

# 安裝和設定 VMware vRealize Orchestrator

vRealize Orchestrator 7.3

本文件支援所列的每個產品版本，並支援後續版本直到新版本的文件取代本文件為止。若要查看本文件的最新版本，請參閱 <http://www.vmware.com/tw/support/pubs>。

ZH\_TW-002546-00

**vmware**<sup>®</sup>

您可以在 VMware 網站上找到最新的技術說明文件，網址為：

<http://www.vmware.com/tw/support/>

VMware 網站還提供了最新的產品更新。

如果您對此文件有何想法，請將您的回應意見提交至：

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

Copyright © 2008–2017 VMware, Inc. 版權所有。 [版權和商標資訊](#)。

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

# 內容

- 安裝及設定 VMware vRealize Orchestrator 7
- 1 VMware vRealize Orchestrator 簡介 9
  - Orchestrator 平台的主要功能 9
  - Orchestrator 使用者類型和相關責任 11
  - Orchestrator 架構 11
  - Orchestrator 外掛程式 12
- 2 Orchestrator 系統需求 13
  - Orchestrator Appliance 的硬體需求 13
  - Orchestrator 支援的瀏覽器 13
  - Orchestrator 資料庫需求 14
  - Orchestrator Appliance 包含的軟體 14
  - 國際化支援層級 14
  - Orchestrator 網路連接埠 15
- 3 設定 Orchestrator 元件 17
  - vCenter Server 安裝 17
  - 驗證方法 17
  - 設定 Orchestrator 資料庫 17
- 4 安裝 Orchestrator 19
  - 下載並部署 Orchestrator Appliance 19
    - 開啟 Orchestrator Appliance 的電源並開啟首頁 20
    - 變更根密碼 20
    - 在 vRealize Orchestrator 應用裝置中啟用或停用 SSH 系統管理員登入 21
    - 設定 Orchestrator Appliance 的網路設定 21
- 5 初始組態 23
  - 設定獨立式 Orchestrator 伺服器 23
    - 設定具有 vRealize Automation 驗證的獨立式 Orchestrator 伺服器 23
    - 設定具有 vSphere 驗證的獨立式 Orchestrator 伺服器 25
  - Orchestrator 網路連接埠 26
  - 設定 Orchestrator 資料庫連線 27
    - 匯入資料庫 SSL 憑證 27
    - 設定資料庫連線 28
    - 匯出 Orchestrator 資料庫 29
    - 匯入 Orchestrator 資料庫 29

- 管理憑證 30
  - 管理 Orchestrator 憑證 30
- 設定 Orchestrator 外掛程式 31
  - 管理 Orchestrator 外掛程式 32
  - 將外掛程式解除安裝 32
- Orchestrator 啟動選項 33
- Orchestrator 可用性和延展性 33
  - 設定 Orchestrator 叢集 34
  - 監控 Orchestrator 叢集 36
- 控制中心的角色型存取管理 36
  - 在控制中心中將使用者角色指派給使用者 37
- 設定客戶經驗改進計劃 37
  - VMware 收到的資訊類別 37
  - 參與客戶經驗改進計劃 38
  
- 6 使用 API 服務 39**
  - 使用 REST API 管理 SSL 憑證和金鑰儲存區 39
    - 使用 REST API 刪除 SSL 憑證 39
    - 使用 REST API 匯入 SSL 憑證 40
    - 使用 REST API 建立金鑰儲存區 40
    - 使用 REST API 刪除金鑰儲存區 41
    - 使用 REST API 新增金鑰 41
  - 使用控制中心 REST API 自動化 Orchestrator 組態 42
  
- 7 其他設定選項 43**
  - 重新設定驗證 43
    - 變更驗證提供者 43
    - 變更驗證參數 44
  - 匯出 Orchestrator 組態 44
  - 匯入 Orchestrator 組態 45
  - 設定工作流程執行內容 46
  - Orchestrator 記錄檔案 46
    - 持續型記錄 47
    - Orchestrator 記錄組態 47
    - 檢查工作流程 48
    - 篩選 Orchestrator 記錄 48
  
- 8 組態使用案例和疑難排解 49**
  - 將 Orchestrator 登錄為 vCenter Server 延伸模組 49
  - 解除登錄 Orchestrator 驗證 50
  - 變更 SSL 憑證 50
    - 新增憑證到本機存放區 50
    - 變更 Orchestrator 硬體裝置管理網站的憑證 51
  - 取消正在執行的工作流程 51
  - 啟用 Orchestrator 伺服器偵錯 52
  - 備份 Orchestrator 組態和元素 52

- 備份與還原 vRealize Orchestrator 54
  - 備份 vRealize Orchestrator 54
  - 還原 vRealize Orchestrator 執行個體 55
- 使用 Site Recovery Manager 進行 Orchestrator 的災難復原 56
  - 為 vSphere Replication 設定虛擬機器 56
  - 建立保護群組 57
  - 建立復原計劃 57
  - 在資料夾中組織復原計劃 58
  - 編輯復原計劃 58
- 9 設定系統內容 61**
  - 透過非管理員停用 Orchestrator 用戶端的存取權 61
  - 為工作流程和動作設定伺服器檔案系統存取 62
    - js-io-rights.conf 檔案中的規則允許對 Orchestrator 系統的寫入權限 62
    - 為工作流程和動作設定伺服器檔案系統存取 62
  - 為工作流程和動作設定作業系統命令的存取 63
  - 設定 Java 類別的 JavaScript 存取 63
  - 設定自訂逾時內容 64
- 10 下一步 67**
  - 從 Orchestrator 應用裝置網路主控台登入 Orchestrator 用戶端 67
- 索引 69



# 安裝及設定 VMware vRealize Orchestrator

---

〈安裝及設定 VMware vRealize Orchestrator〉一章提供安裝、升級和設定 VMware® vRealize Orchestrator 的資訊與說明。

## 主要對象

本章資訊主要提供給較進階的 vSphere 管理員，以及熟悉虛擬機器技術和資料中心運作的資深系統管理員。





# VMware vRealize Orchestrator 簡介

---

VMware vRealize Orchestrator 是一個開發與程序自動化平台，提供可延伸工作流程的程式庫，讓您能夠建立與執行自動執行、可設定的程序，以管理 VMware 產品及第三方技術。

vRealize Orchestrator 會自動執行 VMware 與第三方應用程式 (例如服務台、變更管理系統，及 IT 資產管理系統) 的管理與運作工作。

本章節討論下列主題：

- “Orchestrator 平台的主要功能,” 第 9 頁
- “Orchestrator 使用者類型和相關責任,” 第 11 頁
- “Orchestrator 架構,” 第 11 頁
- “Orchestrator 外掛程式,” 第 12 頁

## Orchestrator 平台的主要功能

Orchestrator 由各自不同的三層組成：提供協調工具所需一般功能的協調平台、整合子系統控制的外掛程式架構，以及工作流程的程式庫。Orchestrator 是可藉由新外掛程式和程式庫加以擴充的開放平台，而且可透過 REST API 整合到更大型的架構。

下列清單列出主要的 Orchestrator 功能。

- |             |   |
|-------------|---|
| <b>持續性</b>  | 生產級資料庫用於儲存相關資訊，例如程序、工作流程狀態，以及組態資訊。  |
| <b>集中管理</b> | Orchestrator 可用來集中管理您的程序。具有完整版本歷程記錄的應用程式伺服器型平台，能夠將指令碼和程序相關的原始類型儲存於同一個儲存位置。如此一來，您即可避免在伺服器上存有無版本設定和適當變更控制項的指令碼。 |

<b>檢查點</b>	工作流程的每個步驟均儲存於資料庫，這可避免必須重新啟動伺服器時造成的資料遺失。此功能對於長時間執行的程序而言特別實用。
<b>控制中心</b>	控制中心介面提供一個集中式的管理介面，用於執行階段作業、工作流程監視、統一的記錄存取和組態，以及工作流程執行和系統資源之間的相互關聯，提升 vRealize Orchestrator 執行個體的管理效率。vRealize Orchestrator 記錄機制由於額外的記錄檔而更加完善，這個記錄檔會收集 vRealize Orchestrator 引擎輸送量的各種效能指標。
<b>版本設定</b>	所有 Orchestrator 平台物件都有相關聯的版本歷程記錄。版本歷程記錄可用於將程序散佈至專案階段或位置時的基本變更管理。
<b>指令碼引擎</b>	<p>Mozilla Rhino JavaScript 引擎可用來建立 Orchestrator 平台的建置區塊。指令碼引擎由於具備基本版本控制、變數類型檢查、命名空間管理和例外狀況處理而更加強化。引擎能夠用於下列建置區塊：</p> <ul style="list-style-type: none"> <li>■ 動作</li> <li>■ 工作流程</li> <li>■ 原則</li> </ul>
<b>工作流程引擎</b>	<p>工作流程引擎可用於業務程序自動化。它使用下列物件建立工作流程的逐步程序自動化：</p> <ul style="list-style-type: none"> <li>■ Orchestrator 提供的工作流程和動作</li> <li>■ 客戶建立的自訂建置區塊</li> <li>■ 外掛程式新增至 Orchestrator 的物件</li> </ul> <p>使用者、其他工作流程、排程或原則都能夠啟動工作流程。</p>
<b>原則引擎</b>	您能夠使用原則引擎來監視和產生事件，以便回應 Orchestrator 伺服器或外掛技術中不斷變化的情況。原則能夠彙總平台或任何外掛程式的事件，協助您處理任何整合式技術中不斷變化的情況。
<b>安全性</b>	<p>Orchestrator 提供下列進階安全功能：</p> <ul style="list-style-type: none"> <li>■ 公開金鑰基礎結構 (PKI)，可簽署和加密伺服器之間匯入和匯出的內容。</li> <li>■ 數位版權管理 (DRM)，可控制如何檢視、編輯和轉散佈的匯出內容。</li> <li>■ 安全通訊端層 (SSL)，提供桌面用戶端與伺服器之間的加密通訊，以及 Web 前端的 HTTPS 存取。</li> <li>■ 進階存取權限管理，可控制對於程序以及這些程序控管的物件進行的存取。</li> </ul>
<b>加密</b>	vRealize Orchestrator 使用 FIPS 相容的進階加密標準 (AES)，透過 256 位元加密金鑰進行字串加密。加密金鑰是隨機產生的，在不屬於叢集的應用裝置上，加密金鑰都是不重複的。叢集中的所有節點都共用相同的加密金鑰。

## Orchestrator 使用者類型和相關責任

Orchestrator 按照全域使用者角色的特定責任提供不同的工具和介面。在 Orchestrator 中，可以有具備完整權限的使用者、屬於管理員群組 (管理員) 的使用者，以及權限有限且不屬於管理員群組 (使用者) 的使用者。

### 具備完整權限的使用者

Orchestrator 管理員與開發人員具備同等的管理權限，但是在責任上的分工不同。

#### 管理員

這個角色有 Orchestrator 平台功能的完整存取權。基本的管理責任包括下列項目：

- 安裝及設定 Orchestrator
- 管理 Orchestrator 和應用程式的存取權限
- 匯入和匯出套件
- 執行工作流程和排程工作
- 管理匯入元素的版本控制
- 建立新的工作流程和外掛程式

#### 開發人員

這個使用者類型有 Orchestrator 平台功能的完整存取權。開發人員獲得授與 Orchestrator 用戶端介面的存取權，而且有下列責任：

- 建立應用程式來擴充 Orchestrator 平台功能
- 自訂現有的工作流程，並建立新的工作流程和外掛程式，使程序自動進行

### 權限有限的使用者

#### 使用者

使用者能夠在 Orchestrator 用戶端中，執行和排程管理員或開發人員提供的工作流程與原則。

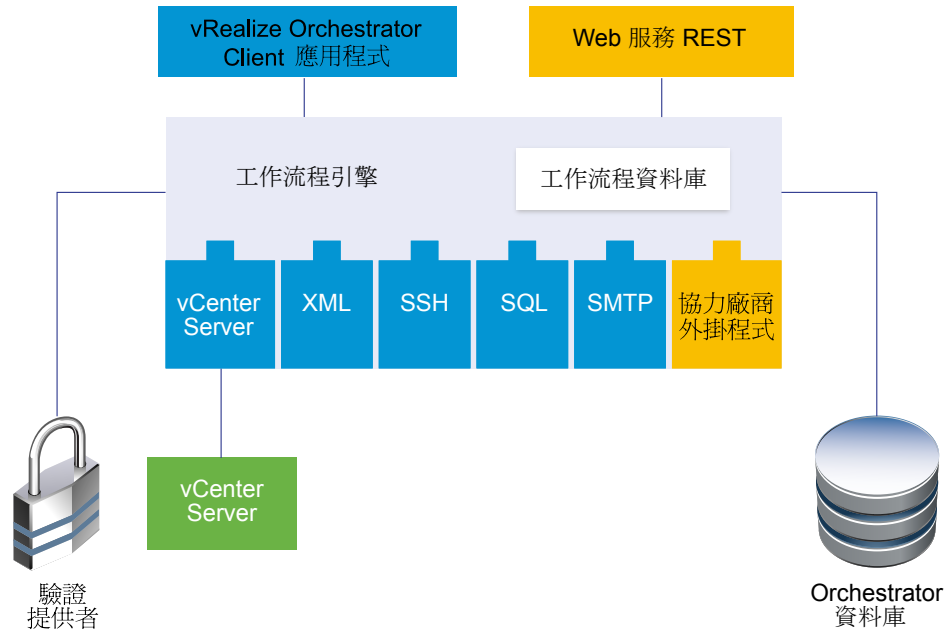
## Orchestrator 架構

Orchestrator 包含工作流程式庫和工作流引擎，能夠讓您建立和執行使協調程序自動化的工作流程。對於 Orchestrator 透過一系列外掛程式存取的不同技術物件，您可以執行工作流程。

Orchestrator 提供一組標準的外掛程式，包括 vCenter Server 的外掛程式，以便您協調外掛程式公開的不同環境中出現的工作。

Orchestrator 也提供開放式架構，能夠讓您將外部第三方應用程式外掛至協調平台。對於您自行定義的外掛技術物件，您可以執行工作流程。Orchestrator 會連接到驗證提供者來管理使用者帳戶，以及連接到資料庫以儲存執行工作流程的資訊。您可以存取 Orchestrator、Orchestrator 工作流程，以及透過 Orchestrator 用戶端介面或透過 Web 服務公開的物件。

圖 1-1 VMware vRealize Orchestrator 架構



## Orchestrator 外掛程式

外掛程式允許您使用 Orchestrator 存取並控制外部技術和應用程式。開放 Orchestrator 外掛程式使用外部技術，將可讓您整合工作流程中存取該外部技術物件和函數的物件和函數。

您可以使用外掛程式存取的外部技術包含虛擬化管理工具、電子郵件系統、資料庫、目錄服務，以及遠端控制介面。

Orchestrator 提供一系列的標準外掛程式，您可以使用這些外掛程式將 VMware vCenter Server API 和電子郵件功能等技術整合到工作流程中。透過使用外掛程式，您可以自動化新 IT 服務的提供，或調整既有 vRealize 自動化基礎架構及應用程式服務的功能。此外，您可以使用 Orchestrator 的開放外掛程式架構，開發存取其他應用程式的外掛程式。

VMware 開發的 Orchestrator 外掛程式以 .vmoapp 檔案發佈。若需要更多有關 VMware 開發並發佈的 Orchestrator 外掛程式之資訊，請參閱 [http://www.vmware.com/support/pubs/vco\\_plugins\\_pubs.html](http://www.vmware.com/support/pubs/vco_plugins_pubs.html)。若需要更多有關第三方 Orchestrator 外掛程式之資訊，請參閱 <https://solutionexchange.vmware.com/store/vco>。

## Orchestrator 系統需求

---

您的系統必須符合 Orchestrator 正常運作所需的技術需求。

如需 vCenter Server、vSphere Web Client、vRealize Automation 和其他 VMware 解決方案支援版本的清單，以及相容資料庫版本的清單，請參閱 [VMware 產品互通性對照表](#)。

本章節討論下列主題：

- “Orchestrator Appliance 的硬體需求,” 第 13 頁
- “Orchestrator 支援的瀏覽器,” 第 13 頁
- “Orchestrator 資料庫需求,” 第 14 頁
- “Orchestrator Appliance 包含的軟體,” 第 14 頁
- “國際化支援層級,” 第 14 頁
- “Orchestrator 網路連接埠,” 第 15 頁

### Orchestrator Appliance 的硬體需求

Orchestrator Appliance 是已預先完成設定、採用 Linux 技術的虛擬機器。在您開始部署裝置之前，請先確認您的系統符合最低硬體需求。

Orchestrator Appliance 配備以下硬體組態：

- 2 顆 CPU
- 6 GB 記憶體
- 17 GB 硬碟

請勿減少預設的記憶體大小，Orchestrator 伺服器至少需要 2 GB 的可用記憶體才能運作。

### Orchestrator 支援的瀏覽器

控制中心需要網頁瀏覽器。

您必須使用下列其中一種瀏覽器連線至控制中心。

- Microsoft Internet Explorer 10 或更新版本
- Mozilla Firefox
- Google Chrome

## Orchestrator 資料庫需求

Orchestrator 伺服器需要資料庫。預先設定的 Orchestrator PostgreSQL 資料庫可供生產環境使用。端視環境而定，您也可以使用外部資料庫。

如需支援的資料庫版本清單，請參閱 [VMware 產品互通性對照表](#)。

## Orchestrator Appliance 包含的軟體

Orchestrator Appliance 是預先設定的虛擬機器，已針對執行 Orchestrator 進行最佳化。應用裝置隨附預先安裝的軟體。

Orchestrator Appliance 套件包含下列軟體：

- 適用於 VMware 64 位元版本的 SUSE Linux Enterprise Server 11 Update 3
- PostgreSQL
- Orchestrator

預設 Orchestrator Appliance 資料庫組態可供生產使用。

---

**備註** 若要在生產環境中使用 Orchestrator Appliance，您必須設定 Orchestrator 伺服器以透過 vRealize Automation 或 vSphere 進行驗證。如需有關設定驗證提供者的詳細資訊，請參閱“[設定獨立式 Orchestrator 伺服器](#)”第 23 頁。

---

如需設定用於生產環境的資料庫相關資訊，請參閱“[設定 Orchestrator 資料庫](#)”第 17 頁。

## 國際化支援層級

Orchestrator 控制中心包含西班牙文、法文、德文、繁體中文、簡體中文、韓文和日文地區設定。Orchestrator 用戶端支援國際化第 1 級。

## Orchestrator 的非 ASCII 字元支援

雖然 Orchestrator 用戶端並未當地語系化，但仍可在非英文作業系統上執行及支援非 ASCII 文字。

**表格 2-1.** Orchestrator GUI 的非 ASCII 字元支援

非 ASCII 字元的支援				
Orchestrator 項目	說明欄位	名稱欄位	輸入與輸出參數	屬性
動作	是	否	否	否
資料夾	是	是	-	-
組態元素	是	是	-	否
套件	是	是	-	-
原則	是	是	-	-
原則範本	是	是	-	-
資源元素	是	是	-	-
工作流程	是	是	否	否
工作流程呈現顯示群組和輸入步驟	是	是	-	-

## Oracle 資料庫的非 ASCII 字元支援

若要將字元以正確的格式儲存在 Oracle 資料庫中，請將 NLS\_CHARACTER\_SET 參數設定為 AL32UTF8，然後再設定資料庫連線並建置 Orchestrator 的資料表結構。此設定對國際化環境而言至關重要。

## Orchestrator 網路連接埠

Orchestrator 使用特定連接埠與其他系統進行通訊。這些連接埠是以無法變更的預設值來設定。

### 預設組態連接埠

若要提供 Orchestrator 服務，您必須設定預設連接埠，並設定防火牆允許傳入 TCP 連線。

**備註** 如果您使用自訂外掛程式，則可能需要其他連接埠。

**表格 2-2.** VMware vRealize Orchestrator 預設組態連接埠

連接埠	數字	通訊協定	來源	目標	說明
虛擬應用裝置管理介面	5480	TCP			應用裝置系統設定介面的存取連接埠。
HTTP 伺服器連接埠	8280	TCP	使用者網頁瀏覽器	Orchestrator 伺服器	傳送至 Orchestrator 預設 HTTP Web 連接埠 8280 的要求將重新導向至預設 HTTPS Web 連接埠 8281。
HTTPS 伺服器連接埠	8281	TCP	使用者網頁瀏覽器	Orchestrator 伺服器	Web Orchestrator 首頁的存取連接埠。
Web 組態 HTTPS 存取連接埠	8283	TCP	使用者網頁瀏覽器	Orchestrator 組態	Orchestrator 組態 Web UI 的 SSL 存取連接埠。

### 外部通訊連接埠

您必須設定防火牆允許傳出連線，Orchestrator 才能與外部服務進行通訊。

**表格 2-3.** VMware vRealize Orchestrator 外部通訊連接埠

連接埠	數字	通訊協定	來源	目標	說明
SQL Server	1433	TCP	Orchestrator 伺服器	Microsoft SQL Server	與設定為 Orchestrator 資料庫的 Microsoft SQL Server 執行個體進行通訊所用的連接埠。
PostgreSQL	5432	TCP	Orchestrator 伺服器	PostgreSQL 伺服器	與設定為 Orchestrator 資料庫的 PostgreSQL 伺服器進行通訊所用的連接埠。
Oracle	1521	TCP	Orchestrator 伺服器	Oracle DB Server	與設定為 Orchestrator 資料庫的 Oracle Database Server 進行通訊所用的連接埠。
SMTP 伺服器連接埠	25	TCP	Orchestrator 伺服器	SMTP 伺服器	用於電子郵件通知的連接埠。
vCenter Server API 連接埠	443	TCP	Orchestrator 伺服器	vCenter Server	vCenter Server API 通訊連接埠由 Orchestrator 用來從協調的 vCenter Server 執行個體取得虛擬基礎結構和虛擬機器資訊。





## 設定 Orchestrator 元件

---

下載和部署 Orchestrator Appliance 時，將預先設定 Orchestrator 伺服器。部署後，服務將自動啟動。

若要加強 Orchestrator 安裝的可用性和擴充性，請遵循下列準則：

- 安裝並設定資料庫，然後設定 Orchestrator 連線到該資料庫。
- 安裝並設定驗證提供者，然後設定 Orchestrator 使用該驗證提供者。
- 安裝負載平衡器伺服器，並將其設定為在兩個或更多個 Orchestrator 伺服器之間散佈工作流程。

本章節討論下列主題：

- “vCenter Server 安裝,” 第 17 頁
- “驗證方法,” 第 17 頁
- “設定 Orchestrator 資料庫,” 第 17 頁

### vCenter Server 安裝

增加 Orchestrator 安裝中的 vCenter Server 執行個體數目會導致 Orchestrator 要管理更多工作階段。如果作用中的工作階段太多，可能會造成 Orchestrator 在執行 10 個以上的 vCenter Server 連線時發生逾時情況。

如需支援的 vCenter Server 版本清單，請參閱《VMware 產品互通性對照表》。

---

**備註** 如果您的網路有足夠的頻寬和延遲，您可以在 Orchestrator 安裝中，在不同的虛擬機器上執行多個 vCenter Server 執行個體。如果您要使用 LAN 改善 Orchestrator 和 vCenter Server 之間的通訊，則必須使用 100 MB 的線路。

---

### 驗證方法

若要驗證並管理使用者權限，Orchestrator 需要連線至 vRealize Automation 或 vSphere 伺服器執行個體。

下載並部署 Orchestrator Appliance 時，您必須設定與 vRealize Automation 或 vSphere 的連線。

### 設定 Orchestrator 資料庫

Orchestrator 需要資料庫才能儲存工作流程和動作。

下載並部署 Orchestrator Appliance 時，Orchestrator 伺服器會預先設定為搭配使用連同應用裝置散佈的 PostgreSQL 資料庫。預設 Orchestrator Appliance 資料庫組態可供生產使用。不過，若要在高負載生產環境中使用 Orchestrator，您必須從控制中心設定個別的資料庫並設定 Orchestrator 與其搭配使用。

Orchestrator 伺服器支援 Oracle、Microsoft SQL Server 和 PostgreSQL 資料庫。

---

**備註** Microsoft SQL Server 資料庫與 Oracle 資料庫的支援已經過時，未來的版本將取消支援。

---

設定 Orchestrator 資料庫的一般工作流程包含下列步驟：

- 1 建立資料庫。如需建立資料庫的詳細資訊，請參閱資料庫提供者的說明文件。
- 2 啟用資料庫的遠端連線。
- 3 設定資料庫連線參數。如需詳細資訊，請參閱“[設定 Orchestrator 資料庫連線](#),” 第 27 頁。

如果您打算安裝 Orchestrator 叢集，您必須設定資料庫接受多個連線，以便接受叢集中不同 Orchestrator 伺服器執行個體的連線。

資料庫安裝會影響 Orchestrator 效能。在並非安裝 Orchestrator 伺服器的機器上安裝資料庫。此方法可確保 JVM 和資料庫伺服器不共用 CPU、RAM 和 I/O。

資料庫的位置相當重要，因為 Orchestrator 伺服器上的幾乎每個活動都會觸發資料庫的作業。若要避免資料庫連線延遲，請連接到距離最靠近您的 Orchestrator 伺服器，且其所在網路有最高可用頻寬的資料庫伺服器。

Orchestrator 資料庫的大小會由於安裝和如何處理工作流程 Token 而有所不同。對於每個 vCenter Server 物件配置大約 50 KB，對於每次工作流程執行配置 4 KB。



**警告** 確定安裝 Orchestrator 資料庫的機器上至少有 1 GB 的磁碟空間可供使用。

硬碟空間不足可能導致 Orchestrator 伺服器和用戶端無法正常運作。

---

# 安裝 Orchestrator

Orchestrator 是由伺服器元件與用戶端元件所組成。

可安裝的 Orchestrator 用戶端可在 64 位元的 Windows、Linux 和 Mac 電腦上執行。

若要使用 Orchestrator，您須啟動 Orchestrator 伺服器服務，然後啟動 Orchestrator 用戶端。

您可以使用 Orchestrator 控制中心變更預設的 Orchestrator 組態設定。

## 下載並部署 Orchestrator Appliance

若要下載並安裝 Orchestrator Appliance，請透過範本進行部署。

### 先決條件

- 確認已安裝並執行 vCenter Server。
- 確認部署應用裝置的主機符合最低硬體需求。如需詳細資訊，請參閱“[Orchestrator Appliance 的硬體需求](#)”第 13 頁。
- 如果您的系統單獨隔離而沒有網際網路連線，您必須從 VMware 網站下載應用裝置的 .ova 檔。

### 程序

- 1 以管理員身分登入 vSphere Web Client。
- 2 在 vSphere Web Client 中，選取虛擬機器有效父系物件的詳細目錄物件，如資料中心、資料夾、叢集、資源集區或主機。
- 3 選取**動作 > 部署 OVF 範本**。
- 4 輸入 .ova 檔的路徑或 URL，然後按**下一步**。
- 5 檢閱 OVF 範本詳細資料，然後按**下一步**。
- 6 接受授權合約中的條款，然後按**下一步**。
- 7 輸入部署的應用裝置名稱和位置，然後按**下一步**。
- 8 選取用來做為應用裝置主機執行目的地的叢集、資源集區或 vApp，然後按**下一步**。

- 9 選取應用裝置虛擬磁碟和儲存區所用的儲存格式。

格式	說明
完整佈建消極式歸零	以預設的完整格式建立虛擬磁碟。虛擬磁碟所需的空間會在建立時加以配置。在建立程序中，系統不會清除保留在實體裝置中的任何資料，但是稍後從虛擬機器首次執行寫入操作時，您可按需要將這些資料歸零。
完整佈建積極式歸零	支援叢集功能，如 <b>Fault Tolerance</b> 。虛擬磁碟所需的空間會在建立時加以配置。如果實體裝置有任何資料，在建立虛擬磁碟時會將這些資料歸零。建立此類格式的磁碟所需的時間可能會比建立其他格式的磁碟久得多。
精簡佈建格式	節省硬碟空間。對於精簡佈建磁碟，可根據選取的磁碟大小值來佈建磁碟所需的資料存放區空間。精簡佈建磁碟啟動時所佔空間小，一開始只使用與初始作業所需大小相同的資料存放區空間。

- 10 選取要啟用的選項，並設定根使用者帳戶的初始密碼。

您的初始密碼必須至少有 8 個字元。

---

**重要事項** Orchestrator Appliance 的根帳戶密碼將於 365 天後到期。您可以使用根使用者身分登入 Orchestrator Appliance 並執行 `passwd -x number_of_days name_of_account`，以延長帳戶到期時間。如果要將 Orchestrator Appliance 的根密碼增加至不受時間限制，請執行 `passwd -x 99999 root`。

---

- 11 (選擇性) 設定網路設定，然後按下一步。

依預設，Orchestrator Appliance 使用 DHCP。您可以從應用裝置網路主控台中變更此設定，並指派固定 IP 位址。

- 12 檢閱 [即將完成] 頁面，然後按一下完成。

Orchestrator Appliance 至此部署完成。

## 開啟 Orchestrator Appliance 的電源並開啟首頁

若要使用 Orchestrator Appliance，您必須開啟其電源，並為虛擬裝置取得 IP 位址。

### 程序

- 1 以管理員身分登入 vSphere Web Client。
- 2 在 Orchestrator Appliance 上方按滑鼠右鍵，並選取**電源 > 開啟電源**。
- 3 在**摘要**標記中檢視 Orchestrator Appliance 的 IP 位址。
- 4 在網頁瀏覽器中，前往 Orchestrator Appliance 虛擬機器的 IP 位址。

`http://orchestrator_appliance_ip`

## 變更根密碼

為了安全性理由，您可以變更 Orchestrator Appliance 的根密碼。

---

**重要事項** Orchestrator Appliance 的根帳戶密碼將於 365 天後到期。您可以使用根使用者身分登入 Orchestrator Appliance 並執行 `passwd -x number_of_days name_of_account`，以延長帳戶到期時間。如果要將 Orchestrator Appliance 的根密碼增加至不受時間限制，請執行 `passwd -x 99999 root` 命令。

---

### 先決條件

- 下載並部署 Orchestrator Appliance。
- 請確認應用裝置已啟動且正在執行中。

**程序**

- 1 在網頁瀏覽器中，前往 [https://orchestrator\\_appliance\\_ip:5480](https://orchestrator_appliance_ip:5480)。
- 2 請輸入應用裝置使用者名稱與密碼。
- 3 按一下**管理員**索引標記。
- 4 在**目前管理員密碼**文字方塊裡輸入目前的根密碼。
- 5 在**新的管理員密碼**和**重新輸入新的管理員密碼**文字方塊裡輸入新的密碼。
- 6 按一下**變更密碼**。

您已成功變更 Orchestrator Appliance 的 Linux 根使用者密碼。

**在 vRealize Orchestrator 應用裝置中啟用或停用 SSH 系統管理員登入**

您可以啟用或停用使用 SSH 以 root 身分登入 Orchestrator Appliance 的能力。

**先決條件**

- 下載並部署 Orchestrator Appliance。
- 請確認應用裝置已啟動且正在執行中。

**程序**

- 1 在網頁瀏覽器中，前往 [https://orchestrator\\_appliance\\_ip:5480](https://orchestrator_appliance_ip:5480)。
- 2 以根使用者身分登入。
- 3 在**系統管理**索引標記中，選取 **SSH 服務已啟用**，以啟用 Orchestrator SSH 服務。
- 4 (選擇性) 按一下**系統管理員 SSH 登入已啟用**，允許使用 SSH 以 root 身分登入 Orchestrator Appliance。
- 5 按一下**儲存設定**。

SSH 狀態顯示為**執行中**。

**設定 Orchestrator Appliance 的網路設定**

設定 Orchestrator Appliance 適用的網路設定，以利指派靜態 IP 位址和定義代理設定。

**先決條件**

- 下載並部署 Orchestrator Appliance。
- 請確認應用裝置已啟動且正在執行中。

**程序**

- 1 在網頁瀏覽器中，前往 [https://orchestrator\\_appliance\\_ip:5480](https://orchestrator_appliance_ip:5480)。
- 2 以根使用者身分登入。
- 3 在**網路**索引標記中按一下**位址**。
- 4 選取應用裝置取得 IP 位址設定的方式。

選項	描述
<b>DHCP</b>	從 DHCP 伺服器取得 IP 設定。這是預設設定。
<b>靜態</b>	使用靜態 IP 設定。輸入 IP 位址、網路遮罩及閘道。

根據網路設定而定，您可能需要選取 IPv4 和 IPv6 位址類型。

- 5 (選擇性) 輸入必要的網路組態資訊。
- 6 按一下**儲存設定**。
- 7 (選擇性) 設定代理設定並按一下**儲存設定**。

## 初始組態

使用 Orchestrator 啟動自動化管理系統及應用程式之前，您必須先將其設為使用外部驗證提供者，並且指派角色給不同使用者。您也可以設定外部資料庫、匯入 CA 簽署的憑證、安裝外掛程式或變更預設記錄組態。

本章節討論下列主題：

- [“設定獨立式 Orchestrator 伺服器,”](#) 第 23 頁
- [“Orchestrator 網路連接埠,”](#) 第 26 頁
- [“設定 Orchestrator 資料庫連線,”](#) 第 27 頁
- [“管理憑證,”](#) 第 30 頁
- [“設定 Orchestrator 外掛程式,”](#) 第 31 頁
- [“Orchestrator 啟動選項,”](#) 第 33 頁
- [“Orchestrator 可用性和延展性,”](#) 第 33 頁
- [“控制中心的角色型存取管理,”](#) 第 36 頁
- [“設定客戶經驗改進計劃,”](#) 第 37 頁

### 設定獨立式 Orchestrator 伺服器

儘管 Linux 虛擬機器已預先設定 Orchestrator Appliance，您仍須遵循組態設定精靈的步驟，才能存取 Orchestrator 控制中心。

#### 設定具有 vRealize Automation 驗證的獨立式 Orchestrator 伺服器

若要準備讓 Orchestrator Appliance 提供使用，您必須設定主機設定以及驗證提供者。您可以透過 vRealize Automation 元件登錄設定 Orchestrator 以進行驗證。

##### 先決條件

- 下載並部署 vRealize Orchestrator 7.3 Appliance。請參閱[“下載並部署 Orchestrator Appliance,”](#) 第 19 頁。
- 安裝並設定 vRealize Automation 以及確認您的 vRealize Automation 伺服器正在執行。請參閱 vRealize Automation 說明文件。

若您計劃建立叢集：

- 設定負載平衡器以在多個 vRealize Orchestrator 執行個體之間散佈流量。如需詳細資訊，請參閱 [《vRealize Orchestrator 負載平衡》](#)。

- 設定您計劃做為共用資料庫的外部資料庫，讓資料庫接受來自不同 Orchestrator 執行個體的連線。

## 程序

- 1 存取控制中心以啟動組態設定精靈。
  - a 瀏覽至 `https://your_orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter`。
  - b 使用您在 OVA 部署期間輸入的密碼，以**根使用者**身分登入。
- 2 選取**獨立式 Orchestrator** 部署類型。  
只要選取此類型，即表示您設定了單一 Orchestrator 節點或叢集中的第一個 Orchestrator 節點。
- 3 按一下**變更**，設定要提供控制中心讓使用者存取的主機名稱。

---

**備註** 如果您即將設定 Orchestrator 叢集，請輸入負載平衡器虛擬伺服器的主機名稱。

---

- 4 設定驗證提供者。
  - a 在設定驗證提供者頁面上，從**驗證模式**下拉式功能表選取 **vRealize Automation**。
  - b 在**主機位址**文字方塊中，輸入您的 vRealize Automation 主機位址，然後按一下**連線**。
  - c 按一下**接受憑證**。
  - d 在**使用者名稱**和**密碼**文字方塊中，輸入使用者帳戶的認證 (在 vRealize Automation 中設定用於進行 SSO 連線)。  
依預設，SSO 帳戶為**管理員**，而預設的承租人名稱是 **vsphere.local**。
  - e 在**管理員群組**文字方塊中，輸入管理員群組的名稱，然後按一下**搜尋**。  
例如：**vsphere.local\administrators**
  - f 在群組清單中，按兩下群組名稱加以選取。
    - a 按一下**儲存變更**。  
系統會顯示您已成功儲存的訊息，並將您重新導向控制中心的主要視圖。
- 5 (選擇性) 設定 Orchestrator 節點以使用外部共用資料庫。如需詳細資訊，請參閱“[設定資料庫連線](#)”第 28 頁
- 6 按一下控制中心首頁右上角的設定圖示，然後按一下**登出**。  
您就會從控制中心登出**根**帳戶。

---

**備註** 根帳戶無法再次存取控制中心。

---

- 7 按一下**返回控制中心**。  
系統會將您重新導向 VMware Identity Manager (vIDM) 登入畫面。

---

**備註** 如果您使用負載平衡器伺服器，則僅可透過負載平衡器虛擬伺服器位址存取控制中心。

---

- 8 以 **vsphere.local** 承租人中的**管理員**使用者帳戶登入控制中心。  
您可以在控制中心查看**角色型存取管理**功能表選項。

您已順利完成控制中心組態設定。

## 下一個

- 確認 **VRA** 是否為**授權**頁面上設定的授權提供者。
- 確認是否已在**驗證組態**頁面上正確地設定節點。



## 設定具有 vSphere 驗證的獨立式 Orchestrator 伺服器

您可使用 vSphere 驗證模式，以 vCenter Single Sign-On 伺服器登錄 Orchestrator 伺服器。將 vCenter Single Sign-On 驗證與 vCenter Server 6.0 和更新版本搭配使用。

### 先決條件

- 下載並部署 vRealize Orchestrator 7.3 Appliance。請參閱“[下載並部署 Orchestrator Appliance](#),” 第 19 頁。
- 在 vCenter Single Sign-On 伺服器執行中的狀態下安裝與設定 vCenter Server。如需相關資訊，請參閱 vSphere 說明文件。

若您計劃建立叢集：

- 設定負載平衡器以在多個 vRealize Orchestrator 執行個體之間散佈流量。如需詳細資訊，請參閱《[vRealize Orchestrator 負載平衡](#)》。
- 設定您計劃做為共用資料庫的外部資料庫，讓資料庫接受來自不同 Orchestrator 執行個體的連線。

### 程序

- 1 存取控制中心以啟動組態設定精靈。
  - a 瀏覽至 `https://your_orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter`。
  - b 使用您在 OVA 部署期間輸入的密碼，以**根使用者**身分登入。
- 2 選取**獨立式 Orchestrator** 部署類型。  
只要選取此類型，即表示您設定了單一 Orchestrator 節點或叢集中的第一個 Orchestrator 節點。
- 3 按一下**變更**，設定要提供控制中心讓使用者存取的主機名稱。

---

**備註** 如果您即將設定 Orchestrator 叢集，請輸入負載平衡器虛擬伺服器的主機名稱。

---

- 4 設定驗證提供者。
  - a 在設定驗證提供者頁面上，從**驗證模式**下拉式功能表選取 **vSphere**。
  - b 在**主機位址**文字方塊中，輸入您的 vSphere 主機位址，然後按一下**連線**。
  - c 按一下**接受憑證**。
  - d 在**使用者名稱**和**密碼**文字方塊中，輸入 vCenter Single Sign-On 網域的本機管理員帳戶憑證。  
依預設，此帳戶為 `administrator@vsphere.local`。

---

**備註** 預設承租人的名稱已預先設定。

---

- e 在**管理員群組**文字方塊中，輸入管理員群組的名稱，然後按一下**搜尋**。  
例如：`vsphere.local\Administrators`
  - f 在群組清單中，按兩下群組名稱加以選取。
    - a 按一下**儲存變更**。  
系統會顯示您已成功儲存的訊息，並將您重新導向控制中心的主要視圖。
- 5 (選擇性) 設定 Orchestrator 節點以使用外部共用資料庫。如需詳細資訊，請參閱“[設定資料庫連線](#),” 第 28 頁

- 按一下控制中心首頁右上角的設定圖示，然後按一下**登出**。

您就會從控制中心登出**根**帳戶。

---

**備註** 根帳戶無法再次存取控制中心。

---

- 按一下**返回控制中心**。

系統會將您重新導向 vCenter Single Sign-On 登入畫面。

---

**備註** 如果您使用負載平衡器伺服器，則僅可透過負載平衡器虛擬伺服器位址存取控制中心。

---

- 以您在**步驟 4e**中所設定的**管理員群組**的身分 (依預設為 **administrator@vsphere.local**)，登入「控制中心」。

您可以在控制中心查看**角色型存取管理**功能表選項。

您已順利完成控制中心組態設定。

#### 下一個

- 確認 CIS 是否為**授權**頁面上設定的授權提供者。
- 確認是否已在**驗證組態**頁面上正確地設定節點。

## Orchestrator 網路連接埠

Orchestrator 使用特定連接埠與其他系統進行通訊。這些連接埠是以無法變更的預設值來設定。

### 預設組態連接埠

若要提供 Orchestrator 服務，您必須設定預設連接埠，並設定防火牆允許傳入 TCP 連線。

---

**備註** 如果您使用自訂外掛程式，則可能需要其他連接埠。

---

**表格 5-1.** VMware vRealize Orchestrator 預設組態連接埠

連接埠	數字	通訊協定	來源	目標	說明
虛擬應用裝置管理介面	5480	TCP			應用裝置系統設定介面的存取連接埠。
HTTP 伺服器連接埠	8280	TCP	使用者網頁瀏覽器	Orchestrator 伺服器	傳送至 Orchestrator 預設 HTTP Web 連接埠 8280 的要求將重新導向至預設 HTTPS Web 連接埠 8281。
HTTPS 伺服器連接埠	8281	TCP	使用者網頁瀏覽器	Orchestrator 伺服器	Web Orchestrator 首頁的存取連接埠。
Web 組態 HTTPS 存取連接埠	8283	TCP	使用者網頁瀏覽器	Orchestrator 組態	Orchestrator 組態 Web UI 的 SSL 存取連接埠。

### 外部通訊連接埠

您必須設定防火牆允許傳出連線，Orchestrator 才能與外部服務進行通訊。

表格 5-2. VMware vRealize Orchestrator 外部通訊連接埠

連接埠	數字	通訊協定	來源	目標	說明
SQL Server	1433	TCP	Orchestrator 伺服器	Microsoft SQL Server	與設定為 Orchestrator 資料庫的 Microsoft SQL Server 執行個體進行通訊所用的連接埠。
PostgreSQL	5432	TCP	Orchestrator 伺服器	PostgreSQL 伺服器	與設定為 Orchestrator 資料庫的 PostgreSQL 伺服器進行通訊所用的連接埠。
Oracle	1521	TCP	Orchestrator 伺服器	Oracle DB Server	與設定為 Orchestrator 資料庫的 Oracle Database Server 進行通訊所用的連接埠。
SMTP 伺服器 連接埠	25	TCP	Orchestrator 伺服器	SMTP 伺服器	用於電子郵件通知的連接埠。
vCenter Server API 連接埠	443	TCP	Orchestrator 伺服器	vCenter Server	vCenter Server API 通訊連接埠由 Orchestrator 用來從協調的 vCenter Server 執行個體取得虛擬基礎結構和虛擬機器資訊。

## 設定 Orchestrator 資料庫連線

Orchestrator 伺服器需要資料庫才能儲存資料。

下載並部署 Orchestrator Appliance 時，Orchestrator 伺服器會設定為搭配使用在應用裝置中預先安裝的 PostgreSQL 資料庫。

預先設定的 Orchestrator PostgreSQL 資料庫可供生產環境使用。為了提升高負載生產環境的效能，可安裝個別的關聯式資料庫管理系統 (RDBMS) 並建立 Orchestrator 的資料庫。如需關於如何建立 Orchestrator 資料庫的詳細資訊，請參閱“設定 Orchestrator 資料庫，”第 17 頁。若要搭配 Orchestrator 使用外部資料庫，請設定資料庫進行遠端連線。

### 匯入資料庫 SSL 憑證

如果您的資料庫使用 SSL，您必須將 SSL 憑證匯入至 [控制中心]，在 Orchestrator 與資料庫之間建立安全的連線。

#### 先決條件

- 設定資料庫以存取 SSL。請參閱資料庫的說明文件，以取得設定指示。
- 取得自我簽署的伺服器憑證，或由憑證授權機構單位簽署的憑證。
- 明確指定信任憑證，以便正確執行 SSL 授權。

#### 程序

- 1 以**管理員**身分登入控制中心。
- 2 按一下**憑證**。
- 3 在**信任憑證**索引標記，按一下**匯入**。
- 4 從 URL 或檔案載入資料庫 SSL 憑證。

選項	動作
從 URL 或 Proxy URL 匯入	輸入資料庫伺服器的 URL： <b>https://your_database_server_IP_address</b> 或 <b>your_database_server_IP_address:port</b>
從檔案匯入	取得資料庫的 SSL 憑證檔案，瀏覽至檔案位置將其匯入。

匯入的憑證會出現在 [信任 SSL 憑證] 清單，Orchestrator 與資料庫間的安全連線也已成功建立。

## 下一個

設定資料庫連線時，您必須在控制中心的**設定資料庫**頁面啟用 SSL。

## 設定資料庫連線

若要建立 Orchestrator 資料庫的連線，您必須設定資料庫連線參數。

### 先決條件

- 設定搭配 Orchestrator 伺服器使用的新資料庫。請參閱“[設定 Orchestrator 資料庫](#),” 第 17 頁。
- 如果您使用的 SQL Server 資料庫設定為使用動態連接埠，請確定 SQL Server 瀏覽器服務正在執行中。
- 使用 Microsoft SQL Server 資料庫時若要避免交易鎖死，必須啟用 ALLOW\_SNAPSHOT\_ISOLATION 和 READ\_COMMITTED\_SNAPSHOT 資料庫選項。
- 如果 Microsoft SQL Server 資料庫使用動態連接埠，請確保 SQL Server 瀏覽器正在執行。
- 若要避免使用 Oracle 資料庫時發生 ORA-01450 錯誤，請確認您已正確設定資料庫區塊大小。最小必要大小取決於 Oracle 資料庫索引正在使用的區塊大小。
- 若要將字元以正確的格式儲存在 Oracle 資料庫中，請將 NLS\_CHARACTER\_SET 參數設定為 AL32UTF8，然後再設定資料庫連線並建置 Orchestrator 的資料表結構。此設定對國際化環境而言至關重要。
- 若要設定 Orchestrator 透過安全連線與資料庫通訊，請務必匯入資料庫 SSL 憑證。如需詳細資訊，請參閱“[匯入資料庫 SSL 憑證](#),” 第 27 頁。

### 程序

- 1 以**管理員**身分登入控制中心。
- 2 按一下**設定資料庫**。
- 3 從**資料庫類型**下拉式功能表中，選取您要 Orchestrator 伺服器使用的資料庫類型。

選項	說明
<b>Oracle</b>	設定 Orchestrator 搭配 Oracle 資料庫執行個體使用。
<b>SQL Server</b>	設定 Orchestrator 搭配 Microsoft SQL Server 資料庫執行個體使用。
<b>PostgreSQL</b>	設定 Orchestrator 搭配 PostgreSQL 資料庫執行個體使用。
<b>處理中 DerbyDB</b>	設定 Orchestrator 搭配處理中 DerbyDB 資料庫使用。 <b>備註</b> 您不得使用 DerbyDB。

**備註** Microsoft SQL Server 資料庫與 Oracle 資料庫的支援已經過時，未來的版本將取消支援。

- 4 輸入資料庫連線參數，然後按一下**儲存變更**。

選項	說明
<b>伺服器位址</b>	資料庫伺服器 IP 位址或 DNS 名稱。 此選項適用於所有的資料庫。
<b>連接埠</b>	資料庫伺服器連接埠用於與您的資料庫通訊。 此選項適用於所有的資料庫。
<b>使用 SSL</b>	選取 <b>使用 SSL</b> 可使用 SSL 連線至資料庫。若要使用此選項，您必須確定將資料庫 SSL 憑證匯入至 Orchestrator。 此選項適用於所有的資料庫。
<b>資料庫名稱</b>	資料庫的唯一全名。在初始化參數檔案的 SERVICE_NAMES 參數中，指定資料庫名稱。 此選項只對 SQL Server 和 PostgreSQL 資料庫有效。

選項	說明
<b>使用者名稱</b>	Orchestrator 用來連線與操作所選資料庫的使用者名稱。您選取的名稱必須是目標資料庫上具有 <b>db_owner</b> 權限的有效使用者。 此選項適用於所有的資料庫。 <b>備註</b> 預先設定的 PostgreSQL 資料庫的預設使用者名稱為 <b>vmware</b> 。
<b>密碼</b>	使用者名稱的密碼。 此選項適用於所有的資料庫。 <b>備註</b> 預先設定的 PostgreSQL 資料庫的預設密碼為 <b>vmware</b> 。
<b>執行個體名稱 (如果有的話)</b>	可由資料庫初始化參數檔案中的 <b>INSTANCE_NAME</b> 參數識別的資料庫執行個體名稱。 此選項只對 SQL Server 和 Oracle 資料庫有效。
<b>網域</b>	若要使用 Windows 驗證，請輸入 SQL Server 機器的網域名稱，例如 <i>company.org</i> 。 若要使用 SQL 驗證，請將此文字方塊保留空白。 此選項僅對 SQL Server 有效，可指定您要使用 Windows 或 SQL Server 驗證。
<b>使用 Windows 驗證模式 (NTLMv2)</b>	選取此選項可在使用 Windows 驗證時傳送 NTLMv2 回應。 此選項只對 SQL Server 有效。

如果指定的參數正確，會出現一則訊息表示資料庫連線成功。

- 更新 Orchestrator 的表格結構 (若需要)。
- 按一下 **儲存變更**。

資料庫連線設定成功。

## 匯出 Orchestrator 資料庫

建立含有伺服器資料庫完整備份的封存檔。此資料庫僅是在 PostgreSQL 並於 Linux 上執行時才能匯出。

### 程序

- 以**管理員**身分登入控制中心。
- 按一下**匯出資料庫**。
- 選取是否匯出工作流程 Token 和資料庫相關記錄事件。
- 按一下**匯出資料庫**。

控制中心可以在您安裝 Orchestrator 伺服器的機器上建立 `vco-db-dump-databaseName@hostname.gz` 檔案。您可以使用此檔案複製和還原系統。

## 匯入 Orchestrator 資料庫

您可以在重新安裝 Orchestrator 或系統故障時，匯入先前匯出的資料庫。

### 先決條件

新的 Orchestrator 資料庫裡不可有任何內容。

### 程序

- 以**管理員**身分登入控制中心。
- 按一下**匯入資料庫**。
- 瀏覽並選取您從上次安裝作業匯出的 `.gz` 檔案。

#### 4 按一下匯入資料庫

畫面會顯示訊息表示資料庫已成功匯入，新系統也順利取得舊系統的資料庫。

## 管理憑證

憑證乃針對特定伺服器而發出，其中包含伺服器公開金鑰的資訊，可供您簽署 Orchestrator 中建立的所有元素，達到保證真確性的效果。用戶端收到來自於您伺服器的元素 (一般是套件) 時，用戶端會驗證您的身分識別，並決定是否信任您的簽章。

---

**重要事項** 如果 Orchestrator 使用內含式 Apache Derby 資料庫，則您無法變更伺服器憑證。

---

### 管理 Orchestrator 憑證

您可以從控制中心的憑證頁面或透過 Orchestrator 用戶端，使用 [組態] 工作流程類別中的 [SSL 信任管理員] 工作流程來管理 Orchestrator 憑證。

#### 將憑證匯入至 Orchestrator 信任存放區

控制中心使用安全連線與 vCenter Server、關聯式資料庫管理系統 (RDBMS)、LDAP、Single Sign-On 和其他伺服器進行通訊。您可以從 URL 或 PEM 編碼的檔案匯入所需的 SSL 憑證。每次要使用伺服器執行個體的 SSL 連線時，您必須從憑證頁面的信任憑證索引標籤匯入對應的憑證，並匯入對應的 SSL 憑證。

您可以從 URL 網址或 PEM 編碼的檔案將 SSL 憑證載入 Orchestrator 中。

選項	說明
從 URL 或 Proxy URL 匯入	遠端伺服器的 URL: <b>https://your_server_IP_address</b> 或 <b>your_server_IP_address:port</b>
從檔案匯入	PEM 編碼憑證檔案的路徑。 如需有關匯入 PEM 編碼之憑證檔案的詳細資訊，請參閱〈 <a href="#">透過控制中心匯入信任憑證</a> 〉第 31 頁。

#### 產生自我簽署的伺服器憑證

Orchestrator Appliance 包含按照應用裝置之網路設定自動產生的自我簽署憑證。如果應用裝置的網路設定變更，您必須手動產生新的自我簽署憑證。您可以建立自我簽署憑證來確保提供加密通訊，以及套件的簽章。不過，收件者無法確定自我簽署的套件實際上是由您的伺服器所發出，而非宣稱是您本人的第三方所發出的套件。若要提供您伺服器的身分識別，請使用憑證授權機構簽署的憑證。

您可以透過控制中心裡憑證頁面中的 Orchestrator 伺服器 SSL 憑證索引標籤產生自我簽署憑證。

選項	說明
簽章演算法	產生數位簽章的加密演算法。
一般名稱	Orchestrator 伺服器的主機名稱。
組織	您組織的名稱。例如，VMware。
組織單位	您組織單位的名稱。例如，R&D。
國碼	國碼縮寫。例如，US。

Orchestrator 會產生您環境專用的伺服器憑證。憑證公開金鑰的詳細資料會出現在 Orchestrator 伺服器 SSL 憑證索引標籤中。私密金鑰儲存於 Orchestrator 資料庫的 vmo\_keystore 資料表中。

## 匯入 Orchestrator 伺服器 SSL 憑證

vRealize Orchestrator 使用 SSL 憑證在安全通訊期間向用戶端和遠端伺服器表明身分。依預設，Orchestrator 包含按照應用裝置的網路設定所自動產生的自我簽署 SSL 憑證。您可以匯入憑證授權機構簽署的 SSL 憑證，以避免憑證信任錯誤。

您必須匯入憑證授權機構簽署的憑證成為包含公開和私密金鑰的 PEM 編碼檔案。

### 封裝簽署憑證

從 Orchestrator 伺服器匯出的套件會經數位簽署。匯入、匯出或產生將用於簽署套件的新憑證。封裝簽署憑證是一種數位身分識別，用於確保加密通訊和 Orchestrator 套件的簽章。

Orchestrator Appliance 包含按照應用裝置的網路設定自動產生的封裝簽署憑證。如果應用裝置的網路設定變更，您必須手動產生新的封裝簽署憑證。

---

**備註** Orchestrator Appliance 包含初始 Orchestrator 組態期間自動產生的自我簽署封裝簽署憑證。您可以變更封裝簽署憑證，此後便會使用新憑證來簽署未來所有匯出的套件。

---

### 透過控制中心匯入信任憑證

若要與其他伺服器安全進行通訊，Orchestrator 伺服器必須能驗證其身分識別。在此情況下，您可能需要將遠端實體的 SSL 憑證匯入 Orchestrator 信任存放區。若要信任憑證，您可以透過建立特定 URL 連線，或直接採用 PEM 編碼檔的方式，將憑證匯入至信任存放區。

#### 先決條件

尋找您希望 Orchestrator 可透過 SSL 連線之目標伺服器的完整網域名稱。

#### 程序

- 1 透過 SSH，以 **root** 身分登入 Orchestrator Appliance。
- 2 執行命令擷取遠端伺服器的憑證。
 

```
openssl s_client -connect host_or_dns_name:secure_port
```

  - a 若您使用非加密的連接埠，請透過 `openssl` 命令使用 `starttls` 及必要的通訊協定。
 

```
openssl s_client -connect host_or_dns_name:25 -starttls smtp
```
- 3 將 -----BEGIN CERTIFICATE----- 到 -----END CERTIFICATE----- 索引標籤的文字複製到文字編輯器，並另存為檔案。
- 4 以**管理員**身分登入控制中心。
- 5 前往**憑證**頁面。
- 6 在**信任憑證**索引標籤上，按一下**匯入**，然後選取從**PEM 編碼的檔案匯入**選項。
- 7 瀏覽至憑證檔案，然後按一下**匯入**。

您已順利將遠端伺服器憑證匯入至 Orchestrator 信任存放區。

## 設定 Orchestrator 外掛程式

預設的 Orchestrator 外掛程式只能透過工作流程設定。

如果要設定任何預設的 Orchestrator 外掛程式，需要從 Orchestrator 用戶端使用特定的工作流程進行。

## 管理 Orchestrator 外掛程式

在控制中心的**管理外掛程式**頁面中，您可以檢視安裝在 Orchestrator 中之所有外掛程式的清單，並執行基本管理動作。

### 變更外掛程式記錄層級

您可以只變更特定外掛程式的記錄層級，而不需變更 Orchestrator 的記錄層級。

### 安裝新外掛程式

透過 Orchestrator 外掛程式，Orchestrator 伺服器能夠與其他軟體產品整合。Orchestrator Appliance 包含一組預先安裝的外掛程式，您也可以安裝自訂外掛程式。

所有 Orchestrator 外掛程式都是從控制中心安裝。可使用的副檔名是 `.vmoapp` 和 `.dar`。`.vmoapp` 檔可包含多個 `.dar` 檔，而且可安裝作為應用程式，而 `.dar` 檔包含與一個外掛程式相關聯的所有資源。

### 停用外掛程式

您可以取消選取外掛程式旁邊的**啟用**核取方塊，將外掛程式停用。

此動作不會移除外掛程式檔案。如需在 Orchestrator 中解除安裝外掛程式的詳細資訊，請參閱[“將外掛程式解除安裝”](#) 第 32 頁。

## 將外掛程式解除安裝

您可以使用控制中心停用外掛程式，但此動作並不會將外掛程式檔案從 Orchestrator Appliance 檔案系統移除。若要移除外掛程式檔案，您必須登入 Orchestrator Appliance 並手動移除外掛程式檔案。

### 程序

- 1 從 Orchestrator Appliance 刪除外掛程式。
  - a 透過 SSH，以 **root** 身分登入 Orchestrator Appliance。
  - b 使用文字編輯器開啟 `/etc/vco/app-server/plugins/_VSOPuginInstallationVersion.xml` 檔案。
  - c 刪除您要移除之外掛程式對應的程式碼。
  - d 瀏覽至 `/var/lib/vco/app-server/plugins` 目錄。
  - e 刪除包含您要移除之外掛程式的 `.dar` 封存。
- 2 重新啟動 vRealize Orchestrator 服務。
 

```
service vco-configurator restart && service vco-server restart
```
- 3 以**管理員**身分登入控制中心。
- 4 前往**管理外掛程式**頁面，確認是否已移除外掛程式。
- 5 透過 Orchestrator 用戶端，刪除和該外掛程式相關的套件和資料夾。
  - a 登入 Orchestrator 用戶端。
  - b 從左上角的下拉式功能表中選取**設計**。
  - c 按一下**套件**視圖。
  - d 在您要刪除的套件上按一下滑鼠右鍵，然後選取**刪除包含內容的元素**。

---

**備註** 鎖定在唯讀狀態的 Orchestrator 元素不會刪除，例如標準程式庫中的工作流程。

---



- e 在右上角的工具功能表中，選取**使用者喜好設定**。  
**喜好設定**內容功能表隨即開啟。
  - f 在**一般**頁面，選取**允許刪除非空白資料夾**的核取方塊。  
現在，您可以一鍵刪除包括子資料夾和工作流程在內的整個資料夾。
  - g 按一下**工作流程**視圖。
  - h 刪除您要移除之外掛程式的資料夾。
  - i 按一下**動作**視圖。
  - j 刪除您要移除之外掛程式的動作模組。
- 6 重新啟動 vRealize Orchestrator 服務。

您已移除所有與外掛程式相關的自訂工作流程、動作、原則、組態、設定和資源。

## Orchestrator 啟動選項

第一次啟動 Orchestrator 可能需要 5 至 10 分鐘，因為伺服器會安裝資料庫資料表中的 Orchestrator 外掛程式內容。

控制中心的組態變更會觸發 Orchestrator 伺服器服務自動重新啟動。在控制中心的**啟動選項**頁面上，您可以手動啟動、停止和重新啟動 Orchestrator 伺服器服務。

**啟動選項**頁面會顯示 vco-server 服務的狀態。

狀態	說明
執行中	Orchestrator 伺服器服務正確初始化並執行。
未定義	Orchestrator 伺服器服務正在啟動。
已停止	Orchestrator 伺服器服務未執行。

在叢集化環境中，按一下**啟動選項**頁面上的**重新啟動**按鈕，僅重新啟動本機節點的 Orchestrator 伺服器服務。

**備註** 若要確認您存取的是叢集中的哪一個 Orchestrator 執行個體，請瀏覽至控制中心的 **Orchestrator 叢集管理** 頁面，然後查看**本機節點**核取符號。

若要重新啟動叢集中所有節點的 Orchestrator 伺服器服務，您必須透過 SSH 登入每個節點，然後執行 `service vco-server restart` 命令。

## Orchestrator 可用性和延展性

若要增加 Orchestrator 服務的可用性，請在一個有共用資料庫的叢集中開啟數個 Orchestrator 伺服器執行個體。vRealize Orchestrator 以單一執行個體運作，除非 Orchestrator 經設定要作為叢集的一部分運作。

### Orchestrator 叢集

具有相同的伺服器和外掛程式組態的數個 Orchestrator 伺服器執行個體，會在一個叢集中一同運作，並共用一個資料庫。

所有的 Orchestrator 伺服器執行個體透過交換活動訊號來彼此溝通。活動訊號是節點在特定時間間隔寫入到叢集共用資料庫的時間戳記。網路問題、未回應的資料庫伺服器，或者過載都可能導致 Orchestrator 叢集節點停止回應。如果作用中的 Orchestrator 伺服器執行個體在容錯移轉的逾時時間內傳送活動訊號失敗，該執行個體將視為沒有回應。容錯移轉的逾時時間為活動訊號時間間隔乘以容錯移轉活動訊號數量的數值。該值可用來定義不可靠的節點，並可依據可用資源以及生產負載進行自訂。

Orchestrator 節點中斷資料庫的連線時，會進入待命模式，而且會停留在此模式中，直到資料庫連線恢復為止。叢集中的其他節點會控制作用中的工作，方法是從上次未完成的项目繼續執行所有中斷的工作流程，這些项目包含可編寫指令碼工作和工作流程引動過程等等。

Orchestrator 並未提供監控叢集狀態和傳送容錯移轉通知的內建工具。您可以使用負載平衡器等外部元件監控叢集狀態。若要檢查節點是否正在執行，您可以使用健全狀況狀態 REST API 服務，網址是 [https://your\\_orchestrator\\_server\\_IP\\_or\\_DNS\\_name:8281/vco/api/healthstatus](https://your_orchestrator_server_IP_or_DNS_name:8281/vco/api/healthstatus)，然後檢查節點狀態，或造訪網址 [https://your\\_orchestrator\\_server\\_IP\\_or\\_DNS\\_name:8283/vco-controlcenter/docs/](https://your_orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter/docs/) 以監控控制中心狀態。

## 設定 Orchestrator 叢集

若要擴充 Orchestrator 服務並以高可用性模式使用 Orchestrator，您可以建立含有兩個或多個 Orchestrator 執行個體的叢集。

### 設定具有 vRealize Automation 驗證之 Orchestrator 7.3 執行個體的叢集

若要形成叢集，您可以設定 Orchestrator 執行個體使用 vRealize Automation 做為驗證提供者，並在該叢集中加入其他 Orchestrator 節點。

Orchestrator 叢集至少包含兩個共用同一個資料庫的 Orchestrator 伺服器執行個體。

#### 先決條件

- 設定獨立式 Orchestrator 伺服器節點。請參閱“[設定具有 vRealize Automation 驗證的獨立式 Orchestrator 伺服器](#),” 第 23 頁。
- 同步其上安裝有 Orchestrator 伺服器執行個體之虛擬機器的時鐘。
- 設定負載平衡器以在多個 vRealize Orchestrator 執行個體之間散佈流量。請參閱《[vRealize Orchestrator 負載平衡](#)》。

#### 程序

- 1 存取您要新增之目標叢集的節點的控制中心，以啟動組態設定精靈。
  - a 瀏覽至 [https://your\\_orchestrator\\_server\\_IP\\_or\\_DNS\\_name:8283/vco-controlcenter](https://your_orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter)。
  - b 使用您在 OVA 部署期間輸入的密碼，以**根使用者**身分登入。
- 2 選取**叢集化 Orchestrator** 部署類型。
 

只要選擇此類型，即表示您要將節點加入現有的 Orchestrator 叢集。
- 3 在**主機名稱**文字方塊中，輸入第一個 Orchestrator 伺服器執行個體的主機名稱或 IP 位址。

---

**備註** 這必須是 Orchestrator 執行個體 (即您要加入之叢集的目標執行個體) 的本機 IP 或主機名稱。請勿使用負載平衡器位址。

---

- 4 在**使用者名稱和密碼**文字方塊中，輸入第一個 Orchestrator 伺服器執行個體的根憑證。
- 5 按一下**加入**

Orchestrator 執行個體會複製它加入之節點本身的組態。
- 6 按一下控制中心首頁右上角的設定圖示，然後按一下**登出**。
 

您就會從控制中心登出**根**帳戶。系統會將您重新導向 vSphere Identity Manager (vIDM) 登出畫面。

---

**備註** 根帳戶無法再次存取控制中心。

---

- 7 按一下**返回登入頁面**。

系統會將您重新導向 VMware Identity Manager (vIDM) 登入畫面。

---

**備註** 叢集中個別 Orchestrator 節點的要求是由負載平衡器伺服器管理，因此您無法繼續分別存取控制中心。

---

- 8 以 `vsphere.local` 承租人中的**管理員**使用者帳戶登入控制中心。

您已成功設定 Orchestrator 執行個體叢集。

### 下一個

確認是否已在**驗證組態**頁面上正確地設定節點。

## 設定具有 vSphere 驗證的 Orchestrator 7.3 執行個體叢集

若要形成叢集，您可以設定 Orchestrator 執行個體使用 vCenter Single Sign-On 做為驗證提供者，並在該叢集中加入其他 Orchestrator 節點。

Orchestrator 叢集至少包含兩個共用同一個資料庫的 Orchestrator 伺服器執行個體。

### 先決條件

- 設定獨立式 Orchestrator 伺服器節點。請參閱“[設定具有 vSphere 驗證的獨立式 Orchestrator 伺服器](#),” 第 25 頁。
- 同步其上安裝有 Orchestrator 伺服器執行個體之虛擬機器的時鐘。
- 設定負載平衡器以在多個 vRealize Orchestrator 執行個體之間散佈流量。請參閱《[vRealize Orchestrator 負載平衡](#)》。

### 程序

- 1 存取您要新增之目標叢集的節點的控制中心，以啟動組態設定精靈。
  - a 瀏覽至 `https://your_orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter`。
  - b 使用您在 OVA 部署期間輸入的密碼，以**根使用者**身分登入。
- 2 選取**叢集化 Orchestrator** 部署類型。
 

只要選擇此類型，即表示您要將節點加入現有的 Orchestrator 叢集。
- 3 在**主機名稱**文字方塊中，輸入第一個 Orchestrator 伺服器執行個體的主機名稱或 IP 位址。

---

**備註** 這必須是 Orchestrator 執行個體 (即您要加入之叢集的目標執行個體) 的本機 IP 或主機名稱。請勿使用負載平衡器位址。

---

- 4 在**使用者名稱**和**密碼**文字方塊中，輸入第一個 Orchestrator 伺服器執行個體的根憑證。

- 5 按一下**加入**

Orchestrator 執行個體會複製它加入之節點本身的組態。

- 6 按一下控制中心首頁右上角的設定圖示，然後按一下**登出**。

您就會從控制中心登出**根**帳戶。系統會將您重新導向 vCenter Single Sign-On 登入畫面。

---

**備註** 根帳戶無法再次存取控制中心。

---



---

**備註** 叢集中個別 Orchestrator 節點的要求是由負載平衡器伺服器管理，因此您無法繼續分別存取控制中心。

---

- 7 使用驗證提供者**管理員群組**成員的帳戶登入控制中心。  
依預設，管理員帳戶為 `administrator@vsphere.local`。

您已成功設定 Orchestrator 執行個體叢集。

### 下一個

確認是否已在**驗證組態**頁面上正確地設定節點。

## 監控 Orchestrator 叢集

建立叢集之後，您可以監控叢集節點的狀態，並進一步採取動作，確保節點保持同步。

您可以從 **Orchestrator 叢集管理**頁面的 **Orchestrator 節點設定**索引標籤，查看已加入叢集的 Orchestrator 執行個體的組態同步化狀態。

**重要事項** 控制中心會回報與叢集中其他節點比較的本機節點狀態。

組態同步化狀態	本機節點	遠端節點
已同步化	上次重新啟動後，本機節點的組態並未變更。	遠端節點的組態和本機節點的組態相同。
擱置中的重新啟動	本機節點的組態已變更，或已從遠端節點複寫。Orchestrator 伺服器服務已重新啟動以套用擱置中的組態。	遠端節點的組態已經與本機節點同步化，但尚未套用。Orchestrator 伺服器服務已重新啟動以套用擱置中的組態。
需要進行組態同步化	不適用	遠端節點的作用中組態和本機節點的作用中組態不同。
節點的控制中心無法使用	不適用	遠端節點的控制中心服務 ( <code>vco-configurator</code> ) 已停止或無法連線取得。無法擷取同步化狀態。
不適用。缺少本機節點	本機節點不在叢集節點的清單中。無法擷取本機節點的同步化狀態。	不適用

## 從 Orchestrator 叢集移除節點

Orchestrator 叢集管理包含新增和移除叢集的節點。您可以從 Orchestrator 叢集移除現有節點，以新的節點取代或是減少容量。

若要從 Orchestrator 叢集永久移除節點，您必須關閉 Orchestrator Appliance 電源，然後刪除主控該裝置的虛擬機器。如需詳細資訊，請參閱《*vSphere 虛擬機器管理*》說明文件。完成之後，您必須編輯負載平衡器組態，以刪除叢集中無法再使用的 Orchestrator 節點項目。

如果控制中心顯示不再屬於叢集的節點，請存取進階 **Orchestrator 叢集管理**頁面 (網址為 [https://your\\_orchestrator\\_server\\_IP\\_or\\_DNS\\_name:8283/vco-controlcenter/#/control-app/ha?remove-nodes](https://your_orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter/#/control-app/ha?remove-nodes))，以移除殘餘記錄。

## 控制中心的角色型存取管理

透過角色型存取管理，由已設定之驗證提供者所提供的使用者或群組，在控制中心可擁有不同的角色。

將 Orchestrator 設定為搭配 vRealize Automation 或 vSphere 使用以做為驗證提供者後，您無法再以**根**使用者身分登入控制中心。如需詳細資訊，請參閱“**設定獨立式 Orchestrator 伺服器**”第 23 頁。

控制中心具有三個預先定義的角色。**管理員**角色包含**承租人管理員**角色的權限。**承租人管理員**角色包含**取用者**角色的權限。

控制中心角色	權限
管理員	具有控制中心中所有組態功能表的存取權。
承租人管理員	具有以下存取權： <ul style="list-style-type: none"> <li>■ 角色型存取管理。</li> <li>■ 檢查工作流程。如需詳細資訊，請參閱“檢查工作流程，”第 48 頁。</li> </ul>
取用者	具有檢查工作流程的存取權。

**備註** 部分驗證提供者角色會自動對應至控制中心角色。

如果驗證方式採用 vSphere，則在設定提供者期間所選取的**管理員群組**的使用者可查看控制中心的所有選項。來自 vSphere 身分識別提供者的所有其他使用者皆可登入，但無法查看控制中心的任何功能表。

如果驗證提供者是 vRealize Automation，則 vRealize Automation **系統管理員**可查看控制中心的所有組態選項。vRealize Automation **承租人管理員**會自動接收**承租人管理員**權限，而 vRealize Automation 身分識別提供者的所有其他使用者都會對應至**取用者**角色。

## 在控制中心中將使用者角色指派給使用者

若要設定身分識別提供者的使用者和群組，且該身分識別提供者是 vRealize Automation 或 vSphere 用以在控制中心享有特定權限者，則您必須將其新增至角色型存取管理，然後指派一個或多個預先定義的角色。

### 程序

- 1 以**管理員**身分登入控制中心。
- 2 在**角色型存取管理**頁面上，按一下**新增**按鈕。
- 3 在**使用者或群組**文字方塊中，輸入您要新增之使用者或群組的名稱或部分名稱。
- 4 按一下**搜尋**。  
符合搜尋條件的項目或項目清單將會顯示在清單中。
- 5 按一下您要新增的使用者或群組項目。
- 6 選取一個或多個可用角色。

**備註** 依預設，驗證提供者的**管理員群組**成員具有管理員存取權。系統不會顯示成員的權限，且您無法在控制中心的**角色型存取管理**頁面修改權限。

- 7 按一下**新增**以指派一個或多個角色給選取的使用者或群組。  
您可以查看有權限存取控制中心的使用者和群組清單，以及其角色指派。

## 設定客戶經驗改進計劃

如果您選擇參加客戶經驗改進計劃 (Customer Experience Improvement Program, CEIP)，VMware 會收到協助改善 VMware 產品和服務品質、可靠度及功能的匿名資訊。

### VMware 收到的資訊類別

客戶經驗改進計劃 (CEIP) 為 VMware 提供了可讓 VMware 改善其產品及服務並修正問題的相關資訊。當您選擇參與 CEIP 時，VMware 會在 CEIP 報告中定期收集有關您使用 VMware 產品和服務的某些類型的技術資訊。

若要瞭解 VMware 所收集的資訊類型，以及如何使用此資訊，請造訪 VMware CEIP 入口網站，網址為 <http://www.vmware.com/trustvmware/ceip.html>

## 參與客戶經驗改進計劃

透過控制中心參與客戶經驗改進計劃。

### 程序

- 1 以**管理員**身分登入控制中心，然後開啟**客戶經驗改進計劃**頁面。
- 2 選取**加入客戶經驗改進計劃**核取方塊以啟用 CEIP，或取消選取該核取方塊停用計劃，然後按一下**儲存**。
- 3 (選擇性) 如果您要手動新增 Proxy 主機，請取消選取**自動 Proxy 探索**核取方塊。

## 使用 API 服務

除了使用控制中心設定 Orchestrator 之外，您也可以使用 Orchestrator REST API、控制中心 REST API 或命令列公用程式 (儲存於應用裝置) 修改 Orchestrator 伺服器組態設定。

依預設，組態外掛程式包含在 Orchestrator 套件中。您可以從 Orchestrator 工作流程程式庫或 Orchestrator REST API 存取 [組態外掛程式] 工作流程。藉由這些工作流程，您可以變更 Orchestrator 伺服器的受信任的憑證和金鑰儲存區設定。如需所有可用 Orchestrator REST API 服務呼叫的資訊，請參閱 *Orchestrator REST API 參考說明文件*，網址為 [https://orchestrator\\_server\\_IP\\_or\\_DNS\\_name:8281/vco/api/docs](https://orchestrator_server_IP_or_DNS_name:8281/vco/api/docs)。

- [使用 REST API 管理 SSL 憑證和金鑰儲存區](#) 第 39 頁

除了使用控制中心管理 SSL 憑證外，您可以在從組態外掛程式執行工作流程時管理信任憑證和金鑰儲存區，或使用 REST API 進行管理。

- [使用控制中心 REST API 自動化 Orchestrator 組態](#) 第 42 頁

控制中心 REST API 可存取設定 Orchestrator 伺服器適用的資源。您可以使用控制中心 REST API 和第三方系統自動化 Orchestrator 組態。

## 使用 REST API 管理 SSL 憑證和金鑰儲存區

除了使用控制中心管理 SSL 憑證外，您可以在從組態外掛程式執行工作流程時管理信任憑證和金鑰儲存區，或使用 REST API 進行管理。

組態掛程式包含匯入及刪除 SSL 憑證和金鑰儲存區的工作流程。若要存取這些工作流程，您可以從 Orchestrator 用戶端的 [工作流程] 視圖導覽至 **程式庫 > 設定 > SSL 信任管理員**，以及 **程式庫 > 設定 > KeyStore**。您也可以使用 Orchestrator REST API 來執行這些工作流程。

### 使用 REST API 刪除 SSL 憑證

執行組態外掛程式的刪除信任憑證工作流程或使用 REST API，您便能刪除 SSL 憑證。

#### 程序

- 1 在刪除信任憑證工作流程的工作流程服務 URL 中，提出 GET 要求。

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name>Delete trusted certificate
```

- 2 在定義的 URL 提出 GET 要求，即可擷取刪除信任憑證工作流程的定義。

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/8a70a326-ffd7-4fef-97e0-2002ac49f5bd
```

- 3 在保有刪除信任憑證工作流程執行物件的 URL 中，提出 POST 要求。

```
POST https://{orchestrator_host}:{port}/vco/api/workflows/8a70a326-ffd7-4fef-97e0-2002ac49f5bd/executions/
```

- 4 在要求內文中，將您想要刪除的憑證名稱，作為執行內容要素中刪除信任憑證工作流程的輸入參數。

## 使用 REST API 匯入 SSL 憑證

您可以從組態外掛程式執行工作流程或使用 REST API 來匯入 SSL 憑證。

您可以從檔案或 URL 匯入信任憑證。如需使用控制中心將憑證匯入 Orchestrator 的資訊，請參閱“[管理 Orchestrator 憑證](#),” 第 30 頁。

### 程序

- 1 在工作流程服務的 URL 提出 GET 要求。

選項	說明
從檔案匯入信任憑證	從檔案匯入信任的憑證。
從 URL 匯入信任憑證	從 URL 網址匯入信任的憑證。
使用 Proxy 伺服器從 URL 匯入信任憑證	使用 Proxy 伺服器，從 URL 網址匯入信任的憑證。
使用憑證別名從 URL 匯入信任憑證	使用憑證別名，從 URL 網址匯入信任憑證。

若要從檔案匯入信任憑證，請提出以下 GET 要求：

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Import
trusted certificate from a file
```

- 2 若要擷取工作流程定義，請在定義的 URL 提出 GET 要求。

若要擷取 [從檔案匯入信任憑證] 工作流程的定義，請提出以下 GET 要求：

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/93a7bb21-0255-4750-9293-2437abe9d2e5
```

- 3 在擁有工作流程執行物件的 URL 中提出 POST 要求。

若為 [從檔案匯入信任憑證] 工作流程，請提出以下 POST 要求：

```
POST https://{orchestrator_host}:
{port}/vco/api/workflows/93a7bb21-0255-4750-9293-2437abe9d2e5/executions
```

- 4 在要求主體的執行內容元素中，提供工作流程的輸入參數值。

參數	說明
cer	您想要匯入 SSL 憑證的來源 CER 檔案。 此參數適用於 [從檔案匯入信任憑證] 工作流程。
url	您想要匯入 SSL 憑證的來源 URL。若為非 HTTPS 的服務，支援的格式為 <i>IP_address_or_DNS_name:port</i> 。 此參數適用於 [從 URL 匯入信任憑證] 工作流程。

## 使用 REST API 建立金鑰儲存區

您可以執行組態外掛程式的金鑰儲存區工作流程或使用 REST API 來建立金鑰儲存區。

### 程序

- 1 在建立金鑰儲存區工作流程的工作流程服務 URL 中提出 GET 要求。

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Create a keystore
```



- 2 在定義 URL 中提出 GET 要求，以擷取建立金鑰儲存區工作流程的定義。

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/
```

- 3 在保留建立金鑰儲存區工作流程的執行物件 URL 中提出 POST 要求。

```
POST https://{orchestrator_host}:{port}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/executions/
```

- 4 提供要建立的鑰儲存區名稱，以便在要求主體的執行內容元素中作為建立金鑰儲存區工作流程的輸入參數。

## 使用 REST API 刪除金鑰儲存區

執行刪除組態外掛程式的金鑰儲存區 工作流程或使用 REST API，您便能刪除金鑰儲存區。

### 程序

- 1 在刪除金鑰儲存區 工作流程的工作流程服務 URL 中，提出 GET 要求。

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Delete a keystore
```

- 2 在定義的 URL 提出 GET 要求，即可擷取刪除金鑰儲存區 工作流程的定義。

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/7a3389eb-1fab-4d77-860b-81b66bb45b86/
```

- 3 在保有刪除金鑰儲存區 工作流程執行物件的 URL 中，提出 POST 要求。

```
POST https://{orchestrator_host}:{port}/vco/api/workflows/7a3389eb-1fab-4d77-860b-81b66bb45b86/executions/
```

- 4 在要求內文中，將您想要刪除的金鑰儲存區 作為執行內容要素中刪除金鑰儲存區 工作流程的輸入參數。

## 使用 REST API 新增金鑰

您可以透過執行組態外掛程式中的新增金鑰工作流程或使用 REST API 來新增金鑰。

### 程序

- 1 向新增金鑰工作流程的工作流程服務的 URL 提出 GET 要求。

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Add key
```

- 2 透過向新增金鑰工作流程的定義的 URL 提出 GET 要求來擷取該定義。

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/
```

- 3 向保留新增金鑰工作流程的執行物件的 URL 提出 POST 要求。

```
POST https://{orchestrator_host}:{port}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/executions/
```

- 4 提供金鑰儲存區、金鑰別名、PEM 編碼金鑰、憑證鏈結和金鑰密碼做為要求主體內執行內容元素中新增金鑰工作流程的的輸入參數。

## 使用控制中心 REST API 自動化 Orchestrator 組態

控制中心 REST API 可存取設定 Orchestrator 伺服器適用的資源。您可以使用控制中心 REST API 和第三方系統自動化 Orchestrator 組態。

控制中心 REST API 的根端點為 [https://orchestrator\\_server\\_IP\\_or\\_DNS\\_name:8283/vco-controlcenter/api](https://orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter/api)。如需可向控制中心 REST API 撥打的所有可用服務呼叫之相關資訊，請參閱 *控制中心 REST API 參考資料說明文件*，網址為：[https://orchestrator\\_server\\_IP\\_or\\_DNS\\_name:8283/vco-controlcenter/docs](https://orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter/docs)。

## 命令行公用程式

您可以使用 Orchestrator 命令行公用程式自動化 Orchestrator 組態。

透過 SSH 以 root 身分登入 Orchestrator Appliance，以存取命令行公用程式。此公用程式位於 `/var/lib/vco/tools/configuration-cli/bin`。若要查看可用的組態選項，請執行 `./vro-configure.sh --help`。

## 其他設定選項

---

您可以使用控制中心來變更 Orchestrator 的預設行為。

本章節討論下列主題:

- “重新設定驗證,” 第 43 頁
- “匯出 Orchestrator 組態,” 第 44 頁
- “匯入 Orchestrator 組態,” 第 45 頁
- “設定工作流程執行內容,” 第 46 頁
- “Orchestrator 記錄檔案,” 第 46 頁

### 重新設定驗證

在設定控制中心的初始組態期間設定驗證方法之後，您可隨時變更驗證提供者或已設定的參數。

#### 變更驗證提供者

若要變更驗證模式或驗證提供者連線設定，您必須先解除登錄現有的驗證提供者。

##### 先決條件

##### 程序

- 1 以**管理員**身分登入控制中心。
- 2 在**設定驗證提供者**頁面上，按一下 [主機位址] 文字方塊旁的**解除登錄**按鈕，以解除登錄使用中的驗證提供者。
- 3 在**身分識別服務**區段中，按一下**解除登錄**，以刪除伺服器認證。

您已成功解除登錄驗證提供者。

##### 下一個

在控制中心中重新設定驗證。如需詳細資訊，請參閱“設定具有 [vRealize Automation 驗證的獨立式 Orchestrator 伺服器](#),” 第 23 頁或“設定具有 [vSphere 驗證的獨立式 Orchestrator 伺服器](#),” 第 25 頁。

## 變更驗證參數

若您在控制中心使用 vRealize Automation 做為驗證提供者，可能要變更 Orchestrator 管理員群組中的預設承租人。使用 vSphere 驗證時，您可以變更管理員群組。

### 先決條件

- 以**管理員**身分登入控制中心。
- 選取驗證模式並設定驗證提供者的連線設定。

### 程序

- 1 變更預設承租人。

---

**備註** 若使用 vRealize Automation 驗證模式，則您僅可變更預設承租人。

---

- a 在控制中心的**設定驗證提供者**頁面中，按一下**預設承租人**文字方塊旁的**變更**按鈕。
- b 在文字方塊中，將現有的預設承租人名稱更換為您要使用的名稱。
- c 按一下**管理員群組**文字方塊旁的**變更**按鈕。

---

**備註** 如果您不重新設定管理員群組，則群組將保留空白，且您將無法再次存取控制中心。

---

- d 輸入管理員群組的名稱，然後按一下**搜尋**。
  - e 在群組清單中，按兩下群組名稱以選取。
  - f 按一下**儲存變更**。
- 您已登出控制中心，系統會將您重新導向 Single Sign-On 登入畫面。

- 2 變更管理員群組。

- a 按一下**管理員群組**文字方塊旁的**變更**按鈕。
- b 輸入管理員群組的名稱，然後按一下**搜尋**。
- c 在群組清單中，按兩下群組名稱以選取。
- d 按一下**儲存變更**。

您已登出控制中心，系統會將您重新導向 Single Sign-On 登入畫面。

## 匯出 Orchestrator 組態

控制中心提供一個機制，可將 Orchestrator 組態設定匯出至本機檔案。您可以使用該機制隨時拍攝系統組態的快照，並將此組態匯入新的 Orchestrator 執行個體。

請定期匯出並儲存您的組態設定，特別是在進行修改、執行維護工作，或升級系統時請務必執行此動作。

---

**重要事項** 請確保包含已匯出組態的檔案安全無虞，因為當中有敏感的管理資訊。

---

### 程序

- 1 以**管理員**身分登入控制中心。
- 2 按一下**匯出/匯入組態**。

- 3 選取您要匯出的檔案類型。

---

**備註** 若您選取**匯出外掛程式組態**，且外掛程式組態包含加密的內容，就必須再選取**匯出伺服器組態**，以在匯入時成功將資料解密。

---

- 4 (選擇性) 請輸入密碼來保護組態檔。

稍後匯入組態時請使用相同的密碼。

- 5 按一下**匯出**。

Orchestrator 會建立名為 `orchestrator-config-export-hostname-dateReference.zip` 的檔案，並將其下載至您的本機電腦。您可以使用此檔案複製或還原系統。

---

**備註** 如果您選擇複製 Orchestrator 執行個體，則不可將資料庫設定匯入至複製的 Orchestrator。您必須設定不同的外部資料庫連線。

---

## 匯入 Orchestrator 組態

在重新安裝 Orchestrator 後或系統故障時，您可以還原先前匯出的系統組態。

若您透過匯入程序複製 Orchestrator 組態，vCenter Server 外掛程式組態將變成無效且無法運作，因為已產生新的 vCenter Server 外掛程式識別碼。

### 先決條件

從控制中心的**啟動選項**頁面停止 Orchestrator 伺服器。

### 程序

- 1 以**管理員**身分登入控制中心。
- 2 按一下**匯出/匯入組態**，然後瀏覽至**匯入組態**索引標籤。
- 3 瀏覽至您從上次安裝作業匯出的 `.zip` 檔案，並選取該檔案。
- 4 輸入匯出組態時使用的密碼。  
若您尚未匯出以密碼保護的組態，就不一定要進行此步驟。
- 5 按一下**匯入**。
- 6 選取要匯入之檔案的類型。

---

**重要事項** 請勿使用 **Force** 匯入外掛程式，除非您想要以已匯出檔案可能包含的舊版外掛程式來取代所有新版外掛程式。版本若不相容，可能會導致外掛程式停止運作。

---

- 7 按一下**完成匯入**。

隨即會顯示一則訊息表示組態已成功匯入。

新系統會複寫整個舊組態。Orchestrator 伺服器服務會自動重新啟動。

### 下一個

- 在**啟動選項**頁面上，確定**作用中組態指紋**與**擱置中組態指紋**兩個字串相符。

---

**備註** 您可能需要多次重新整理頁面，直到兩個字串相符為止。

---

- 請在控制中心的**驗證組態**頁面確認 Orchestrator 設定正確。

## 設定工作流程執行內容

依預設，如果已經達到有效執行中的工作流程數量，您可以在每個節點執行最多 300 個工作流程，也可以將最多 10,000 個工作流程排入佇列。

如果 Orchestrator 節點必須同時執行超過 300 個工作流程，擱置的工作流程執行便會排入佇列。當作用中的工作流程執行完成時，佇列中的下一個工作流程便會開始執行。如果佇列中的工作流程數量達到上限，後續的工作流程執行將會失敗，直到有擱置中的工作流程開始執行。

在控制中心的**進階選項**頁面上，您可以設定工作流程執行內容。

選項	說明
啟用安全模式	如果已啟用安全模式，則所有正在執行的工作流程都會被取消，並且不會在下一個 Orchestrator 節點啟動時繼續執行。
同時執行的工作流程數量	同時執行的同時 Orchestrator 節點工作流程數量上限。
佇列中正在執行的工作流程數量上限	成為無法使用之前，Orchestrator 節點接受的工作流程執行要求數量。
每一個工作流程保留的執行數量上限	對於叢集中的每個工作流程可保留成為記錄的完成工作流程執行數上限。如果超過，會刪除最舊的工作流程執行。
記錄事件到期天數	叢集的記錄事件在清除前於資料庫中保留的天數。

## Orchestrator 記錄檔案

在您提交支援要求之後，VMware 技術支援會定期要求診斷資訊。該診斷資訊包含從執行產品的主機取得之產品特定的記錄和組態檔案。

您可以從控制中心的**匯出記錄**功能表下載包含 Orchestrator 組態檔和記錄檔案的 zip 服務包。

**表格 7-1.** Orchestrator 記錄檔案清單

檔案名稱	位置	說明
scripting.log	/var/log/vco/app-server	提供工作流程和動作的指令碼記錄訊息。使用 <b>scripting.log</b> 檔案將工作流程執行和動作執行與正常的 Orchestrator 作業隔離。此資訊也包含在 <b>server.log</b> 檔案中。
server.log	/var/log/vco/app-server	提供有關 Orchestrator 伺服器上所有活動的資訊。為 Orchestrator 或任何在 Orchestrator 上執行的應用程式偵錯時，請分析 <b>server.log</b> 檔案。
metrics.log	/var/log/vco/app-server	提供有關伺服器的執行階段資訊。每 5 分鐘會將該資訊新增到此記錄檔案中。
localhost_access_log.txt	/var/log/vco/app-server	這是伺服器的 HTTP 要求記錄。
localhost_access_log.date.txt	/var/log/vco/configuration	這是控制中心服務的 HTTP 要求記錄。
controlcenter.log	/var/log/vco/configuration	控制中心服務的記錄檔案。

## 持續型記錄

您可以記錄各種 Orchestrator 命令碼的資訊，例如工作流程、原則或動作。這些資訊可分為不同的類型和層級。類型可以是持續型和非持續型。層級可以是偵錯、資訊、警告、錯誤、追蹤和嚴重。

**表格 7-2. 建立持續型和非持續型記錄**

記錄層級	持續型	非持續型
偵錯	Server.debug("簡短文字", "長文字");	System.debug("文字");
資訊	Server.log("簡短文字", "長文字");	System.log("文字");
警告	Server.warn("簡短文字", "長文字");	System.warn("文字");
錯誤	Server.error("簡短文字", "長文字");	System.error("文字");

### 持續型記錄

持續型記錄 (伺服器記錄) 會追蹤過去的工作流程執行記錄，並儲存在 Orchestrator 資料庫中。若要檢視伺服器記錄，您必須選取工作流程、已完成的工作流程執行或原則，然後按一下 Orchestrator 用戶端的**事件**索引標記。

### 非持續型記錄

若您使用非持續型記錄 (系統記錄) 來建立命令碼，Orchestrator 伺服器會針對此記錄通知所有執行中的 Orchestrator 應用程式，但此資訊不會儲存在資料庫中。若是重新啟動應用程式，記錄資訊便不復存在。非持續型記錄可用於偵錯及取得最即時的資訊。若要檢視系統記錄，您必須在 Orchestrator 用戶端選取已完成的工作流程執行，然後按一下**架構**索引標記上的**記錄**。

## Orchestrator 記錄組態

在控制中心的**設定記錄**頁面上，您可以設定伺服器記錄的層級，以及您需要的指令碼記錄。如果一天之內多次產生任一份記錄，則難以判斷造成問題的原因。

伺服器記錄和指令碼記錄的記錄層級是資訊。變更記錄層級會影響伺服器在記錄中輸入的所有新訊息，以及資料庫的作用中連線數。記錄詳細資訊依遞減順序減少。



**警告** 僅將記錄層級設定為偵錯或全部進行問題的偵錯。請勿在生產環境中使用這些設定，因為這會嚴重影響效能。

### 記錄輪換設定

若要避免伺服器記錄變得過大，您可以修改**檔案計數上限**和**檔案大小上限 (MB)** 文字方塊中的值，設定伺服器記錄的檔案大小上限和計數上限。

### Orchestrator 記錄檔案匯出

在控制中心的**匯出記錄**頁面上，您可以產生含有組態、伺服器、包裝函式及安裝記錄檔的疑難排解資訊 ZIP 封存檔。

記錄資訊會儲存在名為 `vco-logs-date_hour.zip` 的 ZIP 封存檔。

**備註** 如果叢集中具有多個 Orchestrator 執行個體，則 ZIP 封存檔會納入叢集中所有 Orchestrator 執行個體的記錄。

## 檢查工作流程

您可以存取控制中心的 [檢查工作流程] 頁面，快速檢查並匯出已完成的工作流程的系統記錄和伺服器記錄。

---

**重要事項** 記錄資訊僅為暫時儲存。

- 系統記錄會儲存在大小上限為 10 MB 的檔案中。每節點的記錄檔數目上限為 5 個。
  - 伺服器記錄會儲存在資料庫中保留 15 天。
- 

### 程序

- 1 以**管理員**身分登入控制中心。
- 2 按一下**檢查工作流程**。
- 3 按一下**已完成的工作流程**索引標籤。
- 4 (選擇性) 選取您要檢查的工作流程 **Token** 類型，然後選取日期範圍並按一下**套用**。
- 5 (選擇性) 依名稱、識別碼或 **Token** 識別碼搜尋工作流程。
- 6 按一下您要檢查的 **Token** 識別碼。  
 工作流程執行記錄視圖會以全螢幕顯示。
- 7 檢查系統記錄和伺服器記錄。

---

**備註** 叢集中具有多個 **Orchestrator** 執行個體時，控制中心只會在 **Orchestrator** 節點 (即啟動此工作流程的來源節點) 上顯示工作流程 **Token** 記錄。

---

- 8 (選擇性) 按一下**匯出 Token 記錄**，將工作流程 **Token** 記錄以 **.zip** 檔匯出。

## 篩選 Orchestrator 記錄

您可以篩選特定工作流程執行作業的 **Orchestrator** 伺服器記錄，並收集有關工作流程執行作業的診斷資料。

**Orchestrator** 記錄包含許多您可即時監控的實用資訊。相同的工作流程中有多個執行個體同時執行時，您可以在 **Orchestrator** 即時記錄資料流中篩選每次執行的相關診斷資料，進而追蹤不同的工作流程執行作業。

---

**備註** 叢集中具有多個 **Orchestrator** 執行個體時，即時記錄資料流會僅顯示本機 **Orchestrator** 節點的記錄。

---

### 程序

- 1 以**管理員**身分登入控制中心。
- 2 按一下**即時記錄資料流**。
- 3 在搜尋列中，輸入您的搜尋參數。  
 例如，您可以依使用者名稱、工作流程名稱、工作流程識別碼或 **Token** 識別碼篩選記錄。
- 4 (選擇性) 選取**區分大小寫**和**篩選 (grep)**，進一步篩選搜尋結果。  
 若選取**篩選 (grep)**，即時資料流會僅顯示符合搜尋參數的資料行。

**Orchestrator** 即時記錄資料流將根據您的搜尋參數進行篩選。

### 下一個

如果您想要篩選無法透過控制中心**即時記錄資料流**存取的舊記錄，可以使用第三方記錄分析工具。



## 組態使用案例和疑難排解

您可以設定 Orchestrator 伺服器搭配使用 vCenter Server 應用裝置，也可從 Orchestrator 取消安裝外掛程式，或是變更自我簽署憑證。

組態使用案例提供了為符合 Orchestrator 伺服器特定組態需求所執行的工作流程，以及疑難排解主題供您瞭解問題並加以解決 (若有相關因應措施)。

本章節討論下列主題：

- “將 Orchestrator 登錄為 vCenter Server 延伸模組,” 第 49 頁
- “解除登錄 Orchestrator 驗證,” 第 50 頁
- “變更 SSL 憑證,” 第 50 頁
- “取消正在執行的工作流程,” 第 51 頁
- “啟用 Orchestrator 伺服器偵錯,” 第 52 頁
- “備份 Orchestrator 組態和元素,” 第 52 頁
- “備份與還原 vRealize Orchestrator,” 第 54 頁
- “使用 Site Recovery Manager 進行 Orchestrator 的災難復原,” 第 56 頁

### 將 Orchestrator 登錄為 vCenter Server 延伸模組

在透過 vCenter Single Sign-On 來登錄 Orchestrator 伺服器並將之設定來和 vCenter Server 並用時，必須將 Orchestrator 登錄為 vCenter Server 的延伸模組。

#### 程序

- 1 以管理員身分登入 Orchestrator 用戶端。
- 2 按一下**工作流程**視圖。
- 3 在工作流程階層清單裡展開**資料庫 > vCenter > 組態**。
- 4 在**將 vCenter Orchestrator 登錄為 vCenter Server 延伸模組**工作流程上按一下滑鼠右鍵並選取**開始工作流程**。
- 5 選取 vCenter Server 執行個體來登錄 Orchestrator。
- 6 輸入 `https://your_orchestrator_server_IP_or_DNS_name:8281` 或負載平衡器 (將要求重新導向至 Orchestrator 伺服器節點) 的服務 URL。
- 7 按一下**提交**。

## 解除登錄 Orchestrator 驗證

在控制中心的設定驗證提供者頁面中，解除登錄使用 Single Sign-On 解決方案的 Orchestrator。

如果要重新設定 Orchestrator vCenter Single Sign-On 或 vRealize Automation 驗證，您必須先解除登錄 Orchestrator 驗證。

### 程序

- 1 以**管理員**身分登入控制中心。
- 2 按一下**設定驗證提供者**。
- 3 按一下**解除登錄**。
- 4 (選擇性) 如果要從身分識別伺服器刪除登錄資料，請輸入您的認證。
- 5 按一下**身分識別伺服器**區段中的**解除登錄**。

您已成功將 Orchestrator 伺服器執行個體解除登錄。

## 變更 SSL 憑證

依預設，Orchestrator 伺服器使用自我簽署 SSL 憑證來和 Orchestrator 用戶端進行遠端通訊。舉例來說，如果您公司的安全性原則需要使用 SSL 憑證，則您可以變更 SSL 憑證。

當您嘗試透過信任的 SSL 網際網路連線來使用 Orchestrator，並且在網頁瀏覽器開啟控制中心時，如果您使用的是 Mozilla Firefox，則會收到連線不被信任的警告；或者如果您使用 Internet Explorer，則會收到偵測到網站安全性憑證出現問題的警告。

在按下**繼續瀏覽此網站 (不建議)**之後，即使您已經把 SSL 憑證匯入信任的存放區，您還是會在網頁瀏覽器的網址列看到紅色的憑證錯誤通知。您可以在網頁瀏覽器中使用 Orchestrator，但嘗試透過 HTTPS 存取 API 時，第三方系統可能無法正常作業。

在您啟動 Orchestrator 用戶端並嘗試透過 SSL 連線和 Orchestrator 伺服器連線時，可能也會收到憑證警告。

您可以透過安裝由商業憑證授權機構 (CA) 簽署的憑證來解決此問題。若需停止從 Orchestrator 用戶端收到憑證警告，請將您的根 CA 憑證新增到安裝 Orchestrator 用戶端的機器上的 Orchestrator 金鑰儲存區。

## 新增憑證到本機存放區

收到來自 CA 的憑證之後，您必須把憑證新增到本機存放區，如此才能在不收到憑證警告或錯誤訊息的情況下存取控制中心。

此工作流程描述透過 Internet Explorer 把憑證新增到本機存放區的過程。

- 1 開啟 Internet Explorer 並前往 `https://orchestrator_server_IP_or_DNS_name:8283/`。
- 2 看到提示後，按一下**繼續瀏覽此網站 (不建議)**。  
憑證錯誤訊息會出現在 Internet Explorer 網址列的右邊。
- 3 按一下憑證錯誤訊息並選取**檢視憑證**。
- 4 按一下**安裝憑證**。
- 5 在憑證匯入精靈的歡迎畫面上按一下**下一步**。
- 6 在憑證存放區視窗中，選取**將所有憑證放置於以下存放區**。
- 7 流覽並選取**信任的根憑證授權機構**。

8 完成精靈的操作並重新啟動 Internet Explorer。

9 透過您的 SSL 連線前往 Orchestrator 伺服器。

您將不再收到警告，也不會在網址列看到憑證錯誤。

VMware 服務管理員等其他應用程式及系統必須具備透過 SSL 連線存取 Orchestrator REST API 的能力。

## 變更 Orchestrator 硬體裝置管理網站的憑證

Orchestrator Appliance 使用 Light HTTPd 來執行自己的管理網站。舉例來說，如果您公司的安全性原則需要使用其 SSL 憑證，則您可以變更 Orchestrator Appliance 管理網站的 SSL 憑證。

### 先決條件

依預設，Orchestrator Appliance SSL 憑證和私密金鑰儲存於 PEM 檔案，該檔案位於：`/opt/vmware/etc/lighttpd/server.pem`。要安裝新憑證時，請務必從 Java 金鑰儲存區匯出新的 SSL 憑證和私密金鑰到 PEM 檔案。

### 程序

1 以根使用者身分登入 Orchestrator Appliance 的 Linux 主控台。

2 找到 `/opt/vmware/etc/lighttpd/lighttpd.conf` 檔案並以編輯器開啟。

3 找到以下這一系列：

```
#### SSL engine
ssl.engine = "enable"
ssl.pemfile = "/opt/vmware/etc/lighttpd/server.pem"
```

4 將 `ssl.pemfile` 屬性變更，使其指向含有您新的 SSL 憑證和私密金鑰之 PEM 檔案。

5 儲存 `lighttpd.conf` 檔案。

6 執行以下的命令來重新啟動 `light-httpd` 伺服器。

```
service vami-lighttp restart
```

您已成功變更 Orchestrator Appliance 管理網站的憑證。

## 取消正在執行的工作流程

請在 Orchestrator 伺服器已停止時取消工作流程，否則作業可能不會成功。

### 先決條件

從控制中心裡的**啟動選項**頁面停止 Orchestrator 伺服器。

### 程序

1 以**管理員**身分登入控制中心。

2 按一下**疑難排解**。

- 取消正在執行的工作流程。

選項	描述
<b>取消所有工作流程執行</b>	輸入工作流程 識別碼 來取消該工作流程的所有 Token。如果伺服器未停止，則工作流程 Token 可能不會取消。
<b>依 識別碼 取消工作流程執行</b>	輸入所有要取消的 Token 識別碼。使用逗號來分隔。如果伺服器未停止，則工作流程 Token 可能不會取消。
<b>取消所有 Token</b>	取消伺服器上所有正在執行的工作流程。您必須停止伺服器才能使用這個選項。

在下次伺服器啟動時，工作流程會設為取消的狀態。

### 下一個

請確認工作流程是從控制中心的[檢查工作流程](#)頁面中取消。

## 啟用 Orchestrator 伺服器偵錯

您可以使用偵錯模式啟動 Orchestrator 伺服器，以便在開發外掛程式時進行問題偵錯。

### 程序

- 以**管理員**身分登入控制中心。
- 按一下 **Orchestrator 偵錯**。
- 按一下**啟用偵錯**。
- (選擇性) 輸入預設連接埠以外的連接埠。
- (選擇性) 按一下**暫停**。

若選取此選項，必須連結偵錯工具才能啟動 Orchestrator 伺服器。

- 按一下**儲存**。
- 在控制中心開啟啟動選項頁面，然後按一下**重新啟動**。

Orchestrator 伺服器會在啟動時暫停，直到您連結遠端 Java 偵錯工具至定義的連接埠。

## 備份 Orchestrator 組態和元素

您可以擷取 Orchestrator 組態快照，然後將此組態匯入新的 Orchestrator 執行個體，以備份 Orchestrator 組態。也可備份您修改的 Orchestrator 元素。

如果您先編輯任何標準工作流程、動作、原則或組態元素，再匯入含有相同元素但 Orchestrator 版本號碼較高的套件，則您對該元素所做的變更將會遺失。若要在升級之後使用修改過和自訂的元素，您必須先將其由套件中匯出，然後再開始程序。

每個 Orchestrator 伺服器執行個體都具有唯一憑證，且每個 vCenter Server 外掛程式執行個體都具有唯一識別碼。此憑證和唯一識別碼可用於定義 Orchestrator 伺服器和 vCenter Server 外掛程式的身分識別。如果您不備份 Orchestrator 元素或匯出 Orchestrator 組態做為備份，請務必變更這些識別碼。

### 先決條件

部署並設定新的 Orchestrator 伺服器執行個體。請參閱 [<設定獨立式 Orchestrator 伺服器>](#)。

### 程序

- 以**管理員**身分登入控制中心。

- 2 按一下**匯出/匯入組態**。
- 3 選取您要匯出的檔案類型。
- 4 (選擇性) 請輸入密碼來保護組態檔。  
請在匯入組態時使用相同的密碼。
- 5 按一下**匯出**。
- 6 登入 Orchestrator 用戶端應用程式。
- 7 建立一個套件，其中包含您已建立或編輯的所有 Orchestrator 元素。
  - a 按一下**套件**視圖。
  - b 按一下 [套件] 清單標題列中的功能表按鈕，然後選取**新增套件**。
  - c 輸入新套件的名稱，然後按一下**確定**。  
套件名稱的語法為 *domain.your\_company.folder.package\_name*。  
例如 *com.vmware.myfolder.mypackage*。
  - d 在套件上按一下滑鼠右鍵並選取**編輯**。
  - e 在**一般**索引標籤上新增套件的說明。
  - f 在**工作流程**索引標籤上新增工作流程到套件。
  - g (選擇性) 將原則範本、動作、組態元素、資源元素和外掛程式新增至套件中。
- 8 匯出套件。
  - a 在要匯出的套件上按一下滑鼠右鍵，並選取**匯出套件**。
  - b 瀏覽並選取您希望的套件儲存位置，然後按一下**開啟**。
  - c (選擇性) 使用對應憑證來簽署套件。
  - d (選擇性) 對已匯出的套件施加限制。
  - e (選擇性) 若要對已匯出套件的內容套用限制，請視需要取消選取選項。

選項	說明
<b>匯出版本歷程記錄。</b>	套件的版本歷程記錄不會匯出。
<b>匯出組態設定值</b>	套件中組態元素的屬性值不會匯出。
<b>匯出全域標記</b>	套件中的全域標記不會匯出。

  - f 按一下**儲存**。
- 9 將 Orchestrator 組態匯入到新的 Orchestrator 伺服器執行個體。
  - a 以**管理員**身分登入新 Orchestrator 執行個體的控制中心。
  - b 按一下**匯出/匯入組態**，然後瀏覽至**匯入組態**索引標籤。
  - c 瀏覽以選取從先前安裝中匯出的 .zip 檔案。
  - d 輸入在匯出組態時使用的密碼。  
如果您還未指定密碼，則不必進行步驟。
  - e 按一下**匯入**。

- 10 匯入您要匯出至新 Orchestrator 執行個體的套件。
  - a 登入新 Orchestrator 執行個體的 Orchestrator 用戶端應用程式。
  - b 從 Orchestrator 用戶端的下拉式功能表中選取**管理**。
  - c 按一下**套件**視圖。
  - d 在左邊窗格中按一下滑鼠右鍵，然後選取**匯入套件**。
  - e 瀏覽並選取您要匯入的套件，然後按一下**開啟**。  
隨即會出現匯出工具的憑證資訊。
  - f 檢閱套件匯入詳細資料，並選取**匯入**或**匯入並信任提供者**。  
[匯入套件] 視圖隨即顯示。若匯入的套件元素版本比伺服器的版本新，則系統會選取該元素來匯入。
  - g 取消選取您不想匯入的元素。  
例如，取消選取存有較新版本的自訂元素。
  - h (選擇性) 若您不想從套件匯入組態元素的屬性值，請取消選取**匯入組態設定值**核取方塊。
  - i 從下拉功能表中選擇您是否要從套件匯入標記。

選項	說明
匯入標記但保留現有的值	從套件匯入標記，但不覆寫現有的標記值。
匯入標記並覆寫現有的值	從套件匯入標記，並覆寫其值。
不要匯入標記	不從套件匯入標記。

- j 按一下**匯入**選取的元素。

## 備份與還原 vRealize Orchestrator

您可以使用 vSphere Data Protection 來備份與還原含有一個 vRealize Orchestrator 執行個體的虛擬機器 (VM)。

vSphere Data Protection 是 VMware 的一款以磁碟為基礎的備份與還原解決方案，專為 vSphere 環境設計。vSphere Data Protection 與 vCenter Server 完全整合。有了 vSphere Data Protection，您可以管理備份作業並將備份儲存於重複的目的地儲存位置。完成 vSphere Data Protection 的布署和設定後，您可以用 vSphere Web Client 介面來存取 vSphere Data Protection，進行虛擬機器備份與還原的選取、排定、設定和管理。備份過程中，vSphere Data Protection 會建立虛擬機器的靜止快照。每次的備份作業將自動執行重複資料刪除。

如需布署與設定 vSphere Data Protection 的相關資訊，請參閱 *vSphere Data Protection Administration* 的說明文件。

### 備份 vRealize Orchestrator

您可以備份您的 vRealize Orchestrator 執行個體作為虛擬機器。

您可以在完整虛擬機器備份前匯出您的資料庫。如需如何匯出您資料庫的詳細資訊，請參閱“[匯出 Orchestrator 資料庫](#)”第 29 頁。如果 vRealize Orchestrator 和外部資料庫在不同的機器上，則您必須個別備份資料庫。

**備註** 若要確定單一產品中的所有虛擬機器元件均一併備份，請將 vRealize Orchestrator 環境的虛擬機器儲存於單一 vCenter Server 資料夾中，並建立該資料夾的備份原則工作。

### 先決條件

- 確認 vSphere Data Protection 應用裝置已部署及設定。如需部署與設定 vSphere Data Protection 的相關資訊，請參閱 *vSphere Data Protection Administration* 的說明文件。
- 使用 vSphere Web Client 登入用於管理環境的 vCenter Server 執行個體。以具備管理員權限且在 vSphere Data Protection 組態期間使用的使用者身分登入。

### 程序

- 1 在 vSphere Web Client 首頁上，按一下 **vSphere Data Protection**。
- 2 從 **VDP 應用裝置** 下拉式功能表中選取您的 vSphere Data Protection 應用裝置，並按一下 **連線**。
- 3 在 **開始使用** 索引標籤上，按一下 **建立備份工作**。
- 4 按一下 **客體映像** 備份您的 vRealize Orchestrator 執行個體，並且按 **下一步**。
- 5 選取 **完整映像** 備份整個虛擬機器，並且按 **下一步**。
- 6 展開 **虛擬機器** 樹狀結構，並選取您 vRealize Orchestrator 虛擬機器的核取方塊。
- 7 按照提示設定備份排程、保留原則，以及備份工作的名稱。

如需如何備份和還原虛擬機器的詳細資訊，請參閱 *vSphere Data Protection Administration* 說明文件。

您的備份工作將出現在 **備份** 索引標籤上的備份工作清單中。

- 8 (選擇性) 開啟 **備份** 索引標籤，並選取您的備份工作，然後按一下 **立即備份** 備份您的 vRealize Orchestrator。

---

**備註** 或者，您也可以等候備份按照您設定的排程自動開始。

---

備份程序將出現在 **最近的工作** 頁面上。

您虛擬機器的映像將出現在 **還原** 索引標籤上的備份清單中。

### 下一個

開啟 **還原** 索引標籤，並確認您虛擬機器的映像出現在備份清單中。

## 還原 vRealize Orchestrator 執行個體

您可以在原始位置或同一個 vCenter Server 上的不同位置還原 vRealize Orchestrator 執行個體。

如果您的 vRealize Orchestrator 和外部資料庫在不同機器上執行，您必須先還原資料庫，然後還原 vRealize Orchestrator 虛擬機器。

### 先決條件

- 確認 vSphere Data Protection 應用裝置已部署及設定。如需部署與設定 vSphere Data Protection 的相關資訊，請參閱 *vSphere Data Protection Administration* 的說明文件。
- 備份您的 vRealize Orchestrator 執行個體。請參閱“[備份 vRealize Orchestrator](#),” 第 54 頁。
- 使用 vSphere Web Client 登入用於管理環境的 vCenter Server 執行個體。以具備管理員權限且在 vSphere Data Protection 組態期間使用的使用者身分登入。

### 程序

- 1 在 vSphere Web Client 首頁上，按一下 **vSphere Data Protection**。
- 2 從 **VDP 應用裝置** 下拉式功能表中選取您的 vSphere Data Protection 應用裝置，並按一下 **連線**。
- 3 開啟 **還原** 索引標籤。

- 4 從備份工作的清單中，選取要還原的 vRealize Orchestrator 備份。

---

**備註** 如果您有多個虛擬機器，必須同時還原這些虛擬機器，這些虛擬機器才會同步。

---

- 5 若要還原同一個 vCenter Server 上的 vRealize Orchestrator 執行個體，請按一下**還原**圖示，並按照提示來設定 vCenter Server 上將還原 vRealize Orchestrator 的位置。

請勿選取**開啟電源**，因為應用裝置必須是最後一個開啟電源的元件。如需如何備份和還原虛擬機器的相關資訊，請參閱 *vSphere Data Protection Administration* 說明文件。

表示成功啟始還原的訊息隨即顯示。

- 6 (選擇性) 如果資料庫主機在外部，而且將還原您的負載平衡器組態，請開啟資料庫主機的電源。
- 7 開啟 vRealize Orchestrator 應用裝置的電源。

還原的 vRealize Orchestrator 虛擬機器將出現在 vCenter Server 詳細目錄中。

### 下一個

開啟控制中心的**驗證組態**頁面，確認已正確設定 vRealize Orchestrator。

## 使用 Site Recovery Manager 進行 Orchestrator 的災難復原

您必須設定 Site Recovery Manager 以便保護您的 vRealize Orchestrator。請完成 Site Recovery Manager 的一般組態工作，以便落實這項保護。

### 準備環境

開始設定 Site Recovery Manager 之前，您必須確定自己符合下列必要條件。

- 確認受保護的站台和復原站台均已安裝 vSphere 5.5。
- 確認您正在使用 Site Recovery Manager 5.8。
- 確認已設定 vRealize Orchestrator。

### 為 vSphere Replication 設定虛擬機器

您必須為 vSphere Replication 或陣列式複寫設定虛擬機器，才能使用 Site Recovery Manager。

若要在所需的虛擬機器上啟用 vSphere Replication，請執行下列步驟。

#### 程序

- 1 在 vSphere Web Client 中，選取應該啟用 vSphere Replication 的虛擬機器，並按一下**動作 > 全部 vSphere Replication 動作 > 設定複寫**。
- 2 在複寫類型視窗中，選取**複寫至 vCenter Server**，然後按下一步。
- 3 在目標站台視窗中，選取復原站台的 vCenter，然後按下一步。
- 4 在複寫伺服器視窗中，選取 vSphere Replication 伺服器，然後按下一步。
- 5 在目標位置視窗中，按一下**編輯**，並選取目標資料存放區，此資料存放區將用來儲存複寫的檔案，然後按下一步。
- 6 在複寫選項視窗中，維持預設設定，然後按下一步。
- 7 在復原設定視窗中，輸入**復原點目標 (RPO)** 和**時間點執行個體**，然後按下一步。
- 8 在即將完成視窗中，確認設定並按一下**完成**。
- 9 為所有必須啟用 vSphere Replication 的虛擬機器重複上述步驟。



## 建立保護群組

您可以建立保護群組，讓 Site Recovery Manager 能夠保護虛擬機器。

建立保護群組時請您耐心等待，以確保作業順利完成。確定 Site Recovery Manager 已建立保護群組，且可順利保護群組中的虛擬機器。

### 先決條件

確認您已執行下列其中一項工作：

- 已加入資料存放區的虛擬機器，且您已在虛擬機器上設定陣列式複寫
- 已在虛擬機器上設定 vSphere Replication
- 已執行前述部分或全部的工作

### 程序

- 1 在 vSphere Web Client 中，選取**站台復原 > 保護群組**。
- 2 在**物件**索引標籤上，按一下建立保護群組的圖示。
- 3 在保護群組類型頁面上，先選取受保護的站台再選取複寫類型，然後按**下一步**。

選項	動作
陣列式複寫群組	選取 <b>陣列式複寫 (ABR)</b> ，並選取陣列配對。
vSphere Replication 保護群組	選取 vSphere Replication。

- 4 選取要新增至保護群組的資料存放區群組或虛擬機器。

選項	動作
陣列式複寫保護群組	選取資料存放區群組，然後按 <b>下一步</b> 。
vSphere Replication 保護群組	選取清單中的虛擬機器，然後按 <b>下一步</b> 。

在您建立 vSphere Replication 保護群組時，只有已為 vSphere Replication 完成設定且不在保護群組中的虛擬機器，才會出現在清單中。

- 5 檢閱設定，然後按一下**完成**。  
在**保護群組**下的**物件**索引標籤上，您可以監控保護群組的建立進度。
  - 若 Site Recovery Manager 已順利將詳細目錄對應套用至受保護的虛擬機器，保護群組的保護狀態會變成「正常」。
  - 若 Site Recovery Manager 已順利為與儲存區原則相關的所有虛擬機器提供保護，保護群組的保護狀態會變成「正常」。

## 建立復原計劃

您可以建立復原計劃，設定 Site Recovery Manager 如何復原虛擬機器。

### 程序

- 1 在 vSphere Web Client 中，選取**站台復原 > 復原計劃**。
- 2 在**物件**索引標籤上，按一下建立復原計劃的圖示。
- 3 輸入計劃的名稱和說明，並選取資料夾，然後按**下一步**。
- 4 選取復原站台，然後按**下一步**。

- 5 從功能表中選取群組類型。

選項	說明
<b>虛擬機器保護群組</b>	選取此選項將建立包含陣列式複寫與 vSphere Replication 保護群組的復原計劃。
<b>儲存區原則保護群組</b>	選取此選項將建立包含儲存區原則保護群組的復原計劃。

預設為**虛擬機器保護群組**。

**備註** 如果使用延伸的儲存區，請選取群組類型的**儲存區原則保護群組**。

- 6 為欲復原的計劃選取一或多個保護群組，然後按**下一步**。
- 7 按一下**測試網路**值，並選取欲在測試復原期間使用的網路，然後按**下一步**。  
預設選項是自動建立隔離的網路。
- 8 檢閱摘要資訊，並按一下**完成**建立復原計劃。

## 在資料夾中組織復原計劃

您可以建立用來組織復原計劃的資料夾。

如果您有許多復原計劃，將復原計劃組織到資料夾中將十分有用。您可以將復原計劃放到資料夾中，再向不同的使用者或群組指派資料夾的不同權限，藉以限制對復原計劃的存取。

### 程序

- 1 在 vSphere Web Client 的 [首頁] 視圖中，按一下**網站復原**。
- 2 展開**詳細目錄樹狀結構**，並按一下**復原計劃**。
- 3 選取**相關物件**標記，並按一下**資料夾**。
- 4 按一下**建立資料夾**圖示，輸入要建立的資料夾之名稱，再按下**確定**。
- 5 將新的或現有的復原計劃新增到該資料夾中。

選項	描述
<b>建立新的復原計劃</b>	在資料夾上按滑鼠右鍵，並選取 <b>建立復原計劃</b> 。
<b>新增既有的復原計劃</b>	將復原計劃從詳細目錄樹狀結構拖放至資料夾中。

- 6 (選擇性) 若要重新命名或刪除資料夾，請在資料夾上按滑鼠右鍵，並選取**重新命名資料夾**或**刪除資料夾**。  
您只能刪除空白的資料夾。

## 編輯復原計劃

您可以編輯復原計劃，變更建立該計劃時指定的內容。您可以從受保護的站台或從復原站台編輯復原計劃。

### 程序

- 1 在 vSphere Web Client 中，選取**站台復原 > 復原計劃**。
- 2 在復原計劃上按一下滑鼠右鍵，並選取**編輯計劃**。  
您也可以按一下**監控索引標籤**的**復原步驟**視圖中出現的**編輯復原計劃**圖示，編輯復原計劃。
- 3 (選擇性) 在**復原計劃名稱**文字方塊中變更計劃的名稱或說明，然後按**下一步**。
- 4 在 [復原站台] 頁面上，按**下一步**。  
您無法變更復原站台。

- 5 (選擇性) 選取或取消選取一個或多個保護群組，在計劃中新增或移除保護群組，然後按**下一步**。
- 6 (選擇性) 按一下測試網路，選取與復原站台所在的網路不同的測試網路，然後按**下一步**。
- 7 檢閱摘要資訊，並且按一下**完成**，對於復原計劃進行指定的變更。

您即可在 [最近的工作] 視圖中監控計劃的更新。



## 設定系統內容

您可以設定系統內容，以變更預設的 Orchestrator 行為。

本章節討論下列主題：

- “透過非管理員停用 Orchestrator 用戶端的存取權,” 第 61 頁
- “為工作流程和動作設定伺服器檔案系統存取,” 第 62 頁
- “為工作流程和動作設定作業系統命令的存取,” 第 63 頁
- “設定 Java 類別的 JavaScript 存取,” 第 63 頁
- “設定自訂逾時內容,” 第 64 頁

### 透過非管理員停用 Orchestrator 用戶端的存取權

您可以設定 Orchestrator 伺服器，以拒絕非 Orchestrator 管理員群組會員之所有使用者的 Orchestrator 用戶端存取權。


依預設，所有授予執行權限的使用者可以連線至 Orchestrator 用戶端。但您可以限制 Orchestrator 管理員的 Orchestrator 用戶端存取權，只要設定 Orchestrator 組態系統內容即可。

---

**重要事項** 如果未設定內容或內容設定錯誤，則 Orchestrator 允許所有使用者存取 Orchestrator 用戶端。

---

#### 程序

- 1 以**管理員**身分登入控制中心。
- 2 按一下**系統內容**。
- 3 按一下**新增**圖示 ()。
- 4 在**金鑰**文字方塊中輸入 `com.vmware.o11n.smart-client-disabled`。
- 5 在**值**文字方塊中輸入 `true`。
- 6 (選擇性) 在**說明**文字方塊中輸入**停用 Orchestrator 用戶端連線**。
- 7 按一下**新增**。
- 8 從快顯功能表按一下**儲存變更**。  
出現表示您已成功儲存的訊息。
- 9 重新啟動 Orchestrator 伺服器。

除了 Orchestrator 管理員群組的會員之外，您停用了所有使用者的 Orchestrator 用戶端存取權。

## 為工作流程和動作設定伺服器檔案系統存取

在 Orchestrator 中，工作流程和動作擁有特定檔案系統目錄的有限存取權。您可以透過修改 `js-io-rights.conf` Orchestrator 組態檔案，將存取延伸至伺服器檔案系統中的其他部分。

### js-io-rights.conf 檔案中的規則允許對 Orchestrator 系統的寫入權限

`js-io-rights.conf` 檔案包含的規則，允許對伺服器檔案系統指定的目錄之寫入權限。

#### js-io-rights.conf 檔案的必要內容

`js-io-rights.conf` 中的每一行必須包含下列資訊。

- 加號 (+) 或減號 (-) 以說明權限受到允許或拒絕
- 權限的讀取 (r)、寫入 (w) 和執行 (x) 層級。
- 套用權限的路徑

#### js-io-rights.conf 檔案的預設內容

Orchestrator Appliance 中 `s-io-rights.conf` 的預設內容如下：

```
-rwx /
+rwX /var/run/vco
-rwx /etc/vco/app-server/security/
+rX /etc/vco
+rX /var/log/vco/
```

預設 `js-io-rights.conf` 組態檔案的前兩行允許下列權限：

```
-rwx /                拒絕所有對檔案系統的存取。
+rwX /var/run/vco    允許對 /var/run/vco 目錄的讀取、寫入及執行存取
```

#### js-io-rights.conf 檔案中的規則

Orchestrator 依照存取權限出現在 `js-io-rights.conf` 檔案中的順序，依序解析存取權限。每一行的規則皆覆蓋前一行規則。

---

**重要事項** 您可以透過在 `js-io-rights.conf` 檔案中設定 `+rwx /`，允許對檔案系統所有部分的存取。然而，這麼做會造成高度的安全性風險。

---

## 為工作流程和動作設定伺服器檔案系統存取

若要變更工作流程和 Orchestrator API 可以存取伺服器檔案系統的範圍，請修改 `js-io-rights.conf` 組態檔案。當工作流程嘗試存取 Orchestrator 伺服器檔案系統時，便會建立 `js-io-rights.conf` 檔案。

#### 程序

- 1 以 `root` 身分登入 Orchestrator Appliance 的 Linux 主控台。
- 2 瀏覽至 `/etc/vco/app-server`。
- 3 以文字編輯器開啟 `js-io-rights.conf` 組態檔案。

- 4 在 `js-io-rights.conf` 檔案中新增必要的行，以允許或拒絕存取檔案系統的不同區域。

例如，下行拒絕了 `/path_to_folder/noexec` 目錄中的執行權限：

```
-x /path_to_folder/noexec
```

`/Path_to_folder/noexec` 會保留執行權限，`/path_to_folder/noexec/bar` 則不會。兩個目錄仍保留讀取及寫入權限。


您為工作流程和 Orchestrator API 修改了檔案系統的存取權限。

## 為工作流程和動作設定作業系統命令的存取

Orchestrator API 提供的指令碼類別 `Command` 可執行 Orchestrator 伺服器主機作業系統中的命令。若要防止未授權存取 Orchestrator 伺服器主機，依預設 Orchestrator 應用程式沒有執行 `Command` 類別的權限。如果 Orchestrator 應用程式需要在主機作業系統執行命令的權限，您可以啟用 `Command` 指令碼類別。

透過設定 Orchestrator 組態系統內容，您可以授與使用 `Command` 類別的權限。

### 程序

- 1 以**管理員**身分登入控制中心。
- 2 按一下**系統內容**。
- 3 按一下**新增**圖示 ( )。
- 4 在**金鑰**文字方塊中，輸入 `com.vmware.js.allow-local-process`。
- 5 在**值**文字方塊中，輸入 `true`。
- 6 在**說明**文字方塊中，輸入該系統內容的說明。
- 7 按一下**新增**。
- 8 從快顯功能表按一下**儲存變更**。  
出現表示您已成功儲存的訊息。
- 9 重新啟動 Orchestrator 伺服器。

您向 Orchestrator 應用程式授與了在 Orchestrator 伺服器主機作業系統中執行本機命令的權限。

---

**備註** 透過將 `com.vmware.js.allow-local-process` 系統內容設定為 `true`，您允許 `Command` 指令碼類別在檔案系統中的任何地方寫入。該內容只會為 `Command` 指令碼類別覆寫您在 `js-io-rights.conf` 檔案中設定的任何檔案系統存取權限。您在 `js-io-rights.conf` 檔案設定的檔案系統存取權限仍會套用在 `Command` 之外的所有指令碼類別。

---

## 設定 Java 類別的 JavaScript 存取


依預設，Orchestrator 會限制 JavaScript 存取有限的 Java 類別。若您需要 JavaScript 存取更廣泛的 Java 類別，您必須正確設定 Orchestrator 系統，以允許此存取。

允許 JavaScript 引擎可完整存取 Java 虛擬機器 (JVM) 會導致潛在的安全性問題。格式錯誤或惡意的指令碼可能執行 Orchestrator 伺服器的使用者可存取的所有系統元件。因此，依預設，Orchestrator JavaScript 引擎只能存取 `java.util.*` 套件中的類別。

如果您需要 `java.util.*` 套件外部類別的 JavaScript 存取權，您可以在組態檔中列出允許 JavaScript 存取的 Java 套件。接著您即可設定 `com.vmware.scripting.rhino-class-shutter-file` 系統內容來指向此檔案。

**程序**

- 1 建立文字組態檔以儲存允許 JavaScript 存取的 Java 套件清單。  
 例如，若要允許 java.net 套件中所有類別和 java.lang.Object 類別的 JavaScript 存取權，您可以將下列內容新增至該檔案。  

```
java.net.*
java.lang.Object
```
- 2 以適當的名稱將組態檔儲存於適當位置。
- 3 以**管理員**身分登入控制中心。
- 4 按一下**系統內容**。
- 5 按一下**新增**圖示 ( )。
- 6 在**索引鍵**文字方塊中，輸入 `com.vmware.scripting.rhino-class-shutter-file`。
- 7 在**值**文字方塊中，輸入組態檔的路徑。
- 8 在**說明**文字方塊中，輸入該系統內容的說明。
- 9 按一下**新增**。
- 10 從快顯功能表按一下**儲存變更**。  
 隨即出現表示您已成功儲存的訊息。
- 11 重新啟動 Orchestrator 伺服器。

JavaScript 引擎即可存取您指定的 Java 類別。


**設定自訂逾時內容**

當 vCenter Server 過載時，將回應傳回 Orchestrator 伺服器所需要的時間會比預設設定的 20000 毫秒還長。為了防止該情況，您必須修改 Orchestrator 組態檔案，以調高預設的逾時時間。

如果預設的逾時時間在特定作業完成前到期，Orchestrator 伺服器記錄會包含錯誤。

```
Operation 'getPropertyContent' total time : '5742228' for 1823 calls, mean time : '3149.0', min
time : '0', max time : '32313' Timeout, unable to get property 'info'
com.vmware.vmo.plugin.vi4.model.TimeoutException
```

**程序**

- 1 以**管理員**身分登入控制中心。
- 2 按一下**系統內容**。
- 3 按一下**新增**圖示 ( )。
- 4 在**金鑰**文字方塊中輸入 `com.vmware.vmo.plugin.vi4.waitUpdatesTimeout`。
- 5 在**值**文字方塊中輸入新的逾時時間 (單位為毫秒)。
- 6 (選擇性) 在**說明**文字方塊中輸入該系統內容的說明。
- 7 按一下**新增**。
- 8 按一下彈出式功能表中的**儲存變更**。  
 會有個訊息說明您已成功儲存這些設定。
- 9 重新啟動 Orchestrator 伺服器。



您設定的值將覆寫預設逾時設定的 20000 毫秒。



安裝和設定完成後 vRealize Orchestrator，便能使用 Orchestrator 將虛擬環境管理相關的經常重複程序自動化。

- 登入 Orchestrator Client、執行然後排定 vCenter Server 詳細目錄物件或 Orchestrator 透過外掛程式存取之其他物件上的工作流程。請參閱 *使用 VMware vRealize Orchestrator Client*。
- 複製和修改標準 Orchestrator 工作流程，以及寫入您自己的動作和工作流程，即可自動化 vCenter Server 中的作業。
- 開發外掛程式和 Web 服務，即可擴充 Orchestrator 平台。
- 使用 vSphere Web Client，執行 vSphere 詳細目錄物件上的工作流程。

## 從 Orchestrator 應用裝置網路主控台登入 Orchestrator 用戶端

若要執行一般管理工作或編輯及建立工作流程，您必須登入 Orchestrator 用戶端介面。

Orchestrator 用戶端介面專為具有管理權限，並想要開發工作流程、動作及其他自訂元素的開發人員所設計。

---

**重要事項** 確保 Orchestrator Appliance 時脈與 Orchestrator 用戶端機器皆同步化。

---

### 先決條件

- 下載並部署 Orchestrator Appliance。
- 請確認應用裝置已啟動且正在執行中。
- 在即將執行 Orchestrator 用戶端的工作站安裝 64 位元 Java。

---

**備註** 不支援 32 位元 Java

---

### 程序

- 1 在網頁瀏覽器中，前往 Orchestrator Appliance 虛擬機器的 IP 位址。

`http://orchestrator_appliance_ip`

- 2 按一下 **啟動 Orchestrator 用戶端**。
- 3 在 **主機名稱** 文字方塊中輸入 IP 或網域名稱 Orchestrator Appliance。  
依預設將顯示 Orchestrator Appliance 的 IP 位址。
- 4 使用 Orchestrator 用戶端使用者名稱和密碼登入。

若您使用 vRealize Automation 驗證、vCenter Single Sign-On 或其他目錄服務做為驗證方法，請鍵入個別認證以登入至 Orchestrator 用戶端。

- 5 在安全性警告視窗中，選取用於處理憑證警告的選項。

Orchestrator 用戶端使用 SSL 憑證與 Orchestrator 伺服器進行通訊。受信任的 CA 不會在安裝期間簽署憑證。每次連線到 Orchestrator 伺服器時都會收到憑證警告。

選項	說明
<b>略過</b>	繼續使用目前的 SSL 憑證。 重新連線至相同的 Orchestrator 伺服器或嘗試將工作流程與遠端 Orchestrator 伺服器同步時，警告訊息再次出現。
<b>取消</b>	關閉視窗並停止登入程序。
<b>安裝此憑證，並且不再為其顯示任何安全性警告。</b>	選取此核取方塊並按一下 <b>略過</b> ，以安裝憑證並停止接收安全性警告。

您可以使用 CA 簽署的憑證變更預設 SSL 憑證。如需有關變更 SSL 憑證的詳細資訊，請參閱 *安裝和設定 VMware vRealize Orchestrator*。

### 下一個

您可以在此系統中匯入套件、啟動工作流程或設定根存取權。

# 索引

## 字母

指派靜態 IP 21

設定

網路設定 21

代理設定 21

控制中心 REST API 42

客戶經驗改進計劃, 收集的資訊 37

偵錯模式 52

偵錯 52

停用 Orchestrator 用戶端的存取權 61

停用 SSH 登入 21

啟用 SSH 登入 21

匯出資料庫 29

繼續閱讀 67

i18n 支援 14

JavaScript 63

js-io-rights.conf 檔案

內容 62

規則 62

LDAP 14

Orchestrator, 登錄為延伸模組 49

Orchestrator API

js-io-rights.conf 檔案 62

檔案系統存取 62

Orchestrator Appliance

下載 19

系統需求 13

記憶體 13

部署 19

硬碟 13

Orchestrator 用戶端, 停用存取權 61

Orchestrator 伺服器偵錯 52

Orchestrator 元素, 備份 52

Orchestrator 外掛程式 12

Orchestrator 伺服器備份 54

Orchestrator 伺服器還原 54

Orchestrator 版本 14

Orchestrator 架構 11

Orchestrator 硬體裝置, 變更密碼 20

Orchestrator 叢集 36

Orchestrator 簡介 9

REST API

建立金鑰儲存區 40

刪除 SSL 憑證 39

SSL 憑證匯入 40

刪除金鑰儲存區 41

新增金鑰 41

管理 SSL 憑證 39

情境 49

SSH 登入 21

SSL 信任管理員 39

SSL 憑證 50

解除登錄 Orchestrator 驗證 50

使用案例 49

vCenter Server 49

VMware vRealize Orchestrator 伺服器, 安裝成為  
Windows 服務 33

vRealize Automation 驗證 23

vSphere 驗證 25

下一步 67

## 三劃

下載 Orchestrator 應用裝置 19

工作流程引擎 9

已完成的工作流程, 工作流程記錄 48

## 四劃

內容, js-io-rights.conf 檔案 62

升級 Orchestrator 19

## 五劃

可用性 17

外掛程式, 移除外掛程式 32

本機存放區, 憑證 50

## 六劃

同時執行的工作流程數量上限 46

安全性 9

安裝 Orchestrator 19

安裝準則

vCenter Server 17

vRealize Automation 驗證 17

vSphere 驗證 17

驗證方法 17

## 七劃

- 伺服器記錄
  - 記錄層級 47
  - 匯出 47
- 伺服器模式 33
- 伺服器憑證
  - CA 簽署 30
  - 自我簽署 30
- 作業系統 14
- 作業系統命令, 存取 63
- 即時資料流 48
- 災難復原 56
- 系統內容 46, 61, 63, 64
- 系統需求
  - Orchestrator Appliance 13
  - 支援的資料庫 14
  - 支援的瀏覽器 13
- 角色型存取管理 36

## 八劃

- 使用者角色 11, 37
- 其他設定選項 43
- 取消工作流程 51
- 取消正在執行的工作流程, 取消工作流程 識別碼 51
- 命令列工具 39
- 命令指令碼類別 63
- 服務
  - VMware vRealize Orchestrator 伺服器 33
  - 啟動 33
- 版本設定 9
- 初始組態 23
- 非 ASCII 字元 14, 28

## 九劃

- 保護群組
  - vSphere Replication 57
  - 建立 57
  - 陣列式複寫 57
  - 儲存區原則 57
- 持續性 9
- 指令碼, shutter 系統內容 63
- 指令碼引擎 9
- 為 vSphere Replication 設定虛擬機器 56
- 重新設定驗證 43

## 十劃

- 原則引擎 9
- 記錄
  - 非持續型記錄 47
  - 持續型記錄 47

- 記錄檔 48
- 陣列式復原計劃, 建立 57

## 十一劃

- 停用 38
- 偵錯記錄 32
- 國際化 14
- 執行指令碼
  - 存取 Java 類別 63
  - 存取作業系統命令 63
- 啟用 38
- 移除節點 36
- 組態
  - 匯入組態設定 45
  - 匯出組態設定 44
  - 資料庫連線 27, 28
- 組態設定精靈 23
- 規則, js-io-rights.conf 檔案 62
- 設定初始組態 25
- 部署 Orchestrator 應用裝置 19

## 十二劃

- 備份, 組態 52
- 備份 Orchestrator 54
- 復原計劃
  - 建立資料夾 58
  - 重新命名資料夾 58
  - 新增到資料夾 58
  - 變更內容 58
- 登入, Orchestrator 用戶端 67
- 登入到, Linux 主控台 20
- 硬體需求, Orchestrator Appliance 13
- 開啟電源 20

## 十三劃

- 匯入資料庫 29
- 新增, 憑證 50
- 資料庫
  - Oracle 17
  - SQL Server 17
  - SQL Server Express 17
  - 安裝 17
  - 伺服器大小 17
  - 設定 17
  - 連線參數 28
  - 匯入 SSL 憑證 27
- 資料庫需求 14
- 逾時 64
- 預設連接埠
  - HTTP 連接埠 15, 26
  - HTTPS 連接埠 15, 26
  - Oracle 連接埠 15, 26

SMTP 連接埠 15, 26  
SQL Server 連接埠 15, 26  
vCenter API 連接埠 15, 26  
Web 組態 HTTP 存取連接埠 15, 26  
Web 組態 HTTPS 存取連接埠 15, 26  
命令連接埠 15, 26  
查詢連接埠 15, 26  
訊息連接埠 15, 26  
資料連接埠 15, 26

## 十四劃

對象 7

## 十五劃

層級或權限, js-io-rights.conf 檔案 62

## 十六劃

篩選, Orchestrator 記錄 48

## 十七劃

擱置的工作流程數量上限 46

檔案系統

從工作流程存取 62

設定工作流程存取 62

檢查工作流程 48

檢查點 9

還原 Orchestrator 54, 55

還原 Orchestrator 伺服器 55

還原 Orchestrator 虛擬機器 55

叢集模式 33–35

## 十八劃

擴充性 17

## 二十二劃

權限允許, js-io-rights.conf 檔案 62

權限拒絕, js-io-rights.conf 檔案 62

## 二十三劃

變更 Orchestrator 硬體裝置的密碼 20

變更管理網站的 SSL 憑證。 51

變更驗證參數 44

變更驗證提供者 43

