	值
URL	anyURI	https://vcenter.vmware.local:443/sdk

- 針對平台服務控制器

表 42. 平台服務控制範例

名稱	類型	值
URL	anyURI	https://psc.vmware.local/sts/STSService/vsphere.local

8. 將 sslTrust 欄位的內容複製到文字文件，並將文件儲存為 old_machine.txt。
9. 在文字編輯器中開啟 old_machine.txt。
10. 請在 old_machine.txt 檔案的開頭及結尾分別加上下列字串：

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

11. 現在將 old_machine.txt 另存為 old_machine.crt。

您現在可以由此憑證擷取指紋。

從舊憑證擷取指紋

您可以從舊的憑證擷取指紋，並使用以下選項上傳到平台服務：

- 利用憑證檢視器工具擷取指紋。請參閱[利用憑證檢視器工具擷取憑證指紋](#) 第頁的 123。
- 在應用裝置上使用命令列擷取指紋。請參閱[使用命令列擷取指紋](#) 第頁的 124。

利用憑證檢視器工具擷取憑證指紋

執行下列步驟以擷取憑證指紋：

1. 在 Windows 中，按兩下 old_machine.txt 檔案以使用 Windows 憑證檢視器開啟。
2. 在 Windows 憑證檢視器中，選取 **SHA1 指紋** 欄位。
3. 將指紋字串複製到純文字編輯器中，將字串中的空白以冒號替代或移除。

例如，指紋字串可能顯示為下列其中一種：

- ea87e150bb96fbbe1fa95a3c1d75b48c30db7971
- ea:87:e1:50:bb:96:fb:be:1f:a9:5a:3c:1d:75:b4:8c:30:db:79:71

使用命令列擷取指紋

您可以參閱以下各節，以瞭解如何在應用裝置與 Windows 安裝上使用命令列擷取指紋。

在 vCenter 伺服器應用裝置上使用命令列擷取指紋

執行下列步驟：

1. 將 old_machine.crt 憑證移動或上傳至 PSC 中擷取舊憑證程序的步驟 1 所建立的 C:\certificates\old_machine.crt 位置。您可以使用 Windows Secure Copy (WinSCP) 或另一個 SCP 用戶端來移動或上傳憑證。
2. 透過 Secure Shell (SSH) 登入外部平台服務控制器應用裝置。
3. 執行以下命令來啟用存取 Bash shell：shell.set --enabled true。
4. 輸入 shell 並按下 **Enter** 鍵。
5. 執行以下命令來擷取指紋：openssl x509 -in /certificates/old_machine.crt -noout -sha1 -fingerprint

註：指紋會顯示為等號後的一組數字與字母，如下所示：SHA1 Fingerprint=
ea:87:e1:50:bb:96:fb:be:1f:a9:5a:3c:1d:75:b4:8c:30:db:79:71

在 Windows 安裝上使用命令列擷取指紋

執行下列步驟：

1. 將 old_machine.crt 憑證移動或上傳至 PSC 中擷取舊憑證程序的步驟 1 所建立的 C:\certificates\old_machine.crt 位置。您可以使用 Windows Secure Copy (WinSCP) 或另一個 SCP 用戶端來移動或上傳憑證。
2. 透過遠端桌面連線連接至外部平台服務控制器。
3. 以系統管理員模式開啟命令提示字元。
4. 執行以下命令來擷取指紋："%VMWARE_OPENSSL_BIN%" x509 -in c:\certificates\old_machine.crt -noout -sha1 -fingerprint

註：指紋會顯示為等號後的一組數字與字母，如下所示：SHA1
Fingerprint=09:0A:B7:53:7C:D9:D2:35:1B:4D:6D:B8:37:77:E8:2E:48:CD:12:1B

使用舊指紋來執行 ls_update_certs.py。待服務順利更新後登出並再次登入 vCenter Web 用戶端。隨後 Dell 外掛程式便能順利啟動。

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。

解決方法：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。

從「工作佇列」頁面選取時，保固和清查排程未套用到所有的 vCenter

瀏覽至 Dell 首頁 > 監視 > 工作佇列 > 保固/清查歷史記錄 > 排程。接著選取一個 vCenter，然後選取修改排程按鈕。當對話方塊出現時，您會看到套用到所有註冊的 vCenter 訊息的核取方塊。當您選取該核取方塊，並按下套用時，設定會套用到您最初選取的那個 vCenter，而不是所有的 vCenter。但是當您在工作佇列頁面修改保固或清查排程之後，套用到所有註冊的 vCenter 就不適用了。

解決方式：請只在要修改選取的 vCenter 時，才從工作佇列使用修改保固或清查排程。

受影響的版本：2.2 以後的版本

如果在 OMIVV 變更 DNS 設定後，vCenter Web 用戶端出現 Web 通訊錯誤，我該如何做

如果您在變更 DNS 設定後，進行任何 OMIVV 相關工作時，vCenter Web 用戶端上出現任何種類的 Web 通訊錯誤，請執行以下任一項：

- 清除瀏覽器快取記憶體。
- 登出後再登入 Web 用戶端。

若瀏覽到其他頁面再返回「設定」頁面，「設定」頁面就無法載入

如果您用的是 vSphere v5.5，則在 Web 用戶端中離開再回到設定頁面時，該頁面可能會無法載入，微調按鈕會持續微調。無法載入是一種重新整理問題，頁面無法正確重新整理。

解決方式：按一下全域重新整理，畫面就會正確重新整理。

受影響的版本：2.2 和 3.0

在初始組態精靈的「清查排程與保固排程」頁面上，出現「不能將工作排程在過去的時間」錯誤

在 Web 用戶端中，遇到以下情況就會顯示「不能將工作排程在過去的時間」錯誤：

- 如果您在初始組態精靈中選取「所有登錄的 vCenter」，而且有些 vCenters 沒有主機。
- 當某些 vCenter 已經排定清查或保固工作。
- 當某些 vCenters 尚未設定清查或保固排程。

解決方案：從 vCenter 的設定頁面再次分別執行清查及保固排程的設定。

受影響的版本：2.2 以後的版本

韌體頁面上有些韌體的安裝日期顯示為 1969 年 12 月 31 日

在 Web 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

連續全域重新整理會在最近的工作視窗中擲出例外。

如果您重複按了重新整理按鈕，VMware UI 可能會擲出例外。

解決方法：您可以解除這個錯誤，然後繼續進行。

受影響的版本：2.2 以後的版本

使用 IE 10 時，為什麼有些 Dell 畫面的 Web 用戶端 UI 會扭曲

有時候當快顯對話方塊顯示時，背景中的資料會變成白色，而且會扭曲。

解決方法：關閉對話方塊，畫面就會恢復正常。

受影響的版本：2.2 以後的版本

我已向 vCenter 成功登錄外掛程式，但在 Web 用戶端上看不到 OpenManage Integration 圖示

除非 vCenter Web 用戶端服務重新啟動，否則 OpenManage Integration 圖示不會顯示在 Web 用戶端上。當您登錄 OpenManage Integration for VMware vCenter 應用裝置時，該應用裝置會同時在 Web 用戶端上註冊。如果您取消登錄應用裝置，然後再重新登錄相同版本，或是登錄該應用裝置的新版本，系統會成功登錄，但是 Web 用戶端上可能不會出現 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 Web 用戶端服務。這樣外掛程式便會顯示在 UI 中。

解決方法：在 vCenter Server 上重新啟動 Web 用戶端服務。

受影響的版本：2.2 以後的版本

即使儲存庫中有所選第 11 代系統的套件組合，韌體更新卻顯示沒有套件組合可供韌體更新使用

將處於鎖定模式的主機新增至連線設定檔時，清查展開後卻失敗，並指出「找不到遠端存取控制器，或是此主機不支援清查」。但是清查功能應適用於鎖定模式的主機。

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，才能執行下一個作業。如果您是使用 11G 主機進行韌體更新，那麼即使儲存庫具有該系統的套件組合，韌體更新精靈也不會顯示任何套件組合。這是因為 11G 主機可能尚未設定為讓 OMSA 傳送陷阱到 OpenManage Integration。

解決方法：使用 OpenManage Integration Web 用戶端的主機相容性精靈，確保該主機相容。如果不相容，請使用「修復主機相容性」讓主機相容。

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。

解決方法：如果 DNS 伺服器設定與 DHCP 不同，請以靜態方式指派 IP 設定。

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 第 12 代伺服器和部分搭載 13.5.2 版韌體的 Intel 網路卡具有已知問題。如果韌體更新是使用 Lifecycle Controller 加以套用，則搭載本版韌體之部分型號的 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：注意：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

使用無效的 DUP 來更新韌體時，雖然 LC 內的工作狀態顯示為「失敗」，但是 vCenter 主控台上的硬體更新工作狀態卻不是失敗，也不是逾時數小時。為什麼會這樣

如果挑選無效的 DUP 來更新韌體，vCenter 主控台視窗中的工作狀態仍是「進行中」，但訊息則會改為故障原因。這是已知的 VMware 問題，這個問題在未來版本的 VMware vCenter 中會解決。

解決方法：必須手動取消工作。

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，則「失敗：連線至 URL...時發生錯誤」這則錯誤訊息會顯示在「應用裝置更新」檢視的頂端。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 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 PowerEdge 第 12 代和更高世代的 Dell 伺服器中，處理器版本是位於「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。如需進一步瞭解 OMIVV 如何以連結模式運作，請參閱 *OpenManage Integration for VMware vCenter：以連結模式運作* 這份白皮書，網址為 www.dell.com。

OMIVV 有哪些必要的連接埠設定

註：使用 OMIVV 相容性視窗中提供的修復不相容的 vSphere 主機連結部署 OMSA 代理程式時，OMIVV 會啟動 http 用戶端服務，並在 ESXI 5.5 以後的版本上啟用連接埠 8080，以下載並安裝 OMSA VIB。OMSA VIB 安裝完成後，服務會自動停止，且連接埠會關閉。

使用下列適用於 OMIVV 的連接埠設定：

表 43. 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 43. 虛擬裝置 (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
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。
80	HTTP	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 OS 部署流程，讓安裝後指令碼能和 OMIVV 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 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 裝置公開給受管節點的 NFS 公用共用，用於韌體更新和 OS 部署流程。
4001 至 4004	NFS	UDP/TCP	無	輸入/輸出	OMIVV 裝置至 NFS	公用共用	由 OMIVV 裝置公開給受管節點的 NFS 公用共用，用於韌體更新和 OS 部署流程。
11620	SNMP 代理程式	UDP	無	輸入	iDRAC 至 OMIVV 裝置	SNMP 代理程式 (伺服器)	iDRAC、OMSA 和 CMC 通訊，用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	代理伺服器 (Proxy)	使用 Proxy 伺服器進行通訊

表 44. 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；下載 OMSA VIB 和修復不相容的 vSphere 主機	可協助 ESXi 下載 OMSA/驅動程式 VIB。

表 45. 受管節點 (iDRAC/CMC)

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 裝置至 iDRAC/CMC	iDRAC 通訊	用來提供資訊給管理站。此連接埠必須從 iDRAC 和 CMC 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。這用於 OS 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。這用於 OS 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 (Trivial File Transfer)	用於從管理站順利管理 iDRAC。

成功套用硬體設定檔或系統設定檔 (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

如果僅選取硬體設定檔或系統設定檔範本以進行部署，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 Web 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。

如何使用 OMSA 模擬溫度硬體故障，來測試事件設定

為確保事件正常運作，請執行下列步驟：

1. 在 OMSA 使用者介面上，瀏覽至**警示管理 > 平台事件**。
2. 選取**啟用平台事件篩選器警示核取方塊**。
3. 向下捲動到底部，然後按一下**套用變更**。
4. 為了確保啟用溫度警告等特定事件，請從左側樹狀結構選取**主系統機箱**。
5. 在**主系統機箱**選取**溫度**。
6. 選取**警示管理索引標籤**，然後選取**溫度探針警告**。
7. 選取**廣播訊息核取方塊**，然後選取**套用變更**。
8. 從左側樹狀檢視畫面選取**主系統機箱**，引起溫度警告事件。
9. 在**主系統機箱**選取**溫度**。
10. 選取**主機板周圍溫度連結**，然後選取**設定值選項按鈕**。
11. 將**警告閾值上限**設定為目前所列讀數前面的值。
例如，如果目前讀數為 27，請將閾值設定為 **25**。
12. 選取**套用變更**，隨後就會產生溫度警告事件。

若要導致另一個事件，請使用同一個設定值選項來還原原始設定。這時事件會當作警告產生，然後進入正常狀態。如果一切正常運作，請瀏覽至 **vCenter 工作與事件檢視**；隨後應該會顯示一個溫度探針警告事件。

i 註：重複事件有篩選器可用；如果嘗試連續觸發同一個事件太多次，您只會收到一個事件。事件之間至少要等 30 秒，才能查看所有事件。

我明明已將 OMSA 代理程式安裝在 OMIVV 主機系統上了，卻還是收到錯誤訊息，說 OMSA 尚未安裝。

若要在第 11 代伺服器解決這個問題：

1. 用主機系統上的遠端啟用元件安裝 **OMSA**。
2. 如果您是使用命令列來安裝 OMSA，請務必指定 **-c** 選項。如果您已經安裝了 OMSA，請以 **-c** 選項重新安裝它，然後重新啟動服務：

```
srvadmin-install.sh -c  
srvadmin-services.sh restart
```

如果是 ESXi 主機，請務必使用 **VMware 遠端 CLI 工具** 來安裝 **OMSA VIB**，然後將系統重新開機。

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 5.0 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連線設定檔時，清查啟動後卻失敗，表示「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。

使用參照伺服器時無法建立硬體設定檔

請檢查以確認您有安裝基本建議版本的 iDRAC 韌體、Lifecycle Controller 韌體和 BIOS。

為了確保從參照伺服器擷取的是最新資料，請啟用**在重新啟動時收集系統清查 (CSIOR)**，然後重新啟動參照伺服器，再擷取資料。

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. 確定指派伺服器身份時所選取的 **NIC** 與虛擬裝置位於相同的網路上。
3. 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。
4. 確定系統至少找到 1 個**虛擬磁碟**。

ESXi 也可以安裝到內部 SD 卡。

Hypervisor 無法部署在 Dell PowerEdge R210 II 機器上

由於 BIOS 無法從連接的 ISO 啟動，因此 Dell PowerEdge R210 II 系統上的逾時問題，會導致 Hypervisor 部署失敗。

解決方法：將 Hypervisor 手動安裝在機器上。

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，不符合建議的基本需求。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 到應用裝置。
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 強制移除虛擬應用裝置

1. 前往 https://<vcenter_serverIPAddress>/mob
2. 輸入 VMware vCenter 管理員認證。
3. 按一下 **內容**。
4. 按一下 **ExtensionManager**。
5. 按一下 **UnregisterExtension**。
6. 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**。
7. 在 vSphere Web 用戶端中關閉 OMIVV，並加以刪除。取消登錄機碼必須用於 Web 用戶端。

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「加密碼」欄位。您必須向下捲動頁面，才能輸入加密碼。

在 vSphere Web 用戶端按一下「Dell 伺服器管理 Portlet」或 Dell 圖示，結果傳回 404 錯誤


請檢查 OMIVV 裝置是否在執行中；如果沒有，請從 vSphere Web 用戶端重新啟動它。然後等候幾分鐘，待虛擬裝置 Web 服務啟動之後，再重新整理頁面。如果錯誤持續發生，請嘗試在命令列使用 IP 位址或完整網域名稱來 Ping 應用裝置。如果 Ping 無法解決問題，請查看您的網路設定，確認它們是正確的。

韌體更新失敗時該怎麼辦

檢查虛擬裝置記錄，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，解決方法之一就是改用靜態 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** (完整的網域名稱)。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。

連線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 主控台的使用者清單，然後按以下其中一項：
 - iDRAC6：選取 **iDRAC 設定** > **「網路/安全性」** 標籤 > **「使用者」** 標籤。
 - iDRAC7：選取 **iDRAC 設定** > **「使用者」** 標籤。
 - iDRAC8：選取 **iDRAC 設定** > **「使用者」** 標籤。
4. 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。
5. 按一下**設定使用者**，然後按一下**下一步**。
6. 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**。

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。

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。因此，即使主機已從 vCenter 樹狀結構中移除，仍會顯示在機箱底下，直到下次執行機箱清查為止。

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。

解決方法：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。

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。

解決方法：在 OpenManage Integration for VMware GUI 的**管理 > 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，Hypervisor 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)，Hypervisor 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。

解決方法：如果您要在進行部署時透過系統設定檔變更 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

當可用版本比目前版本舊時，可用的虛擬裝置版本會顯示錯誤的資訊

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。

i 註：建議您將更新儲存庫路徑設定為最新版本，且不支持虛擬設備版本降級。

當新增具有 Express 授權的第 12 代裸機伺服器時，會擲出 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。

在第 14 代上部署 OS 期間，硬體設定檔會因 iDRAC 錯誤而套用失敗

在第 14 代伺服器上部署 OS 期間，在套用硬體設定檔時，會在 iDRAC 中建立組態更新工作。但是，該工作有時會失敗，並顯示訊息指出組態工作已建立。

解決方法：若要清除陳舊項目並重試作 OS 部署，請執行 `racadm jobqueue delete -i JID_CLEARALL_FORCE` 命令。

當 Proxy 設定有網域使用者驗證時，OMIVV RPM 升級會失敗

如果 OMIVV 應用裝置已設定使用 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，而無法套用到相同 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。

解決方法：從 FX2 機箱插槽 1 的 FC640 伺服器取得的系統設定檔，只能套用到另一個 FX2 機箱插槽 1 的另一個 FC640 伺服器。

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
```

相關說明文件

除了本指南外，您還可以在 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 4.2** 以存取下列文件：

- *OpenManage Integration for VMware vCenter 4.2 版 Web 用戶端使用者指南*
- *OpenManage Integration for VMware vCenter 4.2 版版本資訊*
- *OpenManage Integration for VMware vCenter 4.2 版相容性比較表*

您可在 delltechcenter.com 上找到包含白皮書在內的技術性作品。在 Dell TechCenter Wiki 首頁上，按一下**系統管理 > OpenManage Integration for VMware vCenter** 即可存取文章。

主題：

- 從 Dell EMC 支援網站存取文件

從 Dell EMC 支援網站存取文件

您可以用下列方式之一存取所需文件：

- 使用下列連結：
 - Dell EMC 企業系統管理、Dell EMC 遠端企業系統管理，以及 Dell EMC 虛擬化解決方案文件 — www.dell.com/esmmanuals
 - Dell EMC OpenManage 文件 — www.dell.com/openmanagemanuals
 - 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 — <https://www.dell.com/serviceabilitytools>
- 從 Dell EMC 支援網站：
 1. 前往 <https://www.dell.com/support>。
 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
 - 大型主機
 - 作業系統
 - 公共事業解決方案
 - 服務性工具
 - 支援
 - 公用程式
 - 虛擬化解決方案
 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。

系統專有屬性

iDRAC

表 46. 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
DNSDomainName	DNS 網域名稱	NIC 靜態資訊
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
DNS1	DNS 伺服器 1	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 47. 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

表 47. 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
IscsiDev1Con1TargetIp	目標 IP 位址	連線 1 設定
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 48. 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 49. 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

表 49. 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
IscsiInitiatorGateway	預設閘道	iSCSI 啟動器參數
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 50. 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

自訂屬性

表 51. 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	RAIDPState	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。

其他資訊

下列 Dell 技術白皮書可提供更多有關係統設定檔組態範本、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*

元件與基準版本比較表

表 52. 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	硬體元件不符合相關的基準。	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版本，但未提供元件或屬性。	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	韌體元件符合相關聯的基準。	相容
	可用	可用	韌體元件不符合相關的基準。	不相容
	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	驅動程式元件符合相關聯的基準。	相容
	可用	可用	驅動程式元件不符合相關的基準。	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，但未提供元件或屬性，或是有提供新元件。	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