

管理 vRealize Automation

2020 年 12 月 21 日

vRealize Automation 8.1

您可以在 VMware 網站上找到最新的技術文件，網址如下：

<https://docs.vmware.com/tw/>

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2021 VMware, Inc. 保留所有權利。 [版權與商標資訊](#)。

目錄

- 1 管理 vRealize Automation 4**
- 2 管理使用者 5**
 - 如何在 vRealize Automation 中為專案啟用 Active Directory 群組 6
 - 如何在 vRealize Automation 中移除使用者 7
 - f 如何在 vRealize Automation 中編輯使用者角色 7
 - 如何在 vRealize Automation 中編輯群組角色指派 8
 - 什麼是 vRealize Automation 使用者角色 8
- 3 維護您的應用裝置 16**
 - 啟動和停止 vRealize Automation 16
 - 更新 vRealize Automation 的 DNS 指派 17
 - 如何啟用時間同步 18
 - 如何停用時間同步 19
 - 如何重設 root 密碼 19
- 4 在 vRealize Automation 中使用多組織承租人組態 21**
 - 為 vRealize Automation 設定多組織租戶 23
 - 管理單一節點多組織部署下的憑證和 DNS 組態 25
 - 管理叢集化 vRealize Automation 部署下的憑證和 DNS 組態 26
 - 登入承租人並在 vRealize Automation 中新增使用者 28
 - 將 vRealize Orchestrator 與 vRealize Automation 多組織部署搭配使用 29
- 5 使用記錄 30**
 - 如何使用記錄和記錄服務包 30
 - 如何設定將記錄轉送到 vRealize Log Insight 32
 - 如何建立或更新 Syslog 整合 34
 - 如何刪除用於記錄的 Syslog 整合 35
- 6 參與客戶經驗改進計劃 37**
 - 如何加入或退出計劃 37
 - 如何設定計劃的資料收集時間 37

管理 vRealize Automation

1

本指南說明了如何監控和管理 vRealize Automation 部署的關鍵基礎結構和使用者管理方面。

此處所述的工作對於保持 vRealize Automation 部署適當運作至關重要。這些工作包括使用者和群組管理以及監控系統記錄。

此外，還說明了如何設定和管理多組織部署。

雖然部分 vRealize Automation 管理工作是在 vRealize Automation 中完成的，但其他工作需要使用 vRealize Suite Lifecycle Manager 和 Workspace ONE Access 等相關產品。使用者應先自行熟悉這些產品及其功能，然後再完成適當的工作。

例如，如需備份、還原和災難復原的相關資訊，請參閱 [vRealize Suite 產品說明文件](#) 的〈[備份與還原以及災難復原 > 2019](#)〉一節。

備註 vRealize Automation 8.0.1 及更新版本支援災難復原。

如需使用 vRealize Suite Lifecycle Manager 安裝、升級和管理的相關資訊，請參閱 [Lifecycle Manager 產品說明文件](#)。

在 vRealize Automation 中管理使用者和群組

2

vRealize Automation 使用 VMware Workspace ONE Access (VMware 提供的身分識別管理應用程式) 來匯入並管理使用者和群組。匯入或建立使用者和群組之後，您可以使用 [身分識別與存取管理] 頁面管理單一承租人部署的角色指派。

使用 VMware Lifecycle Manager (vRSLCM 或 LCM) 來安裝 vRealize Automation。安裝 vRealize Automation 時，必須匯入現有的 Workspace ONE Access 執行個體，或部署一個新的執行個體以支援身分識別管理。這兩種案例定義了您的管理選項。

- 如果您部署新的 Workspace ONE Access 執行個體，可以透過 LCM 管理使用者和群組。在安裝期間，您可以使用 Workspace ONE Access 設定 Active Directory 連線。或者，您可以使用此處所述的 [身分識別與存取管理] 頁面檢視和編輯 vRealize Automation 中使用者和群組的某些方面。
- 如果您使用現有的 Workspace ONE Access 執行個體，則會在安裝期間將其匯入，以便透過 LCM 與 vRealize Automation 搭配使用。在此情況下，您可以繼續使用 Workspace ONE Access 來管理使用者和群組，也可以使用 LCM 中的管理功能。

如需有關管理多組織部署下的使用者的詳細資訊，請參閱[登入承租人並在 vRealize Automation 中新增使用者](#)。

vRealize Automation 使用者必須指派有角色。這些角色定義了對應用程式中的功能的存取權。當 vRealize Automation 安裝有 Workspace ONE Access 執行個體時，將會建立一個預設組織，且安裝程式指派有組織擁有者角色。所有其他 vRealize Automation 角色由組織擁有者指派。

vRealize Automation 中有三種類型的角色：組織角色、服務角色和專案角色。對於 vRealize Automation Cloud Assembly、Service Broker 和 Code Stream，通常使用者層級角色可使用資源，而管理員層級角色則需要建立和設定資源。組織角色會在承租人內定義權限；組織擁有者具有管理員層級的權限，而組織成員擁有使用者層級的權限。組織擁有者可以新增和管理其他使用者。

組織角色	服務角色
■ 組織擁有者	■ Cloud Assembly 管理員
■ 組織成員	■ Cloud Assembly 使用者
	■ Cloud Assembly 檢視者
	■ Service Broker 管理員
	■ Service Broker 使用者
	■ Service Broker 檢視者
	■ Code Stream 管理員
	■ Code Stream 使用者
	■ Code Stream 檢視者

此外，資料表中不顯示兩個主要的專案層級角色：專案管理員和專案使用者。將按照每個專案為 Cloud Assembly 隨機指派這些角色。這些角色有些不穩定。同一使用者可以是一個專案中的管理員，同時是另一個專案中的使用者。如需詳細資訊，請參閱[什麼是 vRealize Automation 使用者角色](#)。

如需有關使用 LCM 和 Workspace ONE Access 的詳細資訊，請參閱〈[使用 VMware Identity Manager 管理使用者](#)〉。

本章節討論下列主題：

- [如何在 vRealize Automation 中為專案啟用 Active Directory 群組](#)
- [如何在 vRealize Automation 中移除使用者](#)
- [f 如何在 vRealize Automation 中編輯使用者角色](#)
- [如何在 vRealize Automation 中編輯群組角色指派](#)
- [什麼是 vRealize Automation 使用者角色](#)

如何在 vRealize Automation 中為專案啟用 Active Directory 群組

如果在新增使用者至專案時 [新增群組] 頁面上沒有群組，請檢查 [身分識別與存取管理] 頁面並新增群組 (如果可用)。如果群組未列在 vRealize Automation 的 [身分識別與存取管理] 頁面上，可能不會在 Workspace One Access 執行個體中同步該群組。您可以確認它是否已同步，然後使用此程序來新增群組，如此處所示。

若要將 Active Directory 群組的成員新增至專案，您必須確保此群組與 Workspace One Access 執行個體同步並且該群組已新增至組織。

必要條件

如果這些群組未同步，則當您嘗試將其新增至專案時將無法使用。確認您已將 Active Directory 群組與 Lifecycle Manager 執行個體同步。

程序

- 1 以使用者身分從新增的同一個 Active Directory 網域登入 vRealize Automation。例如，@mycompany.com

- 2 在 Cloud Assembly 中，按一下標頭右側導覽中的 [身分識別與存取管理]。
- 3 按一下**企業群組**，然後按一下**指派角色**。
- 4 使用搜尋功能找到您要新增的群組，然後選取該群組。
- 5 指派組織角色。

該群組必須至少具有組織成員角色。如需詳細資訊，請參閱〈[什麼是 vRealize Automation Cloud Assembly 使用者角色](#)〉。

- 6 按一下**新增服務存取權**，新增一或多個服務，然後為每個服務選取角色。
- 7 按一下**指派**。

結果

您現在可以將 Active Directory 群組新增至專案。

如何在 vRealize Automation 中移除使用者

您可以視需要在 vRealize Automation 中移除使用者。

依預設會列出所有使用者，且您無法使用 [身分識別與存取管理] 頁面來新增使用者。您可以刪除使用者。

程序

- 1 在 [身分識別與存取管理] 頁面上，選取 [作用中使用者] 索引標籤。
- 2 找到並選取您要刪除的使用者。
- 3 按一下**移除使用者**。

結果

將會移除選取的使用者。

f 如何在 vRealize Automation 中編輯使用者角色

您可以編輯指派給已匯入至 vRealize Automation 的 Workspace One Access 使用者的角色。

必要條件

程序

- 1 在 Cloud Assembly 中，按一下標頭右側導覽中的 [身分識別與存取管理]。
- 2 在 [作用中使用者] 索引標籤上選取所需的使用者，然後按一下**編輯角色**。
- 3 您可以編輯使用者的組織和服務角色。
 - 選取 [指派組織角色] 標題旁邊的下拉式功能表，以變更使用者與組織的關係。
 - 按一下 [新增服務存取權]，為使用者新增服務角色。

- 若要移除使用者角色，請按一下相應服務旁邊的 X。

4 按一下**儲存**。

結果

將按指定的方式更新使用者角色指派。

如何在 vRealize Automation 中編輯群組角色指派

您可以在 vRealize Automation 中編輯群組的角色指派

必要條件

使用者和群組已從與 vRealize Automation 部署相關聯的有效 vIDM 執行個體中匯入。

程序

- 1 在 Cloud Assembly 中，按一下標頭右側導覽中的 [身分識別與存取管理]。
- 2 選取 [企業群組] 索引標籤。
- 3 在搜尋欄位中，輸入您要編輯其角色指派的群組的名稱。
- 4 編輯所選群組的角色指派。您有兩個選項可供選擇。
 - 指派組織角色
 - 指派服務角色

5 按一下**指派**。

結果

將按指定的方式更新角色指派。

什麼是 vRealize Automation 使用者角色

做為組織擁有者，您可以為使用者指派組織角色和服務角色。角色決定了使用者可以執行的動作或查看的內容。然後，在服務中，服務管理員可以指派專案角色。若要確定您要指派的角色，請評估下表中的工作。

Cloud Assembly 服務角色

vRealize Automation Cloud Assembly 服務角色決定了您可以在 vRealize Automation Cloud Assembly 中看到和執行什麼。這些服務角色由組織擁有者在主控台中定義。

表 2-1. vRealize Automation Cloud Assembly 服務角色說明

角色	說明
Cloud Assembly 管理員	必須具有整個使用者介面和 API 資源的讀取和寫入權限。這是唯一可查看和執行所有操作的使用者角色，包括新增雲端帳戶、建立新專案，以及指派專案管理員。
Cloud Assembly 使用者	沒有 Cloud Assembly 管理員角色的使用者。 在 vRealize Automation Cloud Assembly 專案中，管理員會將使用者新增至專案做為專案成員。管理員也可以新增專案管理員。這兩種角色的權限定義如下。
Cloud Assembly 檢視者	可查看資訊，但無法建立、更新或刪除值的使用者。這是唯讀角色。

除了服務角色以外，vRealize Automation Cloud Assembly 還具有專案角色。

專案角色是在 vRealize Automation Cloud Assembly 中定義的，可能會因專案而異。

在以下說明不同的服務和專案角色可以查看和執行哪些動作的資料表中，請記住，服務管理員對使用者介面的所有區域擁有完整權限。

這些專案角色的說明將有助於您決定授與使用者哪些權限。

- 專案管理員利用服務管理員所建立的基礎結構，來確保其專案成員具有其開發工作所需的資源。
- 專案成員在其專案中運作，以設計和部署藍圖。
- 專案檢視者僅限於唯讀存取，但在某些情況下，他們可以執行下載藍圖等不具破壞性的操作。

表 2-2. vRealize Automation Cloud Assembly 服務角色和專案角色

UI 內容	工作	Cloud Assembly 管理員	Cloud Assembly 檢視者	Cloud Assembly 使用者		
				使用者必須是專案管理員或成員，才能查看和執行與專案相關的工作。		
				專案管理員	專案成員	專案檢視者
存取 Cloud Assembly						
主控台	在 vRA 主控台中，您可以查看並開啟 Cloud Assembly	是	是	是	是	是
基礎結構						
	查看並開啟 [基礎結構] 索引標籤	是	是	是	是	是
設定 - 專案	建立專案	是				
	更新或刪除專案摘要、使用者、佈建、Kubernetes、整合和測試專案組態中的值。	是		是。您的專案		
	在專案中新增使用者和指派角色。	是		是。您的專案。		
	檢視專案	是	是	是。您的專案	是。您的專案	是。您的專案

表 2-2. vRealize Automation Cloud Assembly 服務角色和專案角色 (續)

UI 內容	工作	Cloud Assembly 管理員	Cloud Assembly 檢視者	Cloud Assembly 使用者 使用者必須是專案管理員或成員，才能查看和執行與專案相關的工作。		
				專案管理員	專案成員	專案檢視者
設定 - 雲端區域	建立、更新或刪除雲端區域	是				
	檢視雲端區域	是	是			
設定 - Kubernetes 區域	建立、更新或刪除 Kubernetes 區域	是				
	檢視 Kubernetes 區域	是	是			
設定 - 類型模板	建立、更新或刪除類型模板	是				
	檢視類型模板	是	是			
設定 - 映像對應	建立、更新或刪除映像對應	是				
	檢視映像對應	是	是			
設定 - 網路設定檔	建立、更新或刪除網路設定檔	是				
	檢視映像網路設定檔	是	是			
設定 - 儲存區設定檔	建立、更新或刪除儲存區設定檔	是				
	檢視映像儲存區設定檔	是	是			
設定 - 定價卡	建立、更新或刪除定價卡	是				
	檢視定價卡	是	是			
設定 - 標籤	建立、更新或刪除標籤	是				
	檢視標籤	是	是			
資源 - 計算	將標籤新增至探索到的計算資源	是				
	檢視探索到的計算資源	是	是			
資源 - 網路	修改網路標籤、IP 範圍、IP 位址	是				
	檢視探索到的網路資源	是	是			
資源 - 安全性	將標籤新增至探索到的安全群組	是				
	檢視探索到的安全群組	是	是			
資源 - 儲存區	將標籤新增至探索到的儲存區	是				
	檢視儲存區	是	是			
資源 - 機器	新增和刪除機器	是				
	檢視機器	是	是	是。您的專案	是。您的專案	是。您的專案
資源 - 磁碟區	刪除探索到的儲存磁碟區	是				
	檢視探索到的儲存磁碟區	是	是	是。您的專案	是。您的專案	是。您的專案。

表 2-2. vRealize Automation Cloud Assembly 服務角色和專案角色 (續)

UI 內容	工作	Cloud Assembly 管理員	Cloud Assembly 檢視者	Cloud Assembly 使用者 使用者必須是專案管理員或成員，才能查看和執行與專案相關的工作。		
				專案管理員	專案成員	專案檢視者
資源 - Kubernetes	部署或新增 Kubernetes 叢集，以及建立或新增命名空間	是				
	檢視 Kubernetes 叢集和命名空間	是	是	是。您的專案	是。您的專案	是。您的專案
活動 - 要求	刪除部署請求記錄	是				
	檢視部署請求記錄	是	是	是。您的專案	是。您的專案	是。您的專案
活動 - 事件記錄	檢視事件記錄	是	是	是。您的專案	是。您的專案	是。您的專案
連線 - 雲端帳戶	建立、更新或刪除雲端帳戶	是				
	檢視雲端帳戶	是	是			
連線 - 整合	建立、更新或刪除整合	是				
	檢視整合	是	是			
上線	建立、更新或刪除上線計劃	是				
	檢視上線計劃	是	是			是。您的專案
市集						
	查看並開啟 [市集] 索引標籤	是	是			
	使用 [設計] 索引標籤上已下載的藍圖	是		是。如果與您的專案相關聯。	是。如果與您的專案相關聯。	
市集 - 藍圖	下載藍圖	是				
	檢視藍圖	是	是			
市集 - 映像	下載映像	是				
	檢視映像	是	是			
市集 - 下載	檢視所有已下載項目的記錄	是	是			
擴充性						
	查看並開啟 [擴充性] 索引標籤	是	是			是
事件	檢視擴充性事件	是	是			
訂閱	建立、更新或刪除擴充性訂閱	是				
	停用訂閱	是				
	檢視訂閱	是	是			

表 2-2. vRealize Automation Cloud Assembly 服務角色和專案角色 (續)

UI 內容	工作	Cloud Assembly 管理員	Cloud Assembly 檢視者	Cloud Assembly 使用者 使用者必須是專案管理員或成員，才能查看和執行與專案相關的工作。		
				專案管理員	專案成員	專案檢視者
程式庫 - 事件主題	檢視事件主題	是	是			
程式庫 - 動作	建立、更新或刪除擴充性動作	是				
	檢視擴充性動作	是	是			
程式庫 - 工作流程	檢視擴充性工作流程	是	是			
活動 - 動作執行	取消或刪除擴充性動作執行	是				
	檢視擴充性動作執行	是	是			是。您的專案
活動 - 工作流程執行	檢視擴充性工作流程執行	是	是			
設計						
設計	開啟 [設計] 索引標籤並查看藍圖清單	是	是	是。您的專案	是。您的專案	是。您的專案
藍圖	建立、更新和刪除藍圖	是		是。您的專案	是。您的專案	
	檢視藍圖	是	是	是。您的專案	是。您的專案	是。您的專案
	下載藍圖	是	是	是。您的專案	是。您的專案	是。您的專案
	上傳藍圖	是		是。您的專案	是。您的專案	
	部署藍圖	是		是。您的專案	是。您的專案	
	版本設定和還原藍圖	是		是。您的專案	是。您的專案	
	將藍圖發佈到目錄	是		是。您的專案		
自訂資源	建立、更新或刪除自訂資源	是				
	檢視自訂資源	是	是	是。您的專案	是。您的專案	是。您的專案
自訂動作	建立、更新或刪除自訂動作	是				
	檢視自訂動作	是	是	是。您的專案	是。您的專案	是。您的專案
部署						
	查看並開啟 [部署] 索引標籤	是	是	是	是	是

表 2-2. vRealize Automation Cloud Assembly 服務角色和專案角色 (續)

UI 內容	工作	Cloud Assembly 管理員	Cloud Assembly 檢視者	Cloud Assembly 使用者 使用者必須是專案管理員或成員，才能查看和執行與專案相關的工作。		
				專案管理員	專案成員	專案檢視者
	檢視部署，包括部署詳細資料、部署歷程記錄，以及疑難排解資訊。	是	是	是。您的專案	是。您的專案	是。您的專案
	根據原則對部署執行第 2 天動作	是		是。您的專案	是。您的專案	

Service Broker 服務角色

vRealize Automation Service Broker 服務角色決定了您可以在 vRealize Automation Service Broker 中看到和執行什麼。這些服務角色由組織擁有者在主控台中定義。

表 2-3. Service Broker 服務角色說明

角色	說明
Service Broker 管理員	必須具有整個使用者介面和 API 資源的讀取和寫入權限。這是可以執行所有工作 (包括建立新專案和指派專案管理員) 的唯一使用者角色。
Service Broker 使用者	沒有 vRealize Automation Service Broker 管理員角色的任何使用者。 在 vRealize Automation Service Broker 專案中，管理員會將使用者新增至專案做為專案成員。管理員也可以新增專案管理員。這兩種角色的權限定義如下。
Service Broker 檢視者	具有唯讀權限的使用者，可以查看資訊，但無法建立、更新或刪除值。

除了服務角色以外，vRealize Automation Service Broker 還具有專案角色。

專案角色是在 vRealize Automation Service Broker 中定義的，可能會因專案而異。

在以下說明不同的服務和專案角色可以查看和執行哪些動作的資料表中，請記住，服務管理員對使用者介面的所有區域擁有完整權限。

使用下列專案角色說明將有助於您決定授與使用者哪些權限。

- 專案管理員利用服務管理員所建立的基礎結構，來確保其專案成員具有其開發工作所需的資源。
- 專案成員在其專案中運作，以設計和部署藍圖。
- 專案檢視者僅限於唯讀存取。

表 2-4. Service Broker 服務角色和專案角色

UI 內容	工作	Service Broker 管理員	Service Broker 檢視者	Service Broker 使用者		
				使用者必須是專案管理員，才能查看和執行與專案相關的工作。		
				專案管理員	專案成員	專案檢視者
存取 Service Broker						
主控台	在主控台中，您可以查看並開啟 Service Broker	是	是	是	是	是
基礎結構						
	查看並開啟 [基礎結構] 索引標籤	是	是			
設定 - 專案	建立專案	是				
	更新或刪除專案摘要、使用者、佈建、Kubernetes 和整合中的值	是				
	檢視專案	是	是			
設定 - 雲端區域	建立、更新或刪除雲端區域	是				
	檢視雲端區域	是	是			
設定 - Kubernetes 區域	建立、更新或刪除 Kubernetes 區域	是				
	檢視 Kubernetes 區域	是	是			
連線 - 雲端帳戶	建立、更新或刪除雲端帳戶	是				
	檢視雲端帳戶	是	是			
連線 - 整合	建立、更新或刪除整合	是				
	檢視整合	是	是			
活動 - 要求	刪除部署請求記錄	是				
	檢視部署請求記錄	是				
活動 - 事件記錄	檢視事件記錄	是				
內容和原則						
	查看並開啟 [內容和原則] 索引標籤	是	是			
內容來源	建立、更新或刪除內容來源	是				
	檢視內容來源	是	是			
內容共用	新增或移除共用內容	是				
	檢視共用內容	是	是			
內容	自訂表單和設定項目	是				
	檢視內容	是	是			
原則 - 定義	建立、更新或刪除原則定義	是				

表 2-4. Service Broker 服務角色和專案角色 (續)

UI 內容	工作	Service Broker 管理員	Service Broker 檢視者	Service Broker 使用者 使用者必須是專案管理員，才能查看和執行與專案相關的工作。		
				專案管理員	專案成員	專案檢視者
	檢視原則定義	是	是			
原則 - 強制執行	檢視強制執行記錄	是	是			
通知 - 電子郵件伺服器	設定電子郵件伺服器	是				
目錄						
	查看並開啟 [目錄] 索引標籤	是	是	是	是	是
	檢視可用的目錄項目	是	是	是。您的專案	是。您的專案	是。您的專案
	請求目錄項目	是		是。您的專案	是。您的專案	
部署						
	查看並開啟 [部署] 索引標籤	是	是	是。	是	是
	檢視部署，包括部署詳細資料、部署歷程記錄，以及疑難排解資訊。	是	是	是。您的專案	是。您的專案	是。您的專案
	根據原則對部署執行第 2 天動作	是		是。您的專案	是。您的專案	
核准						
	查看並開啟 [核准] 索引標籤	是	是	是	是	是
	回應核准請求	是		僅限 Service Broker 使用者角色	僅限 Service Broker 使用者角色	僅限 Service Broker 使用者角色

維護您的 vRealize Automation 應用裝置

3

做為系統管理員，您可能需要執行各種工作，以確保已安裝的 vRealize Automation 應用程式正常運作。

如果您剛剛開始使用 vRealize Automation，則這些不是必要工作。如果您需要解決效能或產品行為問題，則瞭解如何執行這些工作非常有用。

本章節討論下列主題：

- [啟動和停止 vRealize Automation](#)
- [更新 vRealize Automation 的 DNS 指派](#)
- [如何啟用 vRealize Automation 的時間同步](#)
- [如何停用時間同步](#)
- [如何重設 vRealize Automation 的 root 密碼](#)

啟動和停止 vRealize Automation

啟動或關閉 vRealize Automation 時，請遵循適當的程序。

關閉 vRealize Automation

若保留資料完整性，請先關閉 vRealize Automation 服務，然後再關閉虛擬應用裝置的電源。

備註 如果可能，請避免使用 `vraccli reset vidm` 命令。此命令會重設 Workspace One Access 的所有組態，並中斷使用者與已佈建資源之間的關聯。

- 1 透過使用 SSH 或 VMRC 登入任何 vRealize Automation 應用裝置的主控台。
- 2 若要關閉所有叢集節點上的 vRealize Automation 服務，請執行下列命令集。

備註 如果您複製其中任何命令來執行但失敗，請先將其貼到記事本中，然後重新複製該命令後再執行。此程序去除了任何隱藏字元和說明文件來源中可能存在的其他構件。

```
/opt/scripts/svc-stop.sh
sleep 120
/opt/scripts/deploy.sh --onlyClean
```

- 3 關閉 vRealize Automation 應用裝置。

您的 vRealize Automation 部署現在已關閉。

啟動 vRealize Automation

在計劃外的關閉、控制關閉或復原程序之後，必須以特定順序重新啟動 vRealize Automation 元件。vRLCM 是非關鍵元件，因此您可以隨時啟動。必須先啟動 VMware Workspace ONE Access (以前稱為 VMware Identity Management) 元件，然後再啟動 vRealize Automation。

備註 在啟動 vRealize Automation 元件之前，請確認適用的負載平衡器正在執行。

- 1 開啟所有 vRealize Automation 應用裝置的電源，並等待其啟動。
- 2 透過使用 SSH 或 VMRC 登入任何應用裝置的主控台，然後執行下列命令以還原所有節點上的服務。

```
/opt/scripts/deploy.sh
```

- 3 透過下列命令，確認所有服務均已啟動且正在執行。

```
kubectl get pods --all-namespaces
```

備註 您應該會看到每個服務有三個執行個體，其狀態為 [執行中] 或 [已完成]。

當所有服務均列示為 [執行中] 或 [已完成]，則表示 vRealize Automation 已準備好可供使用。

重新啟動 vRealize Automation

您可以從叢集中的任何應用裝置集中重新啟動所有 vRealize Automation 服務。依照前述指示關閉 vRealize Automation，然後使用指示啟動 vRealize Automation。重新啟動 vRealize Automation 之前，請確認所有適用的負載平衡器和 VMware Workspace ONE Access 元件正在執行中。

當所有服務均列示為 [執行中] 或 [已完成]，則表示 vRealize Automation 已準備好可供使用。

執行以下命令，以確認所有服務正在執行：

```
kubectl -n prelude get pods
```

更新 vRealize Automation 的 DNS 指派

管理員可以更新 vRealize Automation 的 DNS 指派。

程序

- 1 透過使用 SSH 或 VMRC 登入任何 vRealize Automation 應用裝置的主控台。
- 2 若要關閉所有叢集節點上的 vRealize Automation 服務，請執行下列命令集。

```
/opt/scripts/svc-stop.sh
sleep 120
/opt/scripts/deploy.sh --onlyClean
```

- 3 登入 vCenter，並使用 Shut Down Guest OS 命令關閉所有 vRealize Automation 節點。
- 4 更新每個 vRealize Automation 節點的 OVF DNS 內容。
 - a 從 vCenter 詳細目錄導覽至 vRealize Automation 節點。
 - b 選取 [設定] 索引標籤，然後展開 [設定]。
 - c 選取 vApp 選項。
 - d 在 OVF 內容清單中找到並選取 vami.DNS.vRealize_Automation。
 - e 按一下**設定值**，然後在 [內容值] 文字方塊中輸入新的 DNS 項目。
 - f 按一下**確定**。
- 5 啟動所有 vRealize Automation 節點並等待其完全啟動，這將在主控台上以藍色畫面表示。
- 6 再次重新啟動 vRealize Automation 節點，並等待其完全啟動。
- 7 使用 SSH 登入每個 vRealize Automation 節點，並確認是否在 `/etc/resolve.conf` 中列出了新的 DNS 伺服器。
- 8 在其中一個 vRealize Automation 節點上，執行下列命令以啟動 vRealize Automation 服務：`/opt/scripts/deploy.sh`

結果

vRealize Automation DNS 設定將按指定的方式進行變更。

如何啟用 vRealize Automation 的時間同步

您可以使用 vRealize Automation 應用裝置命令列在 vRealize Automation 部署上啟用時間同步。

可以使用網路時間通訊協定 (NTP) 網路通訊協定為獨立或叢集化 vRealize Automation 部署設定時間同步。vRealize Automation 支援兩個相互排斥的 NTP 組態：

NTP 組態	說明
ESXi	<p>當主控 vRealize Automation 應用裝置的 ESXi 伺服器與 NTP 伺服器同步時，可以使用此組態。如果使用的是叢集化部署，則所有 ESXi 主機都必須與 NTP 伺服器同步。</p> <p>備註 如果 vRealize Automation 部署已移轉至未與 NTP 伺服器同步的 ESXi 主機，則可能會遇到時鐘偏差。</p> <p>如需有關為 ESXi 設定 NTP 的詳細資訊，請參閱知識庫文章 57147 使用 vSphere Web Client 在 ESXi 主機上設定網路時間通訊協定 (NTP)。</p>
systemd	<p>此組態會使用 systemd-timesyncd 精靈來同步 vRealize Automation 部署的時鐘。</p> <p>備註 依預設，systemd-timesyncd 精靈已啟用，但未設定 NTP 伺服器。如果 vRealize Automation 應用裝置使用動態 IP 組態，則應用裝置可以使用 DHCP 通訊協定所接收的任何 NTP 伺服器。</p>

程序

- 1 以根使用者身分登入 vRealize Automation 應用裝置命令列。

2 對 ESXi 啟用 NTP。

- a 執行 `vracli ntp esxi` 命令。
- b 執行 `vracli ntp apply` 命令。

ESXi NTP 組態會套用至 vRealize Automation 部署。

3 對 systemd 啟用 NTP。

- a 執行 `vracli ntp systemd --set FQDN_or_IP_of_systemd_server` 命令。

備註 可以新增多個 systemd NTP 伺服器，方法是使用逗號分隔其網路位址。

- b 執行 `vracli ntp apply` 命令。

systemd NTP 組態會套用至 vRealize Automation 部署。

4 (選擇性) 若要確認 NTP 組態的狀態，請執行 `vracli ntp status` 命令。

如果 NTP 伺服器與 vRealize Automation 部署之間的時間誤差超過 10 分鐘，則 NTP 組態可能會失敗。若要解決此問題，請將與 NTP 伺服器同步的 vRealize Automation 應用裝置重新開機。

如何停用時間同步

您可以使用 vRealize Automation 應用裝置命令列，在 vRealize Automation 部署上停用網路時間通訊協定 (NTP) 時間同步。

也可以透過執行 `vracli ntp reset` 命令來重設 vRealize Automation 應用裝置的 NTP 組態，並透過執行 `vracli ntp apply` 命令套用新的組態。

必要條件

確認您已設定與 ESXi 或 systemd 的時間同步。請參閱[如何啟用 vRealize Automation 的時間同步](#)。

程序

- 1 以根使用者身分登入 vRealize Automation 應用裝置命令列。
- 2 若要停用與 ESXi 或 systemd 的時間同步，請執行 `vracli ntp disable` 命令。
- 3 執行 `vracli ntp apply` 命令。
- 4 (選擇性) 若要確認 NTP 組態的狀態，請執行 `vracli ntp status` 命令。

如何重設 vRealize Automation 的 root 密碼

您可以重設遺失或忘記的 vRealize Automation root 密碼。

在此程序中，您可以使用主機 vCenter 應用裝置上的命令列視窗來重設組織的 vRealize Automation 根密碼。

必要條件

此程序適用於 vRealize Automation 管理員，並且需要存取主機 vCenter 應用裝置所需的認證。

程序

- 1 使用[啟動和停止 vRealize Automation](#) 中所述的程序，關閉和啟動 vRealize Automation。
- 2 當 Photon 作業系統命令列視窗出現時，請輸入 **e** 並按 **Enter** 鍵，以開啟 GNU GRUB 開機功能表編輯器。
- 3 在 GNU GRUB 編輯器中，在以 `linux "/" $photon_linux root=rootpartition` 開頭的一行的結尾處輸入 `rw init=/bin/bash`，如下所示：

```

GNU GRUB  version 2.02~beta2

setparams 'Photon'

  linux "/"$photon_linux root=$rootpartition root=$rootpartition $photon_cmd\
line coredump_filter=0x37 consoleblank=0 rw init=/bin/bash_
  if [ "$photon_initrd" ]; then
    initrd "/"$photon_initrd
  fi

Minimum Emacs-like screen editing is supported. TAB lists
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a
command-line or ESC to discard edits and return to the GRUB
menu.

```

- 4 按一下 **F10** 鍵以推送變更，然後重新啟動 vRealize Automation。
- 5 等待 vRealize Automation 重新啟動。
- 6 在 root [/]# 提示字元中，輸入 `passwd` 並按 **Enter** 鍵。
- 7 在 New password: 提示字元中，輸入新密碼並按 **Enter** 鍵。
- 8 在 Retype new password: 提示字元中，重新輸入新密碼並按 **Enter** 鍵。
- 9 在 root [/]# 提示字元中，輸入 `reboot -f` 並按 **Enter** 鍵，以完成 root 密碼重設程序。

```

root [/]# passwd
New password:
Retype new password:
passwd: password updated successfully
root [/]# reboot -f_

```

後續步驟

做為 vRealize Automation 管理員，您現在可以使用新 root 密碼登入 vRealize Automation。

在 vRealize Automation 中使用多組織承租人組態

4

vRealize Automation 可讓客戶 IT 提供者在每個部署內設定多個承租人或組織。提供者可以設定多個承租人組織，並在每個部署中配置基礎結構。提供者還可以為承租人管理使用者。每個承租人都管理其自己的專案、資源和部署。

在 vRealize Automation 多組織組態中，提供者可以建立多個組織，而每個承租人組織使用其自己的專案、資源和部署。雖然提供者無法遠端管理承租人基礎結構，但他們可以登入承租人並管理其承租人中的基礎結構。

多租戶依賴三個不同 VMware 產品的協調和組態，如下所示：

- **Workspace ONE Access-** 本產品為多租戶以及在承租人組織內提供使用者和群組管理的 Active Directory 網域連線提供基礎結構支援。
- **vRealize Suite Lifecycle Manager-** 此產品支援為受支援的產品 (例如 vRealize Automation) 建立和設定承租人。此外，它還提供了一些憑證管理功能。
- **vRealize Automation-** 提供者和使用者登入 vRealize Automation 以存取其建立和管理部署所在的承租人。

設定多租戶時，使用者應熟悉所有這三個產品及其相關的說明文件。

如需有關使用 LCM 和 Workspace ONE Access 的詳細資訊，請參閱〈[使用 VMware Identity Manager 管理使用者](#)〉和〈[VMware Workspace ONE Access 管理](#)〉。

具有 vRealize Suite Lifecycle Manager 權限的管理員使用身分識別與承租人管理服務下的 Lifecycle Manager [承租人] 頁面來建立和管理承租人。承租人是使用 Active Directory IWA 或 LDAP 連線來建構的，它們由 vRealize Automation 部署所需的相關聯 VMware Workspace ONE Access 執行個體所支援。如需使用 Lifecycle Manager 的相關資訊，請參閱相關的說明文件。

設定多租戶時，您可以從基礎或主要承租人開始。此承租人是基礎 Workspace ONE Access 應用程式部署時所建立的預設承租人。其他承租人 (稱為子承租人) 可以基於主要承租人。vRealize Automation 目前最多可支援 20 個具有標準三個節點部署的承租人組織。

設定多租戶的 vRealize Automation 時，您必須先在單一組織組態中安裝應用程式，然後使用 Lifecycle Manager 設定多組織組態。Workspace ONE Access 部署支援管理承租人和相關聯的 Active Directory 網域連線。

最初設定多租戶時，會在 Lifecycle Manager 中指定提供者管理員。如果需要，可以稍後變更此指定或新增管理員。在多組織組態下，vRealize Automation 使用者和群組主要透過 Workspace ONE Access 進行管理。

建立組織後，已獲得授權的使用者可以登入其應用程式，以建立或使用專案和資源並建立部署。管理員可以在 vRealize Automation 中管理使用者角色。

設定多組織組態

您可以在完成 vRealize Automation 安裝後啟用多組織部署。設定多組織組態時，您必須設定外部 Workspace ONE Access 以供多租戶使用，然後使用 Lifecycle Manager 來建立和設定承租人。這同時適用於新的和現有的部署。作為設定承租人的初始步驟，您必須使用 Lifecycle Manager 為 Workspace ONE Access 上預設建立的主要承租人設定別名。根據此主要承租人建立的子承租人會從此主要承租人繼承 Active Directory 網域組態。

在 Lifecycle Manager 中，將承租人指派給產品 (例如 vRealize Automation) 和特定環境。設定承租人時，還必須指定承租人管理員。依預設，會根據承租人主機名稱啟用多租戶。使用者可以選擇手動依 DNS 名稱設定承租人名稱。在此程序執行期間，您必須設定數個旗標以支援多租戶，並且必須同時設定負載平衡器。

如果您使用叢集化執行個體，則 Workspace ONE Access 和 vRealize Automation 以承租人為基礎的主機名稱將指向負載平衡器。

如果您的叢集化 vRealize Automation 和 Workspace ONE Access 負載平衡器不使用萬用字元憑證，則使用者必須將承租人主機名稱新增為憑證上的 SAN 項目。適用於所建立的每個新承租人。

您無法刪除 vRealize Automation 或 Lifecycle Manager 中的承租人。如果您需要將承租人新增至現有的多租戶部署，可以使用 Lifecycle Manager 來執行此操作，但會導致三到四小時的停機時間。

主機名稱和多租戶

在舊版 vRealize Automation 中，使用者使用以目錄路徑為基礎的 URL 存取承租人。在目前的多租戶實作中，使用者會根據主機名稱存取承租人。

此外，vRealize Automation 使用者將用來存取承租人的主機名稱格式與在 Workspace ONE Access 內存取承租人時所用的格式不同。例如，有效的主機名稱如下所示：`tenant1.example.eng.vmware.com`，而非 `vidm-node1.eng.vmware.com`。

多租戶和憑證

必須為多組織組態中涉及的所有元件建立憑證。您將需要 Workspace ONE Access、Lifecycle Manager 和 vRealize Automation 的一或多個憑證，具體取決於您使用的是單一節點組態還是叢集化組態。

設定憑證時，您可以使用萬用字元搭配 SAN 名稱，也可以使用專用名稱。使用萬用字元將在某種程度上簡化憑證管理，因為每次新增承租人時都必須更新憑證。如果您的 vRealize Automation 和 Workspace ONE Access 負載平衡器不使用萬用字元憑證，則必須針對建立的每個新承租人將承租人主機名稱新增為憑證上的 SAN 項目。此外，如果您使用 SAN，則在新增或刪除主機或變更主機名稱時，必須手動更新憑證。您還必須更新承租人的 DNS 項目。

請注意，Lifecycle Manager 不會為每個承租人建立單獨的憑證。相反，它會使用列出的每個承租人主機名稱建立單一憑證。對於基本組態，承租人的 CNAME 使用下列格式：

tenantname.vrahostname.domain。對於高可用性組態，名稱使用下列格式：

tenantname.vraLBhostname.domain。

如果您使用的是叢集化 Workspace ONE Access 組態，請注意，Lifecycle Manager 無法更新負載平衡器憑證，因此您必須手動更新它。此外，如果您需要重新登錄 Lifecycle Manager 外部的產品或服務，則這是一種手動程序。

本章節討論下列主題：

- 為 vRealize Automation 設定多組織租戶
- 登入承租人並在 vRealize Automation 中新增使用者
- 將 vRealize Orchestrator 與 vRealize Automation 多組織部署搭配使用

為 vRealize Automation 設定多組織租戶

您可以使用 vRealize Suite Lifecycle Manager 為 vRealize Automation 設定多組織租戶。

以下是針對 vRealize Automation 設定多租戶的程序的高階說明，其中包括設定 DNS 和憑證。此程序重點說明了單一節點部署，但也包括叢集化組態的說明。

如需設定 vRealize Automation 多組織組態的詳細資訊和視訊示範，請參閱 <https://vmwarelab.org/2020/04/14/vrealize-automation-8-1-multi-tenancy-setup-with-vrealize-suite-lifecycle-manager-8-1/>。

必要條件

- 安裝並設定 Workspace ONE Access 版本 3.3.2。
- 安裝並設定 vRealize Suite Lifecycle Manager 版本 8.1。

程序

1 建立所需的 A 和 CNAME 類型的 DNS 記錄。

- 對於您的主要承租人和每個子承租人，必須建立並套用 SAN 憑證。
- 對於單一節點部署，vRealize Automation FQDN 指向 vRealize Automation 應用裝置，而 Workspace ONE Access FQDN 則指向 Workspace ONE Access 應用裝置。
- 對於叢集化部署，以 Workspace ONE Access 和 vRealize Automation 承租人為基礎的 FQDN 必須指向其各自的負載平衡器。Workspace ONE Access 已設定 SSL 終止，因此憑證會同時套用至 Workspace ONE Access 叢集和負載平衡器。vRealize Automation 負載平衡器使用 SSL 傳遞，因此憑證僅套用至 vRealize Automation 叢集。

如需詳細資料，請參閱[管理單一節點多組織部署下的憑證和 DNS 組態](#)和[管理叢集化 vRealize Automation 部署下的憑證和 DNS 組態](#)。

2 為 Workspace ONE 3.3.2 和 vRA 8.1 建立或匯入所需的多網域 (SAN) 憑證。

可以使用可讓您建立憑證授權和密碼的鎖定器服務在 Lifecycle Manager 中建立憑證。或者，您可以使用 CA 伺服器或一些其他機制來產生憑證。

如果您需要新增或建立其他承租人，則必須重新建立並套用您的 vRealize Automation 和 Workspace ONE Access 承租人。

建立憑證後，您可以使用生命週期作業功能在 Lifecycle Manager 中套用這些憑證。您必須選取環境和產品，然後在右側功能表中選取 [取代憑證] 選項。然後，您可以選取產品。取代憑證時，必須在環境中重新信任所有相關聯的產品。

您必須等待套用憑證並重新啟動所有服務，然後再繼續進行下一步。

如需詳細資料，請參閱[管理單一節點多組織部署下的憑證和 DNS 組態](#)和[管理叢集化 vRealize Automation 部署下的憑證和 DNS 組態](#)。

3 在 Workspace ONE Access 執行個體或叢集上套用 Workspace ONE SAN 憑證。

4 在 vRealize Suite Lifecycle Manager 8.1 中，執行 [啟用租戶] 精靈以啟用多租戶，並為預設主要承租人建立別名。

啟用租戶時需要您為提供者組織主要承租人或預設承租人建立別名。啟用租戶後，您可以透過主要承租人 FQDN 存取 Workspace ONE Access。

例如，如果現有 Workspace ONE Access FQDN 為 `idm.example.local` 並且您建立了預設承租人的別名，則在啟用租戶後，Workspace ONE Access FQDN 會變更為 `default-tenant.example.local`，並且與 Workspace ONE Access 通訊的所有用戶端現在會透過 `default-tenant.example.local` 進行通訊。

5 在 vRealize Automation 執行個體或叢集上套用 vRealize Automation SAN 憑證。

您可以透過 Lifecycle Manager 生命週期作業服務來套用 SAN 憑證。您需要檢視環境的詳細資料，然後在右側功能表中選取 [取代憑證]。您必須等待憑證取代工作完成後再新增承租人。在憑證取代過程中，vRealize Automation 服務將會重新啟動。

6 在 Lifecycle Manager 中，執行 [新增承租人] 精靈以設定所需的承租人。

您可以使用位於 [身分識別和承租人管理] 下的 [Lifecycle Manager 承租人管理] 頁面來新增承租人。您只能新增先前已設定憑證和 DNS 設定的承租人。

建立承租人時，您必須指定承租人管理員，並且可以為此承租人選取 Active Directory 連線。可用的連線是基於預設或主要承租人中設定的連線。還必須選取將與承租人相關聯的產品或產品執行個體。

後續步驟

建立承租人後，您可以使用位於 [身分識別和承租人管理] 下的 [Lifecycle Manager 承租人管理] 頁面來變更或新增承租人管理員，將 Active Directory 目錄新增至承租人，以及為承租人變更產品關聯。

您也可以登入 Workspace ONE Access 執行個體，以檢視和驗證您的承租人組態。

管理單一節點多組織部署下的憑證和 DNS 組態

多組織租戶 vRealize Automation 組態依賴於數個產品之間的協調組態，您必須確保已正確設定 DNS 設定和憑證，多組織租戶組態才能正常運作。

此多組織組態假設下列元件採用單一節點部署：

- Lifecycle Manager
- Workspace ONE Access Identity Manager
- vRealize Automation

此外，假設您從預設承租人 (即提供者組織) 開始，然後建立兩個子承租人，稱為 **tenant-1** 和 **tenant-2**。

可以在 vRealize Suite Lifecycle Manager 中使用鎖定器服務建立和套用憑證，也可以使用其他機制。還可以透過 Lifecycle Manager 在 vRealize Automation 或 Workspace ONE Access 上取代或重新信任憑證。

DNS 需求

必須針對系統元件建立主要 A 類型記錄和 CNAME 類型記錄，如下所述。

- 針對每個系統元件以及將在啟用多租戶時建立的每個承租人同時建立兩個主要 A 類型記錄。
- 針對將要建立的每個承租人以及主要承租人建立多租戶 A 類型記錄。
- 針對將建立的每個承租人 (不包括主要承租人) 建立多租戶 CNAME 類型記錄。

單一節點多租戶部署的憑證需求

必須建立兩個主體別名 (SAN) 憑證，一個用於 Workspace ONE Access，一個用於 vRealize Automation。

- vRealize Automation 憑證會列出 vRealize Automation 伺服器的主機名稱以及您將建立之承租人的名稱。
- Workspace ONE Access 憑證會列出 Workspace ONE Access 伺服器的主機名稱以及您要建立的承租人名稱。
- 如果您使用專用 SAN 名稱，則在新增或刪除主機或變更主機名稱時，必須手動更新憑證。您還必須更新承租人的 DNS 項目。作為簡化組態的選項，您可以對 Workspace ONE Access 和 vRealize Automation 憑證使用萬用字元。例如，`*.example.com` 和 `*.vra.example.com`。

備註 vRealize Automation 8.x 僅對與公用尾碼清單 (網址為 <https://publicsuffix.org>) 中與規格相符的 DNS 名稱支援萬用字元憑證。例如，`*.myorg.com` 是有效的名稱，而 `*.myorg.local` 無效。

請注意，Lifecycle Manager 不會為每個承租人建立單獨的憑證。相反，它會使用列出的每個承租人主機名稱建立單一憑證。對於基本組態，承租人的 CNAME 使用下列格式：

`tenantname.vrahostname.domain`。對於高可用性組態，名稱使用下列格式：

`tenantname.vraLBhostname.domain`。

摘要

下表概述了單一節點 Workspace ONE Access 和單一節點 vRealize Automation 部署的 DNS 和憑證需求。

DNS 需求	SAN 憑證需求
Main A Type Records lcm.example.local WorkspaceOne.example.local vra.example.local	Workspace One Certificate 主機名稱： WorkspaceOne.example.local、default-tenant.example.local、 tenant-1.vra.example.local、tenant-2.vra.example.local
Multi-tenancy A Type Records default-tenant.example.local tenant-1.example.local tenant-2.example.local	
Multi-Tenancy CNAME Type Records tenant-1.vra.example.local tenant-2.vra.example.local	vRealize Automation Certificate 主機名稱： vra.example.local、tenant-1.vra.example.local、tenant-2.vra.example.local

管理叢集化 vRealize Automation 部署下的憑證和 DNS 組態

您必須協調所有適用元件之間的憑證和 DNS 組態，才能設定多組織叢集化 vRealize Automation 部署。

在典型的叢集化組態中，有三個 Workspace ONE Access 應用裝置和三個 vRealize Automation 應用裝置以及單一 Lifecycle Manager 應用裝置。

此組態假設下列元件採用叢集化部署：

- Workspace ONE Access Identity Manager 應用裝置：
 - idm1.example.local
 - idm2.example.local
 - idm3.example.local
 - idm-lb.example.local
- vRealize Automation 應用裝置：
 - vra1.example.local
 - vra2.example.local
 - vra3.example.local
 - vra-lb.example.local
- Lifecycle Manager 應用裝置

DNS 需求

必須針對每個元件以及將在啟用多租戶時建立的每個承租人建立主要 A 類型記錄。此外，還必須針對將建立的每個承租人 (不包括主要承租人) 建立多租戶 CNAME 類型記錄。最後，還必須為 Workspace ONE Access 和 vRealize Automation 負載平衡器建立主要 A 類型記錄。

- 針對三個 Workspace ONE Access 應用裝置以及指向其各自 FQDN 的 vRealize Automation 應用裝置建立 A 類型記錄。
- 此外，針對 Workspace ONE Access 負載平衡器以及指向其各自 FQDN 的 vRealize Automation 負載平衡器建立 A 類型記錄。
- 針對預設承租人以及指向 Workspace ONE Access 負載平衡器之 IP 位址的 tenant-1 和 tenant-2 建立多租戶 A 類型記錄。
- 針對指向 vRealize Automation 負載平衡器之 IP 位址的 tenant-1 和 tenant-2 建立 CNAME 記錄。

主體別名 (SAN) 憑證需求

您必須建立兩個 Workspace ONE Access 憑證，一個套用在叢集應用裝置上，另一個套用在負載平衡器上。此外，請建立一個將套用至 vRealize Automation 應用裝置、您正在建立的承租人 (不包括預設承租人) 以及負載平衡器的憑證。

- 為 Workspace ONE Access 應用裝置建立憑證，其中列出 Workspace ONE Access 應用裝置的 FQDN 以及您建立的預設承租人和其他承租人。此憑證應包含 Workspace ONE Access 應用裝置的 IP 位址。
- 最佳做法是在負載平衡器上建立 SSL 終止。若要支援此終止，請為 Workspace ONE Access 負載平衡器建立憑證，其中列出 Workspace ONE Access 負載平衡器的 FQDN 以及您建立的預設承租人和所有其他承租人。此憑證應包含負載平衡器的 IP 位址。
- 您必須為 vRealize Automation 建立憑證，其中列出三個 vRealize Automation 應用裝置的主機名稱、相關負載平衡器以及您要建立的承租人。此外，還應該列出三個 vRealize Automation 應用裝置的 IP 位址。
- 作為簡化組態的選項，您可以對 Workspace ONE Access 和 vRealize Automation 憑證使用萬用字元。例如，*.example.com、*.vra.example.com 和 *.vra-lb.example.com。

備註 vRealize Automation 8.x 僅對與公用尾碼清單 (網址為 <https://publicsuffix.org>) 中與規格相符的 DNS 名稱支援萬用字元憑證。例如，*.myorg.com 是有效的名稱，而 *.myorg.local 無效。

如果您使用的是叢集化 Workspace ONE Access 組態，請注意，Lifecycle Manager 無法更新負載平衡器憑證，因此必須手動進行更新。此外，如果您需要重新登錄 Lifecycle Manager 外部的產品或服務，則這是一種手動程序。

叢集化多組織組態的 DNS 項目和憑證摘要

下表概述了叢集化 Workspace ONE Access 和叢集化 vRealize Automation 多組織部署的 DNS 和憑證需求。

DNS 需求	SAN 憑證需求
Main A Type Records lcm.example.local WorkspaceOne-1.example.local WorkspaceOne-2.example.local WorkspaceOne-3.example.local vra.example-1.local vra.example-2.local vra.example-3.local	Workspace One Certificate 主機名稱: WorkspaceOne.example.local、default-tenant.example.local、tenant-1.example.local、tenant-2.example.local
Multi-Tenancy A Type Records default-tenant.example.local tenant-1.vra.example.local tenant-2.vra.example.local	Workspace One LB Certificate (LB Terminated) 主機名稱: WorkSpaceOne-lb.example.local、default-tenant.example.local、vra.example.local、tenant-1.example.local、tenant-2.example.local
Multi-Tenancy CNAME Type Records tenant-1.vra-lb.example.local - vra-lb.example.local tenant-2.vra-lb.example.local - vra.lb.exmple.local	vRealize Automation Certificate 主機名稱: vra-1.example.local、vra-2.example.local、vra-3.example.local、vra-lb.example.local、tenant-1.example.local、tenant-2.example.local vRealize Automation 負載平衡器上不需要憑證，因為它使用 SSL 傳遞。

登入承租人並在 vRealize Automation 中新增使用者

在 Lifecycle Manager 中為 vRealize Automation 建立承租人之後，您可以登入 Workspace ONE Access 以檢視承租人並新增使用者。

您可以透過登入相關聯的 Workspace ONE Access 執行個體來檢視為 vRealize Automation 部署建立的承租人。要使用的 URL 是 `https://default-tenant name.domainname.local` 或 (對於非叢集化部署) `https://idm.domainname.local`，它會將您引導回預設承租人 Workspace ONE Access URL。

您可以使用下列 URL 來驗證 Workspace ONE Access 中的特定承租人：`https://tenant-1.domainname.local`。此 URL 將開啟一個頁面，其中顯示指定承租人的使用者。您可以按一下**新增使用者**，以隨機建立其他使用者。

已獲得授權的使用者可以使用 `https://vra.domainname.local` 在 vRealize Automation 中登入主要提供者組織。此視圖提供所有 vRealize Automation 相關服務的存取權。

已獲得授權的使用者可以使用 `https://tenantname.vra.domainname.local` 在 vRealize Automation 中登入適用的承租人。

如需有關在 Workspace ONE Access 中管理使用者的詳細資訊，請參閱 <https://docs.vmware.com/tw/VMware-Workspace-ONE-Access/3.3/idm-administrator.pdf>。

新增本機使用者

您可以使用相關聯的 Workspace ONE Access 執行個體，將本機使用者新增至您的部署。本機使用者是不會儲存在任何外部身分識別提供者中的使用者。

將 vRealize Orchestrator 與 vRealize Automation 多組織部署 搭配使用

您可以將 vRealize Orchestrator 與 vRealize Automation 多組織租戶部署搭配使用。

預設承租人支援與可立即使用的內嵌式 vRealize Orchestrator 整合進行整合。vRealize Orchestrator 可在 [整合] 頁面上預先設定。子承租人沒有任何預先登錄的 vRealize Orchestrator 整合。他們有數個選項可用於新增 vRealize Orchestrator 整合。

- 可以透過導覽至 vRealize Orchestrator 中的 [設定驗證提供者] 並使用適用 vRealize Automation 承租人的主機位址進行連線，來新增與內嵌式 vRealize Orchestrator 的整合。然後，他們可以選取**基礎結構 > 連線 > 整合**並將內嵌式 vRO 新增為整合。
- 他們可以新增外部 vRealize Orchestrator 執行個體，該執行個體使用多組織 vRealize Automation 作為驗證提供者。

可以透過建立新整合並提供 vRealize Orchestrator FQDN (而不提供任何認證)，向任何承租人登錄使用 vRealize Automation 多組織部署作為驗證提供者的任何 vRealize Orchestrator 執行個體。

在 vRealize Automation 中使用記錄

5

您可以使用提供的 `vraccli` 命令列公用程式，在 vRealize Automation 中建立和使用記錄。

您可以直接在 vRealize Automation 中使用記錄，也可以改為將所有記錄轉送到 vRealize Log Insight。

本章節討論下列主題：

- [如何在 vRealize Automation 中使用記錄和記錄服務包](#)
- [如何設定將記錄轉送到 vRealize Log Insight](#)
- [如何在 vRealize Automation 中建立或更新 Syslog 整合](#)

如何在 vRealize Automation 中使用記錄和記錄服務包

您可以在 vRealize Automation 中建立和使用 vRealize Automation 記錄和記錄服務包。

也可以自動將記錄轉送到 vRealize Log Insight。如需如何將記錄轉送到 vRealize Log Insight 的相關資訊，請參閱[如何設定將記錄轉送到 vRealize Log Insight](#)。

有關如何使用 `vraccli` 命令列公用程式的資訊，可透過在 `vraccli` 命令列中使用 `--help` 引數取得。例如：
`vraccli log-bundle --help`。

記錄服務包命令

您可以建立簡單的記錄服務包或所有服務的彙總 (冷儲存) 記錄。雖然這兩個記錄服務包都包含服務的所有記錄，但冷儲存服務包將包含服務記錄後援版本的彙總串流複本，具有更大的疑難排解價值。冷儲存代理程式會持續彙總來自服務的記錄，並將其儲存在本機檔案系統上。疑難排解通常只需要一個簡單的記錄服務包。

您也可以變更從每個節點收集記錄的預設逾時值。

在叢集環境中，您只需要在一個節點上執行 `vraccli log-bundle` 命令。

- 顯示記錄服務包命令說明：
`vraccli log-bundle --help`
- 建立簡單的記錄服務包。
`vraccli log-bundle`
- 建立冷儲存記錄服務包：

```
vracli log-bundle --include-cold-storage
```

- 變更從每個節點收集記錄的逾時值。例如，如果您的環境包含較大的記錄檔、網路速度緩慢、CPU 使用率過高等，則可能需要將逾時設定為大於 1000 秒預設值。

```
vracli log-bundle --collector-timeout $CUSTOM_TIMEOUT_IN_SECONDS
```

記錄服務包結構

vRealize Automation 服務將在 Kubernetes 網繭中進行容器化。產生的記錄服務包是使用 `log-bundle-{{TIMESTAMP}}.tar.xz` 名稱格式的 `tar.xz` 封存檔，其中 `TIMESTAMP` 是 epoch 時間戳記 (以秒為單位)。一般記錄服務包包含環境中所有節點的記錄。如果由於任何原因而無法產生記錄服務包，則會改為建立後援服務包。後援服務包僅包含目前節點的記錄。兩個記錄服務包類型的結構略有差異。

- 一般記錄服務包

一般記錄服務包將分成下列類別：

- 主機記錄和組態

將在一個目錄中按叢集節點 (主機) 收集每個主機的組態及其主機特定的記錄。目錄名稱與節點主機名稱相符。目錄內容與主機檔案系統相符。目錄數目與叢集節點數目相符。

冷儲存記錄位於結構化 JSON 記錄中，即 `/hostname/services-logs/all/aggregated.log`。

- 網繭記錄

服務將在 Kubernetes 網繭中進行容器化。服務記錄位於 `pods` 目錄中，其中包含每個命名空間的單一目錄，且檔案名稱與命名空間名稱相符。每個叢集節點的每個網繭通常有一個執行個體。網繭目錄包含其各個容器應用程式的記錄檔。

例如，vRealize Orchestrator 控制中心記錄位於每個 `/pods/prelude/vco-app-hash/` 目錄的 `vco-controlcenter-app.log` 檔案中。

- 環境檔案

環境檔案包含每個節點和每個網繭的目前資源使用量的相關資訊。此外，還包含所有可用 Kubernetes 實體的叢集資訊和說明。

- 後援記錄服務包

如果您在等待 `vracli` 命令完成時收到錯誤訊息，則會產生後援服務包。如果收到此錯誤，您應在叢集中的每個主機或節點上執行 `vracli log-bundle` 命令，以收集盡可能多的資訊。

- 後援容器記錄

後援記錄位於 `/fallback-containers` 目錄中。您可以檢查記錄檔的名稱，以識別網繭產生記錄所在的容器：

```
pod-name-some-hash-container-name-other-hash.log
```

- 後援冷儲存

如果您要使用服務包收集冷儲存記錄，則目前主機中的後援記錄位於 `/fallback-cold-storage` 目錄中。

如何設定將記錄轉送到 vRealize Log Insight

您可以將記錄從 vRealize Automation 轉送到 vRealize Log Insight，以充分利用更強大的記錄分析和報告產生功能。

vRealize Automation 與基於 [fluentd](#) 的記錄代理程式綁定。代理程式會收集並儲存記錄，以便將其包含在記錄服務包中並稍後進行檢查。您可以將代理程式設定為使用 vRealize Log Insight API 將記錄複本轉送到 vRealize Log Insight 伺服器。提供的 API 允許其他程式與 vRealize Log Insight 進行通訊。

如需有關 vRealize Log Insight 的詳細資訊，包括 vRealize Log Insight API 的說明文件，請參閱 [vRealize Log Insight 說明文件](#) 以及 [/api/v1/events/ingest/{agentId}](#) 頁面。

將記錄代理程式設定為使用提供的 `vraccli` 命令列公用程式，自動並持續將 vRealize Automation 記錄轉送到 vRealize Log Insight。

所有記錄行會以主機名稱和環境標籤進行標記，並且可在 vRealize Log Insight 中進行檢查。在高可用性 (HA) 環境中，記錄會以不同的主機名稱進行標記，具體取決於其來源節點。如〈設定或更新 vRealize Log Insight 的整合〉一節中所述，環境標籤可使用 `--environment ENV` 選項進行設定。在 HA 環境中，無論其來源節點為何，環境標籤的所有記錄行都具有相同的值。

有關如何使用 `vraccli` 命令列公用程式的資訊，可透過在 `vraccli` 命令列中使用 `--help` 引數取得。例如：
`vraccli vrli --help`。

檢查 vRealize Log Insight 的現有組態

Command

```
vraccli vrli
```

Arguments

沒有命令列引數。

Output

vRealize Log Insight 整合的目前組態以 JSON 格式輸出。

Exit codes

以下是可能的結束代碼：

- 0 - 已設定與 vRealize Log Insight 的整合。
- 1 - 命令執行過程中發生例外狀況。如需詳細資料，請查看錯誤訊息。
- 61 (ENODATA) - 未設定與 vRealize Log Insight 的整合。如需詳細資料，請查看錯誤訊息。

Example – check integration configuration

```
$ vraccli vrli
No vRLI integration configured

$ vraccli vrli
{
  "agentId": "0",
```



```

    "environment": "prod",
    "host": "my-vrli.local",
    "port": 443,
    "scheme": "https",
    "sslVerify": false
}

```

備註 您可以設定不同的主機配置 (預設為 https) 和連接埠 (預設為 443) 以用於傳送記錄，如下列範例所示：

```

vracli vrli set some-host
vracli vrli set some-host:9543
vracli vrli set http://some-host:9543

```

vRealize Log Insight 擷取 API 將會使用連接埠 9543，如 [vRealize Log Insight 說明文件](#) 中《管理 vRealize Log Insight》中的〈連接埠和外部介面〉主題所述。

設定或更新 vRealize Log Insight 的整合

Command

```
vracli vrli set [options] FQDN_OR_URL
```

Arguments

可用命令列引數如下：

- FQDN_OR_URL - vRealize Log Insight 伺服器的 FQDN 或 IP 位址，用於透過 vRealize Log Insight API 組態發佈記錄。預設使用連接埠 443 和 HTTPS 配置。若必須變更其中任何設定，您可以改為使用 URL。
- 選項
 - **--agent-id SOME_ID** - 針對此應用裝置設定記錄代理程式的識別碼。預設值為 0。用於針對使用 vRealize Log Insight API 組態發佈到 vRealize Log Insight 的記錄識別記錄代理程式。
 - **--environment ENV** - 設定目前環境的識別碼。將在 vRealize Log Insight 記錄中做為每個記錄行事件的標籤提供。預設值為 prod。
 - **--ca-file /path/to/server-ca.crt** - 指定包含用於簽署 vRealize Log Insight 伺服器憑證之憑證授權機構 (CA) 憑證的檔案。強制記錄代理程式信任指定的 CA，並啟用它來驗證 vRealize Log Insight 伺服器的憑證。此檔案可在必要時包含整個憑證鏈結以驗證憑證。如果是自我簽署憑證，將傳遞憑證本身。
 - **--ca-cert CA_CERT** - 以與 **--ca-file** 相同的方式指定檔案，但以字串形式內嵌傳遞憑證 (鏈結)。
 - **--insecure** - 停用伺服器憑證的 SSL 驗證。在發佈記錄時強制記錄代理程式接受任何 SSL 憑證。

Output

預期沒有輸出。

Exit codes

以下是可能的結束代碼：

- 0 - 組態已更新。
- 1 - 執行過程中發生例外狀況。如需詳細資料，請查看錯誤訊息。

Examples – Configure or update integration configuration

```
$ vracli vrli set my-vrli.local
$ vracli vrli set 10.20.30.40

$ vracli vrli set --ca-file /etc/ssl/certs/ca.crt 10.20.30.40

$ vracli vrli set --ca-cert "$(cat /etc/ssl/certs/ca.crt)" 10.20.30.40

$ vracli vrli set --insecure http://my-vrli.local:8080

$ vracli vrli set --agent-id my-vrli-agent my-vrli.local

$ vracli vrli set --environment staging my-vrli.local
```

清除 vRealize Log Insight 的整合

Command

```
vracli vrli unset
```

Arguments

沒有命令列引數。

Output

以純文字格式輸出確認。

Exit codes

以下是可能的結束代碼：

- 0 - 組態已清除或不存在任何組態。
- 1 - 執行過程中發生例外狀況。如需詳細資料，請查看錯誤訊息。

Examples – Clear integration

```
$ vracli vrli unset
Clearing vRLI integration configuration

$ vracli vrli unset
No vRLI integration configured
```

如何在 vRealize Automation 中建立或更新 Syslog 整合

您可以設定 vRealize Automation 以將記錄資訊傳送至遠端 Syslog 伺服器。

`vracli remote-syslog set` 命令可用來建立 Syslog 整合或覆寫現有整合。

vRealize Automation 遠端 Syslog 整合支援下列連線類型：

- 透過 UDP。
- 透過 TCP，且不使用 TLS。

備註 若要在不使用 TLS 的情況下建立 Syslog 整合，請將 `--disable-ssl` 旗標新增至 `vracli remote-syslog set` 命令。

- 透過 TCP，且使用 TLS。

如需設定與 vRealize Log Insight 的記錄整合的相關資訊，請參閱[如何設定將記錄轉送到 vRealize Log Insight](#)。

必要條件

設定一或多個遠端 Syslog 伺服器。

程序

- 1 以根使用者身分登入 vRealize Automation 應用裝置命令列。
- 2 若要建立與 Syslog 伺服器的整合，請執行 `vracli remote-syslog set` 命令。

```
vracli remote-syslog set -id name_of_integration protocol_type://syslog_URL_or_FQDN:syslog_port
```

備註 如果您未在 `vracli remote-syslog set` 命令中輸入連接埠，則連接埠值預設為 514。

備註 您可以將憑證新增至 Syslog 組態。若要新增憑證檔案，請使用 `--ca-file` 旗標。若要將憑證新增為純文字，請使用 `--ca-cert` 旗標。

- 3 (選擇性) 若要覆寫現有的 Syslog 整合，請執行 `vracli remote-syslog set`，並將 `-id` 旗標值設定為您想要覆寫的整合的名稱。

備註 依預設，vRealize Automation 應用裝置會要求您確認要覆寫 Syslog 整合。若要略過確認要求，請將 `-f` 或 `--force` 旗標新增至 `vracli remote-syslog set` 命令。

後續步驟

若要在應用裝置中檢閱目前的 Syslog 整合，請執行 `vracli remote-syslog` 命令。

如何在 vRealize Automation 中刪除用於記錄的 Syslog 整合

您可以透過執行 `vracli remote-syslog unset` 命令，從 vRealize Automation 應用裝置刪除 Syslog 整合。

必要條件

在 vRealize Automation 應用裝置中建立一或多個 Syslog 整合。請參閱[如何在 vRealize Automation 中建立或更新 Syslog 整合](#)。

程序

- 1 以根使用者身分登入 vRealize Automation 應用裝置命令列。
- 2 使用下列其中一種方法，從 vRealize Automation 應用裝置刪除 Syslog 整合：
 - 若要刪除特定的 Syslog 整合，請執行 `vracli remote-syslog unset -id Integration_name` 命令。
 - 若要刪除 vRealize Automation 應用裝置上的所有 Syslog 整合，請執行不含 `-id` 旗標的 `vracli remote-syslog unset` 命令。

備註 依預設，vRealize Automation 應用裝置會要求您確認要刪除所有 Syslog 整合。若要略過確認要求，請將 `-f` 或 `--force` 旗標新增至 `vracli remote-syslog unset` 命令。

參與 vRealize Automation 的客戶經驗改進計劃

6

此產品參與了 VMware 客戶經驗改進計劃 (CEIP)。CEIP 為 VMware 提供能讓其改進產品與服務、修正問題的資訊，並就如何以最佳方式部署和使用我們的產品為您提供建議。

有關透過 CEIP 收集之資料以及 VMware 使用此資料之目的的詳細資料，請詳見信任與保證中心，網址為：<http://www.vmware.com/trustvmware/ceip.html>。

本章節討論下列主題：

- 如何加入或退出 vRealize Automation 的客戶經驗改進計劃
- 如何設定 vRealize Automation 客戶經驗改進計劃的資料收集時間

如何加入或退出 vRealize Automation 的客戶經驗改進計劃

透過 vRealize Automation 應用裝置命令列加入或退出客戶經驗改進計劃 (CEIP)。

當您使用 vRealize Lifecycle Manager (LCM) 安裝 vRealize Automation 時，您可以加入 CEIP 計劃。您也可以安裝後使用命令列選項，加入或退出計劃。

使用命令列選項加入客戶經驗改進計劃：

- 1 以根使用者身分登入 vRealize Automation 應用裝置命令列。
- 2 執行 `vracli ceip on` 命令。
- 3 檢閱客戶經驗改進計劃資訊，並執行 `vracli ceip on --acknowledge-ceip` 命令。
- 4 若要重新啟動 vRealize Automation 服務，請執行 `/opt/scripts/deploy.sh` 命令。

使用命令列選項退出客戶經驗改進計劃：

- 1 以根使用者身分登入 vRealize Automation 應用裝置命令列。
- 2 執行 `vracli ceip off` 命令。
- 3 若要重新啟動 vRealize Automation 服務，請執行 `/opt/scripts/deploy.sh` 命令。

如何設定 vRealize Automation 客戶經驗改進計劃的資料收集時間

您可以設定客戶經驗改進計劃 (CEIP) 傳送資料給 VMware 的日期和時間。

程序

1 以根使用者身分登入 vRealize Automation 應用裝置命令列。

2 在文字編輯器中開啟下列檔案。

```
/etc/telemetry/telemetry-collector-vami.properties
```

3 針對星期幾 (dow) 和一天的某時 (hod) 編輯內容。

內容	說明
<code>frequency.dow=<day-of-week></code>	資料收集於星期幾發生。
<code>frequency.hod=<hour-of-day></code>	資料收集發生的一天中的當地時間。可能的值為 0-23。

4 儲存並關閉 `telemetry-collector-vami.properties`。

5 透過輸入以下命令來套用設定。

```
vcac-config telemetry-config-update --update-info
```

變更將套用至部署中的所有節點。