vCloud Director 服務提供者管理入口網站指南

2019 年 3 月 28 日

VMware Cloud Director 9.7

vmware®

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

目錄

關於 vCloud Director Service Provider Admin Portal

1

《vCloud Director Service Provider Admin Portal 指南》提供有關如何使用 Service Provider Admin Portal 的資訊。您可以使用 service provider admin portal 管理和監控雲端中的組織、權限、角色、使用者和群組。此外，也可以建立和管理 NSX-T 支援的組織虛擬資料中心網路。

主要對象

本指南適用於想要使用 vCloud Director Service Provider Admin Portal 所提供功能的服務提供者管理員。

相關說明文件

如需使用 vCloud Director Web 主控台 (而非 vCloud Directorservice provider admin portal) 的組織管理員可使用的特性和功能的相關資訊，請參閱《vCloud Director 管理員指南》。

VMware Technical Publications Glossary

VMware 技術出版品提供您可能不熟悉的專有詞彙表。如需 VMware 技術說明文件中所用專有詞彙的定義，請前往 https://docs.vmware.com。

更新資訊

本《vCloud Director Service Provider Admin Portal 指南》隨產品的每個版本更新或在必要時進行更新。

下表提供了《vCloud Director Service Provider Admin Portal 指南》的更新歷程記錄。

修訂版	描述
2019 年 4 月 05 日	改善了瞭解配置模型和瞭解運算原則章節中的資訊。
2019 年 3 月 28 日	初始版本。

vCloud Director Service Provider Admin Portal 入門

2

vCloud Director Service Provider Admin Portal 是服務提供者管理員的專用介面。

本章節討論下列主題：

- vCloud Director 管理的概觀
- 登入 vCloud Director Service Provider Admin Portal。
- 檢視工作
- 停止正在進行中的工作
- 檢視事件

vCloud Director 管理的概觀

藉由 VMware vCloud Director，您可以透過將虛擬基礎結構資源集中到虛擬資料中心，並透過網頁型入口網站與程式化介面以目錄型式的全自動服務讓使用者使用，建立安全的多承租人雲端。

《vCloud Director 管理員指南》提供有關新增資源至系統、建立並佈建組織、管理資源與組織以及監控系統的資訊。

vSphere 和 NSX 資源

vCloud Director 依賴 vSphere 資源來提供用於執行虛擬機器的 CPU 與記憶體。此外，vSphere 資料存放區可儲存虛擬機器檔案及虛擬機器運作所需的其他檔案。vCloud Director 也使用 vSphere Distributed Switch、vSphere 連接埠群組和 NSX Data Center for vSphere 來支援虛擬機器網路。

vCloud Director 也可以使用 NSX-T Data Center 中的資源。如需向雲端登錄 NSX-T Manager 執行個體的相關資訊，請參閱《vCloud Director Service Provider Admin Portal 指南》或《服務提供者適用的 vCloud API 程式設計指南》。

您可以使用基礎的 vSphere 和 NSX 資源以建立雲端資源。

從 9.7 版開始，vCloud Director 可用作 HTTP Proxy 伺服器，藉此可以讓組織能夠存取基礎 vSphere 環境。

雲端資源

雲端資源是其基礎 vSphere 資源的抽象概念。它們為 vCloud Director 虛擬機器與 vApp 提供計算與記憶體資源。vApp 是包含一或多個個別的虛擬機器，以及定義操作詳細資料之參數的虛擬系統。雲端資源也可存取儲存與網路連線性。

雲端資源包含提供者與組織虛擬資料中心、外部網路、組織虛擬資料中心網路，以及網路集區。此外，vCloud Director 9.7 還採用軟體定義資料中心 (SDDC) 和 SDDC Proxy 做為雲端資源，以便從 vCloud Director 存取基礎 vSphere 環境。

您必須先新增 vSphere 資源，才能將雲端資源新增至 vCloud Director。

SDDC 和 SDDC Proxy

vCloud Director 9.7 採用 SDDC 做為封裝整個 vCenter Server 安裝的雲端資源。一個 SDDC 包含一或多個 SDDC Proxy，這些 Proxy 是基礎 vSphere 環境中不同元件的存取點。提供者可以建立並啟用 SDDC 和 Proxy。提供者可以向承租人發佈 SDDC 及其 Proxy。

若要建立並管理 SDDC 和 Proxy，您必須使用 vCloud OpenAPI。請參閱《vCloud OpenAPI 入門》，網址為：https://code.vmware.com。

提供者虛擬資料中心

提供者虛擬資料中心結合了單一 vCenter Server 資源集區的計算與記憶體資源，以及可供該資源集區使用的一或多個資料存放區的儲存資源。

提供者虛擬資料中心可以使用與 vCenter Server 執行個體相關聯的 NSX Manager 執行個體中的網路資源，也可以使用向雲端登錄的 NSX-T Manager 執行個體中的網路資源。

您可以建立多個提供者虛擬資料中心供不同地理位置或業務單位的使用者使用，或是供有不同效能需求的使用者使用。

組織虛擬資料中心

組織虛擬資料中心為組織提供資源，而且是分割自提供者虛擬資料中心。組織虛擬資料中心提供的環境可儲存、部署以及操作虛擬系統。也為虛擬機器提供如軟碟與 CD ROM 等儲存。

一個組織可以有多個組織虛擬資料中心。

vCloud Director 網路

vCloud Director 支援三種網路類型。

- 外部網路
- 組織虛擬資料中心網路
- vApp 網路

部分組織虛擬資料中心網路與所有 vApp 網路均由網路集區提供支援。

外部網路

外部網路是依據 vSphere 連接埠群組的邏輯、差異化網路。組織虛擬資料中心網路可連線至外部網路，以便為 vApp 內的虛擬機器提供網際網路連線。

從 9.5 版開始，vCloud Director 支援 IPv6 外部網路。IPv6 外部網路支援 IPv4 和 IPv6 子網路，且 IPv4 外部網路支援 IPv4 和 IPv6 子網路。

依預設，只有**系統管理員**可以建立與管理外部網路。

組織虛擬資料中心網路

組織虛擬資料中心網路屬於 vCloud Director 組織虛擬資料中心，且可供組織內的所有 vApp 使用。組織虛擬資料中心網路可讓組織內的 vApp 彼此通訊。若要提供外部連線，您可以將組織虛擬資料中心網路連線至外部網路。您也可以建立組織內部的隔離組織虛擬資料中心網路。

vCloud Director 9.5 採用了對直接和路由的組織虛擬資料中心網路的 IPv6 支援。

從 vCloud Director 9.5 開始，**系統管理員**可以建立受 NSX-T 邏輯交換器支援的隔離虛擬資料中心網路。**組織管理員**可以建立受網路集區支援的隔離虛擬資料中心網路。

vCloud Director 9.5 還採用了跨虛擬資料中心的網路，方法是在虛擬資料中心群組中設定延伸網路。

依預設，只有**系統管理員**可以建立直接和跨虛擬資料中心的網路。即使**組織管理員**可執行的動作存在一些限制，**系統管理員**與**組織管理員**仍可以管理組織虛擬資料中心網路。

vApp 網路

vApp 網路屬於 vApp，而且允許 vApp 內的虛擬機器彼此通訊。若要讓 vApp 能夠與組織內的其他 vApp 進行通訊，您可以將 vApp 網路連線至組織虛擬資料中心網路。如果組織虛擬資料中心網路連線至外部網路，vApp 可與其他組織中的 vApp 進行通訊。vApp 網路由網路集區提供支援。

大多數可存取 vApp 的使用者可以建立並管理專屬的 vApp 網路。如需使用 vApp 中的網路的相關資訊，請參閱《vCloud Director 租用戶入口網站指南》。

網路集區

網路集區是組織虛擬資料中心內可供使用的非差異化網路群組。網路集區受 vSphere 網路資源 (例如 VLAN 識別碼或連接埠群組) 支援。vCloud Director 使用網路集區建立 NAT 路由的和內部組織虛擬資料中心的網路以及所有 vApp 網路。集區內每個網路上的網路流量會從所有其他網路隔離在第 2 層。

vCloud Director 中的每個組織虛擬資料中心可以擁有一個網路集區。多個組織虛擬資料中心可共用一個網路集區。組織虛擬資料中心的網路集區可提供為滿足組織虛擬資料中心的網路配額而建立的網路。

只有**系統管理員**可以建立與管理網路集區。

組織

vCloud Director 透過使用組織來支援多租戶。組織是使用者、群組以及計算資源集合的管理單元。使用者於組織層級驗證，並在建立或匯入使用者時，提供由組織管理員建立的認證。**系統管理員**建立並佈建組織，而**組織管理員**則管理組織使用者、群組以及目錄。**組織管理員**工作會在《vCloud Director 租用戶入口網站指南》中加以說明。

使用者與群組

組織可包含任意的使用者與群組數。**組織管理員**可以建立使用者，並從 LDAP 等目錄服務匯入使用者和群組。**系統管理員**可以管理每個組織可用的權限集。**系統管理員**可以建立全域承租人角色並將其發佈到一或多個組織。**組織管理員**可以在其組織中建立本機角色。

目錄

組織使用目錄以儲存 vApp 範本與媒體檔案。可存取目錄的組織成員可以使用內含的 vApp 範本與媒體檔案來建立其專屬 vApp。**系統管理員**允許組織發佈目錄以供其他組織使用。然後，**組織管理員**可決定為其使用者提供哪些目錄項目。

登入 vCloud Director Service Provider Admin Portal。

您可以使用網頁瀏覽器來存取 vCloud DirectorService Provider Admin Portal。

必要條件

您必須擁有系統管理員權限才能存取 vCloud Director Service Provider Admin Portal。

程序

1. 在瀏覽器中，輸入 vCloud Director 站台的 Service Provider Admin Portal URL，並按 Enter 鍵。

   例如，輸入 **`https://vcloud.example.com/provider`**。
2. 使用系統管理員使用者名稱和密碼登入。

檢視工作

您可以從 Service Provider Admin Portal 檢視最近的工作及其狀態。

工作視圖很適合用來快速檢視服務提供者管理員入口網站中的工作狀態。該視圖會顯示執行工作的時間以及執行是否成功。對環境中的任何問題進行疑難排解時，先使用此工具是很好的辦法。

[工作] 圖示上方的藍色與紅色資訊提示分別顯示已執行及失敗的工作數目。

程序

- 從右上方功能表中，選取 [工作] 圖示 ()。

結果

最近的工作清單即會顯示，還會顯示執行工作的時間和工作狀態。

停止正在進行中的工作

如果在套用或檢閱所有必要設定之前不小心啟動了作業，您可以停止正在進行中的工作。

依預設，**最近的工作**面板顯示在入口網站的底部。啟動作業時，例如建立虛擬機器，該工作會顯示在此面板中。

必要條件

最近的工作面板必須處於開啟狀態。

程序

1 啟動長時間執行的作業。

長時間執行的作業包括建立虛擬機器或 vApp、在虛擬機器和 vApp 上執行的電源作業等。

2 在**最近的工作**面板中，按一下**取消**圖示 ( )。

3 在**取消工作**對話方塊中，按一下**確定**確認取消工作。

結果

此作業將停止。

檢視事件

從入口網站中，您可以檢視所有事件的清單及其詳細資料和狀態。

事件視圖是一種在入口網站中檢視事件狀態的方式。該視圖會顯示事件發生的時間以及事件是否成功。事件視圖中包含一次性事件，例如使用者登入和物件建立或刪除。

程序

1 從主功能表 ( ) 中，選取**事件**。

將顯示所有事件的清單，以及事件發生的時間和事件狀態。

2 按一下編輯器圖示 ( )，以變更您要檢視的事件的詳細資料。

3 (選擇性) 按一下事件以檢視事件詳細資料。

詳細資料	說明
事件	事件的名稱。 例如，如果您修改 vApp 以在其中包含虛擬機器，則啟動整個作業的事件是 *Task 'Modify vApp' start*。
事件識別碼	工作的識別碼。
類型	在此執行工作的物件。例如，如果您已建立虛擬機器，則類型為 *vm*。
目標	事件的目標物件。 例如，當您修改 vApp 以在其中包含虛擬機器時，*Task 'Modify vApp' start* 事件的目標為 *vdcUpdateVapp*。
狀態	事件的狀態，如 [成功] 或 [失敗]。
服務命名空間	服務名稱，例如 *com.vmware.vcloud*。
組織	組織的名稱。

詳細資料	說明
擁有者	觸發事件的使用者。
發生時間	事件發生的日期和時間。

管理 vSphere 資源

3

vCloud Director 會從基礎的 vSphere 虛擬基礎結構衍生其資源。在 vCloud Director 中登錄 vSphere 資源後，您可以配置這些資源供 vSphere 安裝中的組織使用。

vCloud Director 使用一或多個 vCenter Server 環境來支援其虛擬資料中心。從 9.7 版開始，vCloud Director 也可以使用 vCenter Server 環境封裝具有一或多個 Proxy 的 SDDC。您可以允許承租人將這些 Proxy 用作 vCloud Director 及其 vCloud Director 帳戶的基礎 vSphere 環境的存取點。

必須先連結此 vCenter Server 執行個體，才能在 vCloud Director 中使用 vCenter Server 執行個體。

當您建立由連結的 vCenter Server 執行個體所支援的提供者虛擬資料中心時，此 vCenter Server 執行個體會顯示為已發佈至服務提供者，也稱為已納入提供者範圍。如需建立提供者虛擬資料中心的相關資訊，請參閱《vCloud Director 管理員指南》。

當您建立用於封裝連結的 vCenter Server 執行個體的 SDDC 時，此 vCenter Server 執行個體會顯示為已發佈至承租人，也稱為已納入承租人範圍。如需建立 SDDC 的相關資訊，請參閱第 9 章 管理 SDDC 和 SDDC Proxy。

備註 依預設，使用連結的 vCenter Server 執行個體，您可以建立提供者 VDC 或 SDDC。如果已建立由 vCenter Server 執行個體支援的提供者 VDC，則無法使用此 vCenter Server 執行個體建立 SDDC，反之亦然。您可以使用 vCloud API 修改 vCloud Director 安裝的系統設定，以便 vCenter Server 執行個體可以同時支援提供者 VDC 和 SDDC。

本章節討論下列主題：

- 修改 NSX-T Manager 設定
- 刪除 NSX-T Manager 執行個體
- 多站台資源清單

新增 vCenter Server 和 NSX 資源

vCloud Director 依賴 vSphere 資源來提供用於執行虛擬機器的 CPU、記憶體和儲存區。此外，從 9.7 版開始，vCloud Director 可做為承租人與基礎 vSphere 環境之間的 HTTP 伺服器。

如需 vCloud Director 系統需求以及 vCenter Server 和 ESXi 支援版本的相關資訊，請參閱《VMware 產品互通性對照表》，網址為：http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php。

單獨連結 NSX Manager 執行個體或與 vCenter Server 執行個體連結在一起

連結 vCenter Server 執行個體，以便其資源可在 vCloud Director 中使用。您可以將 vCenter Server 執行個體與其相關聯的 NSX Manager 執行個體連結在一起，也可以單獨連結 vCenter Server 執行個體。

vCloud Director 可以搭配使用 vCenter Server 執行個體及其相關聯的 NSX Manager 執行個體或 NSX-T Manager 執行個體。

如果您希望 vCloud Director 搭配使用此 vCenter Server 執行個體及其相關聯的 NSX Manager 執行個體，您必須將 vCenter Server 和 NSX Manager 連結在一起。

如果您希望 vCloud Director 搭配使用此 vCenter Server 執行個體與 NSX-T Manager 執行個體，必須單獨連結 vCenter Server 執行個體。單獨連結 vCenter Server 執行個體後，您必須登錄 NSX-T Manager 執行個體。

備註 單獨連結 vCenter Server 執行個體後，稍後便無法新增其相關聯的 NSX Manager 執行個體。您可以解除登錄並重新連結 vCenter Server 執行個體及其相關聯的 NSX Manager 執行個體。

您可以將 vCenter Server 執行個體連結至 vCloud Director 環境中的任何站台。

必要條件

- 如果設定了 vCloud Director 以驗證 vCenter 和 vSphere SSO 憑證，請確認您已將 vCenter Server 憑證上傳至 vCloud Director。如需一般系統設定的相關資訊，請參閱《vCloud Director 管理員指南》。
- 如果設定了 vCloud Director 以驗證 NSX Manager 憑證，請確認您已將 NSX Manager 憑證上傳至 vCloud Director。如需一般系統設定的相關資訊，請參閱《vCloud Director 管理員指南》。

程序

1 新增 vCenter Server 執行個體

若要新增 vCenter Server 執行個體，請輸入 vCenter Server 存取詳細資料。

2 (選擇性) 新增相關聯的 NSX Manager 執行個體

如果您希望 vCloud Director 搭配使用此 vCenter Server 執行個體及其相關聯的 NSX Manager 執行個體，您必須新增 NSX Manager 存取詳細資料。

新增 vCenter Server 執行個體

若要新增 vCenter Server 執行個體，請輸入 vCenter Server 存取詳細資料。

程序

1 從主功能表 (☰) 中，選取 **vSphere 資源**。

2 在左窗格中，按一下 **vCenter**，然後按一下**新增**。

3 如果您有多站台 vCloud Director 部署，請從**站台**下拉式功能表中，選取您要向其新增此 vCenter Server 執行個體的站台，然後按**下一步**。

4 輸入 vCloud Director 中 vCenter Server 執行個體的名稱，並選擇性地輸入說明。

5 輸入 vCenter Server 執行個體的 URL。

如果使用預設連接埠，則可以略過連接埠號碼。如果使用自訂連接埠，請包含連接埠號碼

例如，`https://FQDN_or_IP_address:<custom_port_number>`。

6 輸入 vCenter Server **管理員**帳戶的使用者名稱和密碼。

7 (選擇性) 若要在登錄後停用 vCenter Server 執行個體，請關閉**已啟用**切換按鈕。

8 設定 vCenter Server Web Client 的 URL。

選項	描述
使用 vSphere 服務提供 URL	若要使用此選項，您必須使用 vCloud API 將 vCloud Director 設定為使用 vSphere Lookup Service。
vSphere Web Client URL	若要使用此選項，您必須輸入 vSphere Web Client 的 URL。例如，`https://example.vmware.com/vsphere-client`。

9 按**下一步**。

10 (選擇性) 略過新增與 vCenter Server 執行個體相關聯的 NSX Manager 執行個體，並完成登錄。

如果您希望 vCloud Director 搭配使用此 vCenter Server 執行個體與 NSX-T Manager 執行個體，您必須單獨新增 vCenter Server 執行個體。

備註 稍後無法新增相關聯的 NSX Manager 執行個體。您可以解除登錄並重新連結 vCenter Server 執行個體及其相關聯的 NSX Manager 執行個體。

a 在 **NSX-V Manager 設定**頁面上，關閉**設定組態**切換按鈕，然後按**下一步**。

b 在**即將完成**頁面上，檢閱登錄詳細資料並按一下**完成**。

(選擇性) 新增相關聯的 NSX Manager 執行個體

如果您希望 vCloud Director 搭配使用此 vCenter Server 執行個體及其相關聯的 NSX Manager 執行個體，您必須新增 NSX Manager 存取詳細資料。

程序

1 在 **NSX-V Manager 設定**頁面上，將**設定組態**切換按鈕保持開啟。

2 輸入 NSX Manager 執行個體的 URL。

如果使用預設連接埠，則可以略過連接埠號碼。如果使用自訂連接埠，請包含連接埠號碼

例如，**https://*FQDN_or_IP_address*:*<custom_port_number>***。

3 輸入 NSX **管理員**帳戶的使用者名稱和密碼。

4 (選擇性) 若要針對此 vCenter Server 執行個體支援的虛擬資料中心啟用跨虛擬資料中心網路，請開啟**跨 VDC 網路**切換按鈕，並輸入控制虛擬機器部署內容和網路提供者範圍的名稱。

控制虛擬機器部署內容用於在 NSX Manager 執行個體上部署可用於跨虛擬資料中心網路元件 (例如通用路由器) 的應用裝置。

選項	描述
資源集區路徑	vCenter Server 執行個體中特定資源集區的階層路徑，以叢集開頭，*Cluster/Resource_Pool_Parent/Target_Resource*。例如，**TestbedCluster1/mgmt-rp**。 或者，您可以輸入資源集區的受管理的物件參考識別碼。例如，**resgroup-1476**。
資料存放區名稱	用於主控應用裝置檔案的資料存放區的名稱。例如，**shared-disk-1**。
管理介面	用於 HA DLR 管理介面的 vCenter Server 中的網路或連接埠群組的名稱。例如，**TestbedPG1**。
網路提供者範圍	對應於資料中心群組之網路拓撲中的網路容錯網域。例如，**boston-fault1**。 如需管理跨虛擬資料中心群組的相關資訊，請參閱《vCloud Director 租用戶入口網站指南》。

5 在**即將完成**頁面上，檢閱登錄詳細資料並按一下**完成**。

後續步驟

- 在 vCenter Server 中指派 NSX 授權金鑰。
- 如需建立提供者虛擬資料中心的相關資訊，請參閱《vCloud Director 管理員指南》。

在 vCenter Server 中指派 NSX 授權金鑰

如果已將 vCenter Server 執行個體與其相關聯的 NSX Manager 執行個體連結在一起，您必須使用 vSphere Client 為支援 vCloud Director 網路的 NSX Manager 執行個體指派授權金鑰。

必要條件

此作業限於系統管理員。

程序

1 從連線至 vCenter Server 系統的 vSphere Client，選取**首頁 > 授權**。

2 選取**資產**報表檢視。

3 在 NSX Manager 資產上按一下滑鼠右鍵並選取**變更授權金鑰**。

4 選取**指定新授權金鑰**後再按一下**輸入金鑰**。

5 輸入授權金鑰、輸入選擇性的金鑰索引標籤，然後按一下**確定**。

使用您購買 vCloud Director 時收到的 NSX Manager 授權金鑰。您可以在多個 vCenter Server 執行個體中使用這個授權金鑰。

6 按一下**確定**。

登錄 NSX-T Manager 執行個體

您可以向 vCloud Director 登錄 NSX-T Manager 執行個體，以便 vCloud Director 可以使用其網路資源。提供者虛擬資料中心可以使用 NSX Data Center for vSphere 或 NSX-T Data Center 中的網路資源。

程序

1 從主功能表 (☰) 中，選取 **vSphere 資源**。

2 在左窗格中，按一下 **NSX-T Manager**，然後按一下**新增**。

3 如果您有多站台 vCloud Director 部署，請從**站台**下拉式功能表中，選取您要向其新增此 NSX-T Manager 執行個體的站台，然後按**下一步**。

4 輸入 vCloud Director 中 NSX-T Manager 執行個體的名稱，並選擇性地輸入說明。

5 輸入 NSX-T Manager 執行個體的 URL。

例如，**https://*FQDN_or_IP_address***。

6 輸入 NSX-T Manager **管理員**帳戶的使用者名稱和密碼。

7 按一下**儲存**。

後續步驟

如需建立 NSX-T Data Center 支援的提供者虛擬資料中心的相關資訊，請參閱《服務提供者適用的 vCloud API 程式設計指南》，網址為：https://code.vmware.com。

檢視 vCenter Server 執行個體

您可以查看 vCloud Director 安裝中所有站台之間的 vCenter Server 執行個體清單。您可以查看 vCloud Director 如何使用每個 vCenter Server 執行個體。

程序

1 從主功能表 (☰) 中，選取 **vSphere 資源**。

2 在左面板中，按一下 **vCenter**。

結果

此時會顯示所有連結的 vCenter Server 執行個體的清單。清單中包含每個 vCenter Server 執行個體的以下資訊。

	描述
名稱	vCloud Director 中的 vCenter Server 執行個體的名稱。
狀態	已啟用或已停用。請參閱 啟用或停用 vCenter Server 執行個體。
連線	是否連線到 vCloud Director。請參閱 重新連線 vCenter Server 執行個體。
VC 主機	vCenter Server 執行個體的 FQDN。
版本	vCenter Server 版本。
服務提供者	是否發佈以供虛擬資料中心使用。
承租人	是否發佈以用作軟體定義資料中心 (SDDC)。
站台	vCenter Server 執行個體所屬站台的 vCloud Director FQDN。

修改 vCenter Server 設定

如果已連結的 vCenter Server 執行個體的連線資訊發生變更，或者您要變更其在 vCloud Director 中的名稱和說明，您可以修改其設定。

您可以修改新增 vCenter Server 執行個體時所進行的設定。請參閱新增 vCenter Server 執行個體。

程序

1 從主功能表 (☰) 中，選取 **vSphere 資源**。

2 在左窗格中，按一下 **vCenter**，然後按一下您要修改的 vCenter Server 執行個體的名稱。

3 在 **vCenter 資訊**區段的右上角，按一下**編輯**。

4 編輯 vCenter Server 設定，然後按一下**儲存**。

後續步驟

如果您已修改連線資訊，則必須重新連線 vCenter Server 執行個體。

啟用或停用 vCenter Server 執行個體

執行維護或解除登錄 vCenter Server 執行個體之前，您必須停用目標 vCenter Server 執行個體。若要將其資源提供給 vCloud Director 中的虛擬資料中心，您必須啟用 vCenter Server 執行個體。

程序

1 從主功能表 (☰) 中，選取 **vSphere 資源**。

2 在左面板中，按一下 **vCenter**。

3 按一下目標 vCenter Server 執行個體名稱旁邊的選項按鈕，然後按一下**啟用**或**停用**。

4 按一下**確定**以確認。

重新連線 vCenter Server 執行個體

如果 vCenter Server 執行個體顯示為已中斷連線，或者您已修改連線設定，則可以嘗試重設連線。

備註 在建立新連線期間，vCenter Server 執行個體不可用於操作。

程序

1 從主功能表 (☰) 中，選取 **vSphere 資源**。

2 在左面板中，按一下 **vCenter**。

3 按一下目標 vCenter Server 執行個體名稱旁邊的選項按鈕，然後按一下**重新連線**。

4 按一下**確定**以確認。

重新整理 vCenter Server 執行個體

若要更新 vCloud Director 資料庫中有關基礎 vCenter Server 資源的資訊，您必須重新整理 vCenter Server 執行個體。

程序

1 從主功能表 (☰) 中，選取 **vSphere 資源**。

2 在左面板中，按一下 **vCenter**。

3 按一下目標 vCenter Server 執行個體名稱旁邊的選項按鈕，然後按一下**重新整理**。

4 按一下**確定**以確認。

重新整理 vCenter Server 執行個體的儲存區原則

若要更新 vCloud Director 資料庫中有關基礎 vSphere 環境中虛擬機器儲存區原則的資訊，您必須重新整理 vCenter Server 執行個體的儲存區原則。

程序

1 從主功能表 (☰) 中，選取 **vSphere 資源**。

2 在左面板中，按一下 **vCenter**。

3 按一下目標 vCenter Server 執行個體名稱旁邊的選項按鈕，然後按一下**重新整理原則**。

4 按一下**確定**以確認。

解除登錄 vCenter Server 執行個體

若要停止使用 vCenter Server 執行個體的資源，您可以從 vCloud Director 安裝移除此 vCenter Server 執行個體。

必要條件

- 停用 vCenter Server 執行個體。請參閱啟用或停用 vCenter Server 執行個體。
- 從此 vCenter Server 執行個體刪除所有使用資源集區的提供者虛擬資料中心。請參閱刪除提供者虛擬資料中心。

程序

1 從主功能表 (☰) 中，選取 **vSphere 資源**。

2 在左面板中，按一下 **vCenter**。

3 按一下目標 vCenter Server 執行個體名稱旁邊的選項按鈕，然後按一下**解除登錄**。

4 按一下**確定**以確認。

修改 NSX Manager 設定

如果已登錄的 NSX Manager 執行個體的連線資訊發生變更，或者您要變更其在 vCloud Director 中的名稱和說明，您可以修改其設定。

您可以修改新增 NSX Manager 執行個體時所進行的設定。請參閱(選擇性) 新增相關聯的 NSX Manager 執行個體。

程序

1 從主功能表 (☰) 中，選取 **vSphere 資源**。

2 在左窗格中，按一下 **vCenter**，然後按一下與目標 NSX Manager 執行個體相關聯的 vCenter Server 執行個體的名稱。

3 在 **NSX-V Manager 資訊**區段的右上角，按一下**編輯**。

4 編輯 vCenter Server 設定，然後按一下**儲存**。

修改 NSX-T Manager 設定

如果已登錄的 NSX-T Manager 執行個體的連線資訊發生變更，或者您要變更其在 vCloud Director 中的名稱和說明，您可以修改其設定。

您可以修改新增 vCenter Server 執行個體時所進行的設定。請參閱登錄 NSX-T Manager 執行個體。

程序

1 從主功能表 (☰) 中，選取 **vSphere 資源**。

2 在左窗格中，按一下 **NSX-T Manager**，然後按一下您要修改的 NSX-T Manager 執行個體的名稱。

3 在**一般**索引標籤的右上角，按一下**編輯**。

4 編輯 NSX-T Manager 設定，然後按一下**儲存**。

刪除 NSX-T Manager 執行個體

若要停止使用 NSX-T Manager 執行個體的資源，您可以從 vCloud Director 安裝移除此 vCenter Server 執行個體。

必要條件

刪除使用此 NSX-T Manager 執行個體中的資源的所有提供者虛擬資料中心。請參閱刪除提供者虛擬資料中心。

程序

1 從主功能表 (☰) 中，選取 **vSphere 資源**。

2 在左窗格中，按一下 **NSX-T Manager**。

3 按一下要移除之 NSX-T Manager 執行個體名稱旁邊的選項按鈕，然後按一下**刪除**。

4 按一下**刪除**以確認。

多站台資源清單

如果您要在多個位置使用 vCloud Director 部署，您可以檢視資源清單，其中包含所有已連線站台中的物件的相關資訊。

為了協助從 Service Provider Admin Portal (從 9.7 版開始) 導覽 vSphere 和雲端資源，vCloud Director 引入了多站台資源清單。

您可以透過 **vSphere 資源**和**雲端資源**功能表存取資源清單。

您可以從不同的站台存取有關物件的詳細資訊，也可以同時在本機站台和遠端站台上建立物件。

vCenter Server 執行個體、NSX-T Manager 執行個體、資源集區、資料存放區、主機、分散式交換器、連接埠群組、停頓項目和儲存區原則支援多站台 vSphere 資源清單。

組織 VDC、組織 VDC 範本、提供者 VDC、雲端儲存格、Edge 閘道、外部網路和網路集區支援多站台雲端資源清單。

備註 不支援多站台組織清單。

管理提供者虛擬資料中心

4

建立提供者虛擬資料中心後，您可以修改其內容、停用或刪除此提供者虛擬資料中心，以及管理其儲存區原則和資源集區。

若要建立提供者虛擬資料中心，您必須使用 vCloud Director Web Console 或 vCloud API。如需使用 vCloud Director Web Console 的相關資訊，請參閱《vCloud Director 管理員指南》。如需使用 vCloud API 的相關資訊，請參閱《服務提供者適用的 vCloud API 程式設計指南》。

本章節討論下列主題：

啟用或停用提供者虛擬資料中心

若要停用使用提供者虛擬資料中心之資源的所有現有組織虛擬資料中心，您可以停用此提供者虛擬資料中心。您無法建立使用已停用的提供者虛擬資料中心資源的組織虛擬資料中心。

執行中 vApp 與開啟電源的虛擬機器會繼續在此提供者虛擬資料中心支援的現有組織虛擬資料中心執行，但您無法建立或啟動其他 vApp 或虛擬機器。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下**提供者 VDC**。

3 按一下目標提供者虛擬資料中心名稱旁邊的選項按鈕，然後按一下**啟用**或**停用**。

4 按一下**確定**以確認。

刪除提供者虛擬資料中心

若要從 vCloud Director 移除提供者虛擬資料中心的資源，您可以刪除此提供者虛擬資料中心。

vSphere 中的基礎資源仍保持不受影響。

必要條件

- 停用目標提供者虛擬資料中心。請參閱啟用或停用提供者虛擬資料中心。
- 刪除使用此提供者虛擬資料中心的資源的所有組織虛擬資料中心。請參閱刪除組織虛擬資料中心。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下**提供者 VDC**。

3 按一下要移除之提供者虛擬資料中心名稱旁邊的選項按鈕，然後按一下**刪除**。

4 按一下**確定**以確認。

編輯提供者虛擬資料中心的一般設定

您可以變更提供者虛擬資料中心的名稱和說明。如果支援資源集區支援較高的虛擬硬體版本，您可以升級提供者虛擬資料中心支援的最高虛擬硬體。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下**提供者 VDC**，然後按一下您要修改的提供者虛擬資料中心的名稱。

3 在**設定 > 一般**索引標籤的右上角，按一下**編輯**。

4 (選擇性) 修改提供者虛擬資料中心的名稱和說明。

5 (選擇性) 從下拉式功能表中，選取此提供者虛擬資料中心支援的最高硬體版本，然後按一下**儲存**。

   您可以選取的最高版本取決於支援提供者虛擬資料中心之資源集區中的 ESXi 主機。

   備註 您只能升級提供者虛擬資料中心支援的硬體版本，並且不能將硬體版本降級。

6 按一下**儲存**。

合併提供者虛擬資料中心

若要合併兩個提供者虛擬資料中心的資源，您可以將這些提供者虛擬資料中心合併至單一提供者虛擬資料中心。

必要條件

- 目標提供者虛擬資料中心屬於同一個站台。
- 目標提供者虛擬資料中心僅包含彈性的組織虛擬資料中心。

程序

1. 從主功能表 (☰) 中，選取**雲端資源**。
2. 在左面板中，按一下**提供者 VDC**。
3. 按一下要擴充之提供者虛擬資料中心名稱旁邊的選項按鈕，然後按一下**合併**。
4. 按一下要與其合併資源的提供者虛擬資料中心名稱旁邊的選項按鈕，然後按一下**合併**。

檢視提供者虛擬資料中心的組織虛擬資料中心

您可以檢視使用提供者虛擬資料中心資源的組織虛擬資料中心的清單。

程序

1. 從主功能表 (☰) 中，選取**雲端資源**。
2. 在左面板中，按一下**提供者 VDC**，然後按一下目標提供者虛擬資料中心的名稱。
3. 按一下**組織 VDC** 索引標籤。

結果

此時會顯示使用此提供者虛擬資料中心資源的組織虛擬資料中心的清單。針對每個組織 VDC，此清單均包含狀態、狀況、配置模型、組織、vCenter Server 執行個體、網路數目、vApp 數目、儲存區原則數目和資源集區數目的相關資訊。

後續步驟

- 您可以按一下目標組織虛擬資料中心名稱旁邊的**快顯**圖示 (↗)，前往 vCloud Director Tenant Portal 中的組織虛擬資料中心視圖。
- 透過按一下組織虛擬資料中心名稱旁邊的選項按鈕，您可以執行管理作業，類似於第 6 章 管理組織虛擬資料中心中所述的作業。

檢視提供者虛擬資料中心上的資料存放區

您可以檢視有關為提供者虛擬資料中心提供儲存區容量的資料存放區的詳細資料。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下**提供者 VDC**，然後按一下目標提供者虛擬資料中心的名稱。

3 按一下**資料存放區**索引標籤。

此時會顯示提供者虛擬資料中心的所有資料存放區的清單。清單中包含每個資料存放區的以下資訊。

標題	描述
名稱	資料存放區的名稱
狀態	已啟用或已停用
類型	資料存放區所使用的檔案系統類型，為虛擬機器檔案系統 (VMFS) 或網路檔案系統 (NFS)。
已使用	資料存放區空間由包括記錄檔案、快照以及虛擬磁碟等虛擬機器檔案佔用。啟動虛擬機器時，使用的儲存空間也包括了記錄檔案。
已佈建	保證給予虛擬機器的資料存放區空間。如果任何虛擬機器使用精簡佈建，可能不會使用到部分已佈建空間，其他虛擬機器就會佔用未使用空間。如果使用精簡佈建，此值可能會大於實際的資料存放區容量。
要求的儲存空間	僅限資料存放區上由 vCloud Director 物件使用的已佈建儲存區，包括： ■ vCloud Director 中佈建的虛擬機器 ■ 目錄項目 (範本和媒體) ■ NSX Edge ■ 虛擬機器的已使用和未使用的記憶體交換需求 此值不包含陰影虛擬機器或連結複製樹狀結構中的中繼磁碟所要求的儲存區。
vCenter	與資料存放區相關聯的 vCenter Server 執行個體。

檢視提供者虛擬資料中心的外部網路

您可以檢視提供者虛擬資料中心可存取的外部網路的清單。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下**提供者 VDC**，然後按一下目標提供者虛擬資料中心的名稱。

3 按一下**外部網路**索引標籤。

結果

您可以檢視可用外部網路的清單及其閘道 CIDR 設定和 IP 集區使用狀況的相關資訊。

管理提供者虛擬資料中心上的虛擬機器儲存區原則

您可以新增、啟用、停用虛擬機器儲存區原則，以及將其從提供者虛擬資料中心移除。還可以新增、編輯和刪除提供者虛擬資料中心上虛擬機器儲存區原則的中繼資料。

將虛擬機器儲存區原則新增至提供者虛擬資料中心

您可以將虛擬機器儲存區原則新增至提供者虛擬資料中心，隨後設定此提供者虛擬資料中心所支援的組織虛擬資料中心以支援新增的儲存區原則。

重要 vCloud Director 不支援以主機為基礎的資料服務 (例如加密和 Storage I/O Control) 的虛擬機器儲存區原則。

必要條件

- vSphere 管理員已建立目標虛擬機器儲存區原則。如需以儲存區原則為基礎的管理 (SPBM) 的相關資訊，請參閱《vSphere 儲存區》說明文件。
- 重新整理 vCenter Server 執行個體的儲存區原則。

程序

1. 從主功能表 (☰) 中，選取**雲端資源**。
2. 在左面板中，按一下**提供者 VDC**，然後按一下目標提供者虛擬資料中心的名稱。
3. 在**儲存區原則**索引標籤上，按一下**新增**。
4. 選取一或多個要新增的儲存區原則，然後按一下**新增**。

   如果您選取 *** (任何)**，則在提供者虛擬資料中心的資料存放區叢集中新增和移除資料存放區時，vCloud Director 也會隨之動態新增和移除這些資料存放區。

後續步驟

設定提供者虛擬資料中心支援的組織虛擬資料中心，以支援儲存區原則。請參閱將虛擬機器儲存區原則新增至組織虛擬資料中心。

啟用或停用提供者虛擬資料中心上的虛擬機器儲存區原則

停用提供者虛擬資料中心中的虛擬機器儲存區原則後，其組織虛擬資料中心無法再使用此虛擬機器儲存區原則。

程序

1. 從主功能表 (☰) 中，選取**雲端資源**。
2. 在左面板中，按一下**提供者 VDC**，然後按一下目標提供者虛擬資料中心的名稱。
3. 按一下**儲存空間原則**索引標籤。
4. 按一下目標虛擬機器儲存區原則旁邊的選項按鈕，然後按一下**啟用**或**停用**。

5 按一下**確定**以確認。

從提供者虛擬資料中心刪除虛擬機器儲存區原則

您可以從提供者虛擬資料中心刪除虛擬機器儲存區原則。

必要條件

停用目標虛擬機器儲存區原則。請參閱啟用或停用提供者虛擬資料中心上的虛擬機器儲存區原則。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下**提供者 VDC**，然後按一下目標提供者虛擬資料中心的名稱。

3 按一下**儲存空間原則**索引標籤。

4 按一下目標虛擬機器儲存區原則旁邊的選項按鈕，然後按一下**移除**。

5 按一下**移除**以確認。

修改提供者虛擬資料中心上的虛擬機器儲存區原則的中繼資料

您可以新增、編輯和刪除提供者虛擬資料中心上儲存區原則的中繼資料。

透過使用物件中繼資料，您可以將使用者定義的 *name=value* 配對與提供者虛擬資料中心上的儲存區原則建立關聯。您可以在 vCloud API 查詢篩選器運算式中使用物件中繼資料。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下**提供者 VDC**，然後按一下目標提供者虛擬資料中心的名稱。

3 按一下**儲存空間原則**索引標籤。

4 按一下目標虛擬機器儲存區原則旁邊的選項按鈕，然後按一下**中繼資料**。

5 按一下**編輯**。

6 (選擇性) 若要新增索引鍵-值配對，請按一下**新增**，輸入名稱和值，然後選取新索引鍵-值配對的類型。

7 (選擇性) 若要編輯索引鍵-值配對，輸入新名稱和值，並為索引鍵-值配對選取新類型。

8 (選擇性) 若要移除索引鍵-值配對，請在資料列的右側按一下**刪除**圖示。

9 按一下**儲存**，然後按一下**確定**。

管理提供者虛擬資料中心的資源集區

您可以新增、啟用、停用次要資源集區，以及將其與提供者虛擬資料中心中斷連結。您無法停用提供者虛擬資料中心上的主要資源集區或將其中斷連結。

將資源集區新增至提供者虛擬資料中心

您可以將一或多個次要資源集區新增到提供者虛擬資料中心，以便擴充隨收隨付和配置集區組織虛擬資料中心。

如果計算資源受多個資源集區支援，則可以擴充資源集區以容納更多虛擬機器。

您可以新增受 vSphere 叢集支援的資源集區，這些叢集會以最佳方式設定，以用於主控具有 VLAN 上行的 NSX Edge。vCloud Director 可以使用中繼資料指示系統必須將組織 VDC Edge 閘道置於這些叢集所支援的資源集區中。如需詳細資訊，請參閱 VMware 知識庫文章 https://kb.vmware.com/kb/2151398。

必要條件

您的 vSphere 管理員已在 vCenter Server 執行個體中建立目標次要資源集區，該集區支援提供者虛擬資料中心的主要資源集區。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下**提供者 VDC**，然後按一下目標提供者虛擬資料中心的名稱。

3 在**資源集區**索引標籤上，按一下**新增**。

4 選取一或多個要新增的資源集區，然後按一下**新增**。

結果

vCloud Director 會新增供提供者虛擬資料中心使用的資源集區，讓所有隨收隨付和配置集區組織虛擬資料中心 (由該提供者虛擬資料中心所支援) 更有彈性。

vCloud Director 也會在新的資源集區下新增系統 VDC 資源集區。此資源集區用於建立系統資源，例如 NSX Edge 虛擬機器和用作連結複製範本的虛擬機器。

重要 請勿編輯或刪除系統 VDC 資源集區。

啟用或停用提供者虛擬資料中心上的資源集區

停用資源集區時，資源集區的記憶體與計算資源就不再可供提供者虛擬資料中心使用。

已在進行的程序不會停止使用已停用資源集區中的資源。

備註 您無法停用提供者虛擬資料中心上的主要資源集區。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下**提供者 VDC**，然後按一下目標提供者虛擬資料中心的名稱。

3 按一下**資源集區**索引標籤。

4 按一下目標資源集區旁邊的選項按鈕，然後按一下**啟用**或**停用**。

5 按一下**確定**以確認。

將資源集區與提供者虛擬資料中心中斷連結

如果提供者虛擬資料中心有一個以上的資源集區，您可以將次要資源集區與提供者虛擬資料中心中斷連結。您無法將主要資源集區與提供者虛擬資料中心中斷連結。

必要條件

- 停用提供者虛擬資料中心上的目標資源集區。請參閱 啟用或停用提供者虛擬資料中心上的資源集區。
- 從該資源集區移轉任何虛擬機器至已啟用的資源集區。如需在提供者虛擬資料中心上資源集區之間移轉虛擬機器的相關資訊，請參閱《vCloud Director 管理員指南》。
- 重新部署受停用資源集區影響的所有網路。
- 重新部署受停用資源集區影響的所有 Edge 閘道。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下**提供者 VDC**，然後按一下目標提供者虛擬資料中心的名稱。

3 按一下**資源集區**索引標籤。

4 按一下目標資源集區旁邊的選項按鈕，然後按一下**中斷連結**。

5 按一下**確定**以確認。

修改提供者虛擬資料中心的中繼資料

您可以新增、編輯和刪除提供者虛擬資料中心的中繼資料。

透過使用物件中繼資料，您可以將使用者定義的 *name=value* 配對與提供者虛擬資料中心建立關聯。您可以在 vCloud API 查詢篩選器運算式中使用物件中繼資料。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下**提供者 VDC**，然後按一下目標提供者虛擬資料中心的名稱。

3 在**設定 > 中繼資料**索引標籤的右上角，按一下**編輯**。

4 (選擇性) 若要新增索引鍵-值配對，請按一下**新增**，輸入名稱和值，然後選取新索引鍵-值配對的類型。

5 (選擇性) 若要編輯索引鍵-值配對，輸入新名稱和值，並為索引鍵-值配對選取新類型。

6 (選擇性) 若要移除索引鍵-值配對，請在資料列的右側按一下**刪除**圖示。

7 按一下**儲存**，然後按一下**確定**。

管理組織

5

vCloud Director Service Provider Admin Portal 可讓您建立、設定及管理 vCloud Director 組織。

使用 vCloud Director Service Provider Admin Portal 管理組織、設定原則以決定使用者如何使用配置給組織的資源，以及管理目錄發佈和共用。

本章節討論下列主題：

瞭解租用

建立組織涉及指定租用事宜。租用藉由指定可執行 vApp 以及可儲存 vApp 與 vApp 範本的最長時間數，為組織的儲存與計算資源提供控制層級。

執行階段租用目的在於防止非使用中的 vApp 耗用計算資源。例如某使用者啟動 vApp 後出門度假，但未停止 vApp，該 vApp 仍會繼續耗用資源。

執行階段租用在使用者啟動 vApp 時即開始生效。執行階段租用到期時，vCloud Director 便會停止該 vApp。

儲存租用目的在於防止未使用的 vApp 和 vApp 範本消耗儲存資源。vApp 儲存租用在使用者停止 vApp 時即開始生效。儲存租用不會影響 vApp 的執行。在使用者新增 vApp 範本至 vApp、新增 vApp 範本至工作區、下載、複製或移動 vApp 範本時，vApp 範本儲存租用即開始生效。

儲存租用到期時，vCloud Director 會將 vApp 或 vApp 範本標示為已到期，或刪除 vApp 或 vApp 範本，視您所設的組織原則而定。

建立組織

您可以從 vCloud Director Service Provider Admin Portal 建立新的組織。

程序

1 從主功能表 (☰) 中，選取**雲端資源**

a 從左面板中，選取**組織**。

現有組織的清單會顯示在網格視圖中。

2 若要建立新組織，請按一下 **+新增**按鈕。

新增組織對話方塊隨即開啟。

3 輸入下列值。

選項	描述
組織名稱	構成用於存取組織租用戶入口網站的 URL 的唯一識別碼。
組織全名	組織的全名。
描述	組織的選擇性說明。

4 按一下**建立**按鈕以完成建立。

設定組織目錄

您可以設定組織共用其服務目錄的方式。

程序

1 從主功能表 (☰) 中，選取**雲端資源**

a 從左面板中，選取**組織**。

現有組織的清單會顯示在網格視圖中。

2 使用每個項目左側的清單列 (⋮)，以顯示可針對每個組織採取的動作。

3 按一下**目錄**。

組織的**目錄設定**對話方塊隨即開啟。

4 設定下列共用和發佈選項。

選項	描述
共用	允許組織管理員將此組織的目錄與此 vCloud Director 執行個體中的其他組織共用。如果您未選取此選項，組織管理員還是可以共用組織內的目錄。
允許發佈至外部目錄	允許組織管理員將目錄發佈到此 vCloud Director 執行個體外部的組織。
允許訂閱外部目錄	允許組織管理員訂閱此 vCloud Director 執行個體外部的目錄。

設定組織原則

租用、配額及限制會約束組織使用者能夠耗用的儲存與運算資源。您可以修改這些設定以避免使用者減少或獨占組織的資源。

必要條件

請參閱 瞭解租用。

程序

1 從主功能表 (☰) 中，選取**雲端資源**

a 從左面板中，選取**組織**。

現有組織的清單會顯示在網格視圖中。

2 使用每個項目左側的清單列 (⋮)，以顯示可針對每個組織採取的動作。

3 按一下**原則**，以編輯組織的租用、配額、資源限制和密碼原則。

4 針對 vApp 租用進行下列設定。

選項	描述
執行階段租用上限	vApp 自動停止以前，可以執行的時間長度。
儲存空間租用上限	已停止的 vApp 自動清除以前，可供使用的時間長度。
儲存空間清除	vApp 停止和清除之後的處理方式。

5 針對 vApp 範本租用進行下列設定。

選項	描述
儲存空間租用上限	vApp 範本自動清除以前，可供使用的時間長度。
儲存空間清除	到期的 vApp 範本清除之後的處理方式。

6 針對配額進行下列設定。

選項	描述
所有虛擬機器配額	在此組織中，使用者可儲存的可用虛擬機器總數。
執行中虛擬機器配額	在此組織中，使用者可開啟電源的虛擬機器總數。

7 針對限制進行下列設定。

選項	描述
每一使用者的資源密集作業數目	輸入每個使用者的最大同時資源密集作業數目，或選取**繼承系統限制**。
為每一使用者排入佇列的資源密集作業數目	輸入每個使用者排入佇列的最大資源密集作業數目，或選取**繼承系統限制**。
每一組織的資源密集作業數目	輸入每個組織的最大同時資源密集作業數目，或選取**繼承系統限制**。
為每一組織排入佇列的資源密集作業數目	輸入每個組織排入佇列的最大資源密集作業數目，或選取**繼承系統限制**。

選項	描述
每一虛擬機器的同時連線數目	輸入每個虛擬機器的最大同時主控台連線數目，或選取**繼承系統限制**。
每一組織的虛擬資料中心數目	輸入每個組織的最大虛擬資料中心數目，或選取**繼承系統配額**。

8 針對密碼原則進行下列設定。

選項	描述
已啟用帳戶鎖定	在若干次無效的登入嘗試之後，啟用使用者帳戶鎖定。
鎖定前的無效登入次數	在使用者帳戶鎖定前的無效登入嘗試次數。
帳戶鎖定間隔	鎖定的使用者帳戶無法登入的期間。

管理組織虛擬資料中心

6

若要提供資源給組織，您可以為此組織建立一或多個組織虛擬資料中心。建立組織虛擬資料中心後，您可以修改其內容、停用或刪除此組織虛擬資料中心以及管理其配置模型、儲存和網路設定。

本章節討論下列主題：

瞭解配置模型

配置模型決定了配置的提供者虛擬資料中心 (VDC) 的計算和記憶體資源認可給組織 VDC 的方式與時機。

下表基於組織 VDC 配置模式顯示虛擬機器 (VM) 或資源集區層級的 vSphere 資源分佈設定。

	彈性配置模型	彈性配置集區模型	非彈性配置集區模型	隨收隨付模型	保留集區模型
彈性	以組織 VDC 組態為基礎。	是	否	是	否
vCPU 速度	如果在 VDC 運算原則中未定義虛擬機器 CPU 限制，則 vCPU 速度可能會影響 VDC 內的虛擬機器 CPU 限制。	影響在組織 VDC 內執行的 vCPU 數目。	不適用	影響虛擬機器 CPU 限制	不適用

	彈性配置模型	彈性配置集區模型	非彈性配置集區模型	隨收隨付模型	保留集區模型
資源集區 CPU 限制	組織 VDC CPU 限制根據資源集區中的虛擬機器數目進行分配。	組織 VDC CPU 配置	組織 VDC CPU 配置	無限制	組織 VDC CPU 配置
資源集區 CPU 保留	組織 VDC CPU 保留根據資源集區中的 vCPU 數目進行分配。組織 VDC CPU 保留等於組織 VDC CPU 配置乘以 CPU 保證。	開啟電源的虛擬機器總和，等於 CPU 保證乘以 vCPU 速度，再乘以 vCPU 數目。	組織 VDC CPU 配置乘以 CPU 保證	無，可擴充	組織 VDC CPU 配置
資源集區記憶體限制	組織 VDC 記憶體限制根據資源集區中的虛擬機器數目進行分配。	無限制	組織 VDC RAM 配置	無限制	組織 VDC RAM 配置
資源集區記憶體保留	組織 VDC RAM 保留根據資源集區中的虛擬機器數目進行分配。組織 VDC RAM 保留等於組織 VDC RAM 配置乘以 RAM 保證。	RAM 保證的總和乘以資源集區中所有已開啟電源的虛擬機器的 vRAM。資源集區 RAM 保留是可擴充的。	組織 VDC RAM 配置乘以 RAM 保證	無，可擴充	組織 VDC RAM 配置
虛擬機器 CPU 限制	以虛擬機器的 VDC 運算原則為基礎。	無限制	無限制	vCPU 速度乘以 vCPU 數目	自訂
虛擬機器 CPU 保留	以虛擬機器的 VDC 運算原則為基礎。	0	0	等於 CPU 速度乘以 vCPU 速度，再乘以 vCPU 數目。	自訂
虛擬機器 RAM 限制	以虛擬機器的 VDC 運算原則為基礎。	無限制	無限制	vRAM	自訂
虛擬機器 RAM 保留	以虛擬機器的 VDC 運算原則為基礎。	0	等於 vRAM 乘以 RAM 保證加上 RAM 負載。	等於 vRAM 乘以 RAM 保證加上 RAM 負載。	自訂

配置模型的建議使用

每種配置模式可用於不同層級的效能控制和管理。

下表包含每個配置模型的建議使用的相關資訊。

配置模型	建議使用
彈性配置模型	使用彈性配置模式時，您可以在工作負載層級實現更為精細的效能控制。透過使用彈性配置模式，vCloud Director **系統管理員**可以管理個別組織 VDC 的彈性。彈性配置模型使用以原則為基礎的工作負載管理。使用彈性配置模式時，**雲端提供者**可以更好地控制組織 VDC 中的記憶體負載，並且可以對承租人強制執行嚴格的高載容量使用量。
配置集區配置模型	將配置集區配置模式用於長期穩定的工作負載，其中承租人訂閱了固定的計算資源耗用量，而**雲端提供者**可以預測和管理計算資源容量。配置集區配置模型最適合具有不同效能需求的工作負載。使用配置集區配置模型時，所有工作負載會共用 vCenter Server 的資源集區中已配置的資源。無論是啟用還是停用彈性，承租人都會接收有限數量的計算資源。透過配置集區配置模式，**雲端提供者**可以在系統層級啟用或停用彈性，並且設定會套用至所有配置集區組織 VDC。如果您使用非彈性配置集區配置，組織 VDC 會預先保留 VDC 資源集區，並且承租人可以過度認可 vCPU 但不可過度認可任何記憶體。如果您使用彈性集區配置，組織 VDC 不會預先保留任何計算資源，並且容量可跨越多個叢集。雲端提供者可管理實體計算資源的過度認可，而承租人不可過度認可 vCPU 和記憶體。

配置模型	建議使用
隨收隨付	如果不需要先期配置 vCenter Server 中的計算資源，請使用隨收隨付模型。保留、限制及共用會套用至承租人在 VDC 中部署的每個工作負載。使用隨收隨付配置模型時，組織 VDC 中的每個工作負載都會接收相同的已設定的保留計算資源百分比。對於 vCloud Director，每個工作負載之每個 vCPU 的 CPU 速度是相同的，您只能在組織 VDC 層級定義 CPU 速度。從效能角度來看，由於您無法變更個別工作負載的保留設定，因此每個工作負載會接收相同的喜好設定。隨收隨付配置模式最適合需要在同一個組織 VDC 中執行具有不同效能需求的工作負載的承租人。由於具有彈性，隨收隨付模型適用於做為自動調整應用程式一部分的通用、短期工作負載。透過隨收隨付，承租人可應對組織 VDC 內的計算資源需求突增情形。
保留集區	如果您需要對執行於組織 VDC 中的工作負載效能進行更為精細的控制，請使用保留集區配置模型。從**雲端提供者**的觀點來看，保留集區配置模式需要先期配置 vCenter Server 中的所有計算資源。保留集區配置模式不具彈性。保留集區配置模式最適合在專用於特定承租人的硬體上執行的工作負載。在此類情況下，承租人使用者可以管理計算資源的使用與過度認可。

彈性配置模型

從 vCloud Director 9.7 開始，**系統管理員**可以使用彈性配置模式建立組織虛擬資料中心 (VDC)。透過組合使用彈性配置和 VDC 運算原則，**系統管理員**可以控制 VDC 和個別虛擬機器 (VM) 層級的 CPU 與 RAM 使用量。彈性配置模型支援現有配置模型中可用的所有配置組態。

如果您在 vCloud Director 9.7 中建立非彈性組織 VDC，可以重新設定組織 VDC 以使用彈性配置模型。如果使用低於 9.7 的 vCloud Director 版本建立組織 VDC，則無法將組織資料中心重新設定為使用彈性配置模式。

建立彈性組織 VDC 時，**系統管理員**會控制組織 VDC 的下列屬性：

- 啟用或停用彈性集區功能。
- 包含或排除記憶體負載。
- 指定組織 VDC 的預設 VDC 運算原則。
- 記憶體和 CPU 配置與保證
- 網路配額
- 儲存區設定檔

做為 **vCloud Director 系統管理員**，您可以將彈性組織 VDC 設定為具有彈性或不具彈性。當彈性組織 VDC 啟用彈性集區功能時，組織 VDC 會跨越並使用所有與其提供者 VDC 相關聯的資源集區。在 vCloud Director 9.7 中，如果您將非彈性組織 VDC 轉換為彈性組織 VDC，則無法將同一個組織 VDC 重新轉換為非彈性。

彈性配置模型支援組織 VDC 運算原則的各種功能，且沒有其他配置模型存在的任何限制。在彈性配置模型中，虛擬機器的計算資源配置取決於組織 VDC 運算原則。如果您沒有定義組織 VDC 的 VDC 運算原則，計算資源配置則取決於組織 VDC 配置模式。透過組合使用彈性配置模式和組織 VDC 運算原則，一個組織 VDC 可容納使用所有其他配置模式之通用組態的虛擬機器。如需詳細資訊，請參閱〈瞭解運算原則〉。

若要建立彈性組織 VDC，您可以使用 vCloud Director Service Provider Admin Portal 或 vCloud API。如需 vCloud API 的相關資訊，請參閱《服務提供者適用的 vCloud API 程式設計指南》。

配置集區配置模型

使用配置集區配置模型時，您從提供者 VDC 配置的資源中有一部分會認可給組織 VDC。您可以指定 CPU 與記憶體的百分比。此百分比稱為百分比保證因素，允許您過度認可資源。

從 vCloud Director 5.1.2 開始，系統管理員可以將配置集區組織 VDC 設定為具有彈性或不具彈性。彈性屬於全域設定，會影響所有配置集區組織 VDC。如需修改一般系統設定的相關資訊，請參閱《vCloud Director 管理員指南》。

依預設，配置集區組織 VDC 會啟用彈性的配置集區。從 vCloud Director 5.1 升級的系統，其配置集區組織 VDC 具有跨越多個資源集區的虛擬機器時，預設會啟用彈性的配置集區。

當配置集區 VDC 啟用彈性的配置集區功能時，組織 VDC 會跨越並使用所有與其提供者 VDC 相關聯的資源集區。因此，vCPU 頻率現在是配置集區的強制參數。

以如下方式設定 vCPU 頻率和百分比保證因子，可在組織 VDC 上部署足夠數目的虛擬機器，而 CPU 不會成為瓶頸因素。

建立虛擬機器時，放置引擎會將其放置在最適合該虛擬機器要求的提供者 vDC 資源集區上。系統會在該提供者 VDC 資源集區下方為此組織 VDC 建立一個子資源集區，該虛擬機器會放置在該子資源集區下方。

虛擬機器開啟電源時，放置引擎會檢查提供者 VDC 資源集區，以確定它仍可開啟虛擬機器電源。如果沒有容量，放置引擎會將虛擬機器移動至具有足夠資源執行虛擬機器的提供者 vDC 資源集區。如果組織 VDC 不存在子資源集區，則會建立一個。

系統會為該子資源集區設定足夠執行新虛擬機器的資源。子資源集區的記憶體保留將增加，增加的數量為虛擬機器的已設定記憶體大小乘以組織 VDC 的百分比保證因子。子資源集區的 CPU 保留將增加，增加的數量為虛擬機器的已設定 vCPU 數目乘以在組織 VDC 層級指定的 vCPU 再乘以在組織 VDC 層級設定的 CPU 百分比保證因子。如果已啟用彈性的配置集區功能，則子資源集區的記憶體限制會增加，增加的數量為虛擬機器的已設定記憶體大小，同時子資源集區的 CPU 限制也會增加，增加的數量為虛擬機器的已設定 vCPU 數目乘以在組織 VDC 層級指定的 vCPU 頻率。系統會重新設定虛擬機器以將其記憶體和 CPU 保留設定為零，而虛擬機器放置引擎會將該虛擬機器放置在提供者 VDC 資源集區上。

如果您使用彈性的配置集區配置模型，僅由 vCloud Director 監控和管理限制。如果停用具有彈性的功能，將另外設定資源集區限制。

配置集區模型的效益是虛擬機器可以善用相同子資源集區上的閒置虛擬機器資源，此模型可以善用新增至提供者 VDC 的新資源。

在少數情況下，虛擬機器會在開啟電源時從建立時為其指派的資源集區切換至不同的資源集區，這是因為原始資源集區上的資源不足所致。此變更可能會產生小幅成本，用於將虛擬機器磁碟檔案移動至新的資源集區。

當彈性配置集區功能停用時，配置集區組織 VDC 的行為類似於 vCloud Director 1.5 中的配置集區模型。在此模型中，無法設定 vCPU 頻率。過度認可會透過設定保證資源百分比的方式來控制。

依預設，在配置集區 VDC 中，虛擬機器從 VDC 設定取得其保留、限制和共用設定。若要使用自訂的 CPU 和記憶體資源配置設定建立或重新設定虛擬機器，您可以使用 vCloud API。請參閱《服務提供者適用的 vCloud API 程式設計指南》。

隨收隨付配置模型

使用隨收隨付配置模型時，當使用者於組織 VDC 中建立 vApp 時才會認可資源。您可以指定保證給予的資源百分比，您可以過度認可資源。您可藉由新增多個資源集區到提供者 vDC 來讓隨收隨付組織 vDC 具有彈性。

認可給組織的資源會套用在虛擬機器層級。

當虛擬機器已開啟電源時，如果原始資源集區無法容納該虛擬機器，放置引擎會檢查資源集區，並向另一個資源集區指派虛擬機器。如果資源集區沒有可用的子資源集區，vCloud Director 會以無限限制與零速率建立一個子資源集區。虛擬機器的速率設定為其限制乘以其認可的資源，而虛擬機器放置引擎會將該虛擬機器放置在提供者 VDC 資源集區上。

隨收隨付模型的效益為模型可以善用新增至提供者 VDC 的新資源。

在少數情況下，虛擬機器會從建立時指派給機器的資源集區，於開啟電源時切換至不同的資源集區，這是因為原始資源集區上的資源不足所致。此變更可能會產生小幅成本，用於將虛擬機器磁碟檔案移動至新的資源集區。

在隨收隨付模型中，不會預先保留資源，如果資源不足，虛擬機器可能就無法開啟電源。在此模型下作業的虛擬機器無法利用相同子資源集區上閒置虛擬機器的資源，因為資源是在虛擬機器層級設定。

依預設，在隨收隨付 VDC 中，虛擬機器從 VDC 設定取得其保留、限制和共用設定。若要使用自訂的 CPU 和記憶體資源配置設定建立或重新設定虛擬機器，您可以使用 vCloud API。請參閱《服務提供者適用的 vCloud API 程式設計指南》。

保留集區配置模型

使用保留集區配置模型時，您配置的所有資源會立即認可給組織 VDC。組織中的使用者可透過指定個別虛擬機器的保留、限制及優先順序設定，控制過度認可。

因為此模型中只有一個資源集區與一個子資源集區，因此開啟虛擬機器電源時，放置引擎不會重新指定虛擬機器的資源集區。且不會修改虛擬機器的速率與限制。

使用保留集區模型，來源在需要時皆為可用。此模型也提供對虛擬機器速率、限制以及共用的精細控制，如果仔細規劃，就可讓保留資源達到最佳使用量。如需在保留集區 VDC 內設定虛擬機器資源配置設定的相關資訊，請參閱《vCloud Air - Virtual Private Cloud OnDemand 使用者指南》。

在此模型中，保留一定是在主要叢集中完成。如果沒有足夠的資源可在主要叢集上建立組織 VDC，則組織 VDC 建立會失敗。

此模型的其他限制為此模型不具彈性，組織使用者可能會在虛擬機器上設定不佳的共用、速率以及限制，導致資源使用量過低。

瞭解運算原則

從 vCloud Director 9.7 開始，您可以使用運算原則來控制資源配置和虛擬機器 (VM) 放置。根據範圍和功能，有兩種類型的運算原則 - 提供者虛擬資料中心 (VDC) 運算原則與 VDC 運算原則。

提供者 VDC 運算原則

提供者 VDC 運算原則會定義直接影響承租人工作負載放置的虛擬機器-主機相似性規則。承租人使用者無法查看提供者 VDC 運算原則。

提供者 VDC 運算原則的範圍是處於提供者 VDC 層級。

VDC 運算原則

VDC 運算原則可控制組織 VDC 層級的虛擬機器的計算特性。由於承租人使用者無法查看提供者 VDC 運算原則，因此，若要公開虛擬機器-主機相似性規則以供承租人使用，可在 VDC 運算原則內參考提供者 VDC 運算原則。

提供者虛擬資料中心運算原則

透過使用提供者虛擬資料中心 (VDC) 運算原則，vCloud Director **系統管理員**可以向承租人公開虛擬機器 (VM) 群組和邏輯虛擬機器群組。

提供者 VDC 運算原則可能包含下列內容的集合：

- 包含類似虛擬機器的虛擬機器群組。每個虛擬機器群組屬於不同的叢集。
- 適用於各種功能的邏輯虛擬機器群組。
- 虛擬機器群組和邏輯虛擬機器群組。

提供者 VDC 運算原則和邏輯虛擬機器群組

系統管理員可以使用虛擬機器群組和邏輯虛擬機器群組，向承租人公開 vSphere Distributed Resource Scheduler (DRS) 虛擬機器-主機相似性規則。在 vCloud Director 中，DRS 虛擬機器-主機相似性規則在提供者層級公開為虛擬機器群組。虛擬機器-主機相似性規則會繫結到特定的叢集。由於彈性的提供者 VDC 可以跨越多個 vSphere 叢集，因此，邏輯虛擬機器群組透過對邏輯上相同的叢集繫結虛擬機器群組進行分組，提供跨多個叢集運作的 DRS 虛擬機器-主機相似性規則的抽象概念。若要管理邏輯虛擬機器群組，您可以使用 vCloud OpenAPI。如需 vCloud OpenAPI 的相關資訊，請參閱《vCloud OpenAPI 入門》，網址為 https://code.vmware.com。

若要公開虛擬機器-主機相似性規則，您可以將虛擬機器群組和邏輯虛擬機器群組新增至提供者 VDC 運算原則，並建立提供者 VDC 運算原則與 VDC 運算原則之間的參考。

在提供者 VDC 運算原則環境中，邏輯虛擬機器群組之間具有 AND 關聯性。

使用提供者 VDC 運算原則和邏輯虛擬機器群組，**vCloud Director 系統管理員**可以向組織 VDC 內的承租人使用者公開多個虛擬機器群組。例如，假設環境中包含兩個叢集：*cluster1* 和 *cluster2*。*cluster1* 中具有主機 *SQL_host_1*，而 *cluster2* 中具有主機 *SQL_fast_host* 和 *Fast_host*。

1 在 *cluster1* 中，您建立了 *SQL_host_group1* 和 *VM_group1*，

   您在 *VM_group1* 和 *SQL_host_group1* 之間建立了正相似性。

2 在 *cluster2* 中，您建立了四個群組。

   - 建立 *SQL_host_group2* 和 *VM_group2*

     您在 *VM_group2* 和 *SQL_host_group2* 之間建立了正相似性。

   - 建立 *fast_host_group* 和 *VM_group3*。

您在 *VM_group3* 和 *fast_host_group* 之間建立了正相似性。

您建立了包含 *logical_VM_group1* 和 *logical_VM_group2* 的 *PVDC_compute_policy1*。*logical_VM_group1* 包含 *VM_group1* 和 *VM_group2*。*logical_VM_group2* 包含 *VM_group3*。

您建立了 *SQL_and_fast* VDC 運算原則並將其發佈至組織 VDC，而且新增了 *PVDC_compute_policy1* 的參考。當您建立 *SQL_and_fast* VDC 運算原則和 *PVDC_compute_policy1* 之間的參考時，您會向組織 VDC 內的承租人使用者公開邏輯虛擬機器群組和虛擬機器群組資訊。如此一來，當承租人套用 *SQL_and_fast* VDC 運算原則至虛擬機器時，放置引擎會將該虛擬機器新增至 *cluster2* 內的 *SQL_fast_host*。

工作流程如下所示。

1 **vCenter Server 管理員**使用 vSphere Client 建立主機群組。

   如需相關資訊，請參閱 VMware vSphere ESXi 和 vCenter Server 說明文件中的〈建立主機 DRS 群組 (MSCS)〉主題。

2 **vCenter Server 管理員**或 **vCloud Director 系統管理員**建立虛擬機器群組。

   如需相關資訊，請參閱《vCloud Director 管理員指南》中的〈建立或更新虛擬機器群組〉主題。

3 **vCloud Director 系統管理員**建立虛擬機器群組和主機群組之間的適當相似性規則。

   如需相關資訊，請參閱《vCloud Director 管理員指南》中的〈管理虛擬機器-主機相似性規則〉主題。

4 **vCloud Director 系統管理員**群組使用 vCloud OpenAPI 將邏輯上相同的虛擬機器群組分為邏輯虛擬機器群組。

5 **vCloud Director 系統管理員**使用 vCloud OpenAPI 建立提供者 VDC 運算原則並新增邏輯虛擬機器群組。

6 **vCloud Director 系統管理員**使用 vCloud OpenAPI 建立參考提供者 VDC 運算原則的 VDC 運算原則，並向組織 VDC 發佈此 VDC 運算原則。

當承租人在組織 VDC 中建立虛擬機器並選取 VDC 運算原則時，vCloud Director 會將該虛擬機器新增至 VDC 運算原則中參考的虛擬機器群組。如此一來，vCloud Director 會在適當的主機上建立虛擬機器。

提供者 VDC 運算原則和虛擬機器群組

一個提供者 VDC 運算原則可以包含每個叢集中的零個或一個虛擬機器群組。例如，提供者 VDC 運算原則 *oracle_license* 可以包含虛擬機器群組 *oracle_license1* 和 *oracle_license2*，其中虛擬機器群組 *oracle_license1* 屬於叢集 *oracle_cluster1*，虛擬機器群組 *oracle_license2* 屬於叢集 *oracle_cluster2*。

將提供者 VDC 運算原則指派給虛擬機器時，放置引擎會將此虛擬機器新增至其所在叢集的對應虛擬機器群組。例如，如果您選取將虛擬機器部署在叢集 *oracle_cluster1* 上，並將提供者 VDC 運算原則 *oracle_license* 指派給此虛擬機器，放置引擎會將此虛擬機器新增至虛擬機器群組 *oracle_license1*。

工作流程如下所示。

1 **系統管理員**使用 vCloud OpenAPI 建立一或多個提供者 VDC 運算原則。

2 **系統管理員**使用 vCloud OpenAPI 建立一或多個 VDC 運算原則。

VDC 運算原則可與零個或一個提供者 VDC 運算原則相關聯。VDC 運算原則的名稱和提供者 VDC 運算原則是唯一的。

3 **系統管理員**使用 vCloud OpenAPI 將 VDC 運算原則發佈到一或多個組織 VDC。

承租人只能看到發佈至其組織 VDC 的 VDC 運算原則。在承租人層級無法使用提供者 VDC 運算原則。

4 承租人可以使用 vCloud API 或 vCloud Director 租用戶入口網站，在建立或更新虛擬機器時將組織 VDC 運算原則指派給虛擬機器。

一開始，系統不包含任何提供者 VDC 運算原則，每個組織 VDC 只包含一個預設運算原則，並且該預設原則不會與提供者 VDC 運算原則相關聯。

若要建立和管理提供者和全域 VDC 運算原則，您必須使用 vCloud OpenAPI。請參閱《vCloud OpenAPI 入門》，網址為：https://code.vmware.com。

虛擬資料中心運算原則

虛擬資料中心 (VDC) 運算原則可控制承租人工作負載的實體計算資源配置。若要根據特定的工作負載需求配置實體資源，承租人使用者可以在預設運算原則和自訂 VDC 運算原則之間進行選取。

VDC 運算原則可對屬性進行分組，這些屬性用於定義組織 VDC 內虛擬機器的計算資源配置。計算資源配置包括 CPU 和記憶體配置、保留、限制和共用。

vCloud Director **系統管理員**建立並管理全域層級的運算原則，並且可以向一或多個組織 VDC 發佈個別運算原則。當您向組織 VDC 發佈 VDC 運算原則時，組織中的使用者便可使用該原則。建立並管理組織 VDC 中的虛擬機器時，**承租人管理員**可將可用的 VDC 運算原則指派給虛擬機器。組織 VDC 中的**承租人管理員**和使用者無法查看特定的 VDC 運算原則組態。

雲端提供者可以利用 VDC 運算原則定義具名 CPU 和記憶體耗用量設定檔，承租人可將其與組織 VDC 內的虛擬機器相關聯。使用 VDC 運算原則是雲端提供者定義和提供差異化服務層級的一種機制，例如大量 CPU 設定檔或高記憶體使用量設定檔。透過 VDC 運算原則，雲端提供者還可以限制或約束組織 VDC 中虛擬機器的 CPU 和記憶體耗用量。

透過 VDC 運算原則，vCloud Director 系統管理員可以控制虛擬機器層級的計算資源耗用量的下列方面：

- vCPU 數目和 vCPU 時脈速度
- 配置給虛擬機器的記憶體數量
- 記憶體和 CPU 保留、限制及共用

虛擬資料中心運算原則的屬性

當您建立虛擬資料中心 (VDC) 運算原則時，可以指定所有可用屬性的子集。唯一的必要屬性是 VDC 運算原則名稱。

下表列出了您可以在 VDC 運算原則中定義的所有屬性。

表 6-1. VDC 運算原則屬性

VDC 運算原則屬性	API 參數	描述
Name	name	用作 VDC 運算原則識別碼的必要參數。
Description	description	表示 VDC 運算原則的簡短說明。
vCPU Speed	cpuSpeed	定義虛擬機器 (VM) 的 vCPU 速度 (以 MHz 為單位)。
Memory	memory	定義為虛擬機器設定的記憶體 (以 MB 為單位)。 當承租人將 VDC 運算原則指派給虛擬機器時，虛擬機器會收到此屬性所定義的記憶體數量。
Number of vCPUs	cpuCount	定義為虛擬機器設定的 vCPU 數目。 當承租人將 VDC 運算原則指派給虛擬機器時，虛擬機器會收到此屬性所定義的 vCPU 數目。
Cores per Socket	coresPerSocket	虛擬機器之每個通訊端的核心數目。 VDC 運算原則中定義的 vCPU 數目必須能被每個通訊端的核心數目整除。 如果 vCPU 數目無法被每個通訊端的核心數目整除，則每個通訊端的核心數目會變得無效。
Memory Reservation Guarantee	memoryReservationGuarantee	定義為虛擬機器設定的保留記憶體數量。 屬性值的範圍介於 0 到 1 之間。 值為 0 的記憶體保留保證表示未定義任何記憶體保證。值為 1 的記憶體保留保證表示定義 100% 保留記憶體。
CPU Reservation Guarantee	cpuReservationGuarantee	定義保留虛擬機器的 CPU 資源數量。 虛擬機器的已配置 CPU 等於 vCPU 數目乘以 vCPU 速度 (以 MHz 為單位)。 屬性值的範圍介於 0 到 1 之間。值為 0 的 CPU 保留保證定義無任何 CPU 保留。值為 1 表示定義 100% 的 CPU 保留。
CPU Limit	cpuLimit	定義虛擬機器的 CPU 限制 (以 MHz 為單位)。 值為減一 (-1) 表示未定義任何 CPU 限制。 如果未在 VDC 運算原則中定義，則 CPU 限制等於虛擬機器的已配置 CPU。
Memory Limit	memoryLimit	定義虛擬機器的記憶體限制 (以 MB 為單位)。 值為 -1 定義沒有任何記憶體限制。 如果未在 VDC 運算原則中定義，則記憶體限制等於虛擬機器的已配置記憶體。
CPU Shares	cpuShares	定義虛擬機器的 CPU 共用數目。 如果未在 VDC 運算原則中定義，則會向虛擬機器套用一般共用。
Memory Shares	memoryShares	定義虛擬機器的記憶體共用數目。 如果未在 VDC 運算原則中定義，則會向虛擬機器套用一般共用。
Extra Configurations	extraConfigs	表示在虛擬機器上做為額外組態值套用的索引鍵和值配對之間的對應。
Provider VDC Compute Policy	pvdcComputePolicy	定義 VDC 運算原則對提供者 VDC 運算原則的參考。

使用虛擬資料中心運算原則

vCloud Director 將為所有虛擬資料中心 (VDC) 產生預設運算原則。預設 VDC 運算原則僅包含名稱和說明，而所有其餘的 VDC 運算原則屬性都是空的。

您也可以定義另一個 VDC 運算原則做為組織 VDC 的預設原則。預設 VDC 運算原則將會控制承租人在組織 VDC 中建立的虛擬機器 (VM) 的資源配置及耗用量，除非承租人向虛擬機器指派另一個特定的 VDC 運算原則。

若要限制承租人可為組織 VDC 內的個別虛擬機器配置的計算資源上限，雲端提供者可以定義 VDC 上限運算原則。指派給組織 VDC 時，VDC 上限運算原則可用作組織 VDC 內所有虛擬機器的計算資源組態上限。建立虛擬機器時，承租人使用者無法使用 VDC 上限運算原則。當您定義 VDC 運算原則做為 VDC 上限運算原則時，vCloud Director 會在內部複製原則內容，並將複製的內容用作 VDC 上限運算原則。如此一來，組織 VDC 不依賴於最初使用的 VDC 運算原則。

如果您向組織 VDC 發佈多個 VDC 運算原則，則建立和管理組織 VDC 中的虛擬機器時，承租人使用者可以在所有自訂原則與預設原則之間進行選取。

以下是雲端提供者的可用 VDC 運算原則作業：

- 建立 VDC 運算原則。
- 將 VDC 運算原則發佈到一或多個組織 VDC。
- 從組織 VDC 解除發佈 VDC 運算原則。
- 刪除 VDC 運算原則。

擁有 **ORG_VDC_MANAGE_COMPUTE_POLICIES** 權限的使用者可以建立、更新和發佈 VDC 運算原則。若要建立 VDC 運算原則，您可以使用 vCloud API。

下表列出了承租人使用者可用的 VDC 運算原則作業。

表 6-2. 承租人使用者的 VDC 運算原則作業

作業	描述
在建立虛擬機器期間，將 VDC 運算原則指派給虛擬機器。	有權在組織 VDC 中建立虛擬機器的承租人使用者可以選擇性地將 VDC 運算原則指派給虛擬機器。如此一來，在 VDC 運算原則中定義的參數可控制虛擬機器的 CPU 和記憶體耗用量。在建立虛擬機器期間，承租人不需要指派 VDC 運算原則。如果承租人未明確選取要指派給虛擬機器的 VDC 運算原則，則會將預設 VDC 原則套用至虛擬機器。在建立虛擬機器期間，承租人使用者可以使用 vCloud Director 租用戶入口網站，將 VDC 運算原則指派給虛擬機器。
將 VDC 運算原則指派給現有的虛擬機器。	有權管理組織 VDC 中的虛擬機器的承租人使用者可以更新虛擬機器與 VDC 運算原則之間的關聯。因此，系統會將虛擬機器重新設定為使用新的 VDC 運算原則中所指定的計算資源。承租人使用者可以使用 vCloud Director 租用戶入口網站，將 VDC 運算原則指派給現有的虛擬機器。

透過使用 VDC 運算原則，雲端提供者可以限制組織 VDC 中所有虛擬機器的計算資源耗用量，例如限制為三個預先定義的大小 (例如*小型*、*中型*和*大型*)。工作流程如下所示。

1 **系統管理員**會建立三個具有下列屬性的 VDC 運算原則：

名稱	屬性
小型	■ 說明：小型虛擬機器原則 ■ 名稱：小型 ■ 記憶體：1024 ■ vCPU 數目：1
中型	■ 說明：中型虛擬機器原則 ■ 名稱：中型 ■ 記憶體：2048 ■ vCPU 數目：2
大型	■ 說明：大型虛擬機器原則 ■ 名稱：大型 ■ 記憶體：4096 ■ vCPU 數目：4

2 向組織 VDC 發佈新的 VDC 運算原則。

向組織 VDC 發佈 VDC 運算原則，使該原則可供組織 VDC 中的承租人使用者使用。

3 或者，將其中一個 VDC 運算原則定義為組織 VDC 的預設 VDC 原則。

若您為組織 VDC 定義預設原則，並且承租人使用者在虛擬機器建立期間未指定其他原則，則會將預設原則套用至虛擬機器。

若要檢視和修改 VDC 運算原則，您必須使用 vCloud API。

建立組織虛擬資料中心

若要為組織配置資源，您必須建立組織虛擬資料中心。組織虛擬資料中心會從提供者虛擬資料中心取得其資源。一個組織可以有多個組織虛擬資料中心。

必要條件

建立提供者虛擬資料中心。請參閱《vCloud Director 管理員指南》。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下**組織 VDC**，然後按一下**新增**。

3 輸入新組織虛擬資料中心的名稱，並選擇性地輸入說明。

4 (選擇性) 若要在建立後停用新的組織虛擬資料中心，請關閉**啟用組織 VDC** 切換按鈕。

使用者無法在已停用的組織虛擬資料中心上部署 vApp。

5 按**下一步**。

6 選取要新增此虛擬資料中心的組織名稱旁邊的選項按鈕，然後按**下一步**。

7 選取希望組織虛擬資料中心從中取得計算和儲存資源的提供者虛擬資料中心名稱旁邊的選項按鈕，然後按**下一步**。

提供者虛擬資料中心清單顯示站台中所有已啟用的提供者虛擬資料中心以及可用資源的相關資訊。網路清單顯示可供選取的提供者虛擬資料中心使用的網路相關資訊。

8 為此組織虛擬資料中心選取配置模型，然後按**下一步**。

選項	描述
配置集區	您從提供者虛擬資料中心配置的資源中有一部分會認可給組織虛擬資料中心。您可以指定 CPU 與記憶體的百分比。
隨收隨付	當使用者於組織虛擬資料中心中建立 vApp 時才會認可資源。
保留集區	您所配置的所有資源會立即認可給組織虛擬資料中心。
Flex	您可以控制 VDC 和個別虛擬機器層級的資源耗用量。彈性配置模型支援組織 VDC 運算原則的功能。彈性配置模型支援其他配置模型中可用的所有配置組態。

9 為選取的配置模型進行配置設定，然後按**下一步**。

選項	描述	配置模型
彈性	啟用或停用彈性集區功能。彈性的組織 vDC 可以跨越和使用與其提供者 vDC 相關聯的所有資源集區。	Flex
包含虛擬機器記憶體負載	包含或排除記憶體負載。	Flex
CPU 配置	您想要配置給在此組織虛擬資料中心中執行的虛擬機器的 CPU 數量上限。	■ 配置集區 ■ 保留集區 ■ Flex
允許 CPU 資源增加超過	若要向此組織虛擬資料中心提供無限制的 CPU 資源，請開啟此切換按鈕。	保留集區
CPU 配額	此組織虛擬資料中心的 CPU 耗用量上限。	■ 隨收隨付 ■ Flex
保證的 CPU 資源	您想要保證配置給在此組織虛擬資料中心中執行的虛擬機器的 CPU 資源百分比。您可以透過保證低於 100% 的方式控制過度認可 CPU 資源。 針對「配置集區」配置模型，百分比保證還決定了為此組織虛擬資料中心認可的 CPU 配置百分比。	■ 配置集區 ■ 隨收隨付 ■ Flex
vCPU 速度	vCPU 速度。執行於組織虛擬資料中心的虛擬機器將獲指派此數量的 GHz (每 vCPU)。	■ 隨收隨付 ■ Flex
記憶體配置	您想要配置給在此組織虛擬資料中心中執行的虛擬機器的記憶體數量上限。	■ 配置集區 ■ 保留集區
記憶體配額	此組織虛擬資料中心的記憶體耗用量上限。	■ 隨收隨付 ■ Flex

選項	描述	配置模型
保證的記憶體資源	您想要保證配置給在組織虛擬資料中心中執行的虛擬機器的記憶體資源百分比。您可以透過保證低於 100% 的方式過度認可資源。 針對「配置集區」配置模型，百分比保證還決定了為此組織虛擬資料中心認可的記憶體配置百分比。	■ 配置集區 ■ 隨收隨付 ■ Flex
虛擬機器數目上限	輸入組織虛擬資料中心中可存在的虛擬機器數目上限。	■ 配置集區 ■ 隨收隨付 ■ 保留集區 ■ Flex

10 為此組織虛擬資料中心進行儲存區設定，然後按**下一步**。

此清單中包含來源提供者虛擬資料中心上已啟用的儲存區原則。

a 選取您想要新增到此組織虛擬資料中心的一或多個儲存區原則的核取方塊。

b (選擇性) 若要限制針對所選儲存區原則配置的儲存區容量，請從**配置類型**儲存格中的下拉式功能表選取**受限制**，然後在**配置的儲存區**儲存格中輸入容量上限。

c (選擇性) 若要變更預設儲存區原則，請從**預設的具現化原則**下拉式功能表中，選取目標預設儲存區原則。

vCloud Director 將預設儲存區原則用於所有虛擬機器佈建作業，這些作業均未在虛擬機器或 vApp 範本層級指定儲存區原則。

d (選擇性) 若要針對組織虛擬資料中心的虛擬機器啟用精簡佈建，請開啟**精簡佈建**切換按鈕。

e (選擇性) 若要針對組織虛擬資料中心的虛擬機器停用快速佈建，請關閉**快速佈建**切換按鈕。

11 為此組織虛擬資料中心進行網路集區設定，然後按**下一步**。

vCloud Director 使用網路集區來建立 vApp 網路及內部組織虛擬資料中心網路。

- 若要在此階段跳過新增網路集區，請關閉**使用網路集區**切換按鈕。
- 若要設定網路集區，請選取目標網路集區的名稱旁邊的選項按鈕，然後輸入此組織虛擬資料中心的配額。

  配額是指此網路集區支援的組織虛擬資料中心內已佈建網路的數目上限。不得超過可用於所選網路集區的網路數目。

12 檢閱**即將完成**頁面，然後按一下**完成**。

啟用或停用組織虛擬資料中心

若要防止其他 vApp 和虛擬機器使用組織虛擬資料中心的計算與儲存資源，您可以停用此組織虛擬資料中心。執行中 vApp 與開啟電源虛擬機器會繼續執行，但您無法建立或啟動其他 vApp 或虛擬機器。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下**組織 VDC**。

3 選取目標組織虛擬資料中心名稱旁邊的選項按鈕，然後按一下**啟用**或**停用**。

4 按一下**確定**以確認。

刪除組織虛擬資料中心

若要從組織移除組織虛擬資料中心的所有資源，您可以刪除此組織虛擬資料中心。資源在來源提供者虛擬資料中心中不受影響。

重要 此作業將永久移除組織虛擬資料中心及其所有虛擬機器、vApp、組織虛擬資料中心網路和 Edge 閘道。

必要條件

如果您想要保留屬於目標組織虛擬資料中心的特定虛擬機器、vApp、vApp 範本或媒體檔案，請將其移到另一個組織虛擬資料中心。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下**組織 VDC**。

3 選取要移除之組織虛擬資料中心名稱旁邊的選項按鈕，然後按一下**刪除**。

4 如果此組織虛擬資料中心包含任何資源，例如虛擬機器、vApp、組織虛擬資料中心網路和 Edge 閘道，請選取每種資源類型對應的核取方塊以確認將其移除。

5 按一下**刪除**以確認。

修改組織虛擬資料中心的名稱和說明

隨著 vCloud Director 安裝擴充，您可能想為現有組織虛擬資料中心指派更有意義的名稱或說明。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下**組織 VDC**，然後按一下目標組織虛擬資料中心的名稱。

3 在**一般**索引標籤的右上角，按一下**編輯**。

4 輸入新名稱和說明，然後按一下**儲存**。

修改組織虛擬資料中心的配置模型設定

您無法變更組織虛擬資料中心的配置模型，但您可以針對在建立組織虛擬資料中心期間所指定的配置模型，變更配置設定。

您可以針對在建立組織虛擬資料中心期間所設定的配置模型，修改配置設定。請參閱 步驟 9。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下**組織 VDC**，然後按一下目標組織虛擬資料中心的名稱。

3 在**配置**索引標籤的右上角，按一下**編輯**。

4 編輯配置模型設定，然後按一下**儲存**。

修改組織虛擬資料中心的儲存區設定

您可以修改在建立組織虛擬資料中心期間所設定的儲存區設定。

修改組織虛擬資料中心的虛擬機器佈建設定

您可以修改在建立組織虛擬資料中心期間所設定的虛擬機器精簡佈建和快速佈建設定。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下**組織 VDC**，然後按一下目標組織虛擬資料中心的名稱。

3 在**儲存區**索引標籤的右上角，按一下**編輯**。

4 (選擇性) 修改精簡佈建設定。

- 若要針對組織虛擬資料中心的虛擬機器停用精簡佈建，請關閉**精簡佈建**切換按鈕。
- 若要針對組織虛擬資料中心的虛擬機器啟用精簡佈建，請開啟**精簡佈建**切換按鈕。

5 (選擇性) 修改快速佈建設定。

- 若要針對組織虛擬資料中心的虛擬機器啟用快速佈建，請開啟**快速佈建**切換按鈕。
- 若要針對組織虛擬資料中心的虛擬機器停用快速佈建，請關閉**快速佈建**切換按鈕。

6 按一下**編輯**。

將虛擬機器儲存區原則新增至組織虛擬資料中心

您可以設定組織虛擬資料中心，以支援您先前新增至支援提供者虛擬資料中心的虛擬機器儲存區原則。

必要條件

已將目標虛擬機器儲存區原則新增至來源提供者虛擬資料中心。請參閱將虛擬機器儲存區原則新增至提供者虛擬資料中心。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下**組織 VDC**，然後按一下目標組織虛擬資料中心的名稱。

3 按一下**儲存區**索引標籤，然後按一下**新增**。

您可以查看來源提供者虛擬資料中心的其他可用儲存區原則的清單。

4 選取一或多個要新增的儲存區原則的核取方塊，然後按一下**新增**。

變更組織虛擬資料中心上的預設儲存區原則

您可以變更在建立組織虛擬資料中心期間所設定的預設儲存區原則。

vCloud Director 將預設儲存區原則用於所有虛擬機器佈建作業，這些作業均未在虛擬機器或 vApp 範本層級指定儲存區原則。

必要條件

- 目標預設儲存區原則已新增至組織虛擬資料中心。請參閱 將虛擬機器儲存區原則新增至組織虛擬資料中心。
- 組織虛擬資料中心上已啟用目標預設儲存區原則。請參閱 啟用或停用組織虛擬資料中心上的儲存區原則。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下**組織 VDC**，然後按一下目標組織虛擬資料中心的名稱。

3 按一下**儲存區**索引標籤。

4 按一下目標預設儲存區原則名稱旁邊的選項按鈕，然後按一下**設定為預設值**。

5 按一下**確定**以確認。

編輯組織虛擬資料中心上儲存區原則的限制

您可以變更在建立組織虛擬資料中心期間為儲存區原則設定的已配置儲存區容量的限制。

您可以將已配置的儲存區容量設定為無限制，也可以為組織虛擬資料中心上的儲存區原則設定已配置儲存區容量的上限。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下**組織 VDC**，然後按一下目標組織虛擬資料中心的名稱。

3 按一下**儲存區**索引標籤。

4 按一下目標儲存區原則名稱旁邊的選項按鈕，然後按一下**編輯限制**。

5 設定此儲存區原則的限制設定。

- 若要設定限制，請選取上方的選項按鈕，然後針對此組織虛擬資料中心上的此儲存區原則輸入儲存資源的數量上限。
- 若要設定無限制，請選取**無限制**選項按鈕。

6 按一下**編輯**。

修改組織虛擬資料中心上的虛擬機器儲存區原則的中繼資料

您可以新增、編輯和刪除組織虛擬資料中心上儲存區原則的中繼資料。

透過使用物件中繼資料，您可以將使用者定義的 *name=value* 配對與組織虛擬資料中心上的儲存區原則建立關聯。您可以在 vCloud API 查詢篩選器運算式中使用物件中繼資料。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下**組織 VDC**，然後按一下目標組織虛擬資料中心的名稱。

3 按一下**儲存區**索引標籤。

4 按一下目標儲存區原則名稱旁邊的選項按鈕，然後按一下**中繼資料**。

5 按一下**編輯**。

6 (選擇性) 若要新增索引鍵-值配對，請按一下**新增**，輸入名稱和值，然後選取新索引鍵-值配對的類型。

7 (選擇性) 若要編輯索引鍵-值配對，輸入新名稱和值，並為索引鍵-值配對選取新類型。

8 (選擇性) 若要移除索引鍵-值配對，請在資料列的右側按一下**刪除**圖示。

9 按一下**儲存**，然後按一下**確定**。

啟用或停用組織虛擬資料中心上的儲存區原則

若要防止其他 vApp 和虛擬機器使用組織虛擬資料中心上的儲存區原則，您可以停用組織虛擬資料中心上的此儲存區原則。執行中 vApp 與開啟電源的虛擬機器會繼續執行，但您無法在此儲存區原則上建立或啟動其他 vApp 或虛擬機器。

您無法停用預設儲存區原則。

必要條件

如果您想要停用預設儲存區原則，變更組織虛擬資料中心上的預設儲存區原則。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下**組織 VDC**，然後按一下目標組織虛擬資料中心的名稱。

3 按一下**儲存區**索引標籤。

4 按一下目標儲存區原則名稱旁邊的選項按鈕，然後按一下**啟用**或**停用**。

5 按一下**確定**以確認。

從組織虛擬資料中心刪除儲存區原則

若要防止組織虛擬資料中心使用儲存區原則，您可以從組織虛擬資料中心移除此儲存區原則。執行中 vApp 與開啟電源的虛擬機器會繼續執行，但您無法在此儲存區原則上建立或啟動其他 vApp 或虛擬機器。

必要條件

停用您要移除的儲存區原則。請參閱 啟用或停用組織虛擬資料中心上的儲存區原則。

程序

1. 從主功能表 (☰) 中，選取**雲端資源**。
2. 在左面板中，按一下**組織 VDC**，然後按一下目標組織虛擬資料中心的名稱。
3. 按一下**儲存區**索引標籤。
4. 按一下目標儲存區原則名稱旁邊的選項按鈕，然後按一下**移除**。
5. 按一下**移除**以確認。

編輯組織虛擬資料中心的網路設定

您可以變更在組織虛擬資料中心中佈建新網路的網路集區。也可以啟用組織虛擬資料中心，以符合跨虛擬資料中心網路的資格。

網路集區為一組無差異網路，可用來建立 vApp 網路、路由組織 VDC 網路及內部組織 VDC 網路。您可以變更新網路的網路集區。現有網路會繼續使用舊的網路集區。

透過針對跨虛擬資料中心網路啟用的組織虛擬資料中心，具有相關權限的組織使用者可以建立資料中心群組以及在這些群組中建立延伸的第 2 層網路。

必要條件

如果您想要針對組織虛擬資料中心啟用跨 VDC 網路，請確認已在支援提供者虛擬資料中心設定跨 vCenter NSX。

程序

1. 從主功能表 (☰) 中，選取**雲端資源**。
2. 在左面板中，按一下**組織 VDC**，然後按一下目標組織虛擬資料中心的名稱。
3. 在**網路集區**索引標籤的右上角，按一下**編輯**。

   您可以看到此組織虛擬資料中心所使用的網路數目。
4. (選擇性) 設定此組織虛擬資料中心的網路集區設定。
   - 如果您不想使用此組織虛擬資料中心的網路集區，請關閉**使用網路集區**切換按鈕。
   - 如果您想要設定此組織虛擬資料中心的網路集區，請遵循下列步驟：
     a 開啟**使用網路集區**切換按鈕。

您可以查看可用網路集區的清單及其使用量、可用網路和容量的相關資訊。

b 選取目標資源集區名稱旁邊的選項按鈕。

c 針對此組織虛擬資料中心中的此網路集區設定配額。

配額是已佈建網路的數目上限。不得超過可用於所選網路集區的網路數目。

5 若要針對此組織虛擬資料中心啟用跨虛擬資料中心網路，請開啟**跨 VDC 網路**切換按鈕。

6 按一下**儲存**。

結果

在 vCloud Director 租用戶入口網站中，已啟用跨虛擬資料中心網路的虛擬資料中心顯示在用於建立資料中心群組的資料中心清單中。如需建立資料中心群組的相關資訊，請參閱《vCloud Director 租用戶入口網站指南》。

修改組織虛擬資料中心的中繼資料

您可以新增、編輯和刪除組織虛擬資料中心的中繼資料。

透過使用物件中繼資料，您可以將使用者定義的 *name=value* 配對與組織虛擬資料中心建立關聯。您可以在 vCloud API 查詢篩選器運算式中使用物件中繼資料。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下**組織 VDC**，然後按一下目標組織虛擬資料中心的名稱。

3 按一下**中繼資料**索引標籤。

4 按一下**編輯**。

5 (選擇性) 若要新增索引鍵-值配對，請按一下**新增**，輸入名稱和值，然後選取新索引鍵-值配對的類型。

6 (選擇性) 若要編輯索引鍵-值配對，輸入新名稱和值，並為索引鍵-值配對選取新類型。

7 (選擇性) 若要移除索引鍵-值配對，請在資料列的右側按一下**刪除**圖示。

8 按一下**儲存**，然後按一下**確定**。

檢視組織虛擬資料中心的資源集區

您可以檢視組織虛擬資料中心使用的 vCenter Server 資源集區的清單。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下**組織 VDC**，然後按一下目標組織虛擬資料中心的名稱。

3 按一下**資源集區**索引標籤。

結果

您可以看到一張資料表，其中包含組織虛擬資料中心正在使用的資源集區和每個資源集區所屬的 vCenter Server 執行個體。

在組織虛擬資料中心上管理 Distributed Firewall

若要在組織虛擬資料中心提供第 3 層和第 2 層網路安全性，您可以為此組織虛擬資料中心上的 Distributed Firewall 啟用和建立規則。透過 Distributed Firewall 規則，您可以保護在組織虛擬資料中心的虛擬機器之間傳輸的流量。

vCloud Director 支援受 NSX Data Center for vSphere 支援的組織虛擬資料中心上的分散式防火牆服務。

您可以使用各種群組物件和安全群組來建立 Distributed Firewall 規則。請參閱自訂群組物件與使用安全群組。

如需保護進出 Edge 閘道之流量的相關資訊，請參閱管理 Edge 閘道防火牆。

啟用組織虛擬資料中心上的 Distributed Firewall

必須在組織虛擬資料中心上啟用 Distributed Firewall，才能在此組織虛擬資料中心上管理 Distributed Firewall 設定。

vCloud Director 支援受 NSX Data Center for vSphere 支援的組織虛擬資料中心上的分散式防火牆服務。

程序

1. 從主功能表 (☰) 中，選取**雲端資源**。
2. 在左面板中，按一下**組織 VDC**。
3. 按一下目標組織虛擬資料中心旁邊的選項按鈕，然後按一下**管理防火牆**。
4. 在 **Distributed Firewall** > **一般**索引標籤上，開啟**啟用 Distributed Firewall** 切換按鈕。

結果

您可以查看預設防火牆規則，這些規則允許所有第 3 層和第 2 層流量通過組織虛擬資料中心。

- 在 **Distributed Firewall** > **一般**索引標籤上，您可以查看第 3 層流量的預設 Distributed Firewall 規則，名為 Default Allow Rule。
- 在 **Distributed Firewall** > **乙太網路**索引標籤上，您可以看到第 2 層流量的預設 Distributed Firewall 規則的名稱為 Default Allow Rule。

新增 Distributed Firewall 規則

首先將 Distributed Firewall 規則新增至組織虛擬資料中心範圍內。然後，您可以縮小要套用規則的範圍。Distributed Firewall 可讓您在來源和目的地層級針對每個規則新增多個物件，這有助於減少要新增的防火牆規則總數。

如需可在規則使用中的預先定義的服務和服務群組的相關資訊，請參閱檢視可用於防火牆規則的服務和檢視可用於防火牆規則的服務群組。

必要條件

- 啟用組織虛擬資料中心上的 Distributed Firewall
- 如果您想要使用 IP 集做為規則中的來源或目的地，建立用於防火牆規則和 DHCP 轉送組態的 IP 集。
- 如果您想要使用 MAC 集做為規則中的來源或目的地，建立用於防火牆規則的 MAC 集。
- 如果您想要使用安全群組做為規則中的來源或目的地，建立安全群組。

程序

1. 從主功能表 (☰) 中，選取**雲端資源**。
2. 在左面板中，按一下**組織 VDC**。
3. 按一下目標組織虛擬資料中心旁邊的選項按鈕，然後按一下**管理防火牆**。
4. 選取要建立的規則類型。您可以選擇建立一般規則或乙太網路規則。

   第 3 層 (L3) 規則會在**一般**索引標籤上設定。第 2 層 (L2) 規則會在**乙太網路**索引標籤上設定。
5. 若要在防火牆資料表中的現有規則下方新增某個規則，請按一下現有的資料列，然後按一下**建立** (+) 按鈕。

   新規則的資料列會新增至所選規則下方，並且預設獲指派任何目的地、任何服務和**允許**動作。如果系統定義的預設允許規則是防火牆資料表中的唯一規則，新規則便會新增到預設規則之上。
6. 按一下**名稱**儲存格，然後輸入名稱。
7. 按一下**來源**儲存格，並使用現在顯示的圖示來選取要新增至規則的來源：

動作	描述
按一下 IP 圖示	適用於**一般**索引標籤上定義的規則。 輸入您想要使用的來源值。有效值為 IP 位址、CIDR、IP 範圍或關鍵字 **any**。Distributed Firewall 僅支援 IPv4 格式。
按一下 + 圖示	使用 **+** 圖示將來源指定為除特定 IP 位址以外的物件： ■ 使用**選取物件**視窗新增符合您選取項目的物件，然後按一下**保留**將其新增至規則。 ■ 若要從規則中排除某個來源，請使用**選取物件**視窗將其新增到此規則，然後選取切換排除圖示以從此規則中排除此來源。 在來源上選取切換排除時，此規則會套用至來自除了已排除來源以外的所有來源的流量。如果未選取切換排除，此規則會套用至來自**選取物件**視窗中所指定來源的流量。

8 按一下**目的地**儲存格，然後執行下列其中一個動作：

動作	描述
按一下 IP 圖示	適用於**一般**索引標籤上定義的規則。 輸入您想要使用的目的地值。有效值為 IP 位址、CIDR、IP 範圍或關鍵字 **any**。Distributed Firewall 僅支援 IPv4 格式。
按一下 + 圖示	使用 **+** 圖示將來源指定為除特定 IP 位址以外的物件： ■ 使用**選取物件**視窗新增符合您選取項目的物件，然後按一下**保留**將其新增至規則。 ■ 若要從規則中排除某個來源，請使用 [選取物件] 視窗將其新增到此規則，然後選取切換排除圖示以從此規則中排除此來源。 在來源上選取切換排除時，此規則會套用至來自除了已排除來源以外的所有來源的流量。如果未選取切換排除，此規則會套用至來自**選取物件**視窗中所指定來源的流量。

9 按一下新規則的**服務**儲存格，然後執行下列其中一個動作：

動作	描述
按一下 IP 圖示	以連接埠–通訊協定組合形式指定服務： a 選取服務通訊協定。 b 輸入來源和目的地連接埠的連接埠號碼，或指定 **any**，然後按一下**保留**。
按一下 + 圖示	若要選取預先定義的服務或服務群組，或定義新的服務或服務群組： a 選取一或多個物件，然後將其新增至篩選器。 b 按一下**保留**。

10 在新規則的**動作**儲存格中，設定規則的動作。

選項	描述
允許	允許流出或流入指定來源、目的地和服務的流量。
拒絕	封鎖流出或流入指定來源、目的地和服務的流量。

11 在新規則的**方向**儲存格中，選取此規則是否套用至傳入流量和/或傳出流量。

12 如果此為**一般**索引標籤上的規則，請在新規則的**封包類型**儲存格中，選取**任何**、**IPV4** 或 **IPV6** 封包類型。

13 選取**套用至**儲存格，並使用 **+** 圖示定義此規則適用的物件範圍。

備註 當規則包含**來源**和**目的地**儲存格中的虛擬機器時，您必須同時將來源和目的地虛擬機器新增至規則的**套用至**，才能使規則正常運作。

14 按一下**儲存變更**。

編輯 Distributed Firewall 規則

在 vCloud Director 環境中，若要修改組織虛擬資料中心的現有 Distributed Firewall 規則，請使用 **Distributed Firewall** 畫面。

如需有關可用於各種規則儲存格之設定的詳細資料，請參閱新增 Distributed Firewall 規則。

程序

1. 從主功能表 (☰) 中，選取**雲端資源**。
2. 在左面板中，按一下**組織 VDC**。
3. 按一下目標組織虛擬資料中心旁邊的選項按鈕，然後按一下**管理防火牆**。
4. 執行下列任何動作以管理 Distributed Firewall 規則：
   - 透過按一下**編號**儲存格中的綠色核取記號停用規則。

     綠色核取記號會變成紅色的已停用圖示。如果規則已停用並且您想要啟用此規則，請按一下紅色的已停用圖示。
   - 透過按兩下規則的**名稱**儲存格並輸入新名稱，編輯規則名稱。
   - 透過選取適當的儲存格並使用顯示的控制項來修改規則設定，例如來源或動作設定。
   - 選取一個規則，然後按一下規則資料表上方的**刪除** () 按鈕以刪除規則。
   - 透過選取規則，然後按一下位於規則資料表上方的向上和向下箭頭按鈕，可在規則資料表中將該規則上移或下移。
5. 按一下**儲存變更**。

自訂群組物件

vCloud Director 環境中的 NSX 軟體提供定義特定實體之集合與群組的功能，可供您在指定其他網路相關組態 (例如在防火牆規則中) 時加以使用。

建立用於防火牆規則和 DHCP 轉送組態的 IP 集

IP 集是可在組織虛擬資料中心層級建立的一組 IP 位址。您可以使用 IP 集做為防火牆規則或 DHCP 轉送組態中的來源或目的地。

您可以使用**群組物件**頁面建立 IP 集。若要開啟此頁面，您必須導覽至組織 VDC 的 Distributed Firewall 設定，或屬於組織 VDC 之 Edge 閘道的服務設定。

程序

1 開啟**群組物件**頁面。

選項	動作
從組織 VDC 的 Distributed Firewall 設定	a 從主功能表 (☰) 中，選取**雲端資源**。 b 在左面板中，按一下**組織 VDC**。 c 選取目標組織虛擬資料中心名稱旁邊的選項按鈕，然後按一下**管理防火牆**。 d 按一下**群組物件**索引標籤。
從組織 VDC 上的 Edge 閘道的服務設定	a 從主功能表 (☰) 中，選取**雲端資源**。 b 在左面板中，按一下 **Edge 閘道**。 c 選取屬於目標組織虛擬資料中心的 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。 d 按一下**群組物件**索引標籤。

2 按一下 **IP 集**索引標籤。

畫面上將會顯示已定義的 IP 集。

3 若要新增 IP 集，請按一下**建立** (+) 按鈕。

4 輸入 IP 集的名稱和選擇性說明，以及要包含在此集中的 IP 位址。

5 若要儲存此 IP 集，請按一下**保留**。

結果

新 IP 集可選取做為防火牆規則或 DHCP 轉送組態中的來源或目的地。

建立用於防火牆規則的 MAC 集

MAC 集是一組可在組織虛擬資料中心層級建立的 MAC 位址。您可以使用 MAC 集做為防火牆規則中的來源或目的地。

您可以使用**群組物件**頁面建立 MAC 集。若要開啟此頁面，您必須導覽至組織 VDC 的 Distributed Firewall 設定，或屬於組織 VDC 之 Edge 閘道的服務設定。

程序

1 開啟**群組物件**頁面。

選項	動作
從組織 VDC 的 Distributed Firewall 設定	a 從主功能表 (☰) 中，選取**雲端資源**。 b 在左面板中，按一下**組織 VDC**。 c 選取目標組織虛擬資料中心名稱旁邊的選項按鈕，然後按一下**管理防火牆**。 d 按一下**群組物件**索引標籤。
從組織 VDC 上的 Edge 閘道的服務設定	a 從主功能表 (☰) 中，選取**雲端資源**。 b 在左面板中，按一下 **Edge 閘道**。 c 選取屬於目標組織虛擬資料中心的 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。 d 按一下**群組物件**索引標籤。

2 按一下 **MAC 集**索引標籤。

畫面上將會顯示已定義的 MAC 集。

3 若要新增 MAC 集，請按一下**建立** (+) 按鈕。

4 輸入集的名稱、說明 (選擇性) 以及要包含在集中的 MAC 位址。

5 若要儲存 MAC 集，請按一下**保留**。

結果

新 MAC 集可選取做為防火牆規則中的來源或目的地。

檢視可用於防火牆規則的服務

您可以檢視可用於防火牆規則的服務清單。在此內容中，服務是通訊協定與連接埠的組合。

您可以使用**群組物件**頁面檢視可用的服務。若要開啟此頁面，您必須導覽至組織 VDC 的 Distributed Firewall 設定，或屬於組織 VDC 之 Edge 閘道的服務設定。

程序

1 開啟**群組物件**頁面。

選項	動作
從組織 VDC 的 Distributed Firewall 設定	a 從主功能表 (☰) 中，選取**雲端資源**。 b 在左面板中，按一下**組織 VDC**。 c 選取目標組織虛擬資料中心名稱旁邊的選項按鈕，然後按一下**管理防火牆**。 d 按一下**群組物件**索引標籤。
從組織 VDC 上的 Edge 閘道的服務設定	a 從主功能表 (☰) 中，選取**雲端資源**。 b 在左面板中，按一下 **Edge 閘道**。 c 選取屬於目標組織虛擬資料中心的 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。 d 按一下**群組物件**索引標籤。

2 按一下**服務**索引標籤。

結果

可用服務即會顯示在畫面上。

檢視可用於防火牆規則的服務群組

您可以檢視可用於防火牆規則的服務群組清單。在此內容中，服務是通訊協定與連接埠的組合，而服務群組是一組服務或其他服務群組。

您可以使用**群組物件**頁面檢視可用的服務群組。若要開啟此頁面，您必須導覽至組織 VDC 的 Distributed Firewall 設定，或屬於組織 VDC 之 Edge 閘道的服務設定。

程序

1 開啟**群組物件**頁面。

選項	動作
從組織 VDC 的 Distributed Firewall 設定	a 從主功能表 (☰) 中，選取**雲端資源**。 b 在左面板中，按一下**組織 VDC**。 c 選取目標組織虛擬資料中心名稱旁邊的選項按鈕，然後按一下**管理防火牆**。 d 按一下**群組物件**索引標籤。
從組織 VDC 上的 Edge 閘道的服務設定	a 從主功能表 (☰) 中，選取**雲端資源**。 b 在左面板中，按一下 **Edge 閘道**。 c 選取屬於目標組織虛擬資料中心的 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。 d 按一下**群組物件**索引標籤。

2 按一下**服務群組**索引標籤。

結果

可用服務群組將會顯示在畫面上。[說明] 資料行會顯示分組到各服務群組的服務。

使用安全群組

安全群組是資產或群組物件的集合，例如虛擬機器、組織虛擬資料中心網路或安全性標籤。

安全群組可具有以安全性標籤、虛擬機器名稱、虛擬機器客體作業系統名稱或虛擬機器客體主機名稱為基礎的動態成員資格準則。例如，具有安全性標籤「web」的所有虛擬機器都會自動新增至傳送到 Web 伺服器的特定安全群組。建立安全群組後，安全性原則將會套用至該群組。

建立安全群組

您可以建立使用者定義的安全群組。

必要條件

如果您要搭配使用安全性標籤與安全群組，建立並指派安全性標籤。

程序

1. 從主功能表 (☰) 中，選取**雲端資源**。
2. 在左面板中，按一下**組織 VDC**。
3. 按一下目標組織虛擬資料中心旁邊的選項按鈕，然後按一下**管理防火牆**。
4. 按一下**群組物件 > 安全群組**索引標籤。
5. 按一下**建立** (+) 按鈕。
6. 輸入安全群組的名稱，並選擇性地輸入說明。

   此說明會顯示在安全群組的清單中，因此新增有意義的說明可讓您輕鬆、快速地識別安全群組。
7. (選擇性) 新增動態成員集。
   a. 按一下 [動態成員集] 下的**新增** (+) 按鈕。
   b. 選取是否符合陳述式中的**任何**或**全部**準則。
   c. 輸入要相符的第一個物件。

      選項包括**安全性標籤**、**虛擬機器客體作業系統名稱**、**虛擬機器名稱**和**虛擬機器客體主機名稱**。
   d. 選取運算子，如**包含**、**開頭為**或**結尾為**。
   e. 輸入值。
   f. (選擇性) 若要新增另一個陳述式，請使用布林運算子 **And** 或 **Or**。

8 (選擇性) 包含成員。

a 從**瀏覽以下類型的物件**下拉式功能表中，選取物件類型，如**虛擬機器**、**組織 VDC 網路**、**IP 集**、**MAC 集**或**安全性標籤**。

b 若要在 [包含成員] 清單中包含物件，請從左面板中選取物件，然後按一下向右箭頭將其移到右面板。

9 (選擇性) 排除成員。

a 從**瀏覽以下類型的物件**下拉式功能表中，選取物件類型，如**虛擬機器**、**組織 VDC 網路**、**IP 集**、**MAC 集**或**安全性標籤**。

b 若要在 [排除成員] 清單中包含物件，請從左面板中選取物件，然後按一下向右箭頭將其移到右面板。

10 按一下**保留**以保留變更。

此作業可能需要一些時間才能完成。

結果

安全群組目前可以在規則中使用，例如防火牆規則。

編輯安全群組

您可以編輯使用者定義的安全群組。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下**組織 VDC**。

3 按一下目標組織虛擬資料中心旁邊的選項按鈕，然後按一下**管理防火牆**。

4 按一下**群組物件 > 安全群組**索引標籤。

5 選取您要編輯的安全群組。

安全群組的詳細資料會顯示在安全群組清單下方。

6 (選擇性) 編輯安全群組的名稱和說明。

7 (選擇性) 新增動態成員集。

a 按一下**動態成員集**下的**新增** () 按鈕。

b 選取是否符合陳述式中的**任何**或**全部**準則。

c 輸入要相符的第一個物件。

選項包括**安全性標籤**、**虛擬機器客體作業系統名稱**、**虛擬機器名稱**和**虛擬機器客體主機名稱**。

d 選取運算子，如**包含**、**開頭為**或**結尾為**。

e 輸入值。

f (選擇性) 若要新增另一個陳述式，請使用布林運算子 **And** 或 **Or**。

8 (選擇性) 透過按一下要編輯的成員集旁邊的**編輯** (⚙) 圖示來編輯動態成員集。

a 將必要的變更套用到動態成員集。

b 按一下**確定**。

9 (選擇性) 透過按一下要刪除的成員集旁邊的**刪除** (✖) 圖示來刪除動態成員集。

10 (選擇性) 透過按一下 [包含成員] 清單旁邊的**編輯** (⚙) 圖示來編輯所包含成員的清單。

a 從**瀏覽以下類型的物件**下拉式功能表中，選取物件類型，如**虛擬機器**、**組織 VDC 網路**、**IP 集**、**MAC 集**或**安全性標籤**。

b 若要在 [包含成員] 清單中包含物件，請從左面板中選取物件，然後按一下向右箭頭將其移到右面板。

c 若要將某個物件排除在 [包含成員] 清單之外，請從右面板中選取物件，然後按一下向左箭頭將其移至左面板。

11 (選擇性) 透過按一下 [排除成員] 清單旁邊的**編輯** (⚙) 圖示來編輯所排除成員的清單。

a 從**瀏覽以下類型的物件**下拉式功能表中，選取物件類型，如**虛擬機器**、**組織 VDC 網路**、**IP 集**、**MAC 集**或**安全性標籤**。

b 若要在 [排除成員] 清單中包含物件，請從左面板中選取物件，然後按一下向右箭頭將其移到右面板。

c 若要將某個物件排除在 [排除成員] 清單之外，請從右面板中選取物件，然後按一下向左箭頭將其移至左面板。

12 按一下**儲存變更**。

將會儲存安全群組的變更。

刪除安全群組

您可以刪除使用者定義的安全群組。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下**組織 VDC**。

3 按一下目標組織虛擬資料中心旁邊的選項按鈕，然後按一下**管理防火牆**。

4 按一下**群組物件 > 安全群組**索引標籤。

5 選取您要刪除的安全群組。

6 按一下**刪除** (✖) 按鈕。

7 按一下**確定**以確認刪除。

結果

將會刪除安全群組。

使用安全性標籤

安全性標籤是可與一個虛擬機器或虛擬機器群組相關聯的標籤。安全性標籤設計為與安全群組搭配使用。一旦建立安全性標籤，便可將其與防火牆規則中所使用的安全群組相關聯。您可以建立、編輯或指派使用者定義的安全性標籤。也可以檢視哪些虛擬機器或安全群組已套用特定的安全性標籤。

安全性標籤的常見使用案例是以動態方式分組物件來簡化防火牆規則。例如，您可以根據在指定虛擬機器上預期發生的活動類型建立數個不同的安全性標籤。為資料庫伺服器建立一個安全性標籤，並且為電子郵件伺服器建立另一個安全性標籤。然後，將適當的標籤套用至容納資料庫伺服器或電子郵件伺服器的虛擬機器。稍後，可將標籤指派給安全群組並據此撰寫防火牆規則，從而根據虛擬機器正在執行的是資料庫伺服器還是電子郵件伺服器來套用不同的安全性設定。之後，如果您變更虛擬機器功能，可以從安全性標籤移除虛擬機器，而非編輯防火牆規則。

建立並指派安全性標籤

您可以建立安全性標籤，並將其指派給一個虛擬機器或一組虛擬機器。

您可以建立安全性標籤，並將其指派給一個虛擬機器或一組虛擬機器。

程序

1. 從主功能表 (☰) 中，選取**雲端資源**。
2. 在左面板中，按一下**組織 VDC**。
3. 按一下目標組織虛擬資料中心旁邊的選項按鈕，然後按一下**管理防火牆**。
4. 按一下**安全性標籤**索引標籤。
5. 按一下**建立** (+) 按鈕，然後輸入安全性標籤的名稱。
6. (選擇性) 輸入安全性標記的描述。
7. (選擇性) 將安全性標籤指派給一個虛擬機器或一組虛擬機器。

   在**瀏覽以下類型的物件**下拉式功能表中，預設會選取**虛擬機器**。

   a 從左面板中選取虛擬機器。

   b 按一下向右箭頭，將安全性標籤指派給所選的虛擬機器。

   此虛擬機器將移到右面板，並獲指派安全性標籤。
8. 完成將標籤指派給所選虛擬機器後，按一下**保留**。

結果

安全性標籤已建立，如果您選擇，將會指派給所選虛擬機器。

後續步驟

安全性標籤設計為與安全群組搭配使用。如需有關建立安全群組的詳細資訊，請參閱建立安全群組。

變更安全性標籤指派

建立安全性標籤後，您可以手動將其指派給虛擬機器。您也可以編輯安全性標籤，以將其從已獲指派的虛擬機器中移除。

如果您已建立安全性標籤，可以將其指派給虛擬機器。您可以使用安全性標籤來分組虛擬機器，以撰寫防火牆規則。例如，您可能會將安全性標籤指派給一組包含高度敏感資料的虛擬機器。

程序

1. 從主功能表 (☰) 中，選取**雲端資源**。
2. 在左面板中，按一下**組織 VDC**。
3. 按一下目標組織虛擬資料中心旁邊的選項按鈕，然後按一下**管理防火牆**。
4. 按一下**安全性標籤**索引標籤。
5. 從安全性標籤清單中，選取要編輯的安全性標籤，然後按一下**編輯** () 按鈕。
6. 從左面板中選取虛擬機器，然後透過按一下向右箭頭為其指派安全性標籤。

   安全性標籤即會派給右面板中的虛擬機器。
7. 在右面板中選取虛擬機器，然後透過按一下向左箭頭從中移除標籤。

   安全性標籤便不會指派給左面板中的虛擬機器。
8. 完成新增變更後，按一下**保留**。

結果

安全性標籤將指派給所選虛擬機器。

後續步驟

安全性標籤設計為與安全群組搭配使用。如需有關建立安全群組的詳細資訊，請參閱建立安全群組。

檢視套用的安全性標籤

您可以檢視套用至您環境中的虛擬機器的安全性標籤。還可以查看套用至您環境中的安全群組的安全性標籤。

必要條件

安全性標籤必須已建立並套用至虛擬機器或安全群組。

程序

1. 從主功能表 (☰) 中，選取**雲端資源**。
2. 在左面板中，按一下**組織 VDC**。
3. 按一下目標組織虛擬資料中心旁邊的選項按鈕，然後按一下**管理防火牆**。

4 從**安全性標籤**索引標籤檢視指派的標籤。

   a 在**安全性標籤**索引標籤中，選取您要查看其指派的安全性標籤，然後按一下**編輯**圖示。

   b 在**指派/取消指派虛擬機器**下，您可以查看指派給安全性標籤的虛擬機器清單。

   c 按一下**捨棄**。

5 從**安全群組**索引標籤檢視指派的標籤。

   a 按一下**群組物件**索引標籤，然後按一下**安全群組**。

   b 選取一個安全群組。

   c 從**包含成員**下的清單中，您可以查看指派給安全群組的安全性標籤。

結果

您可以檢視現有安全性標籤以及相關聯的虛擬機器和安全群組。這樣，您便可以決定根據安全性標籤和安全群組建立防火牆規則的策略。

編輯安全性標籤

您可以編輯使用者定義的安全性標籤。

如果變更虛擬機器的環境或功能，可能還需要使用不同的安全性標籤，以便新機器組態的防火牆規則正確無誤。例如，如果您有將不再儲存敏感資料的虛擬機器，可能需要指派不同的安全性標籤，以便套用到敏感資料的防火牆規則不再針對虛擬機器執行。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下**組織 VDC**。

3 按一下目標組織虛擬資料中心旁邊的選項按鈕，然後按一下**管理防火牆**。

4 按一下**安全性標籤**索引標籤。

5 從安全性標籤清單中，選取您要編輯的安全性標籤。

6 按一下**編輯** () 按鈕。

7 編輯安全性標籤的名稱和說明。

8 將標籤指派給所選的虛擬機器或從中移除指派。

9 若要儲存變更，請按一下**保留**。

後續步驟

如果編輯安全性標籤，您可能還需要編輯相關聯的安全群組或防火牆規則。如需有關安全群組的詳細資訊，請參閱使用安全群組

。

刪除安全性標籤

您可以刪除使用者定義的安全性標籤。

如果虛擬機器的功能或環境發生變更，您可能需要刪除安全性標籤。例如，如果您有 Oracle 資料庫的安全性標籤，但決定使用其他資料庫伺服器，則可以移除安全性標籤，以便套用到 Oracle 資料庫的防火牆規則不再針對虛擬機器執行。

程序

1. 從主功能表 (☰) 中，選取**雲端資源**。
2. 在左面板中，按一下**組織 VDC**。
3. 按一下目標組織虛擬資料中心旁邊的選項按鈕，然後按一下**管理防火牆**。
4. 按一下**安全性標籤**索引標籤。
5. 從安全性標籤清單中，選取您要刪除的安全性標籤。
6. 按一下**刪除** (✖) 按鈕。
7. 按一下**確定**以確認刪除。

結果

將會刪除安全性標籤。

後續步驟

如果刪除安全性標籤，您可能還需要編輯相關聯的安全群組或防火牆規則。如需有關安全群組的詳細資訊，請參閱使用安全群組。

管理 Edge 閘道 7

Edge 閘道提供路由組織虛擬資料中心網路與外部網路的連線，並可提供負載平衡、網路位址轉譯和防火牆之類的服務。vCloud Director 支援 IPv4 和 IPv6 Edge 閘道。

Edge 閘道需要 NSX Data Center for vSphere。如需相關資訊，請參閱《NSX 管理指南》。

從 vCloud Director 9.7 開始，計算工作負載和網路工作負載使用不同的 vSphere 資源集區和儲存區原則進行隔離。Edge 叢集位於您必須先前建立的 Edge 閘道上。請參閱 使用 Edge 叢集。

您可以透過重新部署舊版 Edge 閘道，將這些 Edge 閘道移轉到相應的 Edge 叢集。請參閱重新部署 Edge 閘道。

重要 從 9.7 版開始，vCloud Director 僅支援進階 Edge 閘道。您必須將任何舊版非進階 Edge 閘道轉換為進階閘道。請參閱 https://kb.vmware.com/kb/66767。

本章節討論下列主題：

- 使用 Edge 叢集
- 新增 Edge 閘道
- 設定 Edge 閘道服務
- 檢視 Edge 閘道上的網路使用狀況和 IP 配置
- 編輯 Edge 閘道內容
- 重新部署 Edge 閘道
- 刪除 Edge 閘道
- Edge 閘道的統計資料和記錄
- 啟用對 Edge 閘道的 SSH 命令列存取

使用 Edge 叢集

為了將計算工作負載與網路工作負載隔離開，vCloud Director 9.7 採用了 Edge 叢集物件。Edge 叢集包含僅用於組織 VDC Edge 閘道的 vSphere 資源集區和儲存區原則。提供者虛擬資料中心無法使用專用於 Edge 叢集的資源，並且 Edge 叢集無法使用專用於提供者虛擬資料中心的資源。

Edge 叢集提供專用的 L2 廣播網域，進而減少 VLAN 蔓延，並確保網路安全性與隔離。例如，Edge 叢集可包含其他 VLAN，以便與實體路由器對等。

您可以建立任意數量的 Edge 叢集。您可以將 Edge 叢集指派給組織 VDC，做為主要或次要 Edge 叢集。

- 組織 VDC 的主要 Edge 叢集用於組織 VDC Edge 閘道的主要 Edge 應用裝置。
- 組織 VDC 的次要 Edge 叢集則用於待命 Edge 應用裝置 (當 Edge 閘道處於 HA 模式時)。

不同的組織 VDC 可共用 Edge 叢集，也可以有自己專屬的 Edge 叢集。

在 vCloud Director 9.7 版中，使用中繼資料控制 Edge 閘道放置的舊程序已被取代。請參閱 https://kb.vmware.com/kb/2151398。

您可以透過重新部署舊版 Edge 閘道，以將其移轉到新建立的 Edge 叢集。請參閱重新部署 Edge 閘道。

針對 Edge 叢集準備您的環境

1 在 vSphere 中，建立目標 Edge 叢集的資源集區。

  如果組織虛擬資料中心使用的是 VLAN 網路集區，則此組織虛擬資料中心的 VLAN 網路集區和 Edge 叢集必須位於同一個 vSphere Distributed Switch 上。

2 如果組織虛擬資料中心使用的是 VXLAN 網路集區，則在 NSX 中向 VXLAN 傳輸區域新增 Edge 叢集後，會同步 vCloud Director 中的 VXLAN 網路集區。

3 在 vSphere 中，建立 Edge 叢集儲存區設定檔。

建立和管理 Edge 叢集

準備您的環境之後，您必須使用 vCloud OpenAPI `EdgeClusters` 方法來建立和管理 Edge 叢集。請參閱《vCloud OpenAPI 入門》，網址為：https://code.vmware.com。

檢視 Edge 叢集需要 **Edge 叢集檢視**權限。建立、更新和刪除 Edge 叢集需要 **Edge 叢集管理**權限。

當您建立 Edge 叢集時，您可以指定名稱、vSphere 資源集區和儲存區設定檔名稱。

建立 Edge 叢集後，您可以修改其名稱和說明。刪除或移動其包含的 Edge 閘道後，您可以刪除 Edge 叢集。

將 Edge 叢集指派給組織 VDC

建立 Edge 叢集後，您可以透過更新組織 VDC 網路設定檔，為組織 VDC 指派此 Edge 叢集。您可以將 Edge 叢集指派給組織 VDC，做為主要或次要 Edge 叢集。

如果您未指派次要 Edge 叢集，將在主要 Edge 叢集上部署處於 HA 模式之 Edge 閘道的待命 Edge 應用裝置，但該叢集所在主機不同於執行主要 Edge 應用裝置的主機。

若要更新、檢視和刪除組織 VDC 網路設定檔，您必須使用 vCloud OpenAPI `VdcNetworkProfile` 方法。請參閱《vCloud OpenAPI 入門》，網址為：https://code.vmware.com。

考量事項：

- 主要和次要 Edge 叢集必須位於同一個 vSphere Distributed Switch 上。

- 如果組織 VDC 使用 VXLAN 網路集區，則 NSX 傳輸區域必須跨越運算叢集和 Edge 叢集。
- 如果組織 VDC 使用 VLAN 網路集區，Edge 叢集和運算叢集必須位於同一個 vSphere Distributed Switch 上。

如果您再次更新組織 VDC 的主要或次要 Edge 叢集，則必須重新部署現有 Edge 閘道才能將此 Edge 閘道移至新叢集。請參閱重新部署 Edge 閘道

新增 Edge 閘道

Edge 閘道提供路由組織虛擬資料中心網路與外部網路的連線，並可提供負載平衡、網路位址轉譯和防火牆之類的服務。

從 vCloud Director 9.7 開始，會在您先前已建立並指派給組織虛擬資料中心的 Edge 叢集上部署 Edge 閘道。

您可以新增連線到一或多個外部網路的 IPv4 或 IPv6 Edge 閘道。

備註 IPv6 Edge 閘道支援的服務有限。IPv6 Edge 閘道支援 Edge 防火牆、Distributed Firewall 和靜態路由。

必要條件

- 如需部署 Edge 閘道的系統需求的相關資訊，請參閱《NSX 管理指南》。
- 如果您想要在專用 Edge 叢集上部署 Edge 閘道，請建立 Edge 叢集並將其指派給組織虛擬資料中心。請參閱 使用 Edge 叢集。

程序

1. 從主功能表 (☰) 中，選取**雲端資源**。
2. 在左窗格中，按一下 **Edge 閘道**，然後按一下**新增**。
3. 按一下您要建立 Edge 閘道的組織虛擬資料中心名稱旁邊的選項按鈕，然後按**下一步**。
4. 輸入新 Edge 閘道的名稱，並選擇性地輸入說明。
5. 開啟或保持關閉下列一般 Edge 閘道設定。

一般設定	描述
分散式路由	設定 Edge 閘道以提供分散式邏輯路由。
FIPS 模式	設定 Edge 閘道以使用 NSX FIPS 模式。
高可用性	允許自動容錯移轉至備用 Edge 閘道。

6 選取系統資源的 Edge 閘道組態，然後按**下一步**。

選項	描述
精簡	需要較少的記憶體和計算資源。
大型	相較於使用 [精簡] 選項，可提供更大的容量和更高的效能。大型與超大型組態提供相同的安全性功能。
超大型	用於具有負載平衡器及大量並行工作階段的環境。
四倍大	用於高輸送量環境。需要高連線速率。

7 從 Edge 閘道可連線的外部網路中選取一或多個子網路，然後按**下一步**。

如果您已向組織 VDC 指派 Edge 叢集，則顯示的清單中將包含此 Edge 叢集可以存取的外部網路。

8 (選擇性) 將網路設定為預設閘道。

a 開啟**設定預設閘道**切換按鈕。

b 選取目標外部網路名稱旁邊的選項按鈕，然後選取目標 IP 位址旁邊的選項按鈕。

c (選擇性) 開啟**使用預設閘道進行 DNS 轉送**切換按鈕。

9 按**下一步**。

10 開啟或保持關閉下列進階 Edge 閘道設定，然後按**下一步**。

進階設定	描述
IP 設定	您可以為 Edge 閘道上的每個子網路手動指定 IP 位址。
子配置 IP 集區	您可以從 Edge 閘道上每個外部網路的可用 IP 集區中子配置多個靜態 IP 集區。
速率限制	您可以設定 Edge 閘道上每個外部網路的輸入和輸出速率限制。

11 (選擇性) 如果您在步驟 步驟 10 中啟用了一或多個進階設定，請設定每個已啟用的設定。

進階設定	步驟
IP 設定	對於 Edge 閘道上的每個網路，請在 **IP 位址**儲存格中輸入 IP 位址，然後按**下一步**。 如果您未輸入網路的 IP 位址，系統會將任意 IP 位址指派給此網路。
子配置 IP 集區	1 按一下外部網路名稱旁邊的選項按鈕，然後按一下**編輯**。 您可以查看此外部網路的可用 IP 集區，以及目前子配置的 IP 集區 (如果已設定)。 2 編輯為此外部網路子配置的 IP 集區，然後按一下**儲存**。 您可以從可用 IP 集區範圍中新增 IP 位址和範圍。 3 按一下**儲存**。 系統會合併重疊的 IP 範圍。 4 按**下一步**。 **備註** 將 IP 位址配置給 Edge 閘道是提供者向閘道指派 IP 位址擁有權的程序。vCloud Director 會在配置過程中自動設定適當的閘道介面與次要位址。如果在 vCloud Director 之外使用任何 IP 位址，則可能會導致 IP 位址衝突。
速率限制	對於 Edge 閘道上的每個外部網路，請開啟**啟用**切換按鈕，在**傳入速率**和**傳出速率**儲存格中輸入限制，然後按**下一步**。

12 檢閱**即將完成**頁面，然後按一下**完成**。

設定 Edge 閘道服務

您可以在 Edge 閘道上設定 DHCP、防火牆、網路位址轉譯 (NAT) 和 VPN 等服務。

管理 Edge 閘道防火牆

若要保護進出 Edge 閘道的流量，您可以建立和管理該 Edge 閘道上的防火牆規則。

如需保護在組織虛擬資料中心的虛擬機器之間傳輸之流量的相關資訊，請參閱在組織虛擬資料中心上管理 Distributed Firewall。

在 Distributed Firewall 畫面上建立且在其 [套用至] 資料行中已指定進階 Edge 閘道的規則，不會顯示在該進階 Edge 閘道的 [防火牆] 畫面中。

Edge 閘道的 Edge 閘道防火牆規則會顯示在**防火牆**畫面中，並按以下順序強制執行：

1 內部規則，亦稱為自動連接規則。這些內部規則可控制 Edge 閘道服務的流量流動。

2 使用者定義的規則。

3 預設規則。

預設規則的設定會套用至不符合任何使用者定義之防火牆規則的流量。預設規則會顯示在 [防火牆] 畫面上的規則底部。

在租用戶入口網站中，使用 Edge 閘道之 [防火牆規則] 畫面上的**啟用**切換按鈕，可停用或啟用 Edge 閘道防火牆。

新增 Edge 閘道防火牆規則

使用 Edge 閘道 [防火牆] 畫面，新增該 Edge 閘道的防火牆規則。您可以新增多個 NSX Edge 介面和多個 IP 位址群組，以做為這些防火牆規則的來源和目的地

針對規則的來源或目的地指定**內部**，指示連線至 NSX Edge 閘道之連接埠群組上的所有子網路的流量。如果您選取**內部**做為來源，會在 NSX Edge 閘道上設定其他內部介面時自動更新規則。

備註 將 Edge 閘道設定為進行動態路由時，內部介面上的 Edge 閘道防火牆規則無法運作。

程序

1 開啟 Edge 閘道服務。

   a 從主功能表 (☰) 中，選取**雲端資源**。

   b 在左面板中，按一下 **Edge 閘道**。

   c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 如果 [防火牆規則] 畫面尚未顯示，請按一下**防火牆**索引標籤。

3 若要在防火牆規則資料表中的現有規則下方新增某個規則，請按一下現有的資料列，然後按一下**建立**按鈕。

新規則的資料列會新增至所選規則下方，並且預設獲指派任何目的地、任何服務和**允許**動作。如果系統定義的預設規則是防火牆資料表中的唯一規則，新規則便會新增到預設規則之上。

4 按一下**名稱**儲存格，然後輸入名稱。

5 按一下**來源**儲存格，並使用現在顯示的圖示來選取要新增至規則的來源：

選項	描述
按一下 IP 圖示	輸入您想要使用的來源值。有效值為 IP 位址、CIDR、IP 範圍或關鍵字 **any**。Edge 閘道防火牆同時支援 IPv4 和 IPv6 格式。
按一下 + 圖示	使用 **+** 圖示將來源指定為除特定 IP 位址以外的物件： ■ 使用**選取物件**視窗新增符合您選取項目的物件，然後按一下**保留**將其新增至規則。 ■ 若要從規則中排除某個來源，請使用**選取物件**視窗將其新增到此規則，然後選取切換排除圖示以從此規則中排除此來源。 在來源上選取切換排除時，此規則會套用至來自除了已排除來源以外的所有來源的流量。如果未選取切換排除，此規則會套用至來自**選取物件**視窗中所指定來源的流量。

6 按一下**目的地**儲存格，然後執行下列其中一個選項：

選項	描述
按一下 IP 圖示	輸入您想要使用的目的地值。有效值為 IP 位址、CIDR、IP 範圍或關鍵字 **any**。Edge 閘道防火牆同時支援 IPv4 和 IPv6 格式。
按一下 + 圖示	使用 **+** 圖示將來源指定為除特定 IP 位址以外的物件： ■ 使用**選取物件**視窗新增符合您選取項目的物件，然後按一下**保留**將其新增至規則。 ■ 若要從規則中排除某個來源，請使用 [選取物件] 視窗將其新增到此規則，然後選取切換排除圖示以從此規則中排除此來源。 在來源上選取切換排除時，此規則會套用至來自除了已排除來源以外的所有來源的流量。如果未選取切換排除，此規則會套用至來自**選取物件**視窗中所指定來源的流量。

7 按一下新規則的**服務**儲存格，然後按一下 **+** 圖示，以連接埠-通訊協定組合形式指定服務：

a 選取服務通訊協定。

b 輸入來源和目的地連接埠的連接埠號碼，或指定 **any**。

c 按一下**保留**。

8 在新規則的**動作**儲存格中，設定規則的動作。

選項	描述
接受	允許流出或流入指定來源、目的地和服務的流量。
拒絕	封鎖流出或流入指定來源、目的地和服務的流量。

9 按一下**儲存變更**。

儲存作業需要一分鐘時間才能完成。

修改 Edge 閘道防火牆規則

您只能編輯和刪除已新增至 Edge 閘道的使用者定義的防火牆規則。您無法編輯或刪除自動產生的規則或預設規則，但可以變更預設規則的動作設定。您可以變更使用者定義之規則的優先順序。

如需有關可用於各種規則儲存格之設定的詳細資料，請參閱新增 Edge 閘道防火牆規則。

程序

1 開啟 Edge 閘道服務。

a 從主功能表 (☰) 中，選取**雲端資源**。

b 在左面板中，按一下 **Edge 閘道**。

c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 按一下**防火牆**索引標籤。

3 管理防火牆規則。

- 透過按一下**編號**儲存格中的綠色核取記號停用規則。綠色核取記號會變成紅色的已停用圖示。如果規則已停用並且您想要啟用此規則，請按一下紅色的已停用圖示。
- 透過按兩下規則的**名稱**儲存格並輸入新名稱，編輯規則名稱。
- 透過選取適當的儲存格並使用顯示的控制項來修改規則設定，例如來源或動作設定。
- 透過選取規則，然後按一下位於規則資料表上方的**刪除**按鈕以刪除規則。
- 透過使用**僅顯示使用者定義的規則**切換按鈕，可隱藏系統產生的規則。
- 透過選取規則，然後按一下位於規則資料表上方的向上和向下箭頭按鈕，可在規則資料表中將該規則上移或下移。

4 按一下**儲存變更**。

將 Syslog 伺服器設定套用至 Edge 閘道

如果已為一或多個 Edge 閘道防火牆規則啟用記錄，Edge 閘道會連線至 Syslog 伺服器。如果已在初始設定 Syslog 伺服器之前建立 Edge 閘道，或變更了 Syslog 伺服器設定，您必須同步此 Edge 閘道的 Syslog 伺服器設定。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下 **Edge 閘道**。

3 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**同步 Syslog**。

4 按一下**確定**以確認。

管理 Edge 閘道 DHCP

您可以設定 Edge 閘道，以針對連線至相關聯的組織虛擬資料中心網路的虛擬機器提供動態主機設定通訊協定 (DHCP) 服務。

如 NSX 說明文件中所述，NSX Edge 閘道功能包括 IP 位址集區、一對一靜態 IP 位址配置，以及外部 DNS 伺服器組態。靜態 IP 位址繫結以要求用戶端虛擬機器的受管理物件識別碼和介面識別碼為基礎。

NSX Edge 閘道的 DHCP 服務：

- 接聽用於 DHCP 探索之 Edge 閘道的內部介面。
- 將 Edge 閘道之內部介面的 IP 位址用作所有用戶端的預設閘道位址。
- 將內部介面的廣播及子網路遮罩值用於 Container 網路。

在下列情況下，您需要在具有指派了 DHCP 的 IP 位址的用戶端虛擬機器上重新啟動 DHCP 服務：

- 已變更或刪除 DHCP 集區、預設閘道或 DNS 伺服器。
- 已變更 Edge 閘道執行個體的內部 IP 位址。

備註 如果變更了啟用 DHCP 的 Edge 閘道上的 DNS 設定，Edge 閘道可能會停止提供 DHCP 服務。如果發生此情況，請使用 [DHCP 集區] 畫面上的 **DHCP 服務狀態**切換按鈕，以停用然後重新啟用該 Edge 閘道上的 DHCP。請參閱新增 DHCP IP 集區。

新增 DHCP IP 集區

您可以設定進階 Edge 閘道之 DHCP 服務所需的 IP 集區。DHCP 會自動指派 IP 位址給連線到組織虛擬資料中心網路的虛擬機器。

如《NSX 管理》說明文件中所述，DHCP 服務需要 IP 位址的集區。IP 集區是網路中的連續 IP 位址範圍。會為受 Edge 閘道保護且沒有位址繫結的虛擬機器配置此集區中的 IP 位址。IP 集區範圍不能彼此相交，因此一個 IP 位址只能屬於一個 IP 集區。

備註 必須將至少一個 DHCP IP 集區設定為已開啟 DHCP 服務狀態。

程序

1 開啟 Edge 閘道服務。

   a 從主功能表 (☰) 中，選取**雲端資源**。

   b 在左面板中，按一下 **Edge 閘道**。

   c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 導覽至 **DHCP > 集區**。

3 如果目前尚未啟用 DHCP 服務，請開啟 **DHCP 服務狀態**切換按鈕。

   備註 在開啟 **DHCP 服務狀態**切換按鈕後，請先新增至少一個 DHCP IP 集區，再儲存變更。如果畫面上未列出任何 DHCP IP 集區，請開啟 **DHCP 服務狀態**切換按鈕並儲存變更，畫面便會顯示且會關閉切換按鈕。

4 在 [DHCP 集區] 下，按一下**建立** () 按鈕，以指定 DHCP 集區的詳細資料，然後按一下**保留**。

選項	描述
IP 範圍	輸入 IP 位址的範圍。
網域名稱	DNS 伺服器的網域名稱。
自動設定 DNS	開啟此切換按鈕，可針對此 IP 集區的 DNS 繫結使用 DNS 服務組態。 如果啟用，則**主要名稱伺服器**與**次要名稱伺服器**均會設定為**自動**。
主要名稱伺服器	如果沒有啟用**自動設定 DNS**，請輸入主要 DNS 伺服器的 IP 位址。 此 IP 位址可用於主機名稱至 IP 位址的解析。
次要名稱伺服器	如果沒有啟用**自動設定 DNS**，請輸入次要 DNS 伺服器的 IP 位址。 此 IP 位址可用於主機名稱至 IP 位址的解析。
預設閘道	輸入預設閘道位址。 如果沒有指定預設閘道 IP 位址，則 Edge 閘道執行個體的內部介面會被視為預設閘道。
子網路遮罩	輸入 Edge 閘道介面的子網路遮罩。
租用永不到期	啟用此切換按鈕，可永遠保留所指派的此集區中的 IP 位址 (繫結至指派的虛擬機器)。 如果選取此選項，**租用時間**將設定為無限。
租用時間 (秒)	DHCP 指派的 IP 位址租用給用戶端的時間長度 (以秒為單位)。 預設租用時間為一天 (86400 秒)。 **備註** 如果選取**租用永不到期**，則無法指定租用時間。

5 按一下**儲存變更**。

結果

vCloud Director 會更新 Edge 閘道以提供 DHCP 服務。

新增 DHCP 繫結

如果您有服務在虛擬機器上執行，且不想要變更 IP 位址，則可以將虛擬機器 MAC 位址繫結到 IP 位址。繫結的 IP 位址不得與 DHCP IP 集區重疊。

必要條件

您具有想要設定繫結之虛擬機器的 MAC 位址。

程序

1 開啟 Edge 閘道服務。

a 從主功能表 (☰) 中，選取**雲端資源**。

b 在左面板中，按一下 **Edge 閘道**。

c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 在 **DHCP > 繫結**索引標籤上，按一下**建立** () 按鈕，指定繫結的詳細資料，然後按一下**保留**。

選項	描述
MAC 位址	輸入要繫結到 IP 位址之虛擬機器的 MAC 位址。
主機名稱	輸入在虛擬機器要求 DHCP 租用時，要為該虛擬機器設定的主機名稱。
IP 位址	輸入您要繫結到 MAC 位址的 IP 位址。
子網路遮罩	輸入 Edge 閘道介面的子網路遮罩。
網域名稱	輸入 DNS 伺服器的網域名稱。
自動設定 DNS	啟用此切換按鈕，可針對此 DNS 繫結使用 DNS 服務組態。 如果啟用，則**主要名稱伺服器**與**次要名稱伺服器**均會設定為**自動**。
主要名稱伺服器	如果沒有選取**自動設定 DNS**，請輸入主要 DNS 伺服器的 IP 位址。 此 IP 位址可用於主機名稱至 IP 位址的解析。
次要名稱伺服器	如果沒有選取**自動設定 DNS**，請輸入次要 DNS 伺服器的 IP 位址。 此 IP 位址可用於主機名稱至 IP 位址的解析。
預設閘道	輸入預設閘道位址。 如果沒有指定預設閘道 IP 位址，則 Edge 閘道執行個體的內部介面會被視為預設閘道。
租用永不到期	啟用此切換按鈕，可永遠保留繫結到該 MAC 位址的 IP 位址。 如果選取此選項，**租用時間**將設定為無限。
租用時間 (秒)	DHCP 指派的 IP 位址租用給用戶端的時間長度 (以秒為單位)。 預設租用時間為一天 (86400 秒)。 **備註** 如果選取**租用永不到期**，則無法指定租用時間。

3 按一下**儲存變更**。

設定 Edge 閘道的 DHCP 轉送

由 vCloud Director 環境中的 NSX 所提供的 DHCP 轉送功能可讓您從 vCloud Director 環境中利用現有 DHCP 基礎結構，而不會中斷現有 DHCP 基礎結構中的 IP 位址管理。DHCP 訊息會從虛擬機器轉送到實體 DHCP 基礎結構中的指定 DHCP 伺服器，以允許 NSX 軟體所控制的 IP 位址繼續與其餘 DHCP 控制環境中的 IP 位址進行同步。

Edge 閘道的 DHCP 轉送組態可列出多個 DHCP 伺服器。要求將傳送至所有列出的伺服器。從虛擬機器轉送 DHCP 要求時，Edge 閘道會將閘道 IP 位址新增至要求。外部 DHCP 伺服器會使用此閘道位址以符合集區並針對要求配置 IP 位址。閘道位址必須屬於 Edge 閘道介面的子網路。

您可以針對每個 Edge 閘道指定不同的 DHCP 伺服器，並且在每個 Edge 閘道上設定多個 DHCP 伺服器以提供多個 IP 網域的支援。

備註

- DHCP 轉送不支援重疊的 IP 位址空間。
- DHCP 轉送和 DHCP 服務無法同時在相同的 vNIC 上執行。如果已在 vNIC 上設定轉送代理程式，則無法在該 vNIC 的子網路上設定 DHCP 集區。如需詳細資料，請參閱《NSX 管理指南》。

指定 Edge 閘道的 DHCP 轉送組態

vCloud Director 環境中的 NSX 軟體可提供讓 Edge 閘道將 DHCP 訊息轉送至 vCloud Director 組織虛擬資料中心之外部 DHCP 伺服器的功能。您可以設定 Edge 閘道的 DHCP 轉送功能。

如《NSX 管理》說明文件中所述，可以使用現有 IP 集、IP 位址區塊、網域或所有上述項目的組合指定 DHCP 伺服器。DHCP 訊息將轉送至每個指定的 DHCP 伺服器。

您還必須設定至少一個 DHCP 轉送代理程式。DHCP 轉送代理程式是 Edge 閘道上的介面，可從中將 DHCP 要求轉送至外部 DHCP 伺服器。

必要條件

如果您想使用 IP 集來指定 DHCP 伺服器，請確認 IP 集做為可供 Edge 閘道使用的群組物件存在。請參閱建立用於防火牆規則和 DHCP 轉送組態的 IP 集。

程序

1 開啟 Edge 閘道服務。

   a 從主功能表 (☰) 中，選取**雲端資源**。

   b 在左面板中，按一下 **Edge 閘道**。

   c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 導覽至 **DHCP > 轉送**。

3 使用畫面上的欄位，依 IP 位址、網域名稱或 IP 集指定 DHCP 伺服器。

   您可以使用**新增** () 按鈕從現有 IP 集進行選取，以瀏覽可用的 IP 集。

4 透過按一下**新增** () 按鈕，並選取 vNIC 及其閘道 IP 位址，然後按一下**保留**，即可設定 DHCP 轉送代理程式，以及新增其組態至畫面上的資料表。

   依預設，閘道 IP 位址符合所選 vNIC 的主要位址。您可以保留預設值，或選取替代位址 (如果在該 vNIC 上可用)。

5 按一下**儲存變更**。

新增 SNAT 或 DNAT 規則

您可以建立來源 NAT (SNAT) 規則，將來源 IP 位址從公用 IP 位址變更為私人 IP 位址，或反向變更。您可以建立目的地 NAT (DNAT) 規則，將目的地 IP 位址從公用 IP 位址變更為私人 IP 位址，或反向變更。

建立 NAT 規則時，您可以使用下列格式指定原始和轉譯的 IP 位址：

- IP 位址；例如 192.0.2.0
- IP 位址範圍；例如 192.0.2.0-192.0.2.24
- IP 位址/子網路遮罩；例如 192.0.2.0/24
- any

在 vCloud Director 環境中的 Edge 閘道上設定 SNAT 或 DNAT 規則時，一律從組織虛擬資料中心的角度來設定規則。SNAT 規則會轉譯從組織虛擬資料中心網路傳送至外部網路，或傳送至另一個組織虛擬資料中心網路之封包的來源 IP 位址。DNAT 規則會轉譯組織虛擬資料中心網路從外部網路或另一個組織虛擬資料中心網路接收到之封包的 IP 位址，並會選擇性地轉譯連接埠。

必要條件

公用 IP 位址必須已新增至您要在其上新增規則的 Edge 閘道介面。對於 DNAT 規則，原始 (公用) IP 位址必須已新增至 Edge 閘道介面，對於 SNAT 規則，轉譯的 (公用) IP 位址必須已新增至介面。

程序

1 開啟 Edge 閘道服務。

   a 從主功能表 (☰) 中，選取**雲端資源**。

   b 在左面板中，按一下 **Edge 閘道**。

   c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 按一下 **NAT** 以檢視 [NAT 規則] 畫面。

3 根據您要建立的 NAT 規則類型，按一下 **DNAT 規則**或 **SNAT 規則**。

4 設定目的地 NAT 規則 (從外到內)。

選項	描述
套用於	選取要套用規則的介面。
原始 IP/範圍	輸入所需的 IP 位址。 此位址必須是為其設定 DNAT 規則的 Edge 閘道的公用 IP 位址。在要檢查的封包中，此 IP 位址或範圍是顯示為封包之目的地 IP 位址的 IP 位址或範圍。這些封包的目的地位址是此 DNAT 規則所轉譯的位址。
通訊協定	選取要套用規則的通訊協定。若要在所有通訊協定上套用此規則，選取**任何**。
原始連接埠	(選擇性) 選取傳入流量在 Edge 閘道上用於連線到虛擬機器所連線之內部網路的連接埠或連接埠範圍。當**通訊協定**設定為 **ICMP** 或**任何**時，此選取項目無法使用。

選項	描述
ICMP 類型	針對**通訊協定**選取 **ICMP** (裝置間用來傳達錯誤資訊的錯誤報告與診斷公用程式)時，請從下拉式功能表中選取 **ICMP 類型**。 ICMP 訊息透過 [類型] 欄位來識別。依預設，ICMP 類型設定為 [任何]。
轉譯的 IP/範圍	輸入輸入封包上的目的地位址將轉譯到的 IP 位址或 IP 位址範圍。 這些位址是您要為其設定 DNAT 的一或多個虛擬機器的 IP 位址，使其能夠從外部網路接收流量。
轉譯的連接埠	(選擇性) 選取在內部網路的虛擬機器上輸入流量要連線到的連接埠或連接埠範圍。這些連接埠是針對輸入到虛擬機器的封包將 DNAT 規則轉譯到的連接埠。
描述	(選擇性) 輸入可協助識別此規則所執行動作的說明。
已啟用	開啟以啟用此規則。
啟用記錄	開啟以讓系統記錄由此規則執行的位址轉譯。

5 設定來源 NAT 規則 (從內到外)。

選項	描述
套用於	選取要套用規則的介面。
原始來源 IP/範圍	輸入要套用至此規則的原始 IP 位址或 IP 位址範圍。 這些位址是您要為其設定 SNAT 規則的一或多個虛擬機器的 IP 位址，使其能夠將流量傳送至外部網路。
轉譯的來源 IP/範圍	輸入所需的 IP 位址。 此位址一律是為其設定 SNAT 規則之閘道的公用 IP 位址。指定輸出封包的來源位址 (虛擬機器) 在傳送流量至外部網路時要轉譯到的 IP 位址。
描述	(選擇性) 輸入可協助識別此規則所執行動作的說明。
已啟用	開啟以啟用此規則。
啟用記錄	開啟以讓系統記錄由此規則執行的位址轉譯。

6 按一下**保留**，將規則新增至畫面上的資料表。

7 重複步驟來設定其他規則。

8 按一下**儲存變更**，將規則儲存至系統。

後續步驟

針對剛設定的 SNAT 或 DNAT 規則新增對應的 Edge 閘道防火牆規則。請參閱新增 Edge 閘道防火牆規則。

進階路由組態

您可以設定 NSX 軟體為 Edge 閘道提供的靜態和動態路由功能。

若要啟用動態路由，您可以使用邊界閘道協定 (BGP) 或先開啟最短的路徑 (OSPF) 通訊協定設定進階 Edge 閘道。

如需有關 NSX 提供的路由功能的詳細資訊，請參閱《NSX 管理》說明文件中的〈路由〉。

您可以指定每個進階 Edge 閘道的靜態和動態路由。動態路由功能可針對第 2 層廣播網域提供必要的轉送資訊，可讓您減少第 2 層廣播網域，並提升網路效率和規模。NSX 會將此智慧延伸至工作負載的位置以進行東向-西向路由。此功能可讓虛擬機器之間的通訊更為直接，且無需增加擴充躍點所需的成本或時間。

指定 Edge 閘道的預設路由組態

您可以為 Edge 閘道指定靜態路由和動態路由的預設設定。

備註 若要移除所有已設定的路由設定，請使用**路由組態**畫面底部的**清除全域組態**按鈕。此動作將刪除子畫面上目前指定的所有路由設定：預設路由設定、靜態路由、OSPF、BGP 及路由重新分配。

程序

1 開啟 Edge 閘道服務。

   a 從主功能表 (☰) 中，選取**雲端資源**。

   b 在左面板中，按一下 **Edge 閘道**。

   c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 導覽至**路由 > 路由組態**。

3 若要針對此 Edge 閘道啟用等價多路徑 (ECMP) 路由，請開啟 **ECMP** 切換按鈕。

   如《NSX 管理》說明文件中所述，ECMP 是一種路由策略，可讓下一個躍點封包轉送到單一目的地在多個最佳路徑中發生。NSX 使用設定的靜態路由以靜態方式決定這些最佳路徑，或根據動態路由通訊協定 (例如 OSPF 或 BGP) 的度量計算結果加以決定。您可以透過在 [靜態路由] 畫面上指定多個下一個躍點，來指定靜態路由的多個路徑。

   如需有關 ECMP 和 NSX 的更多詳細資料，請參閱《NSX 疑難排解指南》中的路由主題。

4 指定預設路由閘道的設定。

   a 使用**套用於**下拉式清單，選取可從中連線指向目的地網路的下一個躍點的介面。

      若要查看有關所選介面的詳細資訊，請按一下藍色資訊圖示。

   b 輸入閘道 IP 位址。

   c 輸入 MTU。

   d (選擇性) 輸入選擇性說明。

   e 按一下**儲存變更**。

5 指定預設動態路由設定。

備註 如果您的環境中已設定 IPsec VPN，則不應使用動態路由。

a 選取路由器識別碼。

您可以在清單中選取路由器識別碼，或使用 **+** 圖示輸入新的路由器識別碼。此路由器識別碼是 Edge 閘道的第一個上行 IP 位址，可將路由推送至核心以進行動態路由。

b 透過開啟**啟用記錄**切換按鈕並選取記錄層級來設定記錄。

c 按一下**確定**。

6 按一下**儲存變更**。

後續步驟

新增靜態路由。請參閱新增靜態路由。

設定路由重新分配。請參閱設定路由重新分配。

設定動態路由。請參閱下列主題：

- 設定 BGP
- 設定 OSPF

新增靜態路由

您可以為目的地子網路或主機新增靜態路由。

如果在預設路由組態中啟用 ECMP，則可以在靜態路由中指定多個下一個躍點。如需啟用 ECMP 的步驟，請參閱指定 Edge 閘道的預設路由組態。

必要條件

如 NSX 說明文件中所述，靜態路由的下一個躍點 IP 位址必須存在於與其中一個 Edge 閘道介面相關聯的子網路中。否則，設定該靜態路由會失敗。

程序

1 開啟 Edge 閘道服務。

a 從主功能表 (☰) 中，選取**雲端資源**。

b 在左面板中，按一下 **Edge 閘道**。

c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 導覽至**路由 > 靜態路由**。

3 按一下**建立** (+) 按鈕。

4 為靜態路由設定下列選項：

選項	描述
網路	以 CIDR 標記法輸入網路。
下一個躍點	輸入下一個躍點的 IP 位址。 下一個躍點 IP 位址必須存在於與其中一個 Edge 閘道介面相關聯的子網路中。 如果已啟用 ECMP，您可以輸入多個下一個躍點。
MTU	編輯資料封包的最大傳輸值。 MTU 值不能大於所選 Edge 閘道介面上設定的 MTU 值。依預設，可以在 [路由組態] 畫面上查看 Edge 閘道介面上所設定的 MTU。
介面	選擇性地選取您想要在其上新增靜態路由的 Edge 閘道介面。依預設會選取與下一個躍點位址相符的介面。
描述	選擇性地輸入靜態路由的說明。

5 按一下**儲存變更**。

後續步驟

為靜態路由設定 NAT 規則。請參閱新增 SNAT 或 DNAT 規則。

新增防火牆規則，以允許流量周遊靜態路由。請參閱新增 Edge 閘道防火牆規則。

設定 OSPF

您可以針對 Edge 閘道的動態路由功能設定先開啟最短的路徑 (OSPF) 路由通訊協定。在 vCloud Director 環境中，通常在 Edge 閘道上應用 OSPF 是為了在 vCloud Director 中的 Edge 閘道之間交換路由資訊。

NSX Edge 閘道支援 OSPF，一種僅在單一路由網域內路由 IP 封包的內部閘道通訊協定。如《NSX 管理》說明文件中所述，在 NSX Edge 閘道上設定 OSPF 可讓 Edge 閘道學習和通告路由。Edge 閘道使用 OSPF 收集可用 Edge 閘道的連結狀態資訊，並建構網路的拓撲對應。拓撲可決定向網際網路層顯示的路由表，以根據 IP 封包中所找到的目的地 IP 位址來做出路由決定。

如此一來，OSPF 路由原則可針對相同成本路由之間的流量負載平衡提供動態程序。OSPF 網路可分為多個路由區域，來最佳化流量並限制路由表的大小。區域是具有相同區域識別之 OSPF 網路、路由器和連結的邏輯集合。區域由區域識別碼所識別。

必要條件

必須設定路由器識別碼。指定 Edge 閘道的預設路由組態。

程序

1 開啟 Edge 閘道服務。

a 從主功能表 (☰) 中，選取**雲端資源**。

b 在左面板中，按一下 **Edge 閘道**。

c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 導覽至**路由 > OSPF**。

3 如果目前尚未啟用 OSPF，請使用 **OSPF 已啟用**切換按鈕將其啟用。

4 根據您組織的需求進行 OSPF 設定。

選項	描述
啟用正常重新啟動	指定在重新啟動 OSPF 服務時，封包轉寄仍不會中斷。
啟用預設來源	允許 Edge 閘道做為預設閘道向其 OSPF 對等通告其本身。

5 (選擇性) 您可以按一下**儲存變更**，或繼續設定區域定義與介面對應。

6 按一下**新增** () 按鈕，在對話方塊中指定對應的詳細資料，然後按一下**保留**，以新增 OSPF 區域定義。

備註 依預設，系統會以區域識別碼 51 設定次末節區域 (NSSA)，並且此區域將自動顯示在 OSPF 畫面上的區域定義資料表中。您可以修改或刪除 NSSA 區域。

選項	描述
區域識別碼	以 IP 位址或十進位數字形式輸入區域識別碼。
區域類型	選取**一般**或 **NSSA**。 NSSA 可阻止 AS 外部連結狀態通告 (LSA) 洪泛進入 NSSA。其依賴於外部目的地的預設路由。如此一來，NSSA 必須放置在 OSPF 路由網域的 Edge 中。NSSA 可以將外部路由匯入 OSPF 路由網域，從而提供轉換為不屬於 OSPF 路由網域之小型路由網域的服務。
區域驗證	選取 OSPF 在區域層級執行的驗證類型。 區域內的所有 Edge 閘道都必須已設定相同的驗證和對應的密碼。為了使 MD5 驗證運作，接收器和傳送器必須擁有相同的 MD5 金鑰。 選項包括： ■ **無** 無需驗證。 ■ **密碼** 透過此選項，**區域驗證值**欄位中所指定的密碼將包含在已傳輸封包中。 ■ **MD5** 透過此選項，驗證會使用 MD5 (訊息摘要類型 5) 加密。MD5 總和檢查碼包含在已傳輸封包中。在**區域驗證值**欄位中輸入 Md5 金鑰。

7 按一下**儲存變更**，以便新設定的區域定義在您新增介面對應時可供選取。

8 按一下**新增** () 按鈕，在對話方塊中指定對應的詳細資料，然後按一下**保留**，以新增介面對應。

這些對應會將 Edge 閘道介面對應至區域。

a 在對話方塊中，選取您要對應至區域定義的介面。

介面可指定 Edge 閘道將連線到的外部網路。

b 選取區域將對應至所選介面的區域識別碼。

c (選擇性) 從預設值變更 OSPF 設定，以針對此介面對應進行自訂。

在設定新對應時，會顯示這些設定的預設值。在大多數情況下，建議保留預設設定。如果您變更這些設定，請確保 OSPF 對等使用相同的設定。

選項	描述
問詢間隔	在介面上傳送問詢封包的間隔 (以秒為單位)。
無作用間隔	必須在鄰接項目宣告關閉之前從該鄰接項目接收至少一個問詢封包的間隔 (以秒為單位)。
優先順序	介面的優先順序。具有最高優先順序的介面為指定的 Edge 閘道路由器。
成本	透過該介面傳送封包所需的額外負荷。介面的成本與該介面的頻寬成反比。頻寬越大，成本越低。

d 按一下**保留**。

9 在 OSPF 畫面中，按一下**儲存變更**。

後續步驟

在您想要與其交換路由資訊的其他 Edge 閘道上設定 OSPF。

新增防火牆規則，以允許啟用 OSPF 之 Edge 閘道之間的流量。請參閱新增 Edge 閘道防火牆規則。

請確保路由重新分配及防火牆組態允許通告正確的路由。請參閱設定路由重新分配。

設定 BGP

您可以針對 Edge 閘道的動態路由功能設定邊界閘道通訊協定 (BGP)。

如《NSX 管理指南》中所述，BGP 會使用 IP 網路或首碼資料表做出核心路由決定，以指定多個自發系統之間的網路連線性。在 [網路] 欄位中，BGP speaker 一詞是指執行 BGP 的網路裝置。兩個 BGP speaker 會先建立連線，然後交換任何路由資訊。「鄰接項目」一詞是指已建立這種連線的 BGP speaker。建立連線之後，裝置交換路由並同步其資料表。每個裝置傳送保持運作訊息，以使此關係保持運作。

程序

1 開啟 Edge 閘道服務。

a 從主功能表 (☰) 中，選取**雲端資源**。

b 在左面板中，按一下 **Edge 閘道**。

c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 導覽至**路由 > BGP**。

3 如果目前尚未啟用 BGP，請使用**啟用 BGP** 切換按鈕將其啟用。

4 根據您組織的需求進行 BGP 設定。

選項	描述
啟用正常重新啟動	指定在重新啟動 BGP 服務時，封包轉寄仍不會中斷。
啟用預設來源	允許 Edge 閘道做為預設閘道向其 BGP 鄰接項目通告其本身。
本機 AS	必要。指定要用於通訊協定之本機 AS 功能的自發系統 (AS) 識別碼。您指定的值必須是介於 1 到 65534 之間的全域唯一號碼。 本機 AS 是 BGP 的功能。系統會將本機 AS 號碼指派給將要設定的 Edge 閘道。當 Edge 閘道與其他自發系統中的 BGP 鄰接項目對等時，Edge 閘道會通告此識別碼。選取目的地的最佳路徑時，路由會周遊的自發系統路徑將用作動態路由演算法中的一個指標。

5 您可以按一下**儲存變更**，或繼續設定 BGP 路由鄰接項目。

6 按一下**新增** (+) 按鈕，在對話方塊中指定鄰接項目的詳細資料，然後按一下**保留**，以新增 BGP 鄰接項目組態。

選項	描述
IP 位址	針對此 Edge 閘道輸入 BGP 鄰接項目的 IP 位址。
遠端 AS	對於此 BGP 鄰接項目所屬的自發系統，輸入介於 1 到 65534 之間的全域唯一號碼。會在系統的 BGP 鄰接項目資料表的 BGP 鄰接項目中使用此遠端 AS 號碼。
權重	鄰接項目連線的預設權重。視貴組織的需求進行調整。
保持運作時間	軟體向其對等傳送保持運作訊息的頻率。預設頻率為 60 秒。根據您組織的需求進行適當調整。
保持關閉時間	軟體在未收到保持運作訊息後宣告對等失效的間隔。此間隔必須是保持運作間隔的三倍。預設間隔為 180 秒。根據您組織的需求進行適當調整。 一旦在兩個 BGP 鄰接項目之間實現對等，Edge 閘道會啟動保持關閉計時器。從鄰接項目接收到的每個保持運作訊息，都會將保持關閉計時器重設為 0。如果 Edge 閘道無法連續收到三個保持運作訊息，使得保持關閉計時器達到保持運作間隔的三倍，Edge 閘道會將鄰接項目視為關閉並刪除此鄰接項目的路由。

選項	描述
密碼	如果此 BGP 鄰接項目需要驗證，請輸入驗證密碼。 將會驗證在鄰接項目之間的連線上傳送的每個區段。必須使用相同的密碼在這兩個 BGP 鄰接項目上設定 MD5 驗證，否則它們之間將不會進行連線。
BGP 篩選器	使用此表可透過此 BGP 鄰接項目中的首碼清單指定路由篩選。 **注意** 全部封鎖規則會在篩選器的末尾強制執行。 透過按一下 **+** 圖示和設定選項，將篩選器新增至資料表。按一下**保留**以儲存每個篩選器。 ■ 選取方向以指示是否篩選流入或流出鄰接項目的流量。 ■ 選取動作以指示是否允許或拒絕流量。 ■ 輸入您想要篩選進出鄰接項目的網路。以 CIDR 格式輸入 `ANY` 或網路。 ■ 輸入 **IP 首碼 GE** 和 **IP 首碼 LE**，以使用 IP 首碼清單中的 `le` 和 `ge` 關鍵字。

7 按一下**儲存變更**，將組態儲存至系統。

後續步驟

在您想要與其交換路由資訊的其他 Edge 閘道上設定 BGP。

新增防火牆規則，以允許流入和流出 BGP 設定之 Edge 閘道的流量。如需相關資訊，請參閱新增 Edge 閘道防火牆規則。

設定路由重新分配

依預設，路由器僅與其他執行相同通訊協定的路由器共用路由。如果已設定多通訊協定環境，必須設定路由重新分配才能實現跨通訊協定路由共用。您可以為 Edge 閘道設定路由重新分配。

程序

1 開啟 Edge 閘道服務。

a 從主功能表 (☰) 中，選取**雲端資源**。

b 在左面板中，按一下 **Edge 閘道**。

c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 導覽至**路由 > 路由重新分配**。

3 使用通訊協定切換按鈕，開啟要啟用路由重新分配的通訊協定。

4 將 IP 首碼新增至畫面上的資料表。

a 按一下**新增** () 按鈕。

b 以 CIDR 格式輸入網路的名稱和 IP 位址。

c 按一下**保留**。

5 按一下**新增** () 按鈕，在對話方塊中指定準則，然後按一下**保留**，以指定每個 IP 首碼的重新分配準則。

會依序處理資料表中的項目。使用向上和向下箭頭可調整順序。

選項	描述
首碼名稱	選取特定的 IP 首碼以套用此準則，或選取**任何**將準則套用到所有網路路由。
學習器通訊協定	選取要根據此重新分配準則從其他通訊協定學習路由的通訊協定。
允許從以下通訊協定學習	選取針對**學習器通訊協定**清單中選取的通訊協定可從中學習路由的網路類型。
動作	選取是否允許或拒絕從所選類型的網路進行重新分配。

6 按一下**儲存變更**。

負載平衡

負載平衡器會在多個伺服器之間散佈傳入服務要求，以便負載分佈對於使用者是透明的。負載平衡可協助達到最佳的資源使用率、最大化輸送量、最小化回應時間並避免超載。

關於負載平衡

NSX 負載平衡器支援兩個負載平衡引擎。第 4 層負載平衡器以封包為基礎，用於提供快速路徑處理。第 7 層負載平衡器以通訊端為基礎，針對後端服務支援進階流量管理策略和 DDOS 緩和。

由於 Edge 閘道對外部網路的傳入流量進行負載平衡，因此會在外部介面上設定 Edge 閘道的負載平衡。設定虛擬伺服器以進行負載平衡時，指定組織 VDC 中具有的其中一個可用 IP 位址。請參閱《vCloud Director 使用者指南》。

負載平衡策略和概念

以封包為基礎的負載平衡策略在 TCP 和 UDP 層上實作。以封包為基礎的負載平衡不會停止連線，也不會緩衝整個申請，而是在操作封包之後，將封包直接傳送至選取的伺服器。TCP 和 UDP 工作階段均保留在負載平衡器中，以便單一工作階段的封包會導向至相同的伺服器。您可以在全域組態及相關虛擬伺服器組態中選取 [已啟用加速]，從而啟用以封包為基礎的負載平衡。

以通訊端為基礎的負載平衡策略在通訊端介面的頂層實作。針對單一申請建立兩個連線，即用戶端對向連線和伺服器對向連線。伺服器對向連線在選取伺服器之後建立。對於以 HTTP 通訊端為基礎的實作，會在傳送到具有選擇性 L7 操作的所選伺服器之前接收整個申請。對於以 HTTPS 通訊端為基礎的實作，會針對用戶端對向連線或伺服器對向連線交換驗證資訊。以通訊端為基礎的負載平衡是 TCP、HTTP 以及 HTTPS 虛擬伺服器的預設模式。

NSX 負載平衡器的主要概念包括虛擬伺服器、伺服器集區、伺服器集區成員以及服務監視器。

虛擬伺服器

虛擬伺服器是應用程式服務的抽象形式，由 IP、連接埠、通訊協定和應用程式設定檔 (例如 TCP 或 UDP) 的唯一組合來表示。

伺服器集區

後端伺服器群組。

伺服器集區成員

以集區成員表示後端伺服器。

服務監視器

定義如何探查後端伺服器的健全狀況狀態。

應用程式設定檔

表示指定應用程式的 TCP、UDP、持續性和憑證組態。

設定概觀

從設定負載平衡器的全域選項開始。現在可以建立由後端伺服器成員組成的伺服器集區，並將服務監視器與集區建立關聯，以有效地管理和共用後端伺服器。

然後，建立應用程式設定檔以定義負載平衡器中的一般應用程式行為，例如用戶端 SSL、伺服器 SSL、x-forwarded-for 或持續性。持續性會傳送具有類似特性的後續申請，例如需要將來源 IP 或 Cookie 分派給相同的集區成員，而無需執行負載平衡演算法。應用程式設定檔可以跨虛擬伺服器重複使用。

然後，建立選擇性應用程式規則以設定用於流量操作的應用程式專屬設定，例如比對特定 URL 或主機名稱，以便不同的申請可以由不同的集區進行處理。接著，建立專屬於應用程式的服務監視器，也可以使用現有的服務監視器 (如果符合您的需求)。

或者，您也可以建立應用程式規則，以支援 L7 虛擬伺服器的進階功能。應用程式規則的某些使用案例包括內容切換、標頭操作、安全性規則以及 DOS 防護。

最後，建立將伺服器集區、應用程式設定檔和任何潛在的應用程式規則連在一起的虛擬伺服器。

當虛擬伺服器收到申請時，負載平衡演算法會考慮集區成員組態和執行階段狀態。然後，演算法會計算適當的集區以分配包含一或多個成員的流量。集區成員組態包括權重、連線數上限和條件狀態等設定。執行階段狀態包括目前連線數、回應時間和健全狀況檢查狀態資訊。計算方法可以是循環配置資源、加權循環配置資源、連線數下限、來源 IP 雜湊、加權連線數下限、URL、URI 或 HTTP 標頭。

每個集區由相關聯的服務監視器進行監控。當負載平衡器偵測到集區成員有問題時，會將其標記為 [關閉]。從伺服器集區選擇集區成員時，只會選取處於 [啟動] 狀態的伺服器。如果伺服器集區未設定服務監視器，會將所有集區成員視為 [啟動]。

設定負載平衡器服務

全域負載平衡器組態參數包括整體啟用、第 4 層或第 7 層引擎的選取項目，以及要記錄的事件類型的規格。

程序

1 開啟 Edge 閘道服務。

   a 從主功能表 (☰) 中，選取**雲端資源**。

   b 在左面板中，按一下 **Edge 閘道**。

   c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 導覽至**負載平衡器** > **全域組態**。

3 選取您想要啟用的選項：

選項	動作
狀態	透過按一下切換按鈕圖示啟用負載平衡器。 啟用**已啟用加速**，將負載平衡器設定為使用較快的 L4 引擎，而非 L7 引擎。會在 Edge 閘道防火牆之前處理 L4 TCP VIP，以便不需要允許防火牆規則。 **備註** 會在防火牆之後處理 HTTP 和 HTTPS 的 L7 VIP，因此在未啟用加速時，必須存在 Edge 閘道防火牆規則以允許這些通訊協定存取 L7 VIP。如果啟用加速並且伺服器集區處於非透明模式，則會新增 SNAT 規則，因此您必須確保 Edge 閘道上的防火牆已啟用。
啟用記錄	啟用記錄，以便 Edge 閘道負載平衡器收集流量記錄。
記錄層級	選擇要在記錄中收集的事件的嚴重性。

4 按一下**儲存變更**。

儲存作業需要一分鐘時間才能完成。

後續步驟

為負載平衡器設定應用程式設定檔。請參閱建立應用程式設定檔。

建立應用程式設定檔

應用程式設定檔會針對特定類型的網路流量定義負載平衡器行為。設定設定檔之後，可將其與虛擬伺服器建立關聯。然後，虛擬伺服器根據設定檔中指定的值處理流量。使用設定檔可增強對管理網路流量的控制，並使流量管理工作更簡單且更有效。

當您建立 HTTPS 流量的設定檔時，允許使用下列 HTTPS 流量模式：

- 用戶端 -> HTTPS -> LB (終止 SSL) -> HTTP -> 伺服器
- 用戶端 -> HTTPS -> LB (終止 SSL) -> HTTPS -> 伺服器
- 用戶端 -> HTTPS -> LB (SSL 傳遞) -> HTTPS -> 伺服器
- 用戶端 -> HTTP -> LB -> HTTP -> 伺服器

程序

1 開啟 Edge 閘道服務。

a 從主功能表 (☰) 中，選取**雲端資源**。

b 在左面板中，按一下 **Edge 閘道**。

c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 導覽至**負載平衡器** > **應用程式設定檔**。

3 按一下**建立** (+) 按鈕。

4 輸入設定檔的名稱。

5 設定應用程式設定檔。

選項	描述
類型	選取用來將要求傳送至伺服器的通訊協定類型。必要參數的清單取決於您選取的通訊協定。無法輸入不適用於您所選通訊協定的參數。所有其他參數皆為必要。
啟用 SSL 傳遞	按一下可讓 SSL 驗證傳遞至虛擬伺服器。 否則，SSL 驗證會在目的地位址執行。
HTTP 重新導向 URL	(HTTP 和 HTTPS) 輸入應將到達目的地位址的流量重新導向到的 URL。
持續性	指定設定檔的持續性機制。 持續性追蹤並儲存工作階段資料，例如，服務於用戶端要求的特定集區成員。這可確保在工作階段生命週期或後續工作階段期間，用戶端要求導向至同一集區成員。選項包括： ■ **來源 IP** 來源 IP 持續性根據來源 IP 位址追蹤工作階段。當用戶端要求與支援來源位址相似性持續性的虛擬伺服器進行連線時，負載平衡器會先進行檢查，以查看此用戶端之前是否進行過連線，如果是，則會將此用戶端返回至同一集區成員。 ■ **MSRDP** (僅限 TCP) Microsoft 遠端桌面通訊協定 (MSRDP) 持續性維護執行 Microsoft 遠端桌面通訊協定 (RDP) 服務的 Windows 用戶端和伺服器之間的持續工作階段。啟用 MSRDP 持續性的建議案例是建立由執行 Windows Server 客體作業系統的成員組成的負載平衡集區，其中所有成員皆屬於 Windows 叢集並參與 Windows 工作階段目錄。
Cookie 名稱	(HTTP 和 HTTPS) 如果已指定 **Cookie** 做為持續性機制，請輸入 Cookie 名稱。Cookie 持續性使用 Cookie 以在用戶端第一次存取站台時唯一識別工作階段。在工作階段中連線後續要求時，負載平衡器會參照此 Cookie，以便它們全部移至相同的虛擬伺服器。
模式	選取應插入 Cookie 的模式。下列模式受支援： ■ **插入** Edge 閘道會傳送 Cookie。如果伺服器傳送一或多個 Cookie，則用戶端會收到一個額外的 Cookie (伺服器 Cookie 加上 Edge 閘道 Cookie)。如果伺服器不傳送任何 Cookie，則用戶端僅接收 Edge 閘道 Cookie。 ■ **前置詞** 如果您的用戶端不支援多個 Cookie，請選取此選項。 **備註** 所有瀏覽器都接受多個 Cookie。如果您擁有的專屬應用程式使用的專屬用戶端僅支援一個 Cookie，則 Web 伺服器會像往常一樣傳送其 Cookie，但 Edge 閘道會在伺服器 Cookie 值中插入其 Cookie 資訊 (做為前置詞)。當 Edge 閘道將此 Cookie 新增的資訊傳送至伺服器後，會將其移除。 ■ **應用程式工作階段** 對於此選項，伺服器不會傳送 Cookie；而是傳送使用者工作階段資訊做為 URL。例如 `http://example.com/admin/UpdateUserServlet;jsessionid=OI24B9ASD7BSSD`，其中 `jsessionid` 是使用者工作階段資訊，可用於確保持續性。無法查看 [應用程式工作階段持續性] 資料表以進行疑難排解。

選項	描述
有效期限 (秒)	輸入持續性保持有效的時間長度 (以秒為單位)。必須是 1-86400 範圍內的正整數。 **備註** 針對具有 TCP 來源 IP 持續性的 L7 負載平衡，如果未在一段時間內建立新的 TCP 連線，則持續性項目會逾時，即使現有連線仍在作用中亦如此。
插入 X-Forwarded-For HTTP 標頭	(HTTP 和 HTTPS) 選取**插入 X-Forwarded-For HTTP** 標頭，以識別透過負載平衡器連線至 Web 伺服器之用戶端的原始 IP 位址。
啟用集區端 SSL	(僅限 HTTPS) 選取**啟用集區端 SSL**，以在 [集區憑證] 索引標籤中定義用於從伺服器端驗證負載平衡器的憑證、CA 或 CRL。

6 (僅限 HTTPS) 設定要與應用程式設定檔搭配使用的憑證。如果您需要的憑證不存在，可以從**憑證**索引標籤建立。

選項	描述
虛擬伺服器憑證	選取用於解密 HTTPS 流量的憑證、CA 或 CRL。
集區憑證	定義用於從伺服器端驗證負載平衡器的憑證、CA 或 CRL。 **備註** 選取**啟用集區端 SSL** 以啟用此索引標籤。
加密	選取在 SSL/TLS 信號交換期間進行交涉的加密演算法 (或加密套件)。
用戶端驗證	指定是否忽略或需要用戶端驗證。 **備註** 如果設為必要，用戶端必須在要求或信號交換取消之後提供憑證。

7 按一下**保留**以保留變更。

此作業可能需要一些時間才能完成。

後續步驟

新增負載平衡器的服務監控器，以針對不同類型的網路流量定義健全狀況檢查。請參閱建立服務監控器。

建立服務監控器

您可以建立服務監控器，以定義特定類型的網路流量的健全狀況檢查參數。當您將服務監控器與集區相關聯時，集區成員會根據服務監控器參數受到監控。

程序

1 開啟 Edge 閘道服務。

a 從主功能表 (☰) 中，選取**雲端資源**。

b 在左面板中，按一下 **Edge 閘道**。

c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 導覽至**負載平衡器** > **服務監控**。

3 按一下**建立** () 按鈕。

4 輸入服務監視器的名稱。

5 (選擇性) 為服務監控器設定下列選項：

選項	描述
間隔	輸入要使用指定**方法**監控伺服器的間隔。
逾時	輸入必須從伺服器接收回應的時間上限 (以秒為單位)。
重試次數上限	輸入在伺服器宣告關閉之前指定的監控**方法**必須依序失敗的次數。
類型	選取您要將健全狀況檢查要求傳送至伺服器的方式，HTTP、HTTPS、TCP、ICMP 或 UDP。 根據所選類型，**新增服務監控器**對話方塊中的其餘選項會啟用或停用。
預期	(HTTP 和 HTTPS) 輸入 HTTP 或 HTTPS 回應狀態列中監視器預期相符的字串 (例如 HTTP/1.1)。
方法	(HTTP 和 HTTPS) 選取要用於偵測伺服器狀態的方法。
URL	(HTTP 和 HTTPS) 輸入要用於伺服器狀態要求的 URL。 **備註** 當您選取 POST 方法時，必須指定**傳送**的值。
傳送	(HTTP、HTTPS、UDP) 輸入要傳送的資料。
接收	(HTTP、HTTPS 和 UDP) 輸入回應內容中要相符的字串。 **備註** 如果不符合**預期**，監控器不會嘗試與**接收**內容相符。

延伸	(全部) 輸入進階監視器參數為索引鍵=值配對。例如，警告 = 10 表示如果伺服器在 10 秒內未回應，其狀態會設定為 [警告]。所有延伸項目應以歸位字元分隔。例如：
	`<extension>delay=2`
	`critical=3`
	`escape</extension>`

6 按一下**保留**以保留變更。

此作業可能需要一些時間才能完成。

範例： 每個通訊協定支援的延伸

表 7-1. HTTP/HTTPS 通訊協定的延伸

監控器延伸	描述
no-body	不會等待文件本文，並且在 HTTP/HTTPS 標頭之後停止讀取。 **備註** HTTP GET 或 HTTP POST 仍會傳送；非 HEAD 方法。
max-age=*SECONDS*	當文件存留期超過 SECONDS 時發出警告。數值可採用以下形式，10m 表示分鐘、10h 表示小時或 10d 表示天。
content-type=*STRING*	在 POST 呼叫中指定內容-類型標頭媒體類型。
linespan	允許 regex 跨越換行 (必須在 -r 或 -R 之前)。
regex=*STRING* 或 ereg=*STRING*	搜尋 regex STRING 的頁面。
eregi=*STRING*	搜尋不區分大小寫的 regex STRING 的頁面。
invert-regex	若找到，則傳回 CRITICAL；若找不到，則傳回 OK。

表 7-1. HTTP/HTTPS 通訊協定的延伸 (續)

監控器延伸	描述
proxy-authorization=*AUTH_PAIR*	透過基本驗證在 Proxy 伺服器上指定 username:password。
useragent=*STRING*	傳送 HTTP 標頭中的字串做為 `User Agent`。
header=*STRING*	傳送 HTTP 標頭中的任何其他標記。多次使用其他標頭。
onredirect=ok|warning|critical|follow|sticky|stickyport	指示如何處理重新導向的頁面。 `sticky` 類似於 `follow`，但緊隨指定的 IP 位址。`stickyport` 可確保連接埠保持不變。
pagesize=*INTEGER:INTEGER*	指定所需的頁面大小下限和上限 (以位元組為單位)。
warning=DOUBLE	指定導致警告狀態的回應時間 (以秒為單位)。
critical=DOUBLE	指定導致嚴重狀態的回應時間 (以秒為單位)。

表 7-2. 僅限 HTTPS 通訊協定的延伸

監控器延伸	描述
sni	啟用 SSL/TLS 主機名稱延伸支援 (SNI)。
certificate=**INTEGER**	指定憑證必須有效的最少天數。連接埠預設為 443。使用此選項時，不會檢查 URL。
authorization=AUTH_PAIR	透過基本驗證在站台上指定 username:password。

表 7-3. TCP 通訊協定的延伸

監控器延伸	描述
escape	允許傳送或結束字串使用 `\n`、`\r`、`\t` 或`\`。必須出現在傳送或結束選項之前。依預設，不會向傳送選項新增任何內容，會在結束選項的末尾新增 `\r\n`。
all	指定伺服器回應中必須出現的全部預期字串。依預設，會使用 `any`。
quit=*STRING*	將字串傳送至伺服器以完全關閉連線。
refuse=ok|warn|crit	接受 TCP 拒絕，並顯示狀態為 `ok`、`warn` 或 `criti`。依預設，會使用狀態 `crit`。
mismatch=ok|warn|crit	接受預期字串不相符，並顯示狀態為 `ok`、`warn` 或 `crit`。依預設，會使用狀態 `warn`。
jail	隱藏 TCP 通訊端的輸出。
maxbytes=*INTEGER*	如果接收到的位元組數超過指定的位元組數，則關閉連線。
delay=*INTEGER*	等待傳送字串和輪詢回應之間的指定秒數。
certificate=*INTEGER*[,*INTEGER*]	指定憑證必須有效的最少天數。第一個值為 `#days`(表示警告)，第二個值為嚴重 (如果未指定 - 0)。
ssl	使用 SSL 進行連線。
warning=DOUBLE	指定導致警告狀態的回應時間 (以秒為單位)。
critical=DOUBLE	指定導致嚴重狀態的回應時間 (以秒為單位)。

後續步驟

為負載平衡器新增伺服器集區。請參閱新增用於負載平衡的伺服器集區。

新增用於負載平衡的伺服器集區

您可以新增伺服器集區，以彈性且有效地管理和共用後端伺服器。集區會管理負載平衡器散發方法，並針對健全狀況檢查參數為其連結服務監視器。

程序

1 開啟 Edge 閘道服務。

   a 從主功能表 (☰) 中，選取**雲端資源**。

   b 在左面板中，按一下 **Edge 閘道**。

   c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 導覽至**負載平衡器** > **集區**。

3 按一下**建立** (+) 按鈕。

4 輸入負載平衡器集區的名稱，並選擇性地輸入其說明。

5 從**演算法**下拉式功能表中選取服務的平衡方法：

選項	描述
循環配置資源	每個伺服器會根據指派到的權重輪流使用。伺服器處理時間分佈維持相等時，這是最平穩、最公平的演算法。
IP 雜湊	根據每個封包的來源與目的地 IP 位址之雜湊來選取伺服器。
LEASTCONN	根據伺服器上已開啟的連線數目，將用戶端要求分散至多個伺服器。新的連線會傳送至開啟連線數最少的伺服器。
URI	URI 的左側 (問號之前) 為雜湊，並除以執行中伺服器的總權重。結果會指定哪個伺服器將收到要求。只要伺服器不關閉，此選項可確保 URI 一律導向至相同伺服器。
HTTPHEADER	會在每個 HTTP 要求中查詢 HTTP 標頭名稱。括號中的標頭名稱不區分大小寫，類似於 ACL 'hdr()' 函數。如果標頭不存在或不包含任何值，則會套用循環配置資源演算法。HTTP HEADER 演算法參數具有一個選項 `headerName=<name>`。例如，您可以使用 **host** 做為 HTTP HEADER 演算法參數。
URL	會在每個 HTTP GET 要求的查詢字串中查詢引數中指定的 URL 參數。如果參數後跟隨等號 = 和值，則該值會雜湊並除以執行中伺服器的權數總計。結果會指定哪個伺服器接收要求。此程序用於追蹤要求中的使用者識別碼，並確保只要沒有伺服器啟動或關閉，相同的使用者識別碼一律傳送至相同的伺服器。如果找不到任何值或參數，則會套用循環配置資源演算法。URL 演算法參數具有一個選項 `urlParam=<url>`。

6 向集區新增成員。

   a 按一下**新增** (+) 按鈕。

   b 輸入集區成員的名稱。

c 輸入集區成員的 IP 位址。

d 輸入成員用來接收負載平衡器流量的連接埠。

e 輸入成員用來接收健全狀況監控要求的監視器連接埠。

f 在**權重**文字方塊中，輸入此成員將要處理的流量比例。必須是 1-256 範圍內的整數。

g (選擇性) 在**連線數上限**文字方塊中，輸入成員可處理的並行連線數目上限。

如果傳入要求的數目超過上限，要求會排入佇列，且負載平衡器會等待連線釋放。

h (選擇性) 在**連線數下限**文字方塊中，輸入成員必須始終接受的並行連線數目下限。

i 按一下**保留**，將成員新增至集區。

此作業可能需要一些時間才能完成。

7 (選擇性) 若要讓用戶端 IP 位址對後端伺服器可見，請選取**透明**。

如果未選取**透明** (預設值)，後端伺服器便會將流量來源的 IP 位址視為負載平衡器的內部 IP 位址。

如果選取**透明**，來源 IP 位址即為用戶端的實際 IP 位址，且必須將 Edge 閘道設定為預設閘道，才能確保傳回封包通過 Edge 閘道。

8 按一下**保留**以保留變更。

此作業可能需要一些時間才能完成。

後續步驟

為負載平衡器新增虛擬伺服器。虛擬伺服器具有公用 IP 位址，並為所有傳入用戶端要求提供服務。請參閱新增虛擬伺服器。

新增應用程式規則

您可以撰寫應用程式規則，以直接操作和管理 IP 應用程式流量。

程序

1 開啟 Edge 閘道服務。

a 從主功能表 (☰) 中，選取**雲端資源**。

b 在左面板中，按一下 **Edge 閘道**。

c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 導覽至**負載平衡器** > **應用程式規則**。

3 按一下**新增** (+) 按鈕。

4 輸入應用程式規則的名稱。

5 輸入應用程式規則的指令碼。

如需應用程式規則語法的相關資訊，請參閱 http://cbonte.github.io/haproxy-dconv/configuration-1.5.html。

6 按一下**保留**以保留變更。

此作業可能需要一些時間才能完成。

後續步驟

將新應用程式規則關聯至為負載平衡器新增的虛擬伺服器。請參閱 新增虛擬伺服器。

新增虛擬伺服器

新增 Edge 閘道內部或上行介面做為虛擬伺服器。虛擬伺服器具有公用 IP 位址，並為所有傳入用戶端要求提供服務。

依預設，負載平衡器會在每個用戶端要求之後關閉伺服器 TCP 連線。

程序

1 開啟 Edge 閘道服務。

a 從主功能表 (☰) 中，選取**雲端資源**。

b 在左面板中，按一下 **Edge 閘道**。

c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 導覽至**負載平衡器** > **虛擬伺服器**。

3 按一下**新增** () 按鈕。

4 在**一般**索引標籤上，針對虛擬伺服器設定下列選項：

選項	描述
啟用虛擬伺服器	按一下以啟用虛擬伺服器。
啟用加速	按一下以啟用加速。
應用程式設定檔	選取將與虛擬伺服器建立關聯的應用程式設定檔。
名稱	輸入虛擬伺服器的名稱。
描述	輸入虛擬伺服器的選擇性說明。
IP 位址	輸入或瀏覽以選取負載平衡器接聽的 IP 位址。
通訊協定	選取虛擬伺服器接受的通訊協定。您選取的通訊協定必須與所選**應用程式設定檔**使用的通訊協定相同。
連接埠	輸入負載平衡器接聽的連接埠號碼。
預設集區	選擇負載平衡器將使用的伺服器集區。
連線限制	(選擇性) 輸入虛擬伺服器可以處理的並行連線數目上限。
連線速率限制 (CPS)	(選擇性) 輸入每秒傳入新連線要求數目上限。

5 (選擇性) 若要將應用程式規則與虛擬伺服器相關聯，請按一下**進階**索引標籤，並完成下列步驟：

a 按一下**新增** () 按鈕。

此時會顯示為負載平衡器建立的應用程式規則。如有必要，請為負載平衡器新增應用程式規則。請參閱新增應用程式規則。

6 按一下**保留**以保留變更。

此作業可能需要一些時間才能完成。

後續步驟

建立 Edge 閘道防火牆規則，以允許流量進入新虛擬伺服器 (目的地 IP 位址)。請參閱新增 Edge 閘道防火牆規則

使用虛擬私人網路進行安全存取

您可以設定 NSX 軟體為 Edge 閘道提供的 VPN 功能。您可以使用 SSL VPN-Plus 通道、IPsec VPN 通道或 L2 VPN 通道設定與組織虛擬資料中心的 VPN 連線。

如《NSX 管理指南》中所述，NSX Edge 閘道支援下列 VPN 服務：

- SSL VPN-Plus，可讓遠端使用者存取私人企業應用程式。
- IPsec VPN，可提供 NSX Edge 閘道與遠端站台 (其中也包含 NSX 或者第三方硬體路由器或 VPN 閘道) 之間的網站間連線。
- L2 VPN，藉由允許虛擬機器在跨地理界限保留相同 IP 位址的同時保留網路連線，以允許擴充組織虛擬資料中心。

在 vCloud Director 環境中，您可以在以下項目之間建立 VPN 通道：

- 位於相同組織的組織虛擬資料中心網路
- 位於不同組織的組織虛擬資料中心網路
- 在組織虛擬資料中心網路與外部網路之間

備註 vCloud Director 不支援兩個相同的 Edge 閘道間的多個 VPN 通道。如果兩個 Edge 閘道之間存有通道，而您想要將其他子網路新增至通道，請刪除現有 VPN 通道，再建立包含新子網路的新通道。

設定 Edge 閘道的 VPN 通道之後，可以使用 VPN 用戶端從遠端位置連線至該 Edge 閘道所支援的組織虛擬資料中心。

設定 SSL VPN-Plus

vCloud Director 環境中 Edge 閘道的 SSL VPN-Plus 服務，可讓遠端使用者安全地連線至該 Edge 閘道所支援的組織虛擬資料中心內的私人網路和應用程式。您可以在 Edge 閘道上設定各種 SSL VPN-Plus 服務。

在 vCloud Director 環境中，Edge 閘道的 SSL VPN-Plus 功能支援網路存取模式。遠端使用者必須安裝 SSL 用戶端才能進行安全連線，以及存取 Edge 閘道後方的網路和應用程式。做為 Edge 閘道的 SSL VPN-Plus 組態的一部分，您可以新增適用於作業系統的安裝套件並設定特定參數。如需詳細資訊，請參閱新增 SSL VPN-Plus 用戶端安裝套件。

在 Edge 閘道上設定 SSL VPN-Plus 的程序包含多個步驟。

必要條件

確認 SSL VPN-Plus 所需的所有 SSL 憑證已新增至**憑證**畫面。請參閱 SSL 憑證管理。

備註 在 Edge 閘道上，連接埠 443 為 HTTPS 的預設連接埠。對於 SSL VPN 功能，Edge 閘道的 HTTPS 連接埠必須可從外部網路存取。SSL VPN 用戶端要求在 **SSL VPN-Plus** 索引標籤上的 [伺服器設定] 畫面中設定的 Edge 閘道 IP 位址和連接埠，可從用戶端系統進行連線。請參閱設定 SSL VPN 伺服器設定。

程序

1 導覽至 SSL-VPN Plus 畫面

您可以導覽至 SSL-VPN Plus 畫面，開始為 Edge 閘道設定 SSL-VPN Plus 服務。

2 設定 SSL VPN 伺服器設定

這些伺服器設定可設定 SSL VPN 伺服器，例如服務接聽的 IP 位址和連接埠、服務的加密清單及其服務憑證。連線至 Edge 閘道時，遠端使用者會指定您在這些伺服器設定中設定的相同 IP 位址和連接埠。

3 在 Edge 閘道上建立 IP 集區以搭配 SSL VPN-Plus 使用

使用 **SSL VPN-Plus** 索引標籤上的 **IP 集區**畫面，遠端使用者將獲指派您設定之靜態 IP 集區中的虛擬 IP 位址。

4 在 Edge 閘道上新增私人網路以搭配 SSL VPN-Plus 使用

使用 **SSL VPN-Plus** 索引標籤上的 [私人網路] 畫面設定私人網路。私人網路是您想讓 VPN 用戶端在遠端使用者使用其 VPN 用戶端和 SSL VPN 通道進行連線時可存取的網路。將在 VPN 用戶端的路由表中安裝已啟用的私人網路。

5 在 Edge 閘道上設定 SSL VPN-Plus 的驗證服務

使用 **SSL VPN-Plus** 索引標籤上的**驗證**畫面，可設定 Edge 閘道之 SSL VPN 服務的本機驗證伺服器，並選擇性地啟用用戶端憑證驗證。此驗證伺服器可用來驗證連線的使用者。將驗證在本機驗證伺服器中設定的所有使用者。

6 將 SSL VPN-Plus 使用者新增至本機 SSL VPN-Plus 驗證伺服器

使用 **SSL VPN-Plus** 索引標籤上的**使用者**畫面，將遠端使用者帳戶新增至 Edge 閘道 SSL VPN 服務的本機驗證伺服器。

7 新增 SSL VPN-Plus 用戶端安裝套件

使用 **SSL VPN-Plus** 索引標籤上的 [安裝套件] 畫面，可為遠端使用者建立 SSL VPN-Plus 用戶端的具名安裝套件。

8 編輯 SSL VPN-Plus 用戶端組態

使用 **SSL VPN-Plus** 索引標籤上的**用戶端組態**畫面，以自訂 SSL VPN 用戶端通道在遠端使用者登入 SSL VPN 時的回應方式。

9 針對 Edge 閘道自訂一般 SSL VPN-Plus 設定

依預設，系統會在 vCloud Director 環境中的 Edge 閘道上設定一些 SSL VPN-Plus 設定。您可以使用 vCloud Director 租用戶入口網站之 **SSL VPN-Plus** 索引標籤上的**一般設定**畫面，自訂這些設定。

導覽至 SSL-VPN Plus 畫面

您可以導覽至 SSL-VPN Plus 畫面，開始為 Edge 閘道設定 SSL-VPN Plus 服務。

程序

1 開啟 Edge 閘道服務。

a 從主功能表 (☰) 中，選取**雲端資源**。

b 在左面板中，按一下 **Edge 閘道**。

c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 按一下 **SSL VPN-Plus** 索引標籤。

後續步驟

在**一般**畫面上，設定預設 SSL VPN-Plus 設定。請參閱針對 Edge 閘道自訂一般 SSL VPN-Plus 設定。

設定 SSL VPN 伺服器設定

這些伺服器設定可設定 SSL VPN 伺服器，例如服務接聽的 IP 位址和連接埠、服務的加密清單及其服務憑證。連線至 Edge 閘道時，遠端使用者會指定您在這些伺服器設定中設定的相同 IP 位址和連接埠。

如果 Edge 閘道的外部介面上已設定多個覆疊 IP 位址網路，則選取用於 SSL VPN 伺服器的 IP 位址可能不同於 Edge 閘道的預設外部介面。

設定 SSL VPN 伺服器設定時，您必須選擇將哪種加密演算法用於 SSL VPN 通道。您可以選擇一或多種加密。請根據選取項目的優缺點謹慎選擇加密。

依預設，系統會將針對每個 Edge 閘道產生的預設自我簽署憑證，用作 SSL VPN 通道的預設伺服器身分識別憑證。您可以選擇使用您已在**憑證**畫面上新增至系統的數位憑證，而不是使用此預設憑證。

必要條件

- 確認已滿足設定 SSL VPN-Plus 中所述的必要條件。
- 如果您選擇使用與預設憑證不同的服務憑證，請將所需憑證匯入系統中。請參閱將服務憑證新增至 Edge 閘道。
- 導覽至 SSL-VPN Plus 畫面。

程序

1 在 **SSL VPN-Plus** 畫面上，按一下**伺服器設定**。

2 按一下**已啟用**。

3 從下拉式功能表中選取 IP 位址。

4 (選擇性) 輸入 TCP 連接埠號碼。

此 TCP 連接埠號碼由 SSL 用戶端安裝套件使用。依預設，系統會使用連接埠 443，即 HTTPS/SSL 流量的預設連接埠。即使需要連接埠號碼，您仍可以設定任何 TCP 連接埠用於通訊。

備註 SSL VPN 用戶端要求在此處設定的 IP 位址和連接埠可從遠端使用者的用戶端系統進行連線。如果變更連接埠號碼的預設值，請確保 IP 位址和連接埠組合可從預期使用者的系統進行連線。

5 從加密清單中選取加密方法。

6 設定服務的 Syslog 記錄原則。

預設會啟用記錄。您可以變更要記錄的訊息層級或停用記錄。

7 (選擇性) 如果您想要使用服務憑證，而非系統產生的預設自我簽署憑證，請按一下**變更伺服器憑證**，選取憑證，然後按一下**確定**。

8 按一下**儲存變更**。

後續步驟

備註 遠端使用者必須可以連線到所設定的 Edge 閘道 IP 位址和 TCP 連接埠號碼。新增 Edge 閘道防火牆規則，以允許存取此程序中設定的 SSL VPN-Plus IP 位址和連接埠。請參閱新增 Edge 閘道防火牆規則。

新增 IP 集區，以便遠端使用者在使用 SSL VPN-Plus 進行連線時獲指派 IP 位址。請參閱在 Edge 閘道上建立 IP 集區以搭配 SSL VPN-Plus 使用。

在 Edge 閘道上建立 IP 集區以搭配 SSL VPN-Plus 使用

使用 **SSL VPN-Plus** 索引標籤上的 **IP 集區**畫面，遠端使用者將獲指派您設定之靜態 IP 集區中的虛擬 IP 位址。

在此畫面中每新增一個 IP 集區，就會在 Edge 閘道上設定一個 IP 位址子網路。這些 IP 集區中使用的 IP 位址範圍必須不同於 Edge 閘道上設定的所有其他網路。

備註 SSL VPN 會根據 IP 集區在畫面上的資料表中所顯示的順序，將 IP 集區中的 IP 位址指派給遠端使用者。新增 IP 集區至畫面上的資料表後，您可以使用向上和向下箭頭調整其在資料表中的位置。

必要條件

- 導覽至 SSL-VPN Plus 畫面。
- 設定 SSL VPN 伺服器設定。

程序

1 在 **SSL VPN-Plus** 索引標籤上，按一下 **IP 集區**。

2 按一下**建立** () 按鈕。

3 設定 IP 集區設定。

選項	動作
IP 範圍	輸入此 IP 集區的 IP 位址範圍，例如 **127.0.0.1–127.0.0.9**。 當 VPN 用戶端驗證並連線至 SSL VPN 通道時，將為其指派這些 IP 位址。
網路遮罩	輸入 IP 集區的網路遮罩，例如 **255.255.255.0**。
閘道	輸入您想要 Edge 閘道建立並指派為此 IP 集區之閘道位址的 IP 位址。 建立 IP 集區時，會在 Edge 閘道虛擬機器上建立虛擬介面卡，並在該虛擬介面上設定此 IP 位址。此 IP 位址可以是子網路內的任何 IP，但此 IP 並非同時存在於 **IP 範圍**欄位中的範圍內。
描述	(選擇性) 輸入此 IP 集區的說明。
狀態	選取是啟用還是停用此 IP 集區。
主要 DNS	(選擇性) 輸入將用於這些虛擬 IP 位址之名稱解析的主要 DNS 伺服器的名稱。
次要 DNS	(選擇性) 輸入要使用之次要 DNS 伺服器的名稱。
DNS 尾碼	(選擇性) 輸入主控用戶端系統之網域的 DNS 尾碼 (用於以網域為基礎的主機名稱解析)。
WINS 伺服器	(選擇性) 根據您組織的需求，輸入 WINS 伺服器位址。

4 按一下**保留**。

結果

IP 集區組態會新增到畫面上的資料表。

後續步驟

新增您想要可供使用 SSL VPN-Plus 進行連線之遠端使用者存取的私人網路。請參閱在 Edge 閘道上新增私人網路以搭配 SSL VPN-Plus 使用。

在 Edge 閘道上新增私人網路以搭配 SSL VPN-Plus 使用

使用 **SSL VPN-Plus** 索引標籤上的 [私人網路] 畫面設定私人網路。私人網路是您想讓 VPN 用戶端在遠端使用者使用其 VPN 用戶端和 SSL VPN 通道進行連線時可存取的網路。將在 VPN 用戶端的路由表中安裝已啟用的私人網路。

私人網路是 Edge 閘道後方您要針對 VPN 用戶端加密流量或排除在加密之外的所有可連線 IP 網路的清單。必須將需要透過 SSL VPN 通道存取的每個私人網路新增為個別項目。您可以使用路由摘要技術來限制項目數。

- SSL VPN-Plus 可讓遠端使用者根據 IP 集區在畫面上的資料表中所顯示的自上而下順序來存取私人網路。新增私人網路至畫面上的資料表後，您可以使用向上和向下箭頭調整其在資料表中的位置。

- 如果您選取以針對私人網路啟用 TCP 最佳化，處於主動模式的一些應用程式 (例如 FTP) 可能在該子網路內無法運作。若要新增在主動模式下設定的 FTP 伺服器，必須為該 FTP 伺服器新增其他私人網路，並針對該私人網路停用 TCP 最佳化。此外，該 FTP 伺服器的私人網路必須處於啟用狀態，並顯示在畫面上的資料表中 TCP 最佳化私人網路上方。

必要條件

- 導覽至 SSL-VPN Plus 畫面。
- 在 Edge 閘道上建立 IP 集區以搭配 SSL VPN-Plus 使用。

程序

1 在 **SSL VPN-Plus** 索引標籤上，按一下**私人網路**。

2 按一下**新增** () 按鈕。

3 設定私人網路設定。

選項	動作
網路	以 CIDR 格式輸入私人網路 IP 位址，例如 **192169.1.0/24**。
描述	(選擇性) 輸入網路的說明。
傳送流量	指定想要讓 VPN 用戶端傳送私人網路和網際網路流量的方式。 ■ **透過通道** VPN 用戶端會透過已啟用 SSL VPN-Plus 的 Edge 閘道傳送私人網路和網際網路流量。 ■ **略過通道** VPN 用戶端略過 Edge 閘道，直接將流量傳送至私人伺服器。
啟用 TCP 最佳化	(選擇性) 若要最佳化網際網路速度，則在選取**透過通道**傳送流量的同時，也必須選取**啟用 TCP 最佳化** 選取此選項可提高 VPN 通道內 TCP 封包的效能，但無法改善 UDP 流量的效能。 傳統的完整存取 SSL VPN 通道會透過網際網路傳送第二個 TCP/IP 堆疊中的 TCP/IP 資料以進行加密。此傳統方法會將應用程式層資料封裝在兩個單獨的 TCP 資料流中。如果發生封包遺失 (即使在最佳網際網路條件下仍會發生)，會產生稱為 TCP-over-TCP 潰敗的效能降低影響。在 TCP-over-TCP 潰敗過程中，兩個 TCP 儀器會更正相同的單一 IP 資料封包，從而減弱網路輸送量並導致連線逾時。選取**啟用 TCP 最佳化**可降低此 TCP-over-TCP 問題發生的風險。 **備註** 啟用 TCP 最佳化時： ■ 您必須輸入想要最佳化網際網路流量的連接埠號碼。 ■ SSL VPN 伺服器會代表 VPN 用戶端開啟 TCP 連線。當 SSL VPN 伺服器開啟 TCP 連線時，會套用第一個自動產生的 Edge 防火牆規則，以允許從 Edge 閘道開啟的所有連線均可傳遞。未最佳化的流量將由一般 Edge 防火牆規則進行評估。預設產生的 TCP 規則為允許任何連線。
連接埠	選取**透過通道**時，輸入您要開啟供遠端使用者存取內部伺服器的連接埠號碼範圍，例如 **20–21** (針對 FTP 流量) 和 **80–81** (針對 HTTP 流量)。 若要為使用者提供無限制的存取權，請將此欄位保留空白。
狀態	啟用或停用私人網路。

4 按一下**保留**。

5 按一下**儲存變更**，將組態儲存至系統。

後續步驟

新增驗證伺服器。請參閱在 Edge 閘道上設定 SSL VPN-Plus 的驗證服務。

重要 新增對應的防火牆規則，以允許您在此畫面中已新增之私人網路的傳入網路流量。請參閱新增 Edge 閘道防火牆規則。

在 Edge 閘道上設定 SSL VPN-Plus 的驗證服務

使用 **SSL VPN-Plus** 索引標籤上的**驗證**畫面，可設定 Edge 閘道之 SSL VPN 服務的本機驗證伺服器，並選擇性地啟用用戶端憑證驗證。此驗證伺服器可用來驗證連線的使用者。將驗證在本機驗證伺服器中設定的所有使用者。

在 Edge 閘道上只能設定一個本機 SSL VPN-Plus 驗證伺服器。如果您按一下 **+ 本機**，並指定其他驗證伺服器，則當您嘗試儲存組態時會顯示錯誤訊息。

透過 SSL VPN 進行驗證的時間上限為三 (3) 分鐘。此上限值取決於非驗證逾時，預設為 3 分鐘且無法設定。因此，如果鏈結授權中有多個驗證伺服器，且使用者驗證需要超過 3 分鐘，則使用者將無法進行驗證。

必要條件

- 導覽至 SSL-VPN Plus 畫面。
- 在 Edge 閘道上新增私人網路以搭配 SSL VPN-Plus 使用。
- 如果您打算啟用用戶端憑證驗證，請確認已將 CA 憑證新增至 Edge 閘道。請參閱將 CA 憑證新增至 Edge 閘道以進行 SSL 憑證信任驗證。

程序

1 按一下 **SSL VPN-Plus** 索引標籤和**驗證**。

2 按一下**本機**。

3 設定驗證伺服器設定。

a (選擇性) 啟用和設定密碼原則。

選項	描述
啟用密碼原則	開啟您在此處設定的密碼原則設定強制執行。
密碼長度	輸入密碼長度允許的字元數目下限和上限。
字母數目下限	(選擇性) 輸入密碼中所需的字母字元數目下限。
數字數目下限	(選擇性) 輸入密碼中所需的數字字元數目下限。
特殊字元數目下限	(選擇性) 輸入密碼中所需的特殊字元數目下限，例如 & 符號 (&)、雜湊標記 (#)、百分號 (%) 等。
密碼不應包含使用者識別碼	(選擇性) 啟用以強制密碼不得包含使用者識別碼。
密碼到期時間	(選擇性) 輸入使用者必須變更密碼前密碼可存在的天數上限。
到期通知時間	(選擇性) 輸入在**密碼到期時間**值之前，使用者會收到密碼即將到期通知的天數。

b (選擇性) 啟用和設定帳戶鎖定原則。

選項	描述
啟用帳戶鎖定原則	開啟您在此處設定的帳戶鎖定原則設定強制執行。
重試計數	輸入使用者可嘗試存取其帳戶的次數。
重試持續時間	輸入使用者帳戶在登入嘗試失敗後被鎖定的期間 (以分鐘為單位)。 例如，如果指定**重試計數**為 5 次且**重試持續時間**為 1 分鐘，則在 1 分鐘內出現 5 次登入失敗嘗試後，會鎖定使用者帳戶。
鎖定持續時間	輸入使用者帳戶保持鎖定的期間。 此時間之後，該帳戶會自動解除鎖定。

c 在 [狀態] 區段中，啟用此驗證伺服器。

d (選擇性) 設定次要驗證。

選項	描述
將此伺服器用於次要驗證	(選擇性) 指定是否將伺服器用作第二個層級的驗證。
如果驗證失敗，則終止工作階段	(選擇性) 指定是否在驗證失敗時結束 VPN 工作階段。

e 按一下**保留**。

4 (選擇性) 若要啟用用戶端憑證驗證，請按一下**變更憑證**，然後開啟啟用切換按鈕、選取要使用的 CA 憑證，並按一下**確定**。

後續步驟

將本機使用者新增至本機驗證伺服器，使其能夠透過 SSL VPN-Plus 進行連線。請參閱將 SSL VPN-Plus 使用者新增至本機 SSL VPN-Plus 驗證伺服器。

建立包含 SSL 用戶端的安裝套件，以便遠端使用者可將其安裝在本機系統上。請參閱新增 SSL VPN-Plus 用戶端安裝套件。

將 SSL VPN-Plus 使用者新增至本機 SSL VPN-Plus 驗證伺服器

使用 **SSL VPN-Plus** 索引標籤上的**使用者**畫面，將遠端使用者帳戶新增至 Edge 閘道 SSL VPN 服務的本機驗證伺服器。

備註 如果尚未設定本機驗證伺服器，在**使用者**畫面上新增使用者會自動新增具有預設值的本機驗證伺服器。然後，您可以使用**驗證**畫面上的 [編輯] 按鈕來檢視和編輯預設值。如需使用**驗證**畫面的相關資訊，請參閱在 Edge 閘道上設定 SSL VPN-Plus 的驗證服務。

必要條件

導覽至 SSL-VPN Plus 畫面。

程序

1 在 **SSL VPN-Plus** 索引標籤上，按一下**使用者**。

2 按一下**建立** () 按鈕。

3 針對使用者設定下列選項。

選項	描述
使用者識別碼	輸入使用者識別碼。
密碼	輸入使用者的密碼。
重新輸入密碼	重新輸入密碼。
名字	(選擇性) 輸入使用者的名字。
姓氏	(選擇性) 輸入使用者的姓氏。
描述	(選擇性) 輸入使用者的說明。
已啟用	指定此使用者已啟用還是已停用。
密碼永久有效	(選擇性) 指定是否為此使用者永遠保留相同密碼。
允許變更密碼	(選擇性) 指定是否允許使用者變更密碼。
下一次登入時變更密碼	(選擇性) 指定是否要讓此使用者在下次使用者登入時變更密碼。

4 按一下**保留**。

5 重複上述步驟，新增其他使用者。

後續步驟

將本機使用者新增至本機驗證伺服器，使其能夠透過 SSL VPN-Plus 進行連線。請參閱將 SSL VPN-Plus 使用者新增至本機 SSL VPN-Plus 驗證伺服器。

建立包含 SSL 用戶端的安裝套件，以便遠端使用者可將其安裝在本機系統上。請參閱新增 SSL VPN-Plus 用戶端安裝套件。

新增 SSL VPN-Plus 用戶端安裝套件

使用 **SSL VPN-Plus** 索引標籤上的 [安裝套件] 畫面，可為遠端使用者建立 SSL VPN-Plus 用戶端的具名安裝套件。

您可以將 SSL VPN-Plus 用戶端安裝套件新增至 Edge 閘道。新使用者首次登入以使用 VPN 連線時，會收到下載並安裝此套件的提示。新增後，這些用戶端安裝套件便可從 Edge 閘道公用介面的 FQDN 進行下載。

您可以建立在 Windows、Linux 和 Mac 作業系統上執行的安裝套件。如果每個 SSL VPN 用戶端需要不同的安裝參數，請針對各個組態建立安裝套件。

必要條件

導覽至 SSL-VPN Plus 畫面

程序

1 在租用戶入口網站的 **SSL VPN-Plus** 索引標籤上，按一下**安裝套件**。

2 按一下**新增** () 按鈕。

3 設定安裝套件設定。

選項	描述
設定檔名稱	輸入此安裝套件的設定檔名稱。 此名稱會向遠端使用者顯示，以識別 Edge 閘道的此 SSL VPN 連線。
閘道	輸入 Edge 閘道公用介面的 IP 位址或 FQDN。 所輸入的 IP 位址或 FQDN 將繫結至 SSL VPN 用戶端。在遠端使用者的本機系統上安裝用戶端時，會在該 SSL VPN 用戶端上顯示此 IP 位址或 FQDN。 若要將其他 Edge 閘道上行介面繫結至此 SSL VPN 用戶端，請按一下**新增** () 按鈕新增資料列並輸入其介面 IP 位址或 FQDN 和連接埠。
連接埠	(選擇性) 若要從顯示的預設值修改連接埠值，請按兩下該值並輸入新值。
Windows **Linux** **Mac**	選取您要針對其建立安裝套件的作業系統。
描述	(選擇性) 輸入使用者的說明。
已啟用	指定此套件已啟用還是已停用。

4 選取適用於 Windows 的安裝參數。

選項	描述
登入時啟動用戶端	當遠端使用者登入其本機系統時，啟動 SSL VPN 用戶端。
允許記住密碼	可讓用戶端記住使用者密碼。
啟用無訊息模式安裝	向遠端使用者隱藏安裝命令。

選項	描述
隱藏 SSL 用戶端網路介面卡	隱藏 VMware SSL VPN-Plus 介面卡，此介面卡隨 SSL VPN 用戶端安裝套件一起安裝在遠端使用者的電腦上。
隱藏用戶端系統匣圖示	隱藏用於指示 VPN 連線是否處於作用中狀態的 SSL VPN 系統匣圖示。
建立桌面圖示	在使用者桌面上建立一個用於叫用 SSL 用戶端的圖示。
啟用無訊息模式作業	隱藏用於指示該安裝已完成的視窗。
伺服器安全性憑證驗證	SSL VPN 用戶端會在建立安全連線之前驗證 SSL VPN 伺服器憑證。

5 按一下**保留**。

後續步驟

編輯用戶端組態。請參閱編輯 SSL VPN-Plus 用戶端組態。

編輯 SSL VPN-Plus 用戶端組態

使用 **SSL VPN-Plus** 索引標籤上的**用戶端組態**畫面，以自訂 SSL VPN 用戶端通道在遠端使用者登入 SSL VPN 時的回應方式。

必要條件

導覽至 SSL-VPN Plus 畫面

程序

1 在 **SSL VPN-Plus** 索引標籤上，按一下**用戶端組態**。

2 選取**通道模式**。

- 在分割通道模式下，只有 VPN 流量流經 Edge 閘道。
- 在完整通道模式下，Edge 閘道將成為遠端使用者的預設閘道，並且所有流量 (例如 VPN、本機和網際網路) 都會流經 Edge 閘道。

3 如果選取完整通道模式，請輸入遠端使用者的用戶端所使用的預設閘道 IP 位址，然後選擇性地選取是否要排除本機子網路流量使其不流經 VPN 通道。

4 (選擇性) 停用自動重新連線。

啟用自動重新連線預設為啟用。如果已啟用自動重新連線，SSL VPN 用戶端將在使用者中斷連線時自動重新連線使用者。

5 (選擇性) 選擇性啟用在用戶端升級可用時，讓用戶端通知遠端使用者的功能。

此選項預設為停用狀態。如果您啟用此選項，遠端使用者可選擇安裝升級。

6 按一下**儲存變更**。

針對 Edge 閘道自訂一般 SSL VPN-Plus 設定

依預設，系統會在 vCloud Director 環境中的 Edge 閘道上設定一些 SSL VPN-Plus 設定。您可以使用 vCloud Director 租用戶入口網站之 **SSL VPN-Plus** 索引標籤上的**一般設定**畫面，自訂這些設定。

必要條件

導覽至 SSL-VPN Plus 畫面。

程序

1 在 **SSL VPN-Plus** 索引標籤上，按一下**一般設定**。

2 根據您組織的需求，編輯所需的一般設定。

選項	描述
防止使用相同使用者名稱多次登入	開啟此項可將遠端使用者限制為在相同使用者名稱下僅有一個作用中的登入工作階段。
壓縮	開啟此項可啟用以 TCP 為基礎的智慧型資料壓縮並提高資料傳輸速度。
啟用記錄	開啟此項可維護通過 SSL VPN 閘道的流量記錄。 預設會啟用記錄。
強制虛擬鍵盤	開啟此項可要求遠端使用者僅使用虛擬 (畫面上) 鍵盤來輸入登入資訊。
虛擬鍵盤的隨機按鍵	開啟此項可讓虛擬鍵盤使用隨機按鍵配置。
工作階段閒置逾時	輸入工作階段閒置逾時 (以分鐘為單位)。 如果使用者工作階段在指定的時段內沒有任何活動，系統將中斷與使用者工作階段的連線。系統預設值為 10 分鐘。
使用者通知	輸入在遠端使用者登入後向其顯示的訊息。
啟用公用 URL 存取	開啟此項可允許遠端使用者存取您未明確設定用於遠端使用者存取的站台。
啟用強制逾時	開啟此項可讓系統在**強制逾時**欄位中指定的期間結束後中斷與遠端使用者的連線。
強制逾時	輸入逾時期間 (以分鐘為單位)。 當**啟用強制逾時**切換按鈕開啟時，會顯示此欄位。

3 按一下**儲存變更**。

設定 IPsec VPN

vCloud Director 環境中的 Edge 閘道支援網站間網際網路通訊協定安全性 (IPsec)，以保護組織虛擬資料中心網路之間或組織虛擬資料中心網路與外部 IP 位址之間的 VPN 通道的安全。您可以在 Edge 閘道上設定 IPsec VPN 服務。

最常見的情況是設定從遠端網路到組織虛擬資料中心的 IPsec VPN 連線。NSX 軟體提供 Edge 閘道的 IPsec VPN 功能，包括支援憑證驗證、預先共用金鑰模式以及本身和遠端 VPN 路由器之間的 IP 單點傳播流量。您也可以將多個子網路設定為透過 IPsec 通道連線至 Edge 閘道後方的內部網路。將多個子網路設定為透過 IPsec 通道連線至內部網路時，這些子網路和 Edge 閘道後方的內部網路必須不能具有重疊的位址範圍。

備註 如果 IPsec 通道之間的本機和遠端對等具有重疊的 IP 位址，跨通道流量轉寄可能會不一致，具體取決於本機連線的路由和自動探索的路由是否存在。

支援下列 IPsec VPN 演算法：

- AES (AES128-CBC)

- AES256 (AES265-CBC)
- 三重 DES (3DES192-CBC)
- AES-GCM (AES128-GCM)
- DH-2 (Diffie-Hellman 群組 2)
- DH-5 (Diffie-Hellman 群組 5)
- DH-14 (Diffie-Hellman 群組 14)

備註 IPsec VPN 不支援動態路由通訊協定。當您在組織虛擬資料中心的 Edge 閘道與遠端站台上的實體閘道 VPN 之間設定 IPsec VPN 通道時，您無法設定該連線的動態路由。該遠端站台的 IP 位址無法由 Edge 閘道上行中的動態路由學習。

如《NSX 管理指南》中的〈IPSec VPN 概觀〉主題中所述，Edge 閘道上支援的通道數目上限由其設定的大小所決定：精簡型、大型、超大型和四倍大。您可以透過登入 vCloud Director Web 主控台、導覽至 Edge 閘道，並使用**內容**動作檢視 Edge 閘道的組態，以檢視 Edge 閘道的大小。如需使用 vCloud Director Web 主控台的相關資訊，請參閱《vCloud Director 管理員指南》。

在 Edge 閘道上設定 IPsec VPN 的程序包含多個步驟。

備註 如果通道端點之間有防火牆，可以在設定 IPsec VPN 服務之後，更新防火牆規則以允許下列 IP 通訊協定及 UDP 連接埠：

- IP 通訊協定 ID 50 (ESP)
- IP 通訊協定 ID 51 (AH)
- UDP 連接埠 500 (IKE)
- UDP 連接埠 4500

程序

1 導覽至 IPsec VPN 畫面

在 **IPsec VPN** 畫面中，您可以開始為 Edge 閘道設定 IPsec VPN 服務。

2 設定 Edge 閘道的 IPsec VPN 站台連線

使用 vCloud Director 租用戶入口網站中的 **IPsec VPN 站台** 畫面，可設定透過 Edge 閘道的 IPsec VPN 功能建立組織虛擬資料中心與另一個站台之間的 IPsec VPN 連線所需的設定。

3 啟用 Edge 閘道上的 IPsec VPN 服務

已設定至少一個 IPsec VPN 連線時，您可以啟用 Edge 閘道上的 IPsec VPN 服務。

4 指定全域 IPsec VPN 設定

使用**全域組態**畫面，在 Edge 閘道層級設定 IPsec VPN 驗證設定。在此畫面上，可以設定全域預先共用金鑰，並啟用憑證驗證。

導覽至 IPsec VPN 畫面

在 **IPsec VPN** 畫面中，您可以開始為 Edge 閘道設定 IPsec VPN 服務。

程序

1 開啟 Edge 閘道服務。

   a 從主功能表 (☰) 中，選取**雲端資源**。

   b 在左面板中，按一下 **Edge 閘道**。

   c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 導覽至 **VPN > IPsec VPN**。

後續步驟

使用 **IPsec VPN 站台**畫面設定 IPsec VPN 連線。必須設定至少一個連線，然後才能啟用 Edge 閘道上的 IPsec VPN 服務。請參閱設定 Edge 閘道的 IPsec VPN 站台連線。

設定 Edge 閘道的 IPsec VPN 站台連線

使用 vCloud Director 租用戶入口網站中的 **IPsec VPN 站台** 畫面，可設定透過 Edge 閘道的 IPsec VPN 功能建立組織虛擬資料中心與另一個站台之間的 IPsec VPN 連線所需的設定。

當您設定站台之間的 IPsec VPN 連線時，可以從目前位置設定連線。設定連線需要您瞭解 vCloud Director 環境中的概念，以便正確設定 VPN 連線。

- 本機和對等子網路會指定 VPN 連線的網路。當您在 IPsec VPN 站台組態中指定這些子網路時，請輸入網路範圍而非特定的 IP 位址。使用 CIDR 格式，例如 **192.168.99.0/24**。
- 對等識別碼是唯一識別終止 VPN 連線之遠端裝置的識別碼，通常是其公用 IP 位址。對於使用憑證驗證的對等，此識別碼必須為對等憑證中所設定的辨別名稱。對於 PSK 對等，此識別碼可以是任何字串。NSX 最佳做法是使用遠端裝置的公用 IP 位址或 FQDN 做為對等識別碼。如果對等 IP 位址來自另一個組織虛擬資料中心網路，您可以輸入對等的原生 IP 位址。如果為對等設定 NAT，您可以輸入對等的私人 IP 位址。
- 對等端點會指定要連線的遠端裝置的公用 IP 位址。如果對等的閘道無法從網際網路直接存取，但透過另一台裝置連線，則對等端點可能為不同於對等識別碼的其他位址。如果為對等設定 NAT，您可以輸入裝置用於 NAT 的公用 IP 位址。
- 本機識別碼指定組織虛擬資料中心之 Edge 閘道的公用 IP 位址。您可以輸入 IP 位址或主機名稱，以及 Edge 閘道防火牆。
- 本機端點可指定 Edge 閘道傳輸所在的組織虛擬資料中心的網路。通常，Edge 閘道的外部網路為本機端點。

必要條件

- 導覽至 IPsec VPN 畫面。
- 設定 IPsec VPN。
- 如果想要使用全域憑證做為驗證方法，請確認該憑證驗證已在**全域組態**畫面上啟用。請參閱指定全域 IPsec VPN 設定。

程序

1 在 **IPsec VPN** 索引標籤上，按一下 **IPsec VPN 站台**。

2 按一下**新增** () 按鈕。

3 設定 IPsec VPN 連線設定。

選項	動作
已啟用	在兩個 VPN 端點之間啟用此連線。
啟用完整轉寄密碼 (PFS)	啟用此選項可讓系統針對您的使用者起始的所有 IPsec VPN 工作階段產生唯一公開金鑰。 啟用 PFS 可確保系統不會建立 Edge 閘道的私密金鑰和每個工作階段金鑰之間的連結。 損壞工作階段金鑰將不會影響除在受到特定金鑰保護之特定工作階段中交換的資料以外的資料。無法透過損壞伺服器的私密金鑰，來解密已封存的工作階段或未來工作階段。 啟用 PFS 時，此 Edge 閘道的 IPsec VPN 連線會產生輕微的處理額外負荷。 **重要** 唯一工作階段金鑰不得用於衍生任何其他金鑰。此外，IPsec VPN 通道的兩端都必須支援 PFS 才能使其運作。
名稱	(選擇性) 輸入連線的名稱。
本機識別碼	輸入 Edge 閘道執行個體的外部 IP 位址，此為 Edge 閘道的公用 IP 位址。 此 IP 位址將用於遠端站台上的 IPsec VPN 組態中的對等識別碼。
本機端點	輸入做為此連線之本機端點的網路。 本機端點可指定 Edge 閘道傳輸所在的組織虛擬資料中心的網路。通常，外部網路為本機端點。 如果使用預先共用金鑰新增 IP 至 IP 通道，本機識別碼可與本機端點 IP 相同。
本機子網路	輸入要在站台之間共用的網路，並使用逗號做為分隔符號輸入多個子網路。 透過使用 CIDR 格式輸入 IP 位址，以輸入網路範圍 (非特定 IP 位址)。例如，**192.168.99.0/24**。
對等識別碼	輸入唯一識別對等站台的對等識別碼。 對等識別碼是唯一識別終止 VPN 連線之遠端裝置的識別碼，通常是其公用 IP 位址。 對於使用憑證驗證的對等，識別碼必須為對等憑證中的辨別名稱。對於 PSK 對等，此識別碼可以是任何字串。NSX 最佳做法是使用遠端裝置的公用 IP 位址或 FQDN 做為對等識別碼。 如果對等 IP 位址來自另一個組織虛擬資料中心網路，您可以輸入對等的原生 IP 位址。如果為對等設定 NAT，您可以輸入對等的私人 IP 位址。
對等端點	輸入對等站台的 IP 位址或 FQDN，此為要連線的遠端裝置的公用位址。 **備註** 為對等設定 NAT 時，可以輸入裝置用於 NAT 的公用 IP 位址。
對等子網路	輸入 VPN 連線的遠端網路，並使用逗號做為分隔符號輸入多個子網路。 透過使用 CIDR 格式輸入 IP 位址，以輸入網路範圍 (非特定 IP 位址)。例如，**192.168.99.0/24**。

選項	動作
加密演算法	從下拉式功能表中選取加密演算法類型。 **備註** 您選取的加密類型必須符合在遠端站台 VPN 裝置上設定的加密類型。
驗證	選取驗證。選項包括： ■ **PSK** 預先共用金鑰 (PSK) 可指定 Edge 閘道和對等站台之間共用的秘密金鑰將用於驗證。 ■ **憑證** 憑證可指定在全域層級定義的憑證將用於驗證。此選項無法使用，除非您已在 **IPsec VPN** 索引標籤的**全域組態**畫面上設定全域憑證。
變更共用金鑰	(選擇性) 當您更新現有連線的設定時，您可以開啟此選項使**預先共用金鑰**欄位可供使用，以便您可以更新共用金鑰。
預先共用金鑰	如果您選取 **PSK** 做為驗證類型，請輸入英數密碼字串，該字串的長度上限為 128 個位元組。 **備註** 共用金鑰必須符合在遠端站台 VPN 裝置上設定的金鑰。最佳做法是在匿名站台連線至 VPN 服務時設定共用金鑰。
顯示共用金鑰	(選擇性) 啟用此選項，使共用金鑰顯示在畫面中。
Diffie-Hellman 群組	選取允許對等站台與此 Edge 閘道透過不安全的通訊通道建立共用密碼的加密編譯配置。 **備註** Diffie-Hellman 群組必須符合在遠端站台 VPN 裝置上設定的內容。
延伸	(選擇性) 輸入下列其中一個選項： ■ `securelocaltrafficbyip=`*IPAddress*，可透過 IPsec VPN 通道重新導向 Edge 閘道的本機流量。 這是預設值。 ■ `passthroughSubnets=`*PeerSubnetIPAddress*，支援重疊的子網路。

4 按一下**保留**。

5 按一下**儲存變更**。

儲存作業需要一分鐘時間才能完成。

後續步驟

設定遠端站台的連線。您必須在連線的兩端 (組織虛擬資料中心和對等站台) 設定 IPsec VPN 連線。

啟用此 Edge 閘道上的 IPsec VPN 服務。如果已至少設定一個 IPsec VPN 連線，您可以啟用此服務。請參閱啟用 Edge 閘道上的 IPsec VPN 服務。

啟用 Edge 閘道上的 IPsec VPN 服務

已設定至少一個 IPsec VPN 連線時，您可以啟用 Edge 閘道上的 IPsec VPN 服務。

必要條件

- 導覽至 IPsec VPN 畫面。

- 確認已為此 Edge 閘道設定至少一個 IPsec VPN 連線。請參閱設定 Edge 閘道的 IPsec VPN 站台連線中所述的步驟。

程序

1 在 **IPsec VPN** 索引標籤上，按一下**啟用狀態**。

2 按一下 **IPsec VPN 服務狀態**以啟用 IPsec VPN 服務。

3 按一下**儲存變更**。

結果

Edge 閘道 IPsec VPN 服務處於作用中狀態。

指定全域 IPsec VPN 設定

使用**全域組態**畫面，在 Edge 閘道層級設定 IPsec VPN 驗證設定。在此畫面上，可以設定全域預先共用金鑰，並啟用憑證驗證。

全域預先共用金鑰將用於對等端點設定為 **any** 的站台。

必要條件

- 如果您想要啟用憑證驗證，請確認在**憑證**畫面中至少有一個服務憑證和對應的 CA 簽署憑證。自我簽署憑證無法用於 IPsec VPN。請參閱將服務憑證新增至 Edge 閘道。
- 導覽至 IPsec VPN 畫面。

程序

1 開啟 Edge 閘道服務。

   a 從主功能表 (☰) 中，選取**雲端資源**。

   b 在左面板中，按一下 **Edge 閘道**。

   c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 在 **IPsec VPN** 索引標籤上，按一下**全域組態**。

3 (選擇性) 設定全域預先共用金鑰：

   a 啟用**變更共用金鑰**選項。

   b 輸入預先共用金鑰。

   全域預先共用金鑰 (PSK) 由對等端點設定為 any 的所有站台共用。如果全域 PSK 已設定，將 PSK 變更為空白值並儲存對現有設定沒有影響。

   c (選擇性) 選擇性啟用**顯示共用金鑰**，以顯示該預先共用金鑰。

   d 按一下**儲存變更**。

4 設定憑證驗證：

a 開啟**啟用憑證驗證**。

b 選取適當的服務憑證、CA 憑證與 CRL。

c 按一下**儲存變更**。

後續步驟

您可以選擇性地針對 Edge 閘道的 IPsec VPN 服務啟用記錄。請參閱 Edge 閘道的統計資料和記錄。

設定 L2 VPN

vCloud Director 環境中的 Edge 閘道支援 L2 VPN。L2 VPN 藉由允許虛擬機器維持網路連線，同時在跨地理界限保留相同的 IP 位址，進而擴充組織虛擬資料中心。您可以在 Edge 閘道上設定 L2 VPN 服務。

NSX 軟體提供 Edge 閘道的 L2 VPN 功能。L2 VPN 可讓您在兩個站台之間設定通道。即便在這些站台之間移動，虛擬機器仍保留在相同的子網路上，可讓您能夠使用 L2 VPN 延伸其網路以擴充組織虛擬資料中心。某個站台中的 Edge 閘道可以為其他站台上的虛擬機器提供所有服務。

若要建立 L2 VPN 通道，您可以設定 L2 VPN 伺服器和 L2 VPN 用戶端。如《NSX 管理指南》中所述，L2 VPN 伺服器是目的地 Edge 閘道，而 L2 VPN 用戶端是來源 Edge 閘道。在每個 Edge 閘道上設定 L2 VPN 之後，您必須同時在伺服器和用戶端上啟用 L2 VPN 服務。

備註 建立做為子介面的路由組織虛擬資料中心網路，必須存在於 Edge 閘道上。如需建立外部路由組織虛擬資料中心網路的相關步驟，請參閱《vCloud Director 管理員指南》。

程序

1 導覽至 L2 VPN 畫面

若要開始為 Edge 閘道設定 L2 VPN 服務，您必須導覽至 **L2 VPN** 畫面。

2 將 Edge 閘道設定為 L2 VPN 伺服器

L2 VPN 伺服器是 L2 VPN 用戶端即將連線到的目的地 NSX Edge。

3 將 Edge 閘道設定為 L2 VPN 用戶端

L2 VPN 用戶端是來源 NSX Edge，可起始與目的地 NSX Edge (L2 VPN 伺服器) 之間的通訊。

4 啟用 Edge 閘道上的 L2 VPN 服務

如果設定了所需的 L2 VPN 設定，您可以啟用 Edge 閘道上的 L2 VPN 服務。

導覽至 L2 VPN 畫面

若要開始為 Edge 閘道設定 L2 VPN 服務，您必須導覽至 **L2 VPN** 畫面。

程序

1 開啟 Edge 閘道服務。

   a 從主功能表 (☰) 中，選取**雲端資源**。

   b 在左面板中，按一下 **Edge 閘道**。

   c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 導覽至 **VPN > L2 VPN**。

後續步驟

設定 L2 VPN 伺服器。請參閱將 Edge 閘道設定為 L2 VPN 伺服器。

將 Edge 閘道設定為 L2 VPN 伺服器

L2 VPN 伺服器是 L2 VPN 用戶端即將連線到的目的地 NSX Edge。

如《NSX 管理指南》中所述，您可以將多個對等站台連線到此 L2 VPN 伺服器。

備註 變更站台組態設定會導致 Edge 閘道中斷連線並重新連線所有現有的連線。

必要條件

- 確認 Edge 閘道具有設定為 Edge 閘道上之子介面的路由組織虛擬資料中心網路。如需建立外部路由組織虛擬資料中心網路的相關步驟，請參閱《vCloud Director 管理員指南》。
- 導覽至 L2 VPN 畫面。
- 如果您想要將服務憑證繫結至 L2 VPN 連線，請確認伺服器憑證已上傳至 Edge 閘道。請參閱將服務憑證新增至 Edge 閘道。
- 您必須已設定伺服器的接聽程式 IP、接聽程式連接埠、加密演算法，以及至少一個對等站台，然後才能啟用 L2 VPN 服務。

程序

1 在 **L2 VPN** 索引標籤上，針對 L2 VPN 模式選取**伺服器**。

2 在**伺服器全域**索引標籤上，設定 L2 VPN 伺服器的全域組態詳細資料。

選項	動作
接聽程式 IP	選取 Edge 閘道之外部介面的主要或次要 IP 位址。
接聽程式連接埠	根據您組織的需求，適當編輯所顯示的值。 L2 VPN 服務的預設連接埠為 443。
加密演算法	選取加密演算法，以用於伺服器和用戶端之間的通訊。
服務憑證詳細資料	按一下**變更伺服器憑證**，以選取要繫結到 L2 VPN 伺服器的憑證。 在**變更伺服器憑證**視窗中，開啟**驗證伺服器憑證**，從清單中選取伺服器憑證，然後按一下**確定**。

3 若要設定對等站台，請按一下**伺服器站台**索引標籤。

4 按一下**新增** () 按鈕。

5 設定 L2 VPN 對等站台的設定。

選項	動作
已啟用	啟用此對等站台。
名稱	輸入對等站台的唯一名稱。
描述	(選擇性) 輸入描述。
使用者識別碼 **密碼** **確認密碼**	輸入用以驗證對等站台的使用者名稱和密碼。 對等站台上的使用者認證必須與用戶端上的認證相同。
延伸介面	至少選取一個要透過用戶端延伸的子介面。 可供選取的子介面是設定為 Edge 閘道上之子介面的組織虛擬資料中心網路。
出口最佳化閘道位址	(選擇性) 如果兩個站台之間的虛擬機器預設閘道相同，請輸入要在本機路由流量或透過 L2 VPN 通道封鎖流量的子介面的閘道 IP 位址。

6 按一下**保留**。

7 按一下**儲存變更**。

儲存作業需要一分鐘時間才能完成。

後續步驟

啟用此 Edge 閘道上的 L2 VPN 服務。請參閱啟用 Edge 閘道上的 L2 VPN 服務。

將 Edge 閘道設定為 L2 VPN 用戶端

L2 VPN 用戶端是來源 NSX Edge，可起始與目的地 NSX Edge (L2 VPN 伺服器) 之間的通訊。

必要條件

- 導覽至 L2 VPN 畫面。
- 如果此 L2 VPN 用戶端連線至使用伺服器憑證的 L2 VPN 伺服器，請確認對應的 CA 憑證上傳至 Edge 閘道，以針對此 L2 VPN 用戶端啟用伺服器憑證驗證。請參閱將 CA 憑證新增至 Edge 閘道以進行 SSL 憑證信任驗證。

程序

1 在 **L2 VPN** 索引標籤上，針對 L2 VPN 模式選取**用戶端**。

2 在**用戶端全域**索引標籤上，設定 L2 VPN 用戶端的全域組態詳細資料。

選項	描述
伺服器位址	輸入要連線此用戶端的 L2 VPN 伺服器的 IP 位址。
伺服器連接埠	輸入應連線此用戶端的 L2 VPN 伺服器連接埠。 預設連接埠為 443。
加密演算法	選取與伺服器通訊所使用的加密演算法。

選項	描述
延伸介面	選取要延伸到伺服器的子介面。 可供選取的子介面是設定為 Edge 閘道上之子介面的組織虛擬資料中心網路。
出口最佳化閘道位址	(選擇性) 如果兩個站台之間的虛擬機器預設閘道相同，則輸入子介面的閘道 IP 位址或流量不應透過通道傳輸到的 IP 位址。
使用者詳細資料	輸入用於向該伺服器進行驗證的使用者識別碼和密碼。

3 按一下**儲存變更**。

儲存作業需要一分鐘時間才能完成。

4 (選擇性) 若要設定進階選項，請按一下**用戶端進階**索引標籤。

5 如果此 L2 VPN 用戶端 Edge 無法直接存取網際網路，且必須使用 Proxy 伺服器連線到 L2 VPN 伺服器 Edge，請指定 Proxy 設定。

選項	描述
啟用安全 Proxy	選取此項可啟用安全 Proxy。
位址	輸入 Proxy 伺服器的 IP 位址。
連接埠	輸入 Proxy 伺服器連接埠。
使用者名稱 **密碼**	輸入 Proxy 伺服器的驗證認證。

6 若要啟用伺服器憑證驗證，請按一下**變更 CA 憑證**，然後選取適當的 CA 憑證。

7 按一下**儲存變更**。

儲存作業需要一分鐘時間才能完成。

後續步驟

啟用此 Edge 閘道上的 L2 VPN 服務。請參閱啟用 Edge 閘道上的 L2 VPN 服務。

啟用 Edge 閘道上的 L2 VPN 服務

如果設定了所需的 L2 VPN 設定，您可以啟用 Edge 閘道上的 L2 VPN 服務。

備註 如果已在此 Edge 閘道上設定 HA，請確保在 Edge 閘道上設定多個內部介面。如果只有單一介面存在，並且 HA 功能已使用此介面，則相同內部介面上的 L2 VPN 組態將會失效。

必要條件

- 如果此 Edge 閘道為 L2 VPN 伺服器，即目的地 NSX Edge，請確認已設定所需的 L2 VPN 伺服器設定以及至少一個 L2 VPN 對等站台。請參閱將 Edge 閘道設定為 L2 VPN 伺服器中所述的步驟。
- 如果此 Edge 閘道為 L2 VPN 用戶端，即來源 NSX Edge，請確認已設定 L2 VPN 用戶端設定。請參閱將 Edge 閘道設定為 L2 VPN 用戶端中所述的步驟。
- 導覽至 L2 VPN 畫面。

程序

1 在 **L2 VPN** 索引標籤上，按一下**啟用**切換按鈕。

2 按一下**儲存變更**。

結果

Edge 閘道的 L2 VPN 服務變為作用中狀態。

後續步驟

若要啟用 L2 VPN 伺服器以連線至 L2 VPN 用戶端，請在網際網路對向防火牆端建立 NAT 或防火牆規則。

從 Edge 閘道移除 L2 VPN 服務組態

您可以移除 Edge 閘道的現有 L2 VPN 服務組態。此動作還會停用 Edge 閘道上的 L2 VPN 服務。

必要條件

導覽至 L2 VPN 畫面

程序

1 向下捲動至 L2 VPN 畫面的底部，然後按一下**刪除組態**。

2 按一下**確定**以確認刪除。

結果

L2 VPN 服務已停用，並且會從 Edge 閘道移除組態詳細資料。

SSL 憑證管理

vCloud Director 環境中的 NSX 軟體能夠讓您搭配使用安全通訊端層 (SSL) 憑證與為 Edge 閘道設定的 SSL VPN-Plus 和 IPsec VPN 通道。

vCloud Director 環境中的 Edge 閘道支援自我簽署的憑證、憑證授權單位 (CA) 簽署的憑證，以及由 CA 產生和簽署的憑證。您可以產生憑證簽署要求 (CSR)、匯入憑證、管理匯入的憑證，以及建立憑證撤銷清單 (CRL)。

關於搭配使用憑證與組織虛擬資料中心

您可以在 vCloud Director 組織虛擬資料中心內管理下列網路區域的憑證。

- 組織虛擬資料中心網路與遠端網路之間的 IPsec VPN 通道。
- 遠端使用者與組織虛擬資料中心的私人網路和 Web 資源之間的 SSL VPN-Plus 連線。
- 兩個 NSX Edge 閘道之間的 L2 VPN 通道。
- 針對在組織虛擬資料中心內進行負載平衡所設定的虛擬伺服器與集區伺服器

如何使用用戶端憑證

您可以透過 CAI 命令或 REST 呼叫建立用戶端憑證。然後，可以將此憑證散佈到可在其網頁瀏覽器上安裝憑證的遠端使用者。

實作用戶端憑證的主要優點是可以儲存每個遠端使用者的參考用戶端憑證，並對照遠端使用者提供的用戶端憑證進行檢查。若要防止日後與特定使用者連線，您可以從安全伺服器的用戶端憑證清單中刪除參考憑證。刪除憑證即可拒絕與該使用者的連線。

針對 Edge 閘道產生憑證簽署要求

您必須先針對 Edge 閘道產生憑證簽署要求 (CSR)，才能從 CA 排序已簽署憑證或建立自我簽署憑證。

CSR 是必須在需要 SSL 憑證之 NSX Edge 閘道上產生的編碼檔案。使用 CSR 可標準化公司傳送其公開金鑰，以及用於識別其公司名稱和網域名稱之資訊的方式。

可使用必須保留在 Edge 閘道上的相符私密金鑰檔案產生 CSR。CSR 包含相符的公開金鑰及其他資訊，例如您的組織名稱、位置和網域名稱。

程序

1 開啟 Edge 閘道服務。

   a 從主功能表 (☰) 中，選取**雲端資源**。

   b 在左面板中，按一下 **Edge 閘道**。

   c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 按一下**憑證**索引標籤。

3 在**憑證**索引標籤上，按一下 **CSR**。

4 針對 CSR 設定下列選項：

選項	描述
一般名稱	輸入將使用憑證之組織的完整網域名稱 (FQDN) (例如 `www.example.com`)。 請勿在一般名稱中包含 `http://` 或 `https://` 前置詞。
組織單位	使用此欄位可區分與此憑證相關聯的 vCloud Director 組織內的部門。例如，工程部門或銷售部門。
組織名稱	輸入您公司的合法註冊名稱。 列出的組織必須是憑證要求中之網域名稱的合法註冊者。
位置	輸入您公司合法註冊所在的城市或位置。
州或省名稱	輸入您公司合法註冊所在州、省、區域或地區的全名 (請勿使用縮寫)。
國碼	輸入您公司合法註冊所在的國家/地區名稱。
私密金鑰演算法	輸入憑證的金鑰類型 (RSA 或 DSA)。 通常使用 RSA。金鑰類型定義在主機之間進行通訊的加密演算法。 **備註** SSL VPN-Plus 只支援 RSA 憑證。

選項	描述
金鑰大小	輸入金鑰大小 (位元)。 最小值為 2048 位元。
描述	(選擇性) 輸入憑證的說明。

5 按一下**保留**。

系統會產生 CSR，並將類型為 CSR 的新項目新增至畫面清單。

結果

在畫面上的清單中，當您選取類型為 CSR 的項目時，CSR 詳細資料會顯示在畫面中。您可以複製 CSR 顯示的 PEM 格式資料，並提交給憑證授權機構 (CA) 以取得 CA 簽署憑證。

後續步驟

透過以下兩個選項之一，使用 CSR 建立服務憑證：

- 將 CSR 傳輸至 CA 以取得 CA 簽署憑證。當 CA 向您傳送已簽署憑證時，將已簽署憑證匯入系統中。請參閱匯入與針對 Edge 閘道產生之 CSR 對應的 CA 簽署憑證。
- 使用 CSR 建立自我簽署的憑證。請參閱設定自我簽署的服務憑證。

匯入與針對 Edge 閘道產生之 CSR 對應的 CA 簽署憑證

產生憑證簽署要求 (CSR) 並根據該 CSR 取得 CA 簽署憑證後，您可以匯入該 CA 簽署憑證，以便由 Edge 閘道使用。

必要條件

確認您已取得與 CSR 對應的 CA 簽署憑證。如果 CA 簽署憑證中的私密金鑰不符合所選 CSR 的金鑰，則匯入程序會失敗。

程序

1 開啟 Edge 閘道服務。

a 從主功能表 (☰) 中，選取**雲端資源**。

b 在左面板中，按一下 **Edge 閘道**。

c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 按一下**憑證**索引標籤。

3 在您要匯入 CA 簽署憑證之畫面上的資料表中選取 CSR。

4 匯入簽署的憑證。

a 按一下 **為 CSR 產生的已簽署憑證**。

b 提供 CA 簽署憑證的 PEM 資料。

- 如果資料位於系統上可導覽到的 PEM 檔案中，按一下**上傳**按鈕瀏覽到該檔案並加以選取。
- 如果您可以複製並貼上 PEM 資料，請將其貼到**已簽署憑證 (PEM 格式)** 欄位。

  包括 **-----BEGIN CERTIFICATE-----** 和 **-----END CERTIFICATE-----** 行。

c (選擇性) 輸入描述。

d 按一下**保留**。

備註 如果 CA 簽署憑證中的私密金鑰不符合您在 [憑證] 畫面上選取之 CSR 的金鑰，則匯入程序會失敗。

結果

類型為「服務憑證」的 CA 簽署憑證會出現在畫面清單中。

後續步驟

視需要將 CA 簽署憑證連結至 SSL VPN-Plus 或 IPsec VPN 通道。請參閱設定 SSL VPN 伺服器設定與指定全域 IPsec VPN 設定。

設定自我簽署的服務憑證

您可以透過 Edge 閘道設定自我簽署的服務憑證，以用於其 VPN 相關功能。您可以建立、安裝和管理自我簽署憑證。

如果 [憑證] 畫面上有可用的服務憑證，您可以在設定 Edge 閘道的 VPN 相關設定時指定該服務憑證。VPN 會將指定的服務憑證提供給存取 VPN 的用戶端。

必要條件

確認在 Edge 閘道的**憑證**畫面上至少有一個 CSR。請參閱針對 Edge 閘道產生憑證簽署要求。

程序

1 開啟 Edge 閘道服務。

a 從主功能表 (☰) 中，選取**雲端資源**。

b 在左面板中，按一下 **Edge 閘道**。

c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 按一下**憑證**索引標籤。

3 在清單中選取要用於此自我簽署憑證的 CSR，然後按一下**自我簽署 CSR**。

4 輸入自我簽署憑證的有效天數。

5 按一下**保留**。

系統會產生自我簽署的憑證，並將類型為「服務憑證」的新項目新增至畫面清單。

結果

自我簽署的憑證在 Edge 閘道上可供使用。在畫面上的清單中，當您選取類型為「服務憑證」的項目時，其詳細資料會顯示在畫面中。

將 CA 憑證新增至 Edge 閘道以進行 SSL 憑證信任驗證

將 CA 憑證新增至 Edge 閘道，可啟用提供給 Edge 閘道進行驗證之 SSL 憑證的信任驗證，通常是用於 VPN 與 Edge 閘道連線的用戶端憑證。

通常，將公司或組織的根憑證新增為 CA 憑證。典型用途是 SSL VPN，您需要使用憑證來驗證 VPN 用戶端。用戶端憑證會散佈至 VPN 用戶端，當 VPN 用戶端連線時，其用戶端憑證會根據 CA 憑證進行驗證。

備註 新增 CA 憑證時，通常會設定相關的憑證撤銷清單 (CRL)。CRL 用來阻止提供已撤銷憑證的用戶端。請參閱將憑證撤銷清單新增至 Edge 閘道。

必要條件

確認您具有 PEM 格式的 CA 憑證資料。在使用者介面中，可以貼上 CA 憑證的 PEM 資料，或瀏覽到包含該資料並可從您的本機系統網路中存取的檔案。

程序

1 開啟 Edge 閘道服務。

a 從主功能表 (☰) 中，選取**雲端資源**。

b 在左面板中，按一下 **Edge 閘道**。

c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 按一下**憑證**索引標籤。

3 按一下 **CA 憑證**。

4 提供 CA 憑證資料。

- 如果資料位於系統上可導覽到的 PEM 檔案中，按一下**上傳**按鈕瀏覽到該檔案並加以選取。
- 如果您可以複製並貼上 PEM 資料，請將其貼到 **CA 憑證 (PEM 格式)** 欄位。

  包括 `-----BEGIN CERTIFICATE-----` 和 `-----END CERTIFICATE-----` 行。

5 (選擇性) 輸入描述。

6 按一下**保留**。

結果

類型為「CA 憑證」的 CA 憑證會出現在畫面清單中。此 CA 憑證現可供您在設定 Edge 閘道的 VPN 相關設定時進行指定。

將憑證撤銷清單新增至 Edge 閘道

憑證撤銷清單 (CRL) 是核發憑證授權機構 (CA) 宣告已撤銷的數位憑證清單，以便系統可更新，不再信任提供這些已撤銷憑證的使用者。您可以將 CRL 新增至 Edge 閘道。

如《NSX 管理指南》中所述，CRL 包含下列項目：

- 已撤銷的憑證和撤銷原因
- 核發憑證的日期
- 核發憑證的實體
- 下一版本的預定日期

當潛在使用者嘗試存取伺服器時，伺服器會根據該特定使用者的 CRL 項目允許或拒絕存取。

程序

1 開啟 Edge 閘道服務。

   a 從主功能表 (☰) 中，選取**雲端資源**。

   b 在左面板中，按一下 **Edge 閘道**。

   c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 按一下**憑證**索引標籤。

3 按一下 **CRL**。

4 提供 CRL 資料。

   - 如果資料位於系統上可導覽到的 PEM 檔案中，按一下**上傳**按鈕瀏覽到該檔案並加以選取。
   - 如果您可以複製並貼上 PEM 資料，請將其貼到 **CRL (PEM 格式)** 欄位。

     包括 **-----BEGIN X509 CRL-----** 和 **-----END X509 CRL-----** 行。

5 (選擇性) 輸入描述。

6 按一下**保留**。

結果

CRL 會出現在畫面清單中。

將服務憑證新增至 Edge 閘道

將服務憑證新增至 Edge 閘道會使這些憑證可用於 Edge 閘道的 VPN 相關設定中。您可以將服務憑證新增至**憑證**畫面。

必要條件

確認您具有採用 PEM 格式的服務憑證及其私密金鑰。在使用者介面中，可以貼上 PEM 資料，或瀏覽到包含該資料並可從您的本機系統網路中存取的檔案。

程序

1 開啟 Edge 閘道服務。

   a 從主功能表 (☰) 中，選取**雲端資源**。

   b 在左面板中，按一下 **Edge 閘道**。

   c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 按一下**憑證**索引標籤。

3 按一下**服務憑證**。

4 輸入服務憑證之 PEM 格式的資料。

   - 如果資料位於系統上可導覽到的 PEM 檔案中，按一下**上傳**按鈕瀏覽到該檔案並加以選取。
   - 如果您可以複製並貼上 PEM 資料，請將其貼到**服務憑證 (PEM 格式)** 欄位。

     包括 `-----BEGIN CERTIFICATE-----` 和 `-----END CERTIFICATE-----` 行。

5 輸入憑證私密金鑰之 PEM 格式的資料。

   - 如果資料位於系統上可導覽到的 PEM 檔案中，按一下**上傳**按鈕瀏覽到該檔案並加以選取。
   - 如果您可以複製並貼上 PEM 資料，請將其貼到**私密金鑰 (PEM 格式)** 欄位。

     包括 `-----BEGIN RSA PRIVATE KEY-----` 和 `-----END RSA PRIVATE KEY-----` 行。

6 輸入私密金鑰複雜密碼並進行確認。

7 (選擇性) 輸入描述。

8 按一下**保留**。

結果

類型為「服務憑證」的憑證會出現在畫面清單中。此服務憑證現可供您在設定 Edge 閘道的 VPN 相關設定時進行選取。

自訂群組物件

vCloud Director 環境中的 NSX 軟體提供定義特定實體之集合與群組的功能，可供您在指定其他網路相關組態 (例如在防火牆規則中) 時加以使用。

建立用於防火牆規則和 DHCP 轉送組態的 IP 集

IP 集是可在組織虛擬資料中心層級建立的一組 IP 位址。您可以使用 IP 集做為防火牆規則或 DHCP 轉送組態中的來源或目的地。

您可以使用**群組物件**頁面建立 IP 集。若要開啟此頁面，您必須導覽至組織 VDC 的 Distributed Firewall 設定，或屬於組織 VDC 之 Edge 閘道的服務設定。

程序

1 開啟**群組物件**頁面。

選項	動作
從組織 VDC 的 Distributed Firewall 設定	a 從主功能表 (☰) 中，選取**雲端資源**。 b 在左面板中，按一下**組織 VDC**。 c 選取目標組織虛擬資料中心名稱旁邊的選項按鈕，然後按一下**管理防火牆**。 d 按一下**群組物件**索引標籤。
從組織 VDC 上的 Edge 閘道的服務設定	a 從主功能表 (☰) 中，選取**雲端資源**。 b 在左面板中，按一下 **Edge 閘道**。 c 選取屬於目標組織虛擬資料中心的 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。 d 按一下**群組物件**索引標籤。

2 按一下 **IP 集**索引標籤。

畫面上將會顯示已定義的 IP 集。

3 若要新增 IP 集，請按一下**建立** (+) 按鈕。

4 輸入 IP 集的名稱和選擇性說明，以及要包含在此集中的 IP 位址。

5 若要儲存此 IP 集，請按一下**保留**。

結果

新 IP 集可選取做為防火牆規則或 DHCP 轉送組態中的來源或目的地。

建立用於防火牆規則的 MAC 集

MAC 集是一組可在組織虛擬資料中心層級建立的 MAC 位址。您可以使用 MAC 集做為防火牆規則中的來源或目的地。

您可以使用**群組物件**頁面建立 MAC 集。若要開啟此頁面，您必須導覽至組織 VDC 的 Distributed Firewall 設定，或屬於組織 VDC 之 Edge 閘道的服務設定。

程序

1 開啟**群組物件**頁面。

選項	動作
從組織 VDC 的 Distributed Firewall 設定	a 從主功能表 (☰) 中，選取**雲端資源**。 b 在左面板中，按一下**組織 VDC**。 c 選取目標組織虛擬資料中心名稱旁邊的選項按鈕，然後按一下**管理防火牆**。 d 按一下**群組物件**索引標籤。
從組織 VDC 上的 Edge 閘道的服務設定	a 從主功能表 (☰) 中，選取**雲端資源**。 b 在左面板中，按一下 **Edge 閘道**。 c 選取屬於目標組織虛擬資料中心的 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。 d 按一下**群組物件**索引標籤。

2 按一下 **MAC 集**索引標籤。

畫面上將會顯示已定義的 MAC 集。

3 若要新增 MAC 集，請按一下**建立** (+) 按鈕。

4 輸入集的名稱、說明 (選擇性) 以及要包含在集中的 MAC 位址。

5 若要儲存 MAC 集，請按一下**保留**。

結果

新 MAC 集可選取做為防火牆規則中的來源或目的地。

檢視可用於防火牆規則的服務

您可以檢視可用於防火牆規則的服務清單。在此內容中，服務是通訊協定與連接埠的組合。

您可以使用**群組物件**頁面檢視可用的服務。若要開啟此頁面，您必須導覽至組織 VDC 的 Distributed Firewall 設定，或屬於組織 VDC 之 Edge 閘道的服務設定。

程序

1 開啟**群組物件**頁面。

選項	動作
從組織 VDC 的 Distributed Firewall 設定	a 從主功能表 (☰) 中，選取**雲端資源**。 b 在左面板中，按一下**組織 VDC**。 c 選取目標組織虛擬資料中心名稱旁邊的選項按鈕，然後按一下**管理防火牆**。 d 按一下**群組物件**索引標籤。
從組織 VDC 上的 Edge 閘道的服務設定	a 從主功能表 (☰) 中，選取**雲端資源**。 b 在左面板中，按一下 **Edge 閘道**。 c 選取屬於目標組織虛擬資料中心的 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。 d 按一下**群組物件**索引標籤。

2 按一下**服務**索引標籤。

結果

可用服務即會顯示在畫面上。

檢視可用於防火牆規則的服務群組

您可以檢視可用於防火牆規則的服務群組清單。在此內容中，服務是通訊協定與連接埠的組合，而服務群組是一組服務或其他服務群組。

您可以使用**群組物件**頁面檢視可用的服務群組。若要開啟此頁面，您必須導覽至組織 VDC 的 Distributed Firewall 設定，或屬於組織 VDC 之 Edge 閘道的服務設定。

程序

1 開啟**群組物件**頁面。

選項	動作
從組織 VDC 的 Distributed Firewall 設定	a 從主功能表 (☰) 中，選取**雲端資源**。 b 在左面板中，按一下**組織 VDC**。 c 選取目標組織虛擬資料中心名稱旁邊的選項按鈕，然後按一下**管理防火牆**。 d 按一下**群組物件**索引標籤。
從組織 VDC 上的 Edge 閘道的服務設定	a 從主功能表 (☰) 中，選取**雲端資源**。 b 在左面板中，按一下 **Edge 閘道**。 c 選取屬於目標組織虛擬資料中心的 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。 d 按一下**群組物件**索引標籤。

2 按一下**服務群組**索引標籤。

結果

可用服務群組將會顯示在畫面上。[說明] 資料行會顯示分組到各服務群組的服務。

檢視 Edge 閘道上的網路使用狀況和 IP 配置

您可以檢視 Edge 閘道上的網路，以及 IP 集區使用狀況和子網路的相關資訊。您也可以檢視配置給每個網路的 IP 位址。

程序

1. 從主功能表 (☰) 中，選取**雲端資源**。
2. 在左面板中，按一下 **Edge 閘道**，然後按一下目標 Edge 閘道的名稱。
3. 若要檢視外部網路及其 IP 集區使用狀況和子網路的相關資訊，請按一下**外部網路 > 網路與子網路**索引標籤。
4. 若要檢視外部網路及其 IP 位址和類別的相關資訊，請按一下**外部網路 > IP 配置**索引標籤。

編輯 Edge 閘道內容

啟用或停用 Edge 閘道上的分散式路由

在 Edge 閘道上啟用 vCloud Director 分散式路由之後，組織管理員可以建立其分散式介面連線到此 Edge 閘道的多個路由組織虛擬資料中心網路。這些網路上的流量會經過最佳化，用於虛擬機器到虛擬機器的通訊。

必要條件

支援的 NSX Manager 執行個體設定有 NSX Controller 叢集。請參閱《NSX 管理指南》。

程序

1. 從主功能表 (☰) 中，選取**雲端資源**。
2. 在左面板中，按一下 **Edge 閘道**。
3. 選取目標 Edge 閘道的名稱旁邊的選項按鈕，然後按一下**啟用分散式路由**或**停用分散式路由**。
4. 按一下**確定**以確認。

修改外部網路和 Edge 閘道設定

若要修改外部網路和 Edge 閘道設定，您可以使用**編輯 Edge 閘道**精靈，其中包含與用來建立 Edge 閘道的精靈相同的頁面。

您可以修改新增 Edge 閘道時所進行的設定。請參閱 新增 Edge 閘道。

若要修改分散式路由設定，請參閱啟用或停用 Edge 閘道上的分散式路由。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下 **Edge 閘道**。

3 按一下要修改之 Edge 閘道名稱旁邊的選項按鈕，然後按一下**編輯**。

4 若要修改 Edge 閘道設定，請按**下一步**瀏覽**編輯 Edge 閘道**精靈的頁面，然後在**即將完成**頁面上按一下**完成**。

編輯 Edge 閘道的一般設定

您可以修改 Edge 閘道的名稱與說明，啟用或停用 FIPS 模式和高可用性狀態，並變更 Edge 閘道大小組態。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下 **Edge 閘道**，然後按一下目標 Edge 閘道的名稱。

3 在**一般**索引標籤的右上角，按一下**編輯**。

4 (選擇性) 編輯 Edge 閘道的名稱和說明。

5 (選擇性) 開啟或關閉每個一般 Edge 閘道設定。

一般設定	描述
FIPS 模式	設定 Edge 閘道以使用 NSX FIPS 模式。
高可用性	允許自動容錯移轉至備用 Edge 閘道。

6 (選擇性) 變更您的系統資源的 Edge 閘道組態。

選項	描述
精簡	需要較少的記憶體和計算資源。
大型	相較於使用 [精簡] 選項，可提供更大的容量和更高的效能。大型與超大型組態提供相同的安全性功能。
超大型	用於具有負載平衡器及大量並行工作階段的環境。
四倍大	用於高輸送量環境。需要高連線速率。

7 若要確認變更，請按一下**儲存**。

編輯 Edge 閘道的預設閘道

您可以變更 Edge 閘道用作預設閘道的網路。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下 **Edge 閘道**，然後按一下目標 Edge 閘道的名稱。

3 在**外部網路 > 預設閘道**索引標籤的右上角，按一下**編輯**。

4 (選擇性) 將網路設定為預設閘道。

   a 開啟**設定預設閘道**切換按鈕。

   b 選取目標外部網路名稱旁邊的選項按鈕，然後選取目標 IP 位址旁邊的選項按鈕。

   c (選擇性) 開啟**使用預設閘道進行 DNS 轉送**切換按鈕。

5 若要確認變更，請按一下**儲存**。

編輯 Edge 閘道的 IP 設定

您可以修改 Edge 閘道上的外部網路的 IP 設定。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下 **Edge 閘道**，然後按一下目標 Edge 閘道的名稱。

3 在**外部網路 > IP 設定**索引標籤上，按一下**編輯**。

4 對於 Edge 閘道上的每個網路，請在 **IP 位址**儲存格中輸入 IP 位址，或將儲存格保留空白。

   如果您未輸入網路的 IP 位址，系統會將任意 IP 位址指派給此網路。

5 若要確認變更，請按一下**儲存**。

編輯 Edge 閘道上的子配置 IP 集區

您可以從 Edge 閘道上外部網路的可用 IP 集區中子配置多個靜態 IP 集區。

備註 透過子配置將 IP 位址配置給 Edge 閘道是提供者向閘道指派 IP 位址擁有權的程序。vCloud Director 會在子配置程序期間使用次要位址自動設定相應的閘道介面，如果在 vCloud Director 外部使用任何 IP 位址，可能會導致 IP 位址衝突。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下 **Edge 閘道**，然後按一下目標 Edge 閘道的名稱。

3 按一下**外部網路 > 子配置的 IP 集區**索引標籤。

   您可以查看此 Edge 閘道上每個外部網路的目前子配置的 IP 集區。

4 按一下外部網路名稱旁邊的選項按鈕，然後按一下**編輯**。

   您可以查看此外部網路的可用 IP 集區，以及目前子配置的 IP 集區 (如果已設定)。

5 編輯為此外部網路子配置的 IP 集區，然後按一下**儲存**。

   您可以從可用 IP 集區的範圍中新增、修改和移除 IP 位址和範圍。

結果

系統會合併重疊的 IP 範圍。

編輯 Edge 閘道的速率限制

您可以設定 Edge 閘道上每個外部網路的輸入和輸出速率限制。

速率限制僅會套用至有靜態繫結的分散式連接埠群組所支援的外部網路。

程序

1. 從主功能表 (☰) 中，選取**雲端資源**。
2. 在左面板中，按一下 **Edge 閘道**，然後按一下目標 Edge 閘道的名稱。
3. 在**外部網路 > 速率限制**索引標籤的右上角，按一下**編輯**。

   您可以查看此 Edge 閘道上每個外部網路的目前速率限制。
4. 編輯速率限制，然後按一下**儲存**。

   對於 Edge 閘道上的每個外部網路，您可以啟用或停用速率限制，並且可以變更傳入和傳出速率。

重新部署 Edge 閘道

您可以刪除 Edge 閘道後，使用最新組態部署新的 Edge 閘道應用裝置。

如果 Edge 服務未按預期運作，您可以重新部署 Edge 閘道應用裝置。

您可以重新部署舊版 Edge 閘道，以將 Edge 閘道移轉至新建立的 Edge 叢集。

重新部署 Edge 閘道時，vCloud Director 會將其刪除並使用最新組態重新建立。

程序

1. 從主功能表 (☰) 中，選取**雲端資源**。
2. 在左面板中，按一下 **Edge 閘道**。
3. 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**重新部署**。
4. 按一下**確定**以確認。

結果

將 Edge 閘道虛擬機器取代為新的虛擬機器，並還原所有服務。

刪除 Edge 閘道

您可以從組織虛擬資料中心移除 Edge 閘道。

必要條件

刪除使用目標 Edge 閘道的所有組織虛擬資料中心網路。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下 **Edge 閘道**。

3 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**刪除**。

4 按一下**刪除**以確認。

Edge 閘道的統計資料和記錄

您可以檢視 Edge 閘道的統計資料和記錄。

檢視統計資料

您可以在 **Edge 閘道服務**畫面上檢視統計資料。

程序

1 開啟 Edge 閘道服務。

   a 從主功能表 (☰) 中，選取**雲端資源**。

   b 在左面板中，按一下 **Edge 閘道**。

   c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 按一下**統計資料**索引標籤。

3 根據您要檢視的統計資料的類型導覽索引標籤。

選項	描述
連線	[連線] 畫面可提供運作可見度。此畫面會針對流經所選 Edge 閘道之介面的流量以及防火牆和負載平衡器服務的連線統計資料顯示圖表。 選取您要檢視其統計資料的期間。
IPsec VPN	[IPsec VPN] 畫面會顯示 IPsec VPN 狀態和統計資料，以及每個通道的狀態和統計資料。
L2 VPN	[L2 VPN] 畫面會顯示 L2 VPN 狀態和統計資料。

啟用記錄

您可以針對 Edge 閘道啟用記錄。若要完成組態，除了針對要收集其記錄資料的功能啟用記錄以外，您還必須具有 Syslog 伺服器用來接收收集的記錄資料。在 [Edge 設定] 畫面上設定 Syslog 伺服器時，您可以存取該 Syslog 伺服器中記錄的資料。

必要條件

此作業需要預先定義之**組織管理員**角色中包含的權限或一組同等權限。

程序

1 開啟 Edge 閘道服務。

   a 從主功能表 (☰) 中，選取**雲端資源**。

   b 在左面板中，按一下 **Edge 閘道**。

   c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 在 **Edge 設定**索引標籤上，按一下**編輯 Syslog 伺服器**按鈕。

   您可以針對已啟用記錄的服務，自訂 Syslog 伺服器之 Edge 閘道的網路相關記錄。

   如果 vCloud Director 系統管理員已設定用於 vCloud Director 環境的 Syslog 伺服器，系統預設會使用該 Syslog 伺服器，並且其 IP 位址會顯示在 **Edge 設定**畫面上。

3 針對每個功能啟用記錄。

   - 在 **NAT** 索引標籤上，按一下 **DNAT 規則**按鈕，然後開啟**啟用記錄**切換按鈕。

     記錄位址轉譯。

   - 在 **NAT** 索引標籤上，按一下 **SNAT 規則**按鈕，然後開啟**啟用記錄**切換按鈕。

     記錄位址轉譯。

   - 在**路由**索引標籤上，按一下**路由組態**，然後在 [動態路由組態] 下開啟**啟用記錄**切換按鈕。

     記錄動態路由活動。從**記錄層級**下拉式功能表中，您可以選取要記錄的訊息狀態層級的下限。

   - 在**負載平衡器**索引標籤上，按一下**全域組態**，然後開啟**啟用記錄**切換按鈕。

     記錄負載平衡器的流量。從**記錄層級**下拉式功能表中，您可以選取要記錄的訊息狀態層級的下限。

   - 在 **VPN** 索引標籤上，導覽至 **IPSec VPN > 記錄設定**，然後開啟**啟用記錄**切換按鈕。

     記錄本機子網路和對等子網路之間的流量。從**記錄層級**下拉式功能表中，您可以選取要記錄的訊息狀態層級的下限。

   - 在 **SSL VPN-Plus** 索引標籤上，按一下**一般設定**，然後開啟**啟用記錄**切換按鈕。

     維護流經 SSL VPN 閘道的流量記錄。

   - 在 **SSL VPN-Plus** 索引標籤上，按一下**伺服器設定**，然後開啟**啟用記錄**切換按鈕。

     針對 Syslog 記錄 SSL VPN 伺服器上所發生的活動。從**記錄層級**下拉式功能表中，您可以選取要記錄的訊息狀態層級的下限。

啟用對 Edge 閘道的 SSH 命令列存取

您可以啟用對 Edge 閘道的 SSH 命令列存取。

程序

1 開啟 Edge 閘道服務。

   a 從主功能表 (☰) 中，選取**雲端資源**。

   b 在左面板中，按一下 **Edge 閘道**。

   c 按一下目標 Edge 閘道名稱旁邊的選項按鈕，然後按一下**服務**。

2 按一下 **Edge 設定**索引標籤。

3 設定 SSH。

選項	描述
使用者名稱 **密碼** **重新輸入密碼**	輸入對此 Edge 閘道之 SSH 存取的認證。 依預設，SSH 使用者名稱為 **admin**。
密碼到期	輸入密碼的到期期間 (以天為單位)。
登入橫幅	輸入在開始 SSH 連線至 Edge 閘道時，向使用者顯示的文字。

4 開啟**已啟用**切換按鈕。

後續步驟

設定適當的 NAT 或防火牆規則，以允許對此 Edge 閘道的 SSH 存取。

管理組織虛擬資料中心網路

8

本章節討論下列主題：

- 管理 NSX-T 組織虛擬資料中心網路

管理 NSX-T 組織虛擬資料中心網路

只有系統管理員可以建立、修改和刪除以 NSX-T 邏輯交換器的組織虛擬資料中心網路。

若要管理組織虛擬資料中心網路，系統管理員必須登入 Service Provider Admin Portal 並導覽至目標組織的 vCloud Director 租用戶入口網站。

如需管理以 NSX Data Center for vSphere 為基礎的組織虛擬資料中心網路的相關資訊，請參閱《vCloud Director 租用戶入口網站指南》。

新增 NSX-T 組織虛擬資料中心網路

身為系統管理員，您可以透過從相關聯的 NSX-T Manager 執行個體匯入邏輯交換器來建立組織虛擬資料中心網路。

備註 使用 NSX-T 邏輯交換器，您可以只建立 IPv4 隔離組織網路。無法根據 NSX-T 邏輯交換器建立直接或路由的組織網路。

必要條件

- 支援目標組織虛擬資料中心的提供者虛擬資料中心必須與 NSX-T Manager 執行個體相關聯。
- 您建立的 NSX-T 邏輯交換器中至少有一個未被其他組織虛擬資料中心網路使用。

如需設定 NSX-T 邏輯交換器的相關資訊，請參閱《NSX-T 管理指南》。如需建立 NSX-T Manager 執行個體支援的提供者 VDC 的相關資訊，請參閱《服務提供者適用的 vCloud API 程式設計指南》。

程序

1 導覽至目標組織的 vCloud Director 租用戶入口網站。

   a 從主功能表 (☰) 中，選取**雲端資源**。

   b 在**組織**下，按一下目標組織的名稱。

   系統會將您重新導向至此組織的 vCloud Director 租用戶入口網站的**資料中心**視圖。

2 如果組織中有多個 VDC，請按一下目標組織 VDC 的卡。

3 在左面板中的**網路**下，按一下**網路**。

4 按一下**匯入**。

匯入邏輯交換器精靈隨即顯示。

5 輸入新組織 VDC 網路的名稱，並選擇性地輸入其說明，然後按**下一步**。

6 從可用 NSX-T 邏輯交換器清單中，按一下交換器名稱旁邊的選項按鈕以選取目標交換器，然後按**下一步**。

7 輸入網路的無類別網域間路由 (CIDR) 設定。

使用格式 *network_gateway_IP_address/subnet_prefix_length*，例如 **192.167.1.1/24**。

如果交換器設定了子網路，系統會預先填入此資訊。

8 (選擇性) 設定 DNS 設定和靜態 IP 集區。

您可以新增多個 IP 位址和 IP 範圍。

9 按**下一步**。

10 檢視 [即將完成] 頁面並按一下**完成**。

編輯 NSX-T 組織虛擬資料中心網路

您可以修改以 NSX-T 邏輯交換器為基礎的組織虛擬資料中心網路的名稱、說明、DNS 設定和靜態 IP 集區。您無法編輯網路的無類別網域間路由 (CIDR) 設定。

程序

1 導覽至目標組織的 vCloud Director 租用戶入口網站。

a 從主功能表 (☰) 中，選取**雲端資源**。

b 在**組織**下，按一下目標組織的名稱。

系統會將您重新導向至此組織的 vCloud Director 租用戶入口網站的**資料中心**視圖。

2 如果組織中有多個 VDC，請按一下目標組織 VDC 的卡。

3 在左面板中的**網路**下，按一下**網路**。

4 按一下目標網路名稱旁邊的選項按鈕，然後按一下**修改**。

編輯組織 VDC 網路精靈隨即顯示。

5 (選擇性) 在**一般**索引標籤上，編輯網路的名稱和說明。

6 (選擇性) 在**設定網路**索引標籤上，編輯網路的 DNS 設定和靜態 IP 集區。

您可以新增、修改和移除 IP 位址與 IP 範圍。

7 按一下**儲存**。

刪除 NSX-T 組織虛擬資料中心網路

如果您不再使用 NSX-T 組織虛擬資料中心網路，則可以刪除此網路。

程序

1 導覽至目標組織的 vCloud Director 租用戶入口網站。

   a 從主功能表 (☰) 中，選取**雲端資源**。

   b 在**組織**下，按一下目標組織的名稱。

   系統會將您重新導向至此組織的 vCloud Director 租用戶入口網站的**資料中心**視圖。

2 如果組織中有多個 VDC，請按一下目標組織 VDC 的卡。

3 在左面板中的**網路**下，按一下**網路**。

4 按一下目標網路名稱旁邊的選項按鈕，然後按一下**刪除**。

5 按一下**確定**以確認。

管理 SDDC 和 SDDC Proxy

9

從 9.7 版開始，vCloud Director 可做為承租人與基礎 vSphere 環境之間的 HTTP Proxy 伺服器。軟體定義資料中心 (SDDC) 會封裝已連結 vCenter Server 執行個體的基礎結構。SDDC Proxy 可用作 SDDC 中的元件的存取點，例如 vCenter Server 執行個體、ESXi 主機或 NSX Manager 執行個體。

透過 SDDC 功能，您可以將 vCloud Director 用作所有 vSphere 環境的管理中心點。

- 您可以將 vCenter Server 執行個體的資源專用於單一承租人，方法是僅向其組織發佈對應的 SDDC。該承租人不與其他承租人共用這些資源。該承租人可以在不需要 VPN 的情況下使用使用者介面或 API Proxy 存取此 SDDC。
- 您可以將 vCloud Director 用作登錄所有 vCenter Server 執行個體的輕量型目錄。
- 您可以將 vCloud Director 用作所有 vCenter Server 執行個體的 API 端點。

建立 SDDC 之前，您必須將目標 vCenter Server 執行個體連結到 vCloud Director。請參閱單獨連結 NSX Manager 執行個體或與 vCenter Server 執行個體連結在一起。

備註 依預設，使用連結的 vCenter Server 執行個體，您可以建立提供者 VDC 或 SDDC。如果已建立由 vCenter Server 執行個體支援的提供者 VDC，則無法使用此 vCenter Server 執行個體建立 SDDC，反之亦然。您可以使用 vCloud API 修改 vCloud Director 安裝的系統設定，以便 vCenter Server 執行個體可以同時支援提供者 VDC 和 SDDC。

您可以建立 SDDC 和 SDDC Proxy 並將其發佈到雲端中的組織。使用者可以使用 SDDC Proxy 存取基礎 vSphere 環境。使用者可以使用其 vCloud Director 帳戶登入代理元件的使用者介面或 API。

vCloud Director 中的 SDDC 移除了 vCenter Server 可供公開存取的需求。若要控制存取，您可以啟用和停用 vCloud Director 中的 SDDC，並且可以啟用和停用 SDDC Proxy。

建立和管理 SDDC 與 SDDC Proxy

若要建立並管理 SDDC 和 Proxy，您必須使用 vCloud OpenAPI。請參閱《vCloud OpenAPI 入門》，網址為：https://code.vmware.com。

重要 vCloud Director 需要與每個 vCenter Server 執行個體建立直接網路連線以用作 SDDC。如果 vCenter Server 執行個體使用外部 Platform Services Controller 執行個體，vCloud Director 也需要與 Platform Services Controller 執行個體建立直接網路連線。

若要在代理的 SDDC 中使用 VMware OVF Tool，vCloud Director 需要與每台 ESXi 主機的直接連線。

1 建立已連結並啟用的 vCenter Server 執行個體所支援的 SSDC。

   vCloud Director 會為 vCenter Server 執行個體建立具有預設 Proxy 的 SDDC。如果 vCenter Server 執行個體使用外部 Platform Services Controller 執行個體，vCloud Director 也會為 Platform Services Controller 執行個體建立 Proxy。

2 取得已建立的 Proxy 的憑證和指紋，並確認此憑證和指紋存在且正確無誤。

3 啟用 SDDC。

4 將 SDDC 發佈到一或多個組織。

5 若要讓使用者能夠從 vCloud Director Tenant Portal 存取 SDDC 和 SDDC Proxy，您必須向其組織發佈 **CPOM 延伸**外掛程式。請參閱從組織發佈或解除發佈外掛程式。

建立和發佈 SDDC 後，您可以新增、編輯、啟用、停用並移除其 SDDC Proxy。

備註 將 Proxy 新增至 SDDC 時，您必須上傳憑證和指紋，以便在代理的元件使用自我簽署憑證時，承租人可擷取該憑證和指紋。

管理系統管理員與角色

10

透過使用 vCloud Director Web 主控台，您可以將系統管理員個別新增至 vCloud Director，或是當作 LDAP 群組的一部分加以新增。您也可以新增並修改角色，決定使用者在其組織內有哪些權限。

備註 從 vCloud Director 9.5 開始，服務提供者可以使用 vCloud Director Service Provider Admin Portal 或 vCloud OpenAPI 建立提供者角色並管理提供者使用者和群組。如需管理提供者角色、使用者和群組的相關資訊，請參閱《vCloud Director Service Provider Admin Portal 指南》。若要檢查 vCloud OpenAPI 說明文件，請前往 `https://vCloud_Director_IP_address_or_host_name/docs`。

本章節討論下列主題：

- 管理權限和角色
- 管理提供者使用者與群組

管理權限和角色

權限是 vCloud Director 中的基本存取控制單位。角色會將角色名稱與一組權限相關聯。每個組織可以有不同的權限和角色。

vCloud Director 使用角色及其相關聯的權限來判定使用者或群組是否獲得執行作業的授權。vCloud Director 指南中記錄的許多程序包含先決條件角色。這些先決條件假設已命名角色是未修改的預先定義角色，或包含一組同等權限的角色。

vCloud Director 9.5 引入了權限服務包和全域承租人角色，可供系統管理員用於管理每個組織可用的權限和角色。

安裝 vCloud Director 後，系統將僅包含系統權限服務包，其中包含系統中的所有可用權限。系統權限服務包不會發佈到任何組織。系統還包含發佈到所有組織的內建全域承租人角色。如需預先定義的角色的相關資訊，請參閱預先定義的角色與其權限。

從 9.1 或更早版本升級 vCloud Director 之後，除系統權限服務包之外，系統還包含每個現有組織的舊版權限服務包。每個舊版權限服務包都包含升級時可供相關聯的組織使用的權限，且權限服務包僅會發佈到此組織。

備註 若要開始對現有組織使用權限服務包模型，您必須刪除對應的舊版權限服務包。

如果已從 vCloud Director 9.1 版或更早版本升級，現有角色範本會做為全域承租人角色發佈到所有組織，與角色範本取消連結的現有角色則會做為承租人專屬角色提供給其組織。

權限術語

權限

每個權限會提供對 vCloud Director 中特定物件類型的檢視或管理存取權。根據與其相關的物件，權限可屬於多種類別，例如 vApp、目錄、組織等。提供者組織包含系統中的所有可用權限。系統管理員會定義可供每個組織使用的權限。您無法建立或修改 vCloud Director 中包含的權限。

權限服務包

系統管理員可使用權限服務包管理可供每個組織使用的權限。權限服務包是系統管理員可發佈到一或多個組織的權限集。系統管理員可以建立和發佈與服務階層對應的權限服務包、可單獨銷售的功能或任何其他隨機權限群組。只有系統管理員可以檢視和管理權限服務包。您可以將多個服務包發佈到相同的組織。

組織權限

組織權限是可供組織使用的完整權限集。組織權限可包含多個權限服務包，但是組織管理員和使用者僅可看到他們可用於建立和修改承租人專屬角色的一個普通的權限集。

角色術語

角色

角色是可指派給一或多個使用者和群組的權限集。建立或匯入使用者或群組時，您必須為其指派一個角色。

提供者角色

提供者角色是僅可用於提供者組織的角色集。提供者角色僅可指派給提供者使用者。系統管理員可建立自訂提供者角色。

承租人角色

承租人角色是可供組織使用的角色集。

系統管理員可以建立和編輯全域承租人角色，並將其發佈到一或多個組織。全域承租人角色可指派給其所發佈到的組織中的承租人使用者。組織管理員無法編輯全域承租人角色。

備註 承租人使用者只能使用已發佈到其組織的角色中的權限。

承租人專屬角色

組織管理員可以建立和編輯其組織的本機承租人專屬角色。承租人專屬角色僅可指派給其所屬組織中的承租人使用者。承租人專屬角色只能包含一部分組織權限。

如需管理承租人專屬角色的相關資訊，請參閱《vCloud Director 租用戶入口網站指南》。

預先定義的角色與其權限

每個 vCloud Director 預先定義的角色包含執行一般工作流程中包含之作業所需的一組預設權限。依預設，所有預先定義的全域承租人角色會發佈到系統中的每個組織。

預先定義的提供者角色

依預設，僅提供者組織的本機提供者角色為**系統管理員**角色和**多站台系統**角色。**系統管理員**可以建立其他自訂提供者角色。

系統管理員

系統管理員角色僅存在於提供者組織中。**系統管理員**角色包含系統中的所有權限。**系統管理員**認證會在安裝和設定期間建立。**系統管理員**可以在提供者組織中建立其他系統管理員和使用者帳戶。

多站台系統

用於針對多站台部署執行活動訊號程序。此角色只有單一權限**多站台：系統作業**，可讓此帳戶有權提出擷取站台關聯之遠端成員狀態的 vCloud API 要求。

預先定義的全域承租人角色

依預設，預先定義的全域承租人角色及其包含的權限會發佈到所有組織。**系統管理員**可從個別組織解除發佈權限和全域承租人角色。**系統管理員**可以編輯或刪除預先定義的全域承租人角色。**系統管理員**可以建立和發佈其他全域承租人角色。

組織管理員

建立組織後，**系統管理員**可以將**組織管理員**角色指派給組織中的任何使用者。具有預先定義的**組織管理員**角色的使用者可以使用 vCloud Director Web 主控台、租用戶入口網站或 vCloud OpenAPI，管理其組織中的使用者和群組，並為其指派角色，包括預先定義的**組織管理員**角色。其他組織不會看見由**組織管理員**建立或修改的角色。

目錄作者

與預先定義之**目錄作者**角色相關聯的權限允許使用者建立和發佈目錄。

vApp 作者

與預先定義之 **vApp 作者**角色相關聯的權限允許使用者使用目錄和建立 vApp。

vApp 使用者

與預先定義之 **vApp 使用者**角色相關聯的權限允許使用者使用現有 vApp。

僅限主控台存取

與預先定義之**僅限主控台存取**角色相關聯的權限允許使用者檢視虛擬機器狀態和內容，以及使用客體作業系統。

遵從身分識別提供者

與預先定義之**遵從身分識別提供者**角色相關聯的權限依據從使用者之 OAuth 或 SAML 身分識別提供者接收到的資訊決定。當為使用者或群組指派**遵從身分識別提供者**角色時，若要取得加入的權限，身分識別提供者提供的角色或群組名稱必須與在組織中定義的角色或群組名稱完全相符 (區分大小寫)。

- 如果使用者由 OAuth 身分識別提供者定義，將為使用者指派在使用者之 OAuth Token 的 `roles` 陣列中命名的角色。
- 如果使用者由 SAML 身分識別提供者定義，將為使用者指派在 SAML 屬性中命名的角色，其名稱顯示在 `RoleAttributeName` 元素 (位於組織之 `OrgFederationSettings` 中的 `SamlAttributeMapping` 元素) 中。

如果為使用者指派了**遵從身分識別提供者**角色，但在您的組織中沒有相符的角色或群組名稱，使用者可登入組織，但無權限。如果身分識別提供者將使用者和系統層級角色 (如**系統管理員**) 相關聯，使用者可登入組織，但無權限。您必須為此類使用者手動指派角色。

每個預先定義角色都包含一組預設權限，**遵從身分識別提供者**角色除外。僅**系統管理員**可以修改預先定義的角色中的權限。如果**系統管理員**修改預先定義的角色，則這些修改將傳播到系統中角色的所有執行個體。

預先定義之全域承租人角色中的權限

各種權限在多個預先定義的全域角色之間共用。依預設，這些權限會被授與所有新組織，且可用於**組織管理員**建立的其他角色。

表 10-1. vCloud Director 全域承租人角色中包含的權限

權限名稱	組織管理員	目錄作者	vApp 作者	vApp 使用者	僅限主控台存取
目錄：從我的雲端新增 vApp	X	X	X		
目錄：允許目錄的外部發佈/訂閱	X	X			
目錄：變更擁有者	X				
目錄：建立/刪除目錄	X	X			
目錄：編輯目錄內容	X	X			
目錄：將目錄與其他組織共用	X	X			
目錄：在目前組織中與使用者/群組共用目錄	X	X			
目錄：在目前組織中檢視私人與共用目錄	X	X	X		
目錄：檢視其他組織中的共用目錄	X				
目錄項目：新增至我的雲端	X	X	X	X	
目錄項目：複製/移動 vApp 範本/媒體	X	X	X		
目錄項目：建立/上傳 vApp 範本/媒體	X	X			
目錄項目：編輯 vApp 範本/媒體	X	X			
目錄項目：啟用 vApp 範本/媒體下載	X	X			
目錄項目：檢視 vApp 範本/媒體	X	X	X	X	
自訂實體：檢視組織中的所有自訂實體執行個體	X				
自訂實體：檢視自訂實體執行個體	X				

表 10-1. vCloud Director 全域承租人角色中包含的權限 (續)

權限名稱	組織管理員	目錄作者	vApp 作者	vApp 使用者	僅限主控台存取
磁碟：變更擁有者	X	X			
磁碟：建立磁碟	X	X	X		
磁碟：刪除磁碟	X	X	X		
磁碟：編輯磁碟內容	X	X	X		
磁碟：檢視磁碟內容	X	X	X	X	
Distributed Firewall：設定 Distributed Firewall 規則	X				
Distributed Firewall：啟用/停用 Distributed Firewall	X				
Distributed Firewall：檢視 Distributed Firewall 規則	X				
Edge 叢集：檢視 Edge 叢集	X				
Edge 叢集：管理 Edge 叢集	X				
閘道：設定 Syslog 伺服器	X				
閘道：設定系統記錄	X				
閘道：轉換為進階閘道	X				
閘道：檢視閘道	X				
閘道：啟用分散式路由	X				
閘道：匯入 Edge 閘道	X				
閘道服務：BGP 路由設定					
閘道服務：DHCP 設定	X				
閘道服務：防火牆設定	X				
閘道服務：IPSEC VPN 設定	X				
閘道服務：L2 VPN 設定					
閘道服務：負載平衡器設定	X				
閘道服務：NAT 設定	X				
閘道服務：OSPF 路由設定	X				
閘道服務：遠端存取設定	X				
閘道服務：SSL VPN 設定	X				
閘道服務：靜態路由設定	X				
閘道服務：僅 BGP 路由視圖	X				
閘道服務：僅 DHCP 視圖	X				
閘道服務：僅防火牆視圖	X				
閘道服務：僅 IPSEC VPN 視圖	X				

表 10-1. vCloud Director 全域承租人角色中包含的權限 (續)

權限名稱	組織管理員	目錄作者	vApp 作者	vApp 使用者	僅限主控台存取
閘道服務：僅 L2 VPN 視圖	X				
閘道服務：僅負載平衡器視圖	X				
閘道服務：僅 NAT 視圖	X				
閘道服務：僅 OSPF 路由視圖	X				
閘道服務：僅遠端存取視圖	X				
閘道服務：僅 SSL VPN 視圖	X				
閘道服務：僅靜態路由視圖	X				
一般：管理員控制	X				
一般：管理員檢視	X				
一般：傳送通知	X				
混合通道：取得控制票證	X				
混合通道：取得源於雲端通道票證	X				
混合通道：取得通向雲端的通道票證	X				
混合通道：建立源於雲端通道	X				
混合通道：建立通向雲端的通道	X				
混合通道：刪除源於雲端通道	X				
混合通道：刪除通向雲端的通道	X				
混合通道：更新源於雲端通道端點標記	X				
混合通道：檢視雲端通道伺服器設定	X				
混合通道：檢視源於雲端通道	X				
混合通道：檢視通向雲端的通道	X				
組織：允許存取所有組織 VDC	X				
組織：編輯組織 VDC 的存取控制清單	X				
組織：編輯同盟設定	X				
組織：編輯租用原則	X				
組織：編輯組織關聯	X				
組織：編輯組織網路內容	X				
組織：編輯組織 OAuth 設定	X				
組織：編輯組織內容	X				
組織：編輯密碼原則	X				
組織：編輯配額原則	X				
組織：編輯 SMTP 設定	X				
組織：編輯 VDC ACL 時從 IdP 隱式匯入使用者/群組	X				

表 10-1. vCloud Director 全域承租人角色中包含的權限 (續)

權限名稱	組織管理員	目錄作者	vApp 作者	vApp 使用者	僅限主控台存取
組織：檢視組織 VDC 的存取控制清單	X				
組織：檢視目錄 ACL	X	X			
組織：檢視組織網路	X				
組織：檢視組織	X	X	X		
組織：檢視 vApp ACL	X	X	X	X	
組織 VDC：編輯組織 VDC 名稱與說明	X				
組織 VDC：編輯虛擬機器-虛擬機器相似性規則	X	X	X		
組織 VDC：編輯組織 VDC 延伸內容	X				
組織 VDC：管理防火牆	X				
組織 VDC：設定預設儲存區原則	X				
組織 VDC：檢視組織 VDC 的運算原則	X	X	X	X	
組織 VDC：檢視組織 VDC 延伸內容	X				
組織 VDC 網路：檢視內容	X				
組織 VDC 網路：編輯內容	X				
組織 VDC 網路：匯入網路	X				
組織 VDC：檢視組織 VDC	X				
組織 VDC 範本：具現化組織 VDC 範本	X				
組織 VDC 範本：檢視 VDC 範本	X				
提供者網路：檢視提供者網路	X				
提供者網路：建立/刪除提供者網路	X				
角色：建立/更新/刪除角色	X				
服務程式庫：檢視構成服務程式庫的服務	X				
使用者：檢視群組/使用者	X				
VCD 延伸：檢視租用戶入口網站外掛程式資訊	X	X	X	X	
VDC 群組：檢視 VDC 群組	X				
VDC 群組：設定 VDC 群組	X				
虛擬機器監控：檢視組織的歷史度量	X				
虛擬機器監控：檢視組織 VDC 的歷史度量	X				
vApp：存取虛擬機器主控台	X	X	X	X	X
vApp：允許將網域對應至 vCenter Server 的中繼資料	X	X	X		
vApp：變更擁有者	X				
vApp：變更 vApp 範本擁有者	X	X			
vApp：複製 vApp	X	X	X	X	

表 10-1. vCloud Director 全域承租人角色中包含的權限 (續)

權限名稱	組織管理員	目錄作者	vApp 作者	vApp 使用者	僅限主控台存取
vApp：建立/重新設定 vApp	X	X	X		
vApp：建立/還原/移除快照	X	X	X	X	
vApp：刪除 vApp	X	X	X	X	
vApp：下載 vApp	X	X	X		
vApp：編輯/檢視虛擬機器開機選項	X	X	X		
vApp：編輯虛擬機器 CPU	X	X	X		
vApp：編輯虛擬機器硬碟	X	X	X		
vApp：編輯虛擬機器記憶體	X	X	X		
vApp：編輯虛擬機器網路	X	X	X	X	
vApp：編輯虛擬機器內容	X	X	X	X	
vApp：編輯 vApp 內容	X	X	X	X	
vApp：編輯虛擬機器運算原則	X	X	X		
vApp：管理虛擬機器密碼設定	X	X	X	X	X
vApp：共用 vApp	X	X	X	X	
vApp：啟動/停止/暫止/重設 vApp	X	X	X	X	
vApp：上傳 vApp	X	X	X		
vApp：檢視虛擬機器度量	X		X	X	

如需 vCloud Director 9.7 採用的新權限的相關資訊，請參閱此版本中的新權限。

此版本中的新權限

vCloud Director 9.7 採用了新權限，您可能想要將這些權限新增至發佈到您的承租人的任何現有全域角色。

權限	描述	預設角色
SDDC：檢視 SDDC	可讓您檢視向您的組織發佈的所有 SDDC。 **系統管理員**可以檢視所有 SDDC。	**系統管理員**和**組織管理員**
SDDC：管理 SDDC	可讓您新增、移除和編輯 SDDC。	**系統管理員**
SDDC：管理 SDDC Proxy	可讓您新增、移除、啟用及停用 SDDC Proxy。	**系統管理員**
服務應用程式：檢視服務應用程式	可讓您查看已登錄的服務應用程式的清單。 用於 VMC 帳戶。	**系統管理員**
服務應用程式：登錄 VMC SDDC	可讓您建立、檢視、編輯和移除服務應用程式。 用於 VMC 帳戶。	**系統管理員**

權限	描述	預設角色
服務應用程式：管理服務應用程式	可讓您登錄服務應用程式。 用於 VMC 帳戶。	**系統管理員**
Edge 叢集：檢視 Edge 叢集	可讓您查看 Edge 叢集的清單並擷取個別 Edge 叢集。	**系統管理員**和**組織管理員**
Edge 叢集：管理 Edge 叢集	可讓您建立、編輯和移除 Edge 叢集。	**系統管理員**和**組織管理員**
vApp：編輯虛擬機器運算原則	允許使用者變更虛擬機器的運算原則。	**系統管理員**、**組織管理員**、**目錄作者**和 **vApp 作者**
閘道：匯入 Edge 閘道	可讓您匯入第 1 層路由器做為 Edge 閘道。	**系統管理員**和**組織管理員**

如需管理權限和角色的相關資訊，請參閱《vCloud Director Service Provider Admin Portal 指南》。

管理權限服務包

身為系統管理員，您可以建立權限服務包並將其發佈到雲端中的一或多個組織。您可以編輯和刪除現有的權限服務包。您可以從雲端中的組織解除發佈權限服務包。

建立權限服務包

您可以將一組權限分組為一個權限服務包，並將其發佈到系統中的一或多個組織。

程序

1. 從主功能表 (☰) 中，選取**管理**。
2. 在左面板中的**承租人存取控制**下，按一下**權限服務包**。
3. 按一下**新增**。
4. 輸入新權限服務包的名稱，並選擇性地輸入說明。
5. 選取要與此服務包相關聯的權限。

   權限依類別和子類別分組，以檢視或管理相關物件的存取權限。

   您可以個別選取權限，以便按子類別檢視或管理，或者全域檢視或管理。

類別	描述
存取控制	包含用於檢視和管理組織、權限、角色和使用者的權限。
管理	包含用於檢視和管理一般和多站台設定的權限。
計算	包含用於檢視和管理組織和提供者 VDC、vApp、組織 VDC 範本和虛擬機器監控的權限。
延伸	包含用於檢視和管理 vCloud Director 外掛程式和延伸的權限。
基礎結構	包含用於檢視和管理 vSphere 資源的權限。

類別	描述
程式庫	包含用於檢視和管理目錄和目錄項目的權限。
網路作業	包含用於檢視和管理網路資源的權限。

6 按一下**儲存**。

後續步驟

您可以將新建立的權限服務包發佈到系統中的一或多個組織。請參閱發佈或解除發佈權限服務包。

發佈或解除發佈權限服務包

您可以將權限服務包發佈到系統中的一或多個組織。將權限服務包發佈至組織後，此服務包中的權限將成為該組織權限集的一部分。

組織權限可包含多個權限服務包，但是組織管理員和使用者僅可看到他們可用於建立和修改角色的一個普通的權限集。

程序

1 從主功能表 (☰) 中，選取**管理**。

2 在左面板中的**承租人存取控制**下，按一下**權限服務包**。

3 選取目標服務包旁的選項按鈕，然後按一下**發佈**。

4 發佈服務包：

   a 選取**發佈到承租人**。

   b 選取要將角色發佈到的組織。

      - 如果您要將服務包發佈到系統中的所有現有組織和新建立的組織，請選取**發佈到所有承租人**。
      - 如果您要將服務包發佈到系統中的特定組織，請個別選取組織。

5 解除發佈服務包：

   - 如果您要從系統中的所有組織解除發佈服務包，請取消選取**發佈到承租人**。
   - 如果您要從系統中的特定組織解除發佈服務包，請取消選取**發佈到所有承租人**，然後個別取消選取組織。

6 按一下**儲存**。

結果

已發佈的服務包中的權限可供所選組織使用，並可用於這些組織中的角色。

已解除發佈的角色中的權限將從所選組織中移除，且無法在這些組織中的角色中使用。

檢視和編輯權限服務包

您可以檢視權限服務包中包含的權限。您可以修改服務包的名稱、說明和權限。

程序

1 從主功能表 (☰) 中，選取**管理**。

2 在左面板中的**承租人存取控制**下，按一下**權限服務包**。

3 按一下目標服務包的名稱。

您可以展開權限類別以檢視與服務包相關聯的權限。

4 編輯服務包，然後按一下**保留**。

結果

如果您修改了服務包的權限，會將一組新權限套用到此權限服務包發佈到的所有組織。

刪除權限服務包

您可以移除組織中不再使用的權限服務包。

程序

1 從主功能表 (☰) 中，選取**管理**。

2 在左面板中的**承租人存取控制**下，按一下**權限服務包**。

3 選取目標服務包旁邊的選項按鈕，然後按一下**刪除**。

4 按一下**確定**以確認。

管理全域承租人角色

身為系統管理員，您可以建立全域承租人角色並將其發佈到雲端中的一或多個組織。您可以編輯和刪除現有的全域承租人角色。您可以從雲端中的個別組織解除發佈全域承租人角色。

vCloud Director 初始安裝和設定後，系統會包含一組發佈到所有組織的預先定義的全域承租人。請參閱預先定義的角色與其權限。

建立全域承租人角色

您可以建立全域承租人角色並將其發佈到系統中的一或多個組織。

vCloud Director 初始安裝和設定後，系統會包含發佈到所有組織的預先定義的全域承租人角色。如需預先定義的角色的相關資訊，請參閱預先定義的角色與其權限。

您可以將自訂全域角色新增至系統。

程序

1 從主功能表 (☰) 中，選取**管理**。

2 在左面板中的**承租人存取控制**下，按一下**全域角色**。

3 按一下**新增**。

4 輸入新角色的名稱，並選擇性地輸入說明。

5 選取要與角色相關聯的權限。

權限依類別和子類別分組，以檢視或管理相關物件的存取權限。

您可以個別選取權限，以便按子類別檢視或管理，或者全域檢視或管理。

類別	描述
存取控制	包含用於檢視和管理組織、權限、角色和使用者的權限。
管理	包含用於檢視和管理一般和多站台設定的權限。
計算	包含用於檢視和管理組織和提供者 VDC、vApp、組織 VDC 範本和虛擬機器監控的權限。
延伸	包含用於檢視和管理 vCloud Director 外掛程式和延伸的權限。
基礎結構	包含用於檢視和管理 vSphere 資源的權限。
程式庫	包含用於檢視和管理目錄和目錄項目的權限。
網路作業	包含用於檢視和管理網路資源的權限。

6 按一下**保留**。

結果

建立全域承租人角色後，新的全域承租人權限僅供 vCloud Director 提供者組織使用。

後續步驟

您可以將新建立的角色發佈到系統中的一或多個組織。請參閱發佈或解除發佈全域承租人角色。

發佈或解除發佈全域承租人角色

您可以將全域承租人角色發佈到系統中的一或多個組織。將角色發佈到組織後，該角色將成為組織承租人角色集的一部分。

必要條件

如果您想要在其中一個組織中解除發佈全域承租人角色，請確認此組織中不存在指派此角色的使用者。

程序

1 從主功能表 (☰) 中，選取**管理**。

2 在左面板中的**承租人存取控制**下，按一下**全域角色**。

3 選取目標角色旁的選項按鈕，然後按一下**發佈**。

4 發佈角色：

a 選取**發佈到承租人**。

b 選取要將角色發佈到的組織。

- 如果您要將角色發佈到系統中的所有現有組織和新建立的組織，請選取**發佈到所有承租人**。
- 如果您要將角色發佈到系統中的特定組織，請個別選取組織。

5 解除發佈角色：

- 如果您要從系統中的所有組織解除發佈角色，請取消選取**發佈到承租人**。
- 如果您要從系統中的特定組織解除發佈角色，請取消選取**發佈到所有承租人**，然後個別取消選取組織。

6 按一下**儲存**。

結果

已發佈的角色可供所選組織使用，並且可以指派給這些組織中的使用者。組織管理員無法編輯已發佈到其組織的全域承租人角色。

已解除發佈的角色會從所選組織中移除，且無法指派給這些組織中的使用者。

檢視和編輯全域承租人角色

您可以檢視全域承租人角色中包含的權限。您可以修改全域承租人角色的名稱、說明和權限。

程序

1 從主功能表 (☰) 中，選取**管理**。

2 在左面板中的**承租人存取控制**下，按一下**全域角色**。

3 按一下目標角色的名稱。

您可以展開權限類別以檢視與角色相關聯的權限。

4 若要修改角色的名稱、說明或權限，請按一下**編輯**。

5 編輯角色，然後按一下**保留**。

結果

如果您已修改角色的權限，一組新權限將套用到所有組織中指派有此角色的使用者。

刪除全域承租人角色

您可以移除組織中不再使用的全域承租人角色。

必要條件

要刪除的全域承租人角色不得指派給所有組織中的任何使用者。

程序

1 從主功能表 (☰) 中，選取**管理**。

2 在左面板中的**承租人存取控制**下，按一下**全域角色**。

3 選取目標角色旁邊的選項按鈕，然後按一下**刪除**。

4 按一下**確定**以確認。

管理提供者角色

您可以在 vCloud Director 提供者組織中建立和管理角色。

如需管理承租人角色的相關資訊，請參閱《vCloud Director 租用戶入口網站指南》。

建立提供者角色

您可以在 vCloud Director 提供者組織中建立角色。

vCloud Director 初始安裝和設定後，系統會包含部分預先定義的角色，這些角色對提供者組織來說是本機角色，而對所有組織來說是全域角色。如需預先定義的角色的相關資訊，請參閱預先定義的角色與其權限。

您可以將自訂提供者角色新增至提供者組織。

程序

1. 從主功能表 (☰) 中，選取**管理**。
2. 在左面板中的**提供者存取控制**下，按一下**角色**。
3. 按一下**新增**。
4. 輸入新角色的名稱，並選擇性地輸入說明。
5. 選取要與角色相關聯的權限。

   權限依類別和子類別分組，以檢視或管理相關物件的存取權限。

   您可以個別選取權限，以便按子類別檢視或管理，或者全域檢視或管理。

類別	描述
存取控制	包含用於檢視和管理組織、權限、角色和使用者的權限。
管理	包含用於檢視和管理一般和多站台設定的權限。
計算	包含用於檢視和管理組織和提供者 VDC、vApp、組織 VDC 範本和虛擬機器監控的權限。
延伸	包含用於檢視和管理 vCloud Director 外掛程式和延伸的權限。
基礎結構	包含用於檢視和管理 vSphere 資源的權限。
程式庫	包含用於檢視和管理目錄和目錄項目的權限。
網路作業	包含用於檢視和管理網路資源的權限。

6. 按一下**儲存**。

結果

新建立的角色可指派給提供者組織中的使用者。

檢視或編輯提供者角色

您可以檢視 vCloud Director 提供者組織的本機角色中包含的權限。您可以修改角色的名稱、說明和權限。

程序

1 從主功能表 (☰) 中，選取**管理**。

2 在左面板中的**提供者存取控制**下，按一下**角色**。

3 按一下目標角色的名稱。

您可以展開權限類別以檢視與角色相關聯的權限。

4 若要修改角色的名稱、說明或權限，請按一下**編輯**。

5 編輯角色，然後按一下**儲存**。

結果

如果您已修改角色的權限，一組新權限將套用到指派有此角色的使用者。

刪除提供者角色

您可以移除 vCloud Director 提供者組織中不再使用的角色。

必要條件

要刪除的角色不得指派給任何使用者。

程序

1 從主功能表 (☰) 中，選取**管理**。

2 在左面板中的**提供者存取控制**下，按一下**角色**。

3 選取目標角色旁邊的選項按鈕，然後按一下**刪除**。

4 按一下**確定**以確認。

管理提供者使用者與群組

您可以向 vCloud Director 提供者組織新增或匯入使用者和群組。

如需管理組織使用者和群組的相關資訊，請參閱《vCloud Director 租用戶入口網站指南》。

管理提供者使用者

您可以透過 Service Provider Admin Portal 管理提供者組織中的使用者。

如需管理組織中的承租人使用者的相關資訊，請參閱《vCloud Director 租用戶入口網站指南》。

建立提供者使用者

您可以在 vCloud Director 提供者組織中建立使用者。

安裝和設定 vCloud Director 期間，您可以建立一個**系統管理員**帳戶。在初始設定後，您可以為提供者組織建立其他管理員和使用者。

程序

1 從主功能表 (☰) 中，選取**管理**。

2 在左面板中的**提供者存取控制**下，按一下**使用者**。

3 按一下**新增**。

4 輸入新使用者的使用者名稱和密碼。

密碼必須至少包含 6 個字元。

5 選取是否要在建立時啟用使用者。

6 從**可用角色**下拉式功能表中選取使用者的角色。

可用角色清單包括全域角色和系統組織的本機角色。

7 (選擇性) 輸入使用者的連絡資訊。

您可以輸入全名、電子郵件地址、電話號碼和即時訊息識別碼。

8 (選擇性) 設定使用者的配額。

a 您可以設定使用者所擁有的虛擬機器的限制，或選取**無限制**。

b 您可以設定使用者所擁有的執行中虛擬機器的限制，或選取**無限制**。

匯入提供者使用者

您可以將先前設定的 LDAP 或 SAML 身分識別提供者中的使用者匯入您的 vCloud Director 提供者組織。

必要條件

設定系統 LDAP 連線或將系統設定為使用 SAML 身分識別提供者。

程序

1 從主功能表 (☰) 中，選取**管理**。

2 在左面板中的**提供者存取控制**下，按一下**使用者**。

3 按一下**匯入使用者**。

4 從**來源**下拉式功能表中，選取身分識別提供者類型。

可以是 **LDAP** 或 **SAML**。

如果您只設定了一個身分識別提供者，則此選項為硬式編碼。

5 指定使用者。

選項	描述
LDAP	a 輸入使用者的完整或部分名稱，然後按一下**搜尋**。 b 從搜尋結果中，選取要匯入的使用者。 c 從**指派角色**下拉式功能表中，為匯入的使用者選取一個角色。
SAML	a 以 SAML 身分識別提供者支援的名稱識別碼格式輸入要匯入之使用者的使用者名稱。 為每個使用者名稱使用一個新行。 b 從**指派角色**下拉式功能表中，為匯入的使用者選取一個角色。

6 按一下**儲存**。

結果

此時會在使用者清單中顯示所匯入的使用者。

編輯提供者使用者

您可以變更提供者組織中的使用者的密碼、角色、連絡資訊及配額。您無法變更使用者名稱。

程序

1 從主功能表 (☰) 中，選取**管理**。

2 在左面板中的**提供者存取控制**下，按一下**使用者**。

3 按一下目標使用者名稱旁邊的選項按鈕，然後按一下**編輯**。

4 編輯使用者詳細資料，然後按一下**儲存**。

停用或啟用提供者使用者

停用使用者後，該使用者便無法登入 vCloud Director。

程序

1 從主功能表 (☰) 中，選取**管理**。

2 在左面板中的**提供者存取控制**下，按一下**使用者**。

3 按一下目標使用者名稱旁邊的選項按鈕，然後按一下**停用**或**啟用**。

4 如果您想要停用使用者，請按一下**確定**以確認。

刪除提供者使用者

您可以透過刪除使用者帳戶從 vCloud Director 提供者組織中移除使用者。

必要條件

停用您要刪除的使用者。請參閱停用或啟用提供者使用者。

程序

1 從主功能表 (☰) 中，選取**管理**。

2 在左面板中的**提供者存取控制**下，按一下**使用者**。

3 按一下目標使用者名稱旁邊的選項按鈕，然後按一下**刪除**。

4 按一下**確定**以確認。

解除鎖定提供者使用者

如果您已在密碼原則系統設定中啟用帳戶鎖定，使用者在特定次數的無效登入嘗試後可能會鎖定其帳戶。即使已為鎖定設定帳戶鎖定間隔，您也可以解除鎖定使用者帳戶，而無需等待鎖定到期。

如需設定帳戶鎖定原則的相關資訊，請參閱《vCloud Director 管理員指南》。

程序

1 從主功能表 (☰) 中，選取**管理**。

2 在左面板中的**提供者存取控制**下，按一下**使用者**。

3 按一下目標使用者名稱旁的選項按鈕，然後按一下**解除鎖定**。

管理提供者群組

您可以使用 Service Provider Admin Portal 在提供者組織中匯入、編輯和刪除群組。

如需在組織中管理群組的相關資訊，請參閱《vCloud Director 租用戶入口網站指南》。

匯入提供者群組

您可以將先前設定的 LDAP 或 SAML 身分識別提供者中的群組匯入您的 vCloud Director 提供者組織。

必要條件

設定系統 LDAP 連線或將系統設定為使用 SAML 身分識別提供者。

程序

1 從主功能表 (☰) 中，選取**管理**。

2 在左面板中的**提供者存取控制**下，按一下**群組**。

3 按一下**匯入群組**。

4 從**來源**下拉式功能表中，選取身分識別提供者類型。

可以是 **LDAP** 或 **SAML**。

如果您只設定了一個身分識別提供者，則此選項為硬式編碼。

5 指定使用者。

選項	描述
LDAP	a 輸入群組的完整或部分名稱，然後按一下**搜尋**。 b 從搜尋結果中，選取您要匯入的群組。 c 從**指派角色**下拉式功能表中，為所匯入群組中的使用者選取一個角色。
SAML	a 以 SAML 身分識別提供者支援的名稱識別碼格式輸入要匯入之群組的名稱。 為每個群組名稱使用一個新行。 b 從**指派角色**下拉式功能表中，為所匯入群組中的使用者選取一個角色。

6 按一下**儲存**。

編輯提供者群組

您可以編輯說明並變更先前匯入至 vCloud Director 提供者組織的群組成員的角色。

程序

1 從主功能表 (☰) 中，選取**管理**。

2 在左面板中的**提供者存取控制**下，按一下**群組**。

3 按一下目標群組名稱旁邊的選項按鈕，然後按一下**編輯**。

4 編輯群組詳細資料，然後按一下**儲存**。

刪除提供者群組

您可以從 vCloud Director 提供者組織中移除群組

程序

1 從主功能表 (☰) 中，選取**管理**。

2 在左面板中的**提供者存取控制**下，按一下**群組**。

3 按一下目標群組名稱旁邊的選項按鈕，然後按一下**刪除**。

4 按一下**確定**以確認。

管理系統設定

11

vCloud Director 系統管理員可以控制與 LDAP、電子郵件通知、授權以及一般系統喜好設定相關的各種系統設定。

本章節討論下列主題：

- 管理身分識別提供者
- 管理外掛程式
- 自訂 vCloud Director 入口網站

管理身分識別提供者

您可以將雲端與外部身分識別提供者整合，並將使用者和群組匯入到您的組織中。您可以在系統或組織層級設定 LDAP 伺服器連線。您可以在組織層級設定 SAML 整合。

管理 LDAP 連線

身為系統管理員，您可以設定系統中的 vCloud Director 系統組織和任何其他組織，以使用 LDAP 伺服器做為使用者和群組的來源。組織可以使用系統 LDAP 連線或私人 LDAP 連線。

設定系統 LDAP 連線

若要為 vCloud Director 及其組織提供對使用者和群組的共用存取權，可以在系統層級設定 LDAP 連線。

程序

1 從主功能表 (☰) 中，選取**管理**。

2 在左面板中的**身分識別提供者**下，按一下 **LDAP**。

此時會顯示目前的 LDAP 設定。

後續步驟

設定、測試和同步 LDAP 連線。

設定組織 LDAP 連線

可以將組織設定為使用系統 LDAP 連線做為使用者和群組的共用來源。您可以將組織設定為使用單獨的 LDAP 連線做為使用者和群組的私人來源。

程序

1. 從主功能表 (☰) 中，選取**雲端資源**。
2. 在左面板中，按一下**組織**。
3. 按一下目標組織的名稱。

   系統會將您重新導向至組織的 vCloud Director 租用戶入口網站。
4. 從主功能表 (☰) 中，選取**管理**。
5. 在左面板中的**身分識別提供者**下，按一下 **LDAP**。

   此時會顯示目前的 LDAP 設定。
6. 在 **LDAP 選項**索引標籤上，按一下**編輯**。
7. 為此組織設定使用者和群組的 LDAP 來源，然後按一下**儲存**。

選項	描述
不使用 LDAP	組織不使用 LDAP 伺服器做為組織使用者和群組的來源。
VCD 系統 LDAP 服務	組織使用您先前設定的 vCloud Director 系統 LDAP 連線。請參閱設定系統 LDAP 連線。
自訂 LDAP 服務	組織使用私人 LDAP 伺服器做為組織使用者和群組的來源。按一下**自訂 LDAP** 索引標籤，然後設定、測試和同步 LDAP 連線。

設定、測試和同步 LDAP 連線

若要設定系統或組織的 LDAP 連線，請設定 LDAP 伺服器的詳細資料。您可以測試連線來確保輸入正確的設定，且使用者和群組屬性已正確對應。當 LDAP 連線成功後，您可以隨時將 vCloud Director 與 LDAP 伺服器同步。

必要條件

如果您計劃連線至 LDAPS 伺服器，請確認具有正確建構的憑證以改善 Java 8 Update 181 中的 LDAP 支援。如需詳細資訊，請參閱《Java 8 版本變更》，網址為 https://www.java.com。

程序

1 在**連線**索引標籤中，輸入 LDAP 連線所需的資訊。

必要資訊	描述
伺服器	LDAP 伺服器的主機名稱或 IP 位址。
連接埠	LDAP 伺服器接聽的連接埠號碼。 對於 LDAP，預設連接埠號碼為 389。對於 LDAPS，預設連接埠號碼為 636。
基準辨別名稱	基準辨別名稱 (DN) 是 LDAP 目錄中 vCloud Director 要連線的位置。 若要在根目錄連線，請僅輸入網域元件，例如 **DC=example,DC=com**。 若要連線至樹狀結構中的節點，請輸入該節點的辨別名稱，例如 **OU=ServiceDirector,DC=example,DC=com**。 連線至節點會限制 vCloud Director 可用的目錄範圍。
連接器類型	LDAP 伺服器的類型。可以是 **Active Directory** 或 **OpenLDAP**。
使用 SSL	如果您的伺服器為 LDAPS，請選取此核取方塊。
接受所有憑證	如果您的伺服器為 LDAPS，請選取此核取方塊或上傳 LDAP SSL 憑證。
自訂信任存放區	如果您的伺服器為 LDAPS，請按一下上傳圖示 ()，然後匯入 LDAP SSL 憑證或選取**接受所有憑證**。
驗證方法	簡易驗證包含將使用者的 DN 及密碼傳送至 LDAP 伺服器。如果您使用 LDAP，會透過網路傳送純文字的 LDAP 密碼。 如果您想要使用 Kerberos，則必須使用 vCloud Director Web 用戶端設定 LDAP 連線。如需詳細資訊，請參閱《vCloud Director 管理員指南》。
使用者名稱	用於連線至 LDAP 伺服器的完整 LDAP DN 使用者名稱。 如果 LDAP 伺服器啟用匿名讀取支援功能，則您可以不填入這些文字方塊。
密碼	用於連線至 LDAP 伺服器的密碼。 如果 LDAP 伺服器啟用匿名讀取支援功能，則您可以不填入這些文字方塊。

2 按一下**使用者屬性**索引標籤，檢查使用者屬性的預設值，如果您的 LDAP 目錄使用其他架構，請修改這些值。

3 按一下**群組屬性**索引標籤，檢查群組屬性的預設值，如果您的 LDAP 目錄使用其他架構，請修改這些值。

4 按一下**儲存**。

5 測試 LDAP 連線設定和 LDAP 屬性對應：

a 按一下**測試**。

b 輸入您所設定的 LDAP 伺服器使用者的密碼，然後按一下**測試**。

如果連線成功，則會顯示綠色核取記號。

擷取的使用者和群組屬性值會顯示在資料表中。成功對應至 LDAP 屬性的值標有綠色核取記號。未對應至 LDAP 屬性的值為空白，且標有紅色驚歎號。

c 若要結束，請按一下**取消**。

6 若要將 vCloud Director 與設定的 LDAP 伺服器同步，請按一下**同步**。

vCloud Director 會根據您在一般系統設定中設定的同步間隔，定期將使用者和群組資訊與 LDAP 伺服器同步。

等候幾分鐘，讓同步完成。

結果

您可以從新設定的 LDAP 伺服器匯入使用者和群組。

將系統設定為使用 SAML 身分識別提供者

如果您要將使用者和群組從 SAML 身分識別提供者匯入系統組織，您必須為您的系統組織設定此 SAML 身分識別提供者。匯入的使用者可以使用 SAML 身分識別提供者中建立的認證登入系統組織。

若要為 vCloud Director 設定 SAML 身分識別提供者，請透過交換 SAML 服務提供者和身分識別提供者中繼資料來建立相互信任關係。

匯入的使用者嘗試登入時，系統會從 SAML Token (如果可用) 擷取下列屬性，並使用這些屬性解譯對應的使用者相關資訊。

- `email address = "EmailAddress"`
- `user name = "UserName"`
- `full name = "FullName"`
- `user's groups = "Groups"`
- `user's roles = "Roles"` (可以設定此屬性)

如果沒有直接匯入使用者，但仍期望憑藉已匯入群組的成員資格登入，則會使用群組資訊。使用者可能屬於多個群組，因此在工作階段期間可能具有多個角色。

如果將 [遵從身分識別提供者] 角色指派給匯入的使用者或群組，則將根據從 Token 中 [角色] 屬性收集的資訊指派這些角色。如果使用其他屬性，則此屬性名稱僅可使用 API 進行設定，並且僅可設定 [角色] 屬性。如果使用 [遵從身分識別提供者] 角色，但沒有可擷取的角色資訊，則使用者可以登入，但沒有執行任何活動的權限。

必要條件

- 確認您具有 SAML 2.0 相容身分識別提供者的存取權。
- 使用下列來自 SAML 身分識別提供者的中繼資料取得 XML 檔案。
  - 單一登入服務的位置
  - 單一登出服務的位置
  - 服務的 X.509 憑證位置

  如需設定以及從 SAML 提供者取得中繼資料的相關資訊，請參閱 SAML 提供者的說明文件。

程序

1 從主功能表 (☰) 中，選取**管理**。

2 在左面板的 [身分識別提供者] 下，按一下 **SAML**，然後按一下**編輯**。

此時會顯示目前的 SAML 設定。

3 在**服務提供者**索引標籤上，下載 vCloud Director SAML 服務提供者中繼資料。

a 輸入系統組織的實體識別碼。

實體識別碼可向您的身分識別提供者唯一識別您的系統組織。

b 檢查憑證到期日期，如果即將到期，則按一下**重新產生**以重新產生憑證。

此憑證包含在 SAML 中繼資料中，可同時用於加密和簽署。根據在您的組織與 SAML IDP 之間建立信任的方式，可能需要其中一個或兩者都需要。

c 按一下**中繼資料**連結。

此連結類似於 `https://VCD_host_name/cloud/org/System/saml/metadata/alias/vcd`。

您的瀏覽器會下載 SAML 服務提供者中繼資料，這是您必須提供給身分識別提供者的 XML 檔案。

4 在**身分識別提供者**索引標籤上，上傳您先前從身分識別提供者收到的 SAML 中繼資料。

a 選取**使用 SAML 身分識別提供者**。

b 按一下**瀏覽**圖示 (↑) 並上傳檔案，或複製其內容並貼到**中繼資料 XML** 文字方塊中。

5 按一下**儲存**。

結果

管理外掛程式

vCloud Director 外掛程式可延伸 Service Provider Admin Portal 和 vCloud Director Tenant Portal 的功能。您可以上傳、停用外掛程式，以及將其從 Service Provider Admin Portal 刪除。您可以將外掛程式發佈到服務提供者和個別組織。

一些外掛程式會做為 vCloud Director 的一部分進行安裝。

CPOM 延伸

提供使用 vCloud Director Tenant Portal 檢視和管理 SDDC 和 SDDC Proxy 的功能。

自訂入口網站

提供自訂 vCloud Director Service Provider Admin Portal 和 vCloud Director Tenant Portal 的功能。

vCloud Availability

VMware vCloud® Availability™ 外掛程式提供可直接從 vCloud Director 使用者介面存取 vCloud Availability Portal 的功能。如需詳細資訊，請參閱 vCloud Availability 說明文件。

上傳外掛程式

您可以將其他外掛程式上傳至 vCloud Director Service Provider Admin Portal，以供雲端中的服務提供者和組織使用。

必要條件

下載外掛程式安裝檔案。

程序

1. 從主功能表 (☰) 中，選取**自訂入口網站**。
2. 按一下**上傳**。
3. 按一下**選取外掛程式檔案**，瀏覽至目標安裝檔案，然後按一下**開啟**。
4. 按**下一步**。
5. 選取此外掛程式的範圍。

選項	描述
服務提供者	外掛程式功能在 vCloud Director Service Provider Admin Portal 中可用。
承租人	外掛程式功能在您所選組織的 vCloud Director Service Provider Admin Portal 中可用。

6. 如果已將外掛程式限定為承租人，請選取要向其發佈此外掛程式的組織。
7. 檢閱**檢閱並完成**頁面，然後按一下**完成**。

啟用或停用外掛程式

若要防止所有組織使用外掛程式，您可以停用此外掛程式。

程序

1. 從主功能表 (☰) 中，選取**自訂入口網站**。
2. 選取目標外掛程式名稱旁邊的核取方塊，然後按一下**啟用**或**停用**。

刪除外掛程式

您可以從 vCloud Director Service Provider Admin Portal 移除一或多個外掛程式。

程序

1. 從主功能表 (☰) 中，選取**自訂入口網站**。
2. 選取要移除之外掛程式名稱旁邊的核取方塊，然後按一下**刪除**。

3 按一下**儲存**以確認。

從組織發佈或解除發佈外掛程式

您可以修改可使用由外掛程式提供的功能的組織集合。

您可以修改多個外掛程式的組織集合。

程序

1 從主功能表 (☰) 中，選取**自訂入口網站**。

2 選取目標外掛程式名稱旁邊的核取方塊，然後按一下**發佈**。

3 選取此外掛程式的範圍。

選項	描述
服務提供者	外掛程式功能在 vCloud Director Service Provider Admin Portal 中可用。
承租人	外掛程式功能在您所選組織的 vCloud Director Service Provider Admin Portal 中可用。

4 如果已將外掛程式限定為承租人，請選取要向其發佈此外掛程式的組織。

5 按一下**儲存**。

自訂 vCloud Director 入口網站

為了符合您的公司商標標準，並建立完全自訂的雲端體驗，您可以為 vCloud Director Service Provider Admin Portal 和每個組織的 vCloud Director Tenant Portal 設定標誌和主題。此外，還可以修改和新增 vCloud Director 入口網站中兩個右上方功能表的自訂連結。

備註 若要自訂商標屬性和連結，您必須使用 `branding` vCloud OpenAPI 方法。請參閱《vCloud OpenAPI 入門》，網址為：https://code.vmware.com。

入口網站商標

在安裝過程中，vCloud Director 包含兩個主題 - 預設和深色。您可以建立、管理和套用自訂主題。此外，您還可以變更入口網站名稱、標誌與瀏覽器圖示。此外，瀏覽器標題採用您設定的入口網站名稱。

在系統層級設定商標屬性，以便您自訂 vCloud Director Service Provider Admin Portal。每個組織的 vCloud Director Tenant Portal 均採用系統商標屬性，除非您已為特定的承租人設定商標屬性。

對於特定的承租人，您可以選擇性地覆寫入口網站名稱、背景色彩、標誌、圖示、主題以及自訂連結的任意組合。您尚未設定的任何值會使用對應的系統預設值。

備註 依預設，不會在登入的工作階段之外顯示個別承租人商標。個別承租人商標不會出現在登入和登出頁面上，因此承租人無法探索是否存在其他承租人。您可以使用儲存格管理工具在登入的工作階段之外啟用商標：

```
manage-config -n backend.branding.requireAuthForBranding -v false
```

如需使用儲存格管理工具的相關資訊，請參閱《vCloud Director 管理員指南》。

自訂連結

自訂連結是入口網站商標的元件。自訂連結有兩種類型：

- `override` 功能表項目會取代功能表項目**說明**、**關於**和**下載 VMRC** 的現有連結。依預設，**下載 VMRC** 會將使用者重新導向至 https://my.vmware.com 以下載 VMRC，這需要使用者使用已註冊的帳戶進行下載。透過覆寫此連結，您可以將 VMRC 安裝程式重新放置到您自己的伺服器。
- `link` 功能表項目是您新增到入口網站右上角的**登出**功能表項目的新連結。新的自訂連結會以 API 呼叫中指定的順序顯示。

  您可以使用 `section` 和 `separator` 功能表項目組織整理這些自訂連結。`section` 功能表項目在功能表中新增一個標頭，而 `separator` 功能表項目在功能表中新增一行。

自訂連結支援自訂變數，您可以使用這些自訂變數以查詢參數的形式將識別資訊傳遞至其他應用程式。

vCloud Director 支援自訂連結的 `url` 值中的下列自訂變數：

表 11-1. 自訂連結的自訂變數

變數	描述
`${TENANT_NAME}`	組織名稱
`${TENANT_ID}`	組織識別碼
`${SESSION_TOKEN}`	x-vcloud-authorization Token

例如：

```
url: https://host:port/tenant/${TENANT_NAME}/vdcs
```

位於組織 myorg 的 vCloud Director Tenant Portal，將轉換為：

```
url: https://host:port/tenant/myorg/vdcs
```

監視 vCloud Director 12

系統管理員可以監視已完成與進行中的操作，並且檢視在提供者虛擬資料中心、組織虛擬資料中心以及資料存放區層級的資源使用資訊。

本章節討論下列主題：

vCloud Director 與成本報告

您可以使用 VMware vRealize Operations Tenant App for vCloud Director 來設定 vCloud Director 的成本報告系統。

VMware vRealize Operations Tenant App 具有計量功能，可讓服務提供者為客戶群提供計費服務。

VMware vRealize Operations Tenant App 也是面向承租人的應用程式，可讓承租人管理員查看其環境及其計費資料。

如需 vCloud Director 和 VMware vRealize Operations Tenant App 之間相容性的相關資訊，請參閱《VMware 產品互通性對照表》，網址為 http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php。

您可以在 https://marketplace.vmware.com/vsx/solutions/management-pack-for-vcloud-director 下載 VMware vRealize Operations Tenant App。

如需如何使用 VMware vRealize Operations Tenant App 的相關資訊，請參閱使用 vRealize Operations Tenant App for vCloud Director 做為服務提供者和使用 vRealize Operations Tenant App for vCloud Director 做為承租人。

檢視提供者虛擬資料中心的使用資訊

提供者虛擬資料中心為其組織虛擬資料中心提供計算、記憶體和儲存資源。您可以監控提供者虛擬資料中心資源的使用情況，以便決定是否新增更多資源。

程序

1 從主功能表 (☰) 中，選取**雲端資源**。

2 在左面板中，按一下**提供者 VDC**，然後按一下目標提供者虛擬資料中心的名稱。

3 按一下**設定 > 度量**索引標籤。

4 如需有關每個參數的詳細資料，請按一下每個資訊圖示。

管理服務

13

vCloud Director Service Provider Admin Portal 中的內容程式庫視圖提供用於整合 vRealize Orchestrator 的介面。vRealize Orchestrator 工作流程可用作服務提供者管理員可發佈至承租人或其他服務提供者之服務的目錄，藉此延伸所提供的功能集和管理功能。

本章節討論下列主題：

將 vRealize Orchestrator 與 vCloud Director 整合

您可以透過 vCloud Director Service Provider Admin Portal，將 vRealize Orchestrator 與 vCloud Director 整合。

藉由允許服務提供者管理員透過工作流程協調和第三方外掛程式的使用來開發複雜的自動化工作，將 vRealize Orchestrator 與 vCloud Director 整合以延伸 vCloud Director 的基本功能。

透過 vCloud Director Service Provider Admin Portal，服務提供者管理員能夠從已登錄的 vRealize Orchestrator 伺服器執行個體檢視、匯入和執行工作流程。

在 vCloud Director Service Provider Admin Portal 中，vRealize Orchestrator 工作流程可發佈至服務提供者或承租人，以便快速存取控制和執行自訂與內建服務。

vRealize Orchestrator 具有包含預先建立的工作的廣泛工作流程程式庫，這些工作旨在解決特定挑戰和執行一般管理工作。VMware Solution Exchange 中也提供了第三方外掛程式。

向 vCloud Director 登錄 vRealize Orchestrator 執行個體

若要透過 vCloud Director 中的 vRealize Orchestrator 利用工作流程協調和工作自動化，您可以在 vCloud Director Service Provider Admin Portal 中登錄 vRealize Orchestrator 執行個體。

必要條件

- 部署並設定 vRealize Orchestrator 伺服器執行個體。如需詳細資訊，請參閱 vRealize Orchestrator 說明文件中的《安裝和設定 VMware vRealize Orchestrator》。
- 設定 vRealize Orchestrator 使用 vSphere 做為驗證提供者。
- 確認 vCloud Director 已向與 vRealize Orchestrator 用於驗證的 vCenter Single-Sign On 相同的 Platform Services Controller 的 Lookup Service 登錄。

程序

1 從主功能表 (☰) 中，選取**內容程式庫**

   a 從左面板中，選取**服務管理**。

   已登錄的 vRealize Orchestrator 伺服器清單隨即顯示。

2 若要登錄新的 vRealize Orchestrator 伺服器，請按一下 ＋ 按鈕。

   登錄 vRealize Orchestrator 對話方塊隨即顯示。

3 輸入下列值。

選項	描述
名稱	已登錄的 vRealize Orchestrator 執行個體的名稱。
描述	已登錄的 vRealize Orchestrator 伺服器執行個體的說明。
主機名稱	vRealize Orchestrator 伺服器的完整網域名稱和伺服器連接埠。預設 HTTPS 連接埠值為 8281。 **備註** vCloud Director 會連線至 vRealize Orchestrator 的 API 介面。
使用者名稱	做為 vRealize Orchestrator 管理員群組成員的使用者帳戶。
密碼	vRealize Orchestrator 管理員帳戶的密碼。
信任錨點	採用 PEM 格式的 vRealize Orchestrator 伺服器 SSL 憑證。 按一下上傳圖示 (⤒)，以尋找並選取 `.pem` 檔案。

4 按一下**確定**，完成登錄。

   vRealize Orchestrator 伺服器已向 vCloud Director 登錄。

建立服務類別

您可以按服務類別組織整理服務。

程序

1 從主功能表 (☰) 中，選取**內容程式庫**

   a 從左面板中，選取**服務管理**。

   b 導覽至**服務類別**索引標籤。

   現有伺服器類別的清單隨即顯示。

2 若要建立新的服務類別，請按一下 ＋ 按鈕。

   新增服務類別對話方塊隨即顯示。

3 輸入下列值。

選項	描述
名稱	服務類別的名稱。
圖示	匯入服務類別的顯示圖示。
描述	服務類別的簡短說明。

編輯服務類別

您可以編輯現有的服務類別。

程序

1 從主功能表 (☰) 中，選取**內容程式庫**

   a 從左面板中，選取**服務管理**。

   b 導覽至**服務類別**索引標籤。

   現有伺服器類別的清單隨即顯示。

2 使用所選服務類別左側的清單列 (⋮)，然後按一下**編輯**。

3 編輯下列值。

選項	描述
名稱	服務類別的名稱。
圖示	匯入服務類別的顯示圖示。
描述	服務類別的簡短說明。

匯入服務

您可以從已向 vCloud Director 登錄的 vRealize Orchestrator 執行個體的工作流程程式庫匯入服務。

必要條件

- 登錄 vRealize Orchestrator 執行個體。請參閱向 vCloud Director 登錄 vRealize Orchestrator 執行個體。
- 建立服務類別。請參閱建立服務類別。

程序

1 從主功能表 (☰) 中，選取**內容程式庫**。

   a 從左面板中，選取**服務程式庫**。

   可用服務會顯示在卡視圖中，每頁十二個項目，根據名稱按字母順序排序。每張卡片指示項目為 vRealize Orchestrator 工作流程，並且會顯示服務的名稱以及對應工作流程所匯入的服務類別的標籤。

2 若要匯入新的服務，請按一下**匯入**按鈕。

3 請依照**匯入**精靈的步驟操作。

選項	描述
匯入至目標程式庫	選取要匯入服務的服務類別。
選取來源	選取要從中匯入工作流程的 vRealize Orchestrator 執行個體。
選取工作流程	展開階層式樹狀結構視圖，以選取要匯入的一或多個工作流程。
檢閱	檢閱詳細資料，然後按一下**完成**以完成匯入。

   匯入的工作流程會顯示在**服務程式庫**卡視圖中。

搜尋服務

您可以依名稱或所屬服務類別來搜尋服務。

程序

1 從主功能表 (☰) 中，選取**內容程式庫**。

   a 從左面板中，選取**服務程式庫**。

   可用服務會顯示在卡視圖中，每頁十二個項目，根據名稱按字母順序排序。每張卡片指示項目為 vRealize Orchestrator 工作流程，並且會顯示服務的名稱以及對應工作流程所匯入的服務類別的標籤。

2 在頁面上方的**搜尋**文字方塊中，輸入您想要尋找的服務名稱或服務類別的字組或字元。

   a 選取您想要在服務名稱還是類別之間搜尋。

   搜尋結果會顯示在卡視圖中，每頁十二個項目，根據名稱按字母順序排序。

執行服務

您可以匯入服務的形式執行 vRealize Orchestrator 工作流程。

程序

1 從主功能表 (☰) 中，選取**內容程式庫**。

a 從左面板中，選取**服務程式庫**。

可用服務會顯示在卡視圖中，每頁十二個項目，根據名稱按字母順序排序。每張卡片指示項目為 vRealize Orchestrator 工作流程，並且會顯示服務的名稱以及對應工作流程所匯入的服務類別的標籤。

2 若要執行服務，請在所選服務的卡中，按一下**執行**。

執行服務精靈隨即顯示。

3 填寫服務的必要輸入參數，然後按一下**完成**。

結果

您可以在**最近的工作**視圖中監控執行狀態。如需詳細資訊，請參閱檢視工作。

備註 當您啟動 vRealize Orchestrator 工作流程做為 vCloud Director 服務時，vCloud Director 會新增幾個自訂參數至工作流程執行內容。

自訂內容	描述
`_vcd_orgName`	執行服務的使用者所屬組織的名稱。
`_vcd_orgId`	執行服務的使用者所屬組織的識別碼。
`_vcd_userName`	執行服務的使用者名稱。
`_vcd_isAdmin`	如果執行服務的使用者為**管理員**，則值為 `True`。
`_vdc_isAdmin`	已過時。如果執行服務的使用者為**管理員**，則值為 `True`。
`_vdc_userName`	已過時。執行服務的使用者名稱。
`_vcd_sessionToken`	向 vCloud Director 成功驗證後收到的驗證 Token
`_vcd_apiEndpoint`	vCloud Director REST API 端點

變更服務類別

您可以變更服務所屬的類別。

程序

1 從主功能表 (☰) 中，選取**內容程式庫**。

a 從左面板中，選取**服務程式庫**。

可用服務會顯示在卡視圖中，每頁十二個項目，根據名稱按字母順序排序。每張卡片指示項目為 vRealize Orchestrator 工作流程，並且會顯示服務的名稱以及對應工作流程所匯入的服務類別的標籤。

2 在所選服務的卡中，選取**管理 > 變更類別**。

變更類別對話方塊隨即開啟。

3 選取要在其中放置服務的類別，然後按一下**儲存**。

解除登錄服務

透過解除登錄服務，可以移除服務提供者和承租人對服務的存取權。

程序

1 從主功能表 (☰) 中，選取**內容程式庫**。

a 從左面板中，選取**服務程式庫**。

可用服務會顯示在卡視圖中，每頁十二個項目，根據名稱按字母順序排序。每張卡片指示項目為 vRealize Orchestrator 工作流程，並且會顯示服務的名稱以及對應工作流程所匯入的服務類別的標籤。

2 在所選服務的卡中，選取**管理 > 解除登錄工作流程**。

解除登錄工作流程對話方塊隨即開啟。

3 若要從服務程式庫中移除服務，請按一下**刪除**。

發佈服務

您可以透過發佈服務來控制服務提供者和承租人對服務的存取權。

程序

1 從主功能表 (☰) 中，選取**內容程式庫**。

a 從左面板中，選取**服務程式庫**。

可用服務會顯示在卡視圖中，每頁十二個項目，根據名稱按字母順序排序。每張卡片指示項目為 vRealize Orchestrator 工作流程，並且會顯示服務的名稱以及對應工作流程所匯入的服務類別的標籤。

2 在所選服務的卡中，選取**管理 > 發佈工作流程**。

發佈工作流程對話方塊隨即顯示。

3 若要發佈到服務提供者，請選取**發佈到服務提供者**，然後按一下**儲存**。

4 若要發佈到特定承租人組織，請選取**發佈到承租人**按鈕。

a 此時將顯示具有可用承租人組織的清單。選取要將工作流程發佈到的承租人組織，然後按一下**儲存**。

5 若要發佈到所有承租人組織，請選取**發佈到所有承租人**，然後按一下**儲存**。

管理自訂實體

14

vCloud Director 中的自訂實體定義是繫結到 vRealize Orchestrator 物件類型的物件類型。當服務提供者發佈自訂實體定義至其他服務提供者或者一或多個承租人時，使用者 vCloud Director 可以根據需要擁有、管理和變更這些類型。透過執行服務，服務提供者使用者和組織使用者可以具現化自訂實體，並針對物件的執行個體套用動作。

本章節討論下列主題：

搜尋自訂實體

您可以依名稱搜尋自訂實體。

程序

1 從主功能表 (☰) 中，選取**內容程式庫**。

   a 從左面板中，選取**自訂實體定義**。

   自訂實體的清單會顯示在卡視圖中，每頁十二個項目，根據名稱按字母順序排序。每張卡片會顯示自訂實體的名稱、實體對應的 vRealize Orchestrator 類型、實體的類型以及說明 (如果有的話)。

2 在頁面上方的**搜尋**文字方塊中，輸入您想要尋找的實體名稱的字組或字元。

   搜尋結果會顯示在卡視圖中，每頁十二個項目，根據名稱按字母順序排序。

編輯自訂實體定義

您可以修改自訂實體的名稱和說明。無法變更實體類型或實體所繫結的 vRealize Orchestrator 物件類型。這些是自訂實體的預設內容。如果您要修改任何預設內容，必須刪除自訂實體定義並重新建立。

程序

1 從主功能表 (☰) 中，選取**內容程式庫**。

a 從左面板中，選取**自訂實體定義**。

自訂實體的清單會顯示在卡視圖中，每頁十二個項目，根據名稱按字母順序排序。每張卡片會顯示自訂實體的名稱、實體對應的 vRealize Orchestrator 類型、實體的類型以及說明 (如果有的話)。

2 在所選自訂實體的卡中，選取**動作 > 編輯**。

新的對話方塊隨即開啟。

3 修改自訂實體定義的名稱或說明。

4 按一下**確定**以確認變更。

新增自訂實體定義

您可以建立自訂實體，並將其對應到現有的 vRealize Orchestrator 物件類型。

程序

1 從主功能表 (☰) 中，選取**內容程式庫**。

a 從左面板中，選取**自訂實體定義**。

自訂實體的清單會顯示在卡視圖中，每頁十二個項目，根據名稱按字母順序排序。每張卡片會顯示自訂實體的名稱、實體對應的 vRealize Orchestrator 類型、實體的類型以及說明 (如果有的話)。

2 按一下 ＋ 圖示以新增自訂實體。

新的對話方塊隨即開啟。

3 請依照**自訂實體定義**精靈的步驟操作。

步驟	
名稱與描述	輸入新實體的名稱，並選擇性地輸入說明。 輸入實體類型的名稱，例如 `sshHost`。
vRO	從下拉式功能表中，選取您將用來對應自訂實體定義的 vRealize Orchestrator。 **備註** 如果您有多個 vRealize Orchestrator 伺服器，則必須分別為每個伺服器建立自訂實體定義。
類型	按一下檢視清單圖示 (☰)，以瀏覽依外掛程式分組的可用 vRealize Orchestrator 物件類型。例如，**SSH > 主機**。 如果您知道類型的名稱，可以直接將其輸入文字方塊中。例如 `SSH:Host`。
檢閱	檢閱您所指定的詳細資料，然後按一下**完成**以完成建立。

結果

新的自訂實體定義會顯示在卡視圖中。

自訂實體執行個體

執行 vRealize Orchestrator 工作流程時，如果輸入參數是已在 vCloud Director 中定義為自訂實體定義的物件類型，會將輸出參數顯示為自訂實體的執行個體。

程序

1 從主功能表 (☰) 中，選取**內容程式庫**。

   a 從左面板中，選取**自訂實體定義**。

   自訂實體的清單會顯示在卡視圖中，每頁十二個項目，根據名稱按字母順序排序。每張卡片會顯示自訂實體的名稱、實體對應的 vRealize Orchestrator 類型、實體的類型以及說明 (如果有的話)。

2 在所選自訂實體的卡中，按一下**執行個體**。

   可用的執行個體會顯示在網格視圖中。

3 按一下每個實體左側的清單列 (⋮)，以顯示相關聯的工作流程。

   按一下工作流程會起始工作流程執行，以將實體執行個體視為輸入參數。

將動作關聯至自訂實體

透過將動作關聯至自訂實體定義，您可以在特定自訂實體的執行個體上執行一組 vRealize Orchestrator 工作流程。

程序

1 從主功能表 (☰) 中，選取**內容程式庫**。

   a 從左面板中，選取**自訂實體定義**。

   自訂實體的清單會顯示在卡視圖中，每頁十二個項目，根據名稱按字母順序排序。每張卡片會顯示自訂實體的名稱、實體對應的 vRealize Orchestrator 類型、實體的類型以及說明 (如果有的話)。

2 在所選自訂實體的卡中，選取**動作 > 關聯動作**。

   新的對話方塊隨即開啟。

3 請依照**將自訂實體關聯到 VRO 工作流程**精靈的步驟操作。

步驟	詳細資訊
選取 VRO 工作流程	選取其中一個列出的工作流程。這些是**服務程式庫**頁面中提供的工作流程。
選取工作流程輸入參數	從清單中選取可用的輸入參數。將 vRealize Orchestrator 工作流程的類型與自訂實體定義的類型相關聯。
檢閱關聯	檢閱您所指定的詳細資料，然後按一下**完成**以完成關聯。

範例

例如，如果您有 `SSH:Host` 類型的自訂實體，您可以透過選取符合自訂實體類型的 `sshHost` 輸入參數，將其與 `Add a Root Folder to SSH Host` 工作流程相關聯。

解除動作與自訂實體的關聯

您可以從相關聯的動作清單中移除 vRealize Orchestrator 工作流程。

程序

1 從主功能表 (☰) 中，選取**內容程式庫**。

   a 從左面板中，選取**自訂實體定義**。

   自訂實體的清單會顯示在卡視圖中，每頁十二個項目，根據名稱按字母順序排序。每張卡片會顯示自訂實體的名稱、實體對應的 vRealize Orchestrator 類型、實體的類型以及說明 (如果有的話)。

2 在所選自訂實體的卡中，選取**動作 > 解除關聯動作**。

   新的對話方塊隨即開啟。

3 選取您要移除的工作流程，然後按一下**解除關聯動作**。

   vRealize Orchestrator 工作流程不再與自訂實體相關聯。

發佈自訂實體

您必須發佈自訂實體，以便來自其他承租人或服務提供者的使用者可以將自訂實體執行個體用作輸入參數來執行工作流程。

程序

1 從主功能表 (☰) 中，選取**內容程式庫**。

   a 從左面板中，選取**自訂實體定義**。

   自訂實體的清單會顯示在卡視圖中，每頁十二個項目，根據名稱按字母順序排序。每張卡片會顯示自訂實體的名稱、實體對應的 vRealize Orchestrator 類型、實體的類型以及說明 (如果有的話)。

2 在所選自訂實體的卡中，選取**動作 > 發佈**。

   新的對話方塊隨即開啟。

3 選擇您要發佈自訂實體定義至服務提供者、所有承租人，還是僅發佈至所選承租人。

4 按一下**儲存**以確認變更。

   自訂實體定義將可供所選方使用。

刪除自訂實體

如果自訂實體已不再使用、設定錯誤，或者您想要將 vRealize Orchestrator 類型對應至其他自訂實體，可以刪除自訂實體定義。

程序

1 從主功能表 (☰) 中，選取**內容程式庫**。

   a 從左面板中，選取**自訂實體定義**。

   自訂實體的清單會顯示在卡視圖中，每頁十二個項目，根據名稱按字母順序排序。每張卡片會顯示自訂實體的名稱、實體對應的 vRealize Orchestrator 類型、實體的類型以及說明 (如果有的話)。

2 在所選自訂實體的卡中，選取**動作 > 刪除**。

3 確認刪除。

   自訂實體隨即從卡視圖中移除。