

# OpenManage Integration for VMware vCenter for Desktop Client

使用者指南 3.1 版



# 註、警示與警告



註: 「註」表示可以幫助您更有效地使用電腦的重要資訊。



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」表示有可能會導致財產損失、人身傷害甚至死亡。

Copyright © 2016 Dell Inc. 版權所有。本產品受美國與國際著作權及智慧財產權法保護。Dell™ 與 Dell 徽標是 Dell Inc. 在美國和/或其他司法管轄區的商標。本文提及的所有其他標誌與名稱皆屬於其個別公司的商標。

2016 - 02

修正版 A00

# 目錄

<b>1 概觀</b> .....	<b>9</b>
OpenManage Integration for VMware vCenter .....	9
主要特色.....	9
OpenManage Integration for VMware vCenter 如何協助 vCenter 管理.....	9
OpenManage Integration for VMware vCenter 功能.....	10
此版本新特色.....	10
<b>2 OpenManage Integration for VMware vCenter 組態</b> .....	<b>11</b>
安全性角色與權限.....	11
資料完整性.....	11
存取控制驗證、授權與角色.....	12
Dell 操作角色.....	12
Dell 基礎結構部署角色.....	12
瞭解權限.....	13
<b>3 設定或編輯 OpenManage Integration for VMware vCenter 的步驟</b> .....	<b>16</b>
OpenManage Integration for VMware vCenter 首頁.....	17
「組態精靈」歡迎頁面.....	17
建立新連線設定檔 [精靈].....	17
設定事件與警報 [精靈].....	18
設定 Proxy 伺服器 [精靈].....	19
排程庫存工作 [精靈].....	19
執行保固擷取工作 [精靈].....	20
設定部署憑證 [精靈].....	20
設定預設的韌體更新儲存庫 [精靈].....	20
啟用 OMSA 連結 [精靈].....	21
設定 NFS 共用.....	21
設定概觀.....	22
一般設定概觀.....	22
建立新的連線設定檔.....	23
設定事件與警報 .....	25
關於 Proxy 組態.....	26
執行清查工作.....	27
排程保固工作.....	27
檢視或編輯部署憑證.....	27
設定韌體儲存庫 .....	28
部署的伺服器安全性設定.....	28
關於主機、裸機和 iDRAC 規範問題.....	30

執行解決不相容 vSphere 主機精靈.....	30
執行解決不相容裸機主機精靈.....	31
iDRAC 授權規範.....	32
升級 OpenManage Integration for VMware vCenter.....	32
從試用版升級至完整產品版本.....	32
關於 OpenManage Integration for VMware vCenter 授權.....	33
<b>4 端對端硬體管理.....</b>	<b>34</b>
監視資料中心與主機系統.....	34
瞭解事件與警報.....	34
vSphere 用戶端主機概觀.....	36
重設 iDRAC.....	38
有關清查排程.....	39
修改清查工作排程.....	39
在 vCenter 中顯示單一主機系統的清查.....	40
清查與授權.....	41
檢視儲存清查.....	41
檢視主機電源監視.....	42
顯示整個資料中心硬體組態.....	42
管理連線設定檔.....	43
檢視或編輯現有的連線設定檔.....	43
刪除連線設定檔.....	45
測試連線設定檔.....	45
重新整理連線設定檔.....	45
瞭解 vSphere 用戶端主機檢視中的系統事件記錄.....	45
顯示 DELL 管理中心記錄.....	46
顯示個別主機的事件記錄.....	46
關於韌體更新.....	47
執行韌體更新精靈.....	47
更新舊版韌體.....	48
為叢集與資料中心執行更新韌體精靈.....	48
使用 vCenter 執行進階主機管理.....	50
設定實體伺服器前方指示燈.....	51
以伺服器為基礎的管理工具.....	51
保固擷取.....	51
<b>5 硬體管理.....</b>	<b>53</b>
佈建概觀.....	54
瞭解部署工作時間.....	54
部署順序中的伺服器狀態.....	54
下載自訂 Dell ISO 映像.....	55
瞭解如何設定硬體設定檔.....	55

建立新硬體設定檔.....	56
複製硬體設定檔.....	58
關於管理硬體設定檔.....	58
檢視或編輯硬體設定檔.....	59
複製硬體設定檔.....	59
重新命名硬體設定檔.....	59
刪除硬體設定檔.....	59
重新整理硬體設定檔.....	59
建立新 Hypervisor 設定檔.....	60
管理 Hypervisor 設定檔.....	60
VLAN Support.....	61
檢視或編輯 Hypervisor 設定檔.....	62
複製 Hypervisor 設定檔.....	62
重新命名 Hypervisor 設定檔.....	62
刪除 Hypervisor 設定檔.....	62
重新整理 Hypervisor 設定檔.....	62
建立新部署範本.....	62
管理部署範本.....	63
執行部署精靈.....	63
部署精靈步驟 1：選取伺服器.....	64
部署精靈步驟 2：部署範本.....	64
部署精靈步驟 3：全域設定.....	65
部署精靈步驟 4：伺服器識別.....	65
部署精靈步驟 5：連線設定檔.....	66
部署精靈步驟 6：排程工作.....	66
瞭解工作佇列.....	67
手動新增伺服器.....	68
移除裸機伺服器.....	68
<b>6 主控台管理.....</b>	<b>69</b>
Web 管理主控台.....	69
使用管理主控台.....	69
以具必要權限的非系統管理員使用者身分登錄 vCenter 伺服器.....	69
登錄 vCenter 伺服器.....	71
上傳 OpenManage Integration for VMware vCenter 授權至管理主控台.....	74
虛擬設備管理.....	74
重新啟動虛擬設備.....	75
更新儲存庫位置和虛擬設備.....	75
更新虛擬設備軟體.....	75
下載疑難排解配套.....	76
設定 HTTP Proxy.....	76
設定 NTP 伺服器.....	76

產生憑證簽章要求.....	76
設定全域警示.....	77
管理備份和還原.....	78
設定備份和還原.....	78
排程自動備份.....	78
執行立即備份.....	79
從備份還原資料庫.....	79
瞭解 vSphere 用戶端主控台 .....	79
組態網路設定.....	80
變更虛擬設備密碼.....	80
設定當地時區.....	80
重新啟動虛擬設備.....	81
將虛擬設備重設為原廠設定.....	81
重新整理主控台檢視.....	81
從主控台登出.....	81
唯讀使用者角色.....	81
將 OpenManage Integration 外掛程式從 3.0 版升級至最新版本.....	81
從 2.x 移轉到 3.1 的移轉路徑.....	82

## 7 故障排除..... 83

常見問題集 (FAQ).....	83
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.....	83
如果 vCenter 已閒置數小時，在按一下「OpenManage Integration」索引標籤和「管理中心」時，OMIVV 內容會被「！」圖示取代。我該怎麼做才能繼續作業階段？.....	83
在嘗試以嚴重程度類別篩選時，「Dell 管理中心」並未顯示所有相關記錄。我要如何檢視所有記錄？.....	83
我要如何將 OMIVV 外掛程式的狀態變更為「啟用」？.....	84
在為 VMware vCenter 執行 OpenManage Integration 還原後，如果 Dell 管理中心圖示並未顯示在 vSphere 用戶端，我該怎麼做？.....	84
應用裝置更新後，OMIVV 版本未從關於畫面更新.....	84
不支援使用 OpenManage Integration for VMware vCenter 更新搭載 13.5.2 版韌體的 Intel 網路卡。.....	84
在執行保固擷取工作時，保固工作狀態未列於「保固工作佇列」頁面.....	85
因為來自 DUP 的分段需求，使用 OpenManage Integration for VMware vCenter 將 Intel 網路卡由 14.5 或 15.0 更新至 16.x 將會失敗.....	85
嘗試用無效的 DUP 更新韌體時，vCenter 主控台的硬體更新工作狀態不是失敗，就是逾時數小時，不過 LC 內的工作狀態卻顯示「失敗」。為什麼會發生這種情況？.....	85
管理入口網站仍顯示無法聯繫的更新儲存庫位置。.....	85
為什麼如果應用裝置 IP 使用 DHCP 並覆寫 DNS 設定，應用裝置重新啟動後，DNS 組態設定會恢復原始設定.....	85
為什麼執行一對多韌體更新時，系統不會進入維護模式？.....	86
我的儲存庫有選取之第 11 代系統的配套，為什麼韌體更新卻顯示我沒有韌體更新的配套？.....	86

為什麼我的 ESXi 在搭載 PERC S300 開機控制器的伺服器部署失敗？	86
按一下韌體連結後，為什麼會顯示錯誤訊息？	86
OpenManage Integration for VMware vCenter 設定與支援哪一代 Dell 伺服器的 SNMP 設 陷？	87
OpenManage Integration for VMware vCenter 如何在連結模式支援三個以上的 vCenter？	87
OpenManage Integration for VMware vCenter 是否支援連結模式的 vCenter？	87
OpenManage Integration for VMware vCenter 有哪些必要的連接埠設定？	87
虛擬設備順利安裝及操作的最低需求是什麼？	89
成功套用硬體設定檔 (相同使用者在 iDRAC 使用者清單有變更的新憑證) 後，用於裸機探索 的使用者密碼為什麼沒有變更？	89
為什麼處理器版本在系統概觀頁面的處理器檢視「不適用」？	89
為什麼如果應用裝置 IP 使用 DHCP 並覆寫 DNS 設定，應用裝置重新啟動後，DNS 組態設 定會恢復原始設定？	89
為什麼 vCenter 主機與叢集頁面沒有列出我新 iDRAC 版本的詳細資料？	89
如何用 OMSA 測試事件設定，模擬溫度硬體故障？	89
我已經在 Dell 主機系統安裝 OMSA 代理程式，但還是出現未安裝 OMSA 的錯誤訊息。該怎 麼辦？	90
OpenManage Integration for VMware vCenter 啟用鎖定模式時是否支援 ESXi？	90
嘗試使用鎖定模式卻失敗。	90
嘗試用無效的 DUP 更新韌體時，vCenter 主控台的硬體更新工作狀態不是失敗，就是逾時數 小時，不過 LC 內的工作狀態卻顯示「失敗」。為什麼會發生這種情況？	90
UserVars.CIMoeMProviderEnable With ESXi 4.1 U1 應該使用什麼設定？	91
我用參考伺服器建立硬體設定檔，但是卻失敗了。該怎麼辦？	91
我正嘗試在刀鋒伺服器部署 ESXi，結果失敗了。該怎麼辦？	91
為什麼我的 Hypervisor 在 R210 II 機器部署失敗？	91
為什麼在部署精靈看到自動探索到的系統，但是卻沒有型號資訊？	91
NFS 共用以 ESXi ISO 設定成功，但是部署卻失敗，而且出現共用位置裝載錯誤。	91
我該如何強制移除虛擬設備？	91
在立即備份畫面輸入密碼時收到錯誤訊息	92
我的韌體更新失敗。該怎麼做？	92
我的 vCenter 登錄失敗。該怎麼做？	92
連線設定檔測試認證效能超慢或無回應。	92
OpenManage Integration for VMware vCenter 是否支援 VMware vCenter Server 應用裝 置？	92
OpenManage Integration for VMware vCenter 是否支援 vSphere Web 用戶端？	92
在管理主控台時，將應用裝置重設為原廠設定後，為什麼更新儲存庫路徑沒有設定為預設路 徑？	93
為什麼備份及還原 OpenManage Integration for VMware vCenter 後，警報設定沒有還原？	93
裸機部署問題	93
在新購買的系統啟用自動探索	93
與 Dell 公司聯絡	94
OpenManage Integration for VMware vCenter 相關資訊	94

<b>8 Dell PowerEdge 伺服器的虛擬化相關事件.....</b>	<b>95</b>
<b>附錄 A：瞭解自動探索.....</b>	<b>103</b>
自動探索事前準備作業.....	103
在 iDRAC 伺服器啟用或停用管理帳戶.....	104
為自動探索手動設定伺服器 (第 11 代 PowerEdge 伺服器).....	104
為自動探索手動設定 PowerEdge 第 12 代以後的伺服器.....	105

## 概觀

### OpenManage Integration for VMware vCenter

VMware vCenter 是 IT 管理員管理和監視 VMware vSphere ESXi 主機時使用的主要主控台。在標準虛擬化環境中，會用 VMware 警示和監視，提示管理員另外啟動主控台解決硬體問題。現今，若使用 OpenManage Integration for VMware vCenter，管理員有新功能可以管理和監視虛擬化環境中的 Dell 硬體，例如：

- 警示與環境監視
- 單一伺服器監視及報告
- 韌體更新
- 增強的部署選項

### 主要特色

Dell 客戶可以用 OpenManage Integration for VMware vCenter 執行下列工作：

<b>清查</b>	清單重要資產、執行組態工作，以及提供 Dell 平台的叢集與資料中心檢視。
<b>監視與警示</b>	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)。
<b>韌體更新</b>	將 Dell 硬體更新為最新版的 BIOS 和韌體。
<b>部署與佈建</b>	建立硬體設定檔、Hypervisor 設定檔，以及用 vCenter 在裸機 Dell PowerEdge 伺服器以遠端方式部署任兩個設定檔的組合，無須使用 PXE。
<b>服務資訊</b>	從 Dell 線上擷取保固資訊。

### OpenManage Integration for VMware vCenter 如何協助 vCenter 管理

OpenManage Integration for VMware vCenter 提供額外的虛擬化功能，輔助現有的 vCenter 管理功能：

- 壓縮工作及新增管理程序，例如韌體更新和裸機部署至 vCenter Server 管理主控台。
- 無須開機前執行環境 (PXE) 即可組織部署多個裸機伺服器。
- 提供額外情報 (清查、事件、警報) 診斷伺服器問題。
- 整合標準 vCenter 驗證、規則和權限。

# OpenManage Integration for VMware vCenter 功能

OpenManage Integration for VMware vCenter 的高階功能如下：

- 用標準 vCenter 事件與警報子系統監視 Dell 伺服器
- 執行進階硬體管理和組態
- 在裸機系統執行 VMware ESXi Hypervisor 的零接觸部署，無須使用 PXE
- 建立硬體與 VMware ESXi Hypervisor 設定檔
- 執行韌體更新
- 疑難排解基礎結構的問題
- 在資料中心和叢集檢視產生報告—匯出至 CSV 檔案
- 整合 OpenManage Integration for VMware vCenter 功能與標準 vCenter 角色和權限

## 此版本新特色

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

- 支援 OMSA 8.2
- 支援 vCenter 伺服器版本；v5.5 U3 和 v6.0 U1
- 支援 VMware ESXi 版本；v5.5 U3 和 v6.0 U1
- 支援具所需權限的非系統管理員使用者所登錄的 OMIVV 應用裝置
- 支援 C4130、R230、R330、T330 及 T130 平台
- 支援繁體中文
- 支援更新韌體的 64 位元 DUP 配套

# OpenManage Integration for VMware vCenter 組態

下列章節提供 OpenManage Integration for VMware vCenter 初始組態的逐步說明。下列章節還說明升級、解除安裝和安全性角色資訊。

## 安全性角色與權限

OpenManage Integration for VMware vCenter 以加密格式儲存使用者認證，不會提供任何用戶端應用程式的密碼，避免任何不當要求所可能導致的問題。備份資料庫以自訂的安全性短語完全加密，因此資料不會遭濫用。

根據預設，系統管理員群組中的使用者擁有所有權限。系統管理員可以使用 VMware vSphere 用戶端或 Web 用戶端中的 OpenManage Integration for VMware vCenter 所有功能。如果您想要具必要權限的使用者來管理產品，請建立具必要權限的角色，將角色指派至某使用者，並使用該使用者登錄 vCenter 伺服器，並包括兩個 Dell 角色。

## 資料完整性

OpenManage Integration for VMware vCenter 虛擬設備、管理主控台和 vCenter 之間的通訊是以 SSL/HTTPS 完成。OpenManage Integration for VMware vCenter 會產生 vCenter 與應用裝置之間信任通訊用的 SSL 憑證，還會在通訊與 OpenManage Integration for VMware vCenter 登錄之前，驗證與信任 vCenter 伺服器的憑證。OpenManage Integration for VMware vCenter 主控台索引標籤 (在 VMware vCenter) 使用安全性程序，避免金鑰在管理主控台來回傳送時的不當要求和後端服務。這類安全性會導致跨網站要求偽造失敗。

安全管理主控台工作階段有五分鐘閒置逾時，而且工作階段只在目前的瀏覽器視窗和/或索引標籤有效。如果使用者嘗試在新視窗或新索引標籤開啟工作階段，安全性錯誤隨即建立，要求有效的工作階段。這個動作還能避免使用者按下可能嘗試攻擊管理主控台工作階段的任何惡意 URL。

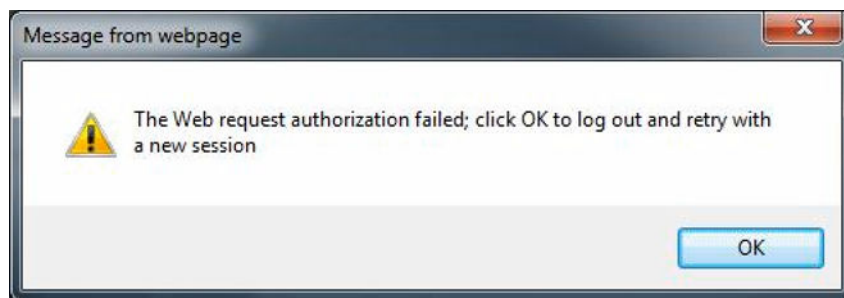


圖 1. 錯誤訊息

## 存取控制驗證、授權與角色

OpenManage Integration for VMware vCenter 使用 vSphere 用戶端目前的使用者工作階段和儲存的管理認證，讓虛擬設備執行 vCenter 作業。OpenManage Integration for VMware vCenter 使用 vCenter 伺服器的內建角色和權限模型，授權在虛擬設備和 vCenter 受管物件 (主機與叢集) 的使用者動作。

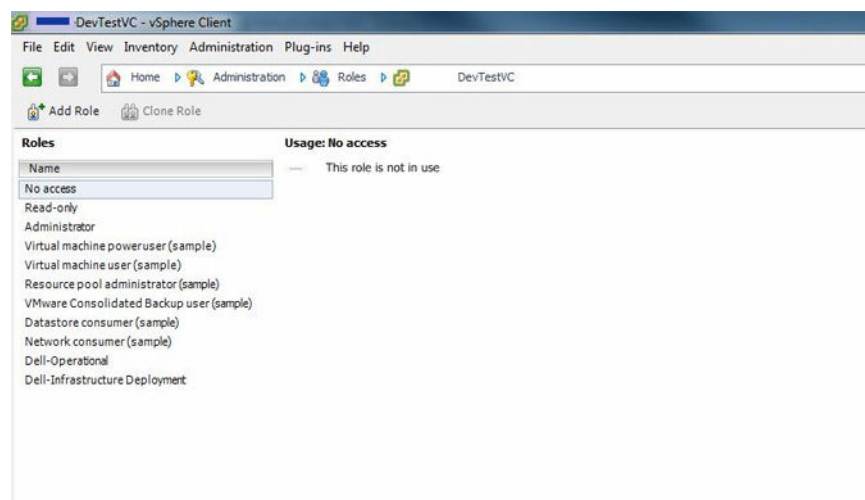


圖 2. vCenter vSphere 用戶端角色與權限

## Dell 操作角色

包含完成應用裝置和 vCenter 伺服器工作的權限/群組，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。

這個角色包含下列權限群組：

表 1. 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

這個角色包含尤其與 Hypervisor 部署功能相關的權限。

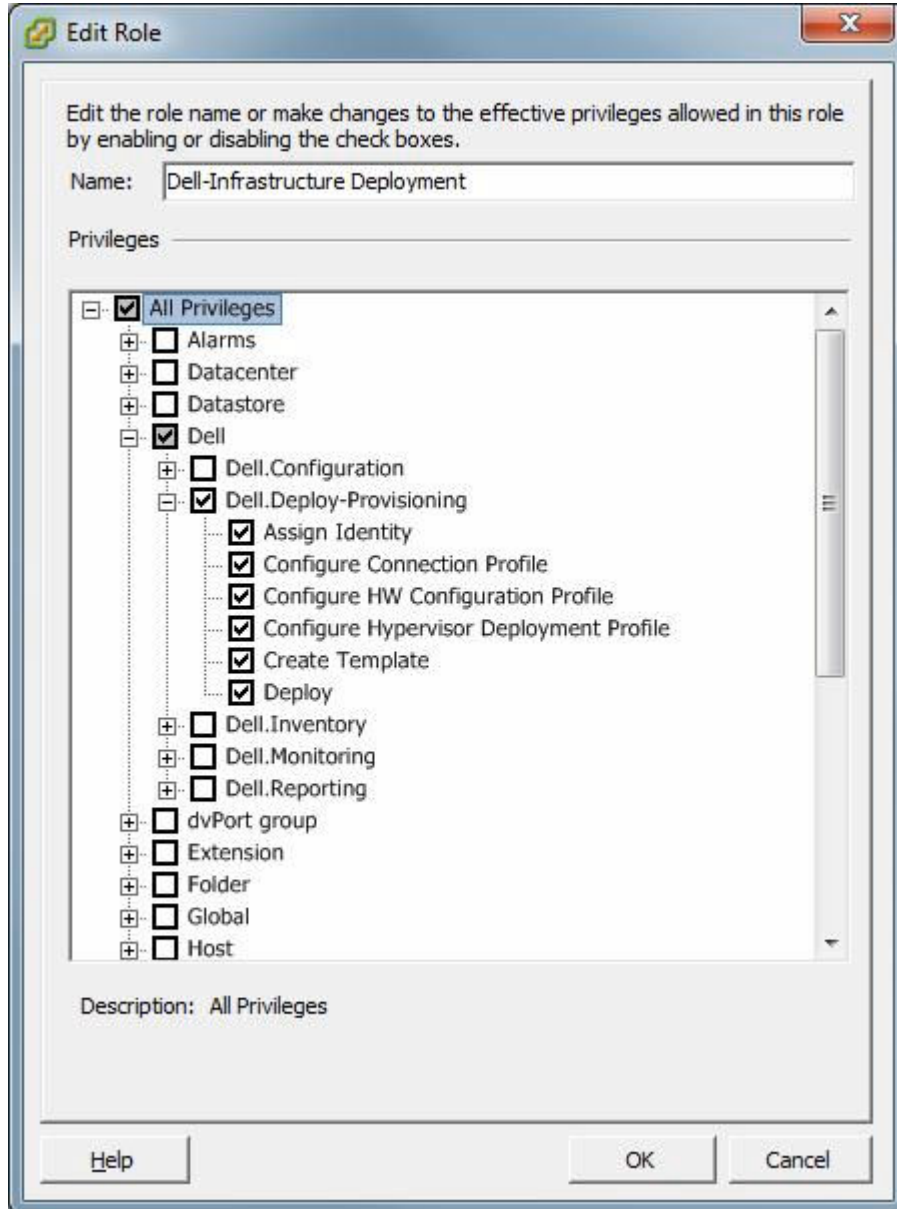


圖 3. Dell 基礎結構部署角色

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。

**Dell.Deploy 一佈建** 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

## 瞭解權限

OpenManage Integration for VMware vCenter 執行的每個動作都有關聯的權限。下列各節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 設陷及發佈事件
- 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
  - 設定暫置資料夾及使用暫置功能執行更新
  - 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

# 設定或編輯 OpenManage Integration for VMware vCenter 的步驟

完成 OpenManage Integration for VMware vCenter 的基本安裝後，您可繼續使用本節後段所述的下列其中一項方法來設定設備：

- 使用組態精靈的組態工作
- 使用設定選項的組態工作

除了精靈外，這兩種方法採用的使用者介面彼此相似，請按一下 *儲存以繼續*，或是在「設定」選項中按一下 *套用*。

## 使用組態精靈的組態工作

使用「組態精靈」設定 OpenManage Integration for VMware vCenter 時，請使用這些工作：

1. [組態精靈歡迎頁面](#)
2. [建立新的連線設定檔](#)
3. [設定事件與警報](#)
4. [設定 Proxy 伺服器](#)
5. [排程清查工作](#)
6. [執行保固擷取工作](#)
7. [設定部署憑證](#)
8. [設定預設韌體更新儲存庫](#)
9. [啟用 OMSA 連結](#)

## 使用設定選項的組態工作

使用這些工作設定或編輯 OpenManage Integration for VMware vCenter 組態工作：

- [建立新的連線設定檔](#)
- [設定事件與警報](#)
- [設定 Proxy 伺服器](#)
- [修改清查工作排程](#)
- [保固擷取](#)
- [檢視或編輯部署憑證](#)
- [設定韌體儲存庫和憑證](#)
- [啟用 OMSA 連結](#)

# OpenManage Integration for VMware vCenter 首頁

登入 OpenManage Integration for VMware vCenter 首頁時，在左窗格會顯示導覽按鈕，且在右窗格會顯示實用連結和資訊。此設計可提供您最常執行工作的重要連結。您可在左窗格導覽下方找到這些所有工作，或者亦可在「概覽」頁面找到這些工作以輕鬆使用。此頁面上提供的工作屬於下列類別：

- 主機和伺服器部署  
此區段提供有關主機和伺服器部署的詳細資訊。
- vSphere 主機和裸機伺服器規範  
此區段提供詳細資訊，並可讓您檢視關於非相容主機或裸機伺服器，或是執行精靈進行修正的詳細資訊。
- 清查排程  
此區段可讓您瞭解關於清查排程的詳細資訊。
- 保固資料擷取排程  
此區段可讓您瞭解詳細資訊，或是檢視 / 變更保固排程。
- 授權  
此區段可讓您瞭解關於授權的詳細資訊。使用連結移至授權工作。在主機連線授權中，您可即時檢視主機連線授權。此外，您可使用「立即購買」連結購買完整版本授權，以管理多部主機。僅在您使用展示授權時才會顯示「立即購買」連結。在「vCenter 連線授權」中，您可檢視 VMware vCenter 連線授權相關資訊。
- 事件與警報設定  
瞭解關於事件與警報設定，或是透過連結進行相關設定詳細資訊。


## 「組態精靈」歡迎頁面


安裝 OMV 後，必須進行設定。

1. 在 vSphere 用戶端中，從首頁頁面的**管理**標籤下方，按一下 **Dell 管理中心** 圖示。  
初次按一下 **Dell 管理中心** 圖示時，其會開啟**組態精靈**。您亦可在 **Dell 管理中心** → **設定** 頁面上存取此精靈。
2. 在**歡迎**標籤中檢閱步驟，然後按一下**下一步**。

## 建立新連線設定檔 [精靈]

連線設定檔會儲存虛擬設備與 Dell 伺服器進行通訊所用的憑證。每個 Dell 伺服器皆必須與由 OMIV 管理的連線設定檔產生關聯。您可以將多個伺服器指派至單一連線設定檔。建立「連線設定檔」與位於**設定**選項下方的「組態精靈」和「Dell 管理中心」之間相似。您可將 OMIV 設定為使用 Active Directory 憑證連線至 iDRAC 和主機。於使用 Active Directory 憑證與連線設定檔前，在 Active Directory 和 iDRAC 中必須具有 Active Directory 使用者帳戶，且必須設定主機使用以 Active Directory 為基礎的驗證。iDRAC 與主機可使用相同的 Active Directory 憑證，或者亦可為其設定個別的 Active Directory 憑證。使用者憑證必須具備管理權限。

 **註:** 若在使用第 12 版或更新版本 Dell PowerEdge 伺服器的主機上執行安裝，則無須安裝 OMSA 代理程式。若要在第 11 版伺服器上執行安裝，則在執行部署程序時會自動安裝 OMSA 代理程式。


 **註:** 建立「連線設定檔」時若新增的主機數量超過授權限制，則無法建立連線設定檔。

若要使用精靈建立新的連線設定檔，請執行下列步驟：

1. 從**連線設定檔**標籤中，按一下**建立新的**。
2. 在**設定檔名稱與說明**面板中，輸入設定檔名稱和選用說明以協助管理自訂連線設定檔，然後按一下**下一步**。
3. 在**關聯主機**區段中，選取要與「連線設定檔」產生關聯的主機，然後按一下**下一步**。
4. 檢視憑證與連線通訊協定的相關資訊，然後按一下**下一步**。
5. 在 **iDRAC** 面板中，輸入 iDRAC 憑證資訊。
  - a. 針對您想要使用 Active Directory 且已針對 Active Directory 設定和啟用的 iDRAC，勾選**使用 Active Directory** 核取方塊；否則請設定 iDRAC 本機憑證。輸入**使用者名稱**、**密碼**和**確認密碼**。使用者名稱最多可包含 16 個字元 (含空格)。密碼必須符合且僅使用 ASCII 可列印字元。
  - b. 針對**憑證檢查**，選取**啟用**以下載和儲存 iDRAC 憑證，並在執行所有後續連線時進行憑證驗證，或是選取**停用**不執行任何檢查且不儲存憑證。
6. 按一下 **下一步**。
7. 在**主機**面板中，執行以下動作：
  - a. 您必須勾選**使用 Active Directory** 核取方塊以啟用 Active Directory 憑證。輸入「使用者名稱」、「密碼」和「確認密碼」。
  - b. 若您未選取**使用 Active Directory**，請針對**根**使用者輸入**密碼**和**確認密碼**。這些密碼必須相符。
  - c. 針對**憑證檢查**，選取**啟用**以下載和儲存 OMSA/ESXI 憑證，並在執行所有後續連線時進行憑證驗證，或是選取**停用**不執行任何檢查且不儲存憑證。
8. 按一下 **Next (下一步)**。
9. **測試連線**視窗可在選定伺服器上測試輸入的 iDRAC 和主機根憑證。「測試連線」為選用，但建議您使用此功能。
  - 若要開始測試，請選取主機然後按一下**已選取測試**。此時會停用其他選項。
  - 若要在完成前中止所有測試，請按一下**中止所有測試**。
10. 若要完成設定檔，按一下**儲存**。
11. 若要繼續設定「事件」與「警報」，請按一下**儲存以繼續**。


## 設定事件與警報 [精靈]


使用「組態精靈」或「Dell 管理中心」、「事件與警報」的「設定」選項，以設定事件和警報。若要從伺服器接收事件，OMIVV 會設為設陷目的地。針對第 12 版主機和更新版本主機，會在 iDRAC 中設定 SNMP 設陷目的地。針對第 12 版之前的主機，則是在 OMSA 中設定設陷產生。

 **註:** OMIVV 支援適用於第 12 代主機及更新版本主機的 SNMP v1 和 v2 警示。如果是第 12 代之前的主機，則 OMIVV 僅支援 SNMP v1 警示。


若要設定事件與警報，請執行下列步驟：

1. 在**事件發佈層級**下方的**組態精靈**中，選取下列其中一個項目：
  - 請勿發佈任何事件 — 封鎖硬體事件。
  - 發佈所有事件 — 發佈所有的硬體事件。
  - 僅發佈嚴重和警告事件 — 僅發佈嚴重或警告層級硬體事件。
  - 僅發佈虛擬化方面的嚴重和警告事件 — 僅發佈虛擬化相關嚴重和警告事件；這是預設的事件發佈層級。
2. 若要啟用所有的硬體警報，請勾選**啟用 Dell 主機的警報**核取方塊。

 **註:** 已啟用警報的 Dell 主機，會以進入維護模式的方式回應嚴重事件。
3. 在顯示的對話方塊中，按一下**繼續**接受這項變更，或按一下**取消**。

 **註:** 僅在選取**啟用 Dell 主機的警報**時才會顯示此步驟。

- 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**。  
變更生效可能需時一分鐘。
- 若要繼續執行精靈，請按一下**儲存以繼續**。

 **註:** 還原 OMIW 設備的備份並不會還原所有的「警報」設定。不過在 OMIW GUI 中，**警報與事件**欄位會顯示已還原的設定。若要解決此問題，請在**管理** → **設定**標籤的 OMIW GUI 中，手動變更「事件與警報」設定。

## 設定 Proxy 伺服器 [精靈]


在「組態精靈」中設定 Proxy 伺服器，或是稍後再使用「Dell 管理中心」、**設定** → **Proxy** 頁面進行設定。

設定 Proxy 伺服器：

- 在**設定 HTTP Proxy** 中，請執行下列其中一項：
  - 若不想使用 Proxy 伺服器，請按一下**儲存以繼續**。
  - 若要使用 Proxy 伺服器，請在**設定**下方輸入 **Proxy 伺服器位址**。
- 輸入 **Proxy 連接埠號碼**。
- 必要時，選取**必要認證**核取方塊。
- 如果選取**必要認證**，請執行以下操作：
  - 在 **Proxy 使用者名稱**文字方塊中，編輯 Proxy 使用者名稱。
  - 在 **Proxy 密碼**文字方塊中，輸入 Proxy 密碼。
  - 在**確認密碼**文字方塊中，再一次輸入 Proxy 密碼。
- 在 **Proxy** 下方選取**使用 Proxy** 核取方塊。
- 若要儲存這些選項並繼續，請按一下**儲存以繼續**。

## 排程庫存工作 [精靈]

「組態精靈」或 **Dell 管理中心** → **設定**選項的庫存排程組態皆彼此近似。唯一的差異在於，若您想要立即執行庫存則精靈會提供選項供您選擇。

 **註:** 若要確定 OMIW 會繼續顯示更新資訊，建議您定期排程庫存工作，庫存工作耗用最小資源，且不會影響主機運作效能。


排程庫存工作：

- 在**組態精靈**的**庫存排程**視窗中，執行下列其中一項：
  - 若要執行庫存排程，請按一下**在選定日期**。
  - 若不想執行庫存排程，請選取**不要在 Dell 主機上執行庫存**。
- 若您選取**在選定日期**，請執行下列動作：
  - 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。
  - 在文字方塊中，以 HH:MM 格式輸入時間。  
您輸入的時間為當地時間，因此若您想要在虛擬設備時區執行庫存，請計算您本機與虛擬設備時區彼此間的時差，然後再輸入正確的時間。
- 若要套用變更並繼續，請按一下**儲存以繼續**。

## 執行保固擷取工作 [精靈]


精靈與 Dell 管理中心 → 設定選項間的保固擷取工作組態彼此相似。此外，您可透過「工作佇列」立即執行「保固擷取工作」。

執行保固擷取工作：

1. 在**組態精靈**的**保固排程**視窗中，執行下列其中一項：
  - 若要執行保固排程，請按一下**在選定日期**。
  - 若不想執行保固排程，請選取**不要擷取保固資料**。
2. 若您選取**在選定日期**，請執行下列動作：
  - a. 針對想要執行保固工作的當週內任何一天，選取旁邊的文字方塊。
  - b. 在文字方塊中，以 HH:MM 格式輸入時間。  
您輸入的時間為當地時間，因此若您想要在虛擬設備時區執行庫存，請計算您本機與虛擬設備時區彼此間的時差，然後再輸入正確的時間。
3. 若要套用變更並繼續，請按一下**儲存以繼續**。  
 **註:** OMIVV 會連線至網際網路擷取您主機的保固資訊。根據您的網路設定，您可能必須設定保固工作的 Proxy 以順利執行。

## 設定部署憑證 [精靈]

系統會使用部署憑證，以與使用「自動探索」所探索的裸機系統進行安全通訊。為了與 iDRAC 進行安全通訊，OMIVV 在從初始探索至部署程序結束的過程當中會使用部署憑證。部署完成後，即會將憑證變更為部署時關聯之連線設定檔中的憑證。若變更部署憑證，則在變更時新增的所有已探索系統皆會使用新憑證進行佈建；不過，在變更前位於已探索伺服器的憑證並不會受到影響。

 **註:** OMIVV 會以佈建伺服器運作。系統會使用「部署」憑證與在「自動探索」程序中使用外掛程式做為佈建伺服器的 iDRAC 進行通訊。

設定部署憑證：

1. 您可在**部署憑證**視窗中，檢視或變更憑證。
2. 若要變更這些憑證，請在**適用於裸機伺服器部署的憑證**下方執行下列動作：
  - a. 在**使用者名稱**文字方塊中，編輯使用者名稱。
  - b. 在**密碼**文字方塊中編輯密碼。
  - c. 在**確認密碼**文字方塊中確認密碼。
3. 若要儲存指定憑證並繼續執行「組態精靈」，請按一下**儲存以繼續**。


## 設定預設的韌體更新儲存庫 [精靈]

韌體儲存庫設定中，包含更新部署伺服器用的韌體目錄位置。您可以一開始就在精靈設定韌體儲存庫，也可以稍後從 Dell 管理中心設定選項設定。此外，稍後從 OpenManage Integration 索引標籤即可執行韌體更新。

若要設定預設的韌體更新儲存庫：

1. 在**組態精靈**的**韌體儲存庫**頁面，若要為韌體更新選擇預設儲存庫，請選取下列其中一個選項：
  - Dell 線上

隨附暫置資料夾的預設韌體儲存庫 (ftp.dell.com)。OMIVV 下載選取的韌體更新後，會儲存在暫置資料夾中，然後在必要時套用。

 **註:** OMIVV 會連線網際網路，取得您主機適用的目錄和韌體套件。視網路設定而定，您可能必須設定 proxy，從 Dell 線上執行韌體更新工作才會成功。

- 本機/共用儲存庫


這些是以 Dell Repository Manager 應用程式所建立。這個本機儲存庫必須屬於網路共用。OMIVV 同時支援 NFS 和 CIFS 共用。

2. 如果選取**本機/共用儲存庫**，請執行以下操作：

- a. 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

- b. 如果使用的是 CIFS 共用，請輸入**使用者名稱**、**密碼**和**確認密碼**；密碼必須相符。輸入 CIFS 共用，這些欄位才處於作用中狀態。

 **註:** 共用網路資料夾的使用者名稱/密碼不支援使用 @ 這個字元。

- c. 若要驗證輸入的內容，請按一下**開始測試**。

3. 若要儲存此選項並繼續**設定精靈**，請按一下**儲存並繼續**。

## 啟用 OMSA 連結 [精靈]

若要在 OMIVV 虛擬設備中啟動 OMSA，則必須安裝和設定「OMSA 網頁伺服器」。如需關於「網頁伺服器」安裝與設定方式的說明，請參閱 *Dell OpenManage Server 管理員安裝手冊*。

 **註:** 僅第 12 版之前的 Dell 伺服器需要使用 OMSA。

您可使用 OMSA 執行以下工作：

- 管理 vCenter 元素 (詳細感應器 / 元件層級健全狀況資訊)。
- 清除命令日誌和系統事件日誌(SEL)。
- 取得 NIC 統計資料。
- 確定 OMIVV 從選定主機擷取事件。

1. 在**組態精靈**的 **OpenManage 伺服器管理**頁面上，使用 **OMSA 網頁伺服器 URL** 文字方塊輸入 OMSA URL。您必須包含完整的 URL (含 HTTPS)。
2. 若要儲存此 URL 並結束「組態精靈」，請按一下**結束**。

## 設定 NFS 共用

若要使用 NFS 共用搭配 OMIVV 執行備份和還原操作、韌體更新以及做為預備資料夾使用，您必須完成特定的組態項目。CIFS 共用不需要進行額外組態。

設定 NFS 共用：

1. 在主控 NFS 共用的 Linux 或 Unix OS 機器上，編輯 **/etc/exports** 新增以下內容：**/share/path <設備 IP> (rw) \*(ro)**。

這可讓虛擬設備具有共用的完整讀取與寫入權限，並限制其他所有使用者僅具唯讀權限。

2. 啟動 NFS 服務：

```
service portmap start service nfs start service nfslock status
```



**註：**根據使用的 Linux 發佈版本而定，以上步驟可能有所差異。

3. 若有任何執行中的服務：

```
exportfs -ra
```

## 設定概觀

OpenManage Integration for VMware vCenter 設定區段：

- 列出 OpenManage Integration for VMware vCenter 的組態設定。
- 啟動初始組態精靈，逐步引導您完成管理與部署 VMware vCenter 中的伺服器所需的 OpenManage Integration for VMware vCenter 功能。
- 啟動 OpenManage Integration for VMware vCenter 管理主控台，讓您執行 vCenter 登錄、虛擬設備管理、警示管理以及備份/還原 OpenManage Integration for VMware vCenter 資料庫。

### 一般設定概觀

一般設定用於：

- 定義 OpenManage Server Administrator (OMSA) URL。
- 啟用或停用保固到期通知。

您可以執行下列工作：

您可以執行下列工作：

- [一般](#)：設定 vCenter 中 Dell 主機索引標籤上顯示的 OMSA URL。您也可以啟用或停用保固到期通知。
- [事件與警報](#)：啟用或停用所有硬體警報（目前的警示狀態顯示於警報索引標籤）。還可設定傳入的事件和警示篩選。
- [HTTP 代理](#)：在與網際網路網站通訊時，啟用或停用使用 HTTP Proxy。
- [清查排程](#)：設定 vCenter 主機清查排程。
- [保固排程](#)：設定 Dell 主機從 Dell 線上擷取保固資訊的排程。
- [部署憑證](#)：設定自動探索和裸機伺服器部署期間，與 Dell 伺服器通訊所使用的憑證。
- [韌體儲存庫](#)：讓您編輯儲存韌體儲存庫的位置。
- [安全性](#)：提供伺服器允許清單，限制部署的伺服器。

Dell PowerEdge 第 11 代伺服器必須有 OMSA 代理程式，下列作業才能進行：

- 詳細的主機清查。
- 從主機接收事件。
- 擷取元件層級健全狀況資訊。
- 清除命令記錄與系統事件記錄 (SEL)



**註：**僅有第 12 代 Dell PowerEdge 伺服器之前的 Dell 伺服器需使用 OMSA。

保固到期通知可用於：


- 監視保固到期日。
- 設定保固剩餘天數下限閾值，超過就會產生警告或嚴重警示。警示會以圖示方式出現在主機 OpenManage Integration 索引標籤。

相關工作：

- [啟用在組態精靈之外的 OMSA 連結](#)
- [啟用或停用伺服器保固到期通知](#)


### 啟用在組態精靈之外的 OMSA 連結

若要在 OpenManage Integration for VMware vCenter 虛擬設備中啟動 OpenManage Server Administrator (OMSA)，則必須安裝和設定「OMSA 網頁伺服器」。如需關於使用的 OMSA 版本之「網頁伺服器」安裝與設定方式的說明，請參閱 *Dell OpenManage Server 管理員安裝手冊*。

 **註:** 僅有第 12 代 Dell PowerEdge 伺服器之前的 Dell 伺服器需使用 OMSA。

啟用 OMSA 連結：

1. 在「OMSA 啟動器」下方的 **Dell 管理中心**、**設定** → **一般**中，按一下**編輯**。
2. 使用 **OMSA 網頁伺服器 URL** 文字方塊輸入 OMSA 的 URL。您必須包含具 HTTPS 和連接埠號碼 1311 的完整 URL。
3. 若要儲存此 URL，請按一下**套用**。

 **註:** 如需設定 OMSA 設陷目的地的相關資訊，請參閱「[設定 OMSA 設陷目的地](#)」。

### 啟用或停用伺服器保固到期通知

您在控制保固設定時，系統會從「Dell 線上」擷取伺服器保固資訊。使用此頁面以針對主機和叢集啟用或停用伺服器保顧到期通知。在「設定」、「一般頁面」的「Dell 管理中心」中，設定或編輯此功能。

啟用或停用伺服器保固到期通知：

1. 在 **Dell 管理中心**中，按一下**設定** → **一般**。
2. 若要在**一般**頁面中啟用通知，請按一下右側的「**編輯**」按鈕。
3. 選取**啟用保固狀態通知**核取方塊。
4. 若要設定**天數下限閾值警示**，請執行下列動作：
  - a. 若要設定警告，請在**警告**下拉式清單中，選取伺服器保固狀態相關警告的天數。
  - b. 若要設定重大保固狀態，請在**重大**下拉式清單中，設定重大伺服器保固狀態警告的天數。
5. 若要**套用**變更，請按一下**套用**。

### 建立新的連線設定檔


連線設定檔儲存了虛擬設備用來與 Dell 伺服器通訊的憑證。每個 Dell 伺服器必須只有一個關聯的連線設定檔，才能受 OpenManage Integration for VMware vCenter 管理。您可以指派多個伺服器給單一連線設定檔。組態精靈與 Dell 管理中心、連線設定檔之間建立連線設定檔的方式差不多。您可以在第一次存取 Dell 管理主控台時執行組態精靈，也可以稍後再在連線設定檔視窗執行。

 **註:** 如需更多授權的相關資訊，請參閱關於 OpenManage Integration for VMware vCenter 授權。如果新增的主機數量超過授權限制，則無法建立連線設定檔。


若要建立新的連線設定檔：

1. 在 **OpenManage Integration for VMware vCenter** 的左窗格中按一下**連線設定檔**。
2. 按一下**新建立連結**。

3. 在**設定檔名稱和說明**頁面，輸入**連線設定檔名稱**和選填的**連線設定檔說明**，協助管理自訂的連線設定檔。
4. 在**關聯主機**頁面，選取連線設定檔的主機，然後按一下**下一步**。
5. 在**憑證**頁面中，閱讀該資訊，然後按一下**下一步**。
6. 在 iDRAC 頁面的憑證下，請執行下列其中一項動作：


 **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。

- 若為要使用 Active Directory，而且已經針對 Active Directory 完成設定及啟用的 iDRAC，請選取**使用 Active Directory** 核取方塊，否則請略過，直接設定 iDRAC 憑證。
  - 在 **Active Directory 使用者名稱** 文字方塊中輸入使用者名稱。以下列其中一種格式輸入使用者名稱：網域\使用者名稱、網域/使用者名稱或 username@domain。使用者名稱限制為 256 個字元。如需使用者名稱限制，請參閱 Microsoft Active Directory 說明文件。
  - 在 **Active Directory 密碼** 文字方塊輸入密碼。密碼限制為 127 個字元。
  - 在 **確認密碼** 文字方塊中，再次輸入密碼。
  - 在憑證檢查下拉式清單中，選擇下列之一：
    - \* 若要在所有未來連線下載及儲存 iDRAC 憑證並加以驗證，請選取**啟用**。
    - \* 若不執行任何檢查且不儲存憑證，請選取**停用**。
- 若不用 Active Directory 設定 iDRAC 憑證，請執行下列步驟：
  - 在**使用者名稱**文字方塊輸入使用者名稱。使用者名稱限制為 16 個字元。有關您 iDRAC 版本使用者名稱限制的資訊，請參閱 iDRAC 文件。

 **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**文字方塊輸入密碼。密碼限制為 20 個字元。
  - 在**確認密碼**文字方塊中，再次輸入密碼。
  - 在憑證檢查下拉式清單中，選擇下列之一：
    - \* 若要在所有未來連線下載及儲存 iDRAC 憑證並加以驗證，請選取**啟用**。
    - \* 若不執行任何檢查且不儲存 iDRAC 憑證，請選取**停用**。
7. 按一下**下一步**。
  8. 在主機憑證頁面的憑證下，請執行下列其中一項動作：
    - 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，否則請略過，直接設定主機憑證。
      - 在 **Active Directory 使用者名稱** 文字方塊中輸入使用者名稱。以下列其中一種格式輸入使用者名稱：網域\使用者名稱、網域/使用者名稱或 username@domain。使用者名稱限制為 256 個字元。如需使用者名稱限制，請參閱 Microsoft Active Directory 說明文件。
      - 在 **Active Directory 密碼** 文字方塊輸入密碼。密碼限制為 127 個字元。
      - 在 **確認密碼** 文字方塊中，再次輸入密碼。
      - 在憑證檢查下拉式清單中，選擇下列之一：
        - \* 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**。

- \* 若不執行任何檢查且不儲存主機憑證，請選取**停用**。
- 若不用 Active Directory 設定主機憑證，請執行下列步驟：
  - 在**密碼**文字方塊輸入根使用者的密碼。密碼限制為 127 個字元。
  - 在**確認密碼**文字方塊中，再次輸入密碼。
  - 在憑證檢查下拉式清單中，選擇下列之一：
    - \* 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**。
    - \* 若不執行任何檢查且不儲存主機憑證，請選取**停用**。
- 9. 按一下 **Next (下一步)**。
- 10. **測試選取項目**連結，用於為所選取伺服器驗證提供的 iDRAC 和主機憑證。
  - 若要開始測試，選取主機，然後按一下**測試選取項目**。其他選項皆為非使用中狀態。
  - 若要中止所有執行中的連線測試，請按一下**中止測試**。

 **註:** 若為不具備 iDRAC Express 或 iDRAC Enterprise 的伺服器，iDRAC 測試連線會導致此系統不適用的狀態。
- 11. 若要完成設定檔，按一下**儲存**。  
若要管理連線設定檔，請參閱[管理連線設定檔](#)。

## 設定事件與警報


Dell 管理中心事件與警報頁面會啟用或停用所有硬體警報。vCenter 警報索引標籤會顯示目前的警示狀態。嚴重事件表示資料實際或即將遺失或系統實際或即將故障。警告事件未必重大，但可能表示日後會有問題。用 VMware 警報管理員也可啟用事件與警報。事件會顯示在主機與叢集檢視的 vCenter 工作與事件索引標籤。

 **註:** 在比 Dell PowerEdge 第 12 代伺服器舊的主機上，此功能規定在 OMSA 將虛擬設備設定為設陷目的地，才能在 vCenter 顯示主機事件。如需 OMSA 相關資訊，請參閱[設定 OMSA 陷阱目的地](#)。

用 Dell 管理中心事件與警報的設定選項，即可設定事件與警報。

若要設定事件和警報：

1. 在 **Dell 管理中心設定** → **事件與警報**，按一下**編輯**。
2. 在**事件發佈層級**中，選取下列其中一個選項：
  - 請勿發佈任何事件 - 封鎖硬體事件。
  - 發佈所有事件 - 發佈所有硬體事件。
  - 僅發佈嚴重和警告事件 - 僅發佈嚴重或警告層級硬體事件。
  - 僅發佈虛擬化方面的嚴重和警告事件 - 僅發佈虛擬化相關嚴重和警告事件；這是預設的事件發佈層級。
3. 若要啟用所有硬體警告和事件，選取**啟用 Dell 主機的警報**核取方塊。
 

 **註:** 已啟用警報的 Dell 主機，會以進入維護模式的方式回應嚴重事件。
4. 在顯示的對話方塊中，按一下**繼續**接受這項變更，或是按一下**取消**。
5. 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**。  
變更生效可能需要一分鐘。
6. 若要儲存，按一下**儲存**。

## 關於 Proxy 組態

Proxy 設定會定義從網路 (包括從「Dell 線上」) 擷取資訊所用的 HTTP Proxy 和任何必要憑證，例如：

- 啟用或停用 Proxy 伺服器
- 輸入需要的 Proxy 伺服器和連接埠號碼
- 定義任何必要認證 - 使用者名稱和密碼

相關工作：

- [設定 Proxy 伺服器](#)
- [使用 HTTP Proxy 擷取網路資料](#)
- [使用管理主控台設定 HTTP Proxy](#)

## 設定 Proxy 伺服器

取決於您的網路設定，OMIVV 可能必須使用 Proxy 資訊以連線至網際網路。若適用，則系統會使用 Proxy 設定執行下列工作：

- 擷取主機的保固資訊
- 從「Dell 線上」擷取韌體目錄和適用的韌體元件
- 執行設備升級時連線至「Dell 線上」。

在「組態精靈」中設定 Proxy 伺服器，或是稍後再使用「設定」選項、HTTP Proxy 進行設定。

 **註：** Proxy 密碼不可超過 31 個字元。

在 OMIVV 中設定 Proxy 詳細資料：

1. 在 **Dell 管理中心**，選取**設定** → **HTTP Proxy**，然後再按一下**編輯**。
2. 輸入 **Proxy 連接埠號碼**。
3. 視需要選取**需要憑證**核取方塊。
4. 若您選取**需要憑證**，請執行下列動作：
  - a. 在 **Proxy 使用者名稱**文字方塊中，輸入 Proxy 使用者名稱。
  - b. 在 **Proxy 密碼**文字方塊中，輸入 Proxy 密碼。
  - c. 在 **確認密碼**文字方塊中，重新輸入您剛輸入的 Proxy 密碼。
5. 在 **Proxy** 下方，選取**使用 Proxy**核取方塊。
6. 若要儲存這些選項，請按一下 **Apply (套用)**。

## 使用 HTTP Proxy 擷取網路資料


使用 HTTP Proxy 擷取網路資料：

1. 在 **Dell 管理中心**，選取**設定** → **HTTP Proxy**，然後再按一下**編輯**。
2. 選取**使用 Proxy**核取方塊。
3. 按一下 **Apply (套用)**。
4. 若要驗證設定，請按一下**測試連線能力**。

## 執行清查工作

執行清查工作：

1. **組態精靈**完成後，系統會針對新增至「連線設定檔」的所有主機自動觸發「清查」。若要依需求執行後續清查，請按一下**工作佇列** → **清查** → **立即執行**以執行清查工作。
2. 若要查看清查工作的狀態，請按一下**重新整理**。
3. 瀏覽至**主機與叢集**檢視，按一下任一 **Dell 主機**，然後再按一下 **OpenManage 整合**索引標籤。應會提供以下資訊：
  - 概觀頁面
  - 系統事件記錄
  - 硬體清單
  - 存放時
  - 韌體 (Firmware)
  - 電源監控

 **註：**超過授權限制的主機清單工作會略過，並標示為故障。

在「OpenManage 整合」索引標籤中執行下列主機命令：


- 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

## 排程保固工作

您可隨時從 **Dell 管理中心** → **設定** → **保固排程**頁面，執行「保固」工作排程。系統現已停用**保固擷取**頁面。您可從**工作佇列** → **保固歷程記錄**頁面，立即執行「保固擷取」工作。

排程保固擷取工作：

1. 在 **Dell 管理中心**，選取**設定** → **保固排程**。
2. 在**保固排程**視窗中，按一下**編輯**。
3. 若要設定排程，請執行下列其中一項動作：
  - a. 若要執行保固排程，請按一下**在選定日期**。
  - b. 若不想執行保固排程，請選取**不要擷取保固資料**。
4. 若您選取**在選定日期**，請執行下列動作：
  - a. 針對想要執行保固工作的當週內任何一天，選取旁邊的核取方塊。
  - b. 在文字方塊中，以小時:分鐘格式輸入時間。  
您輸入的時間為所在當地時間。您必須計算時差以在正確的時間執行保固工作。
5. 若要立即執行保固工作，請瀏覽至**工作佇列** → **保固歷程記錄**，然後再按一下**立即執行**。

 **註：**OMIVV 會連線至網際網路擷取您主機的保固資訊。根據您的網路設定，您可能必須設定保固工作的 Proxy 以順利執行。

## 檢視或編輯部署憑證

您可在「Dell 管理中心」中編輯部署憑證。部署憑證會用於安全地與自動探索的 Dell 裸機伺服器進行通訊，直至完成作業系統部署為止。一旦部署完成並成功部署作業系統後，即會設定在相關連線設定檔中提供的

iDRAC 憑證。若變更部署憑證，則在憑證變更後探索的裸機伺服器會使用新憑證進行通訊：此變更不會影響變更憑證前所探索伺服器上的憑證。使用者名稱應不超過 16 個字元 (僅限 ASCII 可列印字元)。密碼應不超過 20 個字元 (僅限 ASCII 可列印字元)。

檢視或編輯部署憑證：

1. 在 **Dell 管理中心** → **設定** → **部署憑證** 中，按一下 **編輯**。
2. 在 **憑證** 下方的 **適用於裸機伺服器部署的憑證** 中，執行下列動作：
  - 在 **使用者名稱** 文字方塊中，輸入使用者名稱。  
使用者名稱應不超過 16 個字元 (僅限 ASCII 可列印字元)。
  - 在 **密碼** 文字方塊中，輸入密碼。  
密碼應不超過 20 個字元 (僅限 ASCII 可列印字元)。
  - 在 **確認密碼** 文字方塊中，再次輸入密碼。  
密碼必須相符
3. 按一下 **Apply** (套用)。


## 設定韌體儲存庫

若要設定韌體儲存庫與憑證：

1. 在 **OpenManage Integration for VMware vCenter** 選取 **設定** → **韌體儲存庫**，然後按一下 **編輯**。
2. 在 **韌體儲存庫** 頁面，請選取下列其中一個選項，選擇預設的韌體更新儲存庫：
  - **Dell 線上**  
這個選項使用 Dell 線上 (ftp.dell.com) 當預設韌體儲存庫，隨附必要的暫置資料夾。OpenManage Integration for VMware vCenter 下載選取的韌體更新後，會儲存在暫置資料夾中，然後在必要時套用。
  - **共用網路資料夾**  
使用 Lifecycle Controller 的主機，能夠從可存取網路共用資料夾所託管的自訂儲存庫更新。若要建立自訂儲存庫，Dell 建議，用 Dell Repository Manager 建立後，儲存在主機和 OpenManage Integration 都能存取的共用位置。請在下方輸入儲存庫目錄檔案的位置。
3. 如果選取 **共用網路資料夾**，請在 **目錄檔案位置** 欄位輸入完整目錄檔案
4. 按一下 **開始測試**。
5. 按一下 **Apply** (套用)。

## 部署的伺服器安全性設定

用允許清單可限制部署伺服器集合。如果是允許清單中的伺服器，就會在自動探索和信號交換程序提供認證給這部伺服器，並顯示於部署用伺服器清單。手動新增伺服器服務標籤、刪除服務標籤，或從 CSV 檔案匯入服務編號清單，即可維護允許清單。

 **註:** 用 CSV 分隔檔案匯入伺服器。檔案內分行處理多重記錄，每筆記錄有一或多個服務標籤，以逗號分隔。

若要設定及管理允許清單，請從下列選項選擇：

- [啟用伺服器允許清單](#)
- [新增伺服器至允許清單](#)
- [從允許清單刪除伺服器](#)

## 啟用可部署伺服器允許清單

如需可部署伺服器的安全性設定相關資訊，請參閱[部署的伺服器安全性設定](#)。

若要啟用伺服器允許清單：

1. 在左窗格的 **Dell 管理中心**，選取**設定**。
2. 在右窗格選取**安全性**。
3. 在**安全性**視窗按一下**編輯**。
4. 若要使用允許清單限制伺服器部署，請選取**強制執行伺服器允許清單**核取方塊。
5. 按一下**套用**，伺服器允許設定隨即變更為「啟用」。

## 將可部署的伺服器新增至白名單

如需可部署伺服器安全性設定的相關資訊，請參閱「[針對部署的伺服器安全性設定](#)」。若採強制執行，則「伺服器白名單」中的 Dell 伺服器僅供使用 OpenManage Integration for VMware vCenter 進行部署。您可以將可部署的伺服器手動新增至白名單，或是使用清單匯入。

將可部署的伺服器新增至白名單：

1. 在左窗格的 **Dell 管理中心**中，選取**設定** → **安全性**。
2. 在**伺服器白名單**視窗中，按一下**編輯**，然後執行下列其中一項步驟：
  - 若要將伺服器手動新增至白名單，請按一下**新增伺服器**。
    - 在**新增服務標籤**對話方塊中，輸入服務標籤。
    - 若要新增標籤，請按一下**繼續**。
  - 若要匯入服務標籤清單，請按一下**匯入白名單**。
    - 若顯示**選取要上傳的檔案**對話方塊，請瀏覽至 CSV 檔案，然後按一下**開啟**。  
針對範例白名單：

ASDFG12

SDCNRD0

TESCVD3

AS243AS、ASWERF3、FGVCSD9

- 若顯示**在您的檔案中找到這些服務標籤**對話方塊，請按一下**套用**。

隨即會在「服務標籤」清單中顯示服務標籤。

## 從白名單刪除可部署的伺服器

如需可部署伺服器安全性設定的相關資訊，請參閱「[部署的伺服器安全性設定](#)」。

從白名單刪除可部署的伺服器：


1. 在左窗格的 **Dell 管理中心**，選取**設定**。
2. 在右窗格中，選取**安全性**。
3. 在**安全性**視窗中，按一下**編輯**。
4. 請執行下列其中一項動作：
  - 若要刪除個別伺服器，請按一下**服務標籤**核取方塊，然後再按一下**刪除所選項目**。

- 若要刪除所有伺服器，請勾選**服務標籤**核取方塊，然後再按一下**刪除所選項目**。
5. 若顯示**您確定要刪除選取的服務標籤嗎**對話方塊，請按一下**套用**，或是按一下**取消**以取消。
  6. 若要完成變更，請按一下**套用**。

## 關於主機、裸機和 iDRAC 規範問題

若要使用 OpenManage Integration for VMware vCenter 管理主機、裸機伺服器和 iDRAC，則以上每項皆必須符合特定最低標準。若未遵循此標準，則無法使用 OpenManage Integration for VMware vCenter 適當管理這些項目。使用「非相容主機」、「裸機伺服器」和 iDRAC 規範連結，查看組態中的哪些主機 / 裸機伺服器 / iDRAC 未相容並加以修正。此精靈會顯示主機 / 裸機伺服器 / iDRAC，其中：

- 主機未指派至連線設定檔。  
若未將連線設定檔指派至主機，則會顯示對話方塊引導您進入「連線設定檔」畫面。此組態超出本精靈涵蓋範圍。稍後請回頭執行此精靈。
- 「重新啟動時收集系統清查」(CSIOR) 已停用或尚未執行，您必須手動重新啟動。
- OMSA 代理程式 (主機根憑證) 未安裝、已過期或未正確設定。
- 裸機伺服器具有過時的 Integrated Dell Remote Access Controller (iDRAC) 韌體、Lifecycle Controller (LC) 韌體或 BIOS 版本。

 **警告:** 處於「鎖定模式」的主機將不會顯示於規範檢查，即使其為非相容亦然。由於系統無法判斷這些主機的規範狀態，因此其不會顯示。確認以手動方式檢查這些系統的規範。在此情況下會出現警告。

在每項個案中，您必須執行下列其中一項動作以修正規範問題：

- 若要修正 vSphere 主機規範問題，請參閱「[執行修正非相容 vSphere 主機精靈](#)」
- 若要修正裸機伺服器規範問題，請參閱「[執行修正非相容裸機伺服器精靈](#)」
- 若要修正 iDRAC 規範問題：[iDRAC 授權規範](#)

相關資訊：

- [重新檢查裸機伺服器規範](#)

## 執行解決不相容 vSphere 主機精靈

執行解決不相容 vSphere 主機精靈，修正不相容的主機。如需相容性相關資訊，請參閱[關於主機與裸機相容性問題](#)。有些不相容的 ESXi 主機需要重新啟動。如果 OpenManage Server Administrator (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，都需要重新啟動。如果選取自動重新啟動 ESXi 主機，會發生下列動作：

- 若為 CSIOR 狀態修正：  
如果主機未啟用 CSIOR，您可以在主機啟用 CSIOR，然後將主機設定為維護模式並重新啟動。
- 若為 OMSA 狀態修正：
  - a. 在主機安裝 OMSA。
  - b. 將主機設定為維護模式並重新啟動。
  - c. 重新啟動完成後會設定 OMSA，變更才會生效。
  - d. 主機離開維護模式。
  - e. 執行清查，重新整理資料。

若要執行解決不相容 vSphere 主機精靈：

1. 在左窗格中的 **Dell 管理中心**內，按一下**相容性** → **vSphere 主機**。
2. 在 **vSphere 主機相容性**視窗，檢視不相容的主機，然後按一下**解決不相容 vSphere 主機**。
3. 在**解決不相容 vSphere 主機**精靈中，選取您想要修正之主機的核取方塊。
4. 按一下**下一步**。
5. 如果有伺服器缺少連線設定檔，您可以選擇結束精靈，從**連線設定檔**頁面修正這些系統，也可以繼續使用此精靈。請參閱[建立新的連線設定檔](#)。完成時，請返回此精靈。
6. 在**開啟 CSIOR** 視窗選取核取方塊，為選取的主機開啟 **CSIOR**。
7. 按一下**下一步**。
8. 在**修正 OMSA** 視窗選取核取方塊，為選取的主機修正 **OMSA**。
9. 按一下**下一步**。
10. 在**重新啟動主機**視窗，檢視必須重新啟動的 ESXi 主機。如果必須安裝或更新 OMSA，必 ESXi 主機必須重新啟動。此外，凡是未曾執行過 CSIOR 的主機，都需要重新啟動。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。
  - 如果要手動重新啟動，您必須執行下列動作：
    1. 主機的**安裝 OMSA** 工作完成後，重新啟動主機。
    2. 主機啟動後，如果 OMSA 未設定，請手動設定 OMSA 或使用相容性精靈。
    3. 重新執行清查，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。手動重新啟動後，這些動作才會生效。
13. 按一下 **Finish** (完成)。

## 執行解決不相容裸機主機精靈

執行解決不相容裸機主機精靈，以修正不相容的裸機伺服器。如需相容性相關的資訊，請參閱[關於主機和裸機相容性問題](#)。

若要執行解決不相容裸機主機精靈：

1. 在左窗格的 **Dell 管理中心**，按一下**規範** → **裸機伺服器**。
2. 在**裸機伺服器**視窗，檢視不相容的主機，然後按一下**解決不相容裸機伺服器**。
3. 在**修正裸機伺服器**精靈中，針對想要修正的主機選取其核取方塊。
4. 按一下**下一步**。
5. 在**摘要**視窗中，檢查不相容裸機伺服器上發生的動作。
6. 按一下 **Finish** (完成)。


## 重新檢查裸機伺服器相容性

若為您在 OpenManage Integration for VMware vCenter 外修復的伺服器，必須執行本手動伺服器相容性重新檢查，在 Dell 管理中心、相容性、裸機伺服器頁面就找得到。

若要重新檢查裸機伺服器相容性：

1. 在 **Dell 管理中心** → **相容性** → **裸機伺服器**頁面，按一下**重新檢查相容性**。
2. 在**不相容伺服器**視窗中，若要重新整理清單，請按一下**重新整理**。
3. 若要執行重新檢查，請按一下**檢查相容性**。
4. 若要中止重新檢查，請按一下**中止全部測試**。

5. 如果成功修復系統，清單會重新整理，而且您的系統隨即會從清單移除，否則不相容系統會繼續留在清單上。
6. 完成時，按一下**完成**。

 **註:** OMIVV 需要 BIOS、LC 和 iDRAC 韌體達到最低相容性層級，OMIVV 才能正常運作。若為 BIOS、LC 或 iDRAC 韌體未達相容性層級的 Dell 伺服器，請參閱使用 Dell™ Repository Manager 建立部署媒體 (可開機 ISO) 執行系統更新，以手動更新韌體。

## iDRAC 授權規範


若您選取「iDRAC 授權規範」頁面，其即會執行規範測試。此測試會持續進行數分鐘時間。此頁面上所列的 vSphere 主機和裸機伺服器為非相容，這是因為其並無相容的 iDRAC 授權。下表顯示 iDRAC 授權的狀態。您可在此頁面上，查看授權的剩餘天數並視需要進行更新。若您停用 [執行清查工作連結](#)，則表示由於 iDRAC 授權的因素，因此已無非相容的 vSphere 主機。若停用 [重新檢查裸機伺服器規範連結](#)，則表示由於 iDRAC 授權的因素，因此已無非相容的裸機伺服器。

1. 在左窗格的 **Dell 管理中心** 中，按一下 **規範**。
2. 展開 **規範**，然後按一下 **iDRAC 授權**。  
抵達此頁面即會執行規範測試。您按一下 **重新整理** 時亦會執行相同的測試。
3. 若您的授權已過期，請按一下 **購買 / 續訂 iDRAC 授權**。
4. 登入「**Dell 授權管理**」頁面，以更新或購買新的 iDRAC 授權。  
使用此頁面上的資訊，以識別並更新您的 iDRAC。
5. 安裝 iDRAC 授權後，針對 vSphere 主機執行清查工作，並在清查工作完成後返回此頁面。針對裸機伺服器，請重新檢查授權裸機伺服器規範。

## 升級 OpenManage Integration for VMware vCenter

OpenManage Integration for VMware vCenter 的升級案例如下：

- [從試用版升級至完整產品版本](#)

 **註:** 開始升級之前，先備份應用裝置。請參閱 [執行立即備份](#)。

### 從試用版升級至完整產品版本

若要從試用版升級至完整產品版本：

1. 前往 [Dell 網站](#) 購買完整產品版本。  
從 OpenManage Integration for VMware vCenter，使用 **立即購買** 連結之一，例如管理入口網站 **授權** 視窗上的連結，也可以進入 Dell 網站。唯有使用評估授權時，這個方法才適用。
2. 下載包含新的完整版產品與新的授權檔案。
3. 針對您要設定的虛擬機器啟動瀏覽器視窗，然後輸入 **vSphere vCenter 主控台** 索引標籤顯示的 **管理主控台 URL**，或是從 **Dell 管理主控台** → **設定** 頁面使用連結。URL 使用的各式如下，而且必須區分大小寫：  
**https://<ApplianceIPAddress>**
4. 在 **管理主控台** 登入視窗輸入密碼，然後按一下 **登入**。
5. 若要上傳授權檔案，請按一下 **上傳**。
6. 在 **上傳授權** 視窗中，按一下 **瀏覽**，導覽至授權檔案。
7. 選取授權檔案，然後按一下 **上傳**。

# 關於 OpenManage Integration for VMware vCenter 授權

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

<b>評估授權</b>	試用版包含 OpenManage Integration for VMware vCenter 所管理之五個主機 (伺服器) 的評估授權。這僅適用於第 11 代以後。這是預設授權，僅供 90 天試用期。
<b>標準授權</b>	完整產品版本包含最多十個 vCenter 的標準授權，您可以購買之 OpenManage Integration for VMware vCenter 管理的主機連線數量不限。

從評估授權升級為完整的標準授權時，會以電子郵件方式將新授權的 XML 檔案連同包含授權檔案的壓縮檔案傳送給您。請將檔案儲存至本機系統，然後使用管理主控台上傳新的授權檔案。授權會提供下列資訊：

- vCenter 連線授權上限 — 最多允許註冊及使用十個 vCenter 連線。
- 主機連線授權上限 — 購買的主機連線數。
- 使用中 — vCenter 連線的數目或使用中主機連線授權的數目。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) 數量。
- 可用 — 可供日後使用的 vCenter 連線或主機連線授權數量。
- 未授權主機 — 超過授權數量的主機連線數。OpenManage Integration for VMware vCenter 會繼續正常運作，但必須購買並安裝新授權才能解決這個警告。

您購買授權時，無法透過 Dell Digital 商店下載此 XML 檔案。因此，若您需要重新安裝 OMIVV 應用裝置，請務必保留一份此 XML 檔案的備份。若您遺失 XML 檔案且您無法找到該檔案位置時，請傳送電子郵件至 [download\\_software@dell.com](mailto:download_software@dell.com)，並提供下列詳細資料，我們會將新的 XML 檔案傳送給您：

- 原始 Dell 訂單號碼
- 訂單上的 OpenManage Integration for VMware vCenter SKU
- 每一個 SKU 的數量
- 接收 XML 檔案的電子郵件地址

標準的 SLA 程序約需 2 個工作天。

## 端對端硬體管理

端對端硬體管理的用途，在於向管理員提供回應重大硬體事件所需的系統健全狀況狀態與最新基礎資訊，而無須離開「Dell 管理中心」或 vCenter。端對端硬體管理位於 OpenManage Integration for VMware vCenter 中，且分為四個獨立部分：

- 監視
- 清查
- 進階主機管理
- 保固擷取

## 監視資料中心與主機系統

資料中心與主機系統監視會在 vCenter 的工作與事件索引標籤，顯示硬體 (伺服器與儲存裝置) 與虛擬化相關事件，讓管理員監視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。僅少數 Dell 虛擬化相關事件定義的事件，能讓受管的主機系統進入維護模式。

若要執行監視：

1. 進行**事件與警報**設定。
2. 必要時，設定 **SNMP OMSA 設陷目的地**。
3. 用 vCenter 中的**工作與事件**索引標籤檢查事件資訊。

## 瞭解事件與警報

從 OpenManage Integration for VMware vCenter 內的 **Manage (管理)** → **Settings (設定)** 標籤，您可以編輯事件與警報。在這裡，您可以選取事件發佈層級、啟用 Dell 主機的警告或還原預設警報。您可以個別設定每個 vCenter 的事件與警報，也可以一次設定所有已註冊 vCenter 的事件與警報。

事件發佈層級有四個。

**表 2. 事件發佈層級說明**

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。
發佈所有事件	發佈所有事件，包括非正式事件，OpenManage Integration for VMware vCenter 從受管 Dell 主機接收後會轉寄到相關的 vCenter。
僅發佈嚴重和警告事件	僅發佈嚴重性屬於嚴重或警告的事件到相關的 vCenter。

僅發佈虛擬化相關嚴重和警告事件


將從主機接收到的虛擬化相關事件發佈到相關的 vCenter。虛擬化相關事件是指經 Dell 選定，對執行虛擬機器之主機最重要的事件。


設定事件和警報時，可以加以啟用。若啟用，重要硬體警報能夠觸發 OpenManage Integration for VMware vCenter，使主機系統進入維護模式，而且在某些情況下，會將虛擬機器移轉到其他主機系統。OpenManage Integration for VMware vCenter 從受管 Dell 主機收到事件後會轉寄，並為這些事件建立警告。用這些警報觸發 vCenter 的動作，像是重新開機、維護模式或移轉。例如，雙電源供應器故障且建立警報時，導致的動作便是將該機器上的虛擬機器移轉到新機器。

唯有您要求，主機才會進入或離開維護模式。如果主機進入維護模式時處於叢集，您可以選擇撤除關閉的虛擬機器。如果已選取此選項，每台關閉的虛擬機器會移轉到其他主機，除非叢集中的虛擬機沒有相容的主機可用。處於維護模式時，主機不允許部署或開啟虛擬機器。正在主機執行的虛擬機器若進入維護模式，必須移轉到另一個主機或關機，無論是用手動方式或由 VMware Distributed Resource Scheduling (DRS) 自動代勞皆可。

凡是叢集以外的主機，或是叢集內但未啟用 VMware Distributed Resource Scheduling (DRS) 的主機，可看見因為嚴重事件而被關閉的虛擬機器。DRS 會持續監測資源集區的使用情況，並根據業務需求，以智慧方式分配虛擬機器的可用資源。使用設定 DRS 的叢集搭配 Dell 警報，以確保發生嚴重硬體事件時，虛擬機器會自動移轉。畫面訊息詳述的是，此 vCenter 例項上可能受到影響的任何叢集。請先確認叢集是否受到影響，再啟用事件與警報。


如果需要還原預設的警告設定，可以使用重設預設警報按鈕。此按鈕十分方便，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，用這個按鈕即可還原那些變更。

 **註:** 您必須啟用事件，才能接收 Dell 事件。

 **註:** OpenManage Integration for VMware vCenter 預先選取的虛擬化相關事件，攸關主機是否能成功執行虛擬機器。Dell 主機警報預設為停用。如果啟用 Dell 警報，叢集應使用 VMware Distributed Resource Scheduler 確定傳送重要事件的虛擬機器會自動移轉。

## 瞭解適用於第 11 代 Dell PowerEdge 主機的 OMSA

針對第 12 代之前的 PowerEdge 伺服器，您必須安裝 OMSA 以搭配 OpenManage Integration for VMware vCenter 一起使用。執行部署時，系統會自動將 OMSA 安裝於第 11 代 Dell PowerEdge 主機，或者您亦可選擇以手動方式安裝。


 **註:** 使用 OpenManage Integration for VMware vCenter 部署 OMSA 代理程式時，會針對 ESXi 5.0 之後的版本啟動 httpClient 服務並啟用連接埠 8080，以下載並安裝 OMSA VIB。OMSA 安裝完成後，即會自動停止服務並關閉連接埠。

若要在第 11 代 Dell PowerEdge 伺服器上設定 OMSA，您有下列選擇：

- [在 ESXi 系統部署 OMSA 代理程式](#)
- [設定 OMSA 設陷目的地](#)

### 在 ESXi 系統部署 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:** 比 Dell PowerEdge 第 12 代伺服器舊的 Dell 主機，必須有 OpenManage 代理程式。安裝 OpenManage Integration for VMware vCenter 前，先使用 OpenManage Integration for VMware vCenter 安裝 OMSA，或手動安裝到主機。手動安裝代理程式的詳細資料位於 <http://en.community.dell.com/techcenter/systems-management/w/wiki/1760.openmanage-server-administrator-omsa.aspx>。


1. 如果尚未安裝，請從 <http://www.vmware.com> 安裝 vSphere 命令行工具 (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 安裝可能需花幾分鐘。此命令完成後需要重新啟動主機。

## 設定 OMSA 設陷目的地

所有第 11 代主機皆必須設定 OMSA。

 **註:** 僅有第 12 代 Dell PowerEdge 伺服器之前的 Dell 伺服器需要使用 OMSA。

設定 OMSA 設陷目的地：

1. 請使用在**設定** → **一般**中找到的 OMSA 使用者介面連結，或是從網頁瀏覽器 (<https://<HostIP>:1311/>) 瀏覽至 OMSA 代理程式。
2. 登入介面，然後選取 **Alert Management (警示管理)** 索引標籤。
3. 選取 **Alert Actions (警示動作)**，確定凡是要監視的事件都已設定 **Broadcast Message (廣播訊息)** 選項，這樣才會傳送事件。
4. 在索引標籤頂端，選取**平台事件**選項。
5. 按一下灰色的 **Configure Destinations (組態目的地)** 按鈕，然後按一下 **Destination (目的地)** 連結。
6. 選取 **Enable Destination (啟用目的地)** 核取方塊。
7. 在**目的地 IP 位址**欄位中，輸入 OpenManage Integration for VMware vCenter 設備 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。

## 檢視事件

若要檢視事件，請執行以下任一操作：

- 瀏覽至虛擬機器，按一下滑鼠右鍵顯示 **vCenter** → **工作與事件**索引標籤，然後按一下**事件**以顯示所選的事件層級。
- 按一下 vCenter 主機或根資料夾的父節點 (叢集或資料中心)。

事件僅會顯示在 vSphere 樹狀結構中的這些節點上。

# vSphere 用戶端主機概觀

概觀針對金鑰主機伺服器屬性，包括個別元件健全狀況、識別、Hypervisor 和韌體提供相關資訊。

## 硬體元件健全狀況

元件健全狀況會以圖形表示所有主要主機伺服器元件的狀態：系統機箱、電源供應器、溫度、風扇、電壓、處理器、電池、侵入、硬體記錄、電源管理和記憶體。可用狀態如下：

- 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
- 嚴重 (紅色 X) — 元件有嚴重故障
- 不明 (問號) — 狀態不明的元件

右上標題列會顯示全域健全狀況狀態。

## 伺服器資訊

伺服器資訊提供識別、Hypervisor 和韌體資訊，例如：


- 主機名稱、電源狀態、iDRAC IP、管理 IP、使用中的連線設定檔、型號、服務標籤號碼和資產標籤號碼、保固剩餘天數，以及最後一次執行清查掃描的時間。
- Hypervisor、BIOS 韌體和 iDRAC 韌體版本。
- 最近十個系統事件記錄項目。按一下「詳細資料」即可啟動**系統事件記錄**視窗，顯示額外的記錄詳細資料。

## 主機資訊

在主機概觀左窗格中，您會看到下列幾類主機資訊的連結：

- 系統事件記錄  
顯示硬體系統事件記錄的資訊。請參閱[瞭解系統事件記錄](#)。
- 硬體清單  
顯示下列硬體裝置的相關資訊：
  - 可現場更換的零件 (FRU)，例如 DIMM、系統平面、電源供應器、背板，控制器卡與其他零件。
  - 記憶體 — 可用和使用中的插槽數、最大容量與使用中的記憶體數量，以及個別 DIMM 的詳細資料。
  - 網路介面卡 (NIC) — 已安裝的網路介面卡數，以及個別 NIC 的詳細資料。
  - PCI 插槽 — 可用總數與使用中的數量，以及個別插槽的詳細資料。
  - 電源供應器 — 現有的數量及個別 PSU 的相關詳細資料。
  - 處理器 — 現有的數量及個別 CPU 的相關詳細資料。
  - 遠端存取卡 — IP 位址資訊和 RAC 類型，以及 Web 介面的 URL。

請參閱[關於清查工作](#)。
- 存放時  
主機系統儲存針對連接主機型儲存控制器的儲存裝置，以圖形方式提供實體與邏輯儲存裝置容量和類型的詳細檢視，包括：
  - 主機系統總儲存、未設定、已設定和通用與專用熱備援磁碟容量
  - 系統元件資料表列出各儲存元件的數量，還包含該元件的詳細資訊
- 韌體  
執行「韌體更新精靈」或檢視韌體版本。請參閱[韌體更新](#)。
- 電源監視  
主機系統電源監視提供一般電源資訊、能源統計資料和備用電源的資訊，包括：
  - 目前的電源預算、設定檔、警告和故障閾值
  - 能源消耗、系統尖峰電源和安培數統計資料
  - 備用電源和尖峰備用容量

 **註:** 並非所有電源供應器都支援這個功能，不支援刀鋒機櫃的電源供應器。

- 保固  
保固擷取為 Dell 伺服器提供下列資訊：
  - 更新服務保固資訊 (僅會傳送主機服務標籤)
  - 在排定的時間間隔更新保固資訊
  - 使用 Proxy 伺服器與認證進行傳輸加密處理
  - 透過經測試的安全連線傳輸資訊

請參閱[保固擷取](#)。

## 主機的動作

主機的動作是指您在目前這個主機伺服器執行的命令，例如：

- 使用閃爍指示燈來閃爍 LCD 前指示燈。請參閱[設定實體伺服器前指示燈](#)。
- 使用「執行韌體更新精靈」可顯示「韌體更新精靈」，並更新主機伺服器的韌體。請參閱[執行韌體更新精靈](#)。
- 使用 iDRAC 重設即可重設 iDRAC，不需重新啟動主機。

請參閱[重設 iDRAC](#)。

## 管理主控台

管理主控台用於啟動外接式系統管理主控台，例如：


- 按一下遠端存取主控台即可啟動 Integrated Dell Remote Access Controller (iDRAC) Web 使用者介面。
- 按一下「OMSA 主控台」即可啟動 OpenManage Server Administrator (OMSA) 使用者介面 (如果已設定)。請參閱[啟用 OMSA 連結](#)。
- 按一下刀鋒機箱主控台即可啟動機箱管理控制器 (CMC) Web 使用者介面。

## 重設 iDRAC

iDRAC 有時可能不會回應來自 OpenManage Integration for VMware vCenter 的要求。從此狀態復原的唯一方式，即是重設 iDRAC。iDRAC 重設會執行標準 iDRAC 重新啟動作業。此重新啟動作業不會將主機重新開機。執行重設後，請靜待 1 或 2 分鐘讓 iDRAC 回復為可用狀態。

iDRAC 重新啟動時，您可能會發現：

- 在 OpenManage Integration for VMware vCenter 取得其健全狀況狀態時，發生延遲或通訊錯誤。
- iDRAC 所有開啟的工作階段關閉。
- iDRAC 的 DHCP 位址可能會變更。若 iDRAC 的 IP 位址使用 DHCP，則 IP 位址有可能會改變。如果發生這種情況，請重新執行主機清查工作，在清查資料中擷取新的 iDRAC IP。

 **註:** 執行 iDRAC 軟重設並非總能讓 iDRAC 回復可重複使用狀態。您可能需要執行硬重設。若要執行硬重設，請在伺服器上關閉伺服器電源、拔下電源線靜待 2 分鐘後再將其接回。如需關於重設 iDRAC 的詳細資訊，請參閱適用於您 iDRAC 版本的「使用者指南」。

 **註:** Dell 建議您先讓主機進入維護模式，然後再重設 iDRAC。


1. 在**清查**標題下方的 **vSphere 用戶端**中，選取**主機與叢集**。
2. 從樹狀檢視畫面的**主機與叢集**選取主機系統，然後再選取 **OpenManage 整合**索引標籤。
3. 在**主機動作**下方，選擇 **iDRAC 重設**。
4. 在「iDRAC 重設」對話方塊中，選取**繼續執行 iDRAC 重設**，然後再按一下**確定**。

## 有關清查排程

清查排程會設定時間 / 日期以執行清查工作，例如：

- 在每週的特定時間和特定日期
- 在設定的時間間隔

大部分的 OpenManage Integration for VMware vCenter 功能會要求先完成清查以收集需要的資料。您必須收集所有主機系統的清查以顯示此資訊。若要在主機系統上執行清查，請建立提供通訊與驗證資訊的連線設定檔。清查完成後，您可檢視個別主機系統的清查結果。

 **註:** 為確保清查包含最新資訊，每週應至少執行一次清查工作。清查工作會耗用最少的資源，且不會降低主機效能。


**相關工作：**

- [執行清查工作](#)
- [修改清查工作排程](#)
- [顯示單一主機系統的清查](#)
- [顯示資料中心硬體組態和狀態](#)

## 修改清查工作排程

「清查排程」會設定時間 / 日期以執行清查工作，例如：

- 在每週的特定時間和特定日期。
- 在設定的時間間隔內，必須透過完整清查工作以收集大部分 OpenManage Integration for VMware vCenter 功能所需要的資料。

 **註:** 為確保清查包含最新資訊，每週應至少執行一次清查工作。清除工作會耗用最少的資源，且不會降低主機效能。

修改清查工作排程：

1. 從「Dell 管理中心」，選取**設定** → **清查排程**。
2. 若要變更目前的排程，請按一下**編輯**。
3. 選取在**選定日期**選項按鈕，然後選取當週某天的核取方塊並輸入時間。按一下 **清除**以清除項目。
4. 若要變更清查排程，請按一下**套用**，或者若要取消清查排程，請按一下**取消**。
5. 若要立即執行工作，請從管理中心選取**工作佇列**和**清查歷程記錄**索引標籤。
6. 按一下**立即執行**。
7. 若要更新**上次清查工作詳細資料**，請按一下**重新整理**。

## 在 vCenter 中顯示單一主機系統的清查

顯示單一主機系統的清查：

1. 從 vSphere 用戶端的首頁，選取**主機與叢集**。
2. 從左窗格中的**主機與叢集**選取主機系統，然後再選取 **OpenManage 整合** 索引標籤。
3. 顯示所選主機的概觀。

概觀提供關於重要主機伺服器屬性的資訊，包括個別元件的健全狀況，識別、Hypervisor 和韌體資訊。

- 「硬體元件健全狀況」會以圖形化方式顯示所有主要主機伺服器元件的狀態：系統機箱、電源供應器、溫度、風扇、電壓、處理器、電池、侵入、硬體記錄、電源管理和記憶體。可用的狀態如下：

- 健康 (綠色勾號) - 元件運作正常
- 警告 (有驚嘆號的黃色三角形) - 元件有非嚴重錯誤
- 嚴重 (紅色 X) - 元件有嚴重故障
- 不明 (問號) - 狀態不明的元件

在右上角標題列會顯示全域健全狀況狀態。

- 「伺服器資訊」提供識別、Hypervisor 和韌體資訊，例如：
    - 主機名稱、電源狀態、iDRAC IP 位址、管理 IP 位址、使用中的連線設定檔、型號、服務標籤和資產標籤號碼，剩餘保固天數，以及上次執行清查掃描的時間
    - Hypervisor、BIOS 韌體和 iDRAC 韌體版本
    - 記憶體錯誤回復 (FRM)：這是 BIOS 屬性，伺服器初始設定時已在 BIOS 啟用，會顯示伺服器的記憶體作業模式。變更記憶體作業模式的值時，您必須重新啟動系統。這適用於搭載 ESXi 5.5 以上版本的 R620、R720、T620、M620 以及第 13 代伺服器。四個不同的值為：
      - \* 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 以上，而且在 BIOS 將記憶體作業模式設定為 FRM。
      - \* 已啟用未防護：這個值表示 BIOS 中的記憶體作業模式設定為 FRM，但作業系統不支援此功能。
      - \* 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 中的記憶體作業模式並未設定 FRM。
      - \* 空白：如果 BIOS 不支援記憶體錯誤回復，就不會顯示 FRM 屬性。
  - 「最近的系統記錄項目」提供最近 10 筆系統事件記錄項目。若要啟動**系統事件記錄**視窗以顯示其他記錄詳細資料，請按一下**詳細資料**。
4. 在**主機資訊**下方，按一下**硬體清查**，以顯示主機系統之所有安裝元件的清單和進一步詳細資料，包括：
    - 現場可更換裝置 (FRU)：DIMM、系統平面、電源、背板、控制卡等等。
    - 記憶體：可用與使用中的插槽數量、最大容量與可用記憶體數量，以及關於個別 DIMM 的詳細資料。
    - 網路介面卡 (NIC)：安裝的介面卡數量，以及關於個別 NIC 的詳細資料。
    - PCI 插槽 - 總計可用與使用中的數量，以及關於個別插槽的詳細資料。
    - 電源供應器：關於個別 PSU 的顯示號碼和詳細資訊。
    - 處理器：關於個別 PSU 的顯示號碼和詳細資訊。
    - 遠端存取卡：IP 位址資訊、RAC 類型和 Web 介面 URL。
  5. 在**主機資訊**下方按一下**儲存裝置**，以針對實體與虛擬儲存裝置的容量和類型，顯示圖形化詳細檢視，包括：
    - 主機系統總計儲存、未設定、已設定和全域熱備援磁碟容量。

- 列出系統中顯示的每個儲存元件數量。
  - 元件資料表，其中包含該元件的詳細資訊。
6. 在**主機資訊**下方，按一下**韌體**以顯示所有 Dell Lifecycle 控制器韌體資訊，包括：
    - 更新名稱：BIOS、Dell Lifecycle 控制器、電源供應器等等。
    - 更新類型：BIOS、韌體或應用程式。
    - 個別更新詳細資料：版本、安裝時間、更新作業處於進行中或更新狀態，以及更新版本。僅在已排定更新，且更新版本為系統將要更新的目標韌體版本時，更新狀態與版本才會具有資料。
  7. 在**主機資訊**下方，按一下**電源監控**以顯示一般電源資訊、能源統計資料和保留電源資訊，包括：
    - 目前的電源預算，設定檔、警告和故障臨界值。
    - 能源消耗、系統尖峰功率和安培統計資料。
    - 保留電源與尖峰保留容量。
  8. 在**主機資訊**下方，按一下**保固**以顯示系統保固資訊：
    - 保固供應商名稱與保固說明。
    - 保固的開始與結束日期，以及其剩餘天數。
    - 保固的狀態 (作用中、已過期)，以及上次更新保固資訊的時間。

## 清查與授權

如果無法擷取及顯示伺服器資料，原因可能有幾種：

- 伺服器未與連線設定檔建立關聯，因此清查工作無法完成。
- 尚未在伺服器執行清查工作以收集資料，因此沒有資料可以顯示。
- 主機授權數超過，必須準備可用的額外授權，清查工作才能完成。
- 伺服器沒有第 12 代以後伺服器所需的正確 iDRAC 授權，您必須購買正確的 iDRAC 授權。

立即購買連結用於第一次購買產品，而非用於升級。唯有使用評估授權，立即購買連結才會出現。

相關工作：

- [檢視與編輯現有的連線設定檔](#)
- [修改清查工作排程](#)

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

- 評估授權：試用版本內含示範授權，可用於 OpenManage Integration for VMware vCenter 所管理的五部主機 (伺服器)。
- 標準授權：完整產品版本內含的產品授權，可用於 OpenManage Integration for VMware vCenter 所管理的十部 vCenter 和已購買數量的主機連線。

相關工作：

- [關於 OpenManage Integration for VMware vCenter 授權](#)
- [上傳 OpenManage Integration for VMware vCenter 授權至管理主控台](#)

## 檢視儲存清查

主機系統儲存會針對連接至主機型儲存控制器的儲存裝置，提供關於其實體與邏輯儲存容量和類型的圖形化詳細檢視，包括：

- 主機系統總計儲存、未設定、已設定和全域熱備援磁碟容量

- 列出系統中顯示的每個儲存元件數量
- 元件資料表，其中包含該元件的詳細資訊

檢視儲存資料：

1. 在 **vSphere 用戶端** 中選取主機，然後選取 **OpenManage Integration** 索引標籤。
2. 在左窗格的主機資訊下方，按一下 **儲存**。
3. 在 **儲存** 頁面中，檢視圖形摘要或是使用表格以及 **檢視與篩選** 下拉式清單，排序您的清查資訊。

## 檢視主機電源監視

主機系統電源監控提供一般電源資訊、能源統計資料和備用電源資訊，包括：

- 目前的電源預算，設定檔、警告和故障閾值
- 能源消耗、系統尖峰功率和安培統計資料
- 備用電源和尖峰保留容量

檢視主機電源監視：

1. 在 **vSphere 用戶端** 中選取主機，然後選取 **OpenManage Integration** 索引標籤。
2. 在左窗格的主機資訊下方，按一下 **電源監視**。
3. 在 **電源監視** 頁面中，檢視此主機的電源。

## 顯示整個資料中心硬體組態

您必須先完成清查工作，才能顯示整個資料中心的硬體組態。清查執行後，即可檢視下列任何一項：

- 硬體：現場可更換單元
- 硬體：處理器
- 硬體：電源供應器
- 硬體：記憶體
- 硬體：NIC
- 硬體：PCI 插槽
- 硬體：遠端存取卡
- 儲存裝置：實體磁碟
- 儲存裝置：虛擬磁碟
- 韌體
- 電源監視
- 保固

若要顯示整個資料中心硬體組態：

1. 在 **vSphere 用戶端** 的 **清查** 標題下，選取 **主機與叢集**。
2. 在 **主機與叢集** 中從樹狀檢視畫面選取資料中心，然後選取 **OpenManage Integration** 索引標籤。
3. 資料中心內所有主機的概觀隨即顯示。用 **檢視** 下拉式清單檢視清查類別。
4. 用 **篩選** 文字方塊輸入清查資料的篩選條件。
5. 若要重新整理顯示的清查，請按一下 **重新整理**。

## 管理連線設定檔

連線設定檔會將存取和部署憑證與一組主機系統建立關聯，且通常包含以下項目：

- 設定檔名稱與唯一的說明 (協助設定檔管理)
- 與連線設定檔關聯的主機清單
- iDRAC 認證
- 主機認證
- 建立日期
- 修改日期
- 上次修改的使用者

執行**組態精靈**後，使用下列設定檔，從 OpenManage Integration for VMware vCenter **管理索引標籤** → **範本與設定檔**可管理認證設定檔：

- [建立連線設定檔](#)
- [檢視與編輯現有的連線設定檔](#)
- [刪除連線設定檔](#)
- [測試連線設定檔](#)
- [重新整理連線設定檔](#)

### 檢視或編輯現有的連線設定檔

設定連線設定檔後，您可以編輯設定檔名稱、說明、關聯的主機，以及 iDRAC 和 OMSA 代理程式憑證。

檢視或編輯現有的連線設定檔：


1. 從 OpenManage Integration for VMware vCenter 選取**連線設定檔**。
2. 在**可用設定檔**下方，選取您要檢視或編輯的設定檔，然後按一下**編輯/檢視**。
3. 在**設定檔名稱與說明**頁面中，輸入**連線設定檔名稱**和選用的**連線設定檔說明**，以用於協助管理自訂連線設定檔。
4. 在**關聯主機**頁面中，選取連線設定檔的主機，然後按**下一步**。
5. 在**憑證**頁面中檢閱資訊，然後按**下一步**。
6. 在 iDRAC 頁面的「憑證」下方，執行下列其中一項動作：





**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。

- 若為要使用 Active Directory，而且已經針對 Active Directory 完成設定及啟用的 iDRAC，請選取**使用 Active Directory** 核取方塊，否則請略過直接設定 iDRAC 憑證。
  - 在 **Active Directory 使用者名稱** 文字方塊中輸入使用者名稱。以下列其中一種格式輸入使用者名稱：網域\使用者名稱、網域/使用者名稱或 username@domain。使用者名稱限制為 256 個字元。如需使用者名稱限制，請參閱 Microsoft Active Directory 說明文件。
  - 在 **Active Directory Password (Active Directory 密碼)** 文字方塊輸入密碼。密碼限制為 127 個字元。
  - 在 **Verify Password (確認密碼)** 文字方塊中，再次輸入密碼。

- 在「憑證檢查」下拉式清單中，選取下列其中一項動作：
  - \* 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**。
  - \* 若不執行任何檢查且不儲存憑證，請選取**停用**。
- 若不用 Active Directory 設定 iDRAC 憑證，請執行下列步驟：
  - 在**使用者名稱**文字方塊中輸入使用者名稱。使用者名稱限制為 16 個字元。有關您 iDRAC 版本使用者名稱限制的資訊，請參閱 iDRAC 文件。
 

 **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 **Password (密碼)** 文字方塊輸入密碼。密碼限制為 20 個字元。
  - 在 **Verify Password (確認密碼)** 文字方塊中，再次輸入密碼。
  - 在「憑證檢查」下拉式清單中，選取下列其中一項動作：
    - \* 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**。
    - \* 若不執行任何檢查且不儲存 iDRAC 憑證，請選取**停用**。
- 7. 按一下**下一步**。
- 8. 在「主機憑證」頁面的「憑證」下方，執行下列其中一項動作：
  - 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 **Use Active Directory (使用 Active Directory)** 核取方塊，否則請略過，直接設定 Host Credentials (主機憑證)。
    - 在 **Active Directory 使用者名稱**文字方塊中輸入使用者名稱。以下列其中一種格式輸入使用者名稱：網域\使用者名稱、網域/使用者名稱或 username@domain。使用者名稱限制為 256 個字元。如需使用者名稱限制，請參閱 Microsoft Active Directory 說明文件。
    - 在 **Active Directory Password (Active Directory 密碼)** 文字方塊輸入密碼。密碼限制為 127 個字元。
    - 在 **Verify Password (確認密碼)** 文字方塊中，再次輸入密碼。
    - 在「憑證檢查」下拉式清單中，選取下列其中一項動作：
      - \* 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**。
      - \* 若不執行任何檢查且不儲存「主機」憑證，請選取**停用**。
  - 若不用 Active Directory 設定主機憑證，請執行下列步驟：
    - 在**使用者名稱**文字方塊中輸入使用者名稱。使用者名稱必須是根。
    - 在 **Password (密碼)** 文字方塊輸入密碼。密碼限制為 127 個字元。
 

 **註:** 若為不具備 iDRAC Express 或 Enterprise 卡的伺服器，iDRAC 測試連線結果會顯示 Not Applicable for this system (此系統不適用)。

 **註:** OMSA 憑證與 ESXi 主機所用的憑證相同。
    - 在 **Verify Password (確認密碼)** 文字方塊中，再次輸入密碼。
    - 在「憑證檢查」下拉式清單中，選取下列其中一項動作：
      - \* 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**。

\* 若不執行任何檢查且不儲存「主機」憑證，請選取**停用**。

9. 按一下 **Save** (儲存)。
10. 若要關閉視窗，請按一下 **X** (右上角)。

## 刪除連線設定檔

您可從 OpenManage Integration for VMware vCenter 移除連線設定檔。

刪除連線設定檔：

1. 從 **OpenManage Integration for VMware vCenter**，按一下 **連線設定檔**。
2. 在**可用設定檔**下方，選取您要刪除的設定檔，然後按一下**刪除**。
3. 若要在顯示的訊息中移除設定檔，請按一下**刪除**，或是按一下**取消**以取消刪除動作。


## 測試連線設定檔

測試連線設定檔：

1. 在 **OpenManage Integration for VMware vCenter** 中，選取**連線設定檔**。
2. 若要在**可用設定檔**下方針對選定伺服器測試輸入的 iDRAC 和主機根憑證，請選取連線設定檔，然後按一下**測試連線**。
3. 使用核取方塊選取您想要測試的主機，然後按一下**已選取測試**。
4. 若要中止所有已選取的測試並取消測試，請按一下**中止所有測試**。
5. 按一下**完成**即可結束。

## 重新整理連線設定檔

在 OpenManage Integration for VMware vCenter 的**管理** → **連線設定檔**索引標籤上，找到 VMware vSphere Web 用戶端標題列，按一下裡面的**重新整理**圖示。

 **註：**主機從 vCenter 移除時，會自動從連線設定檔移除。

## 瞭解 vSphere 用戶端主機檢視中的系統事件記錄

「系統事件記錄」會針對 OpenManage Integration for VMware vCenter 探索到的硬體提供狀態資訊。

「系統事件記錄」會根據下列條件提供資訊：

<b>Status (狀態)</b>	提供數種狀態圖示：通知 (藍色驚嘆號)、警告 (黃色三角形與驚嘆號)、錯誤 (紅色 X 號)。
<b>時間 (伺服器時間)</b>	顯示事件發生的時間及日期。
<b>搜尋此頁面</b>	顯示特定訊息、伺服器名稱、組態設定等等。

嚴重性等級定義如下：

<b>資訊</b>	OpenManage Integration for VMware vCenter 作業已順利完成。
<b>警告</b>	OpenManage Integration for VMware vCenter 部分作業失敗，部分作業成功。
<b>錯誤</b>	OpenManage Integration for VMware vCenter 作業失敗。

**Security (安全保護)** 包含系統安全性相關資訊。

您可以將記錄另存為外部 CSV 檔案。

相關資訊：

- [顯示個別主機的系統事件記錄](#)

## 顯示 DELL 管理中心記錄

「Dell 管理中心」記錄包括針對探索硬體的狀態資訊，以及使用者動作的歷程記錄。

顯示 DELL 管理中心記錄：

1. 從左窗格的 **Dell 管理中心**，選取**記錄**。
2. 若要為記錄更新最近的資料，請按一下**重新整理**。
3. 若要選取嚴重性類別以篩選記錄資料，請在**所有類別**下拉式清單中選取下列其中一個項目：所有類別、資訊、警告、錯誤或安全性。
4. 若要選取篩選記錄資料的日期範圍，請按一下**最後一週**下拉式清單中，然後選取下列其中一個項目：最後一週、最後一個月、最後一年或自訂範圍。  
若已選取「自訂範圍」，即會顯示**開始日期**與**停止日期**下拉式清單。
5. 若您選取自訂日期範圍：
  - a. 按一下行事曆以填入**開始**日期。
  - b. 按一下行事曆以填入**結束**日期。
  - c. 若要儲存組態，請按一下**套用**。
6. 若要控制記錄的顯示方式，請使用顯示控制項設定**記錄每個畫面**，移至所需的**頁面**，然後使用上一頁和下一頁的頁面控制項。
7. 若要將記錄內容匯出至逗號分隔值 (CSV) 檔，請按一下**匯出**。
8. 在下載位置視窗中，瀏覽至儲存記錄的位置，然後按一下**儲存**。

## 顯示個別主機的事件記錄

系統 HardwareEvent 記錄提供根據下列條件的資訊：

- **Status (狀態)**  
提供數種狀態圖示：通知 (藍色驚嘆號)、警告 (黃色三角形與驚嘆號)、錯誤 (紅色 X 號)。
- **時間 (伺服器時間)**  
顯示事件發生的時間及日期。
- **搜尋此頁面**  
顯示特定訊息、伺服器名稱、組態設定等等。

顯示個別主機的系統事件記錄：

1. 從**清查**標題下方的 **vSphere 用戶端**，選取**主機與叢集**。
2. 在樹狀檢視畫面中，選取主機系統。
3. 選取 **OpenManage Integration** 索引標籤。
4. 從**最近的系統記錄**項目，啟動**系統事件記錄**視窗，按一下**詳細資料**。
5. 若要更新**系統事件記錄**，請按一下**重新整理記錄**。
6. 若要限制 (篩選)事件日誌項目數量，請選擇下列其中一個項目：


- 在搜尋篩選文字方塊中輸入文字字串，以動態篩選記錄項目。
  - 若要清除篩選文字方塊，請按一下 **X** 顯示所有的事件記錄項目。
7. 若要清除所有的事件記錄項目，請按一下 **清除記錄**。此時會顯示訊息指出所有記錄項目皆會清除，然後再選取下列其中一個項目：
    - 若要同意清除記錄項目，請按一下 **確定**。
    - 若要取消，請按一下 **取消**。
  8. 若要將事件記錄匯出至 CSV 檔，請按一下 **匯出**。
  9. 瀏覽系統事件記錄的儲存位置，然後按一下 **儲存**。

## 關於韌體更新

伺服器收到韌體更新的位置屬於全域設定，位在「設定」索引標籤的 OpenManage Integration for VMware vCenter。

韌體儲存庫設定包含用於更新已部署伺服器的韌體目錄位置。位置類型有兩種：

- Dell (ftp.dell.com)** 使用 Dell (**ftp.dell.com**) 的韌體更新儲存庫。OpenManage Integration for VMware vCenter 會從 Dell 儲存庫下載選取的韌體更新。
- 共用網路資料夾** 以 Dell Repository Manager™ 所建立。這些本機儲存庫位於 CIFS 或 NFS 檔案分享器。

 **註：** 儲存庫建立後，將它儲存到已登錄的主機可以存取的位置。儲存庫密碼不能超過 31 個字元。密碼請勿使用下列字元：@、&、%、'、"、, (逗號)、< 及 >


韌體更新精靈一律會檢查 iDRAC、BIOS 和 Lifecycle Controller 的最低韌體層級，並嘗試將它們更新至所需的最低版本。一旦 iDRAC、Lifecycle Controller 和 BIOS 韌體版本符合最低需求，韌體更新精靈便允許所有韌體更新，包括：iDRAC、Lifecycle Controller、RAID、NIC/LOM、電源供應器、BIOS 等。


**相關資訊：**

- [設定韌體儲存庫](#)

## 執行韌體更新精靈

本功能僅適用於具 iDRAC Express 或 Enterprise 插卡的第 11 代和更新版本 Dell 伺服器。


 **註：** 為了避免瀏覽器逾時問題，請將預設逾時變更為 30 秒。如需變更預設逾時設定的資訊，請參閱 *使用者指南*「疑難排解」一節的按一下韌體更新連結後為什麼顯示錯誤訊息。

 **註：** 若為試用/評估授權，只要授權未過期，您都可以使用韌體精靈。

若要執行韌體更新精靈：

1. 在 **vSphere Client** → **OpenManage Integration** 索引標籤 → **主機資訊** 上，按一下 **韌體** → **執行韌體更新精靈**。
2. 若要使用 **從檔案載入單一韌體更新** 選項：
  - a. 以下列格式輸入檔案路徑：
    - CIFS: \\<host accessible share path>\<FileName>.exe or
    - NFS: host:/share/filename.exe
  - b. 如果您有 NFS，請跳至步驟 7，或請用可存取共用磁碟機的網域格式輸入 **使用者名稱** 和 **密碼**。
  - c. 請繼續步驟 7。

或者，若要使用**從儲存庫更新**選項：

- a. 選取**從儲存庫更新**。
  - b. 請確定您的網路有連線至 **ftp.dell.com**。
  - c. 按一下 **下一步**。
3. 為主機選取配套，然後按一下**下一步**。
-  **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。
  - 搭載任何 iDRAC 版本的第 11 代主機不支援 64 位元配套。
4. 選取所需的韌體更新，然後按一下**下一步**。屬於降級、最新或目前排定要更新的元件無法選取。如果選取**允許元件降級**核取方塊，請選取列為「降級」的選項。唯有瞭解降級韌體影響的進階使用者，才建議選取此選項。
5. 選取所需的重新啟動選項。
- **進入維護模式、套用更新，然後重新啟動。**  
主機進入維護模式。如果主機無法進入維護模式，代表主機未重新啟動，會在下次重新開機時套用更新。選取**韌體更新完成後結束維護模式**核取方塊，在更新後結束維護模式。
  - **在下次重新開機時套用更新。**  
為避免服務中斷，建議主機先進入維護模式再重新開機。
  - **套用更新，不進入維護模式就強制重新開機。**  
套用更新，即使主機未處於維護模式中也重新開機。不建議使用此方法。
6. 按一下 **Finish** (完成)。
7. 若要確認更新成功，請在「Dell 管理中心」中選取 **工作佇列** → **清查歷程記錄** → **立即執行**，然後檢閱 **Dell 管理中心概覽** 頁面，查看新版本。

## 更新舊版韌體

要能執行韌體更新精靈，韌體必須位於一定層級。如非此情形，在執行韌體更新精靈前，將提供您選項以協助更新您的韌體。於 2010 年 10 月 14 日後更新的韌體可執行韌體更新精靈。韌體更新係由主機 OpenManage 整合標籤上的 vSphere 用戶端執行。若要設定儲存庫，請參閱 [設定韌體儲存庫](#)。

若要更新舊版韌體：


1. 在 **vSphere 用戶端 OpenManage Integration** 索引標籤的**主機**的動作，按一下**執行韌體更新精靈**。  
若您的主機層級低於精靈所支援的層級，將顯示「必要更新」對話方塊。
2. 在**必要更新**對話方塊中，執行下列其中一項動作：
  - 若要在韌體更新後自動結束維護模式，請選取**韌體更新完成後結束維護模式**核取方塊。
  - 若要進入維護模式檢查及/或測試機器，再將機器加回叢集，請勿勾選這個核取方塊。
3. 按一下 **Update** (更新)。
4. **成功**對話方塊會顯示更新正在進行中。  
如果選擇**韌體更新完成後結束維護模式**，韌體更新會讓主機進入維護模式，然後自動重新啟動。否則，主機會留在維護模式。
5. 請參閱 vSphere 用戶端**最近的工作區域**，查看更新進度。  
在這個程序之後，再次執行韌體更新精靈，確定韌體已完全更新。


## 為叢集與資料中心執行更新韌體精靈

這項功能僅適用於搭載 iDRAC Express 或 iDRAC Enterprise 之第 11 代以後的 Dell 伺服器。如果韌體是在 2010 年 10 月 14 日之後安裝，您可以使用韌體更新精靈自動更新韌體版本。此精靈只會更新屬於連線設定檔

且韌體、CSIOR 狀態、Hypervisor 和 OMSA 狀態相容的主機 (僅限於第 11 代伺服器)。如果清單中沒有您的主機，請從 OpenManage Integration for VMware vCenter 為 vSphere 主機執行遵循精靈，或是從主機和叢集檢視選取未列出的主機，然後使用韌體更新精靈。更新每個主機的韌體元件通常需要 30 至 60 分鐘。在叢集啟用 DRS，主機在韌體更新程序進入/離開維護模式時，才能移轉虛擬機器。您一次僅能排程或執行一個韌體更新工作。

如果要從精靈匯出，請使用 **匯出至 CSV** 按鈕。搜尋可供尋找特定叢集、資料中心、主機或 DataGrid 的任何主題，已套用日期除外。


 **註:** 請務必和儲存庫配套一起更新韌體：BIOS、iDRAC 和 Lifecycle Controller。

 **註:** 如需變更預設逾時設定的資訊，請參閱 *使用者指南*「疑難排解」一節的按一下韌體更新連結後為什麼顯示錯誤訊息。

您可以從 **工作佇列** 頁面檢視狀態和管理韌體更新工作。請參閱 [檢視叢集與資料中心的韌體更新狀態](#)。

1. 在 **vSphere 用戶端** 的 **清查** 標題下，選取 **主機與叢集**。
2. 在 **主機與叢集** 的樹狀圖中，先選取資料中心或叢集，然後選取 **OpenManage Integration** 索引標籤。
3. 按一下 **更新韌體**。  
如果此連結未啟用，或是在按一下此選項時出現快顯訊息，就表示有進行中或已排定的韌體更新工作，請先關閉對話方塊、稍候片刻，然後再試一次。在韌體更新工作索引標籤的工作佇列中，檢視所有工作的狀態。
4. 在 **歡迎** 頁面上，先檢查更新相關資訊，再繼續使用精靈。
5. 按一下 **下一步**。
6. 在 **韌體清查** 頁面中，檢查系統已安裝的元件。
7. 按一下 **下一步**。
8. 在 **選取更新配套** 頁面中，使用核取方塊選取更新配套。  
 **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。
  - 搭載任何 iDRAC 版本的第 11 代主機不支援 64 位元配套。
9. 按一下 **下一步**。
10. 在 **選取要更新的系統/元件** 頁面，請使用核取方塊選取要升級或降級的元件。如果您要降級，請選取 **允許元件降級** 核取方塊。  
 **註:** 如果您已選取所有元件，但卻還有一些元件依然顯示未選取，就表示那些元件沒有可用的升級。若要降級，可以選取那些元件。
11. 按一下 **下一步**。
12. 在 **韌體更新資訊** 頁面中，檢查選取為要升級或降級的元件。
13. 按一下 **下一步**。
14. 在 **排程韌體更新** 頁面中，在工作名稱下，請執行以下操作：
  - a. 在韌體更新工作名稱文字方塊中，輸入 **韌體更新工作名稱**。  
這是必填欄位。如果未填入，就不會排程這項升級。請勿使用已使用中的名稱。如果清除這個名稱，就可以再次重複使用。
  - b. 在韌體更新說明中，輸入 **說明**。
15. 在工作排程下，請執行下列其中一項動作：  
 **註:** 選取必要選項。如果有必要選項未選取，升級就會遭到封鎖。
  - 如果想要立即執行更新工作，請按一下 **立即更新**，然後按一下 **完成**。

- 如果想要稍後執行更新工作，請按一下**排程更新**，然後執行以下操作：
  1. 在行事曆方塊中，選取**月份和日期**。
  2. 在時間文字方塊中，以小時:分鐘格式輸入**時間**，然後按一下**完成**。

 **註:** 此時間是用戶端實際位置的當地時區。無效時間值會導致更新被封鎖。

### 檢視叢集與資料中心的韌體更新狀態

針對要在這個頁面顯示的資訊，請執行叢集或資料中心的韌體更新。這個頁面只會顯示叢集與資料中心韌體更新的相關資訊。請參閱[為叢集與資料中心執行更新韌體精靈](#)。在這個頁面，您可以重新整理、清除或中止您的韌體更新工作。

1. 從 Dell 管理中心選取**工作佇列** → **韌體更新工作**。
2. 若要顯示最新資訊，請按一下**重新整理**。
3. 檢視 DataGrid 中的狀態。此格線會提供韌體更新工作的下列相關資訊：
  - Status (狀態)
  - 排定的時間
  - Name
  - 說明
  - 集合大小  
集合大小是此韌體清查工作上的伺服器數量。
  - 進度摘要  
進度摘要列出此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 DataGrid 按一下**詳細資料**。您可以在這裡找到下列詳細資料：
  - Service Tag
  - iDRAC IP
  - Status (狀態)
  - 警告
  - 韌體更新工作詳細資料
  - 開始時間
  - 結束時間。
5. 如果您想要中止未執行的排程韌體更新，在您要中止之工作的同一行按一下**中止**。
6. 如果要清除排程韌體更新，請按一下**清除工作佇列**。  
您只能清除完成或排定的工作。
7. 選取**早於日期和工作狀態**，然後按一下**套用**。選定工作隨即從佇列清除。

## 使用 vCenter 執行進階主機管理

進階主機管理工作是以主機系統為基礎的動作，可讓系統管理員識別資料中心環境中的實體伺服器、啟動以伺服器為基礎的管理工具，以及顯示伺服器保固資訊。您可透過 vCenter 的「OpenManage Integration」索引標籤，或是針對個別主機系統在**主機與叢集**檢視中用滑鼠右鍵按一下主機，以啟動這些所有動作。

## 設定實體伺服器前方指示燈

您可以將前指示燈設定為閃爍一段設定時間，協助在大型資料中心環境找到實體伺服器。

設定實體伺服器前方指示燈：

1. 在**清查**標題下方的 **vSphere 用戶端** 中，選取**主機與叢集**。
2. 從樹狀檢視畫面的**主機與叢集**選取主機系統，然後再選取 **OpenManage Integration** 索引標籤。
3. 在 **Host Actions (主機動作)** 選取 **Blink Indicator Light (閃爍指示燈)**。
4. 請選擇下列其中一個選項：
  - 若要開啟閃爍並設定時段，在 **Indicator Light (指示燈)** 對話方塊中，按一下 **Blink On (開啟閃爍)**，然後使用 **Timeout (逾時)** 下拉式清單選取逾時增加大小，然後按一下 **OK (確定)**。
  - 若要關閉閃爍，在 **Indicator Light (指示燈)** 對話方塊中，按一下 **Blink Off (關閉閃爍)**，然後按一下 **OK (確定)**。

## 以伺服器為基礎的管理工具

提供 iDRAC 與 OMSA 兩種以伺服器為基礎的管理工具，其可透過 **vSphere 用戶端** → **OpenManage 整合索引標籤**來啟動。您可在左窗格的「管理主控台」連結下方，存取以下項目：

- 啟動遠端存取。  
使用此選項以啟動 iDRAC 使用者介面
- 啟動 OMSA  
使用此選項以啟動 OpenManage Server Administrator 使用者介面 URL，其已在執行初始「組態精靈」或使用**設定** → **一般**時輸入至管理中心。您必須在 Windows 管理站上，安裝伺服器管理員網頁伺服器的 URL。
- 若您位於刀鋒系統，則啟動 CMC 時會啟動「機箱管理控制器」使用者介面。若您並非位於刀鋒系統，則不會顯示此項目。

## 保固擷取

保固擷取針對 Dell 伺服器提供下列資訊：

- 更新服務保固資訊 (僅會傳送主機服務標籤)
- 系統會依排定間隔更新保固資訊
- 使用 Proxy 伺服器與認證進行傳輸加密處理

 **註:** Dell 不會儲存已傳輸的服務標籤資訊。

**相關工作：**

- [執行保固擷取工作](#)
- [檢視單一主機的伺服器保固資訊](#)
- [檢視整體資料中心的保固資訊](#)

## 檢視整體資料中心的伺服器保固資訊

保固工作完成後，您即可在「資料中心檢視」頁面上檢視 vSphere 用戶端的伺服器保固資訊。

檢視整體資料中心的伺服器保固資訊：

1. 從**清查**標題下方的 vSphere 用戶端，選取**主機與叢集**。
2. 從樹狀檢視畫面的**主機與叢集**選取資料中心，然後再選取 **OpenManage 整合**索引標籤。
3. 隨即顯示資料中心內所有主機的概觀。在「檢視」下拉式清單中選取**保固**。
4. 在**篩選**文字方塊中，輸入保固資料的篩選。
5. 若要重新整理顯示的清查，請按一下**重新整理**。
6. 若要將清查匯出為 CSV 檔案，請按一下**匯出**。在「下載位置」視窗中，瀏覽至儲存清查的位置，然後按一下**儲存**。

### 檢視單一主機的伺服器保固資訊

保固工作完成後，您即可在「主機檢視」頁面上檢視 vSphere 用戶端的單一主機保固資訊。

檢視單一主機的伺服器保固資訊：

1. 從 vSphere 用戶端，**清查**標題下方選取**主機與叢集**。
2. 從樹狀檢視畫面的**主機與叢集**選取主機系統，然後再選取 **OpenManage Integration** 索引標籤。
3. 若要顯示系統保固資訊，請選取**保固**。「保固狀態」頁面上的資訊包括：
  - 保固供應商名稱與保固說明
  - 保固的開始與結束日期，以及其剩餘天數
  - 保固狀態 (作用中、已過期)，以及上次更新保固資訊的時間

# 硬體管理

## 先決條件：

實體伺服器必須出現在部署精靈，才能成功執行硬體佈建和部署。所有實體伺服器都必須符合下列先決條件：


- 特定硬體支援資訊請參閱 *OpenManage Integration for VMware vCenter 發行公告*。
- 伺服器必須有最低支援版本的 iDRAC 韌體、Lifecycle Controller 和 BIOS。特定硬體支援資訊請參閱 *OpenManage Integration for VMware vCenter 發行公告*。
  - **註:** 如果韌體版本過期，可能需要執行兩步驟的升級程序。如需詳細的升級說明，請參閱韌體說明文件。
- OpenManage Integration for VMware vCenter 支援僅使用嵌入式/整合式 LOM 部署。部署後，您可以在 PCI 插槽手動設定 NIC。如果使用附加的 NIC，系統必須啟用主機 LOM。
- OpenManage Integration for VMware vCenter 允許部署到 Internal Dual SD Module (僅適用 Hypervisor) 或本機硬碟機上。您必須先從 BIOS 啟用 Internal Dual SD Module，才能以 OpenManage Integration for VMware vCenter 部署 Hypervisor。您可以手動變更管理 NIC，並將系統新增至 vCenter。
  - **註:** 請參閱個別伺服器產品說明文件，瞭解支援的 Dual SD Module。
- 如果 iDRAC 處於專用模式，必須啟用其 NIC，才能與 OpenManage Integration for VMware vCenter 通訊。
- CSIOR 一定要啟用。此外，起始自動探索前，為確定擷取的是最新資料，必須先完全關閉系統電源再開啟 (硬式重新開機)。
- 訂購 Dell 伺服器時，可在出廠時預先設定自動探索和信號交換選項。如果伺服器沒有用這些選項預先設定，就必須手動輸入 OpenManage Integration for VMware vCenter IP 位址或設定本機網路，提供這項資訊。
- 如果硬體組態沒有使用 OpenManage Integration for VMware vCenter，那麼請先確定下列條件皆已符合，再起始 Hypervisor 部署：
  - 在 BIOS 啟用 VT (虛擬化技術) 旗標。
  - 針對作業系統安裝，將系統的開機順序設為可開機虛擬磁碟或 Internal Dual SD Module。
- 如果硬體組態使用了 OpenManage Integration for VMware vCenter，即使 BIOS 組態不是硬體設定檔的一部份，也會自動啟用 VT 的 BIOS 設定。如果目標系統上沒有虛擬磁碟，就需要用到 Express/Clone RAID 組態。
- 如果伺服器版本比 Dell PowerEdge 第 12 代伺服器舊，那麼部署程序會在目標系統安裝 OpenManage Server Administrator 套件，並自動將 SNMP 設陷目的地設為指向 OpenManage Integration for VMware vCenter。
- 部署需要包含所有 Dell 驅動程式的自訂 ESXi 影像。前往 Dell 驅動程式與下載頁面，將自訂影像儲存到部署程序可存取的位置，即可找到正確的影像。此版本最新的支援 ESXi 版本清單，請參閱發行公告。
- *OpenManage Integration for VMware vCenter* 僅支援 BIOS 模式在目標伺服器上自動部署 Hypervisor。確定您在參考硬體設定檔中選擇 BIOS 模式，然後再套用 Hypervisor 設定檔。如果沒有選取的硬體設定檔，請確定手動設定開機模式為 BIOS 並重新啟動伺服器，然後再套用 Hypervisor 設定檔。
  - **註:** 如果目標機器的啟動模式設為 UEFI，就無法從 OpenManage Integration for VMware and vCenter (OMIV) 部署作業系統

## 佈建概觀

完成資料中心的實體清查後，所有自動探索的裸機系統皆可供 OpenManage Integration for VMware vCenter 執行零接觸硬體佈建與 Hypervisor 部署作業。若要準備佈建部署，您必須：

- 建立硬體設定檔** 包含從參考伺服器所收集的硬體設定，其會用於部署新伺服器。請參閱「[建立新硬體設定檔](#)」。
- 建立 Hypervisor 設定檔** 包含 ESXi 部署所需的 Hypervisor 安裝資訊。請參閱「[建立新 Hypervisor 設定檔](#)」。
- 建立部署範本** 您可選擇性地包含硬體設定檔、Hypervisor 設定檔或兩者兼備。您可視需要針對所有可用的資料中心伺服器儲存及重複使用這些設定檔。請參閱「[建置部署範本](#)」。

建立部署範本後，使用「部署精靈」收集建立排程工作所需的資訊，以在 vCenter 中佈建伺服器硬體和部署新主機。如需關於執行「部署精靈」的資訊，請參閱「[執行部署精靈](#)」。最後，請使用「工作佇列」檢視工作狀態，並變更擱置中的部署工作。

 **註：**您無法排程連續執行多個部署工作，多個工作應使用排程功能以錯開部署執行時間。

## 瞭解部署工作時間

佈建和部署裸機伺服器可能需要 30 分鐘至數小時方可完成，根據特定因素而定。開始執行部署工作時，建議您根據提供的指導方針規劃部署時間。完成佈建與部署所需耗費的時間，會依部署類型、複雜度以及同時執行的部署工作數量而異。下表為您提供部署工作所需約略時間的指導方針。執行批次部署工作時最多可同時處理五部伺服器，以改善整體部署工作的時間。同時處理工作的精確數量取決於可用資源。

表 3. 大約部署時間案例

部署類型	每項部署的大約時間
僅限 Hypervisor	30 分鐘至 130 分鐘
僅限硬體	根據複雜度以及要設定的 RAID、BIOS 和開機選項而定，最長可能需要 2 小時
Hypervisor 與硬體設定檔	1 至 4 小時


## 部署順序中的伺服器狀態

執行清查工作時，系統會將自動探索的裸機系統歸類為各種不同狀態，以協助判斷伺服器是否為新加入資料中心，或是具有擱置中的已排程部署工作。管理員可使用這些狀態，判斷是否應在部署工作中包含伺服器，這些狀態包括：

- 未設定** 伺服器已與 OpenManage Integration for VMware vCenter 連線並靜待設定。請參閱「[瞭解部署工作時間](#)」。
- 已設定** 伺服器已設定順利完成 Hypervisor 部署所需的全部硬體資訊。

## 下載自訂 Dell ISO 映像


自訂包含部署所需之全部 Dell 驅動程式的 ESXi 映像。

 **註:** OpenManage Integration for VMware vCenter ISO 未包含部署所需的 ESXi ISO 映像。您必須將這些映像下載至可於部署時存取的位置，否則部署可能會失敗。

1. 導覽至 [support.dell.com](http://support.dell.com)。
2. 瀏覽至您所用語言的**驅動程式與下載**頁面，然後執行下列其中一項動作：
  - 若要使用「服務標籤」或「快速服務代碼」選取驅動程式，請在**是**下方的文字方塊中，輸入服務標籤或快速服務代碼，然後按一下**提交**。
  - 若要使用其他選項選取驅動程式，請在**否**下方選取下列其中一個項目：
    - Automatically detect my Service Tag for me (自動偵測我的服務標籤)
    - Choose from My Products and Services List (從我的產品和服務清單中選擇)
    - Choose from a list of all Dell products (從所有 Dell 產品清單中選擇)

然後按一下**繼續**，並遵循所選選項的指示進行。


3. 在所選伺服器的頁面上，向下捲動至**縮小結果範圍**，並在**作業系統**下方，使用下拉式清單選取您需要的 ESXi 系統。
4. 按一下**企業解決方案**。
5. 在**企業解決方案**清單中，選取所需 ISO 的版本，然後按一下**下載檔案**。


 **註:** 嵌入式 ISO 適用於「雙內部 SD 模組」上的 Hypervisor 安裝。安裝式 ISO 適用於硬碟上的安裝。

6. 在對話方塊中，選取**透過瀏覽器的單一檔案下載**，然後再按一下**立即下載**。
7. 在對話方塊中，瀏覽至儲存供部署用途 ISO 映像的位置。


## 瞭解如何設定硬體設定檔

若要設定伺服器硬體設定，您必須建立硬體設定檔。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：

<b>開機順序</b>	開機順序是指啟動裝置順序和硬碟機順序，啟動模式設為 BIOS 時才可供編輯。
<b>BIOS 設定</b>	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。
<b>iDRAC Settings</b>	iDRAC 設定包括：網路、使用者清單與使用者組態 (IPMI/iDRAC 權限)。  <b>註:</b> 如果是有 iDRAC Express 的系統，iDRAC 組態無法解壓縮，因此請勿將伺服器當成參考伺服器用。如果是當成目標系統用，那麼凡是參考伺服器的 iDRAC 組態都不會套用。
<b>RAID 組態</b>	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。

 **註:** 硬體設定檔設定了兩個 RAID 組態選項：

- *適用時，套用 RAID1+ 建立專用熱備援。* 如果要在目標伺服器套用預設的 RAID 組態設定，請使用此選項。在支援 RAID1 之整合式控制器的前兩個磁碟機，RAID 組態工作預設為 RAID1。此外，如果有符合條件的候選磁碟機，就會為 RAID1 陣列建立專用熱備份磁碟。
- *從參考伺服器複製 RAID 組態，如下所示。* 如果要複製參考伺服器設定，請使用此選項。請參閱[建立新硬體設定檔](#)。

 **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 處理器群組中的若干 BIOS 設定。使用參考伺服器建立新硬體設定檔之前，參考伺服器必須先啟用 Collect System Inventory On Reboot (CSIOR) 設定，然後重新啟動，才能提供準確的清查與組態資訊。

建立硬體設定檔的工作包括：

- [在參考伺服器啟用 CSIOR](#)
- [建立新硬體設定檔](#)
- [複製硬體設定檔](#)
- [關於管理硬體設定檔](#)


## 建立新硬體設定檔

若要建立新硬體設定檔：

1. 在「Dell 管理中心」，選取**部署** → **部署範本** → **硬體設定檔**。
  2. 按一下**新建**。
  3. 在**新硬體設定檔**頁面，請執行下列動作：
    - 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，輸入選填說明。
  4. 按一下 **Save** (儲存)。
  5. 若要繼續，請在左窗格中按一下**參考伺服器**。
  6. 在「參考伺服器」視窗中，按一下**編輯**。
  7. 若要尋找相容、由 vCenter 管理，並由 OpenManage Integration for VMware vCenter 成功清查的參考伺服器，請按一下**瀏覽**。
  8. 在**伺服器**對話方塊中，向下捲動清單找到正確的參考伺服器，然後按一下**選取**。
  9. 若要自訂參考伺服器設定做為預設值，請按一下**從參考伺服器自訂設定**，然後再按一下**儲存**。
  10. 此時會顯示一個對話方塊指出擷取設定需要數分鐘的處理時間。若要產生設定，請按一下**繼續**。在**參考伺服器視窗**中，會顯示所選伺服器的名稱、iDRAC IP 位址和伺服器標籤。
  11. 在左窗格中，選取**開機順序**。若要在設定檔中包含開機順序資訊，請選取**包含此硬體設定檔中的開機順序**核取方塊。
  12. 若要顯示開機順序選項，請展開**開機順序**，然後按一下**編輯**以進行更新：
    -  **註:** 適用於 Dell 第 13 代 PowerEdge 伺服器，針對硬體設定檔僅會顯示目前的開機模式詳細資料。
    -  **註:** 若將處於目標機器的「開機」模式設為 UEFI，則無法從 OpenManage Integration for VMware and vCenter 執行作業系統部署。
- a. 在**開機模式**下拉式清單中，選取「BIOS」或「UEFI」。


- b. 在**檢視 / 設定**下拉式清單的**開機裝置順序**下方，變更顯示的開機裝置順序，選取裝置，然後再按一下**上移**或**下移**。
  - c. 在**開機重試順序**下拉式清單中，選取**啟用**以讓伺服器自動重試開機順序，或是選取**停用**不重試此順序。
  - d. 按一下**儲存**以儲存變更，或是按一下**取消**以取消變更。
13. 若已選取 **BIOS 開機模式**，則您可展開**硬碟機順序**以顯示硬碟機順序選項，然後按一下**編輯**以進行更新：
- 若要變更硬碟機顯示順序，請選取裝置並按一下**上移**或**下移**。
  - 按一下**儲存**以儲存變更，或是按一下**取消**以取消變更。
14. 在左窗格中，選取 **BIOS 設定**。若要在設定檔中包含 BIOS 設定資訊，請選取**在此硬體設定檔中包含 BIOS 設定**核取方塊。展開類別以顯示設定選項，然後按一下**編輯**以更新下列其中一個項目：
- Memory Settings
  - Processor Settings
  - SATA Settings
  - Integrated Devices
  - Serial Communication
  - Embedded Server Management (嵌入式伺服器管理)
  - Power Management (電源管理)
  - System Security
  - Miscellaneous Settings

完成類別的所有更新後，請按一下**套用**以儲存變更，或是按一下**取消**以取消變更。


 **註：**如需詳細 BIOS 資訊 (包括設定選項與說明)，請參閱選定伺服器的「**硬體擁有者手冊**」。

15. 在左窗格中選取 **iDRAC 設定**，然後選取**網路**。
16. 若要在設定檔中包含網路設定資訊，請選取**在此硬體設定檔中包含 BIOS 設定**核取方塊。展開類別以顯示設定選項，然後按一下**編輯**以更新下列其中一個項目：
- 網路
  - 網路設定
  - 虛擬媒體

完成類別的所有更新後，請按一下**套用**以儲存變更，或是按一下**取消**以取消變更。

 **註：**如需詳細 iDRAC 資訊 (包括設定選項與說明)，請參閱選定伺服器的「**iDRAC 使用者手冊**」。

17. 在左窗格中，選取 **iDRAC 設定** → **使用者清單**。若要在設定檔中包含使用者清單資訊，請選取**在此硬體設定檔中包含使用者清單**核取方塊。在「iDRAC 本機使用者清單」下方，執行下列其中一項動作：
- a. **新增使用者：**手動輸入 iDRAC 使用者和必要資訊。完成後，按一下**儲存**以儲存變更，或是按一下**取消**以取消。
  - b. **刪除使用者：**刪除選取的使用者。選取使用者的核取方塊，然後按一下**刪除**，或是按一下**取消**以取消。
  - c. **編輯使用者：**手動輸入 iDRAC 使用者資訊。完成後，按一下**儲存**以儲存變更，或是按一下**取消**以取消。

 **註：**如需詳細 iDRAC 資訊 (包括設定選項與說明)，請參閱選定伺服器的「**iDRAC 使用者手冊**」。

18. 在左窗格中，選取 **RAID 組態**。若要在設定檔中包含 RAID 組態資訊，請選取**在此硬體設定檔中包含 RAID 組態**核取方塊。然後選取下列其中一個項目：
- 套用 RAID1+ 建立專用熱備援 (若適用)。

若您想要套用預設 RAID 組態設定至目標伺服器，請使用此選項。RAID 組態工作預設為 RAID1 相容整合式控制器之前兩個磁碟機上的 RAID1。此外，若存有符合條件的候選磁碟機，則會為 RAID1 陣列建立專用熱備援。

- 從參考伺服器複製 RAID 組態。  
若您想要複製參考伺服器設定，請使用此選項。

系統會自動儲存設定檔，然後在**可用設定檔**下方的**硬體設定檔**視窗中顯示該設定檔

## 在參考伺服器啟用 CSIOR

用參考伺服器建立硬體設定檔前，先啟用「在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 的方式有兩種：

<b>本機</b>	這個方式採用使用 Dell Lifecycle Controller United Server Configurator (USC) 使用者介面的個別主機。
<b>遠端</b>	這個方式採用 WS-MAN 指令碼。如需以指令碼處理此功能的更多資訊，請參閱 <i>Dell 技術中心</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，在 POST 期間按下 **<F10>** 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。

## 複製硬體設定檔

複製新的硬體設定檔：

1. 在 Dell 管理中心，選擇**部署** → **部署範本** → **硬體設定檔**。
2. 按一下**新建**。
3. 在**新硬體設定檔**頁面，請執行下列動作：
  - 在 **Profile Name (設定檔名稱)** 文字方塊中，輸入設定檔名稱。
  - 在 **Description (說明)** 文字方塊中，輸入選填的說明。
4. 按一下 **Save** (儲存)。
5. 在左窗格中，按一下**參考伺服器**。
6. 在**參考伺服器**視窗中，按一下 **編輯**。
7. 若要從參考伺服器擷取所有的硬體設定，請按一下**複製參考伺服器設定**選項按鈕。
8. 按一下**儲存**。
9. 此時會顯示一個對話方塊指出擷取設定需要數分鐘的處理時間。若要產生設定，請按一下**繼續**。此時會填入設定，並在「參考伺服器」視窗中顯示所選伺服器的名稱、iDRAC IP 位址和伺服器標籤。  
系統會儲存設定檔，然後在**可用設定檔**下方的**硬體設定檔**視窗中顯示該設定檔。

## 關於管理硬體設定檔

硬體設定檔使用參考伺服器定義伺服器的硬體組態。您可透過「Dell 管理中心」為現有硬體設定檔執行數種管理動作，包括：

- [檢視或編輯硬體設定檔](#)
- [複製硬體設定檔](#)

- [複製硬體設定檔](#)
- [刪除硬體設定檔](#)
- [重新整理硬體設定檔](#)

## 檢視或編輯硬體設定檔

檢視或編輯硬體設定檔：

1. 在「Dell 管理中心」，選取**部署** → **部署範本** → **硬體設定檔**。
2. 選取一個設定檔，然後按一下**檢視 / 編輯**。
3. 在**硬體設定檔**視窗中進行任何變更，然後按一下**編輯**。
4. 按一下**儲存**以套用變更，或是按一下**取消**以取消變更。

## 複製硬體設定檔

複製硬體設定檔：

1. 在「Dell 管理中心」，選取**部署** → **部署範本** → **硬體設定檔**。
2. 在**硬體設定檔**頁面上選取設定檔，然後按一下**複製**。
3. 在**複製**對話方塊中，輸入唯一的硬體設定檔名稱。
4. 按一下**套用**以使用新名稱建立設定檔複本，或是按一下**取消**以取消。


## 重新命名硬體設定檔

重新命名硬體設定檔：

1. 在 Dell 管理中心，選擇**部署** → **部署範本** → **硬體設定檔**。
2. 在**硬體設定檔**頁面上選取設定檔，然後按一下**重新命名**。
3. 在**重新命名**對話方塊中，輸入唯一的硬體設定檔名稱。
4. 按一下**套用**以使用新名稱，或是按一下**取消**以取消。

## 刪除硬體設定檔

若想刪除硬體設定檔：

 **註:** 刪除的硬體設定檔，若為執行部署工作的一部份，可能會導致工作失敗。

1. 在 Dell 管理中心，選擇**部署** → **部署範本** → **硬體設定檔**。
2. 選擇設定檔，然後按一下**刪除**。
3. 在「訊息」對話方塊，如要移除設定檔，按一下**刪除**，或按一下 **Cancel** 取消。

## 重新整理硬體設定檔

若要重新整理更新硬體設定檔：

1. 在「Dell 管理中心」，選取**部署** → **部署範本** → **硬體設定檔**。
2. 按一下**重新整理**。  
顯示更新的硬體設定檔資訊。

## 建立新 Hypervisor 設定檔

若要在伺服器部署與設定 ESXi，必須建立 Hypervisor 設定檔。Hypervisor 設定檔需要的資訊如下：

- NFS 或 CIFS 共用上，可編寫指令碼的參考 ISO 軟體媒體的位置
- 管理部署主機 vCenter 例項，以及可選的主機設定檔
- 外掛程式在 vCenter 部署伺服器的目的地叢集或資料中心



**註：**參考 ISO 檔案名稱請使用下列其中一個命名慣例：

NFS 格式：`host:/share/hypervisor_image.iso`

CIFS 格式：`\\host\share\hypervisor.iso`

若想建立新的 Hypervisor 設定檔：

1. 在 **Dell 管理中心**，選取 **部署** → **部署範本** → **Hypervisor 設定檔**。
  2. 在 **Hypervisor 設定檔** 頁面中，按一下 **新建立**。
  3. 在 **新 Hypervisor 設定檔** 頁面，請執行以下操作：
    - 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，輸入選填的說明。
  4. 在左窗格按一下 **參考 ISO**，然後按一下 **編輯**，並在 **Hypervisor 安裝來源** 對話方塊輸入下列資訊：
    - 在 **安裝來源 ISO** 文字方塊中，輸入 Hypervisor 共用位置的路徑。此 Hypervisor 影像的複本經過修改，允許執行指令的安裝。參考 ISO 位置必須使用下列格式之一：
      - NFS 格式：`host:/share/hypervisor_image.iso`
      - CIFS 格式：`\\host\share\hypervisor.iso`
    - 在 **選取版本** 下拉式清單，選取 ESXi 版本。
- 使用此 Hypervisor 設定檔部署的所有伺服器都有這個影像，而且如果伺服器是第 12 代之前的版本，就會安裝最新建議版本的 OpenManage Server Administrator。
5. 如果使用的是 CIFS 共用，請輸入 **使用者名稱**、**密碼** 和 **確認密碼**。密碼必須相符。
  6. 若要新增設定至設定檔，請按一下 **儲存**。
  7. 在左窗格中，按一下 **vCenter 設定**，然後編輯必要的地方：
    - **vCenter 例項**：部署後顯示管理主機的伺服器例項。
    - **vCenter 版本**：顯示目前的版本。
    - **vCenter 目的地容器**：託管新實體伺服器的資料中心或叢集；按一下 **瀏覽**，搜尋 vCenter 目的地。
    - **vCenter 主機設定檔**：選取封裝主機組態並協助管理主機組態的設定檔。
  8. 若要新增資訊至設定檔，請按一下 **儲存**。

如需管理 Hypervisor 設定檔的資訊，請參閱 [管理 Hypervisor 設定檔](#)。

## 管理 Hypervisor 設定檔

您可針對現有的 Hypervisor 設定檔執行數項管理動作，包括：

- [瞭解 VLAN 支援](#)
- [檢視或編輯 Hypervisor 設定檔](#)
- [複製 Hypervisor 設定檔](#)

- [重新命名 Hypervisor 設定檔](#)
- [刪除 Hypervisor 設定檔](#)
- [重新整理 Hypervisor 設定檔](#)

## VLAN Support

OpenManagement Integration for VMware vCenter 支援將 Hypervisor 部署至可路由的 VLAN。在「部署精靈」中設定 VLAN 支援。在此「部署精靈」部分，提供指定 VLAN 用途以及指定 VLAN ID 的選項。若提供 VLAN ID，則其在部署時會套用至 Hypervisor 的管理介面，並使用 VLAN ID 標記所有流量。

確定部署時所提供的 VLAN 與虛擬設備和 vCenter 伺服器進行通訊。將 Hypervisor 部署至 VLAN 時若無法與以上其中一個或所有目的地進行通訊，則會導致部署失敗。

若您已在單一部署工作中選取多個裸機伺服器，且想將相同的 VLAN ID 套用至所有伺服器，請在「部署精靈」之「伺服器識別」部分的「預設設定」下方，使用**套用設定至所有選取的伺服器**按鈕。此選項可讓您將相同的 VLAN ID 連同其他網路設定，套用至該部署工作中的所有伺服器。

**註:** OpenManagement Integration for VMware vCenter 不支援多重主目錄組態。若將第二個網路介面新增至此設備以與第二個網路進行通訊，則會引發諸如 Hypervisor 部署、伺服器規範和韌體更新的相關工作流程問題。

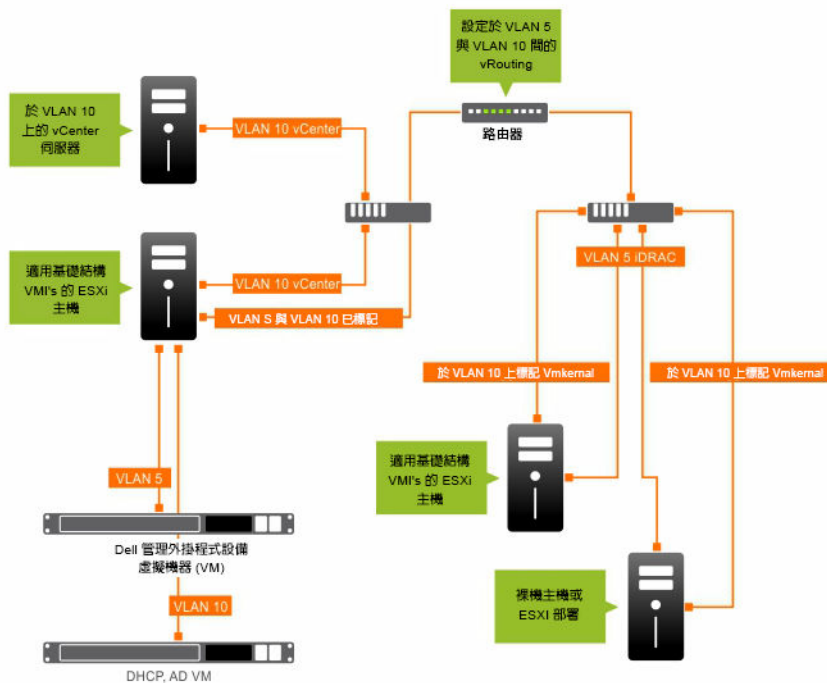


圖 4. 範例 VLAN 網路。

在此範例網路中，OpenManagement Integration for VMware vCenter 係位於 VLAN5 上，且在 VLAN 10 上部署 ESXi 主機的 vCenter 和 VMkernel。由於 OpenManagement Integration for VMware vCenter 不支援多重 VLAN 主目錄，因此 VLAN5 必須路由至所有系統的 VLAN10 方可彼此正確通訊。若未啟用這些 VLAN 間的路由，則會導致部署失敗。

## 檢視或編輯 Hypervisor 設定檔

若要檢視或編輯 Hypervisor 設定檔：

1. 在 Dell 管理中心，選取 **部署** → **部署範本** → **Hypervisor 設定檔** 視窗。
2. 選取一個設定檔，然後按一下 **檢視 / 編輯**。
3. 在 **Hypervisor 設定檔：設定檔名稱** 視窗中，選取要顯示或變更的設定檔區段，然後進行任何必要的變更。
4. 按一下 **儲存** 套用變更，或是若要取消，請按一下 **取消**。

## 複製 Hypervisor 設定檔

若想複製 Hypervisor 設定檔：

1. 在「Dell 管理中心」，選取 **部署** → **部署範本** → **Hypervisor 設定檔**。
2. 在 **Hypervisor 設定檔** 頁面上選取一個設定檔，然後按一下 **複製**。
3. 在 **複製** 對話方塊中，輸入唯一的 Hypervisor 設定檔名稱。
4. 按一下 **套用** 以使用新名稱建立設定檔複本，或是按一下 **取消** 以取消。


## 重新命名 Hypervisor 設定檔

重新命名 Hypervisor 設定檔：

1. 在「Dell 管理中心」，選取 **部署** → **部署範本** → **Hypervisor 設定檔**。
2. 在 **Hypervisor 設定檔** 頁面上選取一個設定檔，然後按一下 **重新命名**。
3. 在 **重新命名** 對話方塊中，輸入唯一的 Hypervisor 設定檔名稱。
4. 按一下 **套用** 以使用新名稱，或是按一下 **取消** 以取消。

## 刪除 Hypervisor 設定檔

若想刪除超管理器設定檔：

 **註：**刪除是執行部署工作的一部份的 Hypervisor 設定檔，可能導致工作失敗。

1. 在「Dell 管理中心」，選取 **部署** → **部署範本** → **Hypervisor 設定檔**。
2. 選擇設定檔，然後按一下 **刪除**。
3. 在訊息對話方塊中，按一下 **刪除** 以移除設定檔，或是按一下 **取消** 以取消。

## 重新整理 Hypervisor 設定檔

重新整理 Hypervisor 設定檔：

1. 在 Dell 管理中心，選擇 **部署** → **部署範本** → **Hypervisor 設定檔**。
2. 按一下 **重新整理**。  
顯示更新的 Hypervisor 設定檔資訊。

## 建立新部署範本

部署範本包含硬體設定檔、Hypervisor 設定檔或兩者都有。部署精靈用這個範本佈建伺服器硬體，以及在 vCenter 部署主機。

若要建立新部署範本：

1. 在 Dell 管理中心選取**部署** → **部署範本**。
2. 在**可用設定檔**下按一下**新建立**。
3. 在**新建立**視窗輸入範本名稱，然後按一下**儲存**。
4. 若要完成範本，按一下**編輯**。
5. 在右窗格的**設定檔**下拉式清單選擇設定檔，然後執行下列其中一項動作：
  - 若要顯示選取之設定檔的硬體/Hypervisor 設定檔設定，請按一下**檢視**。
  - 若要建立新的硬體/Hypervisor 設定檔，請按一下**新建立**。
6. 輸入部署範本的選填**說明**，有助於管理範本。
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

您可透過「Dell 管理中心」，針對現有的部署範本執行數項管理動作，包括：

- [建置部署範本](#)
- [複製部署範本](#)
- [重新命名部署範本](#)
- [刪除部署範本](#)

### 複製部署範本

複製部署範本：

1. 在「Dell 管理中心」，選取**部署** → **部署範本**。
2. 在「部署範本」頁面上選取一個範本，然後按一下**複製**。
3. 輸入範本的新名稱，然後按一下**套用**。範本必須具有唯一的名稱。

### 刪除部署範本

若想刪除部署範本：

1. 在「Dell 管理中心」，選取**部署** → **部署範本**。
2. 在**部署範本**頁面上選取一個範本，然後按一下**刪除**。
3. 在訊息方塊上按一下**刪除**以刪除範本，或是按一下**取消**以取消。

### 重新命名部署範本


重新命名部署範本：


1. 在「Dell 管理中心」，選取**部署** → **部署範本**。
2. 在**部署範本**頁面上選取一個範本，然後按一下**重新命名**。
3. 輸入範本的新名稱，然後按一下**套用**。範本必須具有唯一的名稱。
4. 若要顯示所有部署範本，請從 **Dell 管理中心**選取**部署** → **部署範本**，然後按一下**重新整理**。

## 執行部署精靈

「部署精靈」會引導您逐步完成裸機伺服器部署程序：

- 選取解除部署的伺服器。  
您在部署 Hypervisor 時，可選擇部署至最低 1 GB 儲存容量的「內部雙 SD 模組」。您必須先從 BIOS 啟用「內部雙 SD 模組」，才可使用 OpenManage Integration for VMware vCenter 部署 Hypervisor。
- 使用部署範本 (整合硬體與 Hypervisor 設定檔)。
- 設定全域設定。此頁面可讓您選擇將 Hypervisor 部署至硬碟或「內部雙 SD 模組」。
- 將識別指派至部署的伺服器。
- 將需要的連線設定檔與每部伺服器配對。
- 排程執行伺服器部署工作。
- 顯示「工作佇列」以在其中管理部署工作。

 **註:** 若您僅部署硬體設定檔，則會略過新的「全域設定」、「伺服器識別」和「連線設定檔」頁面，且會將您直接引導至「排程工作」頁面。

 **註:** 您可針對試用版 / 評估授權使用「韌體精靈」(若授權未過期)。

**相關工作：**

- [部署精靈步驟 1：選取伺服器](#)
- [部署精靈步驟 2：部署範本](#)
- [部署精靈步驟 3：全域設定](#)
- [部署精靈步驟 4：伺服器識別](#)
- [部署精靈步驟 5：連線設定檔](#)
- [部署精靈步驟 6：排程工作](#)

## 部署精靈步驟 1：選取伺服器

此頁面涵蓋伺服器部署。若您想要將 Hypervisor 部署至「內部雙 SD 模組」，此頁面會顯示該選項為可用或無法使用。如需關於「內部雙 SD 模組」的詳細資訊，請參閱「[執行部署精靈](#)」。若您想要部署的伺服器未在步驟 2 的清單中顯示，則可手動新增伺服器使其顯示於此步驟的清單，請參閱「[手動新增伺服器](#)」。

選取伺服器：

1. 在 **Dell 管理中心**，選取 **部署** → **部署精靈**。
2. 在 **選取伺服器** 視窗中，將非部署伺服器指派至此部署工作，使用核取方塊選取 **伺服器**。
3. 按一下 **下一步**。

若要繼續執行工作至步驟二，請按一下 [部署精靈步驟 2](#)。

## 部署精靈步驟 2：部署範本

部署至硬體設定檔與 Hypervisor 部署略有差異。若您部署至硬體設定檔，請按一下 [部署精靈步驟 6](#)。

選取部署範本：

1. 「部署範本」會從數種方式中擇一選取 / 建立部署範本：
  - 在 **可用範本** 下方，選取現有的部署範本。在右窗格會填入所選範本的資訊。
  - 選取現有的部署範本，然後按一下 **編輯** 以變更一個或所有關聯的設定檔。
  - 按一下 **建立新的** 以定義新範本。
2. 選取下列其中一個項目：
  - 若您要部署至硬體設定檔，請按 **下一步** 跳至 [部署精靈步驟 6](#)。


- 若您要部署至 Hypervisor 設定檔，請按下一步引導至[部署精靈步驟 3](#)。

## 部署精靈步驟 3：全域設定

您可將 Hypervisor 部署至硬碟機或「內部雙 SD 模組」。若在至少其中一個選取的伺服器上可使用「內部雙 SD 模組」，則依預設會啟用**內部雙 SD 模組**選項。若否，則不會選取**硬碟**和**內部雙 SD 模組**選項。

若要部署 Hypervisor，請執行下列步驟：

1. 在「全域設定」頁面，選取下列其中一個選項：
  - **硬碟**：在硬碟機上部署 Hypervisor。
  - **內部雙 SD 模組**：在「內部雙 SD 模組」上部署 Hypervisor。
2. 若有任何選取的伺服器不支援「內部雙 SD 模組」，或是在部署時未顯示「內部雙 SD 模組」，請執行下列其中一項動作：
  - 若您想要在伺服器的第一個硬碟上部署 Hypervisor，請選取**針對無可用內部雙 SD 模組的伺服器，將 Hypervisor 部署至第一個硬碟**核取方塊。

 **警告：**若您選取此選項，並將 Hypervisor 部署於伺服器的第一個硬碟機，則會清除硬碟機上的所有資料。


  - 清除**針對無可用內部雙 SD 模組的伺服器，將 Hypervisor 部署至第一個硬碟**核取方塊，以跳過這些伺服器的部署作業，並繼續在下一個伺服器上部署 Hypervisor。
3. 按一下**下一步**。

若要繼續執行工作至步驟 4，請按一下[部署精靈步驟 4：伺服器識別](#)。

## 部署精靈步驟 4：伺服器識別

有兩種方式可以提供伺服器識別：

- 輸入網路資訊 (IP 位址、子網路遮罩和閘道)；主機名稱一定要是完整的合格網域名稱。不支援 FQDN 使用本機主機。將主機新增至 vCenter 時會使用 FQDN。
- 使用動態主機組態通訊協定 (DHCP) 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，強烈建議為選取的 NIC MAC 位址使用 IP 保留。

 **註：**主機名稱請使用完整的合格網域名稱 (FQDN)，不要使用本機主機。從 ESXi 5.1 開始，本機主機就有一個值會妨礙 OpenManage Integration for VMware vCenter 處理主機傳來的事件。建立可將 IP 位址解析至 FQDN 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。排定執行部署工作之前，必須先備妥及驗證 DHCP 保留區和 DNS 主機名稱。

這個畫面可讓您選擇指定 VLAN ID。提供 VLAN ID 時，它會在部署時套用至 Hypervisor 的管理介面，並以 VLAN ID 標記所有流量。

若要識別伺服器：

1. 伺服器識別會指派新名稱與新網路識別給部署的伺服器。若要顯示不符合韌體、BIOS 最低要求或有其他問題的伺服器清單，請按一下**不相容伺服器**。
2. 如需其他資訊，請按一下**詳細資料**。
3. 系統更新後，按一下**檢查相容性**，重新測試及驗證修補程式。若要重新整理清單，請按一下**重新整理**，然後按一下**中止所有測試**，取消測試。
4. 按一下 **^** 展開及檢視個別伺服器資訊。
5. 在**主機名稱**和**NIC**中，輸入伺服器的**完整主機名稱**。
6. 在**NIC 管理工作**下拉式清單中，選取管理伺服器用的 NIC。

7. 輸入 **IP 位址**、**子網路遮罩**和其他網路資訊，或選取用 **DHCP 取得**核取方塊。
8. 如果部署至需要 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。
9. 為所有要部署的伺服器重複這些步驟，或是選取**將設定套用到所有選取的伺服器**核取方塊。
10. 按一下**下一步**。  
若要繼續工作至步驟 5，請按一下[部署精靈步驟 5](#)。

## 部署精靈步驟 5：連線設定檔

您可使用連線設定檔將主機與 iDRAC 或「主機根憑證」產生關聯，以為其建立連線憑證。您可透過「連線設定檔」視窗執行下列動作：

- 顯示或編輯目前的連線設定檔
- 刪除連線設定檔
- 重新整理連線設定檔清單，以反映 vCenter 主機變更

建立連線設定檔：

1. 「連線設定檔」在部署工作完成後，會自動將伺服器指派至連線設定檔。  
選取連線設定檔後，請按**下一步**。
2. 選取**將所有伺服器指派至相同的連線設定檔**選項按鈕，然後從下拉式清單中選取連線設定檔，以將所有伺服器指派至相同的現有設定檔。
3. 若要建立新的設定檔，請按一下**新增**，然後按一下**檢視 / 編輯**以檢視或編輯選取的設定檔。
4. 若要顯示選取的連線設定檔設定，請按一下**檢視**。
5. 選取**選取每部伺服器的連線設定檔**選項按鈕，然後從下拉式清單中選取每部伺服器的個別連線設定檔。
6. 選取連線設定檔後，請按**下一步**。  
若要繼續執行工作至步驟 6，請按一下[部署精靈步驟 6](#)。

## 部署精靈步驟 6：排程工作

排程會設定部署工作的排程。執行部署工作時可使用數種選項：立即、排程部署工作於選定日期和時間執行、保留部署工作以手動啟動。

設定排程：

1. 輸入日期和時間，以決定執行部署工作的時間：
  - a. 按一下**排程伺服器部署作業**。
  - b. 使用行事曆控制項以選取日期。
  - c. 輸入一天當中的時間：
    - 立即：按一下**立即部署伺服器**。
    - 延遲工作：按一下**建立部署工作**。
    - 保留：僅在可修改排程且無法變更其他所有部署工作選項時，方使用此選項。
2. 輸入**工作名稱**和**工作說明**。
3. 按一下 **Finish** (完成)。
4. 完成部署精靈後，您可使用**工作佇列**來管理部署工作。
5. 若要顯示必須先進行韌體更新才可完成精靈的非相容伺服器清單，請按一下**非相容伺服器**。


相關工作：

- [使用部署工作佇列管理部署工作](#)

## 瞭解工作佇列

「工作佇列」可管理伺服器部署與清查擷取工作，例如：

- 顯示提交的伺服器部署工作。
- 重新整理「部署工作」或「清查 / 保固歷程記錄」佇列。
- 排程清查工作以更新在目前 vCenter 中找到的 Dell 伺服器屬性。
- 清除部署工作佇列項目。
- 管理叢集和資料庫的韌體更新。

 **註:** 為確保清查 / 保固包含最新資訊，每週應至少執行一次清查 / 保固工作。清查 / 保固工作會耗用最少的資源，且不會降低主機效能。

此頁面上的工作，包括：

- [使用部署工作佇列管理部署工作](#)
- [執行清查工作](#)
- [修改清查工作排程](#)
- [檢視叢集與資料中心的韌體更新狀態](#)


### 使用部署工作佇列管理部署工作

使用部署工作佇列管理部署工作：

1. 從 **Dell 管理中心**，選取工作佇列 → **部署工作**。
2. 若要更新**部署工作詳細資料**，請按一下**重新整理**。
3. 若要顯示「部署工作詳細資料」對話方塊 (其包含部署工作所含伺服器的相關詳細資訊)，請按一下**詳細資料**。這會顯示下列詳細資料：
  - 服務標籤
  - iDRAC IP 位址
  - 伺服器狀態
  - 若發生任何警告
  - 部署工作詳細資料
  - 開始時間與結束時間

若要在對話方塊表格中顯示每個項目的完整資訊，請將滑鼠游標停駐在項目上方，即會顯示額外的快顯文字。

4. 若要保留所選工作或輸入更新排程，請按一下**修改**。
5. 按一下**中止**以中止部署工作。
6. 若顯示訊息，請按一下**中止工作**以中止，或按一下**請勿中止工作**以取消。

 **註:** 您無法中止任何處理中的部署工作。

7. 若要顯示「清除部署工作佇列」視窗，請按一下**清除工作佇列**。選取**早於日期和工作狀態**，然後按一下**套用**。接著即會從佇列清除選取的工作。

## 手動新增伺服器

您可手動新增未由探索程序新增的伺服器。新增伺服器後，其即會顯示於「部署精靈」中的伺服器清單。

1. 在「Dell 管理中心」的**部署**中，按一下**部署精靈**。
2. 在**選取伺服器**索引標籤上，按一下**新增伺服器**。
3. 在 **Add Server** (新增伺服器) 方塊中執行下列步驟：
  - a. 在 **iDRAC IP 位址** 文字方塊，輸入 iDRAC IP 位址。
  - b. 在 **User Name (使用者名稱)** 文字方塊中，輸入使用者名稱。
  - c. 在 **Password (密碼)** 文字方塊中，輸入密碼。
4. 按一下 **新增伺服器**。這可能需要幾分鐘的時間。

## 移除裸機伺服器

您可手動移除已自動探索或手動新增的伺服器。

1. 在「Dell 管理中心」的**部署**下方，按一下**部署精靈**。
2. 在**選取伺服器**索引標籤上，按一下**移除伺服器**。
3. 在**移除伺服器**對話方塊中，選取所移除伺服器的核取方塊。
4. 按一下**移除選取的伺服器**。
5. 在**選取伺服器**索引標籤上，檢視表格中所列出的伺服器，以確認其已移除。

# 主控台管理

您可使用以下兩個額外管理入口網站，管理 OpenManage Integration for VMware vCenter 及其虛擬環境：

- Web 管理主控台
- 個別伺服器的主控台檢視 (設備虛擬機器主控台)。

只要透過這兩個入口網站，即可針對全體 vCenter 例項進入和使用 vCenter 管理的全域設定、OpenManage Integration for VMware vCenter 資料庫備份與還原，以及重設 / 重新啟動等動作。

## Web 管理主控台

「Web 管理主控台」提供數項重要功能：vCenter 伺服器註冊和管理、虛擬設備管理、全域 vCenter 警示設定，以及備份與還原設定。

## 使用管理主控台

從管理主控台的 vCenter 登錄視窗，您可以登錄 vCenter 伺服器，以及上傳或購買授權。如果使用的是示範授權，就會顯示購買軟體連結，用以購買完整版本授權，以管理多部主機。在本節中，您也可以修改、更新及取消登錄伺服器。

相關工作：


- [以具必要權限的非系統管理員使用者身分登錄 vCenter 伺服器](#)
- [登錄 vCenter 伺服器](#)
  - [修改 vCenter 登入](#)
  - [更新登錄 vCenter 的 SSL 憑證](#)
  - [從 vCenter 解除安裝 OpenManage Integration for VMware vCenter](#)
- [上傳 OpenManage Integration for VMware vCenter 授權](#)

## 以具必要權限的非系統管理員使用者身分登錄 vCenter 伺服器


您可使用 vCenter 管理員憑證或具必要權限的非系統管理員使用者身分，為 OMIVV 產品登錄 vCenter 伺服器。

請執行以下步驟，為某使用者啟用所需權限以登錄 vCenter 伺服器：

1. 請新增一個角色，再選擇角色的所需權限，或修改現有的角色，變更為該角色所選的權限。請參閱 VMware vSphere 說明文件檢視相關步驟，瞭解如何建立或修改角色，以及如何在 vSphere 用戶端選取權限。請參閱 [定義權限](#)，為該角色選擇所有必要的權限。

 註: vCenter 管理員應新增或修改角色。

2. 一旦定義某角色並選取該角色的權限後，請將某使用者指定給新建立的角色。請參閱 VMware vSphere 說明文件，深入瞭解如何在 vSphere 用戶端中指定權限。具所需權限的 vCenter 伺服器使用者現可登錄並/或解除登錄 vCenter、修改憑證或更新憑證。

 註: vCenter 管理員應在 vSphere 用戶端指定權限。

3. 以具必要權限的非系統管理員使用者身分，登錄 vCenter 伺服器。請參閱[以具所需權限的非系統管理員使用者身分登錄 vCenter 伺服器](#)。
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[將 Dell 權限指定給角色](#)。


具有必要權限的非系統管理員使用者現可使用 Dell 主機享有 OMIVW 功能。

## 定義權限

為非系統管理員使用者啟用所需權限以登錄 vCenter 伺服器，請選取下列權限：

- 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
  - Settings (設定)
- 主機
  - CIM
    - \* CIM 互動
  - Configuration
    - \* 進階設定
    - \* 連線
    - \* Maintenance (維護)
    - \* 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
- 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:** 如果上述權限並未指定，在具所需權限的非系統管理員使用者登錄 vCenter 伺服器時，便會顯示錯誤訊息。

### 以具所需權限的非系統管理員使用者身分登錄 vCenter 伺服器

您可使用具所需權限的非系統管理員使用者身分，為 OMIVV 應用裝置登錄 vCenter 伺服器。請參閱參閱 [登錄 vCenter 伺服器](#)，瞭解如何登錄 vCenter 伺服器。

### 將 Dell 權限指定給角色

您可編輯現有的角色，以指定 Dell 權限。


 **註:** 請確定您以具管理員權限的使用者身分登入。

若要將 Dell 權限指定給現有的角色，請執行下列步驟：

1. 以具管理權限的身分登入 vSphere 用戶端。
2. 請在 vSphere 用戶端**首頁**中，按一下**角色**。
3. 以滑鼠右鍵按一下進行編輯，並選取**編輯角色**。
4. 選取下列權限，然後按一下**確定**。
  - Dell
    - Dell.Configuration
    - Dell.Deploy-Provisioning
    - Dell.Inventory
    - Dell.Monitoring
    - Dell.Reporting

請參閱 [安全性角色與權限](#) 深入瞭解 vCenter 中可用的 OMIVV 角色。


權限和角色的變更會立即生效。具必要權限的非系統管理員使用者現可執行 OpenManage Integration for VMware vCenter 作業。


 **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。

### 登錄 vCenter 伺服器

安裝完成 OpenManage Integration for VMware vCenter 後，您可登錄 OpenManage Integration for VMware vCenter。OpenManage Integration for VMware vCenter 針對 vCenter 作業使用管理使用者帳戶或

具必要權限的非系統管理員使用者帳戶。OpenManage Integration for VMware vCenter 目前對每個 OMIVV 應用裝置支援 10 個 vCenter，稍後可加以變更。

1. 開啟**管理主控台**。
2. 若要登錄新的 vCenter 伺服器，在左窗格按一下 **VCENTER 登錄**，然後按一下**登錄新 vCenter 伺服器**。
3. 在**登錄新 vCenter** 對話方塊的 **vCenter 名稱** 下，請執行下列步驟：
  - 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。
    -  **註:** 強烈建議使用完整網域名稱 (FQDN) 登錄 OMIVV 與 VMware vCenter。所有登錄的 vCenter 主機名稱應經 DNS 伺服器正確解析。以下為使用 DNS 伺服器的建議作法：
      - 在您使用有效的 DNS 登錄部署 OMIVV 應用裝置時，請指派靜態 IP 位址和主機名稱。靜態 IP 位址可確保在系統重新啟動時，OMIVV 應用裝置的 IP 位址維持不變。
      - 確認 OMIVV 主機名稱項目出現在正向與反向對應中。
  - b. 在**說明**文字方塊中，輸入選填的說明。
4. 在 **vCenter 使用者帳戶**，請執行下列步驟：
  - a. 請在 **vCenter 使用者名稱** 文字方塊中，輸入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**。

 **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。

例如：假設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。

### OpenManage Integration for VMware vCenter 需求

若為舊版的伺服器，OpenManage Integration for VMware vCenter (OMIVV) 需要 OpenManage 的資訊，而且較新版的平台僅限於在可解讀較新晶片組的 vSphere 版本中啟動。因此，可以搭配特定版本 OMIVV 使用的 vSphere 版本有限制。

表 4. 受管主機上安裝支援的 ESXi 版本

ESXi 版本支援	伺服器世代		
	11G	12G	13G
v5.0	Y	Y	N
5.0 版 U1	Y	Y	N
5.0 版 U2	Y	Y	N
5.0 版 U3	Y	Y	N
5.1 版	Y	Y	N
5.1 版 U1	Y	Y	N
5.1 版 U2	Y	Y	Y

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

表 5. 發行版本 3.1 支援的 vCenter 伺服器版本

vCenter 版本	桌上型電腦用戶端支援	Web 用戶端支援
5.1 版 U2	Y	N
5.1 版 U3	Y	N
5.5 版 U1	Y	Y
5.5 版 U2	Y	Y
5.5 版 U3	Y	Y
6.0 版	Y	Y
6.0 版 U1	Y	Y

### 修改 vCenter 登入

具管理權限的使用者或具必要權限的非系統管理員使用者均可修改 vCenter 登入憑證。

1. 在 OpenManage Integration for VMware vCenter 的摘要索引標籤上，用連結開啟管理主控台。
2. 在登入對話方塊輸入密碼。
3. 在左窗格中按一下 **VCENTER 登錄**。右窗格會顯示已登錄的 vCenter。若要開啟修改管理員帳戶視窗，請在憑證下按一下修改。
4. 輸入 vCenter 使用者名稱、密碼和確認密碼；密碼必須相符。
5. 若要變更密碼，請按一下套用，或若要取消變更，請按一下取消。

 註: 如果必要權限並未指派給修改 vCenter 登入憑證的非系統管理員使用者，便會顯示錯誤訊息。

## 更新已登錄 vCenter 伺服器的 SSL 憑證

如果 vCenter 伺服器上的 SSL 憑證改變，請使用下列步驟來匯入 OpenManage Integration for VMware vCenter 的新憑證。OpenManage Integration for VMware vCenter 使用此憑證確定 vCenter 伺服器聯繫的是正確的 vCenter 伺服器，而不是偽裝的伺服器。

OpenManage Integration for VMware vCenter 使用 openssl API 建立憑證簽章要求 (CSR) (使用 2048 位元金鑰長度的 RSA 加密標準)。OpenManage Integration for VMware vCenter 產生的 CSR，用於從受信任的憑證授權單位，取得數位簽署的憑證。OpenManage Integration for VMware vCenter 使用數位憑證，在 Web 伺服器啟用 SSL，保護通訊。

1. 啟動 Web 瀏覽器，然後輸入 `https://<ApplianceIPAddress>`
2. 在左窗格中，按一下 **VCENTER REGISTRATION (VCENTER 登錄)**。右窗格會顯示已登錄的 vCenter。若要更新憑證，請按一下 **Update (更新)**。


## 解除安裝 OpenManage Integration for VMware vCenter


若要移除 OpenManage Integration for VMware vCenter，必須用管理主控台從 vCenter 伺服器將它取消登錄。


1. 啟動 Web 瀏覽器，然後輸入 `https://<ApplianceIPAddress>`
2. 在 **vCenter Registration (vCenter 登錄)** 的 vCenter 伺服器表下，請按一下 **Unregister (取消登錄)** 取消登錄 OpenManage Integration for VMware vCenter。  
您可能有多個 vCenter，請務必選對。
3. **Unregister vCenter (取消登錄 vCenter)** 對話方塊會詢問您是否真的要取消登錄此伺服器，在裡面按一下 **Unregister (取消登錄)**。

## 上傳 OpenManage Integration for VMware vCenter 授權至管理主控台

1. 在 OpenManage Integration for VMware vCenter 的 Summary (摘要) 索引標籤上，用連結開啟管理主控台。
2. 在「登入」對話方塊中，鍵入您的密碼。
3. 在左窗格中，按一下 **VCENTER REGISTRATION (VCENTER 登錄)**。登錄的 vCenter 會顯示在表格中。若要顯示上傳授權對話方塊，按一下 **Upload License (上傳授權)**。
4. 若要瀏覽至授權檔案，按一下 **Browse (瀏覽)** 按鈕，瀏覽至授權檔案，然後按一下 **Upload (上傳)**。

 **註:** 如果授權檔案經任何方式修改或編輯，本應用裝置會將檔案視為損毀，無法運作。

 **註:** 如果您需要新增更多的主機，可以新增授權。遵照上述程序即可新增更多授權。

 **註:** 如果成功清查的第 11、12 和 13 代伺服器的數量，等於已購買授權數。移除幾個第 11、12 或 13 代伺服器，以編輯現有的連線設定檔。為已移除的第 11、12 或 13 代伺服器建立新的連線設定檔。

## 虛擬設備管理

虛擬設備管理包含 OpenManage Integration for VMware vCenter 網路、版本、NTP 和 HTTPS 資訊，並可讓管理員執行以下動作：

- 重新啟動虛擬設備
- 更新虛擬設備，並設定更新儲存庫位置
- 產生包含設備記錄資訊的疑難排解配套。

- 輸入「網路時間通訊協定」(NTP) 設定
- 上傳和管理 HTTPS 憑證

相關工作：

- [重新啟動虛擬設備](#)
- [更新儲存庫位置及更新設備](#)
- [下載疑難排解配套](#)
- [設定 NTP 伺服器](#)

## 重新啟動虛擬設備


重新啟動虛擬設備後，您會從管理主控台登出，而且 OpenManage Integration for VMware vCenter 必須等到虛擬設備及其服務啟用時才能使用。

1. 在 OpenManage Integration for VMware vCenter 的管理主控台下，用連結開啟管理主控台。
2. 在登入對話方塊輸入密碼。
3. 在左窗格中，按一下 **應用裝置管理**。
4. 若要重新啟動 OpenManage Integration for VMware vCenter，按一下 **Restart the Virtual Appliance (重新啟動虛擬設備)**。
5. 在 **重新啟動虛擬設備** 對話方塊中，若要重新啟動虛擬設備，按一下 **套用**，或是若要取消，按一下 **取消**。

## 更新儲存庫位置和虛擬設備

更新虛擬設備之前請執行備份，以確保所有資料受到保護。請參閱[管理備份與還原](#)。

1. 在 OpenManage Integration for VMware vCenter 的管理主控台下，用連結開啟管理主控台。
2. 在登入對話方塊輸入密碼。
3. 在左窗格中，按一下 **應用裝置管理**。
4. 在設備更新旁邊，按一下 **編輯**。
5. 在 **Appliance Update (設備更新)** 視窗中，輸入 **Repository Location URL (儲存庫位置 URL)**，然後按一下 **Apply (套用)**。

 **註：**如果更新位置在外接式網路，例如 Dell FTP 站台，那麼就必須在 HTTP Proxy 區域輸入 Proxy。

## 更新虛擬設備軟體

開始軟體更新之前，請先執行設備備份，防止資料遺失。

1. 啟動 Web 瀏覽器，然後輸入 `https://<ApplianceIPAddress>`。
2. 在左窗格中，按一下 **設備管理**。
3. 若要將虛擬設備更新為列在 **Appliance Update (設備更新)** 下列出的軟體版本，請按一下 **Update Virtual Appliance (更新虛擬設備)**。
4. 在 **Update Appliance (更新設備)** 對話方塊中，會列出目前版本和可用版本。若要開始更新，請按一下 **Update (更新)**。
5. 系統會鎖定並進入維護模式。更新完成時，Appliance (設備) 頁面會顯示新安裝的版本。

## 下載疑難排解配套

使用此資訊協助疑難排解問題，或是傳送給技術支援部門。

1. 啟動 Web 瀏覽器，然後輸入 `https://<ApplianceIPAddress>`。
2. 在左窗格中，按一下**設備管理**。
3. 若要產生疑難排解配套對話方塊，請按一下**產生疑難排解配套**。
4. 按一下**下載疑難排解配套**連結。
5. 按一下 **Close (關閉)** 即可結束。

## 設定 HTTP Proxy


您可以使用管理主控台設定 HTTP Proxy 設定。

1. 在 OpenManage Integration for VMware vCenter 的 Summary (摘要) 索引標籤上，用連結開啟管理主控台。
2. 在「登入」對話方塊中，鍵入您的密碼。
3. 在左窗格中，按一下**設備管理**。
4. 在**設備管理**頁面，向下捲動至 **HTTP Proxy 設定**，然後按一下**編輯**。
5. 在**編輯**頁面，請執行下列步驟：
  - a. 若要啟用 HTTP Proxy 設定，在**使用 HTTP Proxy 設定**旁選取**啟用**。
  - b. 在 **Proxy 伺服器位址**文字方塊中，輸入 Proxy 伺服器位址。
  - c. 在 **Proxy 伺服器連接埠**文字方塊中，輸入 Proxy 伺服器連接埠。
  - d. 若要使用 Proxy 憑證，在**使用 Proxy 憑證**旁選取**是**。
  - e. 如果您使用的是憑證，請在**使用者名稱**文字方塊輸入使用者名稱。
  - f. 在**密碼**文字方塊中，輸入密碼。
6. 按一下 **Apply (套用)**。

## 設定 NTP 伺服器

使用網路時間通訊協定 (Network Time Protocol, NTP) 將虛擬設備和 NTP 伺服器的時鐘同步化。

1. 在 OpenManage Integration for VMware vCenter 的管理主控台下，用連結開啟管理主控台。
2. 在登入對話方塊輸入密碼。
3. 在左窗格中，按一下**應用裝置管理**。
4. 在 **NTP 設定**下按一下**編輯**。
5. 選取**已啟用**核取方塊。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**。
6. 按一下**取消**即可結束。

 **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。

## 產生憑證簽章要求


 **註:** 您必須先上傳憑證，才能在 vCenter 登錄 OpenManage Integration for VMware vCenter。

產生新的憑證簽章要求，可避免以先前所產生之 CSR 建立的憑證上傳至本設備。


1. 在 OpenManage Integration for VMware vCenter 的管理主控台下，用連結開啟管理主控台。
2. 在登入對話方塊輸入密碼。
3. 在左窗格中，按一下**應用裝置管理**。
4. 按一下**產生 HTTPS 憑證的憑證簽章要求**。隨即顯示訊息，表示如果產生新的要求，那麼使用舊 CSR 建立的憑證無法再上傳至本設備。若要繼續此要求，請按一下**繼續**，或是若要取消，請按一下**取消**。
5. 輸入要求的一般名稱、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**。
6. 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


您可以使用 HTTPS 憑證，在虛擬設備與主機系統之間進行安全通訊。若要設定這種類型的安全通訊，必須將憑證簽章要求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。另外有自動簽署的預設憑證可供安全通訊使用；此憑證對每個安裝而言都是唯一的。

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

1. 在 OpenManage Integration for VMware vCenter 的摘要索引標籤上，用連結開啟管理主控台。
2. 在登入對話方塊輸入密碼。
3. 在左窗格中，按一下**應用裝置管理**。
4. 按一下**上傳 HTTPS 憑證的憑證**。
5. 在**上傳憑證**對話方塊中，按一下**確定**。
6. 若要選取欲上傳的憑證，先按一下**瀏覽**，然後按一下**上傳**。
7. 如果您想要中止上傳，請按一下**取消**。

 **註：**憑證必須使用 PEM 格式。

## 還原預設的 HTTPS 憑證

 **註：**如果要上傳設備的自訂憑證，必須先登錄 vCenter 才能上傳新憑證。如果在登錄 vCenter 後上傳新自訂憑證，Web 用戶端會顯示通訊錯誤。若要解決這個問題，您必須取消登錄再重新登錄 vCenter 設備。

1. 在 OpenManage Integration for VMware vCenter 的摘要索引標籤上，用連結開啟管理主控台。
2. 在 Login (登入) 對話方塊輸入密碼。
3. 在左窗格中，按一下**設備管理**。
4. 按一下在 **HTTPS 憑證** 下的**還原預設憑證** 連結。
5. 在還原預設憑證對話方塊中，按一下 **Apply (套用)**。

## 設定全域警示

警示管理可讓您針對如何儲存所有 vCenter 例項的警示，輸入全域設定。

1. 在 OpenManage Integration for VMware vCenter 的管理主控台下，用連結開啟管理主控台。
2. 在登入對話方塊輸入密碼。
3. 在左窗格中，按一下**警示管理**。若要輸入新的 vCenter 警示設定，請按一下**編輯**。
4. 輸入下列項目的數值：
  - 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

從管理主控台即可管理備份和還原。此頁面上的工作包括：

- [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](#)

### 設定備份和還原

備份和還原功能會將 OpenManage Integration for VMware vCenter 資料庫備份至遠端位置，可供稍後還原。備份包含設定檔、範本和主機資訊。建議您排程自動備份，以防止資料遺失。在這個程序後，您必須設定備份排程。

 **註:** NTP 設定不會儲存及還原。

1. 在 OpenManage Integration for VMware vCenter 的管理主控台下，用連結開啟管理主控台。
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**。
4. 若要編輯目前的備份和還原設定，請按一下**編輯**。
5. 在**設定和詳細資料**頁面，請執行下列步驟：
  - a. 在**備份位置**文字方塊中，輸入備份檔案的路徑。
  - 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。
  - d. 在**輸入用於加密備份的密碼**下，在文字方塊中輸入加密密碼。  
加密密碼可以包含字母與數字字元及下列特殊字元：![@](#)<#>[\\$](#)[%](#)[\\*](#)。沒有長度限制。
  - e. 在**密碼**文字方塊中，再次輸入加密的密碼。
6. 若要儲存這些設定，請按一下**套用**。
7. 設定備份排程。如需更多資訊，請參閱[排程自動備份](#)。

### 排程自動備份

這是設定備份和還原的第二部份。如需設定備份位置和認證的詳細資訊，請參閱[設定備份與還原](#)。

若要排程自動備份：


1. 在 OpenManage Integration for VMware vCenter 的管理主控台下，用連結開啟管理主控台。
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**。
4. 若要編輯備份與還原設定，按一下**編輯自動排定備份** (此舉會啟用欄位)。
5. 若要啟用備份，請按一下**啟用**。
6. 選取您要執行備份那幾天的核取方塊。
7. 在**備份時間 (24 小時時間格式, 小時:分鐘)** 文字方塊中，以小時:分鐘格式輸入時間。  
下一次備份隨即填入下一次排定備份的日期與時間。

8. 按一下 **Apply** (套用)。

## 執行立即備份

1. 在 OpenManage Integration for VMware vCenter 的管理主控台下，用連結開啟管理主控台。
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**。
4. 按一下 **立即備份**。
5. 若要使用備份設定的位置和加密密碼，在 **Backup Now (立即備份)** 對話方塊中勾選該核取方塊。
6. 輸入 **備份位置**、**使用者名稱**、**密碼**和**加密密碼**。  
加密密碼可以包含字母與數字字元及下列特殊字元：!@#%\$\*。沒有長度限制。
7. 按一下 **Backup (備份)**。

## 從備份還原資料庫

 **註:** 還原作業會導致虛擬設備在完成後重新啟動。

1. 在 OpenManage Integration for VMware vCenter 的管理主控台下，用連結開啟管理主控台。
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**，目前的備份和還原設定隨即顯示。
4. 按一下 **立即還原**。
5. 在立即還原對話方塊中，輸入檔案位置連同 **backup .gz** 檔案 (CIFS/NFS 格式)。
6. 輸入備份檔案的**使用者名稱**、**密碼**和**加密密碼**。  
加密密碼可以包含字母與數字字元及下列特殊字元：!@#%\$\*。沒有長度限制。
7. 若要儲存變更，請按一下**套用**。  
按一下套用後，本設備會重新開機或重新啟動。

## 瞭解 vSphere 用戶端主控台

**vSphere 用戶端主控台**在虛擬機器的 vSphere 用戶端內。**主控台**必須搭配管理主控台使用。主控台提供下列功能：

- [設定網路設定](#)
- [變更虛擬設備密碼](#)
- [設定當地時區](#)
- [重新啟動虛擬設備](#)
- [將虛擬設備重設為原廠設定](#)
- [重新整理主控台](#)
- [從主控台登出](#)
- [唯讀使用者角色](#)
- [從 OMIVV 3.0 版升級至最新版本](#)
- [從舊版移轉到 OMIVV 3.1 版](#)

使用方向鍵向上或向下瀏覽。如果您已選取想要的選項，請按下 <Enter>。進入 **Console (主控台)** 畫面後，VMware vSphere 用戶端會控制游標。若要脫離控制，請按下 <CTRL> + <ALT>。

## 組態網路設定

在 vSphere 用戶端主控台即可變更網路設定。

1. 在 vSphere Web 用戶端的導覽中，選取 **vCenter**。
2. 在導覽選取您要管理的虛擬設備。
3. 請執行下列其中一項動作：
  - 在物件索引標籤上，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**。
4. 在**主控台**視窗選取**設定網路**，然後按下 <ENTER>。
5. 在**編輯裝置**或**編輯 DNS** 組態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**。

## 變更虛擬設備密碼


只要使用設備主控台，即可在 vSphere 用戶端中變更虛擬設備密碼。

若要變更虛擬設備密碼：

1. 登入已部署 OpenManage Integration for VMware vCenter 的 vCenter/ESXi 主機。選取 OpenManage Integration for VMware vCenter 虛擬機器，然後按一下**主控台**索引標籤。
2. 以 admin 為使用者名稱及先前已設定的密碼登入設備。
3. 在 OpenManage Integration for VMware vCenter 虛擬設備設定視窗中，按一下**變更管理員密碼**。
4. 在**變更密碼**視窗中，輸入「目前的密碼」。
5. 在**新密碼**中，輸入新密碼。
6. 在**確認新密碼**中，輸入新密碼以確認。
7. 按一下**變更密碼**按鈕  
此時會顯示**密碼更新成功**訊息。
8. 按一下**確定**。

## 設定當地時區

若要設定當地時區：

 **註:** 您僅可編輯時區而無法編輯目前的時間和日期。

1. 在 **vSphere 用戶端** 中，選取 OpenManage Integration for VMware vCenter 虛擬機器，然後按一下**主控台**索引標籤。
2. 選取**設定時區**，然後按下 <ENTER>。
3. 在**時區選擇**視窗中選擇您所要的時區，然後按一下**確定**。若要取消變更，請按一下**取消**。接著即會更新時區。

## 重新啟動虛擬設備


若要重新啟動虛擬設備：

1. 在 **vSphere** 用戶端中，選取 OpenManage Integration for VMware vCenter 虛擬機器，然後按一下**主控台**索引標籤。
2. 選取**重新啟動此虛擬設備**，然後按下 **<Enter>**。
3. 隨即顯示下列訊息：  
If there are any processes running on this appliance they will be terminated by this action. Are you sure you wish to do this?
4. 輸入 **y** 重新啟動或輸入 **n** 取消。本設備會重新開機。

## 將虛擬設備重設為原廠設定

若要將虛擬設備重設為原廠設定：

1. 在 **vSphere** 用戶端中，選取 OpenManage Integration for VMware vCenter 虛擬機器，然後按一下**主控台**索引標籤
2. 選取**將此虛擬設備重設為原廠設定**，然後按下 **<ENTER>**。
3. 隨即顯示下列通知：  
This operation is completely Irreversible if you continue you will completely reset \*this\* appliance to its original settings. All changes you have made to this appliance will be Lost. Are you sure you wish to Reset this Appliance to Factory Settings?
4. 輸入 **y** 重設，或輸入 **n** 取消。  
本設備會重設為原廠設定，所有其他設定與儲存的資料都會遺失。

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

## 重新整理主控台檢視

若要重新整理主控台檢視，選取 **Refresh (重新整理)**，然後按下 **<Enter>**。

## 從主控台登出

若要從主控台登出，請按一下右上角您登入帳戶旁的**登出**。

## 唯讀使用者角色


有一不具備所需權限的使用者角色，稱為「基於診斷目的而具殼層存取之唯讀使用者」。此唯讀使用者僅具有有限權限可執行掛載。此唯讀使用者的密碼設為 **readonly**。此唯讀使用者的密碼已從管理員密碼 (OMIVV v1.0 至 v2.3.1) 進行變更，以符合安全性用途。

## 將 OpenManage Integration 外掛程式從 3.0 版升級至最新版本

若要將 OpenManage Integration 外掛程式從 3.0 版升級至最新版本，請執行下列步驟：




1. 開啟 Web 瀏覽器，為要設定之虛擬機器輸入會顯示在 vSphere vCenter **主控台**索引標籤內的管理主控台 URL。您也可以使用在 Dell 管理主控台中的**說明和支援**頁面上顯示的連結。URL 採用下列格式且不區分大小寫：<https://<ApplianceIPAddress>>
2. 在**管理主控台**視窗的左側窗格中，按一下**應用裝置管理**。

3. 根據您的網路設定，如果您的網路需要代理，請啟用代理並提供代理設定。
4. 若要將 OpenManage Integration 外掛程式從 3.0 版升級至最新版本，請執行下列其中一項步驟：
  - 確認**更新儲存庫路徑**設為 <http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/> 路徑。如果路徑不同，請在**裝置管理**視窗的**裝置更新**區段中，按一下**編輯**，以在**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/>。按一下**套用**以儲存更新。
  - 如果沒有網際網路連線，請從 <http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/> 路徑下載所有檔案和資料夾，並將其複製到 HTTP 共用區。在**裝置管理**視窗的**裝置更新**區段中，按一下**編輯**，然後在**更新儲存庫路徑**文字方塊中，將路徑更新為離線 HTTP 共用區，然後按一下**套用**。
5. 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。
6. 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**。
7. 在**更新裝置**對話方塊中，按一下**更新**。按一下**更新**後，您將會登出**管理主控台**視窗。

 **註:** 將 OMIVV 從 3.0 版升級至最新版本時，自訂憑證並不會移轉，且您必須重新套用您先前為憑證套用的設定。

## 從 2.x 移轉到 3.1 的移轉路徑

若要從舊版移轉到 OMIVV 3.1 版，請執行下列動作：

1. 備份較舊版本的資料庫。
2. 從 vCenter 關閉舊應用裝置。
  -  **註:** 請勿從 vCenter 取消註冊外掛程式。從 vCenter 取消註冊外掛程式會移除外掛程式在 vCenter 註冊的所有警報，並移除了在警報執行的所有自訂，例如 vCenter 上的動作等等。
3. 部署新的 OpenManage Integration 3.1 OVF 版。
4. 開啟 OpenManage Integration 3.1 版應用裝置電源。
5. 為應用裝置設定網路與時區等等。新 OpenManage Integration 3.1 版應用裝置和舊應用裝置的 IP 位址必須一模一樣。
  -  **註:** 如果 3.1 應用裝置的 IP 位址與舊版應用裝置的 IP 位址不同，外掛程式可能無法正常運作。在此情況下，您必須先取消註冊，然後重新註冊所有 vCenter 例項。
6. 將資料庫還原到新的應用裝置。
7. 驗證應用裝置。如需更多資訊，請參閱本指南的**安裝驗證**，確保資料庫移轉成功。
8. 在所有已登錄的 vCenter 執行清查。
  -  **註:** 建議您，升級後，在外掛程式管理的所有主機再次執行清查。如需更多資訊，請參閱 *OpenManage Integration for VMware vCenter 使用者指南* 的**執行清查工作**，瞭解隨需執行清查的步驟，網址是：[dell.com/support/manuals](http://dell.com/support/manuals)。

如果新 OpenManage Integration 3.1 版應用裝置的 IP 位址已與舊版的應用裝置有所不同，則 SNMP 設陷的設陷目的地必須設定為指向新的應用裝置。如為第 12 代及更高版本的伺服器，在這些主機上執行清查可修正此問題。對於與舊版相容且早於第 12 代的主機，此 IP 變更會顯示為不相容，且您需要設定 OMSA。

## 故障排除

使用這個章節尋找故障排除問題的答案。本章節包括：


- [常見問題集 \(FAQ\)](#)
- [裸機部署問題](#)
- [與 Dell 公司聯絡](#)
- [相關產品資訊](#)

### 常見問題集 (FAQ)

本節包含一些常見問題和解決方式。

#### 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

在登錄 vCenter 與 OMIVV 應用裝置之後，數個 Dell 權限將會新增至 vCenter 的權限清單。在您從 OMIVV 應用裝置取消登錄 vCenter 時，將不會移除 Dell 權限。

 **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

#### 如果 vCenter 已閒置數小時，在按一下「OpenManage Integration」索引標籤和「管理中心」時，OMIVV 內容會被「！」圖示取代。我該怎麼做才能繼續作業階段？

如果 vCenter 已閒置數小時，當您按一下清查主機的 **OpenManage Integration** 索引標籤及 **Dell 管理中心** 圖示執行任何動作時，OMIVV 內容會被「！」圖示取代。

解決方法：您可以關閉目前的工作階段，並重新登入以恢復工作階段。

受影響的版本：3.1，vCenter 6.0 及更新版本

#### 在嘗試以嚴重程度類別篩選時，「Dell 管理中心」並未顯示所有相關記錄。我要如何檢視所有記錄？

當您從下拉式清單選擇**所有類別**，並選取以嚴重程度類別篩選記錄資料時，所有屬於特定類別的記錄皆會正確顯示。但是，如果您從下拉式清單中選擇**資訊**，將不會顯示韌體更新記錄，且只會顯示初始化記錄。

解決方法：若要在「Dell 管理中心」檢視所有記錄，請從下拉式清單中選取**所有類別**。

受影響的版本：3.1

## 我要如何將 OMIVV 外掛程式的狀態變更為「啟用」？

在某些情況下，安裝 OMIVV 並向 vCenter 伺服器登錄後，OMIVV 外掛程式的狀態可能不會顯示為「啟用」狀態。其將會顯示**下載及安裝**狀態，而不是**啟用**狀態。

若要將 OMIVV 外掛程式的狀態變更為「啟用」，請執行下列步驟：

1. 從 vSphere 用戶端和 vSphere Web 用戶端登出。
2. 將 OMIVV 應用裝置開機為單一使用者模式。
3. 編輯 /etc/hosts 檔案：**<vCenterIP> <myvCenter.mydomain.com> <myvCenter>**，並為 vCenter 伺服器新增 DNS 項目。  
例如 10.35.210.126 myvCenter.us.dell.com myvCenter
4. 重新啟動 OMIVV 應用裝置。依 vCenter 應用裝置的使用方式，執行下列步驟之一。
  - a. 如果您使用 Windows vCenter 伺服器，請編輯位於 c:\system\window32\drivers\etc\hosts 的主機檔案，並為 OMIVV 應用裝置新增 DNS 項目。  
例如 10.35.210.120 myomivv.us.dell.com myomivv。

執行以下命令，排清 DNS：

```
ipconfig /flushdns
```

- b. 如果您使用 vCenter 應用裝置，請編輯 /etc/hosts 檔案，並為 OMIVV 應用裝置新增 DNS 項目。  
例如 10.35.210.120 myomivv.us.dell.com myomivv。

重新啟動 vCenter 應用裝置。

5. 按一下**取消登錄**以取消登錄 OMIVV。
6. 重新登入 vSphere 用戶端和 vSphere Web 用戶端，確認 OMIVV 外掛程式顯示為**啟用**狀態。

受影響的版本：3.0

## 在為 VMware vCenter 執行 OpenManage Integration 還原後，如果 Dell 管理中心圖示並未顯示在 vSphere 用戶端，我該怎麼做？

在從之前建立的備份還原時，OpenManage Integration for VMware vCenter 可能不會顯示 Dell 管理中心的圖示。

解決方法：您可以透過從 OMIVV 應用裝置取消登錄 vCenter 伺服器，並再次登錄 vCenter 伺服器以解決此問題。

受影響的版本：這個問題可能只會在從組建編號 OMIVV 3.0.0.173 還原至組建編號 OMIVV 3.0.0.197 時出現。


## 應用裝置更新後，OMIVV 版本未從關於畫面更新

已知仍使用舊快取值的 Internet Explorer 會有這個問題。清除 IE 的快取便會顯示正確的版本。

## 不支援使用 OpenManage Integration for VMware vCenter 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 網路卡有已知問題。若使用 Lifecycle Controller 套用韌體更新，搭載這個版本韌體的部分型號 Intel 網路卡會更新失敗。此版本韌體的客戶，必須用作業系統更新網路驅動程式軟體。如果 Intel 網路卡有 13.5.2 以外版本的韌體，可以使用 OpenManage

Integration for VMware vCenter 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，避免選取搭載 13.5.2 版的 Intel 網路介面卡，因為更新會失敗，導致更新工作停止更新其餘伺服器。

## 在執行保固擷取工作時，保固工作狀態未列於「保固工作佇列」頁面

如果您的網路需要 Proxy 伺服器詳細資料以連線至網際網路，且 Proxy 並未設定於 OMIVV 應用裝置上，則保固擷取工作將會失敗，且工作將不會列於保固工作佇列之下。

解決方式：設定 Proxy 詳細資料，並再次觸發保固工作。

受影響的版本：全部

## 因為來自 DUP 的分段需求，使用 OpenManage Integration for VMware vCenter 將 Intel 網路卡由 14.5 或 15.0 更新至 16.x 將會失敗

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 後，才能更新至 16.x。

受影響的版本：全部

## 嘗試用無效的 DUP 更新韌體時，vCenter 主控台的硬體更新工作狀態不是失敗，就是逾時數小時，不過 LC 內的工作狀態卻顯示「失敗」。為什麼會發生這種情況？

更新韌體時若挑選無效的 DUP，vCenter 主控台視窗中的工作狀態會維持「進行中」，但訊息會變成故障原因。這是已知的 VMware 問題，未來版本的 VMware vCenter 將會加以解決。

解決方式：必須手動取消工作。

受影響的版本：全部

## 管理入口網站仍顯示無法聯繫的更新儲存庫位置。

如果使用者提供的是無法聯繫的更新儲存庫路徑，設備更新檢視最上方會顯示「失敗：連線至 URL... 時發生錯誤」這個錯誤訊息，不過更新儲存庫路徑不會清除為更新前的值。

解決方式：從這個頁面移到另一個頁面，確定頁面已重新整理。

受影響的版本：全部

## 為什麼如果應用裝置 IP 使用 DHCP 並覆寫 DNS 設定，應用裝置重新啟動後，DNS 組態設定會恢復原始設定

這是已知問題；DHCP 的值會取代靜態指派的 DNS 設定。若使用 DHCP 取得 IP 設定，而且 DNS 值是以靜態方式指派，就可能發生這種狀況。DHCP 租用續約或重新啟動應用裝置時，靜態指派的 DNS 設定就會被移除。解決方式：DNS 伺服器設定與 DHCP 的不同時，靜態指派 IP 設定。

受影響的版本：全部

## 為什麼執行一對多韌體更新時，系統不會進入維護模式？

有些韌體更新不需要重新啟動主機。在這種情況下，不用讓主機進入維護模式，就能執行韌體更新。

## 我的儲存庫有選取之第 11 代系統的配套，為什麼韌體更新卻顯示我沒有韌體更新的配套？

在鎖定模式新增主機至連線設定檔時，清查展開後卻失敗，表示「找不到遠端存取控制器，或是此主機不支援清查」。鎖定模式的主機不是應該支援清查嗎？

將主機設在鎖定模式或將主機從鎖定模式移除後，請先等 30 分鐘再執行下一個作業。如果韌體更新使用的是第 11 代主機，即使提供的儲存庫有該系統的配套，韌體更新精靈也不會顯示任何配套，因為第 11 代主機可能尚未設定，所以 OMSA 無法傳送設陷至 OpenManage Integration。

解決方式：用 OpenManage Integration 桌面用戶端的主機相容性畫面，確定主機相容。如果不相容，請用主機相容性這個修正式讓它相容。

受影響的版本：2.2 以後的版本

## 為什麼我的 ESXi 在搭載 PERC S300 開機控制器的伺服器部署失敗？

在搭載 PERC S300 開機控制器的 Dell PowerEdge 伺服器，無法用不同版本的 ESXi 部署 OpenManage Integration for VMware vCenter。Dell 自訂的 ESXi 作業系統，不具有 PERC S300 開機控制器的驅動程式，導致作業系統安裝期間無法辨識開機控制器 /HDD。搭載 PERC S300 開機控制器的伺服器，不支援部署 OpenManage Integration for VMware vCenter。

## 按一下韌體連結後，為什麼會顯示錯誤訊息？

如果網路速度緩慢 (9600BPS)，可能會收到通訊錯誤訊息。在 OpenManage Integration for VMware vCenter 的 vSphere 用戶端按一下韌體連結時，可能會顯示錯誤訊息。嘗試取得軟體清查清單時若連線逾時，就會發生這個情況。Microsoft Internet Explorer 會起始此逾時。若為 Microsoft Internet Explorer 第 9/10 版，預設的「接收逾時」值設定為 10 秒。遵照下列步驟即可修復此問題。

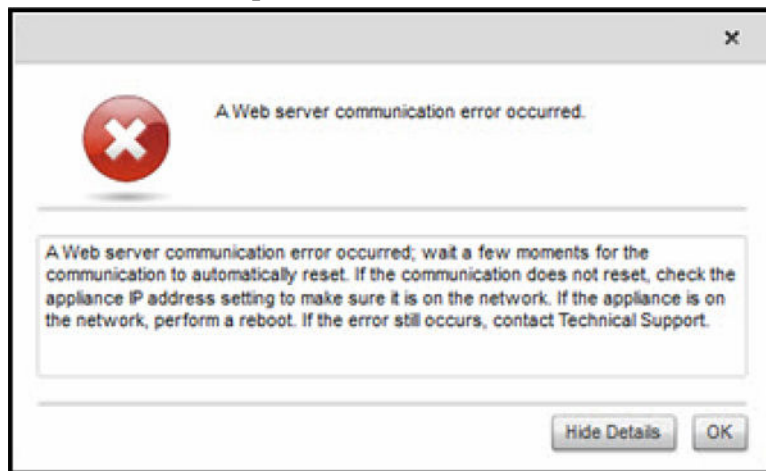


圖 5. 韌體連結通訊錯誤

1. 開啟 Microsoft 登錄編輯程式 (Regedit)。
2. 瀏覽到下列位置：

KHEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings

3. 為 ReceiveTimeout 新增 DWORD 值。
4. 將值設定為 30 秒 (30000) [在您的環境中，這個值可能必須設得更高]。
5. 結束 Regedit。
6. 重新啟動 Internet Explorer。

 註: 光是開啟新的 Internet Explorer 視窗是不夠的，請重新啟動 Internet Explorer 瀏覽器。

## OpenManage Integration for VMware vCenter 設定與支援哪一代 Dell 伺服器的 SNMP 設陷？

OpenManage Integration for VMware vCenter 支援第 12 代以前伺服器的 OMSA SNMP 設限，以及第 12 代伺服器的 iDRAC 設陷。

## OpenManage Integration for VMware vCenter 如何在連結模式支援三個以上的 vCenter ？

在連結模式中，每個虛擬設備最多支援三個 vCenter。如果您有十個以上的 vCenter，每十個有關聯授權的 vCenter，就需要一個新的設備例項。

## OpenManage Integration for VMware vCenter 是否支援連結模式的 vCenter ？

是，無論是否使用連結模式，OpenManage Integration for VMware vCenter 最多都支援 10 個 vCenter。如需 OpenManage Integration for VMware vCenter 在連結模式如何運作的更多資訊，請參閱 *OpenManage Integration for VMware vCenter：在連結模式運作* 白皮書，網址是：[www.Dell.com](http://www.Dell.com)。

## OpenManage Integration for VMware vCenter 有哪些必要的連接埠設定？

 註: 使用 OpenManage Integration for VMware vCenter 相容性視窗提供的 *解決不相容 vSphere 主機連結部署 OMSA 代理程式* 時，OpenManage Integration for VMware vCenter 會啟動 http 用戶端服務，並在 ESXi5.0 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，服務隨即自動停止，連接埠也會關閉。

OpenManage Integration for VMware vCenter 請使用這些連接埠設定。

表 6. 虛擬設備連接埠

連接埠號碼	通訊協定	連接埠類型	最大加密等級	方向	使用	可配置的
21	FTP	TCP	無	輸出	FTP 命令用戶端	無
53	DNS	TCP	無	輸出	DNS 用戶端	無
80	HTTP	TCP	無	輸出	Dell 線上資料存取	無
80	HTTP	TCP	無	輸入	管理主控台	無
162	SNMP 代理程式	UDP	無	輸入	SNMP 代理程式 (伺服器)	無
11620	SNMP 代理程式	UDP	無	輸入	SNMP 代理程式 (伺服器)	無

連接埠號碼	通訊協定	連接埠類型	最大加密等級	方向	使用	可配置的
443	HTTPS	TCP	128 位元	輸入	HTTPS 伺服器	無
443	WSMAN	TCP	128 位元	輸入/輸出	iDRAC/OMSA 通訊	無
4433	HTTPS	TCP	128 位元	輸入	自動探索	無
2049	NFS	UDP	無	輸入/輸出	公用共用	無
4001-4004	NFS	UDP	無	輸入/輸出	公用共用	無
11620	SNMP 代理程式	UDP	無	輸入	SNMP 代理程式 (伺服器)	無

表 7. 受管節點

連接埠號碼	通訊協定	連接埠類型	最大加密等級	方向	使用	可配置的
162,11620	SNMP	UDP	無	輸出	硬體事件	無
443	WSMAN	TCP	128 位元	輸入	iDRAC/OMSA 通訊	無
4433	HTTPS	TCP	128 位元	輸出	自動探索	無
2049	NFS	UDP	無	輸入/輸出	公用共用	無
4001-4004	NFS	UDP	無	輸入/輸出	公用共用	無
443	HTTPS	TCP	128 位元	輸入	HTTPS 伺服器	無
8080	HTTP	TCP		輸入	HTTP 伺服器；下載 OMSA VIB 和解決不相容 vSphere 主機	無
50	RMCP	UDP/TCP	128 位元	輸出	遠端郵件檢查通訊協定	無
51	重要的	UDP/TCP	不適用	不適用	重要的邏輯位址維護	無
5353	mDNS	UDP/TCP		輸入/輸出	多點傳送 DNS	無
631	IPP	UDP/TCP	無	輸出	網際網路列印通訊協定 (IPP)	無
69	TFTP	UDP	128 位元	輸入/輸出	簡單式檔案傳輸 (Trivial File Transfer)	無
111	NFS	UDP/TCP	128 位元	輸入	SUN 遠端程序呼叫 (Portmap)	無
68	BOOTP	UDP	無	輸出	啟動程序通訊協定用戶端	無

## 虛擬設備順利安裝及操作的最低需求是什麼？

下列設定概述最低設備需求：

- Google Chrome 28 版和以上版本。
- Microsoft Internet Explorer 第 9 版和第 10 版
- Mozilla Firefox 22 版和以上版本
- 保留記憶體：2 GB
  - 註：Dell 建議使用 3 GB 效能最佳。
- 磁碟：43.5 GB。
- CPU：2 個虛擬 CPU。

## 成功套用硬體設定檔 (相同使用者在 iDRAC 使用者清單有變更的新憑證) 後，用於裸機探索的使用者密碼為什麼沒有變更？

如果部署僅選取硬體設定檔範本，探索使用的使用者密碼就不會變更為新認證。這是刻意的設計，這樣一來外掛程式才能在日後需要部署時與 iDRAC 通訊。

## 為什麼處理器版本在系統概觀頁面的處理器檢視「不適用」？

若為 PowerEdge 第 12 代以後的 Dell 伺服器，處理器版本寫在品牌欄中。若為 12 代以前的伺服器處理器版本，則是寫在版本欄中。

## 為什麼如果應用裝置 IP 使用 DHCP 並覆寫 DNS 設定，應用裝置重新啟動後，DNS 組態設定會恢復原始設定

這是已知問題；DHCP 的值會取代靜態指派的 DNS 設定。若使用 DHCP 取得 IP 設定，而且 DNS 值是以靜態方式指派，就可能發生這種狀況。DHCP 租用續約或重新啟動應用裝置時，靜態指派的 DNS 設定就會被移除。解決方式：DNS 伺服器設定與 DHCP 的不同時，靜態指派 IP 設定。

受影響的版本：全部

## 為什麼 vCenter 主機與叢集頁面沒有列出我新 iDRAC 版本的詳細資料？


在 vSphere 桌上型用戶端的最近工作窗格內成功完成韌體更新工作之後，請重新整理韌體更新頁面，並確認韌體版本。如果頁面顯示舊版本，那麼請移至 OpenManage Integration for VMware vCenter 的主機相容性頁面，檢查該主機의 CSIOR 狀態。如果未啟用 CSIOR，那麼請啟用 CSIOR，然後重新啟動主機。如果已啟用 CSIOR，那麼請登入 iDRAC 主控台、重設 iDRAC、等待幾分鐘，然後在 vSphere Desktop 用戶端重新整理韌體更新頁面。

## 如何用 OMSA 測試事件設定，模擬溫度硬體故障？

若要確定事件皆正常運作：

1. 在 OMSA 使用者介面，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. 若要確定特定事件已啟用，例如溫度警告，請從左邊樹狀圖選取**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**設為低於目前列出的讀數，例如如果目前讀數為 27，就將閾值設為 **25**。
12. 選取**套用變更**，溫度警告事件隨即產生。若要引起另一個事件，用相同的**設定值**選項還原原始設定。事件會以警告的方式產生，然後回歸正常狀態。如果一切運作正常，導覽至 **vCenter 工作與事件**檢視；溫度探針警告事件應隨即顯示。

 **註:** 重複事件有篩選器；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。事件之間至少等 30 秒，才能查看所有事件。

## 我已經在 Dell 主機系統安裝 OMSA 代理程式，但還是出現未安裝 OMSA 的錯誤訊息。該怎麼辦？

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. 如果使用命令列安裝 OMSA，務必指定 **-c 選項**。如果已安裝 OMSA，請使用 **-c 選項**重新安裝，然後重新啟動服務：

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

若為 ESXi 主機，您必須用 **VMware 遠端 CLI 工具**安裝 **OMSA VIB**，然後重新啟動系統。

## OpenManage Integration for VMware vCenter 啟用鎖定模式時是否支援 ESXi？

是。這個版本的鎖定模式支援 ESXi 5.0 以上的主機。

### 嘗試使用鎖定模式卻失敗。

在鎖定模式新增主機至連線設定檔時，清查展開後卻失敗，表示「找不到遠端存取控制器，或是此主機不支援清查」。鎖定模式的主機不是應該支援清查嗎？

如果將主機設在鎖定模式，或是從鎖定模式移除主機，必須先等待 30 分鐘，才能在 OpenManage Integration for VMware vCenter 執行下一個作業。

### 嘗試用無效的 DUP 更新韌體時，vCenter 主控台的硬體更新工作狀態不是失敗，就是逾時數小時，不過 LC 內的工作狀態卻顯示「失敗」。為什麼會發生這種情況？

更新韌體時若挑選無效的 DUP，vCenter 主控台視窗中的工作狀態會維持「進行中」，但訊息會變成故障原因。這是已知的 VMware 問題，未來版本的 VMware vCenter 將會加以解決。

解決方式：必須手動取消工作。

受影響的版本：全部

## UserVars.CIMoeMProviderEnable With ESXi 4.1 U1 應該使用什麼設定？

將 `UserVars.CIMoemProviderEnabled` 設為 1。

## 我用參考伺服器建立硬體設定檔，但是卻失敗了。該怎麼辦？

請檢查，確定安裝的是最低建議版本的 iDRAC 韌體、Lifecycle Controller 韌體和 BIOS。

若要確定從參考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)**，然後先重新啟動參考伺服器再擷取資料。請參閱 [在參考伺服器設定 CSIOR](#)。

## 我正嘗試在刀鋒伺服器部署 ESXi，結果失敗了。該怎麼辦？

1. 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**，與虛擬設備位於相同的網路上。
3. 如果使用的是 **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。此外，請確定 IP 位址尚未在網路指派。
4. 請確定系統至少找到一個 **虛擬磁碟**。ESXi 也已安裝到內接式 RIPS SD 卡。

## 為什麼我的 Hypervisor 在 R210 II 機器部署失敗？

由於 BIOS 無法從連接的 ISO 啟動，所以 R210 II 系統上的逾時問題會導致 Hypervisor 部署失敗。若要解決這個問題，請在機器手動安裝 Hypervisor。

## 為什麼在部署精靈看到自動探索到的系統，但是卻沒有型號資訊

這通常表示安裝在系統上的韌體版本不符合建議的最低需求。在某些情況下，韌體更新可能還沒在系統登錄。系統冷開機或重新插接刀鋒即可解決這個問題。iDRAC 上新啟用的帳戶必須停用，自動探索必須重新初始化，才能為 OpenManage Integration for VMware vCenter 提供機型資訊和 NIC 資訊。

## NFS 共用以 ESXi ISO 設定成功，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. 確定 iDRAC 能夠偵測到應用裝置。
2. 確定網路執行速度沒有太慢。
3. 確定連接埠 2049、4001-4004 已開啟，防火牆相應設定正確。

## 我該如何強制移除虛擬設備？

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 `com.dell.plugin.openManage_integration_for_VMware_vCenter` 這個擴充碼，然後按一下 **叫用方式**。
7. 輸入 `com.dell.plugin.openManage_integration_for_VMware_vCenter_WebClient` 這個擴充碼，然後按一下 **叫用方式**。

8. 關閉 OpenManage Integration for VMware vCenter 虛擬設備，然後將它刪除。

## 在立即備份畫面輸入密碼時收到錯誤訊息


如果使用的是低解析度螢幕，立即備份視窗就看不到加密密碼欄位。您必須向下捲動頁面才能輸入加密密碼。

## 我的韌體更新失敗。該怎麼做？

檢查虛擬設備記錄，查看工作是否逾時。如果是，iDRAC 必須執行冷開機重設。系統一旦啟動執行，請執行清查或使用韌體索引標籤，檢查更新是否成功。

## 我的 vCenter 登錄失敗。該怎麼做？

vCenter 登錄可能因為通訊問題而失敗，所以如果發生這類問題，解決方式之一就是改用靜態 IP 位址。若要使用靜態 IP 位址，在 OpenManage Integration for VMware vCenter 的主控台索引標籤選取**設定網路** → **編輯裝置**，然後輸入正確的**閘道**和**FQDN** (完全合格的網域名稱)。在編輯 DNS 組態輸入 DNS 伺服器名稱。

 **註:** 請確定虛擬設備可以解析您輸入的 DNS 伺服器。

## 連線設定檔測試認證效能超慢或無回應。

伺服器上的 iDRAC 只有一個使用者 (例如只有**根**)，而使用者處於停用狀態，或是所有使用者都處於停用狀態。與停用狀態的伺服器通訊會導致延遲。若要解決這個問題，可以修正伺服器的停用狀態，或是重設伺服器上的 iDRAC，將根使用者重新啟用為預設設定。

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 GUI**。
3. 導覽至 iDRAC 主控台中的使用者清單，然後執行下列其中一項動作：
  - iDRAC 6：選取 **iDRAC 設定** → **網路/安全性索引標籤** → **使用者索引標籤**。
  - iDRAC 7：選取 **iDRAC 設定** → **使用者索引標籤**。
  - iDRAC 8：選取 **iDRAC 設定** → **使用者索引標籤**。
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. 在選取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**。

## OpenManage Integration for VMware vCenter 是否支援 VMware vCenter Server 應用裝置？

是，OpenManage Integration for VMware vCenter 支援 VMware vCenter Server 應用裝置。

## OpenManage Integration for VMware vCenter 是否支援 vSphere Web 用戶端？

是，OpenManage Integration for VMware vCenter 支援 VMware vSphere Web 用戶端。

## 在管理主控台時，將應用裝置重設為原廠設定後，為什麼更新儲存庫路徑沒有設定為預設路徑？

重設本應用裝置後，移至管理主控台，然後在左窗格按一下**應用裝置管理**。在**應用裝置設定**頁面，**更新儲存庫路徑**沒有變成預設路徑。

**解決方式：**在管理主控台，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。

## 為什麼備份及還原 OpenManage Integration for VMware vCenter 後，警報設定沒有還原？

還原 OpenManage Integration for VMware vCenter 應用裝置備份，不會還原所有警報設定。然而，在 OpenManage Integration for VMware 圖形化使用者介面 (GUI) 中，**警報與事件**欄位會顯示還原的設定。

**解決方式：**在 OpenManage Integration for VMware 圖形化使用者介面 (GUI) 的**管理** → **設定**索引標籤中，手動變更**事件與警報**設定。

## 裸機部署問題

本節處理部署過程所發生的問題。

### 自動探索與信號交換事前準備作業

- 執行自動探索與信號交換之前，請先確定 iDRAC 和 Lifecycle Controller 韌體及 BIOS 版本達到建議下限。
- 您必須在系統或 iDRAC 至少執行一次 CSIOR。

### 硬體組態失敗

- 起始部署工作前，請先確定系統已完成 CSIOR，而且沒有正在重新啟動。
- 強烈建議用複製模式執行 BIOS 組態，參考伺服器的系統才會一模一樣。
- 有些控制器不允許用一部磁碟機建立 RAID 0 陣列。只有高階控制器支援這項功能，套用這類硬體設定檔可能導致失敗。

## 在新購買的系統啟用自動探索

主機系統的自動探索功能預設未啟用，必須在購買時要求啟用。如果在購買時要求啟用自動探索，iDRAC 上的 DHCP 就會啟用，管理員帳戶則會停用。您不一定要為 iDRAC 設定靜態 IP 位址，因為網路上的 DHCP 伺服器就會指派一個給它。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。原廠程序已執行 CSIOR。


如果沒有在購買時要求自動探索，可以用下列方式啟用：

1. 在開機過程按下 **<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

## 與 Dell 公司聯絡

 **註:** 如果無法連線網際網路，則可以在購買發票、包裝單、帳單或 Dell 產品目錄中找到聯絡資訊。

Dell 提供多項線上和電話支援與服務選擇。服務的提供因國家/地區和產品而異，某些服務可能在您所在地區並不提供。若因銷售、技術支援或客戶服務問題要與 Dell 聯絡：

1. 前往 [dell.com/support](http://dell.com/support)
2. 選取您的支援類別。
3. 在網頁底部的 **Choose A Country/Region (選擇國家/地區)** 下拉式選單中確認您所在的國家或地區。
4. 根據您的需求選取適當的服務或支援連結。

## OpenManage Integration for VMware vCenter 相關資訊

- 檢視或下載 PowerEdge™ 伺服器的 Dell 伺服器文件：[Dell PoweEdge 手冊](#)
- Dell OpenManage 系統管理員文件：[Dell OMSA 文件](#)
- Dell Lifecycle Controller 文件：[DLCI 文件](#)

## Dell PowerEdge 伺服器的虛擬化相關事件

下表包含虛擬化相關的嚴重與警告事件，包括第 11、12 和 13 代 PowerEdge 伺服器的事件名稱、說明和嚴重程度。

表 8. 第 11、12 和 13 代 PowerEdge 伺服器的虛擬化相關事件

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	特定系統中的電流感應器超出其警告閾值。	警告	無動作
Dell 電流感應器偵測到故障值	特定系統中的電流感應器超出其故障閾值。	錯誤	讓系統進入維護模式
Dell 電流感應器偵測到無法修復的值	特定系統中的電流感應器偵測到無法修復的錯誤	錯誤	無動作
重新獲得 Dell 冗餘	感應器回到正常值	資訊	無動作
Dell 冗餘降級	特定系統中的冗餘感應器偵測到冗餘裝置有一個元件故障，但裝置仍有冗餘。	警告	無動作
Dell - 冗餘遺失	特定系統中的冗餘感應器偵測到冗餘裝置有一個元件拔除、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	特定系統中的電源感應器超出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	電源已斷開或出故障。	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	特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出可接受的值。	警告	無動作
Dell - 記憶體裝置錯誤	記憶體裝置修正率超出可接受的值，記憶體備用記憶	錯誤	讓系統進入維護模式

事件名稱	說明	重要性	建議動作
	單元已啓用，或發生多位元的 ECC 錯誤。		
Dell - 風扇機櫃插入系統	感應器回到正常值。	資訊	無動作
Dell - 系統已取下風扇機櫃	指定系統已取下風扇機櫃。	警告	無動作
Dell - 系統長時間取下風扇機櫃	特定系統在使用者定義的長度時間下取下風扇機櫃。	錯誤	無動作
Dell - 風扇機櫃感應器偵測到無法修復的值	特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	交流電源線電源中斷，但冗餘足夠，可以將此事件歸類為警告。	警告	無動作
Dell - 交流電源線電源中斷	交流電源線電源中斷，缺乏冗餘必須將此事件歸類為錯誤。	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	特定系統中的處理器感應器處於流速控制狀態。	警告	無動作
Dell - 處理器感應器偵測到故障值	特定系統的處理器感應器已停用，有組態錯誤或發生超出極限溫度。	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	特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	特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
Dell - 電池感應器偵測到故障值	特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	特定系統中的電池感應器偵測到電池故障。	錯誤	無動作

事件名稱	說明	重要性	建議動作
Dell - 熱感應關機保護已啟動	系統設為因錯誤事件而熱感應關機時，就會產生這個訊息。如果溫度感應器讀值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。長時間取下部份系統的風扇機箱也會產生此訊息。	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	特定系統中背板、主機板、CPU 或碟機承載器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	特定系統中背板、主機板或碟機承載器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	特定系統中背板、主機板或碟機承載器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> 的風扇感應器讀值超出警告閾值。	警告	無動作
Dell - 風扇感應器偵測到故障值	特定系統中的風扇感應器偵測到一個或多個風扇有故障。	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	特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	特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

事件名稱	說明	重要性	建議動作
Dell - 儲存裝置：儲存管理錯誤	儲存管理偵測到裝置獨立的錯誤情況。	錯誤	讓系統進入維護模式
Dell - 儲存裝置：控制器警告	控制器警告。詳細資料請參閱 vSphere 用戶端的工作與事件索引標籤。	警告	無動作
Dell - 儲存裝置：控制器故障	控制器故障。詳細資料請參閱 vSphere 用戶端的工作與事件索引標籤。	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
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

事件名稱	說明	重要性	建議動作
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 - 機箱侵入 - 實體安全保護違規	機箱侵入 - 實體安全保護違規	錯誤	無動作
Dell - 機箱侵入 (實體安全保護違規) 事件已清除	機箱侵入 (實體安全保護違規) 事件已清除	資訊	無動作
Dell - CPU 存在 (偵測到處理器存在)	CPU 存在 (偵測到處理器存在)	資訊	無動作
Dell - 系統事件日誌 (SEL) 已滿 (停用登入)	系統事件日誌 (SEL) 已滿 (停用登入)	錯誤	無動作
Dell - 已清除系統事件日誌 (SEL)	已清除系統事件日誌 (SEL)	資訊	無動作
Dell - SD 卡冗餘恢復正常	SD 卡冗餘恢復正常	資訊	無動作
Dell - SD 卡冗餘遺失	SD 卡冗餘遺失	錯誤	無動作
Dell - SD 卡冗餘降級	SD 卡冗餘降級	警告	無動作
Dell - 模組 SD 卡存在 (偵測到 SD 卡存在)	模組 SD 卡存在 (偵測到 SD 卡存在)	資訊	無動作
Dell - 模組 SD 卡故障 (錯誤)	模組 SD 卡故障 (錯誤)	錯誤	無動作
Dell - 模組 SD 卡寫入保護 (警告)	模組 SD 卡寫入保護 (警告)	警告	無動作
Dell - 模組 SD 卡不存在	模組 SD 卡不存在	資訊	無動作
Dell - 監視程式計時器過期	監視程式計時器過期	錯誤	無動作
Dell - 監視程式重設	監視程式重設	錯誤	無動作
Dell - 監視程式電源關閉	監視程式電源關閉	錯誤	無動作
Dell - 監視程式電源週期	監視程式電源週期	錯誤	無動作
Dell - 系統電源超過電源供應器瓦特數	系統電源超過電源供應器瓦特數	錯誤	無動作
Dell - 已清除系統電源超過錯誤	已清除系統電源超過錯誤	資訊	無動作
Dell - 插入電源供應器	插入電源供應器	資訊	無動作

事件名稱	說明	重要性	建議動作
Dell - Internal Dual SD Module 存在	Internal Dual SD Module 存在	資訊	無動作
Dell - Internal Dual SD Module 在線上	Internal Dual SD Module 在線上	資訊	無動作
Dell - Internal Dual SD Module 正常運作	Internal Dual SD Module 正常運作	資訊	無動作
Dell - Internal Dual SD Module 有防寫保護	Internal Dual SD Module 有防寫保護	警告	無動作
Dell - Internal Dual SD Module 可寫入	Internal Dual SD Module 可寫入	資訊	無動作
Dell - 缺少 Integrated Dual SD Module	缺少 Integrated Dual SD Module	錯誤	無動作
Dell - 遺失 Integrated Dual SD Module 冗餘	遺失 Integrated Dual SD Module 冗餘	錯誤	無動作
Dell - Internal Dual SD Module 有冗餘	Internal Dual SD Module 有冗餘	資訊	無動作
Dell - Internal Dual SD Module 沒有冗餘	Internal Dual SD Module 沒有冗餘	資訊	無動作
Dell - Integrated Dual SD Module 故障	Integrated Dual SD Module 故障	錯誤	無動作
Dell - Internal Dual SD Module 離線	Internal Dual SD Module 離線	警告	無動作
Dell - Integrated Dual SD Module 冗餘降級	Integrated Dual SD Module 冗餘降級	警告	無動作
Dell - SD 卡裝置偵測到警告	SD 卡裝置偵測到警告	警告	無動作
Dell - SD 卡裝置偵測到故障	SD 卡裝置偵測到故障	錯誤	無動作
Dell - Integrated Dual SD Module 警告	Integrated Dual SD Module 警告	警告	無動作
Dell - Integrated Dual SD Module 資訊	Integrated Dual SD Module 資訊	資訊	無動作
Dell - Integrated Dual SD Module 冗餘資訊	Integrated Dual SD Module 冗餘資訊	資訊	無動作
Dell - 網路故障或嚴重事件	網路故障或嚴重事件	錯誤	無動作
Dell - 網路警告	網路警告	警告	無動作

事件名稱	說明	重要性	建議動作
Dell - 網路資訊	網路資訊	資訊	無動作
Dell - 實體磁碟故障	實體磁碟故障	錯誤	無動作
Dell - 實體磁碟警告	實體磁碟警告	警告	無動作
Dell - 實體磁碟資訊	實體磁碟資訊	資訊	無動作
Dell - 偵測到 PCI 裝置錯誤	偵測到 PCI 裝置錯誤	錯誤	無動作
Dell - 偵測到 PCI 裝置警告事件	偵測到 PCI 裝置警告事件	警告	無動作
Dell - 偵測到 PCI 裝置資訊事件	偵測到 PCI 裝置資訊事件	資訊	無動作
Dell - 虛擬磁碟分割區故障。	虛擬磁碟分割區故障。	錯誤	無動作
Dell - 虛擬磁碟分割區警告。	虛擬磁碟分割區警告。	警告	無動作
Dell - 纜線故障或嚴重事件	纜線故障或嚴重事件	錯誤	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	無動作
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	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	無動作
Dell - 系統：軟體組態故障。	系統：軟體組態故障。	錯誤	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	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	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	無動作
Dell - 電源使用方式稽核失敗或嚴重事件。	電源使用方式稽核失敗或嚴重事件。	錯誤	無動作
Dell - 組態：軟體組態故障。	組態：軟體組態故障。	錯誤	無動作
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


事件名稱	說明	重要性	建議動作
Dell - 連結狀態警告。	連結狀態警告。	警告	無動作
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 - 儲存安全性警告。	儲存安全性警告。	警告	無動作
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 - PCI 裝置稽核警告。	PCI 裝置稽核警告。	警告	讓系統進入維護模式
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 - 電源使用方式稽核警告。	電源使用方式稽核警告。	警告	無動作
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

## 瞭解自動探索

自動探索這個程序，會將第 11、12 或 13 代 Dell PowerEdge 裸機伺服器，新增至 OpenManage Integration for VMware vCenter 可用的伺服器群。探索到伺服器後，Hypervisor 與硬體部署都可以使用。本附錄提供關於自動探索的充分資訊，協助您完成系統組態。自動探索是 Lifecycle Controller 的功能，可設定新的伺服器，並使用主控台加以登錄。使用這項功能有幾個優點，包括無須費力以手動方式在本機完成新伺服器的組態，支援自動化的方式，由主控台探索已連線網路並插入電源的新伺服器。

自動探索有時因為它所執行的程序，又稱為*探索與信號交換*。啟用自動探索功能的新伺服器插入交流電源並連線網路時，Dell 伺服器的 Lifecycle Controller 會嘗試探索與 Dell 佈建伺服器整合的部署主控台。自動探索接著便會在佈建伺服器和 Lifecycle Controller 之間起始*信號交換*。

OpenManage Integration for VMware vCenter 這個部署主控台含已整合佈建伺服器。佈建伺服器的位置會以不同方式提供給 iDRAC。佈建伺服器位置的 IP 位址或主機名稱，設定為 OpenManage Integration for VMware vCenter 應用裝置虛擬機器的 IP 位址或主機名稱。

 **註：**為自動探索設定的新伺服器，在 24 小時期間每隔 90 秒就會嘗試解析佈建伺服器的位置，之後您便可手動起始自動探索。


OpenManage Integration for VMware vCenter 收到 VMware vCenter 的自動探索要求時，會先驗證 SSL 憑證，然後啟始任何選擇性設定的安全性程序，例如用戶端安全性憑證和根據允許清單驗證。新伺服器的第二個驗證要求，會傳回用來在 iDRAC 設定的暫時使用者名稱/密碼認證。OpenManage Integration for VMware vCenter 會起始 VMware vCenter 的後續呼叫，收集伺服器相關資訊、移除暫時認證，以及設定更多用於管理存取的永久使用者定義認證

如果自動探索成功，就會在目標 iDRAC 建立探索時在**設定** → **部署**頁面所提供的部署認證。自動探索功能接著便會關閉。伺服器現在應該會出現在 OpenManage Integration for VMware vCenter 部署下的可用裸機伺服器群。

目前透過 vSphere 桌上型用戶端即可完成自動探索。

## 自動探索事前準備作業

嘗試探索第 11、12 或更新一代的 Dell PowerEdge 裸機伺服器之前，請先安裝 OpenManage Integration for VMware vCenter。只有第 11 代 Dell PowerEdge 或搭載 iDRAC Express 或 iDRAC Enterprise 的更新版本伺服器，可探索加入 OpenManage Integration for VMware vCenter 的裸機伺服器群。Dell 裸機伺服器的 iDRAC 與 OpenManage Integration for VMware vCenter 虛擬機器之間需要網路連線。

 **註：**已有 Hypervisor 的主機不應探索加入 OpenManage Integration for VMware vCenter，反而應該將 Hypervisor 新增至連線設定檔，然後用主機遵循精靈與 OpenManage Integration for VMware vCenter 同步化


下列條件必須符合，自動探索才會進行：

- **電源：**將伺服器接上電源插座。伺服器電源不需要開啟。

- **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。您可以使用 DHCP 伺服器取得 IP 位址，也可以在 iDRAC 組態公用程式手動指定 IP 位址。
- **其他網路設定**：如果使用的是 DHCP，請啟用從 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。
- **停用帳戶存取**：啟用管理帳戶對 iDRAC 的存取權限，凡是有 iDRAC 帳戶具有管理員權限，請先從 iDRAC Web 主控台予以停用。自動探索成功完成後，管理 iDRAC 帳戶便重新啟用。
- **啟用自動探索**：伺服器的 iDRAC 必須啟用自動探索，自動探索程序才能開始。

## 在 iDRAC 伺服器啟用或停用管理帳戶

請先停用根以外的所有管理帳戶，才能設定自動探索。自動探索程序期間會停用根帳戶。自動探索設定成功後，請返回 Integrated Dell Remote Access Controller 6 圖形化使用者帳戶 (GUI)，重新啟用關閉的帳戶。這項程序適用於第 11、12 和 13 代 Dell PowerEdge 伺服器。

 **註：** 為防止自動探索失敗，不妨在 iDRAC 啟用非管理員帳戶，自動探索若失敗，可進行遠端存取。


1. 在瀏覽器輸入 **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：在左窗格選取 **iDRAC 設定** → **網路/安全性** → **使用者索引標籤**。
  - 若為 iDRAC7：在左窗格選取 **iDRAC 設定** → **使用者驗證** → **使用者索引標籤**。
  - 若為 iDRAC8：在左窗格選取 **iDRAC 設定** → **使用者驗證** → **使用者索引標籤**。
4. 在使用者索引標籤，找到根以外的任何管理帳戶。
5. 若要停用帳戶，在使用者 ID 選取 **ID**。
6. 按一下 **Next** (下一步)。
7. 在使用者組態頁面的一般下方，清除**啟用使用者**核取方塊。
8. 按一下 **Apply** (套用)。
9. 成功設定自動探索後，若要重新啟用每個帳戶，請重複步驟 1 到 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伺服器 (第 11 代 PowerEdge 伺服器)

您必須有 iDRAC 和主機 IP 位址。

如果未指派裸機應用裝置使用原廠的自動探索，您可以手動設定。iDRAC 有兩個使用者介面，用您想要設定的 iDRAC IP 位址即可連線。

成功自動探索裸機伺服器時，隨即建立新的管理員帳戶，或是以信號交換服務傳回的憑證啟用現有帳戶。自動探索前停用的所有其他管理帳戶將不會啟用。您必須在自動探索成功後，重新啟用這些管理員帳戶。請參閱[在 iDRAC 啟用或停用管理帳戶](#)。

 **註：** 如果自動探索因故未成功完成，就無法以遠端方式連線 iDRAC。遠端連線會要求您在 iDRAC 啟用非系統管理帳戶。如果 iDRAC 沒有啟用的帳戶，就只能以本機的方式登入伺服器，並在 iDRAC 啟用帳戶，才能存取 iDRAC。

執行下列步驟，以在目標機器上手動啟用「自動探索」：

1. 將目標系統開機/重新開機。
2. 當您看到按下 **<Ctrl-E>** 以進行遠端存取設定，尚有 5 秒... 訊息時，請按下 **CTRL+E** 以檢視以下畫面。

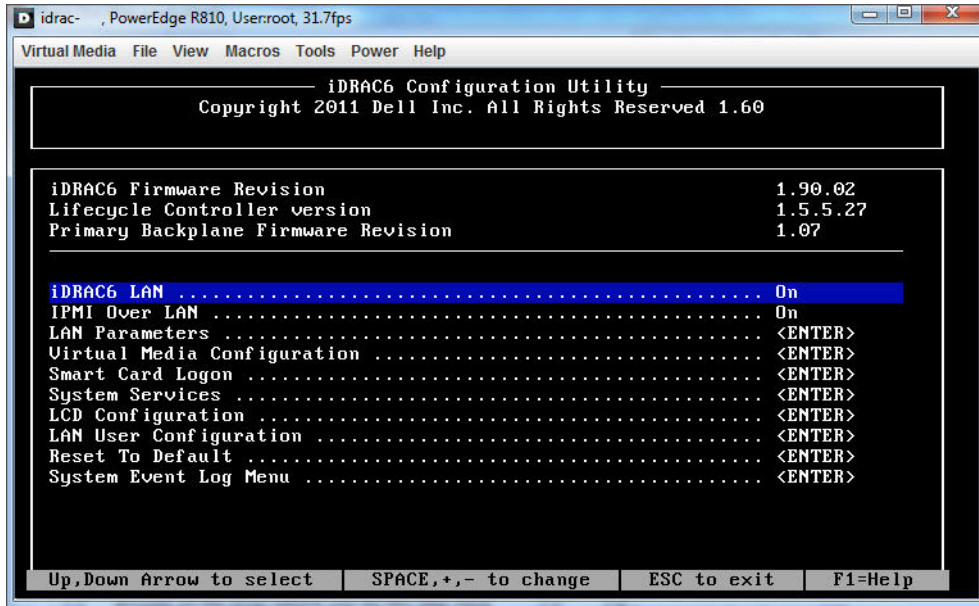


圖 6. 按下 CTRL+E 啟動此畫面。


3. 在 iDRAC6 組態公用程式中，用方向鍵選取 LAN 使用者組態。
4. 使用方向鍵選取自動探索。
5. 使用空白鍵將選項切換為啟用。
6. 使用方向鍵選取佈建伺服器，然後按下 Enter 鍵。
7. 輸入 OMIVV 應用裝置的 IP 位址。
8. 按下 ESC。
9. 使用方向鍵選取帳戶存取。
10. 使用空白鍵將選項切換為停用。
11. 從鍵盤按下 ESC 鍵。
12. 再次按下 ESC 鍵，接收儲存變更的通知，並結束設定。
13. 選取儲存變更並結束，然後按下 Enter 鍵。


將會在下次主機開機循環時自動探索 iDRAC。

## 為自動探索手動設定 PowerEdge 第 12 代以後的伺服器

您必須有 iDRAC 和主機 IP 位址。

透過 Dell 訂購伺服器時，您可在提供佈建伺服器 IP 位址後要求為伺服器啟用自動探索功能。佈建伺服器 IP 位址為 OMIVV 的 IP 位址。在此類情況中，若您從 Dell 收到伺服器並在安裝連接 iDRAC 纜線後開啟伺服器電源，系統即會自動探索伺服器。伺服器會列於「部署」精靈的第一頁。

 **註:** 針對已自動探索的伺服器，系統使用在 **Dell 管理中心** → **設定** → **部署憑證** 下方提供的憑證，以供日後與伺服器進行通訊直至完成作業系統部署為止。成功完成作業系統部署後，會設定關聯連線設定檔中提供的 iDRAC 憑證。

 **註:** 確定停用**伺服器白名單**，否則系統會將要自動探索的伺服器服務標記新增於 **Dell 管理中心** → **設定** → **安全性** 下方的**伺服器白名單**

執行下列步驟，以在目標機器上手動啟用「自動探索」：

1. 將目標系統開機 / 重新開機，然後在初始啟動時按下 F2 以進入「系統設定」。
2. 前往 **iDRAC 設定** → **使用者組態**，然後停用根使用者。確認您在停用根使用者時，該 iDRAC 上已無具有管理員權限且為作用中的其他任何使用者。
3. 按一下**返回**，然後按一下**遠端啟用**。
4. 將**啟用自動探索**設為**啟用**，並將**佈建伺服器**設為 OMIVV 的 IP 位址。
5. 儲存設定。
6. 下次啟動伺服器時即自動探索。成功執行「自動探索」後，即會自動啟用根使用者並自動停用**啟用自動探索**旗標。