VMware Cloud Director 服務提供者管理入口網站指南

修改日期：2021 年 4 月 8 日

VMware Cloud Director 10.2

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

VMware Cloud Director™ 服務提供者管理入口網站指南

1

《VMware Cloud 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 VMware Cloud Director Service Provider Admin Portal 所提供功能的服務提供者管理員。

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。

VMware Cloud Director Service Provider Admin Portal 入門 2

VMware Cloud 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：

VMware Cloud Director 管理的概觀

藉由 VMware VMware Cloud 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。

《VMware Cloud Director Service Provider Admin Portal 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

VMware Cloud 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。VMware Cloud 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。

VMware Cloud 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《VMware Cloud Director Service Provider Admin Portal 指南》或 VMware Cloud Director 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，VMware Cloud 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 VMware Cloud 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。

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

專用 vCenter Server 執行個體和 Proxy

專用 vCenter Server 執行個體是封裝整個 vCenter Server 安裝的雲端資源。一個專用 vCenter Server 執行個體包含一或多個 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專用 vCenter Server 執行個體和 Proxy。提供者可以將專用 vCenter Server 執行個體發佈至承租人。

若要建立和管理專用 vCenter Server 執行個體及 Proxy，您可以使用 Service Provider Admin Portal 或 vCloud OpenAPI。請參閱第 9 章 管理專用 vCenter Server 執行個體 和 VMware Cloud Director 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。

VMware Cloud Director 網路

VMware Cloud 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，VMware Cloud 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 VMware Cloud 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。

VMware Cloud 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 VMware Cloud 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。

VMware Cloud 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《VMware Cloud 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。VMware Cloud 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。

VMware Cloud 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

VMware Cloud 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《VMware Cloud 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 VMware Cloud Director Service Provider Admin Portal。

您可以使用網頁瀏覽器來存取 VMware Cloud Director Service Provider Admin Portal。

必要條件

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

程序

1. 在瀏覽器中，輸入 VMware Cloud 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。

使用 VMware Cloud Director 快速搜尋

您可以使用 VMware Cloud Director 快速搜尋來尋找畫面、實體和動作。結果取決於您在 UI 中的位置。

結果取決於內容、是否已選取實體以及特定實體的可用動作。搜尋結果分為多個區段。

- 全域導覽 - 此區段中的結果與特定實體 (例如，Edge 閘道、LDAP、工作、受信任的憑證、虛擬機器等) 不相關。無論您在 UI 中位於何處，都會得到這些結果。
- 內容導覽 - 此區段中的結果取決於在 UI 中選取的實體。例如，虛擬機器、網狀圖等 vApp 特定視圖。如果您選取諸如 vApp 之類的實體，則搜尋會同時顯示全域和內容導覽結果，以及可能適用於該實體的任何動作。

- 內容動作 - 此區段中的結果取決於在 UI 中選取的實體。根據您在 UI 中的位置以及選取的實體，可以透過使用快速搜尋結果執行與實體相關的動作。例如，從虛擬機器的詳細資料視圖中搜尋，可顯示全域視圖、內容視圖中的結果以及可對所選虛擬機器執行的動作。
- 依名稱的實體搜尋 - 如果您要檢視實體清單，則搜尋結果還會包括與清單中實體類型相同的實體的名稱。例如，如果您要檢視虛擬機器清單，則搜尋結果將包括全域導覽相符項和相符的虛擬機器名稱。如果您要檢視的清單中有多頁實體，則搜尋會檢查完整的實體清單，並且可能會顯示目前頁面上不可見的名稱。

程序

1 開啟**快速搜尋**視窗。
   - 從頂部導覽列中，按一下**說明**功能表，然後選取**快速搜尋**。
   - 根據您的作業系統，按 Ctrl+.或 Cmd+.。
2 輸入搜尋準則。
3 瀏覽結果，然後點選或按 Enter 選取選項或執行動作。

   可以使用向上和向下方向鍵來瀏覽搜尋結果。

檢視工作

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

您可以使用 Service Provider Admin Portal 中的最近的工作視圖監控工作狀態。對環境中的任何問題進行疑難排解時，先使用此視圖是很好的辦法。

在**最近的工作**按鈕旁邊，執行中工作和失敗的工作分別顯示為藍色和紅色。

程序

1 在左下角按一下**最近的工作**。
2 (選擇性) 對最近的工作清單進行排序和篩選。

結果

將顯示最近的工作清單，以及工作的狀態、類型、啟動者、開始時間和完成時間。

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 在頂部導覽列中，按一下**監控**和**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.cloud*。
組織	組織的名稱。
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。

設定使用者喜好設定

您可以設定每次登入系統時啟用的特定顯示與系統警示喜好設定。

若要進一步瞭解租用，請參閱瞭解租用。

程序

1 在頂部導覽列中，按一下您的使用者名稱，然後選取**使用者喜好設定**。

2 選取要在登入時顯示的頁面。

   a 選取**開始頁面**旁的選項按鈕，然後按一下**編輯**。

   b 從下拉式功能表中選取一個選項，然後按一下**儲存**。

3 設定執行階段租用到期的電子郵件通知。

   a 選取**部署租用警示時間**旁的選項按鈕，然後按一下**編輯**。

   b 輸入以秒為單位的值，然後按一下**儲存**。

4 設定針對儲存區租用到期的電子郵件通知。

   a 選取**儲存區租用警示時間**旁的選項按鈕，然後按一下**編輯**。

   b 輸入以秒為單位的值，然後按一下**儲存**。

名稱和描述的長度限制

在 VMware Cloud Director 中輸入值時，請遵循這些準則。

`name` 屬性以及 `Description` 和 `ComputerName` 元素字串值的長度限制取決於其連結的物件。

表 2-1. 物件內容的長度限制

物件	屬性	字元長度上限
`Catalog`	`name`	128
`Catalog`	`Description`	256
`EdgeGateway`	`name`	35
`Media`	`name`	128
`Media`	`Description`	256
`VApp`	`name`	128
`VApp`	`Description`	256
`VAppTemplate`	`name`	128
`VAppTemplate`	`Description`	256
`Vdc`	`name`	128
`Vdc`	`Description`	256
`Vm`	`name`	128

表 2-1. 物件內容的長度限制 (續)

物件	屬性	字元長度上限
Vm	ComputerName	在 Windows 上為 15，在所有其他平台上為 63
Vm	Description	256

管理 vSphere 資源 3

VMware Cloud Director 會從基礎的 vSphere 虛擬基礎結構衍生其資源。在 VMware Cloud 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。

VMware Cloud 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，VMware Cloud 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 VMware Cloud Director 及其 VMware Cloud 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 VMware Cloud 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，即已納入提供者範圍。如需建立提供者虛擬資料中心的相關資訊，請參閱 建立提供者虛擬資料中心。

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

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 或專用 vCenter Server 執行個體。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 執行個體建立專用 vCenter Server 執行個體，反之亦然。

集中式 SSL 管理

從 10.1 版開始，VMware Cloud Director 將移至可識別承租人的集中式儲存區域，以進行憑證管理。如此一來，VMware Cloud Director 會將所有憑證集中在同一個位置，以便**系統管理員**和**組織管理員**可以檢視、稽核和管理系統中各種元件所使用的所有憑證。您可以使用 VMware Cloud Director API 在可識別承租人的新儲存區域中新增、更新或移除憑證。請參閱《VMware Cloud Director API 架構參考》。

新增或編輯新的 vCenter Server 執行個體、NSX Manager 執行個體或 NSX-T Manager 執行個體時，VMware Cloud Director 使用者介面會探查此端點是否存在它要提供的任何憑證。VMware Cloud Director 會將任何您決定信任的憑證新增至集中式憑證儲存區域。

本章節討論下列主題：

- 新增 vCenter Server 和 NSX 資源
- 透過 VMware Cloud Director 端點和 Proxy 存取 vSphere 元件

新增 vCenter Server 和 NSX 資源

VMware Cloud 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，VMware Cloud Director 可做為承租人與基礎 vSphere 環境之間的 HTTP 伺服器。

如需 VMware Cloud 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

可以連結 vCenter Server 執行個體，以便其資源可在 VMware Cloud 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。對於專用 vCenter Server 執行個體或與 NSX-T Manager 執行個體相關聯的執行個體，可以單獨連結 vCenter Server 執行個體。

VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director 環境中的任何站台。

您可以連結可直接存取的 vCenter Server 執行個體，或連結位於 Proxy 後方的 vCenter Server 執行個體。透過使用 vCloud OpenAPI，您可以使用 VMware Cloud Director 內的 Proxy 組態，以建立 VMware Cloud Director 執行個體與其新增的 vCenter Server 執行個體之間的代理連線。如此一來，VMware Cloud Director 和 vCenter Server 執行個體即可存在於不同的位置或站台中。

若要連結位於 Proxy 後方的 vCenter Server 執行個體，您必須先宣告 Proxy 組態。然後，必須連結 vCenter Server 執行個體並設定 VMware Cloud Director，才能在存取 vCenter Server 執行個體時使用 Proxy 組態。您也可以透過 Proxy 連結 NSX Data Center for vSphere 解決方案。VMware Cloud Director 不支援 NSX-T Data Center 的 Proxy 組態。對於 vCenter Server 執行個體登錄的 Platform Services Controller，您不需要額外的 SSL 組態或 Proxy 組態。

必要條件

- 如果設定了 VMware Cloud Director 以驗證 vCenter 和 vSphere SSO 憑證，請確認您已將 vCenter Server 憑證上傳至 VMware Cloud Director。如需一般系統設定的相關資訊，請參閱修改一般系統設定。
- 如果設定了 VMware Cloud Director 以驗證 NSX Manager 憑證，請確認您已將 NSX Manager 憑證上傳至 VMware Cloud Director。如需一般系統設定的相關資訊，請參閱修改一般系統設定。

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 VMware Cloud 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 從頂部導覽列的**資源**下，按一下**基礎結構資源**。

2 在左窗格中，按一下 **vCenter Server 執行個體**，然後按一下**新增**。

3 如果您有多站台 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 如果端點沒有受信任的憑證，請在**信任憑證**視窗中確認您是否信任此端點。

在多站台環境中，如果您已登入 vCloud Director 10.0 站台或嘗試將 vCenter Server 執行個體登錄至 vCloud Director 10.0 站台，則 VMware Cloud Director 不會將端點新增至集中式憑證儲存區域。

- 若要將端點新增至集中式憑證儲存區域並繼續，請按一下**信任**。
- 如果您不信任此端點，請按一下**取消**，並對受信任的端點重複步驟 5 至步驟 9。

11 (選擇性) 若要略過新增與 vCenter Server 執行個體相關聯的 NSX Manager 執行個體，請關閉**設定組態**切換按鈕，然後按**下一步**。

如果您希望 VMware Cloud 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。

12 如果您想要新增將不會用作提供者 VDC 的承租人專用 vCenter Server，請開啟**啟用承租人存取**切換按鈕。

將 vCenter Server 執行個體新增到 VMware Cloud Director 後，承租人相關資訊會顯示在執行個體的詳細資料視圖中。

13 如果您想讓 VMware Cloud Director 為 vCenter Server 執行個體和 SSO 服務產生預設 Proxy，請開啟**產生 Proxy** 切換按鈕。

將 vCenter Server 執行個體新增到 VMware Cloud Director 後，這些 Proxy 會顯示在 **vSphere 資源**下的 **Proxy** 索引標籤中。

14 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 VMware Cloud 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** 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
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《VMware Cloud Director 租用戶入口網站指南》。
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`**。

5 按**下一步**。

6 如果端點沒有受信任的憑證，請在**信任憑證**視窗中確認您是否信任此端點。

- 若要將端點新增至集中式憑證儲存區域並繼續，請按一下**信任**。
- 如果您不信任此端點，請按一下**取消**，並對受信任的端點重複步驟 2 至步驟 4。

7 啟用或停用存取組態設定。

8 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。
- 建立提供者虛擬資料中心.

搜尋和採用 vApp

在預設組態中，組織 VDC 會搜尋在支援 VDC 之任何 vCenter Server 資源集區中建立的虛擬機器。系統會建構一個簡化的 vApp (由系統管理員擁有)，以包含每個搜尋到的虛擬機器 (VM)。當系統管理員授與您對搜尋到的 vApp 的存取權之後，您便可以在撰寫或重新撰寫 vApp 時參考其中的虛擬機器，或修改 vApp 以加以採用或匯入。

搜尋到的 vApp 僅包含一個虛擬機器，並受限於多個限制，這些限制不適用於 VMware Cloud Director 中建立的 vApp。無論是否採用這些搜尋到的 vApp，它們做為撰寫或重新撰寫 vApp 時使用的虛擬機器來源，都非常有用。

系統會為每個搜尋到的 vApp 指定一個名稱，此名稱衍生自 vApp 中所包含之 vCenter 虛擬機器的名稱，組織管理員會指定前置詞。

如果想要搜尋其他 vApp，系統管理員可以使用 VMware Cloud Director API 建立採用提供者 VDC 提供的指定資源集區的組織 VDC。這些已採用資源集區中的 vCenter 虛擬機器會做為搜尋到的 vApp 顯示在新 VDC 中，並且會做為候選進行採用。

備註 只有處於電源關閉狀態時，才會搜尋到具有 IDE 硬碟的虛擬機器。

如果 VMware Cloud Director 無法搜尋到一或多個 vCenter 虛擬機器，您可以透過偵錯 vCenter Server 虛擬機器探索來調查可能的原因。如需詳細資訊，請參閱《VMware Cloud Director 安裝、設定與升級指南》。

啟動虛擬機器探索

虛擬機器探索預設為啟用狀態。若要停用虛擬機器探索，系統管理員必須取消選取**系統設定** > **一般**索引標籤上的**已啟用虛擬機器探索**核取方塊。組織管理員可以使用 VMware Cloud Director API 停用個別 VDC 的虛擬機器探索，或組織中所有 VDC 的虛擬機器探索。

從搜尋到的 vApp 使用虛擬機器

當系統管理員授與您對搜尋到的 vApp 的存取權之後，您便可以使用該 vApp 的虛擬機器，其使用方式與使用任何其他 vApp 或 vApp 範本所包含的虛擬機器相同。例如，您可以在建立新的 vApp 時指定虛擬機器。您也可以複製搜尋到的 vApp 或修改其名稱、描述或租用設定，而不會觸發採用程序。

採用搜尋到的 vApp

您可以透過變更搜尋到的 vApp 的 vApp 網路，或將虛擬機器新增到此 vApp，以採用此 vApp。當您採用搜尋到的 vApp 之後，系統會將其匯入並視為如同在 VMware Cloud Director 中建立的一樣。透過 vCloud API 要求擷取已採用的 vApp 時，它會包含一個名為 `autoNature` 的元素。如果搜尋到的 vApp 已採用或已在 VMware Cloud Director 中建立，則此元素的值為 `false`。您無法將已採用的 vApp 還原為搜尋到的 vApp。

如果刪除或移動搜尋到的 vApp 所包含的虛擬機器，系統也會移除對應的 vApp。此行為不適用於已採用的 vApp。

為包含搜尋到的 vCenter 虛擬機器而建立的 vApp 與您手動將虛擬機器做為 vApp 匯入時建立的 vApp 類似，但是在某些方面做出了簡化，您可能需要先對其進行修改，然後才能在 VDC 中進行部署。例如，您可能必須編輯其網路與儲存區內容，以及針對您組織的特定需求進行其他調整。

備註 採用虛擬機器不會保留 vCenter Server 中設定的虛擬機器保留、限制和共用率設定。匯入的虛擬機器會從所在的組織虛擬資料中心取得資源配置設定。

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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director 登錄 NSX-T Manager 執行個體，以便 VMware Cloud 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. 從頂部導覽列的**資源**下，按一下**基礎結構資源**。
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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director API 程式設計指南，網址為：https://code.vmware.com。

管理 NSX Advanced 負載平衡

從 10.2 版開始，VMware Cloud Director 透過利用 VMware NSX Advanced Load Balancer 的功能來提供負載平衡服務。

身為**系統管理員**，您可以針對 NSX-T Data Center 支援的虛擬資料中心啟用和設定對負載平衡服務的存取權。

負載平衡服務與 NSX-T Data Center Edge 閘道相關聯，其範圍可以限定為 NSX-T Data Center 支援的組織 VDC 或限定為具有 NSX-T Data Center 網路提供者類型的資料中心群組。

部署並設定要用於 NSX-T Data Center 部署的 NSX Advanced Load Balancer 後，向 VMware Cloud Director 登錄控制器。

如需如何使用 NSX-T 設定 NSX Advanced Load Balancer 的相關資訊，請參閱〈Avi 與 NSX-T 整合〉。

如需如何使用 VMware Cloud Director 部署 NSX Advanced Load Balancer 的相關資訊，請參閱〈使用 VMware Cloud Director 部署 NSX Advanced Load Balancer〉。

若要使用 NSX Advanced Load Balancer 提供的虛擬基礎結構，請向 VMware Cloud Director 登錄 NSX-T Cloud 執行個體。控制器可用作負載平衡服務的中央控制平面。登錄控制器後，可以直接從 VMware Cloud Director 進行管理。

由 NSX Advanced Load Balancer 提供的負載平衡計算基礎結構將組織整理到服務引擎群組中。在 VMware Cloud Director 中，可以將多個服務引擎群組指派給 NSX-T Data Center Edge 閘道。指派給單一 Edge 閘道的所有服務引擎群組皆使用相同的網路。

服務引擎群組具有您在建立時定義的一組獨特計算特性。

在**系統管理員**將服務引擎群組指派給 Edge 閘道後，**組織管理員**可以建立並設定在特定服務引擎群組中執行的虛擬服務。

登錄控制器執行個體

若要將 VMware Cloud Director 與 NSX Advanced Load Balancer 部署整合，請向 VMware Cloud Director 執行個體登錄控制器執行個體。

控制器執行個體可用作 NSX Advanced Load Balancer 提供的負載平衡服務的中央控制平面。

必要條件

向 NSX-T Data Center 執行個體安裝和設定 NSX Advanced Load Balancer。

如需如何使用 NSX-T 設定 NSX Advanced Load Balancer 的相關資訊，請參閱〈Avi 與 NSX-T 整合〉。

備註 用於向 NSX Advanced Load Balancer 登錄 NSX-T Manager 的 FQDN 或 IP 位址，必須與您用來向 VMware Cloud Director 登錄 NSX-T Data Center 之 NSX-T Manager 執行個體的 FQDN 或 IP 位址相符。

程序

1 從頂部導覽列的**資源**下，按一下**基礎結構資源**。

2 按一下 **NSX-ALB**，然後按一下**控制器**。

3 若要新增控制器，請按一下**新增**。

4 如果您使用的是多站台部署，請從下拉式功能表中選取要在其中登錄控制器的站台。

5 登錄控制器執行個體。

a 為控制器執行個體輸入有意義的名稱，並選擇性地輸入說明。

b 輸入控制器的 URL。

例如，`https://FQDN-or-IP-address`。

c 輸入控制器的使用者名稱和密碼。

d 按一下**儲存**。

結果

控制器執行個體在清單中顯示為已啟用。

後續步驟

登錄 NSX-T Cloud。

登錄 NSX-T Cloud

若要使用 NSX Advanced Load Balancer 提供的虛擬基礎結構，請向 VMware Cloud Director 登錄 NSX-T Cloud 執行個體。

NSX-T Cloud 是服務提供者層級的建構，由 NSX-T Manager 和 NSX-T Data Center 傳輸區域組成。

NSX-T Manager 提供系統視圖且屬於 NSX-T Data Center 的管理元件。NSX-T Data Center 傳輸區域決定了哪些主機和虛擬機器可以參與特定網路的使用。

如果多個傳輸區域由同一個 NSX-T Manager 管理，則單獨的 NSX-T Cloud 會封裝每對 NSX-T Manager 和 NSX-T Data Center 傳輸區域執行個體。

NSX-T Cloud 與 NSX-T Data Center 傳輸區域支援的網路集區之間存在一對一關聯性。

必要條件

登錄控制器執行個體。

程序

1 從頂部導覽列的**資源**下，按一下**基礎結構資源**。

2 按一下 **NSX-ALB**，然後按一下 **NSX-T Cloud**。

3 若要新增 NSX-T Cloud，請按一下**新增**。

4 從下拉式功能表中，選取要為其建立 NSX-T Cloud 的控制器執行個體。

5 為 NSX-T Cloud 輸入名稱，並選擇性地輸入說明。

6 從清單中選取可用的雲端。

7 若要匯入雲端，請按一下**新增**。

結果

匯入的雲端隨即顯示在可用 NSX-T Cloud 的清單中。

後續步驟

匯入服務引擎群組。

匯入服務引擎群組

若要向您的承租人提供虛擬服務管理功能，請將服務引擎群組匯入至 VMware Cloud Director 部署。

服務引擎群組是一個隔離網域，該網域還定義了大小、網路存取和容錯移轉等共用服務引擎內容。

服務引擎群組中的資源可用於不同的虛擬服務，具體取決於您的承租人需求。這些資源無法在不同的服務引擎群組之間共用。

您可以使用 NSX Advanced Load Balancer 管理和更新服務引擎群組。在 NSX Advanced Load Balancer 中更新服務引擎群組後，必須將其同步以在 VMware Cloud Director 使用者介面中更新其設定。

僅匯入的服務引擎群組可指派給 Edge 閘道。

若要匯入服務引擎群組，需將其與已向 VMware Cloud Director 執行個體登錄的 NSX-T Cloud 建立關聯。

必要條件

- 登錄控制器執行個體。
- 登錄 NSX-T Cloud。

程序

1 從頂部導覽列的**資源**下，按一下**基礎結構資源**。

2 按一下 **NSX-ALB**，然後按一下**服務引擎群組**。

3 若要匯入服務引擎群組，請按一下**新增**。

4 從下拉式功能表中，選取 NSX-T Cloud。

5 選取保留模型。

   - 若要將服務引擎群組指派給單一 Edge 閘道，請選取**專用**。
   - 若要在多個 Edge 閘道之間共用服務引擎群組，請選取**共用**。

6 為服務引擎群組輸入名稱，並選擇性地輸入說明。

7 選取服務引擎群組執行個體。

8 按一下**新增**。

後續步驟

在 Edge 閘道上啟用負載平衡，並將服務引擎群組指派給 Edge 閘道。請參閱在 NSX-T Data Center Edge 閘道上管理 NSX Advanced 負載平衡。

同步服務引擎群組

若要更新已匯入的服務引擎群組的設定，必須將其與 NSX Advanced Load Balancer 同步。

您可以使用 NSX Advanced Load Balancer 管理和更新服務引擎群組。在 NSX Advanced Load Balancer 中更新服務引擎群組後，必須將其同步以在 VMware Cloud Director 使用者介面中更新其設定。

同步服務引擎群組會更新群組高可用性模式的本機記錄，以及服務引擎群組支援的虛擬服務數目上限。

重要 同步服務引擎群組後，如果新的支援虛擬服務數目上限低於保留的虛擬服務數目，則此服務引擎群組會標記為過度配置。

如果服務引擎群組已過度配置，則建立新虛擬服務可能會失敗，即使您在其上建立虛擬服務的 Edge 閘道具有足夠的保留容量亦是如此。

若要避免建立虛擬服務失敗，則在您編輯服務引擎群組的設定時，請勿將受支援的虛擬服務數目上限縮減至初始保留的虛擬服務數目以下。

必要條件

匯入服務引擎群組.

程序

1 從頂部導覽列的**資源**下，按一下**基礎結構資源**。

2 選取 **NSX-ALB**，然後按一下**服務引擎群組**。

3 選取服務引擎群組，然後按一下**同步**。

結果

服務引擎群組的設定會隨即更新。

透過 VMware Cloud Director 端點和 Proxy 存取 vSphere 元件

可以使用 VMware Cloud Director 端點存取基礎 vSphere 環境。當端點連線至 Proxy 時，VMware Cloud Director 充當 HTTP Proxy 伺服器。

端點

VMware Cloud Director 端點是資料中心元件 (例如 vCenter Server 執行個體、ESXi 主機或 NSX Manager 執行個體) 的存取點。使用者可以使用其 VMware Cloud Director 帳戶登入代理元件或非代理元件的使用者介面或 API。

建立專用 vCenter Server 執行個體將同時為其建立預設端點。連結 vCenter Server 執行個體時，您也可以建立 Proxy。但是，依預設，預設端點不會連線至任何 Proxy。您必須編輯預設端點或建立新端點，才能將其連線至 Proxy。

您可以從專用 vCenter Server 執行個體的**端點**索引標籤建立、編輯和刪除端點。請參閱建立端點。

Proxy

VMware Cloud Director 提供的 Proxy 與 VMware Cloud Director 內的 Proxy 組態不同。與適用範圍為承租人的 VMware Cloud Director 提供的 Proxy 不同，VMware Cloud Director 內的 Proxy 組態位於提供者層級，並且沒有任何租用。

透過啟用和停用 VMware Cloud Director 提供的 Proxy，您可以透過該 Proxy 來允許和停止承租人存取。

可以在將 vCenter Server 執行個體連結至 VMware Cloud Director 時建立 Proxy，也可以稍後建立。如果在連結 vCenter Server 並啟用承租人存取時建立 Proxy，則必須手動將 Proxy 連線至預設端點。

如果 vCenter Server 執行個體使用外部 Platform Services Controller，則 VMware Cloud Director 也會為 Platform Services Controller 建立 Proxy。透過父系和子系 Proxy，您可以向承租人隱藏特定 Proxy，也可以透過其父系 Proxy 啟用和停用子系 Proxy 的群組。如需在將 vCenter Server 執行個體新增至 VMware Cloud Director 後建立 Proxy 的相關資訊，請參閱新增用於存取基礎 vCenter Server 資源的 Proxy。

您可以從**基礎結構資源**下的 **Proxy** 索引標籤中編輯、啟用、停用和刪除 Proxy。

備註 將 Proxy 新增至 vCenter Server 執行個體時，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。

若要檢視和管理憑證及憑證撤銷清單 (CRL)，請參閱管理 Proxy 憑證和 CRL。

建立端點

您可以建立可供管理員和承租人用來存取基礎 vSphere 環境的端點。

端點必須連結至專用 vCenter Server 執行個體，並且承租人可以從專用 vCenter Server 執行個體的**動作**功能表中看到這些端點。如果您在將 vCenter Server 執行個體新增至 VMware Cloud Director 時啟用承租人存取，VMware Cloud Director 會以 vCenter Server 執行個體 URL 作為目標 URL 來建立預設端點。如果建立其他端點，則可以變更預設端點。

端點可用作專用 vCenter Server 執行個體與 Proxy 之間的連結。端點可以連線至一個 Proxy，或者可能沒有 Proxy 連線。如果端點連線至 Proxy，則端點的目標為目標 URL，而不是已連線 Proxy 的使用者介面 URL。

必要條件

確認您要為其建立端點的 vCenter Server 執行個體已啟用承租人存取。請參閱啟用連結的 vCenter Server 的承租人存取。

程序

1 從頂部導覽列的**資源**下，按一下**基礎結構資源**。

2 在左面板中，選取 **vCenter Server 執行個體**。

3 選取 vCenter Server 執行個體。

4 在具有詳細 vCenter Server 資訊的頁面上，按一下**端點**索引標籤，然後按一下**新增**。

5 輸入端點的名稱和目標 URL。

6 (選擇性) 將此端點設為此 vCenter Server 執行個體的預設端點。

7 (選擇性) 建立與 Proxy 的連線。

8 按一下**儲存**。

後續步驟

- 編輯端點設定。
- 刪除端點。如果您想要刪除預設端點，則必須選取其他端點作為預設端點。

新增用於存取基礎 vCenter Server 資源的 Proxy

如果希望 VMware Cloud Director 充當 vCenter Server 執行個體及其元件的 HTTP Proxy 伺服器，則可以建立 Proxy。可以為專用 vCenter Server 執行個體和沒有設定用途的 vCenter Server 執行個體建立 Proxy。

如果您想要使用已擷取的憑證和指紋自動產生 vCenter Server Proxy，則可以從 **vCenter Server 執行個體**網格或 vCenter Server 詳細資料視圖中執行此操作。如果 vCenter Server 含外部 Platform Services Controller，則此選項還將為 SSO 端點建立 Proxy。

此程序說明如何為 vCenter Server 執行個體手動建立 Proxy，或為 ESXi 主機、外部 Platform Services Controller 執行個體或 NSX Manager 執行個體建立 Proxy。

程序

1 從頂部導覽列的**資源**下，按一下**基礎結構資源**。

2 在左面板中，選取 **vCenter Server 執行個體**。

3 選取 vCenter Server 執行個體。

4 在具有詳細 vCenter Server 資訊的頁面上，按一下 **Proxy** 索引標籤，然後按一下**新增**。

5 輸入 Proxy 的名稱。

6 根據 VMware Cloud Director 作為 Proxy 所用於的元件，選取 Proxy 的類型。

   建立 Proxy 後，便無法編輯此設定。

   您只能建立一個 vCenter Server Proxy。如果已有一個 vCenter Server Proxy 並且您想要建立新的 Proxy，則**類型**下拉式功能表中不包括 vCenter Server 選項。

   - 如果您想要建立 vCenter Server Proxy，請從**類型**下拉式功能表中選取 **vCenter**，然後繼續執行步驟 10。

- 如果您想要為 ESXi 主機、NSX Manager 或 SSO 建立 Proxy，請從下拉式功能表中進行選取，然後繼續執行步驟 7。

7 輸入新 Proxy 的名稱、目標主機和使用者介面 URL。

目標主機是要讓 VMware Cloud Director 做為 Proxy 的元件的主機名稱或 IP 位址。新 Proxy 的使用者介面 URL 是承租人開啟 Proxy 時，VMware Cloud Director 使用者介面將導向到的 URL。

8 如果您想讓 Proxy 對承租人可見，請開啟**承租人可見**選項。

9 (選擇性) 按一下**選取父系 Proxy**，然後從清單中選取 Proxy。

10 按一下**儲存**。

後續步驟

管理 Proxy 憑證和 CRL.

管理 Proxy 憑證和 CRL

您可以檢視、下載和上傳 Proxy 憑證及憑證撤銷清單 (CRL)。

必要條件

確認至少一個 vCenter Server 執行個體擁有 VMware Cloud Director 提供的 Proxy。請參閱透過 VMware Cloud Director 端點和 Proxy 存取 vSphere 元件。

程序

1 從頂部導覽列的**資源**下，按一下**基礎結構資源**。

2 在左面板中，按一下 **Proxy**，然後選取 Proxy。

3 按一下**管理憑證**。

4 上傳或下載憑證及 CRL。

5 按一下**儲存**。

新增雲端資源

雲端資源是其基礎 vSphere 資源的抽象層，可提供 VMware Cloud Director 虛擬機器及 vApp 適用的計算與記憶體資源，而且可以存取儲存與網路連線。

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

如需組織虛擬資料中心的相關資訊，請參閱第 6 章 管理組織虛擬資料中心。

如需組織虛擬資料中心網路的相關資訊，請參閱《VMware Cloud Director 租用戶入口網站指南》中的〈管理組織虛擬資料中心網路〉一章。

VMware Cloud Director 9.7 採用 SDDC 或專用 vCenter Server 執行個體做為封裝整個 vCenter Server 安裝的雲端資源。提供者可以建立和啟用專用 vCenter Server，將其發佈至承租人，為基礎 vSphere 環境的不同元件建立並啟用 Proxy。若要建立專用 vCenter Server 執行個體和 Proxy、將其發佈至承租人並進行管理，您可以使用 Service Provider Admin Portal 或 vCloud OpenAPI。請參閱第 9 章 管理專用 vCenter Server 執行個體 或 VMware Cloud Director 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 (VDC) 將 vCenter Server 資源集區的計算和記憶體資源與單一 vCenter Server 執行個體中的一或多個儲存區原則的儲存資源相結合。對於網路資源，提供者 VDC 可以使用 NSX Data Center for vSphere 或 NSX-T Data Center。

- 您可以透過使用 Service Provider Admin Portal 或 vCloud API，來建立和管理連結的 vCenter Server 執行個體及其相關聯的 NSX Manager 執行個體所支援的提供者 VDC。
- 您可以透過使用 Service Provider Admin Portal 或 vCloud API，來建立和管理連結的 vCenter Server 執行個體及 NSX-T Manager 執行個體所支援的提供者 VDC。

一般 VMware Cloud Director 系統包含多個設定為符合各種服務層級需求的提供者 VDC。每個提供者 VDC 都具有主要資源集區。您可以從支援的 vCenter Server 執行個體新增和移除非主要資源集區。您無法移除主要資源集區。

建立提供者虛擬資料中心

為了使 vSphere 計算、記憶體和儲存資源可用於 VMware Cloud Director，您可以建立提供者虛擬資料中心 (VDC)。

系統管理員必須先建立提供者 VDC 和耗用其資源的組織 VDC，組織才能開始部署虛擬機器或建立目錄。提供者 VDC 與其支援的組織 VDC 之間的關係是一項管理決策。此決策基於服務供應項目的範圍、vSphere 基礎結構的容量和地理分佈，以及類似的考量事項。由於提供者 VDC 限制可用於承租人的 vSphere 容量和服務，因此**系統管理員**通常會建立提供者 VDC，來提供依效能、容量和功能衡量的不同服務類別。然後，可以使用提供特定服務類別 (由支援提供者 VDC 的組態所定義) 的組織 VDC 佈建承租人。

建立提供者 VDC 之前，先考量好您打算提供給承租人的一組 vSphere 功能。其中某些功能可在提供者 VDC 的主要資源集區中實作。其他功能可能需要您根據專門設定的 vSphere 叢集建立其他資源集區並將其新增至 VDC (如將資源集區新增至提供者虛擬資料中心中所述) 才能實作。

在支援資源集區之叢集中的主機上安裝的 ESXi 版本範圍，決定了可供提供者 VDC 所支援組織 VDC 中部署的虛擬機器使用的客體作業系統和虛擬硬體版本集。

必要條件

- 以**系統管理員**身分登入 Service Provider Admin Portal。
- 確認在設定為使用自動 DRS 的叢集中建立了具有可用容量的目標主要資源集區。您只能針對一個提供者 VDC 使用資源集區。若要建立資源集區，您可以使用 vSphere Client。

如果您打算使用的資源集區屬於使用 vSphere High Availability (HA) 的叢集，請確認您熟悉 vSphere HA 計算插槽大小的方式。如需插槽大小及自訂 vSphere HA 行為的相關資訊，請參閱《vSphere 可用性》說明文件。

- 如果您想要在 VMware Cloud Director 中使用 vSphere with VMware Tanzu，請確認您具有已設定的主管叢集的 vCenter Server 7.0 或更新版本執行個體。請參閱 vSphere 說明文件中的《vSphere with Kubernetes 組態和管理》指南。
- 如果您將 NSX Data Center for vSphere 用於提供者 VDC 的網路資源：
  - 確認包含目標主要資源集區的 vCenter Server 執行個體已連結並擁有 NSX Data Center for vSphere 授權金鑰。
  - 在 NSX Manager 中設定 VXLAN 基礎結構。請參閱相關的《NSX 管理指南》。

    如果您要在此提供者 VDC 中使用自訂 VXLAN 網路集區 (而非預設 VXLAN 網路集區)，請立即建立該網路集區。請參閱建立 NSX Data Center for vSphere 傳輸區域支援的網路集區。
- 如果您將 NSX-T Data Center 用於提供者 VDC 的網路資源：
  - 新增 NSX-T Data Center 第 0 層閘道支援的外部網路
  - 建立 NSX-T Data Center 傳輸區域支援的網路集區

程序

1. 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。
2. 在左面板中，選取**提供者 VDC**。
3. 按一下**新增**。
4. 如果您有多站台 VMware Cloud Director 部署，請從**站台**下拉式功能表中，選取您要向其新增此提供者 VDC 執行個體的站台，然後按**下一步**。
5. 輸入提供者 VDC 的名稱，並選擇性地輸入說明。

   您可以使用這些文字方塊來指示可供此提供者 VDC 支援的組織 VDC 使用的 vSphere 功能，例如，**vSphere HA** 或**具有 IOPS 支援的儲存區原則**。
6. (選擇性) 若要在建立時停用提供者 VDC，請關閉**狀態**切換按鈕。

   您無法使用已停用 VDC 的計算和儲存資源來建立組織 VDC。
7. 按**下一步**。
8. 若要為提供者 VDC 提供資源集區，請選取 vCenter Server 執行個體，然後按**下一步**。

   本頁列出登錄至 VMware Cloud Director 的 vCenter Server 執行個體。按一下 vCenter Server 執行個體以顯示其可用的資源集區。

   如果您想要在 VMware Cloud Director 中使用 vSphere with VMware Tanzu，則必須選取具有已設定的主管叢集的 vCenter Server 7.0 或更新版本執行個體。

9 選取資源集區做為此提供者 VDC 的主要資源集區。

您可以針對一個提供者 VDC 使用一個資源集區。當您將資源集區新增至提供者 VDC 時，此資源集區及其父系鏈結將無法供其他提供者 VDC 選取。

如果您想要使用 vSphere with VMware Tanzu，請選取主管叢集。VMware Cloud Director 會在主管叢集支援的資源集區旁邊顯示 Kubernetes 圖示。

10 如果選取主管叢集支援的資源集區或叢集來建立與 Kubernetes 控制平面的信任關係，您必須信任 Kubernetes 控制平面憑證。

11 選取您想要提供者 VDC 支援的最高虛擬硬體版本，然後按**下一步**。

系統會確定支援資源集區的叢集中所有主機支援的最高虛擬硬體版本，並將其做為**支援的硬體最高版本**下拉式功能表中的預設值提供。您可以使用此預設值，也可以從功能表中選取較低的硬體版本。您指定的版本將成為最高虛擬硬體版本，可用於此提供者 VDC 支援的組織 VDC 中部署的虛擬機器。如果選取較低的虛擬硬體版本，則這些虛擬機器可能不支援使用部分客體作業系統。使用所選的硬體版本建立提供者 VDC 後，您只能將版本升級而無法降級。

備註 提供者 VDC 的可用硬體版本取決於目標叢集中 ESXi 主機的最高可用版本。如果無法選取 ESXi 主機支援的最高硬體版本，請在 vSphere Client 中確認在資料中心建立虛擬機器的預設相容性設定為**使用資料中心設定和主機版本**。也可以將預設相容性設定設定為叢集所需的最高硬體版本。

VMware Cloud Director 9.7 及更新版本支援支援 vSphere 基礎結構所支援的最高硬體版本。從 VMware Cloud Director 10.2.2 開始，您可以設定硬體版本，而無需在 vCenter Server 執行個體中手動設定預設硬體版本。

12 選取提供者 VDC 的一或多個儲存區原則，然後按**下一步**。

會列出您選取的由資源集區支援的所有 vSphere 儲存區原則。

13 針對此提供者 VDC 設定網路集區。

每個提供者 VDC 必須具有一個網路集區。可讓系統為您建立一個具有預設範圍的網路集區，也可以使用基於特定 NSX Data Center for vSphere 的自訂 VXLAN 或基於 NSX-T Data Center 傳輸區域的 Geneve 集區。

備註 如果您想要在 VMware Cloud Director 中使用 vSphere with VMware Tanzu，則必須選取 **NSX-T Manager 和 Geneve 網路集區**選項。

選項	描述
建立預設 VXLAN 網路集區	系統會為此提供者 VDC 建立 VXLAN 集區。
從清單中選取 VXLAN 網路集區	您可以從清單中選取網路集區，以便根據特定的 NSX 傳輸區域使用自訂 VXLAN 集區。
選取 NSX-T Manager 和 Geneve 網路集區	您可以從清單中選取網路集區，以便使用 NSX-T Data Center 傳輸區域支援的自訂 VXLAN 集區。

14 檢閱您選擇的內容，然後按一下**完成**建立提供者 VDC。

後續步驟

您可以新增次要資源集區，讓提供者 VDC 提供某些組織可能需要的專用功能，例如 Edge 叢集、相似性群組以及具有特殊組態的主機。請參閱將資源集區新增至提供者虛擬資料中心。

外部網路

VMware Cloud Director 外部網路會提供可將系統中的網路和虛擬機器連線至系統外的網路的上行介面，例如 VPN、公司內部網路或公用網際網路。只有**系統管理員**可以建立外部網路。

如果有多個 vCenter Server 執行個體登錄到系統，您可以建立多個外部網路，每個網路皆由 vSphere 網路或第 0 層邏輯路由器支援。

VMware Cloud Director 支援 IPv4 和 IPv6 外部網路。

備註 建立外部網路時定義的 IP 位址範圍會配置給 Edge 閘道或直接連線到此網路的虛擬機器。因此，這些 IP 位址不得在 VMware Cloud Director 之外使用。

由 vSphere 網路支援的外部網路

外部網路可由單一 vSphere 網路或多個 vSphere 網路支援。

- 由單一 vSphere 執行個體支援的外部網路。

  若要在 vSphere 網路上為外部網路的每個取用者提供一組非重疊 IP 位址，**系統管理員**必須手動設定基礎 VLAN 上的 IP 範圍。

- 由多個 vSphere 網路支援的外部網路。

  外部網路可由多個 vSphere 網路支援。此方法可簡化 VMware Cloud Director 中的 IP 位址管理。您可以修改外部網路的內容，以變更其網路支援。

  由多個 vSphere 網路支援的外部網路具有多個限制。

  - 網路在登錄到系統的每個 VMware Cloud Director 執行個體上最多可以有一個支援 vSphere 網路。
  - 所有支援網路交換器都必須為同一類型，同為 vSphere Distributed Switch 或標準交換器。

由第 0 層邏輯路由器支援的外部網路

外部網路可由 NSX-T Data Center 第 0 層邏輯路由器支援。

此外，還可以在 NSX-T Data Center 中建立由 VRF-Lite 第 0 層閘道支援的外部網路。

虛擬路由和轉送 (VRF) 閘道是從父系第 0 層閘道建立的。它具有自己的路由表。

多個 VRF 閘道可以同時存在於同一個第 0 層閘道內。因此，透過建立 VRF 支援的外部網路，您可以在 NSX-T Data Center 中擴充第 0 層閘道，以建立 VDC 中的完全路由網路拓撲。

如需 VRF 閘道的相關資訊，請參閱 NSX-T Data Center 管理指南。

新增由 vSphere 資源支援的外部網路

透過新增外部網路，您可以登錄供 VMware Cloud Director 使用的 vSphere 網路資源。您可以建立連線至外部網路的組織 vDC 網路。

您可以新增 IPv4 或 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。

必要條件

確認有一個 vSphere 連接埠群組可用，有無 VLAN 主幹連線均可。具有靜態連接埠繫結的彈性連接埠群組可確保獲得最佳效能。

程序

1. 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。
2. 在左窗格中，按一下**外部網路**，然後按一下**新增**。
3. 選取 **vSphere 資源**，然後選取要支援網路的連接埠群組類型，然後按**下一步**。
4. 輸入新外部網路的名稱，並選擇性地輸入說明。
5. 選取要支援外部網路的連接埠群組，然後按**下一步**。
6. 設定至少一個子網路，然後按**下一步**。
   a. 若要新增子網路，請按一下**新增**。
   b. 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**。
   c. (選擇性) 輸入 DNS 設定。
   d. 透過新增至少一個 IP 範圍或 IP 位址，設定靜態 IP 集區。
   e. 按一下**確定**。
   f. (選擇性) 若要新增其他子網路，請重複此步驟。
7. 檢查網路設定，然後按一下**完成**。

後續步驟

您可以建立連線至外部網路的組織 VDC 網路。

新增 NSX-T Data Center 第 0 層閘道支援的外部網路

若要登錄 NSX-T Data Center 網路資源以供 VMware Cloud Director 使用，請新增第 0 層閘道支援的外部網路。

必要條件

若要建立 NSX-T Data Center 第 0 層閘道支援的外部網路，您必須先建立第 0 層閘道。您可以在 NSX-T Manager 使用者介面中或透過使用 NSX Policy API 建立第 0 層閘道。

如果您想要在 NSX-T Data Center 中建立 VRF 閘道支援的外部網路，則還必須建立連結至第 0 層閘道的 VRF 閘道。

- 在 NSX-T Manager 使用者介面中建立第 0 層閘道。
  a 使用管理權限登入 NSX-T Manager 執行個體。
  b 依序按一下**網路**、**第 0 層閘道**，然後按一下**新增閘道 > 第 0 層**。
  c 輸入第 0 層路由器的名稱。
  d 選取高可用性模式。

  備註 依預設，會使用雙主動模式。在雙主動模式下，流量會在所有成員之間進行負載平衡。在主動-待命模式下，選擇的作用中成員將會處理流量。如果作用中成員失敗，則新成員會成為作用中成員。

  e 從下拉式功能表中選取現有的 NSX-T Edge 叢集以支援此第 0 層邏輯路由器，然後按一下**儲存**。
- 如果您想要在 NSX-T Data Center 中建立 VRF 閘道支援的外部網路，請建立連結至第 0 層閘道的 VRF 閘道。
  a 使用管理權限登入 NSX-T Manager 執行個體。
  b 依序按一下**網路**、**第 0 層閘道**，然後按一下**新增閘道 > VRF**。
  c 輸入 VRF 閘道的名稱。
  d 選取要將 VRF 閘道連線到的第 0 層閘道。
  e 按一下**儲存**。

程序

1 登入 VMware Cloud Director Service Provider Admin Portal。
2 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。
3 在左窗格中，按一下**外部網路**，然後按一下**新增**。
4 選取要在其中登錄新外部網路的站台，然後按**下一步**。
5 在**支援類型**頁面上，選取 **NSX-T 資源 (第 0 層路由器)**，選取已登錄的 NSX-T Manager 以支援網路，然後按**下一步**。
6 輸入新外部網路的名稱，並選擇性地輸入說明。
7 選取第 0 層閘道或 VRF 閘道以連線至外部網路，然後按**下一步**。
8 設定至少一個子網路，然後按**下一步**。
  a 若要新增子網路，請按一下**新增**。
  b 輸入網路的無類別網域間路由 (CIDR) 設定。
  c (選擇性) 輸入 DNS 設定。
  d 透過新增至少一個 IP 範圍或 IP 位址，設定靜態 IP 集區。

e 按一下**確定**。

f (選擇性) 若要新增其他子網路，請重複步驟 8.a 至 8.e。

9 檢查網路設定，然後按一下**完成**。

後續步驟

使用第 0 層閘道建立外部網路的上行。

網路集區

網路集區是在組織 VDC 內使用的非差異網路群組，可以建立 vApp 網路與特定類型的組織 VDC 網路。

網路集區受 vSphere 網路資源 (例如 VLAN 識別碼或連接埠群組)、NSX Data Center for vSphere 資源或 NSX-T Data Center 資源支援。

VMware Cloud Director 使用網路集區建立 NAT 路由網路和內部組織 VDC 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。

每個位於 VMware Cloud Director 內的組織 VDC 可以擁有一個網路集區。多個組織 VDC 可共用一個網路集區。組織 vDC 的網路集區可提供已建立網路以滿足組織 vDC 的網路配額。

VXLAN 網路集區

由 NSX Data Center for vSphere 支援的每個提供者 VDC 都包含 VXLAN 網路集區。

當您建立由 NSX Data Center for vSphere 支援的提供者 VDC 時，您可以將該提供者 VDC 與現有 VXLAN 網路集區相關聯，也可以為提供者 VDC 建立 VXLAN 網路集區。

新建立的 VXLAN 網路集區的名稱衍生自包含的提供者 VDC 的名稱，在建立時會將此名稱連結至集區。您無法刪除或修改此網路集區。如果您重新命名提供者 VDC，就會自動重新命名其 VXLAN 網路集區。

備註 若要確保整個基礎結構中的最佳網路效能，請建立一個 VXLAN 網路集區，並在建立所有提供者 VDC 時將其與此集區相關聯。

VMware Cloud Director VXLAN 網路基於 IETF VXLAN 標準，具有多項優點。

- 跨越第 3 層界限的邏輯網路
- 跨越單一第 2 層上多個機架的邏輯網路
- 廣播內含項目
- 更高效能
- 更大規模 (高達 1 千 6 百萬個網路位址)

如需有關 VMware Cloud Director 環境中 VXLAN 網路的詳細資訊，請參閱《NSX 管理指南》。

建立 NSX Data Center for vSphere 傳輸區域支援的網路集區

若要登錄 NSX Data Center for vSphere 傳輸區域以供 VMware Cloud Director 使用，請新增 VXLAN 支援的網路集區。

必要條件

在登錄至 VMware Cloud Director 的任何 vCenter Server 上建立 NSX Data Center for vSphere 傳輸區域。請參閱《NSX 管理指南》。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，選取**網路集區**，然後按一下**新增**。

3 輸入新網路集區的名稱，並選擇性地輸入說明，然後按**下一步**。

4 選取 **VXLAN 支援**，然後按**下一步**。

5 選取 vCenter Server 執行個體以指定此網路集區要使用的 VXLAN 傳輸區域，然後按**下一步**。

6 選取 NSX Data Center for vSphere 傳輸區域以支援新的網路集區，然後按**下一步**。

備註 若要建立跨虛擬資料中心網路的通用網路集區，請選取 UNIVERSAL_VXLAN 類型傳輸區域。

7 檢查網路集區設定，然後按一下**完成**。

後續步驟

建立網路集區支援的組織 VDC 網路，也可以先建立網路集區與組織 VDC 的關聯性，再建立 vApp 網路。

Geneve 網路集區

由 NSX-T Data Center 支援的每個提供者 VDC 都包含 Geneve 網路集區。

Geneve 是在 NSX-T Data Center 中提供覆疊功能的網路虛擬化標準。

當您建立由 NSX-T Data Center 支援的提供者 VDC 時，您可以將該提供者 VDC 與現有 Geneve 網路集區相關聯，也可以為提供者 VDC 建立 Geneve 網路集區。

備註 VMware Cloud Director 不支援 VLAN 傳輸區域支援的 NSX-T Data Center 網路集區。

VMware Cloud Director Geneve 網路具有多項優點。

- 跨越第 3 層界限的邏輯網路
- 跨越單一第 2 層上多個機架的邏輯網路
- 廣播內含項目
- 更高效能
- 更大規模 (高達 1 千 6 百萬個網路位址)

建立 NSX-T Data Center 傳輸區域支援的網路集區

若要登錄 NSX-T Data Center 傳輸區域以供 VMware Cloud Director 使用，您可以建立 Geneve 支援的網路集區。

必要條件

建立支援覆疊的 NSX-T Data Center 傳輸區域。

備註 VMware Cloud Director 不支援 VLAN 傳輸區域支援的 NSX-T Data Center 網路集區。

如需有關傳輸區域建立和通用網路虛擬化封裝 (稱為 Geneve 覆疊) 的詳細資訊，請參閱 NSX-T Data Center 產品說明文件。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，選取**網路集區**，然後按一下**新增**。

3 輸入新網路集區的名稱，並選擇性地輸入說明，然後按**下一步**。

4 選取 **Geneve 支援**，然後按**下一步**。

5 選取 NSX-T Manager 執行個體以為此網路集區提供傳輸區域，然後按**下一步**。

6 選取 NSX-T 傳輸區域，然後按**下一步**。

7 檢查網路集區設定，然後按一下**完成**。

後續步驟

建立網路集區支援的組織 VDC 網路，也可以先建立網路集區與組織 VDC 的關聯性，再建立 vApp 網路。

建立 VLAN 識別碼支援的網路集區

若要登錄 vSphere VLAN 識別碼以供 VMware Cloud Director 使用，請新增 VLAN 支援的網路集區。VLAN 支援的網路集區可為組織 VDC 網路提供安全性、擴充性及效能。

必要條件

確認 vSphere 中有一系列可用的 VLAN 識別碼及 vSphere Distributed Switch。VLAN 識別碼必須是在連線 ESXi 伺服器之實體交換器中設定的有效識別碼。

注意 至少必須在第 2 層層級隔離 VLAN。若未正確隔離 VLAN，可能會導致網路中斷。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，選取**網路集區**，然後按一下**新增**。

3 輸入新網路集區的名稱，並選擇性地輸入說明，然後按**下一步**。

4 選取 **VLAN 支援**，然後按**下一步**。

5 選取 vCenter Server 執行個體以指定此網路集區要使用的分散式虛擬交換器，然後按**下一步**。

6 輸入 VLAN 識別碼範圍，然後按**下一步**。

7 針對網路集區選取分散式交換器，然後按**下一步**。

8 檢查網路集區設定，然後按一下**完成**。

後續步驟

建立網路集區支援的組織 VDC 網路，也可以先建立網路集區與組織 VDC 的關聯性，再建立 vApp 網路。

建立 vSphere 連接埠群組支援的網路集區

若要登錄 vSphere 連接埠群組以供 VMware Cloud Director 使用，請新增連接埠群組支援的網路集區。不同於其他類型的網路集區，連接埠群組支援的網路集區並不需要 vSphere Distributed Switch，並且可支援與第三方分散式交換器相關聯的連接埠群組。

注意 **連接埠群組必須與第 2 層的所有其他連接埠群組隔離。必須實體隔離或使用 VLAN 標記隔離連接埠群組。若未正確隔離連接埠群組，可能會導致網路中斷。**

必要條件

確認 vSphere 環境中有一或多個可用的連接埠群組。叢集中的每個 ESXi 主機都必須能夠使用這些連接埠群組，而且每個連接埠群組只能使用一個 VLAN。支援具有或不具有 VLAN 主幹連線的連接埠群組。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，選取**網路集區**，然後按一下**新增**。

3 輸入新網路集區的名稱，並選擇性地輸入說明，然後按**下一步**。

4 選取**連接埠群組支援**，然後按**下一步**。

5 選取 vCenter Server 執行個體以提供此網路集區要使用的連接埠群組，然後按**下一步**。

6 選取一或多個連接埠群組，然後按**下一步**。

您可以為每個連接埠群組建立一個網路。

7 檢查網路集區設定，然後按一下**完成**。

後續步驟

建立網路集區支援的組織 VDC 網路，也可以先建立網路集區與組織 VDC 的關聯性，再建立 vApp 網路。

檢視 vCenter Server 執行個體

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

程序

1 從頂部導覽列的**資源**下，按一下**基礎結構資源**。

2 在左面板中，選取 **vCenter Server 執行個體**。

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	VMware Cloud Director 中的 vCenter Server 執行個體的名稱。
狀態	vCenter Server 狀態可以是正常、警告和嚴重。
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 VMware Cloud 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。
使用量	專用 vCenter Server 執行個體已啟用承租人存取權。提供者可以跨多個提供者 VDC 使用共用 vCenter Server 執行個體的不同資源集區，然後將這些資源集區配置給不同的承租人。請參閱第 9 章 管理專用 vCenter Server 執行個體 。
叢集健全狀況	vCenter Server 執行個體中所有叢集的健全狀況彙總。彙總叢集的健全狀況時，會顯示最不健全的叢集的健全狀況。
叢集	vCenter Server 執行個體中的叢集數目。
虛擬機器	vCenter Server 執行個體中的虛擬機器數目。
執行中虛擬機器	vCenter Server 執行個體中正在執行的虛擬機器數目。
CPU	正在使用的虛擬 CPU 數量佔可用 vCenter Server CPU 總數量的百分比。
記憶體	正在使用的虛擬記憶體數量佔可用 vCenter Server 記憶體總數量的百分比。
儲存區	正在使用的虛擬儲存區數量佔可用 vCenter Server 儲存區總數量的百分比。

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 VMware Cloud Director 中的名稱和說明或其計算提供者範圍，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 從頂部導覽列的**資源**下，按一下**基礎結構資源**。

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

3 在 **vCenter Server 資訊**區段的右上角，按一下**編輯**。

4 (選擇性) 編輯執行個體名稱和說明。

5 (選擇性) 編輯 vCenter Server 的計算提供者範圍。

計算提供者範圍表示計算容錯網域，或對承租人可見以及工作負載所在的可用性區域。依預設，提供者虛擬資料中心的計算提供者範圍繼承自支援 vCenter Server 執行個體。您可以區分由單一 vCenter Server 執行個體支援之不同提供者 VDC 的計算提供者範圍。例如，您可以為 vCenter Server 設定 **Germany** 計算提供者範圍，並且可以為提供者 VDC 設定 **Munich** 範圍。

6 (選擇性) 編輯 vCenter Server 執行個體的 URL。

7 (選擇性) 編輯 vCenter Server **管理員**帳戶的使用者名稱和密碼。

8 (選擇性) 開啟或關閉**已啟用**切換按鈕。

9 (選擇性) 設定 vCenter Server Web 用戶端的 URL。

10 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 VMware Cloud Director 中的虛擬資料中心，您必須啟用 vCenter Server 執行個體。

程序

1 從頂部導覽列的**資源**下，按一下**基礎結構資源**。

2 在左面板中，選取 **vCenter Server 執行個體**。

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 從頂部導覽列的**資源**下，按一下**基礎結構資源**。

2 在左面板中，選取 **vCenter Server 執行個體**。

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 VMware Cloud 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。

從 VMware Cloud Director 10.2.2 開始，如果您使用的是 Kubernetes，則重新整理 vCenter Server 執行個體時，會導致還原預設防火牆原則及 NAT 規則，從而封鎖從組織虛擬資料中心外部的網路存取 Tanzu Kubernetes 叢集。

程序

1 從頂部導覽列的**資源**下，按一下**基礎結構資源**。

2 在左面板中，選取 **vCenter Server 執行個體**。

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 VMware Cloud 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 從頂部導覽列的**資源**下，按一下**基礎結構資源**。

2 在左面板中，選取 **vCenter Server 執行個體**。

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 VMware Cloud 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 從頂部導覽列的**資源**下，按一下**基礎結構資源**。

2 在左面板中，選取 **vCenter Server 執行個體**。

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 VMware Cloud 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 從頂部導覽列的**資源**下，按一下**基礎結構資源**。

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 修改 NSX Manager 主機名稱和管理員認證，然後按一下**儲存**。

5 (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，請開啟切換按鈕，並輸入控制虛擬機器內容和網路提供者範圍的名稱。

控制虛擬機器內容用於在 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。

參數	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《VMware Cloud Director 租用戶入口網站指南》。

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 VMware Cloud 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 從頂部導覽列的**資源**下，按一下**基礎結構資源**。

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 VMware Cloud 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 從頂部導覽列的**資源**下，按一下**基礎結構資源**。

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。

設定和管理多站台部署

若要將多個分散在不同地理位置的 VMware Cloud Director 安裝或伺服器群組及其組織作為單一實體進行管理和監控，服務提供者和承租人可以使用 VMware Cloud Director 多站台功能。

有效的多站台實作

關聯兩個 VMware Cloud Director 站台時，可以將這些站台作為單一實體進行管理。您也可以將這些站台上的組織相互關聯。如果組織是關聯的成員，儘管每個成員組織及其資產在其佔用站台的本機上，組織使用者也可以使用 VMware Cloud Director Tenant Portal 存取任何成員站台中的組織資產。

備註 若要關聯站台，則必須使用 VMware Cloud Director API。這些站台必須使用相同的 VMware Cloud Director API 版本，或相隔一個主要版本。例如，可以將 VMware Cloud Director 10.1 (API 版本 34.0) 站台與 VMware Cloud Director 站台版本 10.0、10.1、10.2 或 10.2.2 (分別是 API 版本 33.0、34.0、35.0 或 35.2) 相關聯。

將兩個站台關聯之後，您可以使用 VMware Cloud Director API 或 VMware Cloud Director Tenant Portal 來關聯佔用這些站台的組織。請參閱 VMware Cloud Director API 程式設計指南或《VMware Cloud Director 租用戶入口網站指南》中的設定和管理多站台部署主題。

站台或組織可以形成數目不限的對等關聯，但是每個關聯只包括兩個成員。每個站台或組織必須擁有其自己的私密金鑰。關聯成員透過在成員之間交換用於驗證已簽署要求的公開金鑰來建立信任關係。

關聯中的每個站台由 VMware Cloud Director 伺服器群組 (一組共用 VMware Cloud Director 資料庫的伺服器) 的範圍定義。關聯中的每個組織佔用單一站台。組織管理員控制組織使用者和群組對每個成員站台上資產的存取權。

站台物件和站台關聯

安裝或升級程序會建立代表本機 VMware Cloud Director 伺服器群組的 `Site` 物件。授權機構擴充至多個 VMware Cloud Director 伺服器群組的系統管理員可以將這些伺服器群組設定為 VMware Cloud Director 站台的關聯。

組織的關聯

完成站台關聯後，任何成員站台上的**組織管理員**即可開始關聯其組織。

備註 您無法將 `System` 組織與承租人組織相關聯。任何站台中的 `System` 組織只能與其他站台中的 `System` 組織相關聯。

使用者和群組身分識別

站台和組織的關聯必須同意使用相同的身分識別提供者 (IDP)。關聯中所有組織的使用者和群組身分識別必須透過此 IDP 來管理。

除系統組織 (必須使用 VMware Cloud Director 整合的 IDP) 以外，關聯可自由選擇最適合的 IDP。

用於組織使用者和群組的站台存取控制

組織管理員可以設定其 IDP 以產生使用者或群組存取 Token (在所有成員站台上有效或僅在部分成員站台上有效)。儘管使用者和群組身分識別在所有成員組織中必須相同，但使用者和群組權限仍受各成員組織中為這些使用者和群組所指派的角色限制。和所建立的任何自訂角色一樣，為使用者和群組指派的角色限於成員組織本身。

負載平衡器需求

若要有效實作多站台部署，您必須設定負載平衡器，負載平衡器會將送達機構端點 (例如 `https://vcloud.example.com`) 的要求散佈到站台關聯的每個成員的端點 (例如，`https://us.vcloud.example.com` 和 `https://uk.vcloud.example.com`)。如果站台有多個儲存格，則還必須設定負載平衡器，以在其所有儲存格中散佈傳入要求，讓 `https://cell1.us.vcloud.example.com`、`https://cell2.us.vcloud.example.com` 等能夠處理對 `https://us.vcloud.example.com` 的要求。

備註 全域負載平衡器 (在此案例中為 `https://vcloud.example.com`) 只能用於使用者介面存取。如果您自行開發使用 REST API 的指令碼或程式，則這些呼叫必須針對某個特定的站台。

網路連線需求

如果您要使用多站台功能，則每個站台上的每個儲存格必須能夠向所有站台的 REST API 端點提出 REST API 要求。如果使用「負載平衡器需求」部分中的範例，則 `cell1.us.vcloud.example.com` 和 `cell2.us.vcloud.example.com` 必須能夠連線到 `uk.example.com` 的 REST API 端點。對於 `uk.example.com` 下的所有儲存格，反之亦然。這意味著，儲存格還必須能夠對自己的 REST API 端點進行 REST API 呼叫，以便 `cell1.us.vcloud.example.com` 必須能夠對 `https://us.vcloud.example.com` 進行 REST API 呼叫。

若要進行 REST API 扇出，則必須向所有站台的 REST API 端點提出 REST API 要求。例如，如果使用者介面或 API 用戶端提出多站台要求以從所有站台取得組織頁面，並且 `cell1.us.vcloud.example.com` 處理該要求。儲存格 `cell1` 必須進行 REST API 呼叫，以使用針對該站台設定的 REST API 端點從每個站台取得組織頁面。當所有站台傳回其組織頁面時，`cell1` 會將結果自動分頁並傳回包含所有其他站台中資料的單一結果頁面。

站台和憑證

當某個站台與其他站台相關聯時，如果要更新其憑證，可能必須讓其他站台瞭解變更。如果沒有讓其他站台瞭解憑證變更，則多站台扇出可能會受到影響。

如果您要將站台上的憑證取代為有效且妥善簽署的憑證，則無需通知其他站台。由於憑證有效且經過妥善簽署，因此其他站台中的儲存格可以繼續以安全的方式進行連線而不會中斷。

如果您要將站台上的憑證取代為自我簽署憑證，或者憑證存在其他問題，導致無法自動信任，則其他站台需要瞭解情況。例如，如果憑證到期，您必須讓其他站台瞭解此情況。在每一個其他站台中，必須將憑證上傳至 Service Provider Admin Portal 中的**受信任的憑證**。請參閱匯入受信任的憑證。匯入憑證時，已上傳憑證的站台可以信任取得新憑證的站台。

備註 在遠端站台中安裝這些憑證之前，可以將這些憑證匯入其他站台的 [受信任的憑證] 中。這可確保通訊不會中斷，因為舊憑證和新憑證均位於 [受信任的憑證] 集區中。您不必重新關聯站台。

關聯成員狀態

建立站台或組織的關聯後，本機系統會定期擷取每個遠端關聯成員的狀態，並更新本機站台之 VMware Cloud Director 資料庫中的狀態。成員狀態會顯示在 `SiteAssociationMember` 或 `OrgAssociationMember` 的 `Status` 元素中。此元素的值可以是下列三者之一：

ACTIVE

雙方已建立關聯，且與遠端通訊成功。

ASYMMETRIC

本機站台已建立關聯，但遠端站台尚未交換。

UNREACHABLE

雙方已建立關聯，但遠端站台目前在網路上無法連線。

成員狀態「活動訊號」程序會以多站台系統使用者 (VMware Cloud Director 安裝期間系統組織中建立的本機 VMware Cloud Director 使用者帳戶) 的身分執行。雖然此帳戶是系統組織的成員，但它沒有系統管理員權限。它只有單一權限 `Multisite: System Operations`，可讓其有權提出 VMware Cloud Director API 要求，以擷取站台關聯的遠端成員狀態。

多站台資源清單

如果您要在多個位置使用 VMware Cloud 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，VMware Cloud Director 引入了多站台資源清單。從 10.0 版開始，VMware Cloud Director 支援包含組織的多站台資源清單。

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、組織 VDC、組織 VDC 範本、提供者 VDC、雲端儲存格、Edge 閘道、外部網路、網路集區和虛擬機器大小調整原則支援多站台雲端資源清單。

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 Service Provider Admin Portal 或 vCloud API。如需使用 Service Provider Admin Portal 的相關資訊，請參閱建立提供者虛擬資料中心。如需使用 vCloud API 的相關資訊，請參閱 VMware Cloud Director 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 VDC 中資源的所有現有組織虛擬資料中心 (VDC)，您可以停用此提供者 VDC。無法建立使用已停用提供者 VDC 中資源的組織 VDC。

執行中 vApp 與開啟電源的虛擬機器會繼續在此提供者 VDC 支援的現有組織 VDC 中執行，但您無法建立或啟動其他 vApp 或虛擬機器。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，選取**提供者 VDC**。

3 按一下目標提供者 VDC 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 VMware Cloud 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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，選取**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 從頂部導覽列中，選取**資源**，然後按一下**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) 輸入提供者虛擬資料中心的計算提供者範圍。

計算提供者範圍表示計算容錯網域，或對承租人可見以及工作負載所在的可用性區域。依預設，提供者虛擬資料中心的計算提供者範圍繼承自支援 vCenter Server 執行個體。您可以區分由單一 vCenter Server 執行個體支援之不同提供者 VDC 的計算提供者範圍。例如，您可以為 vCenter Server 設定 **Germany** 計算提供者範圍，並且可以為提供者 VDC 設定 **Munich** 範圍。

6 (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。VMware Cloud Director 10.2 中支援的最高虛擬機器硬體版本為 17 版。當您在叢集或資料中心層級的 vCenter Server 執行個體中啟用硬體版本 17 時，此版本便可使用。

7 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 vCenter Server 資料中心。
- 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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，選取**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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，選取**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 VMware Cloud 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. 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。
2. 在左面板中，選取**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 VMware Cloud Director 物件使用的已佈建儲存區，包括： ■ VMware Cloud 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 Server	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. 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。
2. 在左面板中，選取**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。

將 Kubernetes 與 VMware Cloud Director 搭配使用

透過將 Kubernetes 與 VMware Cloud Director 搭配使用，您可以向承租人提供多承租人 Kubernetes 服務。

Container Service Extension

Kubernetes Container Clusters 是適用於 VMware Cloud Director 的 Container Service Extension 外掛程式。服務提供者和承租人必須使用 Kubernetes Container Clusters 外掛程式來建立 Kubernetes 叢集。從 VMware Cloud Director10.2 開始，無需手動下載該外掛程式並將其上傳至 VMware Cloud DirectorService Provider Admin Portal。依預設，該外掛程式在 VMware Cloud Director 中可用，但您必須將其發佈至承租人，他們才能夠建立 Kubernetes 叢集。

服務提供者和承租人必須使用 Container Service Extension 3.0 版來建立原生和 VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) 叢集。必須完成 Container Service Extension 3.0 伺服器設定，並將 Container Service Extension 原生放置原則發佈到一或多個組織 VDC。

VMware Cloud Director 中的 vSphere with VMware Tanzu

可以使用 VMware Cloud Director 中的 vSphere with VMware Tanzu 建立主管叢集支援的提供者虛擬資料中心 (VDC)。啟用了 vSphere with VMware Tanzu 的主機叢集稱為主管叢集。可以對資源的使用設定限制，並限制可用資源，包括每個組織、使用者或群組的 Kubernetes 叢集數目。如需詳細資訊，請參閱管理組織的資源耗用量配額。

若要使用 VMware Cloud Director 中的 vSphere with VMware Tanzu，您必須先在 vSphere 7.0 或更新版本的叢集上啟用 vSphere with VMware Tanzu 功能，並將該叢集設定為主管叢集。請參閱 vSphere 說明文件中的《vSphere with Kubernetes 組態和管理》指南。您要使用的 vCenter Server 執行個體可以同時擁有主機叢集和主管叢集。

若要建立 Tanzu Kubernetes 叢集，您必須將提供者 VDC Kubernetes 原則發佈到組織，並在建立期間套用組織 VDC Kubernetes 原則。原生和 TKGI 叢集不使用提供者和組織 VDC Kubernetes 原則。

Kubernetes 叢集類型

- 原生叢集 - Kubernetes Container Clusters 外掛程式使用原生 Kubernetes 執行階段管理叢集。這些叢集具有單一控制平面節點，且高可用性功能有所弱化，可提供的持續性磁碟區選擇較少，並且沒有網路自動化。但是，它們的成本可能較低。對於原生 Kubernetes 叢集部署，必須設定 Container Service Extension 伺服器。請參閱 Container Service Extension (CSE) 說明文件中的〈CSE 伺服器管理〉一章。
- Tanzu Kubernetes 叢集 - 您可以使用 vSphere with Tanzu 執行階段選項建立 vSphere with VMware Tanzu 管理的 Tanzu Kubernetes 叢集。此選項提供更多功能，但是成本較高。如需詳細資訊，請參閱 vSphere 說明文件中的《vSphere with Kubernetes 組態和管理》指南。

- TKGI 叢集 - VMware Tanzu Kubernetes Grid Integrated Edition 是一項專門為多雲端企業和服務提供者實作 Kubernetes 而建立的容器解決方案。其部分功能包括對 Kubernetes 叢集執行高可用性、自動調整、健全狀況檢查、自我修復和輪流升級。如需有關 TKGI 叢集的詳細資訊，請參閱 VMware Tanzu Kubernetes Grid Integrated Edition 說明文件。

建立 Tanzu Kubernetes 叢集的工作流程

1 將啟用了 vSphere with VMware Tanzu 功能的 vCenter Server 7.0 或更新版本執行個體新增至 VMware Cloud 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。

2 驗證每個主管叢集上的網路設定，使其能夠執行 Kubernetes 工作負載。

重要 `Ingress CIDRs` 和 `Services CIDR` 參數的 IP 位址範圍不得與 IP 位址 10.96.0.0/12 和 192.168.0.0/16 (這是 `services` 和 `pods` 參數的預設 vSphere 值) 重疊。請參閱《vSphere with Kubernetes 組態和管理》指南中的 Tanzu Kubernetes 叢集組態參數的資訊。

備註 從 VMware Cloud Director 10.2.2 開始，如果在初始設定後修改主管叢集的網路設定，則必須重新整理 vCenter Server 執行個體，以調整會封鎖從建立該叢集之組織虛擬資料中心的外部對 Tanzu Kubernetes 叢集進行存取的自動防火牆原則及 NAT 規則。

3 建立主管叢集支援的提供者 VDC。請參閱建立提供者虛擬資料中心。

或者，您可以將主管叢集新增至現有提供者 VDC。如果您的環境為 vSphere 6.7 或更早版本，還可以將環境升級至 7.0 版，並在現有叢集上啟用 vSphere with VMware Tanzu。

在列出所有提供者 VDC 的網格中，主管叢集支援的提供者 VDC 會在其名稱旁邊顯示 Kubernetes 圖示。

4 (選擇性) VMware Cloud Director 會自動為主管叢集支援的提供者 VDC 產生預設提供者 VDC Kubernetes 原則。您可以為 Tanzu Kubernetes 叢集建立其他提供者 VDC Kubernetes 原則。請參閱建立提供者 VDC Kubernetes 原則。

5 將提供者 VDC Kubernetes 原則發佈到組織 VDC (從**提供者 VDC** 索引標籤)，或新增組織 VDC Kubernetes 原則 (從**組織 VDC** 索引標籤)。

6 將 Kubernetes Container Clusters 外掛程式發佈到服務提供者。請參閱從組織發佈或解除發佈外掛程式。如果您想讓承租人能夠建立 Kubernetes 叢集，則必須將 Kubernetes Container Clusters 外掛程式發佈到這些組織。如需有關管理 VMware Cloud Director 外掛程式的詳細資訊，請參閱管理外掛程式。

7 如果要向承租人授與建立和管理 Tanzu Kubernetes 叢集的權限，則必須將 **vmware:tkgcluster 權利**權限服務包發佈到要使用叢集的任何組織。共用權限服務包後，您必須將**編輯：Tanzu Kubernetes 客體叢集**權限新增至要建立和修改 Tanzu Kubernetes 叢集的角色。如果還想讓使用者刪除叢集，則必須將**完全控制：Tanzu Kubernetes 客體叢集**權限新增至角色。此外，您可以將管理員權限指派給想要檢視組織中所有 Tanzu Kubernetes 叢集的使用者，或想要跨站台管理叢集的使用者。如需執行階段定義的實體 (RDE) 的權限和存取層級的相關資訊，請參閱第 14 章 管理定義的實體。

8 透過建立存取控制清單 (ACL) 項目向承租人或系統管理員授與存取權。如需有關共用執行階段定義的實體 (RDE) 的詳細資訊，請參閱共用定義的實體。

9 建立 Tanzu Kubernetes 叢集

建立原生和 TKGI 叢集的工作流程

1 將 Kubernetes Container Clusters 外掛程式發佈到服務提供者。請參閱從組織發佈或解除發佈外掛程式。如果您想讓承租人能夠建立 Kubernetes 叢集，則必須將 Kubernetes Container Clusters 外掛程式發佈到這些組織。如需有關管理 VMware Cloud Director 外掛程式的詳細資訊，請參閱管理外掛程式。

2 設定 Container Service Extension 伺服器，並將 Container Service Extension 原生放置原則或 TKGI 啟用中繼資料發佈至組織 VDC。如需有關設定 CSE 伺服器的詳細資訊，請參閱 Container Service Extension (CSE) 說明文件中的 CSE 伺服器管理一章。

3 如果要向承租人授與建立和管理原生叢集的權限，則必須將 **cse:nativeCluster 權利**權限服務包發佈到要使用原生叢集的任何組織。共用權限服務包後，您必須將**編輯 CSE:NATIVECLUSTER** 權限新增至要建立和修改原生叢集的角色。如果還想讓使用者刪除叢集，則必須將**完全控制 CSE:NATIVECLUSTER** 權限新增至角色。此外，您可以將管理員權限指派給想要檢視組織中所有 Tanzu Kubernetes 叢集的使用者，或想要跨站台管理叢集的使用者。如需執行階段定義的實體 (RDE) 的權限和存取層級的相關資訊，請參閱第 14 章 管理定義的實體。

4 如果要向承租人授與建立和管理 TKGI 叢集的權限，則必須將 **{cse}:PKS DEPLOY RIGHT** 發佈到特定組織，然後將 **{cse}:PKS DEPLOY RIGHT** 權限新增至要建立和管理 TKGI 叢集的角色。**{cse}:PKS DEPLOY RIGHT** 是在 Container Service Extension 伺服器安裝期間建立的。

5 對於原生叢集，透過建立存取控制清單 (ACL) 項目向承租人或系統管理員授與存取權。如需有關共用執行階段定義的實體 (RDE) 的詳細資訊，請參閱共用定義的實體。

6 建立原生 Kubernetes 叢集或建立 VMware Tanzu Kubernetes Grid Integrated Edition 叢集。

建立 vSphere with VMware Tanzu 叢集

您可以使用提供者 VDC 和組織 VDC Kubernetes 原則來建立 vSphere with VMware Tanzu 叢集。

VMware Cloud Director 中的 vSphere with VMware Tanzu

在 vSphere 叢集上啟用時，vSphere with VMware Tanzu 提供直接在 ESXi 主機上執行 Kubernetes 工作負載，以及在專用資源集區內建立上游 Kubernetes 叢集的功能。如需詳細資訊，請參閱 vSphere 說明文件中的《vSphere with Kubernetes 組態和管理》指南。

可以使用 VMware Cloud Director 中的 vSphere with VMware Tanzu 建立主管叢集支援的提供者虛擬資料中心 (VDC)。啟用了 vSphere with VMware Tanzu 的主機叢集稱為主管叢集。可以對資源的使用設定限制，並限制可用資源，包括每個組織、使用者或群組的 Kubernetes 叢集數目。如需詳細資訊，請參閱管理組織的資源耗用量配額。

若要使用 VMware Cloud Director 中的 vSphere with VMware Tanzu，您必須先在 vSphere 7.0 或更新版本的叢集上啟用 vSphere with VMware Tanzu 功能，並將該叢集設定為主管叢集。請參閱 vSphere 說明文件中的《vSphere with Kubernetes 組態和管理》指南。您要使用的 vCenter Server 執行個體可以同時擁有主機叢集和主管叢集。

承租人可透過套用其中一個組織 VDC Kubernetes 原則來建立 Tanzu Kubernetes 叢集。系統管理員可以使用 Service Provider Admin Portal 或 VMware Cloud Director Tenant Portal 來編輯和刪除組織 VDC Kubernetes 原則。原生和 TKGI 叢集不使用提供者和組織 VDC Kubernetes 原則。

VMware Cloud Director 使用已啟用的 PodSecurityPolicy 許可控制器佈建 Tanzu Kubernetes 叢集。您必須建立網繭安全性原則來部署工作負載。如需在 Kubernetes 中實現使用網繭安全性原則的相關資訊，請參閱《vSphere with Kubernetes 組態和管理》指南中的〈對 Tanzu Kubernetes 叢集使用網繭安全性原則〉主題。

工作流程

1 將啟用了 vSphere with VMware Tanzu 功能的 vCenter Server 7.0 或更新版本執行個體新增至 VMware Cloud 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。

2 建立主管叢集支援的提供者 VDC。請參閱建立提供者虛擬資料中心。

   或者，您可以將主管叢集新增至現有提供者 VDC。如果您的環境為 vSphere 6.7 或更早版本，還可以將環境升級至 7.0 版，並在現有叢集上啟用 vSphere with VMware Tanzu。

   在列出所有提供者 VDC 的網格中，主管叢集支援的提供者 VDC 會在其名稱旁邊顯示 Kubernetes 圖示。

3 (選擇性) VMware Cloud Director 會自動為主管叢集支援的提供者 VDC 產生預設提供者 VDC Kubernetes 原則。您可以為 Tanzu Kubernetes 叢集建立其他提供者 VDC Kubernetes 原則。請參閱建立提供者 VDC Kubernetes 原則。

4 將提供者 VDC Kubernetes 原則發佈到組織 VDC (從**提供者 VDC** 索引標籤)，或新增組織 VDC Kubernetes 原則 (從**組織 VDC** 索引標籤)。

5 將 Kubernetes Container Clusters 外掛程式發佈到服務提供者。請參閱從組織發佈或解除發佈外掛程式。如果您想讓承租人能夠建立 Kubernetes 叢集，則必須將 Kubernetes Container Clusters 外掛程式發佈到這些組織。如需有關管理 VMware Cloud Director 外掛程式的詳細資訊，請參閱管理外掛程式。

6 將 **vmware:tkgcluster 權利**權限服務包發佈到要使用 Tanzu Kubernetes 叢集的任何組織。

7 將**編輯：Tanzu Kubernetes 客體叢集**權限新增至要建立 Tanzu Kubernetes 叢集的角色。如果還想讓使用者刪除叢集，則必須將**完全控制：Tanzu Kubernetes 客體叢集**權限新增至角色。此外，您可以將管理員權限指派給想要檢視組織中所有 Tanzu Kubernetes 叢集的使用者，或想要跨站台管理叢集的使用者。如需執行階段定義的實體 (RDE) 的權限和存取層級的相關資訊，請參閱第 14 章 管理定義的實體。

8 透過建立存取控制清單 (ACL) 項目向承租人或系統管理員授與存取權。如需有關共用執行階段定義的實體 (RDE) 的詳細資訊，請參閱共用定義的實體。

9 建立 Tanzu Kubernetes 叢集

建立提供者 VDC Kubernetes 原則

VMware Cloud Director 會自動為主管叢集支援的提供者 VDC 自動產生預設提供者 VDC Kubernetes 原則。您可以為 Tanzu Kubernetes 叢集建立其他提供者 VDC Kubernetes 原則。

只有在您想要建立或啟用承租人以建立 Tanzu Kubernetes 叢集時，才需要提供者 VDC 和組織 VDC Kubernetes 原則。原生和 TKGI 叢集不會使用這些 Kubernetes 原則。

必要條件

確認您至少有一個提供者 VDC 受到主管叢集支援，或將主管叢集新增至現有提供者 VDC。請參閱將 Kubernetes 與 VMware Cloud Director 搭配使用。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，選取**提供者 VDC**，然後按一下提供者 VDC 的名稱。

3 在 [原則] 下，選取 **Kubernetes**，然後按一下**新增**。

建立 VDC Kubernetes 原則精靈隨即顯示。

4 輸入提供者 VDC Kubernetes 原則的名稱和說明，然後按**下一步**。

5 選取由具有 Kubernetes 功能的主管叢集所支援的資源集區。

6 選擇是否要為此原則中建立的 Kubernetes 叢集節點保留 CPU 和記憶體。

每個類別類型有兩個版本：保證版本和最佳運作版本。保證類別版本會完全保留其已設定的資源，而最佳運作版本則允許過度認可資源。視您的選擇而定，您可以在精靈的下一頁上選取保證版本或最佳運作版本的虛擬機器類別類型。

- 對於保證版本的虛擬機器類別類型，選取**是**以完整保留 CPU 和記憶體。
- 對於最佳運作版本的虛擬機器類別類型，選取**否**以便不保留 CPU 和記憶體。

7 針對在此原則下建立的 Kubernetes 叢集選取 CPU 和記憶體限制。

將原則發佈至組織 VDC 時，所選限制會用作新建立的組織 VDC Kubernetes 原則的上限。

8 按**下一步**。

9 在精靈的**機器類別**頁面上，選取一或多個適用於此原則的虛擬機器類別類型，然後按**下一步**。

選取的機器類別是您向組織 VDC 發佈原則時，承租人可用的唯一類別類型。

10 選取一或多個儲存區原則。

11 檢閱您的選擇，然後按一下**完成**。

後續步驟

將提供者 VDC Kubernetes 原則發佈到組織 VDC

編輯 vSphere Kubernetes 原則

您可以編輯用於建立組織 VDC Kubernetes 原則和 Tanzu Kubernetes 叢集的提供者 VDC Kubernetes 原則設定。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，選取**提供者 VDC**，然後按一下提供者 VDC 的名稱。

3 (選擇性) 在 [原則] 下，選取 **Kubernetes**，選取要發佈的原則，然後按一下**編輯**。

編輯 VDC Kubernetes 原則精靈隨即顯示。

4 (選擇性) 編輯提供者 VDC Kubernetes 原則的名稱和說明，然後按**下一步**。

5 (選擇性) 變更在此原則下建立的 Kubernetes 叢集的 CPU 和記憶體限制，然後按**下一步**。

將原則發佈至組織 VDC 時，所選限制會用作新建立的組織 VDC Kubernetes 原則的上限。

6 (選擇性) 在精靈的**機器類別**頁面上，新增一或多個適用於此原則的虛擬機器類別類型，然後按**下一步**。

選取的機器類別是您向組織 VDC 發佈原則時，承租人可用的唯一類別類型。

7 (選擇性) 新增一或多個儲存區原則。

8 檢閱您的選擇，然後按一下**儲存**。

後續步驟

將提供者 VDC Kubernetes 原則發佈到組織 VDC

將提供者 VDC Kubernetes 原則發佈到組織 VDC

若要使提供者 VDC Kubernetes 原則可供承租人使用，您可以將其發佈到 Flex 組織 VDC。發佈提供者 VDC Kubernetes 原則時，您可以建立可供承租人建立 Kubernetes 叢集的組織 VDC Kubernetes 原則。

將提供者 VDC Kubernetes 原則新增或發佈到組織 VDC 時，您可以將該原則提供給承租人使用。承租人可以使用可用的組織 VDC Kubernetes 原則，在建立 Kubernetes 叢集時利用 Kubernetes 容量。Kubernetes 原則將封裝放置、基礎結構品質，以及持續性磁碟區儲存區類別。Kubernetes 原則可以有不同的計算限制。

您可以將多個提供者 VDC Kubernetes 原則發佈到單一組織 VDC。您可以多次將單一提供者 VDC Kubernetes 原則發佈到組織 VDC。可以使用組織 VDC Kubernetes 原則作為服務品質的指標。例如，您可以發佈 Gold Kubernetes 原則以允許選取保證的機器類別和快速儲存區類別，或發佈 Silver Kubernetes 原則以允許選取最佳運作的機器類別和緩慢儲存區類別。

必要條件

- 建立主管叢集支援的提供者 VDC，或將主管叢集新增至現有提供者 VDC。請參閱將 Kubernetes 與 VMware Cloud Director 搭配使用。
- 確認您的環境中至少有一個 Flex 組織 VDC。請參閱建立組織虛擬資料中心。

- 自行熟悉 Tanzu Kubernetes 叢集的虛擬機器類別類型。請參閱 vSphere 說明文件中的《vSphere with Kubernetes 組態和管理》指南。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，選取**提供者 VDC**，然後按一下提供者 VDC 的名稱。

3 在 [原則] 下，選取 **Kubernetes**，選取要發佈的原則，然後按一下**發佈**。

發佈至組織 VDC 精靈隨即顯示。

4 輸入組織 VDC Kubernetes 原則的承租人可見名稱和說明，然後按**下一步**。

5 選取要將原則發佈到的 Flex 組織 VDC，然後按**下一步**。

6 針對在此原則下建立的 Kubernetes 叢集選取 CPU 和記憶體限制。

最大限制取決於組織 VDC 的 CPU 和記憶體配置。發佈原則時，所選限制將用作承租人的上限。

7 選擇是否要為此原則中建立的 Kubernetes 叢集節點保留 CPU 和記憶體，然後按**下一步**。

每個類別類型有兩個版本：保證版本和最佳運作版本。保證類別版本會完全保留其已設定的資源，而最佳運作版本則允許過度認可資源。視您的選擇而定，您可以在精靈的下一頁上選取保證版本或最佳運作版本的虛擬機器類別類型。

- 對於保證版本的虛擬機器類別類型，選取**是**以完整保留 CPU 和記憶體。
- 對於最佳運作版本的虛擬機器類別類型，選取**否**以便不保留 CPU 和記憶體。

8 在精靈的**機器類別**頁面上，選取一或多個適用於此原則的虛擬機器類別類型。

選取的機器類別是您向組織 VDC 發佈原則時，承租人可用的唯一類別類型。

9 選取一或多個儲存區原則。

10 檢閱您的選擇，然後按一下**發佈**。

結果

已發佈原則的相關資訊會顯示在 Flex 組織 VDC 的 [原則] 區段下。已發佈原則將使用原則中指定的資源限制在主管叢集上建立主管命名空間。

承租人可以開始使用 Kubernetes 原則來建立 Kubernetes 叢集。VMware Cloud Director 會將在此 Kubernetes 原則下建立的每個 Kubernetes 叢集放置在相同的主管命名空間中。原則資源限制將成為主管命名空間的資源限制。主管命名空間中所有承租人建立的 Kubernetes 叢集會在這些限制內爭用資源。

建立 Tanzu Kubernetes 叢集

可以使用 Kubernetes Container Clusters 外掛程式建立 Tanzu Kubernetes 叢集。

如需有關用於叢集建立的不同 Kubernetes 執行階段選項的詳細資訊，請參閱將 Kubernetes 與 VMware Cloud Director 搭配使用。

此外，還可以使用 Container Service Extension CLI 管理 Kubernetes 叢集。請參閱 Container Service Extension 說明文件。

VMware Cloud Director 使用已啟用的 PodSecurityPolicy 許可控制器佈建 Tanzu Kubernetes 叢集。您必須建立網繭安全性原則來部署工作負載。如需在 Kubernetes 中實現使用網繭安全性原則的相關資訊，請參閱《vSphere with Kubernetes 組態和管理》指南中的〈對 Tanzu Kubernetes 叢集使用網繭安全性原則〉主題。

必要條件

- 將 Kubernetes Container Clusters 外掛程式發佈到您想要管理 Tanzu Kubernetes 叢集的任何組織。
- 確認您的組織 VDC 中至少有一個組織 VDC Kubernetes 原則。若要新增組織 VDC Kubernetes 原則，請參閱新增組織 VDC Kubernetes 原則。
- 您必須將 **vmware:tkgcluster 權利**權限服務包發佈到要使用叢集的任何組織。共用權限服務包後，您必須將**編輯：Tanzu Kubernetes 客體叢集**權限新增至要建立和修改 Tanzu Kubernetes 叢集的角色。如果還想讓使用者刪除叢集，則必須將**完全控制：Tanzu Kubernetes 客體叢集**權限新增至角色。此外，您可以將管理員權限指派給想要檢視組織中所有 Tanzu Kubernetes 叢集的使用者，或想要跨站台管理叢集的使用者。如需執行階段定義的實體 (RDE) 的權限和存取層級的相關資訊，請參閱第 14 章 管理定義的實體。
- 透過建立存取控制清單 (ACL) 項目向承租人或系統管理員授與存取權。如需有關共用執行階段定義的實體 (RDE) 的詳細資訊，請參閱共用定義的實體。

程序

1. 從頂部導覽列中，選取**更多 > Kubernetes Container Clusters**。
2. (選擇性) 如果組織 VDC 已啟用 TKGI 叢集建立，請在 **Kubernetes Container Clusters** 頁面上，選取 **vSphere with Tanzu 與原生**索引標籤。
3. 按一下**新增**。
4. 選取 **vSphere with Tanzu** 執行階段選項，然後按**下一步**。
5. 輸入新 Kubernetes 叢集的名稱，然後按**下一步**。
6. 選取要將 Tanzu Kubernetes 叢集發佈到的組織 VDC，然後按**下一步**。
7. 選取組織 VDC Kubernetes 原則和 Kubernetes 版本，然後按**下一步**。

   VMware Cloud Director 會顯示未繫結到任何組織 VDC 或 Kubernetes 原則的預設 Kubernetes 版本集。這些版本是全域設定。若要變更可用版本的清單，請使用儲存格管理工具執行 `./cell-management-tool manage-config --name wcp.supported.kubernetes.versions -v` *`version_numbers`* 命令，以逗號分隔版本號碼。
8. 選取新叢集中的控制平面和 worker 節點數目。
9. 選取控制平面和 worker 節點的機器類別，然後按**下一步**。
10. 為控制平面和 worker 節點選取 Kubernetes 原則儲存區類別，然後按**下一步**。

11 (選擇性) 對於 VMware Cloud Director 10.2.2 及更新版本，指定 Kubernetes 服務的 IP 位址範圍和 Kubernetes 網繭的範圍，然後按**下一步**。

無類別網域間路由 (CIDR) 是一種 IP 路由和 IP 位址配置方法。

選項	描述
`Pods CIDR`	指定要用於 Kubernetes 網繭的 IP 位址範圍。預設值為 192.168.0.0/16。網繭子網路大小必須等於或大於 /24。此值不得與主管叢集設定重疊。您可以輸入一個 IP 範圍。
`Services CIDR`	指定要用於 Kubernetes 服務的 IP 位址範圍。預設值為 10.96.0.0/12。此值不得與主管叢集設定重疊。您可以輸入一個 IP 範圍。

12 檢閱叢集設定，然後按一下**完成**。

後續步驟

- 如果您想要變更 worker 節點的數目，請調整 Kubernetes 叢集的大小。
- 下載 kubeconfig 檔案。kubectl 命令列工具使用 kubeconfig 檔案來取得叢集、使用者、命名空間和驗證機制的相關資訊。
- 刪除 Kubernetes 叢集。

建立原生 Kubernetes 叢集

可以使用 Kubernetes Container Clusters 外掛程式建立 Container Service Extension 3.0 管理的 Kubernetes 叢集。

如需有關用於叢集建立的不同 Kubernetes 執行階段選項的詳細資訊，請參閱將 Kubernetes 與 VMware Cloud Director 搭配使用。

此外，還可以使用 Container Service Extension CLI 管理 Kubernetes 叢集。請參閱 Container Service Extension 說明文件。

必要條件

- 確認您的服務提供者已向您的組織發佈 Kubernetes Container Clusters 外掛程式。Kubernetes Container Clusters 是適用於 VMware Cloud Director 的 Container Service Extension 外掛程式。您可以在頂部導覽列上的**更多 > Kubernetes Container Clusters** 下找到此外掛程式。
- 若要針對原生 Kubernetes 叢集部署啟用組織 VDC，請設定 Container Service Extension 伺服器。請參閱 Container Service Extension (CSE) 說明文件中的 CSE 伺服器管理一章。
- 將在 CSE 伺服器設定期間建立的 CSE 原生原則發佈到組織 VDC。若要運用使用者介面，請參閱將虛擬機器放置原則新增至組織 VDC。或者，您可以使用 CSE 3.0 CLI 來發佈原則，方法是執行 `vcd cse ovdc enable Organization_VDC_Name --org Organization _Name --native` 命令。
- 您必須將 **cse:nativeCluster 權利**權限服務包發佈到要使用原生叢集的任何組織。共用權限服務包後，您必須將**編輯 CSE:NATIVECLUSTER** 權限新增至要建立和修改 Tanzu Kubernetes 叢集的角色。如

果還想讓使用者刪除叢集，則必須將**完全控制 CSE:NATIVECLUSTER** 權限新增至角色。此外，您可以將管理員權限指派給想要檢視組織中所有 Tanzu Kubernetes 叢集的使用者，或想要跨站台管理叢集的使用者。如需執行階段定義的實體 (RDE) 的權限和存取層級的相關資訊，請參閱第 14 章 管理定義的實體。

- 透過建立存取控制清單 (ACL) 項目向承租人或系統管理員授與存取權。如需有關共用執行階段定義的實體 (RDE) 的詳細資訊，請參閱共用定義的實體。

程序

1 從頂部導覽列中，選取**更多 > Kubernetes Container Clusters**。

2 (選擇性) 如果組織 VDC 已啟用 TKGI 叢集建立，請在 **Kubernetes Container Clusters** 頁面上，選取 **vSphere with Tanzu 與原生**索引標籤。

3 按一下**新增**。

4 選取**原生** Kubernetes 執行階段選項。

5 輸入名稱，然後從清單中選取 Kubernetes 範本。

6 (選擇性) 輸入新 Kubernetes 叢集的說明和 SSH 公開金鑰。

7 按**下一步**。

8 選取要將原生叢集發佈到的組織 VDC，然後按**下一步**。

9 為節點選取控制平面和 worker 節點的數目，並選擇性地選取大小調整原則。

10 按**下一步**。

11 如果您想要使用 NFS 軟體部署其他虛擬機器，請開啟**啟用 NFS** 切換按鈕。

12 (選擇性) 為控制平面和 worker 節點選取儲存區原則。

13 按**下一步**。

14 選取 Kubernetes 叢集的網路，然後按**下一步**。

15 檢閱叢集設定，然後按一下**完成**。

後續步驟

- 如果您想要變更 worker 節點的數目，請調整 Kubernetes 叢集的大小。
- 下載 kubeconfig 檔案。kubectl 命令列工具使用 kubeconfig 檔案來取得叢集、使用者、命名空間和驗證機制的相關資訊。
- 刪除 Kubernetes 叢集。

建立 VMware Tanzu Kubernetes Grid Integrated Edition 叢集

您可以使用 Container Service Extension 建立 VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) 叢集。

如需有關用於叢集建立的不同 Kubernetes 執行階段選項的詳細資訊，請參閱將 Kubernetes 與 VMware Cloud Director 搭配使用。

此外，還可以使用 Container Service Extension CLI 管理 Kubernetes 叢集。請參閱 Container Service Extension 說明文件。

透過使用 TKGI 啟用中繼資料，您可以提供對承租人的存取權，以建立 TKGI 叢集並存取已啟用 TKGI 的組織 VDC。如果您想要限制承租人建立 TKGI 叢集的能力，可以僅提供對組織 VDC 的存取權。在此情況下，承租人可以管理現有的 TKGI 叢集，但無法建立新叢集。

必要條件

- 確認您的服務提供者已向您的組織發佈 Kubernetes Container Clusters 外掛程式。Kubernetes Container Clusters 是適用於 VMware Cloud Director 的 Container Service Extension 外掛程式。您可以在頂部導覽列上的**更多 > Kubernetes Container Clusters** 下找到此外掛程式。
- 若要針對 TKGI Kubernetes 叢集部署啟用組織 VDC，請設定 Container Service Extension 伺服器。如需使用 CSE CLI 為 TKGI 啟用組織 VDC 的相關資訊，請參閱 Container Service Extension (CSE) 說明文件中的 CSE 伺服器管理一章。
- 如果您要向承租人提供 TKGI 建立和管理的權限，則必須將 **{cse}:PKS DEPLOY RIGHT** 發佈到特定組織，然後將 **{cse}:PKS DEPLOY RIGHT** 權限新增至要建立和管理 TKGI 叢集的角色。**{cse}:PKS DEPLOY RIGHT** 是在 Container Service Extension 伺服器安裝期間建立的。

程序

1. 從頂部導覽列中，選取**更多 > Kubernetes Container Clusters**。
2. 在 **Kubernetes Container Clusters** 頁面上，選取 **TKGI** 索引標籤，然後按一下**新增**。

   建立新 TKGI 叢集精靈隨即開啟。
3. 選取要將 TKGI 叢集發佈到的組織 VDC，然後按**下一步**。

   此清單可能需要較長時間才能載入，因為 VMware Cloud Director 會從 CSE 伺服器請求資訊。
4. 輸入新 TKGI 叢集的名稱，然後選取 worker 節點的數目。

   TKGI 叢集必須至少有一個 worker 節點。
5. 按**下一步**。
6. 檢閱叢集設定，然後按一下**完成**。
7. (選擇性) 按一下頁面右側的**重新整理**按鈕，使新 TKGI 叢集出現在叢集清單中。

後續步驟

- 如果您想要變更 worker 節點的數目，請調整 Kubernetes 叢集的大小。
- 下載 kubeconfig 檔案。kubectl 命令列工具使用 kubeconfig 檔案來取得叢集、使用者、命名空間和驗證機制的相關資訊。
- 刪除 Kubernetes 叢集。

管理提供者虛擬資料中心上的虛擬機器儲存區原則

您可以在提供者虛擬資料中心 (VDC) 中新增、啟用、停用和移除虛擬機器儲存區原則。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。

從 VMware Cloud Director 10.2.2 開始，可以限制儲存區原則上允許的實體。請參閱編輯儲存區原則支援的實體類型 。

對提供者虛擬資料中心的儲存區原則啟用虛擬機器加密

您可以將已啟用加密的儲存區原則新增至提供者 VDC。您可以將虛擬機器或磁碟與具有虛擬機器加密功能的儲存區原則相關聯，以加密虛擬機器和磁碟。

從 VMware Cloud Director 10.1 開始，您可以使用虛擬機器加密來提高資料的安全性。加密不僅可以保護虛擬機器，還可以保護虛擬機器磁碟和其他檔案。您可以在 API 和使用者介面中檢視儲存區原則的功能，以及虛擬機器和磁碟的加密狀態。您可以在加密的虛擬機器和磁碟上執行相應 vCenter Server 版本中支援的所有作業。

啟用虛擬機器加密

若要在 VMware Cloud Director 中加密虛擬機器，您必須在 vCenter Server 執行個體上至少設定一個金鑰管理伺服器 (KMS)，並將虛擬機器和磁碟與具有虛擬機器加密功能的儲存區原則相關聯。

1. 在 vCenter Server 中，新增 KMS 叢集。vCenter Server 執行個體可以有多個 KMS 叢集。如需設定金鑰管理伺服器叢集的相關資訊，請參閱《vSphere 安全性指南》中的〈設定金鑰管理伺服器叢集〉主題。
2. 在 vCenter Server 中，對儲存區原則啟用加密。請參閱《vSphere 安全性指南》中的〈建立加密儲存區原則〉主題。
3. 在 VMware Cloud Director Service Provider Admin Portal 中，將已啟用加密的原則新增至提供者 VDC。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。
4. 在 VMware Cloud Director Service Provider Admin Portal 中，將已啟用加密的原則新增至組織 VDC。請參閱將虛擬機器儲存區原則新增至組織虛擬資料中心。
5. 在 VMware Cloud Director Tenant Portal 中，承租人可將虛擬機器或磁碟與已啟用虛擬機器加密的儲存區原則相關聯。
6. 若要解密虛擬機器或磁碟，承租人可以將該虛擬機器或磁碟與未啟用加密的儲存區原則相關聯。

虛擬機器加密限制

VMware Cloud Director 不支援下列動作。

- 加密或解密已開啟電源的虛擬機器或其磁碟。
- 匯出已加密虛擬機器的 OVF。
- 使用快照加密和解密虛擬機器的磁碟 (如果磁碟屬於快照的一部分)。
- 在虛擬機器的磁碟位於加密原則上時解密虛擬機器。
- 將已加密的磁碟新增至未加密的虛擬機器。

- 在未加密的虛擬機器上加密現有磁碟。
- 將已加密的具名磁碟新增至未加密的虛擬機器。
- 建立加密的連結複製。
- 加密連結複製虛擬機器或其磁碟。
- 在來源虛擬機器已加密時，在 vCenter Server 執行個體之間具現化、移動或複製虛擬機器。

備註 在快速佈建的組織 VDC 上，如果來源或目標虛擬機器已加密，且您想要建立複製，VMware Cloud Director 一律會建立完整複製。

識別虛擬機器加密儲存區功能

依預設，**系統管理員**和**組織管理員**具有檢視組織 VDC 儲存區功能，以及虛擬機器和磁碟是否加密的必要權限。**vApp 作者**可以檢視虛擬機器和磁碟的加密狀態。如需有關角色和權限的詳細資訊，請參閱預先定義的角色與其權限。

您可以在**資源 > vSphere 資源 > 儲存區原則**下的**功能**資料行中檢視所有儲存區功能。此資料行顯示虛擬機器加密、以標籤為基礎的關聯、vSAN，以及 IOPS 限制儲存區功能。若要檢視儲存區功能的完整清單，請按一下儲存區原則名稱左側的箭頭以展開資料列。

您也可以在提供者 VDC 的**儲存區原則**索引標籤中檢視儲存區功能資訊。

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。

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. 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。
2. 在左面板中，選取**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**原則**下，選取**儲存區**，然後按一下**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，VMware Cloud 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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，選取**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**原則**下，選取**儲存區**。

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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，選取**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**原則**下，選取**儲存區**。

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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，選取**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**原則**下，選取**儲存區**。

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**。

啟用每秒 I/O 作業數設定

您可以為儲存區原則啟用每秒 I/O 作業數 (IOPS) 設定，以便承租人可以設定每個磁碟的 IOPS 限制。

實體儲存裝置和虛擬磁碟中的受管理讀取/寫入效能採用稱為 IOPS (測量每秒讀取/寫入作業數) 單位定義。若要限制 I/O 效能，包含已啟用 IOPS 配置的儲存裝置的提供者 VDC 儲存區原則必須支援組織 VDC 儲存區原則。之後，承租人可以設定使用此原則要求指定層級之 I/O 效能的磁碟。設定了 IOPS 支援的儲存區設定檔會將其預設 IOPS 值傳遞給使用該設定檔的所有磁碟。其中包括未設定為要求特定 IOPS 值的磁碟。設定為要求特定 IOPS 值的硬碟無法使用 IOPS 上限值低於要求值的儲存區原則，或未設定 IOPS 支援的儲存區原則。

備註 虛擬機器所看到的實際 I/O 輸送量是區塊大小與 IOPS 的組合。如果虛擬機器使用不同的區塊大小，即使 IOPS 限制為相同的數值，其輸送量也會不同。如需有關管理 Storage I/O 資源的詳細資訊，請參閱《vSphere 資源管理》指南。

VMware Cloud Director IOPS 儲存區原則

使用此選項時，您可以編輯預設 IOPS 設定。可以對每個磁碟的 IOPS 或每個儲存區原則的 IOPS 設定限制。您可以根據磁碟大小 (以 GB 為單位) 設定每個磁碟的 IOPS 限制，以便為更大的磁碟授與更多 IOPS。承租人可以在這些限制內對磁碟設定自訂 IOPS。無論是否考慮 IOPS 放置容量，均可使用 IOPS 限制。

無法在 Storage DRS 叢集支援的儲存區原則上啟用 IOPS。

1 如果您希望 VMware Cloud Director 在資料存放區上放置磁碟時考慮 IOPS，請在 vCenter Server 中將 IOPS 容量新增至與要修改的儲存區原則相關聯的所有資料存放區。

2 如果您希望 VMware Cloud Director 在資料存放區上放置磁碟時考慮 IOPS，請在 vCenter Server 中建立使用已新增 IOPS 容量之資料存放區的儲存區原則。

3 透過使用 VMware Cloud Director Service Provider Admin Portal 或 VMware Cloud Director API，將儲存區原則新增至一或多個提供者 VDC。

4 透過使用 Service Provider Admin Portal 或 VMware Cloud Director API，將儲存區原則發佈到一或多個組織 VDC。將儲存區原則發佈到的組織 VDC 會繼承原則的 IOPS 設定。

5 如果您想要編輯繼承的儲存區原則 IOPS 設定，請使用 Service Provider Admin Portal 或 VMware Cloud Director API 來更新組織 VDC 儲存區原則。

此原則類型會顯示為儲存區原則的 `VCD/IOPS` 功能。

vCenter Server IOPS 儲存區原則

對於使用此原則的所有磁碟，此選項具有一個 IOPS 設定。您無法在 VMware Cloud Director 中編輯此設定。承租人無法使用這些原則對磁碟設定自訂 IOPS。此選項不會根據磁碟大小或資料存放區之間的負載平衡調整 IOPS。

1 在 vCenter Server 中，使用自訂保留、限制和共用率建立已啟用 VC-IOPS 的儲存區原則。

2 在 vCenter Server 或 VMware Cloud Director Service Provider Admin Portal 中，將磁碟指派給儲存區原則。

此原則類型會顯示為儲存區原則的 `vSphere/IOPS` 功能。如果來源或目標虛擬機器具有 `vSphere/IOPS` 功能，則無法建立快速佈建的虛擬機器。

在 vCenter Server 中對磁碟設定 IOPS

若要變更 IOPS 設定，請在 vCenter Server 中手動更新磁碟上的 IOPS。您無法在 VMware Cloud Director 中編輯這些 IOPS 設定。

對現有儲存區原則啟用 IOPS 限制

備註 無法對已有 `vSphere/IOPS` 功能的原則啟用 VMware Cloud Director IOPS 限制。

- 對 `VCD/IOPS` 儲存區原則啟用 IOPS 限制：
  a 如果您希望 VMware Cloud Director 在資料存放區上放置磁碟時考慮 IOPS 容量，請在 vCenter Server 中將 IOPS 容量新增至與要修改的儲存區原則相關聯的所有資料存放區。
  b 如果您希望 VMware Cloud Director 將磁碟放置在資料存放區上時考慮 IOPS 容量，請使用 VMware Cloud Director Service Provider Admin Portal 或 VMware Cloud Director API 確保對應的提供者 VDC 儲存區原則將 IOPS 容量報告為非零。
  c 透過使用 VMware Cloud Director Service Provider Admin Portal 或 VMware Cloud Director API，更新組織 VDC 儲存區原則以啟用 `VCD/IOPS` 功能，並設定最大 IOPS 值、預設 IOPS 值等。
- 在 vCenter Server 中對 `vSphere/IOPS` 儲存區原則啟用 IOPS 限制。

當您為組織 VDC 儲存區原則啟用 IOPS 限制時，承租人可使用 VMware Cloud Director Tenant Portal 設定每個磁碟的 IOPS 限制。

編輯提供者 VDC 儲存區原則設定

您可以變更提供者 VDC 儲存區原則的每秒 I/O 作業數 (IOPS) 設定。依預設，將原則發佈到的組織 VDC 會繼承提供者 VDC 儲存區原則設定。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，選取**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**原則**下，選取**儲存區**。

4 按一下目標儲存區原則旁邊的選項按鈕，然後按一下**編輯設定**。

5 如果您想要限制每秒 I/O 作業數，請開啟**已啟用 IOPS 限制**切換按鈕。

6 如果您想要在放置期間考慮 IOPS，請開啟**影響放置**切換按鈕。

如果**影響放置**切換按鈕已開啟，VMware Cloud Director 會在資料存放區之間提供 IOPS 負載平衡。設定磁碟的 IOPS 設定時，VMware Cloud Director 會考慮具有足夠 IOPS 容量用於所選磁碟的資料存放區。如果**影響放置**切換按鈕已關閉，則不需要為每個資料存放區設定 IOPS 容量，並且您可以使用 Storage DRS 叢集。

7 設定最大和預設 IOPS 設定，然後按一下**儲存**。

結果

新的儲存區原則設定適用於將此原則發佈到的所有組織 VDC。

編輯儲存區原則支援的實體類型

從 VMware Cloud Director10.2.2 開始，如果不希望提供者 VDC 儲存區原則支援特定類型的 VMware Cloud Director 實體，您可以編輯和限制與該原則相關聯的實體清單。

建立提供者 VDC 儲存區原則時，預設支援所有可用的實體類型。預設實體類型為：

- 虛擬機器
- 具名磁碟
- 目錄媒體
- vApp 和虛擬機器範本
- Tanzu Kubernetes 叢集
- Edge 閘道

可以將儲存區原則支援的實體類型限制為此清單中的一或多個類型。建立實體時，只有支援其類型的儲存區原則可用。例如，如果您要建立目錄，則唯一顯示的是支援目錄媒體和/或 vApp 範本的儲存區原則。如果某個實體使用儲存區原則，並且您從支援的實體類型清單中移除了實體類型，則該實體會繼續使用儲存區原則，但您無法在未選取新儲存區原則的情況下對其進行任何變更。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，選取**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**原則**下，選取**儲存區**。

4 按一下目標儲存區原則旁邊的選項按鈕，然後按一下**編輯支援的類型**。

5 從**支援實體類型**下拉式功能表中，選取**選取特定實體**。

6 選取希望儲存區原則支援的實體，然後按一下**儲存**。

後續步驟

- 將虛擬機器儲存區原則新增至組織虛擬資料中心
- 具有**支援的儲存區實體類型：管理**權限的使用者可以使用 VMware Cloud Director OpenAPI 在所有儲存區原則的可用類型清單中新增或移除實體類型。例如，可以在清單中新增或移除執行階段定義的實體 (RDE)。如需有關建立為承租人提供其他 VMware Cloud Director 功能之延伸的詳細資訊，請參閱第 14 章 管理定義的實體。

  VMware Cloud Director 會自動將變更套用至支援所有實體的儲存區原則。您無法移除在一或多個儲存區原則中專門選取的實體。

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。VMware Cloud 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. 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。
2. 在左面板中，選取**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. 選取要新增的資源集區，然後按一下**新增**。

   如果您想要使用 vSphere with VMware Tanzu，請選取主管叢集。VMware Cloud Director 會在主管叢集支援的資源集區旁邊顯示 Kubernetes 圖示。
5. 如果選取主管叢集支援的資源集區或叢集來建立與 Kubernetes 控制平面的信任關係，您必須信任 Kubernetes 控制平面憑證。
6. 如果您想要新增其他資源集區，請重複步驟 1 至步驟 5。

結果

VMware Cloud 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。

VMware Cloud 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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，選取**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。
- 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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，選取**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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，選取**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

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

使用 VMware Cloud 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，VMware Cloud 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。

儲存區租用到期時，VMware Cloud Director 會將 vApp 或 vApp 範本標記為已到期，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 VMware Cloud Director Service Provider Admin Portal 建立新的組織。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**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 按一下**新增**。

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。

啟用或停用組織

停用組織可避免使用者登入組織並終止目前已登入使用者的工作階段。組織中執行的 vApp 會繼續執行。

身為**系統管理員**，即使在停用組織後，您仍可配置資源和新增網路等。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**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 按一下組織名稱旁邊的選項按鈕，然後按一下**啟用**或**停用**。

刪除組織

刪除組織會將其從 VMware Cloud Director 中永久移除。

必要條件

您必須先將組織停用，並刪除組織中的所有組織虛擬資料中心、範本、媒體檔案和 vApp，然後才能刪除組織。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**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 按一下組織名稱旁邊的選項按鈕，然後按一下**刪除**。

3 按一下**是**以確認。

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 從頂部導覽列中，選取**資源**，然後按一下**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 選取組織，然後在**設定**索引標籤下，選取**目錄**。

3 若要變更共用和發佈設定，請按一下**編輯**。

選項	描述
共用	允許組織管理員將此組織的目錄與此 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 從頂部導覽列中，選取**資源**，然後按一下**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 選取組織，然後選取**原則**索引標籤。

3 若要編輯組織的租用、配額、資源限制和密碼原則，請按一下**編輯**。

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。
執行階段到期動作	如何處理已到期的執行中 vApp。 暫停 vApp 後，會暫停其所有虛擬機器，並透過將記憶體寫入磁碟來保留其目前狀態。**關閉電源**會立即停止其所有虛擬機器和子系 vApp。
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**。
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。

移轉承租人儲存區

您可以將一或多個組織的所有 vApp、獨立磁碟和目錄項目，從一或多個資料存放區移轉不同的資料存放區。

解除委任資料存放區之前，您必須將該資料存放區上儲存的所有項目移轉至新的資料存放區。也可以將組織移轉至新的資料存放區，該資料存放區具有更多儲存區容量或使用更新的儲存技術，例如 VMware vSAN。

重要 承租人儲存區移轉是一項執行時間較長的資源密集作業，尤其是在有許多資產要移轉時。如需有關移轉承租人儲存區的詳細資訊，請參閱 https://kb.vmware.com/kb/2151086。

必要條件

- 確定目標組織的組織 VDC 所使用的儲存區原則。請參閱將虛擬機器儲存區原則新增至組織虛擬資料中心。
- 對於包含您要移轉的來源資料存放區的每個儲存區原則，請確認至少有一個要移轉到的目的地資料存放區。您可以建立目的地資料存放區或使用現有目的地資料存放區。如需有關在目標組織所使用之儲存區原則中確定資料存放區的詳細資訊，請參閱《vSphere 儲存區》說明文件。

程序

1. 以**系統管理員**身分或使用具有**組織: 移轉承租人儲存區**權限的角色，登入 VMware Cloud Director Service Provider Admin Portal。
2. 啟動**移轉承租人儲存區**精靈。
   - 在**雲端資源**下，選取**組織**，然後按一下**移轉承租人儲存區**。
   - 在 **vSphere 資源**下，選取**資料存放區**，然後按一下**移轉承租人儲存區**。
3. 選取一或多個具有要移轉之儲存區項目的組織，然後按**下一步**。
4. 選取要移轉的一或多個來源資料存放區，然後按**下一步**。

   精靈將列出系統中的所有資料存放區。
5. 選取一或多個目的地資料存放區，然後按**下一步**。
6. 檢閱**即將完成**頁面，然後按一下**完成**開始移轉。

管理組織的資源耗用量配額

您可以管理組織的整體資源耗用量限制。您可以新增、編輯和移除組織的虛擬機器、Tanzu Kubernetes 叢集、CPU、記憶體或儲存區配額。

如需限制可供使用者或群組使用的資源的相關資訊，請參閱〈管理使用者的資源配額〉或〈管理群組的資源配額〉。

必要條件

建立組織

程序

1. 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。
2. 從左面板中，選取**組織**。

3 選取要為其設定配額的組織的名稱。

4 在**設定**區段下，選取**配額**。

依預設，組織沒有任何配額。

5 按一下**編輯**。

6 修改所選組織的配額。

可以對 Tanzu Kubernetes 叢集數目、組織中的所有或執行中的虛擬機器、已耗用的 CPU、記憶體和儲存區新增、編輯或移除配額。如果您希望組織擁有所選類型的無限制資源，請選取**無限制**。

7 按一下**儲存**。

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 (VDC)。建立組織 VDC 後，您可以修改其內容、停用或刪除此 VDC 以及管理其配置模型、儲存以及網路設定。

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	如果在虛擬機器大小調整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
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	以虛擬機器的虛擬機器大小調整原則為基礎。	無限制	無限制	vCPU 速度乘以 vCPU 數目	自訂
虛擬機器 CPU 保留	以虛擬機器的虛擬機器大小調整原則為基礎。	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	以虛擬機器的虛擬機器大小調整原則為基礎。	無限制	無限制	vRAM	自訂
虛擬機器 RAM 保留	以虛擬機器的虛擬機器大小調整原則為基礎。	0	等於 vRAM 乘以 RAM 保證加上 RAM 額外負荷。	等於 vRAM 乘以 RAM 保證加上 RAM 額外負荷。	自訂

將舊版 VDC 配置模型轉換為彈性配置模型

您可以將虛擬機器放置和虛擬機器大小調整原則新增至具有彈性配置集區模型、非彈性配置集區模型、隨收隨付模型或保留集區模型的 VDC。如果虛擬機器放置或虛擬機器大小調整原則與現有 VDC 配置模型不相容，您可以決定將 VDC 轉換為彈性組織 VDC。

虛擬機器原則符合性

舊版 VDC 轉換不會導致虛擬機器不符合標準。如果管理員直接在 vCenter Server 執行個體中變更虛擬機器的虛擬機器計算值或虛擬機器群組成員資格，則虛擬機器可能會與指派的虛擬機器大小調整或虛擬機器放置原則不相容。如果具有必要權限的使用者使用 vCloud API 變更虛擬機器保留和限制值，則虛擬機器也會變得不符合標準。如果存在不符合標準的虛擬機器，則 VMware Cloud Director Tenant Portal 使用者介面會顯示警告訊息。承租人可查看有關不符合標準之原因的詳細資訊，並可重新使虛擬機器符合標準，以便將原則重新套用至虛擬機器。

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，VMware Cloud 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。
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 VMware Cloud 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 VMware Cloud 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虛擬機器大小調整原則，**系統管理員**可以控制 VDC 和個別虛擬機器 (VM) 層級的 CPU 與 RAM 耗用量。彈性配置模型支援現有配置模型中可用的所有配置組態。

在 VMware Cloud Director 10.0 及更新版本中，所有非彈性組織 VDC 都可以轉換為彈性 VDC。

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

參數	描述
Elasticity	啟用或停用彈性集區功能。
Include VM Memory Overhead	在此 VDC 中包含或排除記憶體額外負荷。設定為 true 時，您可能無法使用 VDC 的完整容量，因為每個已開啟電源的虛擬機器的記憶體額外負荷也會佔用 VDC 的可用容量。若設定為 false，則記憶體額外負荷會佔用提供者 VDC，而不是 VDC 的已配置容量。
CPU allocation	配置給此 VDC 的 CPU 數量 (以 MHz 或 GHz 為單位)。CPU 配置定義了 VDC 的 CPU 容量。VDC 中執行的所有虛擬機器使用的 CPU 總計不得超過此值。
CPU limit	CPU 限制定義了 VDC 的 CPU 配額。在大多數情況下，CPU 限制等於 VDC 的已配置 CPU 容量。 有時，您可能不需要將任何 CPU 配置給 VDC，正如在隨收隨付模型中一樣。在此情況下，您必須透過將 CPU 配置設定為零，並將 CPU 限制設定為非零值，來設定整體 CPU 耗用量的配額。 您也可以使用此設定，以允許無限制的 CPU 配額。如果設定為無限制，則 vCenter Server 中 VDC 的支援資源集區會得到無限制的 CPU。
CPU resources guaranteed	為 VDC 實體保留的 CPU 配置百分比。
vCPU speed	VDC 中虛擬機器的預設 vCPU 速度。
Memory allocation	配置給此 VDC 的記憶體數量 (以 MB 或 GB 為單位)。此參數會定義 VDC 的記憶體容量總計。VDC 中執行的所有虛擬機器設定的記憶體總計不得超過此值。
Memory resources guaranteed	為 VDC 實體保留的記憶體配置百分比。
Maximum number of VMs	VDC 中的虛擬機器數目上限。

作為 **VMware Cloud 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 VMware Cloud 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。

彈性配置模型支援虛擬機器大小調整原則的各種功能，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虛擬機器大小調整原則。如果您沒有定義組織 VDC 的虛擬機器大小調整原則，計算資源配置則取決於組織 VDC 配置模型。透過組合使用彈性配置模型和組織虛擬機器大小調整原則，一個組織 VDC 可容納使用所有其他配置模型之通用組態的虛擬機器。如需詳細資訊，請參閱瞭解虛擬機器大小調整和虛擬機器放置原則。

若要建立彈性組織 VDC，您可以使用 VMware Cloud Director Service Provider Admin Portal 或 vCloud API。如需 vCloud API 的相關資訊，請參閱 VMware Cloud Director 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，您從提供者虛擬資料中心 (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。

做為系統管理員，您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。請參閱修改一般系統設定。

依預設，配置集區組織 VDC 會啟用彈性的配置集區。從 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director 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，VMware Cloud 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。

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 VMware Cloud Director 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。

瞭解虛擬機器大小調整和虛擬機器放置原則

您可以使用虛擬機器大小調整原則和虛擬機器放置原則來控制特定叢集或主機上的虛擬機器 (VM) 資源配置和放置。

VMware Cloud Director **系統管理員**建立並管理全域層級的虛擬機器大小調整原則，並且可以向一或多個組織 VDC 發佈個別原則。對於 VMware Cloud Director 10.2.1 及更早版本，可以為每個提供者 VDC 分別建立和管理虛擬機器放置原則，因為虛擬機器放置原則的範圍限定在提供者 VDC 層級。從 VMware Cloud Director 10.2.2 開始，可以在虛擬機器放置原則的範圍中包括多個提供者 VDC。此外，從 10.2.2 版開始，如果使用者將 vApp 作為 vApp 範本儲存至目錄，則範本還包括原始 vApp 的放置和大小調整原則，以作為不可修改的標記原則。

當您向組織 VDC 發佈原則時，組織中的使用者便可使用該原則。在組織 VDC 中建立和管理虛擬機器時，承租人可以向虛擬機器指派可用的原則。組織 VDC 中的承租人和使用者無法查看虛擬機器放置原則或虛擬機器大小調整原則的特定組態。

虛擬機器放置和大小調整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。如果您向組織 VDC 發佈多個虛擬機器放置原則和虛擬機器大小調整原則，則在組織 VDC 中建立和管理虛擬機器時，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。會針對每個 VDC 自動產生系統預設原則。您可以刪除 VDC 中的系統預設原則，並將其他自訂原則標記為預設原則。預設原則不會定義任何值，且允許所有虛擬機器組態。

虛擬機器放置原則

虛擬機器放置原則定義虛擬機器在主機或主機群組上的放置。這是**雲端提供者管理員**在提供者 VDC 中建立指定主機群組的機制。指定的主機群組是提供者 VDC 叢集內主機的子集，可以根據任何準則 (例如效能層或授權) 進行選取。從 VMware Cloud Director 10.2.2 開始，可以將虛擬機器放置原則的範圍擴充至多個提供者 VDC。

虛擬機器放置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。管理員使用 vCenter Server 中的虛擬機器群組定義或公開指定的主機群組。虛擬機器群組與主機群組具有直接相似性，並代表與其具有相似性的主機群組。

您可以在提供者 VDC 層級定義虛擬機器放置原則。虛擬機器放置原則包括下列屬性：

- 名稱 (在提供者 VDC 中必須是唯一的)
- 描述
- 從提供者 VDC 的基礎叢集中選取的一或多個虛擬機器群組的集合。您可以為每個叢集選取一個虛擬機器群組

虛擬機器放置原則在虛擬機器建立期間是可選的，承租人只能將一個虛擬機器放置原則指派給虛擬機器。

當承租人在組織 VDC 中建立虛擬機器並選取虛擬機器放置原則時，VMware Cloud Director 會將此虛擬機器新增至原則中參考的一或多個虛擬機器群組。如此一來，VMware Cloud Director 會在適當的主機上建立虛擬機器。

一個虛擬機器放置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，虛擬機器放置原則 *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*。

將虛擬機器放置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，如果您選擇將虛擬機器部署在叢集 *oracle_cluster1*，並將虛擬機器放置原則 *oracle_license* 指派給此虛擬機器，則放置引擎會將此虛擬機器新增至虛擬機器群組 *oracle_license1*。

虛擬機器大小調整原則

虛擬機器大小調整原則可定義組織 VDC 中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。

透過虛擬機器大小調整原則，VMware Cloud 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
- 額外組態。

  `extraConfigs` API 參數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。您只能使用 vCloud API 建立具有額外組態的原則。現有額外組態顯示在 Service Provider Admin Portal 使用者介面的詳細虛擬機器大小調整原則視圖中的**額外組態**下。

您可以在全域層級定義虛擬機器大小調整原則。如需有關虛擬機器大小調整原則屬性的詳細資訊，請參閱虛擬機器大小調整原則的屬性。

VMware Cloud Director 將為所有 VDC 產生預設虛擬機器大小調整原則。預設虛擬機器大小調整原則僅包含名稱和說明，而所有其餘的原則屬性都是空的。

您也可以將另一個虛擬機器大小調整原則定義為組織 VDC 的預設原則。預設虛擬機器大小調整原則將會控制承租人在組織 VDC 中建立的虛擬機器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虛擬機器大小調整原則。

若要限制承租人可為組織 VDC 內的個別虛擬機器配置的最大計算資源，雲端提供者可以定義最大虛擬機器大小調整原則。指派給組織 VDC 時，最大虛擬機器大小調整原則可用作組織 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最大虛擬機器大小調整原則。當您將某個虛擬機器大小調整原則定義為最大原則時，VMware Cloud Director 會在內部複製原則內容，並將複製的內容用作最大虛擬機器大小調整原則。因此，組織 VDC 不依賴於最初使用的虛擬機器大小調整原則。

透過使用虛擬機器大小調整原則，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 (*Small Size*、*Medium Size* 和 *Large Size*)。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虛擬機器大小調整原則。

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 發佈新的虛擬機器大小調整原則。

3 或者，將其中一個虛擬機器大小調整原則定義為組織 VDC 的預設虛擬機器大小調整原則。

以下是雲端提供者的可用原則作業：

- 若要定義虛擬機器在主機或主機群組上的放置，請建立放置原則。請參閱在提供者 VDC 中建立虛擬機器放置原則。
- 若要控制承租人工作負載的實體計算資源配置，請建立大小調整原則。請參閱建立虛擬機器大小調整原則。
- 將虛擬機器放置原則或虛擬機器大小調整原則發佈到一或多個組織 VDC。請參閱將虛擬機器放置原則新增至組織 VDC
- 將虛擬機器放置原則或虛擬機器大小調整原則設定為預設值。
- 編輯虛擬機器放置原則和虛擬機器大小調整原則。只能在 VMware Cloud Director 使用者介面中編輯原則的名稱和說明。
- 從組織 VDC 解除發佈虛擬機器放置原則或虛擬機器大小調整原則。
- 刪除虛擬機器放置原則或虛擬機器大小調整原則。請參閱刪除虛擬機器放置原則和刪除虛擬機器大小調整原則。

擁有 ORG_VDC_MANAGE_COMPUTE_POLICIES 權限的使用者可以建立、更新和發佈虛擬機器放置原則和虛擬機器大小調整原則。

下表列出了適用於承租人使用者的虛擬機器大小調整原則和虛擬機器放置原則作業。

表 6-1. 適用於承租人使用者的虛擬機器大小調整原則和虛擬機器放置原則作業

作業	描述
在虛擬機器建立期間，將原則指派給虛擬機器。	組織 VDC 中有權建立虛擬機器的承租人使用者，可以選擇性地使用 VMware Cloud Director Tenant Portal 向虛擬機器指派虛擬機器大小調整原則和虛擬機器放置原則。如此一來，在虛擬機器大小調整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，承租人不需要指派虛擬機器放置或大小調整原則。如果承租人未明確選取要指派給虛擬機器的虛擬機器大小調整原則，則會將預設虛擬機器大小調整原則套用至虛擬機器。 如果未建立任何虛擬機器放置原則，則虛擬機器放置原則選項對承租人不可見。如果承租人選取具有大小調整資訊的放置原則，則虛擬機器大小調整原則選項會對承租人隱藏。您只能使用 vCloud API 建立具有大小調整資訊的虛擬機器放置原則。 如果只有一個虛擬機器大小調整原則，則虛擬機器大小調整原則選項對承租人不可見。 當**系統管理員**設定虛擬機器大小調整原則中的 **vCPU 計數**、**每個通訊端的核心數**和**記憶體**屬性時，如果承租人選取此原則，則會顯示這些值，但無法編輯。
向現有的虛擬機器指派一個原則。	組織 VDC 中有權管理虛擬機器的承租人使用者，可以使用 VMware Cloud Director Tenant Portal 指派或變更現有虛擬機器的虛擬機器大小調整原則和虛擬機器放置原則。當承租人變更虛擬機器放置原則時，虛擬機器會根據新的虛擬機器放置原則中定義的虛擬機器-主機相似性規則移至新主機。當承租人變更虛擬機器大小調整原則時，系統會將虛擬機器重新設定為使用新虛擬機器大小調整原則中指定的計算資源。

使用虛擬機器放置原則和虛擬機器大小調整原則的工作流程如下所示。

1 **系統管理員**建立一或多個虛擬機器放置原則。請參閱在提供者 VDC 中建立虛擬機器放置原則。

2 **系統管理員**建立一或多個虛擬機器大小調整原則。請參閱建立虛擬機器大小調整原則。

   虛擬機器大小調整原則的名稱在單一 VMware Cloud Director 站台中是唯一的。虛擬機器放置原則的名稱在原則的提供者 VDC 範圍內是唯一的。

3 **系統管理員**將虛擬機器放置原則和虛擬機器大小調整原則發佈到一或多個組織 VDC。請參閱將虛擬機器放置原則新增至組織 VDC。

   發佈虛擬機器放置原則後，組織 VDC 中的承租人使用者在建立虛擬機器和編輯虛擬機器期間便可使用該原則。

4 建立或更新虛擬機器時，承租人可以使用 vCloud API 或 VMware Cloud Director Tenant Portal 將虛擬機器大小調整原則和虛擬機器放置原則指派給虛擬機器。

在提供者 VDC 中建立虛擬機器放置原則

虛擬機器放置原則是包含提供者 VDC 原則參考的 VDC 運算原則。從 VMware Cloud Director 10.2.2 開始，可以將多個提供者 VDC 新增到虛擬機器放置原則的範圍中。您可以使用虛擬機器放置原則來定義特定主機、主機群組或叢集上的虛擬機器放置。

從 VMware Cloud Director 10.2.2 開始，虛擬機器放置原則可包含一或多個提供者 VDC 原則的參考。從提供者 VDC 內建立放置原則時，該原則僅參考選取的提供者 VDC。可以透過編輯虛擬機器放置原則以在原則範圍內包括更多提供者 VDC，也可以從**虛擬機器放置原則**索引標籤建立放置原則以將多個提供者 VDC 納入其範圍中。請參閱編輯虛擬機器放置原則和建立全域虛擬機器放置原則。

必要條件

- 確認您的環境中至少有一個提供者 VDC。
- 確認您的環境中至少有一個虛擬機器群組。

  虛擬機器群組是虛擬機器的集合，您可以將其連結至具有正相似性的主機群組。透過正相似性規則，您可以在特定主機上放置一組虛擬機器。您可以透過 vCenter Server 使用者介面或 VMware Cloud Director API 建立虛擬機器群組。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，選取**提供者 VDC**。

3 從清單中按一下提供者 VDC。

4 按一下**虛擬機器放置原則**索引標籤，然後按一下**新增**。

5 (選擇性) 在精靈的**虛擬機器放置原則定義**頁面上，選取核取方塊以停止顯示虛擬機器放置原則資訊。

6 按**下一步**。

7 輸入虛擬機器放置原則的名稱，並選擇性地輸入說明。

8 選取要將虛擬機器連結到的虛擬機器群組或邏輯虛擬機器群組，然後按**下一步**。

   當您選取多個邏輯群組時，如果承租人將此原則套用至虛擬機器，則該虛擬機器將成為所選邏輯虛擬機器群組中包含的所有虛擬機器群組的成員。虛擬機器可使用套用至這些群組中虛擬機器的所有相似性的組合。從 VMware Cloud Director 10.2.2 開始，可以同時選取虛擬機器群組和邏輯群組。

   您可以透過為每個叢集選取一個虛擬機器群組，建立內嵌邏輯虛擬機器群組。此邏輯虛擬機器群組不具有名稱且僅可用於所選虛擬機器放置原則。

9 檢閱虛擬機器放置原則設定，然後按一下**完成**。

後續步驟

- 建立虛擬機器大小調整原則.
- 將虛擬機器放置原則新增至組織 VDC.
- 從 VMware Cloud Director 10.2.2 開始，可以編輯虛擬機器放置原則。
- 刪除虛擬機器放置原則.

建立全域虛擬機器放置原則

從 VMware Cloud Director 10.2.2 開始，虛擬機器放置原則可包含一或多個提供者 VDC 原則的參考。您可以使用虛擬機器放置原則來定義特定主機、主機群組或一或多個叢集上的虛擬機器放置。

從提供者 VDC 內建立放置原則時，該原則僅參考選取的提供者 VDC。請參閱在提供者 VDC 中建立虛擬機器放置原則。從 VMware Cloud Director 10.2.2 開始，可以透過編輯虛擬機器放置原則以在原則範圍內包括更多提供者 VDC，也可以建立一個全域放置原則。

必要條件

- 確認您的環境中至少有一個提供者 VDC。
- 確認您的環境中至少有一個虛擬機器群組。

  虛擬機器群組是虛擬機器的集合，您可以將其連結至具有正相似性的主機群組。透過正相似性規則，您可以在特定主機上放置一組虛擬機器。您可以透過 vCenter Server 使用者介面或 VMware Cloud Director API 建立虛擬機器群組。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 從左面板中，選取**虛擬機器放置原則**，然後按一下**新增**。

3 (選擇性) 在精靈的**虛擬機器放置原則定義**頁面上，選取核取方塊以停止顯示虛擬機器放置原則資訊。

4 按**下一步**。

5 輸入虛擬機器放置原則的名稱，並選擇性地輸入說明。

6 選取要將虛擬機器連結到的虛擬機器群組和邏輯虛擬機器群組，然後按**下一步**。

  您可以為每個叢集選取一個虛擬機器群組。

  當您選取多個邏輯群組時，如果承租人將此原則套用至虛擬機器，則該虛擬機器將成為所選邏輯虛擬機器群組中包含的所有虛擬機器群組的成員。虛擬機器可使用套用至這些群組中虛擬機器的所有相似性的組合。從 VMware Cloud Director 10.2.2 開始，可以同時選取虛擬機器群組和邏輯群組。

  您可以透過為每個叢集選取一個虛擬機器群組，建立內嵌邏輯虛擬機器群組。此邏輯虛擬機器群組不具有名稱且僅可用於所選虛擬機器放置原則。

7 檢閱虛擬機器放置原則設定，然後按一下**完成**。

後續步驟

- 建立虛擬機器大小調整原則.
- 將虛擬機器放置原則新增至組織 VDC.
- 從 VMware Cloud Director 10.2.2 開始，可以編輯虛擬機器放置原則。
- 刪除虛擬機器放置原則.

編輯虛擬機器放置原則

從 VMware Cloud Director 10.2.2 開始，可以編輯和變更虛擬機器放置原則的範圍。

必要條件

建立全域虛擬機器放置原則

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 從左面板中，選取**虛擬機器放置原則**。

3 選取虛擬機器放置原則，然後按一下**編輯**。

4 (選擇性) 在精靈的**虛擬機器放置原則定義**頁面上，選取核取方塊以停止顯示虛擬機器放置原則資訊。

5 按**下一步**。

6 編輯虛擬機器放置原則的名稱，並選擇性地編輯說明。

7 編輯要將虛擬機器連結到的虛擬機器群組和邏輯虛擬機器群組，然後按**下一步**。

   您可以為每個叢集選取一個虛擬機器群組。您無法取消選取目前使用中的叢集，例如，當您向組織 VDC 發佈放置原則時。

8 檢閱虛擬機器放置原則設定，然後按一下**完成**。

後續步驟

- 建立虛擬機器大小調整原則.
- 將虛擬機器放置原則新增至組織 VDC.
- 刪除虛擬機器放置原則.

將虛擬機器放置原則新增至組織 VDC

當您建立虛擬機器放置原則時，該原則對承租人不可見。您可以將虛擬機器放置原則發佈至組織 VDC，以使其可供承租人使用。

將虛擬機器放置原則發佈至組織 VDC 會使原則對承租人可見。對於 VMware Cloud Director 10.2.2 及更新版本，若要向組織 VDC 發佈放置原則，則必須先透過建立全域虛擬機器放置原則或編輯虛擬機器放置原則，將其支援提供者 VDC 納入虛擬機器放置原則的範圍。當承租人建立新的獨立虛擬機器或從範本建立虛擬機器、編輯虛擬機器、將虛擬機器新增至 vApp，以及從 vApp 範本建立 vApp 時，承租人可選取此原則。您無法刪除可供承租人使用的虛擬機器放置原則。

必要條件

- 確認您的環境中至少有一個組織 VDC。請參閱建立組織虛擬資料中心。
- 確認您至少有一個虛擬機器放置原則。請參閱在提供者 VDC 中建立虛擬機器放置原則。對於 VMware Cloud Director 10.2.2 及更新版本，您可以建立包含一或多個提供者 VDC 原則參考的全域放置原則。請參閱建立全域虛擬機器放置原則。

程序

1. 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。
2. 在左面板中，按一下**組織 VDC**。
3. 選取組織 VDC，然後按一下**虛擬機器放置原則**索引標籤。
4. 按一下**新增**。
5. 選取您想要新增至組織 VDC 的虛擬機器放置原則，然後按一下**確定**。

後續步驟

- 選取原則，然後按一下**移除**以解除發佈原則。
- 選取虛擬機器放置原則，然後按一下**設定為預設值**，以使該原則在虛擬機器和 vApp 建立以及虛擬機器編輯期間顯示為承租人的預設選擇。如果已針對組織 VDC 發佈多個虛擬機器放置原則，則承租人可以選取預設原則以外的原則。

刪除虛擬機器放置原則

如果虛擬機器放置原則未發佈至承租人，您可以從提供者 VDC 中將其刪除。

必要條件

- 確認您的環境中至少有一個虛擬機器放置原則。
- 確認虛擬機器放置原則未新增至組織 VDC。您無法刪除可供承租人使用的虛擬機器放置原則。

程序

1. 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。
2. 在左面板中，選取**提供者 VDC**。
3. 從清單中按一下提供者 VDC。
4. 按一下**虛擬機器放置原則**索引標籤，然後選取虛擬機器放置原則。
5. 按一下**刪除**。

虛擬機器大小調整原則的屬性

當您建立虛擬機器 (VM) 大小調整原則時，可以指定所有可用屬性的子集。唯一的必要屬性是虛擬機器大小調整原則名稱。

虛擬機器大小調整原則中有兩種類型的參數。

- 個別虛擬機器大小調整組態 - 根據目前的原則，為虛擬機器預先設定指定的 RAM、vCPU 計數和每個通訊端的核心數。
- 對最大資源數目的限制 - 根據目前的原則，按單一虛擬機器預先設定記憶體和 CPU 耗用量限制。

下表列出了您可以在虛擬機器大小調整原則中定義的所有屬性。

表 6-2. VDC 運算原則屬性

VDC 運算原則屬性	API 參數	描述
Name	name	用作虛擬機器大小調整原則識別碼的必要參數。
Description	description	表示虛擬機器大小調整原則的簡短說明。
vCPU Speed	cpuSpeed	定義核心的 vCPU 速度 (以 MHz 或 GHz 為單位)。
vCPU Count	cpuCount	定義為虛擬機器設定的 vCPU 數目。這是虛擬機器硬體組態。 當承租人將虛擬機器大小調整原則指派給虛擬機器時，此計數會變成為虛擬機器設定的 vCPU 數目。
Cores Per Socket	coresPerSocket	虛擬機器之每個通訊端的核心數目。這是虛擬機器硬體組態。 虛擬機器大小調整原則中定義的 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。
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 或 GHz 為單位)。 如果未在 VDC 運算原則中定義，則 CPU 限制等於 vCPU 速度乘以 vCPU 數目。
CPU Shares	cpuShares	定義虛擬機器的 CPU 共用數目。 共用率可指定虛擬機器在虛擬資料中心內的相對重要性。如果某個虛擬機器的 CPU 共用率是另一個虛擬機器的兩倍，則在這兩個虛擬機器競爭資源時，前者也有權耗用兩倍的 CPU。 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	memory	定義為虛擬機器設定的記憶體 (以 MB 或 GB 為單位)。這是虛擬機器硬體組態。 當承租人將虛擬機器大小調整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。
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 100% 之間。
Memory Limit	memoryLimit	定義虛擬機器的記憶體限制 (以 MB 或 GB 為單位)。 如果未在虛擬機器大小調整原則中定義，則記憶體限制等於虛擬機器的已配置記憶體。

表 6-2. VDC 運算原則屬性 (續)

VDC 運算原則屬性	API 參數	描述
Memory Shares	memoryShares	定義虛擬機器的記憶體共用數目。 共用率可指定虛擬機器在虛擬資料中心內的相對重要性。如果某個虛擬機器的記憶體共用率是另一個虛擬機器的兩倍，則在這兩個虛擬機器爭用資源時，前者有權取用兩倍的記憶體。 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。 您只能透過 vCloud API 建立具有額外組態的原則。現有額外組態顯示在 Service Provider Admin Portal 使用者介面的詳細虛擬機器大小調整原則視圖中的**額外組態**下。

建立虛擬機器大小調整原則

您可以建立虛擬機器大小調整原則，以便承租人可以使用預先定義的 CPU 和記憶體耗用量限制，這些限制會套用到組織 VDC 中的個別虛擬機器。

程序

1. 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。
2. 在左面板中，按一下**虛擬機器大小調整原則**。
3. 按一下**新增**。
4. 輸入虛擬機器大小調整原則的名稱，並選擇性地輸入說明。
5. 按**下一步**。
6. 在 **CPU** 頁面上，選取您要套用至原則的 CPU 配置設定，然後按**下一步**。
7. 選取您要套用至原則的記憶體配置設定，然後按**下一步**。
8. 檢閱虛擬機器大小調整原則設定，然後按一下**完成**。

後續步驟

- 建立虛擬機器大小調整原則後，您可以僅編輯虛擬機器大小調整原則名稱和說明。請參閱編輯虛擬機器大小調整原則。
- 將虛擬機器大小調整原則新增至組織 VDC.
- 在提供者 VDC 中建立虛擬機器放置原則.

將虛擬機器大小調整原則新增至組織 VDC

當您建立虛擬機器大小調整原則時，該原則對承租人不可見。您可以將虛擬機器大小調整原則發佈至組織 VDC，以使其可供承租人使用。

將虛擬機器大小調整原則發佈至組織 VDC 會使原則對承租人可見。當承租人建立新的獨立虛擬機器或從範本建立虛擬機器、編輯虛擬機器、將虛擬機器新增至 vApp，以及從 vApp 範本建立 vApp 時，承租人可選取此原則。您無法刪除可供承租人使用的虛擬機器大小調整原則。

必要條件

- 確認您的環境中至少有一個組織 VDC。請參閱建立組織虛擬資料中心。
- 確認您至少有一個虛擬機器大小調整原則。請參閱建立虛擬機器大小調整原則。

程序

1. 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。
2. 在左面板中，按一下**組織 VDC**。
3. 選取組織 VDC，然後按一下**虛擬機器大小調整原則**索引標籤。
4. 按一下**新增**。
5. 選取您想要新增至組織 VDC 的虛擬機器大小調整原則，然後按一下**確定**。

後續步驟

- 選取原則，然後按一下**移除**以解除發佈原則。
- 選取虛擬機器大小調整原則，然後按一下**設定為預設值**，以使該原則在虛擬機器和 vApp 建立以及虛擬機器編輯期間顯示為承租人的預設選擇。如果已針對組織 VDC 發佈多個虛擬機器大小調整原則，則承租人可以選取預設原則以外的原則。

編輯虛擬機器大小調整原則

建立虛擬機器大小調整原則後，您可以僅編輯其名稱和說明。不支援編輯 CPU 和記憶體參數。

必要條件

- 確認您的環境中至少有一個組織 VDC。請參閱建立組織虛擬資料中心。
- 確認您至少有一個虛擬機器大小調整原則。請參閱建立虛擬機器大小調整原則。

程序

1. 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。
2. 在左面板中，按一下**虛擬機器大小調整原則**。
3. 按一下您要編輯的虛擬機器大小調整原則的名稱。
4. 若要編輯原則的名稱和說明，請按一下**編輯**。
5. 按一下**儲存**。

後續步驟

將虛擬機器大小調整原則新增至組織 VDC

刪除虛擬機器大小調整原則

您可以刪除未發佈至承租人的虛擬機器大小調整原則。

必要條件

- 確認您的環境中至少有一個虛擬機器大小調整原則。
- 確認虛擬機器大小調整原則未新增至組織 VDC。您無法刪除可供承租人使用的虛擬機器大小調整原則。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，按一下**虛擬機器大小調整原則**。

3 選取虛擬機器大小調整原則，然後按一下**刪除**。

將 Kubernetes 與 VMware Cloud Director 搭配使用

透過將 Kubernetes 與 VMware Cloud Director 搭配使用，您可以向承租人提供多承租人 Kubernetes 服務。

Container Service Extension

Kubernetes Container Clusters 是適用於 VMware Cloud Director 的 Container Service Extension 外掛程式。服務提供者和承租人必須使用 Kubernetes Container Clusters 外掛程式來建立 Kubernetes 叢集。從 VMware Cloud Director10.2 開始，無需手動下載該外掛程式並將其上傳至 VMware Cloud DirectorService Provider Admin Portal。依預設，該外掛程式在 VMware Cloud Director 中可用，但您必須將其發佈至承租人，他們才能夠建立 Kubernetes 叢集。

服務提供者和承租人必須使用 Container Service Extension 3.0 版來建立原生和 VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) 叢集。必須完成 Container Service Extension 3.0 伺服器設定，並將 Container Service Extension 原生放置原則發佈到一或多個組織 VDC。

VMware Cloud Director 中的 vSphere with VMware Tanzu

可以使用 VMware Cloud Director 中的 vSphere with VMware Tanzu 建立主管叢集支援的提供者虛擬資料中心 (VDC)。啟用了 vSphere with VMware Tanzu 的主機叢集稱為主管叢集。可以對資源的使用設定限制，並限制可用資源，包括每個組織、使用者或群組的 Kubernetes 叢集數目。如需詳細資訊，請參閱管理組織的資源耗用量配額。

若要使用 VMware Cloud Director 中的 vSphere with VMware Tanzu，您必須先在 vSphere 7.0 或更新版本的叢集上啟用 vSphere with VMware Tanzu 功能，並將該叢集設定為主管叢集。請參閱 vSphere 說明文件中的《vSphere with Kubernetes 組態和管理》指南。您要使用的 vCenter Server 執行個體可以同時擁有主機叢集和主管叢集。

若要建立 Tanzu Kubernetes 叢集，您必須將提供者 VDC Kubernetes 原則發佈到組織，並在建立期間套用組織 VDC Kubernetes 原則。原生和 TKGI 叢集不使用提供者和組織 VDC Kubernetes 原則。

Kubernetes 叢集類型

- 原生叢集 - Kubernetes Container Clusters 外掛程式使用原生 Kubernetes 執行階段管理叢集。這些叢集具有單一控制平面節點，且高可用性功能有所弱化，可提供的持續性磁碟區選擇較少，並且沒有網路自動化。但是，它們的成本可能較低。對於原生 Kubernetes 叢集部署，必須設定 Container Service Extension 伺服器。請參閱 Container Service Extension (CSE) 說明文件中的〈CSE 伺服器管理〉一章。
- Tanzu Kubernetes 叢集 - 您可以使用 vSphere with Tanzu 執行階段選項建立 vSphere with VMware Tanzu 管理的 Tanzu Kubernetes 叢集。此選項提供更多功能，但是成本較高。如需詳細資訊，請參閱 vSphere 說明文件中的《vSphere with Kubernetes 組態和管理》指南。
- TKGI 叢集 - VMware Tanzu Kubernetes Grid Integrated Edition 是一項專門為多雲端企業和服務提供者實作 Kubernetes 而建立的容器解決方案。其部分功能包括對 Kubernetes 叢集執行高可用性、自動調整、健全狀況檢查、自我修復和輪流升級。如需有關 TKGI 叢集的詳細資訊，請參閱 VMware Tanzu Kubernetes Grid Integrated Edition 說明文件。

建立 Tanzu Kubernetes 叢集的工作流程

1 將啟用了 vSphere with VMware Tanzu 功能的 vCenter Server 7.0 或更新版本執行個體新增至 VMware Cloud 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。

2 驗證每個主管叢集上的網路設定，使其能夠執行 Kubernetes 工作負載。

重要 `Ingress CIDRs` 和 `Services CIDR` 參數的 IP 位址範圍不得與 IP 位址 10.96.0.0/12 和 192.168.0.0/16 (這是 `services` 和 `pods` 參數的預設 vSphere 值) 重疊。請參閱《vSphere with Kubernetes 組態和管理》指南中的 Tanzu Kubernetes 叢集組態參數的資訊。

備註 從 VMware Cloud Director 10.2.2 開始，如果在初始設定後修改主管叢集的網路設定，則必須重新整理 vCenter Server 執行個體，以調整會封鎖從建立該叢集之組織虛擬資料中心的外部對 Tanzu Kubernetes 叢集進行存取的自動防火牆原則及 NAT 規則。

3 建立主管叢集支援的提供者 VDC。請參閱建立提供者虛擬資料中心。

或者，您可以將主管叢集新增至現有提供者 VDC。如果您的環境為 vSphere 6.7 或更早版本，還可以將環境升級至 7.0 版，並在現有叢集上啟用 vSphere with VMware Tanzu。

在列出所有提供者 VDC 的網格中，主管叢集支援的提供者 VDC 會在其名稱旁邊顯示 Kubernetes 圖示。

4 (選擇性) VMware Cloud Director 會自動為主管叢集支援的提供者 VDC 產生預設提供者 VDC Kubernetes 原則。您可以為 Tanzu Kubernetes 叢集建立其他提供者 VDC Kubernetes 原則。請參閱建立提供者 VDC Kubernetes 原則。

5 將提供者 VDC Kubernetes 原則發佈到組織 VDC (從**提供者 VDC** 索引標籤)，或新增組織 VDC Kubernetes 原則 (從**組織 VDC** 索引標籤)。

6 將 Kubernetes Container Clusters 外掛程式發佈到服務提供者。請參閱從組織發佈或解除發佈外掛程式。如果您想讓承租人能夠建立 Kubernetes 叢集，則必須將 Kubernetes Container Clusters 外掛程式發佈到這些組織。如需有關管理 VMware Cloud Director 外掛程式的詳細資訊，請參閱管理外掛程式。

7 如果要向承租人授與建立和管理 Tanzu Kubernetes 叢集的權限，則必須將 **vmware:tkgcluster 權利**權限服務包發佈到要使用叢集的任何組織。共用權限服務包後，您必須將**編輯：Tanzu Kubernetes 客體叢集**權限新增至要建立和修改 Tanzu Kubernetes 叢集的角色。如果還想讓使用者刪除叢集，則必須將**完全控制：Tanzu Kubernetes 客體叢集**權限新增至角色。此外，您可以將管理員權限指派給想要檢視組織中所有 Tanzu Kubernetes 叢集的使用者，或想要跨站台管理叢集的使用者。如需執行階段定義的實體 (RDE) 的權限和存取層級的相關資訊，請參閱第 14 章 管理定義的實體。

8 透過建立存取控制清單 (ACL) 項目向承租人或系統管理員授與存取權。如需有關共用執行階段定義的實體 (RDE) 的詳細資訊，請參閱共用定義的實體。

9 建立 Tanzu Kubernetes 叢集

建立原生和 TKGI 叢集的工作流程

1 將 Kubernetes Container Clusters 外掛程式發佈到服務提供者。請參閱從組織發佈或解除發佈外掛程式。如果您想讓承租人能夠建立 Kubernetes 叢集，則必須將 Kubernetes Container Clusters 外掛程式發佈到這些組織。如需有關管理 VMware Cloud Director 外掛程式的詳細資訊，請參閱管理外掛程式。

2 設定 Container Service Extension 伺服器，並將 Container Service Extension 原生放置原則或 TKGI 啟用中繼資料發佈至組織 VDC。如需有關設定 CSE 伺服器的詳細資訊，請參閱 Container Service Extension (CSE) 說明文件中的 CSE 伺服器管理一章。

3 如果要向承租人授與建立和管理原生叢集的權限，則必須將 **cse:nativeCluster 權利**權限服務包發佈到要使用原生叢集的任何組織。共用權限服務包後，您必須將**編輯 CSE:NATIVECLUSTER** 權限新增至要建立和修改原生叢集的角色。如果還想讓使用者刪除叢集，則必須將**完全控制 CSE:NATIVECLUSTER** 權限新增至角色。此外，您可以將管理員權限指派給想要檢視組織中所有 Tanzu Kubernetes 叢集的使用者，或想要跨站台管理叢集的使用者。如需執行階段定義的實體 (RDE) 的權限和存取層級的相關資訊，請參閱第 14 章 管理定義的實體。

4 如果要向承租人授與建立和管理 TKGI 叢集的權限，則必須將 **{cse}:PKS DEPLOY RIGHT** 發佈到特定組織，然後將 **{cse}:PKS DEPLOY RIGHT** 權限新增至要建立和管理 TKGI 叢集的角色。**{cse}:PKS DEPLOY RIGHT** 是在 Container Service Extension 伺服器安裝期間建立的。

5 對於原生叢集，透過建立存取控制清單 (ACL) 項目向承租人或系統管理員授與存取權。如需有關共用執行階段定義的實體 (RDE) 的詳細資訊，請參閱共用定義的實體。

6 建立原生 Kubernetes 叢集或建立 VMware Tanzu Kubernetes Grid Integrated Edition 叢集。

新增組織 VDC Kubernetes 原則

您可以使用提供者 VDC Kubernetes 原則新增組織 VDC Kubernetes 原則。承租人可以使用組織 VDC Kubernetes 原則來建立 Tanzu Kubernetes 叢集。

將提供者 VDC Kubernetes 原則新增或發佈到組織 VDC 時，您可以將該原則提供給承租人使用。承租人可以使用可用的組織 VDC Kubernetes 原則，在建立 Tanzu Kubernetes 叢集時利用 Kubernetes 容量。Kubernetes 原則將封裝放置、基礎結構品質，以及持續性磁碟區儲存區類別。Kubernetes 原則可以有不同的計算限制。

可以將多個組織 VDC Kubernetes 原則新增至單一組織 VDC。可以使用單一提供者 VDC Kubernetes 原則來建立多個組織 VDC Kubernetes 原則。可以使用組織 VDC Kubernetes 原則作為服務品質的指標。例如，您可以發佈 Gold Kubernetes 原則以允許選取保證的機器類別和快速儲存區類別，或發佈 Silver Kubernetes 原則以允許選取最佳運作的機器類別和緩慢儲存區類別。

必要條件

- 確認您的環境中至少有一個 Flex 組織 VDC。請參閱建立組織虛擬資料中心。
- 確認您的環境中至少有一個受主管叢集支援的提供者 VDC。主管叢集支援的提供者 VDC 在**提供者 VDC** 索引標籤上標有 Kubernetes 圖示。如需有關 VMware Cloud Director 中 vSphere with VMware Tanzu 的詳細資訊，請參閱將 Kubernetes 與 VMware Cloud Director 搭配使用。
- 自行熟悉 Tanzu Kubernetes 叢集的虛擬機器類別類型。請參閱 vSphere 說明文件中的《vSphere with Kubernetes 組態和管理》指南。

程序

1. 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。
2. 在左面板中，選取**組織 VDC**，然後按一下 Flex 組織 VDC 的名稱。
3. 在 [原則] 下，選取 **Kubernetes**，然後按一下**新增**。

   發佈至組織 VDC 精靈隨即顯示。
4. 輸入組織 VDC Kubernetes 原則的承租人可見名稱和說明，然後按**下一步**。
5. 選取要使用的提供者 VDC Kubernetes 原則，然後按**下一步**。
6. 針對在此原則下建立的 Tanzu Kubernetes 叢集選取 CPU 和記憶體限制。

   最大限制取決於組織 VDC 的 CPU 和記憶體配置。新增原則時，所選限制將用作承租人的上限。
7. 選擇是否要為此原則中建立的 Tanzu Kubernetes 叢集節點保留 CPU 和記憶體，然後按**下一步**。

   每個類別類型有兩個版本：保證版本和最佳運作版本。保證類別版本會完全保留其已設定的資源，而最佳運作版本則允許過度認可資源。視您的選擇而定，您可以在精靈的下一頁上選取保證版本或最佳運作版本的虛擬機器類別類型。
   - 對於保證版本的虛擬機器類別類型，選取**是**以完整保留 CPU 和記憶體。
   - 對於最佳運作版本的虛擬機器類別類型，選取**否**以便不保留 CPU 和記憶體。
8. 在精靈的**機器類別**頁面上，選取一或多個適用於此原則的虛擬機器類別類型。

   選取的機器類別是您將原則新增至組織 VDC 時，承租人可用的唯一類別類型。
9. 選取一或多個儲存區原則。
10. 檢閱您的選擇，然後按一下**發佈**。

結果

已發佈原則的相關資訊隨即顯示在 Kubernetes 原則清單中。已發佈原則將使用原則中指定的資源限制在主管叢集上建立主管命名空間。

承租人可以開始使用 Kubernetes 原則來建立 Tanzu Kubernetes 叢集。VMware Cloud Director 會將在此 Kubernetes 原則下建立的每個 Tanzu Kubernetes 叢集放置在相同的主管命名空間中。原則資源限制將成為主管命名空間的資源限制。主管命名空間中所有承租人建立的 Tanzu Kubernetes 叢集會在這些限制內爭用資源。

後續步驟

管理組織的資源耗用量配額

編輯組織 VDC Kubernetes 原則

您可以修改組織 VDC Kubernetes 原則，以變更其說明及 CPU 和記憶體限制。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，選取**組織 VDC**，然後按一下 Flex 組織 VDC 的名稱。

3 在 [原則] 下，選取 **Kubernetes**，選取要編輯的原則，然後按一下**編輯**。

編輯 VDC Kubernetes 原則精靈隨即顯示。

4 編輯組織 VDC Kubernetes 原則的說明，然後按**下一步**。

原則的名稱會連結至在原則發佈期間建立的主管命名空間，您無法對其進行變更。

5 編輯組織 VDC Kubernetes 原則的 CPU 和記憶體限制，然後按**下一步**。

您無法編輯 CPU 和記憶體保留。

6 檢閱新原則詳細資料，然後按一下**儲存**。

建立 Tanzu Kubernetes 叢集

可以使用 Kubernetes Container Clusters 外掛程式建立 Tanzu Kubernetes 叢集。

如需有關用於叢集建立的不同 Kubernetes 執行階段選項的詳細資訊，請參閱將 Kubernetes 與 VMware Cloud Director 搭配使用。

此外，還可以使用 Container Service Extension CLI 管理 Kubernetes 叢集。請參閱 Container Service Extension 說明文件。

VMware Cloud Director 使用已啟用的 PodSecurityPolicy 許可控制器佈建 Tanzu Kubernetes 叢集。您必須建立網繭安全性原則來部署工作負載。如需在 Kubernetes 中實現使用網繭安全性原則的相關資訊，請參閱《vSphere with Kubernetes 組態和管理》指南中的〈對 Tanzu Kubernetes 叢集使用網繭安全性原則〉主題。

必要條件

- 將 Kubernetes Container Clusters 外掛程式發佈到您想要管理 Tanzu Kubernetes 叢集的任何組織。
- 確認您的組織 VDC 中至少有一個組織 VDC Kubernetes 原則。若要新增組織 VDC Kubernetes 原則，請參閱新增組織 VDC Kubernetes 原則。
- 您必須將 **vmware:tkgcluster 權利**權限服務包發佈到要使用叢集的任何組織。共用權限服務包後，您必須將**編輯：Tanzu Kubernetes 客體叢集**權限新增至要建立和修改 Tanzu Kubernetes 叢集的角色。如果還想讓使用者刪除叢集，則必須將**完全控制：Tanzu Kubernetes 客體叢集**權限新增至角色。此外，您可以將管理員權限指派給想要檢視組織中所有 Tanzu Kubernetes 叢集的使用者，或想要跨站台管理叢集的使用者。如需執行階段定義的實體 (RDE) 的權限和存取層級的相關資訊，請參閱第 14 章 管理定義的實體。
- 透過建立存取控制清單 (ACL) 項目向承租人或系統管理員授與存取權。如需有關共用執行階段定義的實體 (RDE) 的詳細資訊，請參閱共用定義的實體。

程序

1 從頂部導覽列中，選取**更多 > Kubernetes Container Clusters**。

2 (選擇性) 如果組織 VDC 已啟用 TKGI 叢集建立，請在 **Kubernetes Container Clusters** 頁面上，選取 **vSphere with Tanzu 與原生**索引標籤。

3 按一下**新增**。

4 選取 **vSphere with Tanzu** 執行階段選項，然後按**下一步**。

5 輸入新 Kubernetes 叢集的名稱，然後按**下一步**。

6 選取要將 Tanzu Kubernetes 叢集發佈到的組織 VDC，然後按**下一步**。

7 選取組織 VDC Kubernetes 原則和 Kubernetes 版本，然後按**下一步**。

VMware Cloud Director 會顯示未繫結到任何組織 VDC 或 Kubernetes 原則的預設 Kubernetes 版本集。這些版本是全域設定。若要變更可用版本的清單，請使用儲存格管理工具執行 `./cell-management-tool manage-config --name wcp.supported.kubernetes.versions -v` *`version_numbers`* 命令，以逗號分隔版本號碼。

8 選取新叢集中的控制平面和 worker 節點數目。

9 選取控制平面和 worker 節點的機器類別，然後按**下一步**。

10 為控制平面和 worker 節點選取 Kubernetes 原則儲存區類別，然後按**下一步**。

11 (選擇性) 對於 VMware Cloud Director 10.2.2 及更新版本，指定 Kubernetes 服務的 IP 位址範圍和 Kubernetes 網繭的範圍，然後按**下一步**。

無類別網域間路由 (CIDR) 是一種 IP 路由和 IP 位址配置方法。

選項	描述
Pods CIDR	指定要用於 Kubernetes 網繭的 IP 位址範圍。預設值為 192.168.0.0/16。網繭子網路大小必須等於或大於 /24。此值不得與主管叢集設定重疊。您可以輸入一個 IP 範圍。
Services CIDR	指定要用於 Kubernetes 服務的 IP 位址範圍。預設值為 10.96.0.0/12。此值不得與主管叢集設定重疊。您可以輸入一個 IP 範圍。

12 檢閱叢集設定，然後按一下**完成**。

後續步驟

- 如果您想要變更 worker 節點的數目，請調整 Kubernetes 叢集的大小。
- 下載 kubeconfig 檔案。kubectl 命令列工具使用 kubeconfig 檔案來取得叢集、使用者、命名空間和驗證機制的相關資訊。
- 刪除 Kubernetes 叢集。

建立原生 Kubernetes 叢集

可以使用 Kubernetes Container Clusters 外掛程式建立 Container Service Extension 3.0 管理的 Kubernetes 叢集。

如需有關用於叢集建立的不同 Kubernetes 執行階段選項的詳細資訊，請參閱將 Kubernetes 與 VMware Cloud Director 搭配使用。

此外，還可以使用 Container Service Extension CLI 管理 Kubernetes 叢集。請參閱 Container Service Extension 說明文件。

必要條件

- 確認您的服務提供者已向您的組織發佈 Kubernetes Container Clusters 外掛程式。Kubernetes Container Clusters 是適用於 VMware Cloud Director 的 Container Service Extension 外掛程式。您可以在頂部導覽列上的**更多 > Kubernetes Container Clusters** 下找到此外掛程式。
- 若要針對原生 Kubernetes 叢集部署啟用組織 VDC，請設定 Container Service Extension 伺服器。請參閱 Container Service Extension (CSE) 說明文件中的 CSE 伺服器管理一章。
- 將在 CSE 伺服器設定期間建立的 CSE 原生原則發佈到組織 VDC。若要運用使用者介面，請參閱將虛擬機器放置原則新增至組織 VDC。或者，您可以使用 CSE 3.0 CLI 來發佈原則，方法是執行 `vcd cse ovdc enable Organization_VDC_Name --org Organization _Name --native` 命令。
- 您必須將 **cse:nativeCluster 權利**權限服務包發佈到要使用原生叢集的任何組織。共用權限服務包後，您必須將**編輯 CSE:NATIVECLUSTER** 權限新增至要建立和修改 Tanzu Kubernetes 叢集的角色。如果還想讓使用者刪除叢集，則必須將**完全控制 CSE:NATIVECLUSTER** 權限新增至角色。此外，您可以將管理員權限指派給想要檢視組織中所有 Tanzu Kubernetes 叢集的使用者，或想要跨站台管理叢集的使用者。如需執行階段定義的實體 (RDE) 的權限和存取層級的相關資訊，請參閱第 14 章 管理定義的實體。

- 透過建立存取控制清單 (ACL) 項目向承租人或系統管理員授與存取權。如需有關共用執行階段定義的實體 (RDE) 的詳細資訊，請參閱共用定義的實體。

程序

1 從頂部導覽列中，選取**更多** > **Kubernetes Container Clusters**。

2 (選擇性) 如果組織 VDC 已啟用 TKGI 叢集建立，請在 **Kubernetes Container Clusters** 頁面上，選取 **vSphere with Tanzu 與原生**索引標籤。

3 按一下**新增**。

4 選取**原生** Kubernetes 執行階段選項。

5 輸入名稱，然後從清單中選取 Kubernetes 範本。

6 (選擇性) 輸入新 Kubernetes 叢集的說明和 SSH 公開金鑰。

7 按**下一步**。

8 選取要將原生叢集發佈到的組織 VDC，然後按**下一步**。

9 為節點選取控制平面和 worker 節點的數目，並選擇性地選取大小調整原則。

10 按**下一步**。

11 如果您想要使用 NFS 軟體部署其他虛擬機器，請開啟**啟用 NFS** 切換按鈕。

12 (選擇性) 為控制平面和 worker 節點選取儲存區原則。

13 按**下一步**。

14 選取 Kubernetes 叢集的網路，然後按**下一步**。

15 檢閱叢集設定，然後按一下**完成**。

後續步驟

- 如果您想要變更 worker 節點的數目，請調整 Kubernetes 叢集的大小。
- 下載 kubeconfig 檔案。kubectl 命令列工具使用 kubeconfig 檔案來取得叢集、使用者、命名空間和驗證機制的相關資訊。
- 刪除 Kubernetes 叢集。

建立 VMware Tanzu Kubernetes Grid Integrated Edition 叢集

您可以使用 Container Service Extension 建立 VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) 叢集。

如需有關用於叢集建立的不同 Kubernetes 執行階段選項的詳細資訊，請參閱將 Kubernetes 與 VMware Cloud Director 搭配使用。

此外，還可以使用 Container Service Extension CLI 管理 Kubernetes 叢集。請參閱 Container Service Extension 說明文件。

透過使用 TKGI 啟用中繼資料，您可以提供對承租人的存取權，以建立 TKGI 叢集並存取已啟用 TKGI 的組織 VDC。如果您想要限制承租人建立 TKGI 叢集的能力，可以僅提供對組織 VDC 的存取權。在此情況下，承租人可以管理現有的 TKGI 叢集，但無法建立新叢集。

必要條件

- 確認您的服務提供者已向您的組織發佈 Kubernetes Container Clusters 外掛程式。Kubernetes Container Clusters 是適用於 VMware Cloud Director 的 Container Service Extension 外掛程式。您可以在頂部導覽列上的**更多 > Kubernetes Container Clusters** 下找到此外掛程式。
- 若要針對 TKGI Kubernetes 叢集部署啟用組織 VDC，請設定 Container Service Extension 伺服器。如需使用 CSE CLI 為 TKGI 啟用組織 VDC 的相關資訊，請參閱 Container Service Extension (CSE) 說明文件中的 CSE 伺服器管理一章。
- 如果您要向承租人提供 TKGI 建立和管理的權限，則必須將 **{cse}:PKS DEPLOY RIGHT** 發佈到特定組織，然後將 **{cse}:PKS DEPLOY RIGHT** 權限新增至要建立和管理 TKGI 叢集的角色。**{cse}:PKS DEPLOY RIGHT** 是在 Container Service Extension 伺服器安裝期間建立的。

程序

1. 從頂部導覽列中，選取**更多 > Kubernetes Container Clusters**。
2. 在 **Kubernetes Container Clusters** 頁面上，選取 **TKGI** 索引標籤，然後按一下**新增**。

   建立新 TKGI 叢集精靈隨即開啟。
3. 選取要將 TKGI 叢集發佈到的組織 VDC，然後按**下一步**。

   此清單可能需要較長時間才能載入，因為 VMware Cloud Director 會從 CSE 伺服器請求資訊。
4. 輸入新 TKGI 叢集的名稱，然後選取 worker 節點的數目。

   TKGI 叢集必須至少有一個 worker 節點。
5. 按**下一步**。
6. 檢閱叢集設定，然後按一下**完成**。
7. (選擇性) 按一下頁面右側的**重新整理**按鈕，使新 TKGI 叢集出現在叢集清單中。

後續步驟

- 如果您想要變更 worker 節點的數目，請調整 Kubernetes 叢集的大小。
- 下載 kubeconfig 檔案。kubectl 命令列工具使用 kubeconfig 檔案來取得叢集、使用者、命名空間和驗證機制的相關資訊。
- 刪除 Kubernetes 叢集。

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 (VDC)。組織虛擬資料中心從提供者 VDC 取得其資源。一個組織可以具有多個組織 VDC。

必要條件

建立提供者 VDC。請參閱建立提供者虛擬資料中心。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，按一下**組織 VDC**，然後按一下**新增**。

3 為新的組織 VDC 輸入名稱，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 VDC，請關閉**啟用組織 VDC** 切換按鈕。

使用者無法在已停用的組織 VDC 上部署 vApp。

5 按**下一步**。

6 選取要新增此 VDC 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 VDC 從中取得計算和儲存資源的提供者 VDC 名稱旁邊的選項按鈕，然後按**下一步**。

提供者 VDC 清單顯示站台中所有啟用的提供者 VDC，以及有關可用資源的資訊。網路清單顯示可供選取的提供者 VDC 使用的網路相關資訊。

8 為此組織 VDC 選取配置模型，然後按**下一步**。

選項	描述
配置集區	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。
隨收隨付	僅當使用者在組織 VDC 中建立 vApp 時才會認可資源。
保留集區	您配置的所有資源會立即認可給組織 VDC。
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額外負荷	包含或排除記憶體額外負荷。	Flex
CPU 配置	您想要配置給在此組織 VDC 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 VDC 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 VDC 的 CPU 耗用量上限。	■ 隨收隨付 ■ Flex

選項	描述	配置模型
保證的 CPU 資源	您想要保證配置給在此組織 VDC 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，百分比保證還決定為此組織 VDC 認可百分之多少的 CPU 配置。	■ 配置集區 ■ 隨收隨付 ■ Flex
vCPU 速度	vCPU 速度。執行於組織 VDC 中的虛擬機器會分配到這麼多 GHz (每 CPU)。	■ 隨收隨付 ■ Flex
記憶體配置	您想要配置給在此組織 VDC 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 VDC 的記憶體耗用量上限。	■ 隨收隨付 ■ Flex
保證的記憶體資源	您想要保證配置給在此組織 VDC 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，百分比保證還決定為此組織 VDC 認可百分之多少的記憶體配置。	■ 配置集區 ■ 隨收隨付 ■ Flex
虛擬機器數目上限	可存在於組織 VDC 中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 VDC 進行儲存區設定，然後按**下一步**。

此清單中包含來源提供者 VDC 上已啟用的儲存區原則。

a 選取您想要新增到此組織 VDC 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。

VMware Cloud 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 VDC 中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 VDC 中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 VDC 進行網路集區設定，然後按**下一步**。

VMware Cloud Director 使用網路集區來建立 vApp 網路及內部組織 VDC 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 VDC 的配額。

  配額是指此網路集區支援的組織 VDC 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。

備註 NSX-T Data Center 支援的組織 VDC 僅支援 Geneve 網路集區。

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 從頂部導覽列中，選取**資源**，然後按一下**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 從頂部導覽列中，選取**資源**，然後按一下**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。

管理虛擬資料中心範本

從 VMware Cloud Director 10.2.2 開始，可以建立虛擬資料中心 (VDC) 範本並將其與承租人組織共用，以便**組織管理員**可以使用這些範本建立 VDC。

透過建立 VDC 範本並將其與組織共用，您可以啟用組織 VDC 的自助佈建，同時保留對系統資源 (例如提供者 VDC 和外部網路) 配置的管理控制。

VDC 範本會指定新組織 VDC 的配置模型、記憶體、CPU 資源組態和儲存區原則，並選擇性地指定 Edge 閘道和組織 VDC 網路。

建立組織虛擬資料中心範本

從 VMware Cloud Director 10.2.2 開始，可以使用 HTML5 使用者介面為 NSX Data Center for vSphere 或 NSX-T Data Center 支援的 VDC 建立組織虛擬資料中心 (VDC) 範本。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，選取**組織 VDC 範本**，然後按一下**新增**。

3 選取網路提供者類型，選取提供者 VDC 和外部網路配對，然後按**下一步**。

對於 NSX Data Center for vSphere，當使用者從此範本具現化組織 VDC 時，VMware Cloud Director 會將選取的 Edge 叢集套用至新組織 VDC。新組織 VDC 內所有新部署的 Edge 閘道都會使用這些主要和次要 Edge 叢集作為放置。

對於 NSX-T Data Center，VMware Cloud Director 會使用**服務 Edge 叢集**部署網路服務，例如 DHCP、VPN 和 DNS 服務。VMware Cloud Director 使用**適用於 NSX-T 閘道的 Edge 叢集**部署閘道。

具現化組織 VDC 範本後，無法編輯 Edge 叢集。

4 為此組織 VDC 選取配置模型，然後按**下一步**。

選項	描述
配置集區	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。
隨收隨付	僅當使用者在組織 VDC 中建立 vApp 時才會認可資源。
保留集區	您配置的所有資源會立即認可給組織 VDC。
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。

5 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額外負荷	包含或排除記憶體額外負荷。	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

選項	描述	配置模型
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
記憶體限制	此組織虛擬資料中心的記憶體耗用量上限。	■ 隨收隨付 ■ Flex
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

6 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 VDC 上已啟用的儲存區原則。

a 選取要新增至此組織 VDC 的一或多個儲存區原則。

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。

VMware Cloud 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 VDC 中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 VDC 中的虛擬機器停用快速佈建，請關閉**快速佈建**切換按鈕。

7 (選擇性) 建立 Edge 閘道。

a 輸入新 Edge 閘道的名稱，並選擇性地輸入說明。

b 如果要為 NSX Data Center for vSphere 支援的 VDC 建立範本，您可以自訂一般 Edge 閘道設定，然後按**下一步**。

一般設定	**描述**
分散式路由	設定進階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。

c 如果要為 NSX Data Center for vSphere 支援的 VDC 建立範本，您可以變更系統資源的 Edge 閘道組態。

組態	**描述**
精簡	需要較少的記憶體和計算資源。
大型	相較於精簡組態，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。

d (選擇性) 指定為使用閘道服務而配置的 IP 數目。

8 設定組織 VDC 網路，然後按**下一步**。

a 輸入網路的名稱，並選擇性地輸入說明。

b 針對網路輸入無類別網域間路由 (CIDR) 設定。

使用格式 *network_gateway_IP_address*/*subnet_prefix_length*，例如 **192.167.1.1/24**。

c 若要使組織 VDC 網路可供相同組織內的其他組織 VDC 使用，請開啟**共用**切換按鈕。

一種可能的使用案例為，如果組織 VDC 內的應用程式具有設定為配置模型的保留區或配置集區。在此情況下，可能沒有足夠的空間來執行更多虛擬機器。以下方法可作為解決方案，即透過隨收隨付模型建立次要組織 VDC，並暫時在該網路上執行更多虛擬機器。

備註 組織 VDC 必須共用相同的網路集區。

9 從可用靜態 IP 集區的範圍新增 IP 位址範圍，然後按**下一步**。

10 (選擇性) 為此組織 VDC 進行網路集區設定，然後按**下一步**。

配額是指此網路集區支援的組織 VDC 內已佈建網路的數目上限。配額不得超過所選網路集區的可用網路數目。

11 選取要從此範本中檢視和具現化 VDC 的組織，然後按**下一步**。

系統管理員可以從任何組織 VDC 範本具現化 VDC。透過使用 VMware Cloud Director Tenant Portal，如果**組織管理員**的組織在範本的存取清單中，則組織管理員可以具現化 VDC。

12 輸入範本的系統名稱和面向承租人的名稱，然後按**下一步**。

13 檢閱組織 VDC 範本組態，然後按一下**完成**。

後續步驟

- 從範本具現化虛擬資料中心.
- 編輯組織 VDC 範本.您可以編輯現有 VDC 範本的所有內容，但網路提供者類型除外。
- 若要建立可選擇性自訂的組織 VDC 範本的複本，請複製該範本。複製步驟與範本編輯步驟類似。
- 刪除組織 VDC 範本。

從範本具現化虛擬資料中心

若要從 VDC 範本建立組織虛擬資料中心 (VDC)，請具現化 VDC。

系統管理員可以從任何組織 VDC 範本具現化 VDC。透過使用 VMware Cloud Director Tenant Portal，如果**組織管理員**的組織在範本的存取清單中，則組織管理員可以具現化 VDC。

必要條件

建立組織虛擬資料中心範本

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，選取**組織 VDC 範本**。

3 選取組織 VDC 範本，然後按一下**具現化 VDC**。

4 輸入新組織虛擬資料中心的名稱，並選擇性地輸入說明。

5 為組織 VDC 選取組織，然後按一下**建立**。

編輯組織 VDC 範本

您可以修改現有虛擬資料中心 (VDC) 範本的所有內容，但網路提供者類型除外。

必要條件

建立組織虛擬資料中心範本

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，選取**組織 VDC 範本**，然後按一下**編輯**。

3 選取提供者 VDC 和外部網路配對，然後按**下一步**。

對於 NSX Data Center for vSphere，當使用者從此範本具現化組織 VDC 時，VMware Cloud Director 會將選取的 Edge 叢集套用至新組織 VDC。新組織 VDC 內所有新部署的 Edge 閘道都會使用這些主要和次要 Edge 叢集作為放置。

對於 NSX-T Data Center，VMware Cloud Director 會使用**服務 Edge 叢集**部署網路服務，例如 DHCP、VPN 和 DNS 服務。VMware Cloud Director 使用**適用於 NSX-T 閘道的 Edge 叢集**部署閘道。

具現化組織 VDC 範本後，無法編輯 Edge 叢集。

4 為此組織 VDC 選取配置模型，然後按**下一步**。

選項	描述
配置集區	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。
隨收隨付	僅當使用者在組織 VDC 中建立 vApp 時才會認可資源。
保留集區	您配置的所有資源會立即認可給組織 VDC。
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。

5 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額外負荷	包含或排除記憶體額外負荷。	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
記憶體限制	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

6 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 VDC 上已啟用的儲存區原則。

a 選取要新增至此組織 VDC 的一或多個儲存區原則。

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。

VMware Cloud 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 VDC 中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 VDC 中的虛擬機器停用快速佈建，請關閉**快速佈建**切換按鈕。

7 (選擇性) 建立 Edge 閘道。

a 輸入新 Edge 閘道的名稱，並選擇性地輸入說明。

b 如果要為 NSX Data Center for vSphere 支援的 VDC 編輯範本，您可以自訂一般 Edge 閘道設定，然後按**下一步**。

一般設定	描述
分散式路由	設定進階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。

c 如果要為 NSX Data Center for vSphere 支援的 VDC 編輯範本，您可以變更系統資源的 Edge 閘道組態。

組態	描述
精簡	需要較少的記憶體和計算資源。
大型	相較於精簡組態，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。

d (選擇性) 指定為使用閘道服務而配置的 IP 數目。

8 設定組織 VDC 網路，然後按**下一步**。

a 輸入網路的名稱，並選擇性地輸入說明。

b 針對網路輸入無類別網域間路由 (CIDR) 設定。

使用格式 *network_gateway_IP_address*/*subnet_prefix_length*，例如 **192.167.1.1/24**。

c 若要使組織 VDC 網路可供相同組織內的其他組織 VDC 使用，請開啟**共用**切換按鈕。

一種可能的使用案例為，如果組織 VDC 內的應用程式具有設定為配置模型的保留區或配置集區。在此情況下，可能沒有足夠的空間來執行更多虛擬機器。以下方法可作為解決方案，即透過隨收隨付模型建立次要組織 VDC，並暫時在該網路上執行更多虛擬機器。

備註 組織 VDC 必須共用相同的網路集區。

9 從可用靜態 IP 集區的範圍新增 IP 位址範圍，然後按**下一步**。

10 (選擇性) 為此組織 VDC 進行網路集區設定，然後按**下一步**。

配額是指此網路集區支援的組織 VDC 內已佈建網路的數目上限。配額不得超過所選網路集區的可用網路數目。

11 選取要從此範本中檢視和具現化 VDC 的組織，然後按**下一步**。

12 輸入範本的系統名稱和面向承租人的名稱，然後按**下一步**。

13 檢閱組織 VDC 範本組態，然後按一下**完成**。

修改組織虛擬資料中心的名稱和說明

隨著 VMware Cloud 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 從頂部導覽列中，選取**資源**，然後按一下**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 從頂部導覽列中，選取**資源**，然後按一下**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。

對組織虛擬資料中心的儲存區原則啟用虛擬機器加密

您可以將已啟用加密的儲存區原則新增至組織 VDC。您可以將虛擬機器或磁碟與具有虛擬機器加密功能的儲存區原則相關聯，以加密虛擬機器和磁碟。

從 VMware Cloud Director 10.1 開始，您可以使用虛擬機器加密來提高資料的安全性。加密不僅可以保護虛擬機器，還可以保護虛擬機器磁碟和其他檔案。您可以在 API 和使用者介面中檢視儲存區原則的功能，以及虛擬機器和磁碟的加密狀態。您可以在加密的虛擬機器和磁碟上執行相應 vCenter Server 版本中支援的所有作業。

如果提供者 VDC 具有已啟用虛擬機器加密的儲存區原則，您可以將已啟用加密的原則新增至組織 VDC。請參閱對提供者虛擬資料中心的儲存區原則啟用虛擬機器加密和將虛擬機器儲存區原則新增至組織虛擬資料中心。之後，透過使用 VMware Cloud Director Tenant Portal，承租人可將虛擬機器或磁碟與已啟用虛擬機器加密的儲存區原則相關聯。

虛擬機器加密限制

VMware Cloud Director10.1 中不支援下列動作。

- 加密或解密已開啟電源的虛擬機器或其磁碟。
- 匯出已加密虛擬機器的 OVF。
- 使用快照加密和解密虛擬機器的磁碟 (如果磁碟屬於快照的一部分)。
- 在虛擬機器的磁碟位於加密原則上時解密虛擬機器。
- 將已加密的磁碟新增至未加密的虛擬機器。
- 在未加密的虛擬機器上加密現有磁碟。

- 將已加密的具名磁碟新增至未加密的虛擬機器。
- 建立加密的連結複製。
- 加密連結複製虛擬機器或其磁碟。
- 在來源虛擬機器已加密時，在 vCenter Server 執行個體之間具現化、移動或複製虛擬機器。

備註 在快速佈建的組織 VDC 上，如果來源或目標虛擬機器已加密，且您想要建立複製，VMware Cloud Director 一律會建立完整複製。

識別虛擬機器加密儲存區功能

依預設，**系統管理員**和**組織管理員**具有檢視組織 VDC 儲存區功能，以及虛擬機器和磁碟是否加密的必要權限。**vApp 作者**可以檢視虛擬機器和磁碟的加密狀態。如需有關角色和權限的詳細資訊，請參閱預先定義的角色與其權限。

您可以在**資源 > vSphere 資源 > 儲存區原則**下的**功能**資料行中檢視所有儲存區功能。此資料行顯示虛擬機器加密、以標籤為基礎的關聯、vSAN，以及 IOPS 限制儲存區功能。若要檢視儲存區功能的完整清單，請按一下儲存區原則名稱左側的箭頭以展開資料列。

您也可以在組織 VDC 的**儲存區**索引標籤中檢視儲存區功能資訊。

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. 從頂部導覽列中，選取**資源**，然後按一下**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**原則**下，選取**儲存區**，然後按一下**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 從頂部導覽列中，選取**資源**，然後按一下**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**原則**下，選取**儲存區**，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。

VMware Cloud 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 從頂部導覽列中，選取**資源**，然後按一下**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**原則**下，選取**儲存區**。

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 從頂部導覽列中，選取**資源**，然後按一下**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**原則**下，選取**儲存區**。

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 從頂部導覽列中，選取**資源**，然後按一下**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**原則**下，選取**儲存區**。

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 從頂部導覽列中，選取**資源**，然後按一下**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**原則**下，選取**儲存區**。

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 從頂部導覽列中，選取**資源**，然後按一下**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**原則**下，選取**儲存區**。

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 VDC 儲存區原則設定

您可以變更組織 VDC 儲存區原則的每秒 I/O 作業數 (IOPS) 設定。依預設，組織 VDC 儲存區原則會繼承提供者 VDC 儲存區原則設定。您可以自訂每個組織 VDC 儲存區原則的設定。

必要條件

將虛擬機器儲存區原則新增至組織虛擬資料中心

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

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

3 在**原則**下，選取**儲存區**。

4 按一下目標儲存區原則旁邊的選項按鈕，然後按一下**編輯設定**。

5 如果您希望組織 VDC 儲存區原則的 IOPS 設定與提供者 VDC 儲存區原則不同，請關閉**從提供者 VDC 繼承**切換按鈕。

6 如果您想要限制每秒 I/O 作業數，請開啟**已啟用 IOPS 限制**切換按鈕。

7 如果您想要在放置期間考慮 IOPS，請開啟**影響放置**切換按鈕。

如果**影響放置**切換按鈕已開啟，VMware Cloud Director 會在資料存放區之間提供 IOPS 負載平衡。設定磁碟的 IOPS 設定時，VMware Cloud Director 會考慮具有足夠 IOPS 容量用於所選磁碟的資料存放區。如果**影響放置**切換按鈕已關閉，則不需要為每個資料存放區設定 IOPS 容量，並且您可以使用 Storage DRS 叢集。

8 (選擇性) 設定最大和預設 IOPS 設定。

9 按一下**儲存**。

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 從頂部導覽列中，選取**資源**，然後按一下**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。

備註 NSX-T Data Center 支援的組織 VDC 僅支援 Geneve 網路集區。

- 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 VMware Cloud 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《VMware Cloud Director 租用戶入口網站指南》。

設定跨虛擬資料中心網路

透過跨虛擬資料中心網路功能，具有多個 vCenter Server 執行個體所支援的虛擬資料中心的組織能夠跨最多四個虛擬資料中心延伸第 2 層網路。跨虛擬資料中心網路取決於跨 vCenter NSX，並且可以跨越多個 VMware Cloud Director 站台。

跨虛擬資料中心網路需要 NSX Data Center for vSphere。

透過跨虛擬資料中心網路，組織可以將最多四個虛擬資料中心進行分組，並在每個群組中設定出口和第 2 層延伸網路。

參與組織虛擬資料中心可以屬於不同的 VMware Cloud Director 站台。請參閱設定和管理多站台部署。

組織可以使用跨虛擬資料中心網路實作高可用性解決方案或分散式系統架構 (也就是一個應用程式可以散佈在多個虛擬資料中心或站台上)。

系統管理員必須設定基礎跨 vCenter NSX 環境和 VMware Cloud Director 伺服器，並為每個虛擬資料中心啟用跨虛擬資料中心網路。

1 將某個 NSX Manager 執行個體設定為主要 NSX Manager 執行個體。請參閱《跨 vCenter NSX 安裝指南》。
   a 在主要 NSX Manager 執行個體上部署 NSX 叢集。
   b 準備主要 NSX Manager 執行個體上的 ESXi 主機。
   c 從主要 NSX Manager 執行個體設定 VXLAN。
   d 為 NSX Manager 執行個體指派主要角色。
   e 為通用傳輸區域的區段 IP 建立集區。
   f 新增通用傳輸區域。
2 將剩餘的 NSX Manager 執行個體設定為次要 NSX Manager。請參閱《跨 vCenter NSX 安裝指南》。
   a 準備每個次要 NSX Manager 執行個體上的 ESXi 主機。
   b 從每個次要 NSX Manager 執行個體設定 VXLAN。
   c 為每個 NSX Manager 執行個體指派次要角色。
   d 將 ESXi 叢集連線至通用傳輸區域。
3 設定每個 NSX Manager 執行個體的控制虛擬機器內容。請參閱修改 NSX Manager 設定。

4 從任何 vCenter Server 執行個體使用通用類型傳輸區域建立支援 VXLAN 的網路集區。請參閱建立 NSX Data Center for vSphere 傳輸區域支援的網路集區。

備註 對於多站台部署，您必須在每個 VMware Cloud Director 站台上建立支援 VXLAN 的網路集區。

5 在每個組織虛擬資料中心上啟用跨虛擬資料中心網路。請參閱編輯組織虛擬資料中心的網路設定。

6 如果組織具有多站台虛擬資料中心，請確認不同 VMware Cloud Director 站台上的安裝識別碼都不相同。如果有 VMware Cloud Director 站台設定了相同的安裝識別碼，請參閱《VMware Cloud Director 安裝、設定與升級指南》中的〈針對多站台延伸網路重新產生 MAC 位址〉。

組織管理員現在可以建立並設定資料中心群組、出口和延伸網路。如需管理跨虛擬資料中心網路的相關資訊，請參閱《VMware Cloud 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 從頂部導覽列中，選取**資源**，然後按一下**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 從頂部導覽列中，選取**資源**，然後按一下**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。

VMware Cloud 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 NSX Data Center for vSphere Edge 閘道防火牆。

啟用組織虛擬資料中心上的分散式防火牆

必須在組織虛擬資料中心上啟用分散式防火牆，才能在此組織虛擬資料中心上管理分散式防火牆設定。

VMware Cloud 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 從頂部導覽列中，選取**資源**，然後按一下**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**分散式防火牆 > 一般**索引標籤上，開啟**啟用分散式防火牆**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**分散式防火牆 > 一般**索引標籤上，您可以查看第 3 層流量的預設分散式防火牆規則，名為 Default Allow Rule。
- 在**分散式防火牆 > 乙太網路**索引標籤上，您可以看到第 2 層流量的預設分散式防火牆規則的名稱為 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分散式防火牆
- 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 從頂部導覽列中，選取**資源**，然後按一下**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。

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。

重要 IP 位址群組 (IP 集)、MAC 位址群組 (MAC 集) 以及包含 IP 集或 MAC 集的安全群組不是有效的輸入參數。

14 按一下**儲存變更**。

編輯分散式防火牆規則

在 VMware Cloud Director 環境中，若要修改組織虛擬資料中心的現有分散式防火牆規則，請使用**分散式防火牆**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 從頂部導覽列中，選取**資源**，然後按一下**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分散式防火牆規則：

- 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

VMware Cloud 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 的分散式防火牆設定	a 從頂部導覽列的**資源**下，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 從頂部導覽列的**資源**下，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 的分散式防火牆設定	a 從頂部導覽列的**資源**下，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 從頂部導覽列的**資源**下，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 的分散式防火牆設定	a 從頂部導覽列的**資源**下，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 從頂部導覽列的**資源**下，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 的分散式防火牆設定	a 從頂部導覽列的**資源**下，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 從頂部導覽列的**資源**下，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 從頂部導覽列中，選取**資源**，然後按一下**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 若要保留變更，請按一下**保留**。

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 從頂部導覽列中，選取**資源**，然後按一下**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 從頂部導覽列中，選取**資源**，然後按一下**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 從頂部導覽列中，選取**資源**，然後按一下**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 從頂部導覽列中，選取**資源**，然後按一下**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 從頂部導覽列中，選取**資源**，然後按一下**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 從頂部導覽列中，選取**資源**，然後按一下**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 從頂部導覽列中，選取**資源**，然後按一下**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 NSX Data Center for vSphere Edge 閘道

7

NSX Data Center for vSphere 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。VMware Cloud Director 支援 IPv4 和 IPv6 Edge 閘道。

從 VMware Cloud 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 NSX Data Center for vSphere 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，VMware Cloud 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 NSX Data Center for vSphere Edge 叢集
- 新增 NSX Data Center for vSphere Edge 閘道
- 設定 NSX Data Center for vSphere 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 NSX Data Center for vSphere Edge 叢集

為了將計算工作負載與網路工作負載隔離開，VMware Cloud Director 支援 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。

從 vCloud Director 9.7 開始，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 VMware Cloud 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 VMware Cloud Director OpenAPI `EdgeClusters` 方法來建立和管理 Edge 叢集。請參閱 VMware Cloud Director 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 VMware Cloud Director OpenAPI `VdcNetworkProfile` 方法。請參閱 VMware Cloud Director 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 NSX Data Center for vSphere Edge 閘道

NSX Data Center for vSphere Edge 閘道可為路由組織 VDC 網路提供外部網路連線，並可提供負載平衡、網路位址轉譯和防火牆等服務。

從 VMware Cloud Director 9.7 開始，會在您先前已建立並指派給組織 VDC 的 Edge 叢集上部署 NSX Data Center for vSphere 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、分散式防火牆和靜態路由。

必要條件

- 如需部署 NSX Data Center for vSphere 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 NSX Data Center for vSphere Edge 叢集。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左窗格中，按一下 **Edge 閘道**，然後按一下**新增**。

3 選取您想要在其上建立 Edge 閘道的支援 NSX-V 的組織虛擬資料中心，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**。

組態	描述
精簡	需要較少的記憶體和計算資源。
大型	相較於精簡組態，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。

組態	描述
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 按一下目標外部網路名稱旁邊的選項按鈕，然後按一下目標 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輸入 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。VMware Cloud 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 VMware Cloud 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 NSX Data Center for vSphere 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 NSX Data Center for vSphere 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。

在分散式防火牆畫面上建立且在其 [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，可啟用或停用 Edge 閘道防火牆。

新增 NSX Data Center for vSphere Edge 閘道防火牆規則

使用 Edge 閘道**防火牆**索引標籤，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 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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。

   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 NSX Data Center for vSphere 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 NSX Data Center for vSphere Edge 閘道防火牆規則。

程序

1 開啟 Edge 閘道服務。

   a 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。

   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 NSX Data Center for vSphere 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 從頂部導覽列中，選取**資源**，然後按一下**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 NSX Data Center for vSphere 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 如果變更了已啟用 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 NSX Data Center for vSphere 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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。
   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

VMware Cloud 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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。

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 NSX Data Center for vSphere Edge 閘道的 DHCP 轉送

由 VMware Cloud Director 環境中的 NSX 所提供的 DHCP 轉送功能可讓您從 VMware Cloud 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 NSX Data Center for vSphere Edge 閘道的 DHCP 轉送組態

VMware Cloud Director 環境中的 NSX 軟體可提供讓 Edge 閘道將 DHCP 訊息轉送至 VMware Cloud 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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。

   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 VMware Cloud 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 NSX Data Center for vSphere 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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。
   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，或從清單中選取已配置的 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。
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。

選項	描述
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。
來源 IP 位址	如果希望僅針對來自特定網域的流量套用規則，則以 CIDR 格式輸入此網域的 IP 位址或 IP 位址範圍。如果將此文字方塊保留空白，則 DNAT 規則會套用至本機子網路中的所有 IP 位址。
來源連接埠	(選擇性) 輸入來源的連接埠號碼。
描述	(選擇性) 為 DNAT 規則輸入有意義的說明。
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	輸入要套用到此規則的原始 IP 位址或 IP 位址範圍，或從清單中選取已配置的 IP 位址。 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。
目的地 IP 位址	(選擇性) 如果希望僅針對特定網域的流量套用規則，則以 CIDR 格式輸入此網域的 IP 位址或 IP 位址範圍。如果將此文字方塊保留空白，則 SNAT 規則會套用至本機子網路外部的所有目的地。
目的地連接埠	(選擇性) 輸入目的地的連接埠號碼。
描述	(選擇性) 為 SNAT 規則輸入有意義的說明。
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 NSX Data Center for vSphere Edge 閘道防火牆規則。

進階路由組態

您可以設定 NSX 軟體為 NSX Data Center for vSphere 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 NSX Data Center for vSphere 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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。

   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 NSX Data Center for vSphere 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 NSX Data Center for vSphere 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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。

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 NSX Data Center for vSphere Edge 閘道防火牆規則。

設定 OSPF

您可以針對 NSX Data Center for vSphere 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 VMware Cloud Director 環境中，通常在 Edge 閘道上應用 OSPF 是為了在 VMware Cloud 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 NSX Data Center for vSphere Edge 閘道的預設路由組態。

程序

1 開啟 Edge 閘道服務。

   a 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。

   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 NSX Data Center for vSphere 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 NSX Data Center for vSphere 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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。

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 NSX Data Center for vSphere 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 NSX Data Center for vSphere Edge 閘道設定路由重新分配。

程序

1 開啟 Edge 閘道服務。

a 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。

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資源使用量、最大化輸送量、最小化回應時間並避免超載。

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 NSX Data Center for vSphere 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此 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。

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

後端伺服器的群組。

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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。

   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**。

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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。

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。 ■ **SSL 工作階段識別碼** 啟用 SSL 傳遞時，可以使用 SSL 工作階段識別碼持續性。SSL 工作階段識別碼持續性可確保將來自相同用戶端的重複連線傳送至同一個伺服器。工作階段識別碼持續性允許使用 SSL 工作階段繼續執行，這會節省用戶端和伺服器的處理時間。
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。

選項	描述
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。而是以 URL 形式傳送使用者工作階段資訊。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。
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。 **備註** 如果啟用了 SSL 傳遞，則不支援使用此標頭。
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**，用戶端必須在請求或信號交換取消之後提供憑證。

7 若要保留變更，請按一下**保留**。

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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。

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 若要保留變更，請按一下**保留**。

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。
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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。

   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 若要保留變更，請按一下**保留**。

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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。

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/2.2/configuration.html。

6 若要保留變更，請按一下**保留**。

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 NSX Data Center for vSphere 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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。

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 若要保留變更，請按一下**保留**。

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 NSX Data Center for vSphere 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 NSX Data Center for vSphere 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 VMware Cloud 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 VMware Cloud 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

VMware Cloud Director 環境中 NSX Data Center for vSphere 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 VMware Cloud 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 NSX Data Center for vSphere 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 NSX Data Center for vSphere 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 NSX Data Center for vSphere 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 NSX Data Center for vSphere 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 NSX Data Center for vSphere 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 NSX Data Center for vSphere 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 NSX Data Center for vSphere Edge 閘道自訂一般 SSL VPN-Plus 設定

依預設，系統會在 VMware Cloud Director 環境中的 Edge 閘道上設定一些 SSL VPN-Plus 設定。您可以使用 VMware Cloud 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 NSX Data Center for vSphere Edge 閘道設定 SSL-VPN Plus 服務。

程序

1 開啟 Edge 閘道服務。

a 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。

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 NSX Data Center for vSphere 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 NSX Data Center for vSphere 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 NSX Data Center for vSphere 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 NSX Data Center for vSphere Edge 閘道上建立 IP 集區以搭配 SSL VPN-Plus 使用。

在 NSX Data Center for vSphere 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。

選項	動作
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 NSX Data Center for vSphere Edge 閘道上新增私人網路以搭配 SSL VPN-Plus 使用。

在 NSX Data Center for vSphere 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 NSX Data Center for vSphere 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。

選項	動作
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 NSX Data Center for vSphere 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 NSX Data Center for vSphere Edge 閘道防火牆規則。

在 NSX Data Center for vSphere 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 NSX Data Center for vSphere 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 NSX Data Center for vSphere 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 NSX Data Center for vSphere 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。

選項	描述
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 NSX Data Center for vSphere 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。

選項	描述
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。
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。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 NSX Data Center for vSphere Edge 閘道自訂一般 SSL VPN-Plus 設定

依預設，系統會在 VMware Cloud Director 環境中的 Edge 閘道上設定一些 SSL VPN-Plus 設定。您可以使用 VMware Cloud 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

VMware Cloud Director 環境中的 NSX Data Center for vSphere 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 (AES256-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。

若要檢視 Edge 閘道組態的大小，請導覽至 Edge 閘道，然後按一下 Edge 閘道名稱。

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 NSX Data Center for vSphere Edge 閘道設定 IPsec VPN 服務。

2 設定 NSX Data Center for vSphere Edge 閘道的 IPsec VPN 站台連線

使用 VMware Cloud 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 NSX Data Center for vSphere 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 NSX Data Center for vSphere Edge 閘道設定 IPsec VPN 服務。

程序

1 開啟 Edge 閘道服務。

a 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。

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 NSX Data Center for vSphere Edge 閘道的 IPsec VPN 站台連線。

設定 NSX Data Center for vSphere Edge 閘道的 IPsec VPN 站台連線

使用 VMware Cloud 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 VMware Cloud 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`。
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。

選項	動作
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**。

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 NSX Data Center for vSphere Edge 閘道上的 IPsec VPN 服務。

啟用 NSX Data Center for vSphere 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 NSX Data Center for vSphere 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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。

   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

VMware Cloud Director 環境中的 NSX Data Center for vSphere Edge 閘道支援 L2 VPN。透過 L2 VPN，您可以允許虛擬機器跨地理界限保留相同的 IP 位址，同時保持網路連線，從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 Data Center for vSphere 提供 Edge 閘道的 L2 VPN 功能。透過 L2 VPN，您可以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。

程序

1 導覽至 L2 VPN 畫面

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

2 將 NSX Data Center for vSphere 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 NSX Data Center for vSphere 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 NSX Data Center for vSphere 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 NSX Data Center for vSphere 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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。

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 NSX Data Center for vSphere Edge 閘道設定為 L2 VPN 伺服器。

將 NSX Data Center for vSphere 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。
- 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。

選項	動作
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**。

後續步驟

啟用此 Edge 閘道上的 L2 VPN 服務。請參閱啟用 NSX Data Center for vSphere Edge 閘道上的 L2 VPN 服務。

將 NSX Data Center for vSphere 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。
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**。

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**。

後續步驟

啟用此 Edge 閘道上的 L2 VPN 服務。請參閱啟用 NSX Data Center for vSphere Edge 閘道上的 L2 VPN 服務。

啟用 NSX Data Center for vSphere 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 NSX Data Center for vSphere 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 NSX Data Center for vSphere 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 NSX Data Center for vSphere 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

VMware Cloud 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。

VMware Cloud 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 VMware Cloud 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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。

   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 VMware Cloud 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。當 FIPS 模式開啟時，RSA 金鑰大小必須大於或等於 2048 位元。 **備註** SSL VPN-Plus 只支援 RSA 憑證。
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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。
   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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。

   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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。

   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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。

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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。

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。

當 FIPS 模式開啟時，RSA 金鑰大小必須大於或等於 2048 位元。

- 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) 輸入說明。

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

VMware Cloud 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 的分散式防火牆設定	a 從頂部導覽列的**資源**下，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 從頂部導覽列的**資源**下，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 的分散式防火牆設定	a 從頂部導覽列的**資源**下，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 從頂部導覽列的**資源**下，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 的分散式防火牆設定	a 從頂部導覽列的**資源**下，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 從頂部導覽列的**資源**下，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 的分散式防火牆設定	a 從頂部導覽列的**資源**下，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 從頂部導覽列的**資源**下，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 從頂部導覽列中，選取**資源**，然後按一下**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 VMware Cloud 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 從頂部導覽列中，選取**資源**，然後按一下**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 NSX Data Center for vSphere 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 從頂部導覽列中，選取**資源**，然後按一下**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 從頂部導覽列中，選取**資源**，然後按一下**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。

組態	描述
精簡	需要較少的記憶體和計算資源。
大型	相較於精簡組態，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 從頂部導覽列中，選取**資源**，然後按一下**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 從頂部導覽列中，選取**資源**，然後按一下**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。VMware Cloud 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 VMware Cloud Director 外部使用任何 IP 位址，可能會導致 IP 位址衝突。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**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 從頂部導覽列中，選取**資源**，然後按一下**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。

重新部署 Edge 閘道時，VMware Cloud Director 會將其刪除並使用最新組態重新建立。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**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 從頂部導覽列中，選取**資源**，然後按一下**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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。

   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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。

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 VMware Cloud Director 系統管理員已設定用於 VMware Cloud 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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。

   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 NSX-T Data Center Edge 閘道

8

NSX-T Data Center Edge 閘道可為路由組織 VDC 網路或資料中心群組網路提供外部網路連線以及 IP 管理內容。還可以提供防火牆、網路位址轉譯 (NAT)、IPSec VPN、DNS 轉送和 DHCP 等服務，這些服務預設為啟用。

本章節討論下列主題：

- 專用外部網路
- 新增 NSX-T Data Center Edge 閘道
- 將 IP 集新增至 NSX-T Data Center Edge 閘道
- 新增 NSX-T Data Center Edge 閘道防火牆規則
- 將 SNAT 或 DNAT 規則新增至 NSX-T Edge 閘道
- 在 NSX-T Edge 閘道上設定 DNS 轉寄站服務
- 編輯 NSX-T Edge 閘道的 IP 配置
- 快速 IP 配置
- 建立自訂應用程式連接埠設定檔
- NSX-T Data Center Edge 閘道的以原則為基礎的 IPsec VPN
- 設定專用外部網路服務
- 在 NSX-T Data Center Edge 閘道上管理 NSX Advanced 負載平衡

專用外部網路

若要在虛擬資料中心提供完全路由的網路拓撲，您可以將外部網路專用於特定的 NSX-T Data Center Edge 閘道。

在此組態中，外部網路與 NSX-T Data Center Edge 閘道之間存在一對一關聯性，任何其他 Edge 閘道都無法連線至外部網路。

與專用外部網路相關聯的第 0 層邏輯路由器或 VRF-Lite 閘道是承租人網路堆疊的一部分。外部網路會被視為 VMware Cloud Director 網路路由網域的一部分。

將外部網路專用於 Edge 閘道會為承租人提供其他 Edge 閘道服務，例如路由通告管理和邊界閘道通訊協定 (BGP) 組態。

承租人可以決定將哪個連結至 Edge 閘道的承租人網路通告至外部網路。這可混合使用 NAT 路由和完全路由的組織虛擬資料中心網路。

在建立 Edge 閘道期間或之後，可透過編輯 Edge 閘道一般設定，將外部網路專用於 NSX-T Data Center Edge 閘道。

新增 NSX-T Data Center Edge 閘道

NSX-T Data Center Edge 閘道可為路由組織 VDC 網路提供外部網路連線，並可提供負載平衡、網路位址轉譯和防火牆等服務。

必要條件

如需部署 NSX-T Data Center Edge 閘道的系統需求的相關資訊，請參閱 NSX-T Data Center 管理指南。

從 10.1 版開始，VMware Cloud Director 支援專用的外部網路組態。將外部網路專用於 Edge 閘道會為承租人提供其他 Edge 閘道服務，例如路由通告管理和邊界閘道通訊協定 (BGP) 組態。如需詳細資訊，請參閱專用外部網路。

VMware Cloud Director 支援基本 NSX-T Data Center Edge 叢集組態。如需有關 NSX Edge 叢集的詳細資訊，請參閱 NSX-T Data Center 安裝指南。

程序

1. 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。
2. 在左面板中，按一下 **Edge 閘道**。
3. 按一下**新增**。
4. 選取您想要在其上建立 Edge 閘道的支援 NSX-T Data Center 的組織 VDC，然後按**下一步**。
5. 輸入新 Edge 閘道的名稱，並選擇性地輸入說明。
6. 若要為 Edge 閘道啟用 BGP 和路由通告，請開啟**專用外部網路**選項，然後按**下一步**。
7. 選取新 Edge 閘道連線到的外部網路，然後按**下一步**。

   如果已開啟**專用外部網路**選項，其他 Edge 閘道將無法存取此外部網路。
8. 選取要在其上部署 Edge 閘道的 Edge 叢集，然後按**下一步**。

   如果您想要在與外部網路相關聯之 Edge 叢集以外的 Edge 叢集上執行 Edge 閘道服務，可以將 Edge 閘道設定為使用不同的 Edge 叢集。
   - 使用 Edge 閘道所連線之外部網路的 Edge 叢集。
   - 從部署 Edge 閘道之組織 VDC 可用的 Edge 叢集清單中進行選取。
9. (選擇性) 編輯配置給 Edge 閘道的 IP 位址或 IP 位址範圍，然後按**下一步**。
10. 檢閱**即將完成**頁面，然後按一下**完成**。

將 IP 集新增至 NSX-T Data Center Edge 閘道

若要建立防火牆規則並將其新增至 NSX-T Data Center Edge 閘道，您必須先建立 IP 集。IP 集是套用防火牆規則的物件群組。將多個物件合併至 IP 集有助於減少要建立的防火牆規則總數。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，按一下 **Edge 閘道**。

3 按一下 NSX-T Edge 閘道。

4 在**安全性**下，按一下 **IP 集**索引標籤，然後按一下**新增**。

5 輸入 IP 集的名稱，並選擇性地輸入其說明。

6 輸入 IP 集包含的虛擬機器的 IP 位址或 IP 位址範圍，然後按一下**新增**。

7 若要儲存防火牆群組，請按一下**儲存**。

結果

您已建立 IP 集並將其新增至 NSX-T Edge 閘道。

後續步驟

新增 NSX-T Data Center Edge 閘道防火牆規則

新增 NSX-T Data Center Edge 閘道防火牆規則

若要控制進出 NSX-T Data Center Edge 閘道的傳入和傳出網路流量，您可以建立防火牆規則。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，按一下 **Edge 閘道**。

3 按一下 Edge 閘道。

4 如果**防火牆**畫面尚未顯示在 [服務] 區段下，請按一下**防火牆**索引標籤。

5 按一下**編輯規則**。

6 按一下**在頂部新增**按鈕。

新規則的資料列會新增至所選規則的上方。

7 設定防火牆規則。

選項	描述
名稱	輸入規則的名稱。
狀態	若要在建立時啟用規則，請開啟**狀態**切換按鈕。

選項	描述
應用程式	(選擇性) 若要選取套用規則的特定連接埠設定檔，請開啟**應用程式**切換按鈕，然後按一下**儲存**。
來源	選取一個選項，然後按一下**保留**。 ■ 若要允許或拒絕來自任何來源位址的流量，請開啟**任何來源**。 ■ 若要允許或拒絕來自特定防火牆群組的流量，請從清單中選取防火牆群組。
目的地	選取一個選項，然後按一下**保留**。 ■ 若要允許或拒絕流入任何目的地位址的流量，請開啟**任何目的地**。 ■ 若要允許或拒絕進入特定防火牆群組的流量，請從清單中選取防火牆群組。
動作	從**動作**下拉式功能表中，選取一個選項。 ■ 若要允許流出或流入指定來源、目的地和服務的流量，請選取**接受**。 ■ 若要封鎖流出或流入指定來源、目的地和服務的流量，而不通知封鎖的用戶端，請選取**捨棄**。 ■ 若要封鎖流出或流入指定來源、目的地和服務的流量，並通知封鎖的用戶端流量已遭拒絕，請選取**拒絕**。
IP 通訊協定	選取是否要將規則套用至 IPv4 或 IPv6 流量。
方向	選取要套用規則的流量方向。 **備註** 在 VMware Cloud Director 10.2.1 及更高版本中，此選項不再可用。
啟用記錄。	若要記錄此規則執行的位址轉譯，請開啟**啟用記錄**切換按鈕。

8 按一下**儲存**。

9 若要設定其他規則，請重複這些步驟。

結果

建立防火牆規則後，這些規則會顯示在 [Edge 閘道防火牆規則] 清單中。您可以視需要上移、下移、編輯或刪除規則。

將 SNAT 或 DNAT 規則新增至 NSX-T Edge 閘道

若要將來源 IP 位址從私人 IP 位址變更為公用 IP 位址，請建立來源 NAT (SNAT) 規則。若要將目的地 IP 位址從公用 IP 位址變更為私人 IP 位址，請建立目的地 NAT (DNAT) 規則。

在 VMware Cloud Director 環境中的 Edge 閘道上設定 SNAT 或 DNAT 規則時，一律從組織 VDC 的角度來設定規則。

SNAT 規則會轉譯從組織 VDC 網路向外傳送至外部網路或另一個組織 VDC 網路的封包的來源 IP 位址。

「無 SNAT」規則會阻止從組織 VDC 向外傳送至外部網路或另一個組織 VDC 網路的封包的內部 IP 位址轉譯。

DNAT 規則會轉譯組織 VDC 網路從外部網路或另一個組織 VDC 網路接收到的封包的 IP 位址，並會選擇性地轉譯連接埠。

「無 DNAT」規則會阻止由組織 VDC 從外部網路或另一個組織 VDC 網路所接收到的封包的外部 IP 位址轉譯。

當您在 NSX-T Data Center Edge 閘道上使用 NAT 服務時，VMware Cloud Director 支援自動路由重新分配。

重要 如果您使用的是 Tanzu Kubernetes 叢集，請記下 Edge 閘道上建立的系統 SNAT 規則，以避免建立衝突的規則。

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。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，按一下 **Edge 閘道**。

3 按一下 Edge 閘道，然後在**服務**下，按一下 **NAT**。

4 若要新增規則，請按一下**新增**。

5 設定 SNAT 或「無 SNAT」規則 (從內到外)。

選項	描述
名稱	為規則輸入有意義的名稱。
描述	(選擇性) 為規則輸入說明。
介面類型	從下拉式功能表中，選取 [SNAT] 或 [無 SNAT]。
外部 IP	根據您要建立的規則類型，選擇其中一個選項。 ■ 如果您要建立 SNAT 規則，則輸入要為其設定 SNAT 規則的 Edge 閘道的公用 IP 位址。 ■ 如果您要建立「無 SNAT」規則，則將此文字方塊保留空白。
內部 IP	輸入要為其設定 SNAT 的虛擬機器的 IP 位址或 IP 位址清單，以便它們可以將流量傳送至外部網路。

選項	描述
目的地 IP	(選擇性) 如果希望僅針對特定網域的流量套用規則，請輸入此網域的 IP 位址或 IP 位址清單。如果將此文字方塊保留空白，則 SNAT 規則會套用至本機子網路外部的所有目的地。
進階設定 (可選)	對於一些其他設定，按一下**進階設定**索引標籤。 **狀態** 若要在建立時啟用規則，請開啟**狀態**選項。 **記錄** 若要記錄此規則執行的位址轉譯，請開啟**記錄**選項。 **優先順序** 如果某個位址具有多個 NAT 規則，您可以為這些規則指派不同的優先順序，以確定規則的套用順序。值越低，表示此規則的優先順序越高。 **防火牆比對** 可以設定防火牆比對規則，以確定在 NAT 期間如何套用防火牆。從下拉式功能表中，選取下列其中一個選項。 ■ 若要將防火牆規則套用至 NAT 規則的內部位址，請選取**符合內部位址**。 ■ 若要將防火牆規則套用至 NAT 規則的外部地址，請選取**符合外部地址**。 ■ 若要略過套用防火牆規則，請選取**略過**。

6 設定 DNAT 或「無 DNAT」規則 (從外向內)。

選項	描述
名稱	為規則輸入有意義的名稱。
描述	(選擇性) 為規則輸入說明。
介面類型	從下拉式功能表中，選取 [DNAT] 或 [無 DNAT]。
外部 IP	輸入要為其設定 DNAT 規則的 Edge 閘道的公用 IP 位址。 您輸入的 IP 位址必須子配置給 Edge 閘道。
外部連接埠	(選擇性) 輸入要針對輸入到虛擬機器的封包將 DNAT 規則轉譯到的連接埠。
內部 IP	根據您要建立的規則類型，選擇其中一個選項。 ■ 如果您要建立 DNAT 規則，則輸入要為其設定 DNAT 的虛擬機器的 IP 位址或 IP 位址清單，以便它們可以從外部網路接收流量。 ■ 如果您要建立「無 DNAT」規則，則將此文字方塊保留空白。

選項	描述
應用程式	(選擇性) 選取要套用規則的特定應用程式連接埠設定檔。 應用程式連接埠設定檔包含一個連接埠和一個通訊協定，可供傳入流量在 Edge 閘道上用來連線至內部網路。
進階設定 (可選)	對於一些其他設定，按一下**進階設定**索引標籤。 **狀態** 若要在建立時啟用規則，請開啟**狀態**選項。 **記錄** 若要記錄此規則執行的位址轉譯，請開啟**記錄**選項。 **優先順序** 如果某個位址具有多個 NAT 規則，您可以為這些規則指派不同的優先順序，以確定規則的套用順序。值越低，表示此規則的優先順序越高。 **防火牆比對** 可以設定防火牆比對規則，以確定在 NAT 期間如何套用防火牆。從下拉式功能表中，選取下列其中一個選項。 ■ 若要將防火牆規則套用至 NAT 規則的內部位址，請選取**符合內部位址**。 ■ 若要將防火牆規則套用至 NAT 規則的外部地址，請選取**符合外部地址**。 ■ 若要略過套用防火牆規則，請選取**略過**。

7 按一下**儲存**。

8 若要設定其他規則，請重複這些步驟。

在 NSX-T Edge 閘道上設定 DNS 轉寄站服務

若要將 DNS 查詢轉送至外部 DNS 伺服器，請設定 DNS 轉寄站。

在設定 DNS 轉寄站服務的過程中，還可以新增條件式轉寄站區域。條件式轉寄站區域設定為包含最多五個 FQDN DNS 區域的清單。如果 DNS 查詢與該清單中的某個網域名稱相符，則查詢會從對應的轉寄站區域轉送到伺服器。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，按一下 **Edge 閘道**。

3 按一下 Edge 閘道，然後在 **IP 管理**下，按一下 **DNS**。

4 在 **DNS 轉寄站**區段中，按一下**編輯**。

5 若要啟用 DNS 轉寄站服務，請開啟**狀態**切換按鈕。

6 輸入預設 DNS 區域的名稱，並選擇性地輸入說明。

7 輸入一或多個上游伺服器的 IP 位址，以逗號分隔。

8 按一下**儲存**。

9 (選擇性) 新增條件式轉寄站區域。

a 在**條件式轉寄站區域**區段中，按一下**新增**。

b 輸入轉寄站區域的名稱。

c 輸入一或多個上游伺服器的 IP 位址，以逗號分隔。

d 輸入一或多個網域名稱 (以逗號分隔)，然後按一下**儲存**。

編輯 NSX-T Edge 閘道的 IP 配置

您可以將外部網路的多個 IP 位址配置給 Edge 閘道。

程序

1 開啟 Edge 閘道服務。

a 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。

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 閘道，然後按一下 **IP 配置**。

在 IP 管理網格中，您可以看到配置給 Edge 閘道的 IP 位址，以及目前由 Edge 閘道使用的 IP 位址。

3 在**已配置的 IP** 區段中，按一下 **IP 管理**。

在 **IP 管理**網格中，您可以檢視可供 Edge 閘道使用的每個外部網路的 IP 使用量。

4 輸入 IP 範圍，然後按一下**新增**。

5 按一下**儲存**。

結果

IP 位址將配置給 Edge 閘道。

後續步驟

檢視配置給 Edge 閘道的 IP 位址、新增更多 IP 位址，或視需要將其移除。

快速 IP 配置

您可以使用快速 IP 配置從外部網路子網路將 IP 位址配置給 Edge 閘道，而無需輸入特定的 IP 位址或 IP 位址範圍。

程序

1 開啟 Edge 閘道服務。

   a 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**索引標籤。

   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 閘道，然後按一下 **IP 配置**。

   在 IP 管理網格中，您可以看到配置給 Edge 閘道的 IP 位址，以及目前由 Edge 閘道使用的 IP 位址。

3 在**已配置的 IP** 區段中，按一下**快速 IP 配置**。

4 從下拉式功能表中，選取要從中指派 IP 位址的子網路。

   如果有多個子網路可供使用，則選取**任何**會導致從一或多個子網路配置 IP 位址。

5 輸入要配置給 Edge 閘道的 IP 位址數目，然後按一下**儲存**。

   此數字必須小於所選子網路中的可用 IP 位址數目。

結果

IP 位址將配置給 Edge 閘道。

後續步驟

檢視配置給 Edge 閘道的 IP 位址、新增更多 IP 位址，或視需要將其移除。

建立自訂應用程式連接埠設定檔

若要建立防火牆和 NAT 規則，您可以使用預先設定的應用程式連接埠設定檔和自訂應用程式連接埠設定檔。

應用程式連接埠設定檔包括通訊協定和連接埠的組合或連接埠群組，用於 Edge 閘道上的防火牆和 NAT 服務。除了為 NSX-T Data Center 預先設定的預設連接埠設定檔之外，您還可以建立自訂應用程式連接埠設定檔。

在 Edge 閘道上建立自訂應用程式連接埠設定檔時，該設定檔對相同組織 VDC 中的所有其他 NSX-T Data Center Edge 閘道可見。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，按一下 **Edge 閘道**。

3 按一下 Edge 閘道。

4 在**安全性**下，按一下**應用程式連接埠設定檔**。

5 在**自訂應用程式**區段中，按一下**新增**。

6 輸入應用程式連接埠設定檔的名稱，並選擇性地輸入說明。

7 從下拉式功能表中選取通訊協定。

8 輸入連接埠或連接埠範圍 (以逗號分隔)，然後按一下**儲存**。

後續步驟

使用應用程式連接埠設定檔建立防火牆和 NAT 規則。請參閱新增 NSX-T Data Center Edge 閘道防火牆規則和將 SNAT 或 DNAT 規則新增至 NSX-T Edge 閘道。

NSX-T Data Center Edge 閘道的以原則為基礎的 IPsec VPN

從 10.1 版開始，VMware Cloud Director 支援在 NSX-T Data Center Edge 閘道執行個體與遠端站台之間建立以站台間原則為基礎的 IPSec VPN。

IPSec VPN 可以在 Edge 閘道與同時使用 NSX-T Data Center 或具有支援 IPSec 的第三方硬體路由器或 VPN 閘道的遠端站台之間提供站台間連線。

以原則為基礎的 IPSec VPN 需要將 VPN 原則套用至封包，才能確定哪些流量在透過 VPN 通道傳遞之前受到 IPSec 保護。此類型的 VPN 被視為是靜態的，因為當本機網路拓撲和組態變更時，還必須更新 VPN 原則設定才能適應變更。

NSX-T Data Center Edge 閘道支援分割通道組態，其中 IPSec 流量優先進行路由。

當您在 NSX-T Edge 閘道上使用 IPSec VPN 時，VMware Cloud Director 支援自動路由重新分配。

設定 NSX-T 以原則為基礎的 IPSec VPN

您可以設定 NSX-T Data Center Edge 閘道與遠端站台之間的站台間連線。遠端站台必須使用 NSX-T Data Center，且具有第三方硬體路由器或支援 IPSec 的 VPN 閘道。

當您在 NSX-T Data Center Edge 閘道上設定 IPSec VPN 時，VMware Cloud Director 支援自動路由重新分配。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**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**服務**下，按一下 **IPSec VPN**。

4 若要設定 IPSec VPN 通道，請按一下**新增**。

5 輸入 IPSec VPN 通道的名稱，並選擇性地輸入說明。

6 若要在建立時啟用通道，請開啟**已啟用**選項。

7 選擇要輸入的預先共用金鑰。

備註 在 IPSec VPN 通道的另一端，預先共用金鑰必須相同。

8 輸入可用於本機端點之 Edge 閘道的 IP 位址之一。

備註 IP 位址必須是 Edge 閘道的主要 IP，或是從外部網路單獨配置給 Edge 閘道的 IP 位址。

9 以 CIDR 標記法輸入至少一個本機 IP 子網路位址，以用於 IPSec VPN 通道。

10 輸入遠端站台的 IP 位址。

11 以 CIDR 標記法輸入至少一個遠端 IP 子網路位址，以用於 IPSec VPN 通道。

12 (選擇性) 若要啟用記錄，請開啟**記錄**選項。

13 按一下**儲存**。

14 若要確認通道是否正常運作，請選取該通道，然後按一下**檢視統計資料**。

如果通道正常運作，**通道狀態**和 **IKE 服務狀態**均顯示啟動。

結果

新建立的 IPSec VPN 通道列於 **IPSec VPN** 視圖中。將會使用預設安全性設定檔建立 IPSec VPN 通道。

後續步驟

您可以根據需要編輯 IPSec VPN 通道設定並自訂其安全性設定檔。

自訂 IPSec VPN 通道的安全性設定檔

如果您決定不使用在建立時指派給 IPSec VPN 通道的由系統產生的安全性設定檔，可以對其進行自訂。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**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**服務**下，按一下 **IPSec VPN**。

4 選取 IPSec VPN 通道，然後按一下**安全性設定檔自訂**。

5 設定 IKE 設定檔。

網際網路金鑰交換 (IKE) 設定檔提供了在建立 IKE 通道時，用於在站台間驗證、加密及建立共用密碼之演算法的相關資訊。

a 選取 IKE 通訊協定版本，以在 IPSec 通訊協定套件中設定安全性關聯 (SA)。

選項	敘述
IKEv1	當您選取此選項時，IPSec VPN 會起始並僅回應 IKEv1 通訊協定。
IKEv2	預設選項。當您選取此版本時，IPSec VPN 會起始並僅回應 IKEv2 通訊協定。
IKE-Flex	當您選取此選項時，如果使用 IKEv2 通訊協定建立通道失敗，則來源站台不會回復並使用 IKEv1 通訊協定起始連線。相反地，如果遠端站台使用 IKEv1 通訊協定起始連線，則會接受連線。

b 選取要在網際網路金鑰交換 (IKE) 交涉期間使用的支援加密演算法。

c 從**摘要**下拉式功能表中，選取要在 IKE 交涉期間使用的安全雜湊演算法。

d 從 **Diffie-Hellman 群組**下拉式功能表中，選取其中一個密碼編譯配置，以允許對等站台和 Edge 閘道透過不安全的通訊通道建立共用密碼。

e (選擇性) 在**關聯存留時間**文字方塊中，修改 IPSec 通道需要重新建立之前的預設秒數。

6 設定 IPSec VPN 通道。

a 若要啟用完全正向加密，請開啟此選項。

b 選取重組原則。

重組原則可協助處理內部封包中存在的重組位元。

選項	敘述
複製	將重組位元從內部 IP 封包複製到外部封包。
清除	忽略內部封包中存在的重組位元。

c 選取要在網際網路金鑰交換 (IKE) 交涉期間使用的支援加密演算法。

d 從**摘要**下拉式功能表中，選取要在 IKE 交涉期間使用的安全雜湊演算法。

e 從 **Diffie-Hellman 群組**下拉式功能表中，選取其中一個密碼編譯配置，以允許對等站台和 Edge 閘道透過不安全的通訊通道建立共用密碼。

f (選擇性) 在**關聯存留時間**文字方塊中，修改 IPSec 通道需要重新建立之前的預設秒數。

7 (選擇性) 在**探查時間間隔**文字方塊中，修改無作用對等偵測的預設秒數。

8 按一下**儲存**。

結果

在 IPSec VPN 視圖中，IPSec VPN 通道的安全性設定檔會顯示為**使用者定義**。

設定專用外部網路服務

若要在虛擬資料中心提供完全路由的網路拓撲，**系統管理員**可以將外部網路專用於特定的 NSX-T Data Center Edge 閘道。

使用專用外部網路時，您可以設定其他路由服務，例如，路由通告管理和邊界閘道通訊協定 (BGP) 組態。

管理路由通告

透過使用路由通告，您可以在組織虛擬資料中心 (VDC) 中建立完全路由的網路環境。

您可以決定將哪個連結至 NSX-T Data Center Edge 閘道的網路子網路通告至專用外部網路。

如果子網路未新增至通告篩選器，則指向該子網路的路由不會通告至外部網路，且子網路將保持私有狀態。

備註 VMware Cloud Director 會通告位於通告路由中的任何組織 VDC 網路。因此，您不需要針對屬於通告網路的每個子網路建立篩選器。

路由通告會在 NSX-T Data Center Edge 閘道上自動設定。

當您在 NSX-T Edge 閘道上使用路由通告時，VMware Cloud Director 支援自動路由重新分配。在代表專用外部網路的第 0 層邏輯路由器上，會自動設定路由重新分配。

必要條件

- 確認您已將外部網路專用於組織中的 NSX-T Data Center Edge 閘道。請參閱專用外部網路。

程序

1. 從頂部導覽列中，選取**資源**，然後按一下**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**路由**下，按一下**路由通告**和**編輯**。
4. 若要新增要通告的子網路，請按一下**新增**。
5. 新增 IPv4 或 IPv6 子網路。

   使用格式 *network_gateway_IP_address/subnet_prefix_length*，例如 **192.167.1.1/24**。

設定 BGP 一般設定

您可以在具有專用外部網路的 NSX-T Data Center Edge 閘道與實體基礎結構中的路由器之間設定外部或內部邊界閘道通訊協定 (eBGP 或 iBGP) 連線。

BGP 透過使用 IP 網路資料表或首碼 (用於指定自發系統 (AS) 之間的多個路由) 做出核心路由決策。

「BGP 發言者」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。

備註 在連線至 VRF 閘道支援之外部網路的 Edge 閘道中，本機 AS 編號和正常重新啟動設定為唯讀。您可以在 NSX-T Data Center 中的父系第 0 層閘道上編輯這些設定。

必要條件

- 確認您已將外部網路專用於組織中的 NSX-T Data Center Edge 閘道。請參閱專用外部網路。

程序

1. 從頂部導覽列中，選取**資源**，然後按一下**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**路由**下，按一下 **BGP**，然後在**組態**下，按一下**編輯**。
4. 開啟**狀態**選項以啟用 BGP。
5. 輸入要用於通訊協定之本機 AS 功能的自發系統 (AS) 識別碼。

   VMware Cloud Director 會將本機 AS 編號指派給 Edge 閘道。當 Edge 閘道與其他自發系統中的 BGP 芳鄰連線時，Edge 閘道會通告此識別碼。

6 從下拉式功能表中，選取**正常重新啟動模式**選項。

選項	敘述
協助程式和正常重新啟動	在 Edge 閘道上啟用正常重新啟動功能不是最佳做法，因為所有閘道中的 BGP 對等始終處於作用中狀態。 在容錯移轉時，正常重新啟動功能會增加遠端芳鄰選取替代第 0 層閘道所需的時間。這會延遲基於 BFD 的聚合。 **備註** Edge 閘道組態會套用至所有 BGP 芳鄰，除非芳鄰特定的組態將其覆寫。
僅限協助程式	有助於減少或避免與從可正常重新啟動之芳鄰中獲知的路由相關聯的流量中斷。在重新啟動後，芳鄰必須能夠保留其轉送表。
停用	在 Edge 閘道上停用正常重新啟動模式。

7 (選擇性) 變更正常重新啟動計時器的預設值。

8 (選擇性) 變更失效路由計時器的預設值。

9 開啟 **ECMP** 選項以啟用 ECMP。

10 按一下**儲存**。

後續步驟

- 建立 IP 首碼清單
- 新增 BGP 芳鄰

建立 IP 首碼清單

您可以建立包含單一或多個 IP 位址的 IP 首碼清單。您可以使用 IP 首碼清單為 BGP 芳鄰指派路由通告的存取權限。

透過 BGP 芳鄰篩選器來參考 IP 首碼清單，以限制在 BGP 對等之間交換的 BGP 更新數目。透過使用路由篩選，可以減少 BGP 更新所需的系統資源量。

例如，您可以將 IP 位址 192.168.100.3/27 新增到 IP 首碼清單，並拒絕將路由重新分配給 Edge 閘道。

也可以附加包含 `less than or equal to` (le) 和 `greater than or equal to` (ge) 修飾詞的 IP 位址，以授與或限制路由重新分配。例如，192.168.100.3/27 ge 26 le 32 修飾詞符合長度大於或等於 26 位元且小於或等於 32 位元的子網路遮罩。

必要條件

- 確認您已將外部網路專用於組織中的 NSX-T Data Center Edge 閘道。請參閱專用外部網路。
- 設定 BGP 一般設定.

程序

1 從頂部導覽列中，選取**資源**，然後按一下**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**路由**下，按一下 **BGP** 和 **IP 首碼清單**。

4 若要新增 IP 首碼清單，請按一下**新增**。

5 輸入首碼清單的名稱，並選擇性地輸入說明。

6 按一下**新增**，然後新增用於首碼的 CIDR 標記法。

7 從下拉式功能表中，選取要套用至首碼的動作。

8 (選擇性) 輸入 `greater than or equal to` 和 `less than or equal to` 修飾詞，以授與或限制路由重新分配。

後續步驟

- 您可以根據需要編輯或刪除 IP 首碼清單。
- 設定路由篩選。請參閱新增 BGP 芳鄰。

新增 BGP 芳鄰

您可以在新增 BGP 路由芳鄰時對其進行個別設定。

必要條件

- 確認您已將外部網路專用於組織中的 NSX-T Data Center Edge 閘道。請參閱專用外部網路。
- 確認您已設定 Edge 閘道的全域 BGP 設定。請參閱設定 BGP 一般設定。
- 如果使用路由篩選，請確認您已建立 IP 首碼清單。請參閱建立 IP 首碼清單。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**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**路由**下，按一下 **BGP** 和**芳鄰**。

4 若要新增 BGP 芳鄰，請按一下**新增**。

5 為新的 BGP 芳鄰輸入一般設定。

   a 為新的 BGP 芳鄰輸入 IPv4 或 IPv6 位址。

   b 以 ASPLAIN 格式輸入遠端自發系統 (AS) 編號。

   c 輸入將保持運作訊息傳送至 BGP 對等的時間間隔。

   d 輸入將 BGP 對等宣告為無作用之前的時間間隔。

e 從下拉式功能表中，針對此芳鄰選取**正常重新啟動模式**選項。

選項	敘述
停用	覆寫全域 Edge 閘道設定，並針對此芳鄰停用正常重新啟動模式。
僅限協助程式	覆寫全域 Edge 閘道設定，並針對此芳鄰將正常重新啟動模式設定為**僅限協助程式**。
正常重新啟動和協助程式	覆寫全域 Edge 閘道設定，並針對此芳鄰將正常重新啟動模式設定為**正常重新啟動和協助程式**。

f 開啟 **AllowAS-in** 切換按鈕，以啟用接收具有相同 AS 的路由。

g 如果 BGP 芳鄰需要驗證，請輸入其密碼。

6 為新的 BGP 芳鄰設定雙向轉送偵測 (BFD) 設定。

a (選擇性) 開啟 **BFD** 選項，以啟用 BFD 進行故障偵測。

b 在 [BFD 間隔] 文字方塊中，定義傳送活動訊號封包的時間間隔。

c 在**多次無作用**文字方塊中，輸入 BGP 芳鄰在 BFD 宣告關閉之前未能傳送活動訊號封包的次數。

7 (選擇性) 設定路由篩選。

a 從 **IP 位址系列**下拉式功能表中，選取 IP 位址系列。

b 若要設定輸入篩選器，請選取 IP 首碼清單。

c 若要設定輸出篩選器，請選取 IP 首碼清單。

8 按一下**儲存**。

後續步驟

您可以根據需要檢視每個 BGP 芳鄰的狀態，編輯或刪除 BGP 芳鄰。

在 NSX-T Data Center Edge 閘道上管理 NSX Advanced 負載平衡

身為**系統管理員**，您可以在 NSX-T Data Center 閘道上啟用負載平衡並將服務引擎群組指派給 Edge 閘道。

組織管理員建立負載平衡器伺服器集區和虛擬服務。

在 NSX-T Data Center Edge 閘道上啟用負載平衡器

系統管理員必須先在 NSX-T Data Center Edge 閘道上啟用負載平衡器，**組織管理員**才能設定負載平衡服務。

必要條件

- 確認您是**系統管理員**。

- 確認您已在雲端基礎結構中整合 VMware NSX Advanced Load Balancer。如需有關管理 NSX Advanced Load Balancer 的詳細資訊，請參閱《VMware Cloud Director Service Provider Admin Portal 指南》。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，按一下 **Edge 閘道**。

3 按一下要在其上啟用負載平衡的 NSX-T Data Center Edge 閘道。

4 在 [負載平衡器] 下，按一下**一般設定**。

5 按一下**編輯**，然後開啟**負載平衡器狀態**選項。

6 輸入要從中使用 IP 位址建立虛擬服務之服務網路子網路的網路 CIDR。

可以透過選取**使用預設值**核取方塊來使用預設服務網路子網路。

7 按一下**儲存**。

後續步驟

將服務引擎群組指派給 NSX-T Data Center Edge 閘道。

將服務引擎群組指派給 NSX-T Data Center Edge 閘道

系統管理員必須先將服務引擎群組指派給 Edge 閘道，**組織管理員**才能在 NSX-T Data Center Edge 閘道上設定負載平衡服務。

由 NSX Advanced Load Balancer 提供的負載平衡計算基礎結構將組織整理到服務引擎群組中。**系統管理員**可以將一或多個服務引擎群組指派給 NSX-T Data Center Edge 閘道。

指派給單一 Edge 閘道的所有服務引擎群組皆使用相同的服務網路。

必要條件

- 確認您是**系統管理員**。
- 在 NSX-T Data Center Edge 閘道上啟用負載平衡器。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，按一下 **Edge 閘道**。

3 按一下要為其指派服務引擎群組的 NSX-T Data Center Edge 閘道。

4 在 [負載平衡器] 下，按一下**服務引擎群組**。

5 按一下**新增**。

6 從清單中選取可用的服務引擎群組。

7 輸入可放置在 Edge 閘道上的虛擬服務數目上限。

8 輸入可供 Edge 閘道使用的保證虛擬服務數目。

9 若要確認您的設定，請按一下**儲存**。

編輯服務引擎群組的設定

系統管理員可以編輯服務引擎群組支援的虛擬服務數目上限和保留的虛擬服務數目。

同步服務引擎群組後，如果新的支援虛擬服務數目上限低於保留的虛擬服務數目，則此服務引擎群組會標記為過度配置。

如果服務引擎群組已過度配置，則建立新虛擬服務可能會失敗，即使您在其上建立虛擬服務的 Edge 閘道具有足夠的保留容量亦是如此。

若要避免建立虛擬服務失敗，則在您編輯服務引擎群組的設定時，請勿將受支援的虛擬服務數目上限縮減至初始保留的虛擬服務數目以下。

必要條件

- 確認您是**系統管理員**。
- 在 NSX-T Data Center Edge 閘道上啟用負載平衡器。
- 將服務引擎群組指派給 NSX-T Data Center Edge 閘道。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，按一下 **Edge 閘道**。

3 按一下已獲指派服務引擎群組的 NSX-T Data Center Edge 閘道。

4 在 [負載平衡器] 下，按一下**服務引擎群組**。

5 按一下**編輯**。

6 編輯 Edge 閘道可使用的允許虛擬服務數目上限。

除非強制要求，否則請勿減少數量。不然在建立虛擬服務時可能會遇到故障。

7 編輯可供 Edge 閘道使用的保證虛擬服務數目。

8 按一下**儲存**。

新增負載平衡器伺服器集區

伺服器集區是包含一或多個伺服器的群組，這些伺服器設定為執行相同的應用程式並提供高可用性。

必要條件

- 在 NSX-T Data Center Edge 閘道上啟用負載平衡器。
- 將服務引擎群組指派給 NSX-T Data Center Edge 閘道。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，按一下 **Edge 閘道**。

3 按一下要為其設定負載平衡器集區的 NSX-T Data Center Edge 閘道。

4 在 [負載平衡器] 下，按一下**集區**，然後按一下**新增**。

5 設定負載平衡器集區的一般設定。

a 為伺服器集區輸入有意義的名稱，並選擇性地輸入說明。

b 選取演算法平衡方法。

負載平衡演算法會定義在伺服器集區成員之間散佈傳入連線的方式。

選項	敘述
最少連線數	新連線會傳送至目前具有最少連線數的伺服器。
循環配置資源	按順序將新連線傳送至集區中的下一個合格伺服器。
最快回應	新連線會傳送至目前對新連線或請求提供最快回應的伺服器。
一致雜湊	透過使用用戶端的 IP 位址產生 IP 雜湊金鑰，會在伺服器之間散佈新連線。
最小負載	新連線會傳送至具有最輕負載的伺服器，無論伺服器擁有的連線數目為何。
最少伺服器	負載平衡器將決定滿足目前用戶端負載所需的最少伺服器數目，而不是嘗試在所有伺服器之間散佈所有連線或請求。
隨機	負載平衡器會隨機挑選伺服器。
最少工作	負載會根據伺服器意見反應進行彈性平衡。
核心相似性	每個 CPU 核心都使用一小部分伺服器，且每個伺服器由一小部分核心使用。實際上，它在伺服器和核心之間提供了多對多對應。

c 若要在建立時啟用伺服器集區，請開啟**狀態**選項。

d 輸入要用於集區成員流量的預設目的地伺服器連接埠。

e (選擇性) 在**正常停用逾時**文字方塊中，輸入可正常停用集區成員的最長時間 (以分鐘為單位)。

虛擬服務會在關閉與已停用成員的現有連線之前等待指定的時間。

f (選擇性) 若要啟用被動健全狀況監控器，請開啟**被動健全狀況監控器**選項。

g (選擇性) 選取主動健全狀況監控器。

選項	敘述
HTTP	HTTP 要求和回應用於驗證健全狀況。
HTTPS	用於針對 HTTPS 加密的 Web 伺服器驗證健全狀況。
TCP	TCP 連線用於驗證健全狀況。
UDP	UDP 資料包用於驗證健全狀況。
PING	ICMP ping 用於驗證健全狀況。

6 將成員新增至伺服器集區。

a 按一下**成員**索引標籤，然後按一下**新增**。

b 輸入集區成員的 IP 位址。

c 開啟**狀態**選項以啟用集區成員。

d (選擇性) 為伺服器集區成員新增自訂連接埠。

連接埠號碼預設為針對集區輸入的目的地連接埠。

e 輸入集區成員的比率。

每個集區成員的比率表示流向各個伺服器集區成員的流量。比率為 2 的伺服器所取得的流量將是比率為 1 的伺服器的兩倍。預設值為 1。

7 在 **SSL 設定**索引標籤上進行 SSL 設定，以驗證負載平衡器集區成員所提供的憑證。

a 若要啟用 SSL，請開啟**啟用 SSL** 選項。

b 若要隱藏具有私密金鑰的憑證並僅查看 CA 憑證清單，請選取**隱藏服務憑證**核取方塊。

8 若要針對伺服器憑證啟用一般名稱檢查，請開啟**一般名稱檢查**選項，並為集區輸入最多 10 個網域名稱。

9 按一下**儲存**。

後續步驟

建立虛擬服務.

建立虛擬服務

虛擬服務會接聽 IP 位址的流量、處理用戶端請求，並將有效請求導向至負載平衡器伺服器集區的成員。

虛擬服務是 IP 位址與使用單一網路通訊協定的連接埠的組合。虛擬服務會通告至外部網路，並且正在接聽用戶端請求。當用戶端連線至虛擬服務時，負載平衡器會將請求導向至您所設定之負載平衡器伺服器集區的成員。

若要保護虛擬服務的 SSL 終止，可以使用憑證程式庫中的憑證。如需詳細資訊，請參閱將憑證匯入至憑證程式庫。

必要條件

- 在 NSX-T Data Center Edge 閘道上啟用負載平衡器。
- 將服務引擎群組指派給 NSX-T Data Center Edge 閘道。
- 新增負載平衡器伺服器集區。

程序

1 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，按一下 **Edge 閘道**。

3 按一下要在其上建立虛擬服務的 NSX-T Data Center Edge 閘道。

4 在 [負載平衡器] 下，按一下**虛擬服務**，然後按一下**新增**。

5 為虛擬服務輸入有意義的名稱，並選擇性地輸入說明。

6 若要在建立時啟動虛擬服務，請開啟**已啟用**選項。

7 為虛擬服務選取服務引擎群組。

8 為虛擬服務選取負載平衡器集區。

9 輸入虛擬服務的 IP 位址。

10 選取虛擬服務類型。

選項	敘述
HTTP	虛擬服務會接聽不安全的第 7 層 HTTP 要求。 如果選取此服務類型，則會將服務連接埠文字方塊自動填入為 80，您可以將其取代為其他有效的連接埠號碼。
HTTPS	虛擬服務會接聽安全的第 7 層 HTTPS 要求。 如果選取此服務類型，則會將服務連接埠文字方塊自動填入為連接埠 443，您可以將其取代為其他有效的連接埠號碼。選取要用於 SSL 終止的 SSL 憑證。
L4	虛擬服務會接聽第 4 層要求。 如果選取此服務類型，則會將服務連接埠文字方塊自動填入為 80，您可以將其取代為其他有效的連接埠號碼。
L4 TLS	虛擬服務會接聽安全的第 4 層 TLS 要求。 如果選取此服務類型，則會將服務連接埠文字方塊自動填入為 TCP 連接埠 443，您可以將其取代為其他有效的連接埠號碼。選取要用於 SSL 終止的 SSL 憑證。

11 按一下**儲存**。

管理專用 vCenter Server 執行個體 9

透過專用 vCenter Server 執行個體，您可以將 VMware Cloud Director 用作 vSphere 環境的管理中心點 (CPOM)。

將 vCenter Server 執行個體新增至 VMware Cloud Director 時，您可以指定執行個體的用途。

專用 vCenter Server

連結的 vCenter Server 執行個體的基礎結構將封裝做為軟體定義資料中心 (SDDC)，並且完全專用於單一承租人。您可以啟用該執行個體的承租人存取以建立專用 vCenter Server 執行個體。啟用承租人存取後，您可以將專用 vCenter Server 執行個體發佈至承租人。

已共用 vCenter Server

提供者可以跨多個提供者 VDC 使用 vCenter Server 執行個體的不同資源集區，然後將這些資源集區配置給不同的承租人。共用 vCenter Server 執行個體無法發佈至承租人。

無

vCenter Server 執行個體沒有任何特定用途。

VMware Cloud Director 可以充當專用 vCenter Server 執行個體以及沒有設定用途之 vCenter Server 執行個體的 HTTP Proxy 伺服器。

透過專用 vCenter Server 執行個體，您可以將 VMware Cloud 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專用 vCenter Server。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 存取此專用 vCenter Server 執行個體。
- 您可以將 VMware Cloud Director 用作登錄所有 vCenter Server 執行個體的輕量型目錄。
- 您可以將 VMware Cloud Director 用作所有 vCenter Server 執行個體的 API 端點。

您可以在目標 vCenter Server 執行個體連結至 VMware Cloud Director 的期間或之後，啟用承租人存取並將 vCenter Server 執行個體標記為專用。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。

透過使用連結的 vCenter Server 執行個體，您可以建立共用 vCenter Server 或專用 vCenter Server。如果已建立共用 vCenter Server 執行個體，則無法使用此 vCenter Server 執行個體建立專用 vCenter Server，反之亦然。

您可以建立可供承租人用來存取基礎 vSphere 環境的端點。透過使用其 VMware Cloud Director 帳戶，使用者可以使用或不使用 Proxy 登入元件的使用者介面或 API。

VMware Cloud Director 中的專用 vCenter Server 執行個體移除了 vCenter Server 可供公開存取的需求。若要控制存取，您可以啟用和停用對 VMware Cloud Director 中 SDDC 的承租人存取。

端點可用作 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。可以將端點連線至 Proxy。透過啟用和停用 Proxy，您可以透過該 Proxy 來允許和停止承租人存取。

從 VMware Cloud Director 10.2 開始，如果使用 API 查詢專用 vCenter Server 和 Proxy 實體，並且您的承租人組態支援多站台關聯，則 VMware Cloud Director 會傳回多站台回應。結果來自所有可用的關聯。

建立和管理專用 vCenter Server 執行個體

若要建立和管理專用 vCenter Server 執行個體及 Proxy，您可以使用服務提供者管理入口網站或 VMware Cloud Director OpenAPI。對於 VMware Cloud Director OpenAPI，請參閱 VMware Cloud Director OpenAPI 入門，網址為：https://code.vmware.com。

重要 VMware Cloud Director 需要與每個專用 vCenter Server 執行個體建立直接網路連線。如果 vCenter Server 執行個體使用外部 Platform Services Controller，VMware Cloud Director 也需要與 Platform Services Controller 建立直接網路連線。

若要在代理的專用 vCenter Server 中使用 VMware OVF Tool，VMware Cloud Director 需要與每台 ESXi 主機建立直接連線。

1 建立專用 vCenter Server 執行個體。

   當您將 vCenter Server 執行個體新增至 VMware Cloud Director 環境時，您可以在**新增 vCenter Server** 精靈中啟用承租人存取，以建立專用的 vCenter Server 執行個體。請參閱新增 vCenter Server 執行個體。

   建立專用 vCenter Server 執行個體將同時為其建立預設端點。連結 vCenter Server 執行個體時，您也可以建立 Proxy。但是，依預設，預設端點不會連線至任何 Proxy。您必須編輯預設端點或建立新端點，才能將其連線至 Proxy。請參閱建立端點。

   您可以啟用已新增至 VMware Cloud Director 且沒有指定用途的 vCenter Server 執行個體的承租人存取。請參閱啟用連結的 vCenter Server 的承租人存取。啟用承租人存取會使 vCenter Server 執行個體可發佈至承租人。

2 新增 Proxy。

   可以在將 vCenter Server 執行個體連結至 VMware Cloud Director 時建立 Proxy，也可以稍後建立。如果 vCenter Server 執行個體使用外部 Platform Services Controller，則 VMware Cloud Director 也會為 Platform Services Controller 建立 Proxy。透過父系和子系 Proxy，您可以向承租人隱藏特定 Proxy，也可以透過其父系 Proxy 啟用和停用子系 Proxy 的群組。如需在將 vCenter Server 執行個體新增至 VMware Cloud Director 後建立 Proxy 的相關資訊，請參閱新增用於存取基礎 vCenter Server 資源的 Proxy。

您可以從 **vSphere 資源**下的 **Proxy** 索引標籤中編輯、啟用、停用和刪除 Proxy。

備註 將 Proxy 新增至專用 vCenter Server 執行個體時，您必須上傳憑證和指紋，以便在代理元件使用自我簽署憑證時，承租人可擷取該憑證和指紋。

若要檢視和管理憑證及憑證撤銷清單 (CRL)，請參閱管理 Proxy 憑證和 CRL。

3 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。請參閱管理 Proxy 憑證和 CRL。

4 將專用 vCenter Server 執行個體發佈到一或多個組織。

您可以將專用 vCenter Server 執行個體發佈至承租人，並使其在 VMware Cloud Director Tenant Portal 中顯示。在大多數情況下，應僅將一個 vCenter Server 執行個體發佈到一個承租人。請參閱發佈專用 vCenter Server。

5 若要讓承租人能夠從 VMware Cloud Director Tenant Portal 存取專用 vCenter Server 執行個體和 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。

本章節討論下列主題：

- 啟用連結的 vCenter Server 的承租人存取
- 發佈專用 vCenter Server

啟用連結的 vCenter Server 的承租人存取

您可以啟用已新增至 VMware Cloud Director 且沒有指定用途的 vCenter Server 執行個體的承租人存取。啟用承租人存取會建立專用的 vCenter Server 執行個體，並使其可發佈至承租人。

透過使用連結的 vCenter Server 執行個體，您可以建立共用 vCenter Server 或專用 vCenter Server。如果您已建立共用 vCenter Server 執行個體，並且想要將其用作專用 vCenter Server，則必須先刪除使用 vCenter Server 執行個體資源的所有提供者虛擬資料中心 (VDC)。刪除連結至共用 vCenter Server 執行個體的所有提供者 VDC 會將其狀態變更為 [無]。

必要條件

確認您的環境中至少有一個非專用或共用的已連結的 vCenter Server。

程序

1 從頂部導覽列的**資源**下，按一下**基礎結構資源**。

2 在左面板中，選取 **vCenter Server 執行個體**。

3 在**使用情況**欄中，選取沒有指定用途的 vCenter Server。

4 按一下**啟用承租人存取**。

後續步驟

發佈專用 vCenter Server.

發佈專用 vCenter Server

您可以將專用 vCenter Server 發佈至承租人，並使其可透過 VMware Cloud Director Tenant Portal 顯示。依預設，應僅將一個 vCenter Server 發佈到一個承租人。

依預設，SDDC 是一個 vCenter Server 執行個體，可透過將對應的專用 vCenter Server 執行個體僅發佈到其組織，使其專用於單一承租人。該承租人不與其他承租人共用專用 vCenter Server 執行個體。將專用 vCenter Server 執行個體發佈到多個承租人會違反承租人邊界。但是，有時承租人必須具有多個專用 vCenter Server 執行個體的存取權。在這些情況下，您可以將專用 vCenter Server 執行個體發佈到多個承租人。

必要條件

- 確認您的 VMware Cloud Director 環境中至少有一個已啟用承租人存取的 vCenter Server 執行個體。請參閱第 9 章 管理專用 vCenter Server 執行個體。

程序

1. 從頂部導覽列的**資源**下，按一下**基礎結構資源**。
2. 在左面板中，選取 **vCenter Server 執行個體**。
3. 選取已啟用承租人存取的 vCenter Server。

   已啟用承租人存取的 vCenter Server 執行個體在**使用量**欄中具有專用值。
4. 按一下**管理承租人**。
5. 選取要將 vCenter Server 執行個體發佈到的一或多個承租人。

   從清單中取消選取承租人會解除發佈 vCenter Server。
6. 按一下**儲存**。

後續步驟

若要讓使用者能夠從 VMware Cloud Director Tenant Portal 存取專用 vCenter Server 執行個體和 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。

管理系統管理員與角色

10

透過使用 VMware Cloud Director 服務提供者管理入口網站，您可以將系統管理員個別新增至 VMware Cloud 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 VMware Cloud Director 9.5 開始，服務提供者可以使用 VMware Cloud Director 服務提供者管理入口網站或 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《VMware Cloud 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 VMware Cloud 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。

VMware Cloud 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。VMware Cloud 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。

系統管理員可以使用權限服務包和全域承租人角色來管理可供每個組織使用的權限和角色。

安裝 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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《VMware Cloud Director 租用戶入口網站指南》。

預先定義的角色與其權限

每個 VMware Cloud 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。如需僅適用於**系統管理員**角色的權限清單，請參閱系統管理員權限。**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 Cloud Director OpenAPI 請求。

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。具有預先定義之**組織管理員**角色的使用者可以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)。

- 如果由 OAuth 身分識別提供者定義使用者，將為使用者指派在使用者之 OAuth Token 的 `roles` 陣列中命名的角色。
- 如果由 SAML 身分識別提供者定義使用者，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

系統管理員可以使用 Service Provider Admin Portal 檢視角色中所包含的權限清單。

1 在頂部導覽列中，按一下**管理**。

2 從左面板中的**提供者存取控制**下，選取**角色**。

3 按一下您要檢視的角色名稱。

組織管理員可以使用 Service Provider Admin Portal 或 Cloud Director OpenAPI 來檢視角色中的權限，或建立組織的本機角色。

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。如需預先定義之承租人角色中的權限清單，請參閱預先定義之全域承租人角色中的權限。

系統管理員權限

系統管理員角色僅存在於提供者組織中。依預設，**系統管理員**角色具有所有 VMware Cloud Director 權限。

系統管理員角色具有所有 VMware Cloud Director 權限。此清單包含僅適用於**系統管理員**的權限。**系統管理員**角色也具有預先定義之全域承租人角色中的權限。

表 10-1. 預設僅供系統管理員使用的權限

此版本的新增內容	權限名稱
	存取所有組織 VDC
	存取控制清單：管理
	存取控制清單：檢視

表 10-1. 預設僅供系統管理員使用的權限 (續)

此版本的新增內容	權限名稱
	其他服務：執行工作流程
	其他服務：檢視執行中工作流程
	其他服務：檢視工作流程
	採用資源集區：檢視
✓	建議定義：建立和刪除
✓	建議定義：讀取
	備用管理實體：檢視
	AMQP 設定：管理
	AMQP 設定：檢視
	API Explorer：檢視
	目錄：從我的雲端新增 vApp
	目錄：變更擁有者
	目錄：建立/刪除目錄
	目錄：編輯內容
	目錄：從 vSphere 匯入媒體
	目錄：發佈
	目錄：陰影虛擬機器視圖
	目錄：共用
	目錄：VCSP 發佈訂閱
	目錄：VCSP 發佈訂閱快取
	目錄：檢視 ACL
	目錄：檢視私人與共用目錄
	目錄：檢視已發佈目錄
	儲存格組態：檢視
	憑證程式庫：管理
	憑證程式庫：檢視
	雲端通道伺服器：管理
	雲端通道伺服器：檢視

表 10-1. 預設僅供系統管理員使用的權限 (續)

此版本的新增內容	權限名稱
	內容程式庫系統設定：管理
	內容程式庫系統設定：檢視
	自訂實體：建立自訂實體定義
	自訂實體：刪除自訂實體定義
	自訂實體：編輯自訂實體定義
	自訂實體：檢視組織中的所有自訂實體執行個體
	自訂實體：檢視自訂實體定義
	自訂實體：檢視自訂實體執行個體
	資料存放區：刪除
	資料存放區：編輯
	資料存放區：啟用或停用
	資料存放區：在 vSphere 中開啟
	資料存放區：檢視
	直接組織 vDC 網路：管理
	分散式虛擬交換器：在 vSphere 中開啟
	Edge 叢集：管理
	Edge 叢集：檢視
	延伸服務 API 定義：管理
	延伸服務 API 定義：檢視
	延伸服務：檢視
	延伸：檢視
	外部服務：管理
	外部服務：檢視
✓	一般 ACL：管理
✓	一般 ACL：檢視
	一般：管理員控制
	一般：管理員檢視
	一般：傳送通知

表 10-1. 預設僅供系統管理員使用的權限 (續)

此版本的新增內容	權限名稱
	一般：檢視錯誤詳細資料
	全域角色：編輯
	全域角色：檢視
	群組/使用者：檢視
	主機：啟用或停用
	主機：管理
	主機：在 vSphere 中開啟
	主機：準備或取消準備
	主機：修復
	主機：升級
	主機：檢視
	混合雲作業：取得控制票證
	混合雲作業：取得源於雲端通道票證
	混合雲作業：取得通向雲端通道票證
	混合雲作業：建立源於雲端通道
	混合雲作業：建立通向雲端通道
	混合雲作業：刪除源於雲端通道
	混合雲作業：刪除通向雲端通道
	混合雲作業：更新源於雲端通道端點標籤
	混合雲作業：檢視源於雲端通道
	混合雲作業：檢視通向雲端通道
	Kerberos 設定：管理
	Kerberos 設定：檢視
	LDAP 設定：管理
	LDAP 設定：檢視
	授權報告：檢視
✓	負載平衡器控制器：編輯
✓	負載平衡器控制器：檢視

表 10-1. 預設僅供系統管理員使用的權限 (續)

此版本的新增內容	權限名稱
✓	負載平衡器服務引擎群組指派：編輯
✓	負載平衡器服務引擎群組指派：檢視
✓	負載平衡器服務引擎群組：編輯
✓	負載平衡器服務引擎群組：檢視
	當地語系化資源：管理
	網路集區：建立或刪除
	網路集區：編輯
	網路集區：在 vSphere 中開啟
	網路集區：修復
	網路集區：檢視
	NSX-T：編輯
	NSX-T：檢視
	物件延伸：管理
	物件延伸：檢視
	組織網路：建立或刪除
	組織網路：編輯內容
	組織網路：在 vSphere 中開啟
	組織網路：檢視
✓	組織配額：管理
	組織 vDC 運算原則：管理檢視
	組織 vDC 運算原則：管理
	組織 vDC 運算原則：檢視
	組織 vDC Distributed Firewall：設定規則
	組織 vDC Distributed Firewall：啟用/停用
	組織 vDC Distributed Firewall：檢視規則
	組織 vDC 閘道：設定 BGP 路由
	組織 vDC 閘道：設定 DHCP
	組織 vDC 閘道：設定 DNS

表 10-1. 預設僅供系統管理員使用的權限 (續)

此版本的新增內容	權限名稱
	組織 vDC 閘道：設定 ECMP 路由
	組織 vDC 閘道：設定防火牆
	組織 vDC 閘道：設定 IPSec VPN
	組織 vDC 閘道：設定 L2 VPN
	組織 vDC 閘道：設定負載平衡器
	組織 vDC 閘道：設定 NAT
	組織 vDC 閘道：設定 OSPF 路由
	組織 vDC 閘道：設定遠端存取
	組織 vDC 閘道：設定路由通告
✓	組織 vDC 閘道：設定 SLAAC 設定檔
	組織 vDC 閘道：設定 SSL VPN
	組織 vDC 閘道：設定靜態路由
	組織 vDC 閘道：設定 Syslog
	組織 vDC 閘道：設定系統記錄
	組織 vDC 閘道：轉換為進階網路
	組織 vDC 閘道：建立
	組織 vDC 閘道：刪除
	組織 vDC 閘道：分散式路由
	組織 vDC 閘道：匯入
	組織 vDC 閘道：修改機器尺寸
	組織 vDC 閘道：更新
	組織 vDC 閘道：更新內容
	組織 vDC 閘道：升級
	組織 vDC 閘道：檢視
	組織 vDC 閘道：檢視 BGP 路由
	組織 vDC 閘道：檢視 DHCP
	組織 vDC 閘道：檢視 DNS
	組織 vDC 閘道：檢視防火牆

表 10-1. 預設僅供系統管理員使用的權限 (續)

此版本的新增內容	權限名稱
	組織 vDC 閘道：檢視 IPSec VPN
	組織 vDC 閘道：檢視 L2 VPN
	組織 vDC 閘道：檢視負載平衡器
	組織 vDC 閘道：檢視 NAT
	組織 vDC 閘道：檢視 OSPF 路由
	組織 vDC 閘道：檢視遠端存取
	組織 vDC 閘道：檢視路由通告
✓	組織 vDC 閘道：檢視 SLAAC 設定檔
	組織 vDC 閘道：檢視 SSL VPN
	組織 vDC 閘道：檢視靜態路由
✓	組織 vDC Kubernetes 原則：編輯
	組織 vDC 具名磁碟：變更擁有者
	組織 vDC 具名磁碟：建立
	組織 vDC 具名磁碟：刪除
	組織 vDC 具名磁碟：編輯內容
	組織 vDC 具名磁碟：檢視加密狀態
	組織 vDC 具名磁碟：檢視內容
	組織 vDC 網路：編輯內容
	組織 vDC 網路：匯入
	組織 vDC 網路：檢視
	組織 vDC 資源集區：在 vSphere 中開啟
	組織 vDC 資源集區：檢視
✓	組織 vDC 共用具名磁碟：建立
	組織 vDC 儲存區原則：編輯
	組織 vDC 儲存區原則：啟用或停用
	組織 vDC 儲存區原則：在 vSphere 中開啟
	組織 vDC 儲存區原則：移除
	組織 vDC 儲存區原則：檢視功能

表 10-1. 預設僅供系統管理員使用的權限 (續)

此版本的新增內容	權限名稱
	組織 vDC 儲存區設定檔：設定預設值
	組織 vDC：建立
	組織 vDC：刪除
	組織 vDC：編輯 ACL
	組織 vDC：啟用或停用
	組織 vDC：延伸編輯
	組織 vDC：延伸檢視
	組織 vDC：管理防火牆
	組織 vDC：簡單編輯
	組織 vDC：使用者檢視
	組織 vDC：檢視 ACL
	組織 VDC：檢視度量
	組織 vDC：虛擬機器-虛擬機器相似性編輯
	組織：啟動或停用
	組織：建立或刪除
	組織：編輯關聯設定
	組織：編輯同盟設定
	組織：編輯 LDAP 設定
	組織：編輯租用原則
	組織：編輯限制
	組織：編輯名稱
	組織：編輯 OAuth 設定
	組織：編輯密碼原則
	組織：編輯內容
	組織：編輯配額原則
	組織：編輯 SMTP 設定
	組織：編輯 VDC ACL 時從 IdP 匯入使用者/群組
	組織：移轉承租人儲存區

表 10-1. 預設僅供系統管理員使用的權限 (續)

此版本的新增內容	權限名稱
	組織：執行管理員查詢
	組織：使用提供者 LDAP 做為承租人
	組織：檢視
	組織：檢視度量
	連接埠群組：在 vSphere 中開啟
	喜好設定：管理喜好設定定義
	提供者網路：建立或刪除
	提供者網路：編輯
	提供者網路：在 vSphere 中開啟
	提供者網路：檢視
	提供者 vDC 運算原則：管理
	提供者 vDC 運算原則：檢視
	提供者 vDC 資源集區：移轉虛擬機器
	提供者 vDC 資源集區：在 vSphere 中開啟
	提供者 vDC 資源集區：檢視
	提供者 vDC 儲存區原則：編輯
	提供者 vDC 儲存區原則：啟用或停用
	提供者 vDC 儲存區原則：在 vSphere 中開啟
	提供者 vDC 儲存區原則：移除
	提供者 vDC 儲存區原則：檢視
	提供者 vDC：新增資源集區
	提供者 vDC：建立或刪除
	提供者 vDC：刪除資源集區
	提供者 vDC：編輯
	提供者 vDC：啟用或停用
	提供者 vDC：啟用或停用資源集區
	提供者 vDC：啟用 vSphere VXLAN
	提供者 vDC：合併

表 10-1. 預設僅供系統管理員使用的權限 (續)

此版本的新增內容	權限名稱
	提供者 vDC：檢視
✓	配額原則功能：檢視
✓	配額原則：管理
✓	配額原則：檢視
	重新載入虛擬機器：管理
	資源類別動作：管理
	資源類別動作：檢視
	資源集區：開啟
	資源集區：在 vSphere 中開啟
	資源集區：檢視
	權限：管理
	權限：檢視
	權限服務包：編輯
	權限服務包：檢視
	角色：建立、編輯、刪除或複製
	SDDC：管理
	SDDC：管理 Proxy
	SDDC：檢視
	選取器延伸：管理
	選取器延伸：檢視
	服務應用程式：管理
	服務應用程式：檢視
	服務授權：管理
	服務組態：管理
	服務組態：檢視
	服務程式庫：建立服務程式庫
	服務程式庫：從服務程式庫中刪除服務
	服務程式庫：編輯服務中繼資料

表 10-1. 預設僅供系統管理員使用的權限 (續)

此版本的新增內容	權限名稱
	服務程式庫：編輯服務的內容
	服務程式庫：檢視服務程式庫
	服務連結：管理
	服務連結：檢視
	服務資源類型：管理
	服務資源類型：檢視
	服務資源：管理
	服務資源：檢視
	共用的組織 vDC 網路：管理
	站台：編輯
	站台：檢視
	SSL 設定：檢視
✓ (在 10.2.2 版及更新版本中提供)	**SSL 設定：管理**
✓	**SSL：測試連線**
	停頓的項目：管理
	停頓的項目：檢視
✓ (在 10.2.2 版及更新版本中提供)	**支援的儲存區實體類型：管理**
	系統作業：執行系統作業
	系統組織：管理
	系統組織：檢視
	系統設定：管理
	系統設定：檢視
✓	**Tanzu Kubernetes 客體叢集：管理員完全控制**
✓	**Tanzu Kubernetes 客體叢集：管理員視圖**
✓	**Tanzu Kubernetes 客體叢集：編輯**
✓	**Tanzu Kubernetes 客體叢集：完全控制**
✓	**Tanzu Kubernetes 客體叢集：視圖**

表 10-1. 預設僅供系統管理員使用的權限 (續)

此版本的新增內容	權限名稱
	工作：繼續、中止或失敗
	工作：更新
	工作：檢視工作
	Token：管理
	Token：管理所有
	信任存放區：管理
	信任存放區：檢視
	UI 外掛程式：定義、上傳、修改、刪除、關聯或解除關聯
	UI 外掛程式：檢視
	UI 入口網站商標：管理
	vApp 範本/媒體：複製
	vApp 範本/媒體：建立/上傳
	vApp 範本/媒體：編輯
	vApp 範本/媒體：檢視
	vApp 範本：新增至我的雲端
	vApp 範本：變更擁有者
	vApp 範本：下載
	vApp 範本：強制儲存區租用到期
	vApp 範本：匯入
	vApp 範本：在 vSphere 中開啟
	vApp：允許所有額外組態
	vApp：允許乙太網路聯合額外組態
	vApp：允許延遲額外組態
	vApp：允許相符的額外組態
	vApp：允許 NUMA 節點相似性額外組態
	vApp：變更擁有者
	vApp：複製
	vApp：建立/重新設定

表 10-1. 預設僅供系統管理員使用的權限 (續)

此版本的新增內容	權限名稱
	vApp：刪除
	vApp：下載
	vApp：編輯內容
	vApp：編輯虛擬機器運算原則
	vApp：編輯虛擬機器 CPU
	vApp：編輯所有 VDC 類型中的虛擬機器 CPU 和記憶體保留設定
	vApp：編輯虛擬機器硬碟
	vApp：編輯虛擬機器記憶體
	vApp：編輯虛擬機器網路
	vApp：編輯虛擬機器內容
	vApp：進入/退出維護模式
	vApp：強制執行階段租用到期
	vApp：強制儲存區租用到期
	vApp：匯入選項
	vApp：維護管理
	vApp：管理虛擬機器密碼設定
	vApp：在 vSphere 中開啟
	vApp：電源作業
	vApp：陰影虛擬機器視圖
	vApp：共用
	vApp：快照作業
	vApp：上傳
	vApp：使用主控台
	vApp：檢視 ACL
	vApp：檢視虛擬機器和虛擬機器的磁碟加密狀態
	vApp：檢視虛擬機器度量
	vApp：虛擬機器開機選項
	vApp：虛擬機器檢查符合性

表 10-1. 預設僅供系統管理員使用的權限 (續)

此版本的新增內容	權限名稱
	vApp：虛擬機器移轉、強制取消部署、重新放置、合併
	VAPP_VM_METADATA_TO_VCENTER
	VCD 延伸：登錄、解除登錄、重新整理、關聯或解除關聯
	VCD 延伸：檢視
	vCenter：連結或中斷連結
	vCenter：啟用或停用
	vCenter：在 vSphere 中開啟
	vCenter：重新整理
	vCenter：檢視
	vDC 群組：設定
✓	vDC 群組：設定記錄
	vDC 群組：檢視
	VDC 範本：ACL 管理
	VDC 範本：延伸檢視
	VDC 範本：具現化
	VDC 範本：管理
	VDC 範本：檢視
	VMC：登錄 SDDC
✓	VMWARE:NATIVECLUSTER：管理員完全控制
✓	VMWARE:NATIVECLUSTER：管理員檢視
✓	VMWARE:NATIVECLUSTER：編輯
✓	VMWARE:NATIVECLUSTER：完全控制
✓	VMWARE:NATIVECLUSTER：檢視
	vRealize Orchestrator：向承租人發佈和解除發佈工作流程
	vRealize Orchestrator：登錄和解除登錄 vRealize Orchestrator 伺服器
	vRealize Orchestrator：檢視已登錄的 vRealize Orchestrator 伺服器
	vSphere 伺服器：管理
	vSphere 伺服器：管理 Proxy

表 10-1. 預設僅供系統管理員使用的權限 (續)

此版本的新增內容	權限名稱
	vSphere 伺服器：管理 Proxy 組態
	vSphere 伺服器：檢視

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。

VMware Cloud Director 全域承租人角色中包含的權限

此版本的新增內容	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
	存取所有組織 VDC	✓				
	目錄：從我的雲端新增 vApp	✓	✓	✓		
	目錄：變更擁有者	✓				
	目錄：建立/刪除目錄	✓	✓			
	目錄：編輯內容	✓	✓			
	目錄：發佈	✓	✓			
	目錄：共用	✓	✓			
	目錄：VCSP 發佈訂閱	✓	✓			
	目錄：檢視 ACL	✓	✓			
	目錄：檢視私人與共用目錄	✓	✓	✓		
	目錄：檢視已發佈目錄	✓				
	憑證程式庫：管理	✓				
	憑證程式庫：檢視	✓				
	自訂實體：檢視組織中的所有自訂實體執行個體	✓				
	自訂實體：檢視自訂實體執行個體	✓				
	一般：管理員控制	✓				
	一般：管理員檢視	✓				
	一般：傳送通知	✓				
	群組/使用者：檢視	✓				
	混合雲作業：取得控制票證	✓				

此版本的新增內容	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
	混合雲作業：取得源於雲端通道憑證	✓				
	混合雲作業：取得通向雲端通道憑證	✓				
	混合雲作業：建立源於雲端通道	✓				
	混合雲作業：建立通向雲端通道	✓				
	混合雲作業：刪除源於雲端通道	✓				
	混合雲作業：刪除通向雲端通道	✓				
	混合雲作業：更新源於雲端通道端點標籤	✓				
	混合雲作業：檢視源於雲端通道	✓				
	混合雲作業：檢視通向雲端通道	✓				
	組織網路：編輯內容	✓				
	組織網路：檢視	✓				
	組織 vDC 運算原則：檢視	✓	✓	✓	✓	
	組織 vDC Distributed Firewall：設定規則	✓				
	組織 vDC Distributed Firewall：檢視規則	✓				
	組織 vDC 閘道：設定 DHCP	✓				
	組織 vDC 閘道：設定 DNS	✓				
	組織 vDC 閘道：設定 ECMP 路由	✓				
	組織 vDC 閘道：設定防火牆	✓				
	組織 vDC 閘道：設定 IPSec VPN	✓				
	組織 vDC 閘道：設定負載平衡器	✓				
	組織 vDC 閘道：設定 NAT	✓				
	組織 vDC 閘道：設定靜態路由	✓				
	組織 vDC 閘道：設定 Syslog	✓				
	組織 vDC 閘道：轉換為進階網路	✓				
	組織 vDC 閘道：檢視	✓				
	組織 vDC 閘道：檢視 DHCP	✓				
	組織 vDC 閘道：檢視 DNS	✓				

此版本的新增內容	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 vDC 閘道：檢視防火牆	✓				
	組織 vDC 閘道：檢視 IPSec VPN	✓				
	組織 vDC 閘道：檢視負載平衡器	✓				
	組織 vDC 閘道：檢視 NAT	✓				
	組織 vDC 閘道：檢視靜態路由	✓				
	組織 vDC 具名磁碟：變更擁有者	✓	✓			
	組織 vDC 具名磁碟：建立	✓	✓	✓		
	組織 vDC 具名磁碟：刪除	✓	✓	✓		
	組織 vDC 具名磁碟：編輯內容	✓	✓	✓		
	組織 vDC 具名磁碟：檢視加密狀態	✓		✓		
	組織 vDC 具名磁碟：檢視內容	✓	✓	✓	✓	
	組織 vDC 網路：編輯內容	✓				
	組織 vDC 網路：檢視	✓		✓		
	組織 vDC 儲存區原則：檢視功能	✓				
	組織 vDC 儲存區設定檔：設定預設值	✓				
	組織 vDC：編輯 ACL	✓				
	組織 vDC：管理防火牆	✓				
	組織 vDC：簡單編輯	✓				
	組織 vDC：使用者檢視	✓	✓			
	組織 vDC：檢視 ACL	✓				
	組織 VDC：檢視度量	✓				
	組織 vDC：虛擬機器-虛擬機器相似性編輯	✓	✓	✓		
	組織：編輯關聯設定	✓				
	組織：編輯同盟設定	✓				
	組織：編輯租用原則	✓				
	組織：編輯 OAuth 設定	✓				
	組織：編輯密碼原則	✓				
	組織：編輯內容	✓				

此版本的新增內容	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：編輯配額原則	✓				
	組織：編輯 SMTP 設定	✓				
	組織：編輯 VDC ACL 時從 IdP 匯入使用者/群組	✓				
	組織：檢視	✓	✓	✓		
	組織：檢視度量	✓				
✓	配額原則功能：檢視	✓				
	角色：建立、編輯、刪除或複製	✓				
	服務程式庫：檢視服務程式庫	✓				
✓	SSL：測試連線	✓	✓			
	UI 外掛程式：檢視	✓	✓	✓	✓	
✓ (在 10.2.1 版及更新版本中提供)	信任存放區：管理	✓				
✓ (在 10.2.1 版及更新版本中提供)	信任存放區：檢視	✓				
	UI 外掛程式：檢視	✓	✓	✓	✓	
	vApp 範本/媒體：複製	✓	✓	✓		
	vApp 範本/媒體：建立/上傳	✓	✓			
	vApp 範本/媒體：編輯	✓	✓	✓		
	vApp 範本/媒體：檢視	✓	✓	✓	✓	
	vApp 範本：新增至我的雲端	✓	✓	✓	✓	
	vApp 範本：變更擁有者	✓	✓			
	vApp 範本：下載	✓	✓			
	vApp：變更擁有者	✓				
	vApp：複製	✓	✓	✓	✓	
	vApp：建立/重新設定	✓	✓	✓		
	vApp：刪除	✓	✓	✓	✓	
	vApp：下載	✓	✓	✓		

此版本的新增內容	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：編輯內容	✓	✓	✓	✓	
	vApp：編輯虛擬機器運算原則	✓	✓	✓		
	vApp：編輯虛擬機器 CPU	✓	✓	✓		
	vApp：編輯虛擬機器硬碟	✓	✓	✓		
	vApp：編輯虛擬機器記憶體	✓	✓	✓		
	vApp：編輯虛擬機器網路	✓	✓	✓	✓	
	vApp：編輯虛擬機器內容	✓	✓	✓	✓	
	vApp：管理虛擬機器密碼設定	✓	✓	✓	✓	✓
	vApp：電源作業	✓	✓	✓	✓	
	vApp：共用	✓	✓	✓	✓	
	vApp：快照作業	✓	✓	✓	✓	
	vApp：上傳	✓	✓	✓		
	vApp：使用主控台	✓	✓	✓	✓	✓
	vApp：檢視 ACL	✓	✓	✓	✓	
	vApp：檢視虛擬機器和虛擬機器的磁碟加密狀態	✓		✓		
	vApp：檢視虛擬機器度量	✓		✓	✓	
	vApp：虛擬機器開機選項	✓	✓	✓		
	vApp：虛擬機器中繼資料至 vCenter	✓	✓	✓		
✓	VDC 群組：設定	✓				
✓	VDC 群組：設定記錄	✓				
✓	VDC 群組：檢視	✓				
	VDC 範本：具現化	✓				
	VDC 範本：檢視	✓				

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 從頂部導覽列中，選取**管理**。

2 在左面板中的**承租人存取控制**下，選取**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 VMware Cloud 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**。

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。

複製權限服務包

您可以將現有的權限服務包用作建立新服務包的範本。

必要條件

確認您具有將新角色新增至 VMware Cloud Director 的權限。

程序

1 從頂部導覽列中，選取**管理**。

2 在左面板中的**承租人存取控制**下，選取**權限服務包**。

3 選取您要複製的權限服務包，然後按一下**複製**。

4 在**複製權限服務包**視窗中，為複製的服務包輸入名稱和說明。

5 (選擇性) 若要編輯複製的權限，請開啟**修改所選權限**切換按鈕，然後選取或取消選取要針對已複製角色變更的權限。

6 按一下**儲存**。

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 從頂部導覽列中，選取**管理**。

2 在左面板中的**承租人存取控制**下，選取**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 從頂部導覽列中，選取**管理**。

2 在左面板中的**承租人存取控制**下，選取**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 從頂部導覽列中，選取**管理**。

2 在左面板中的**承租人存取控制**下，選取**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。

VMware Cloud 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。

VMware Cloud 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 從頂部導覽列中，選取**管理**。

2 在左面板中的**承租人存取控制**下，選取**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 VMware Cloud 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 VMware Cloud 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。

複製全域承租人角色

您可以將現有的全域承租人角色用作建立新角色的範本。

必要條件

確認您具有將新角色新增至 VMware Cloud Director 的權限。

程序

1 從頂部導覽列中，選取**管理**。

2 在左面板中的**承租人存取控制**下，選取**全域角色**。

3 選取您要複製的角色，然後按一下**複製**。

4 在**複製全域角色**視窗中，為複製的角色輸入名稱和說明。

5 (選擇性) 若要編輯複製的權限，請開啟**修改所選權限**切換按鈕，然後選取或取消選取要針對已複製角色變更的權限。

6 按一下**儲存**。

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 從頂部導覽列中，選取**管理**。

2 在左面板中的**承租人存取控制**下，選取**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 從頂部導覽列中，選取**管理**。

2 在左面板中的**承租人存取控制**下，選取**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 從頂部導覽列中，選取**管理**。

2 在左面板中的**承租人存取控制**下，選取**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 VMware Cloud 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《VMware Cloud Director 租用戶入口網站指南》。

建立提供者角色

您可以在 VMware Cloud Director 提供者組織中建立角色。

VMware Cloud 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 從頂部導覽列中，選取**管理**。

2 在左面板中的**提供者存取控制**下，選取**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。

類別	描述
延伸	包含用於檢視和管理 VMware Cloud 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。

複製提供者角色

您可以將現有的提供者角色用作建立新角色的範本。

必要條件

確認您具有將新角色新增至 VMware Cloud Director 的權限。

程序

1 從頂部導覽列中，選取**管理**。

2 在左面板中的**提供者存取控制**下，選取**角色**。

3 選取您要複製的角色，然後按一下**複製**。

4 在**複製角色**視窗中，為複製的角色輸入名稱和說明。

5 (選擇性) 若要編輯複製的權限，請開啟**修改所選權限**切換按鈕，然後選取或取消選取要針對已複製角色變更的權限。

6 按一下**儲存**。

檢視或編輯提供者角色

您可以檢視 VMware Cloud 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 從頂部導覽列中，選取**管理**。

2 在左面板中的**提供者存取控制**下，選取**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 VMware Cloud 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 從頂部導覽列中，選取**管理**。

2 在左面板中的**提供者存取控制**下，選取**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 VMware Cloud 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《VMware Cloud 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《VMware Cloud Director 租用戶入口網站指南》。

建立提供者使用者

您可以在 VMware Cloud Director 提供者組織中建立使用者。

安裝和設定 VMware Cloud 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 從頂部導覽列中，選取**管理**。

2 在左面板中的**提供者存取控制**下，選取**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 VMware Cloud 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 從頂部導覽列中，選取**管理**。

2 在左面板中的**提供者存取控制**下，選取**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 從頂部導覽列中，選取**管理**。

2 在左面板中的**提供者存取控制**下，選取**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**。

啟用或停用提供者使用者

停用使用者後，該使用者便無法登入 VMware Cloud Director。

程序

1 從頂部導覽列中，選取**管理**。

2 在左面板中的**提供者存取控制**下，選取**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 VMware Cloud Director 提供者組織中移除使用者。

若要刪除因刪除其 LDAP 群組而失去存取權之停頓的使用者，請使用 VMware Cloud Director API。

必要條件

停用您要刪除的使用者。請參閱啟用或停用提供者使用者。

程序

1 從頂部導覽列中，選取**管理**。

2 在左面板中的**提供者存取控制**下，選取**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，請參閱設定密碼原則。

程序

1 從頂部導覽列中，選取**管理**。

2 在左面板中的**提供者存取控制**下，選取**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《VMware Cloud 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 VMware Cloud 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 從頂部導覽列中，選取**管理**。

2 在左面板中的**提供者存取控制**下，選取**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 VMware Cloud Director 提供者組織的群組成員的角色。

程序

1 從頂部導覽列中，選取**管理**。

2 在左面板中的**提供者存取控制**下，選取**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 VMware Cloud Director 提供者組織中移除群組

程序

1 從頂部導覽列中，選取**管理**。

2 在左面板中的**提供者存取控制**下，選取**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

VMware Cloud 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：

- 修改一般系統設定
- 一般系統設定
- 在伺服器群組中的儲存格上啟用 FIPS 模式
- 設定系統電子郵件設定
- 變更 VMware Cloud Director 授權
- 設定目錄同步設定
- 建立建議儀表板
- 設定和監控封鎖工作及通知
- 設定公用位址
- 管理身分識別提供者
- 管理憑證
- 管理外掛程式
- 自訂 VMware Cloud Director 入口網站
- 設定密碼原則
- 設定 vSphere 服務

修改一般系統設定

VMware Cloud Director 包含與活動記錄、網路、工作階段逾時、憑證、組織限制、運作限制等相關的一般系統設定。預設設定可正確使用於許多環境，但您可以修改設定以符合您的需求。

如需您可以修改的內容清單，請參閱一般系統設定。

備註 如需變更 VMware Cloud Director 應用裝置的日期、時間或時區的相關資訊，請參閱 https://kb.vmware.com/kb/59674。

程序

1 從頂部導覽列中，選取**管理**。

2 在左面板中的**設定**下，按一下**一般**。

3 針對您要修改的區段按一下**編輯**，編輯內容，然後按一下**儲存**。

一般系統設定

VMware Cloud Director 包括您可以修改以符合需求的一般系統設定。

表 11-1. 一般系統設定

名稱	類別	描述
Activity log history to keep	活動記錄	刪除記錄前要保留的記錄歷程記錄天數。 輸入 0 將永不刪除記錄。
Activity log history shown	活動記錄	顯示記錄歷程記錄天數。 若要顯示所有活動，請輸入 0。
Display debug information	活動記錄	啟用此設定以在 VMware Cloud Director 工作記錄中顯示偵錯資訊。
IP address release timeout	網路作業	將釋放的 IP 位址再次提供配置之前，要保留這些位址的秒數。這項預設設定為 2 小時 (7200 秒)，以允許舊項目從用戶端 ARP 表格到期。
Allow Overlapping External Networks	網路作業	若要新增在相同網路區段上執行的外部網路，請選取核取方塊。 只有在使用不是以 VLAN 為基礎的方法隔離外部網路時，才應該啟用此設定。
Allow FIPS mode	網路作業	允許在 Edge 閘道上啟用 FIPS 模式。需要 NSX 6.3 或更新版本。請參閱 VMware NSX for vSphere 說明文件中的〈FIPS 模式〉。
Default syslog server settings for networks	網路作業	輸入最多兩個 Syslog 伺服器的 IP 位址供網路使用。此設定不會套用至雲端儲存格使用的 Syslog 伺服器。
Provider Locale	當地語系化	選取提供者活動的地區設定，包括記錄項目、電子郵件警示以及其他項目。
Idle session timeout	逾時	VMware Cloud Director 應用程式在沒有使用者互動時保持作用中狀態的時間。
Maximum session timeout	逾時	VMware Cloud Director 應用程式保持作用中狀態的最長時間量。
Host refresh frequency	逾時	VMware Cloud Director 檢查其 ESXi 主機是否可存取的頻率。
Host hung timeout	逾時	選取將主機標示為無回應前的時間數。
Transfer session timeout	逾時	將已暫停或已取消上傳工作 (例如上傳媒體或上傳 vApp 範本) 視為失敗之前的等待時間數。此逾時不會影響進行中的上傳工作。

表 11-1. 一般系統設定 (續)

名稱	類別	描述
Enable upload quarantine with a timeout of __ seconds	逾時	選取核取方塊並輸入逾時數，表示將隔離已上傳檔案的等候時間量。
Verify vCenter and vSphere SSO certificates	憑證	VMware Cloud Director 將始終驗證憑證。啟用後，會驗證 vCenter Server 憑證中的主機名稱。
Verify NSX Manager certificates	憑證	VMware Cloud Director 將始終驗證憑證。啟用後，VMware Cloud Director 會驗證 NSX Manager 憑證中的主機名稱。
Edit Organization Limits	組織 VDC 限制	輸入每一組織的組織虛擬資料中心數目上限，或選取**無限制**。
Number of resource intensive operations running per user	作業限制	輸入每個使用者的同時資源密集型作業數目上限，或選取**無限制**。
Number of resource intensive operations to be queued per user (in addition to running)	作業限制	輸入每個使用者排入佇列的資源密集型作業數目上限，或選取**無限制**。
Number of resource intensive operations running per organization	作業限制	輸入每個組織的同時資源密集型作業數目上限，或選取**無限制**。
Number of resource intensive operations to be queued per organization	作業限制	輸入每個組織排入佇列的資源密集型作業數目上限，或選取**無限制**。
Provide default vApp names	其他	選取此核取方塊以設定 VMware Cloud Director 提供新 vApp 的預設名稱。
Make Allocation pool Org VDCs elastic	其他	選取核取方塊以啟用彈性配置集區，使所有配置集區組織虛擬資料中心具有彈性。在取消選取此選項之前，請確保每個組織虛擬資料中心的所有虛擬機器均已移轉到單一叢集。
VM discovery enabled	其他	依預設，每個組織 VDC 會自動搜尋在支援 VDC 之任何資源集區中建立的 vCenter 虛擬機器。清除核取方塊可針對系統中的所有 VDC 停用此設定。

在伺服器群組中的儲存格上啟用 FIPS 模式

可以將 Linux 上的 VMware Cloud Director 10.2.2 及更新版本設定為使用 FIPS 140-2 驗證的密碼編譯模組，並且在 FIPS 相容模式下執行。

聯邦資訊處理標準 (FIPS) 140-2 是美國和加拿大政府標準，用於指定密碼編譯模組的安全性需求。NIST 密碼編譯模組驗證計劃 (CMVP) 會驗證符合 FIPS 140-2 標準的密碼編譯模組。

VMware Cloud Director FIPS 支援的目的是簡化各種規範環境下的合規性和安全性活動。若要瞭解有關 VMware 產品中的 FIPS 140-2 支援的詳細資訊，請參閱 https://www.vmware.com/security/certifications/fips.html。

在 VMware Cloud Director 中，FIPS 驗證的加密預設為停用狀態。啟用 FIPS 模式後，可以將 VMware Cloud Director 設定為使用 FIPS 140-2 驗證的密碼編譯模組，並且在 FIPS 相容模式下執行。

備註 啟用 FIPS 模式也會啟用主機名稱的反向查閱。

重要 啟用 FIPS 模式時，與 vRealize Orchestrator 的整合無法運作。

在 VMware Cloud Director 10.2.2 中，當您啟用 FIPS 模式時，無法加密 SAML 判斷提示。未處於 FIPS 模式時，判斷提示加密並沒有限制。

VMware Cloud Director 使用以下 FIPS 140-2 驗證的密碼編譯模組：

- VMware BC-FJA (Bouncy Castle FIPS Java API) 版本 1.0.2.1：憑證 #3673
- VMware OpenSSL FIPS 物件模組版本 2.0.20-vmw：憑證 #3857

VMware Cloud Director 與儲存格管理工具 (CMT) 綁定在一起。但是，儲存格管理工具不符合 FIPS 標準。

如需在 VMware Cloud Director 應用裝置上啟用 FIPS 模式的相關資訊，請參閱〈在 VMware Cloud Director 應用裝置上啟用或停用 FIPS 模式〉。

必要條件

- 確認是否已使用 OpenSSL 對憑證進行 `KeyCertSign` 位元判斷提示。FIPS 模式只能在 VMware Cloud Director SSL 憑證已進行 `KeyCertSign` 判斷提示的情況下運作。

  ```
  openssl crl2pkcs7 -nocrl -certfile certificates.pem | openssl pkcs7 -print_certs -text
  -noout
  ```

  如果憑證不包括延伸，請在建立 SSL 憑證金鑰儲存區時指定 `KeyCertSign` 位元。
- 安裝並啟用 `rng-tools` 公用程式集。請參閱 https://wiki.archlinux.org/index.php/Rng-tools。
- 如果已啟用度量收集，請確認 Cassandra 憑證是否遵循 X.509 v3 憑證標準且包括所有必要延伸。必須透過 VMware Cloud Director 使用的相同加密套件來設定 Cassandra。如需允許的 SSL 加密的相關資訊，請參閱〈管理允許的 SSL 加密清單〉。
- 從 vCenter Lookup Service 解除登錄 VMware Cloud Director。請參閱設定 vSphere 服務。

程序

1. 從頂部導覽列中，選取**管理**。
2. 在左面板中的**設定**下，選取 **SSL**。
3. 按一下**啟用**。
4. 確認您的環境符合啟用 FIPS 模式的所有必要條件。

   如果在啟動 FIPS 模式組態前，您的環境未符合所有必要條件，則 VMware Cloud Director 可能會無法存取。

5 若要確認您要啟動程序，請按一下**啟用**。

設定完成後，VMware Cloud Director 會顯示重新啟動雲端儲存格的訊息。

6 當 VMware Cloud Director 顯示重新啟動雲端儲存格的訊息後，將在 VMware Cloud Director 伺服器群組中重新啟動每個儲存格。

後續步驟

- 按一下**停用**以停用 FIPS 模式，當 VMware Cloud Director 指示設定準備就緒後，請重新啟動儲存格。
- 可以使用 `fips-mode` CMT 命令檢視作用中 VMware Cloud Director 儲存格的 FIPS 狀態。請參閱《VMware Cloud Director 安裝、設定與升級指南》中的〈檢視所有作用中儲存格的 FIPS 狀態〉。

設定系統電子郵件設定

您可以編輯系統電子郵件設定，包括設定 SMTP 伺服器設定和 VMware Cloud Director 通知設定。

VMware Cloud Director 需要 SMTP 伺服器，才能將使用者通知和系統警示電子郵件傳送給系統使用者。

VMware Cloud Director 會在需要報告重要資訊時傳送系統警示電子郵件。例如，若資料存放區空間不足，VMware Cloud Director 就會傳送警示。您可以設定 VMware Cloud Director 將電子郵件警示傳送給所有系統管理員，或是傳送至指定的電子郵件地址清單。

程序

1 從頂部導覽列中，選取**管理**。

2 在左窗格的**設定**下，選取**電子郵件**，然後按一下**編輯**。

3 輸入 SMTP 郵件伺服器的 DNS 主機名稱或 IP 位址。

4 輸入 SMTP 伺服器連接埠號碼。

5 (選擇性) 如果該 SMTP 伺服器需要使用者名稱，請開啟**需要驗證**選項並輸入該 SMTP 帳戶的使用者名稱和密碼。

6 選取**通知設定**索引標籤。

7 輸入顯示為 VMware Cloud Director 電子郵件寄件者的電子郵件地址。

VMware Cloud Director 會使用寄件者的電子郵件地址傳送執行階段與儲存區租用到期警示。

8 (選擇性) 為主題前置詞輸入文字。

9 選取通知的收件者。

依預設，只有組織管理員會收到 SMTP 通知。

10 按一下**儲存**。

11 (選擇性) 測試 SMTP 設定。

a 按一下**測試**。

b 如果您已啟用**需要驗證**選項，請輸入 SMTP 伺服器密碼。

c 輸入目的地電子郵件地址，然後按一下**測試**。

變更 VMware Cloud Director 授權

VMware Cloud Director 需要有效授權 (指定為序號) 才能執行。您可以修改在初始 VMware Cloud Director 設定期間輸入的授權資訊。

VMware Cloud Director 產品序號與 vCenter Server 授權金鑰不相同。您可以從 VMware 授權入口網站取得 VMware Cloud Director 序號。

程序

1 從頂部導覽列中，選取**管理**。

2 在左窗格中，選取**授權**，然後按一下**編輯**。

3 輸入新序號，然後按一下**儲存**。

設定目錄同步設定

您可以編輯所有組織和目錄的目錄同步設定，包括目錄訂閱的重新整理頻率。

程序

1 從頂部導覽列中，選取**管理**。

2 在左窗格的**設定**下，選取**目錄**。

3 按一下**編輯**。

4 啟用目錄同步。

5 設定同步的開始和停止時間。

6 設定同步間隔。

同步間隔是目錄訂閱的重新整理頻率。

7 按一下**儲存**。

後續步驟

如需設定目錄同步限制的相關資訊，請參閱《VMware Cloud Director 安裝、設定與升級指南》。

建立建議儀表板

您可以建立在 VMware Cloud Director Service Provider Admin Portal 和 Tenant Portal 中的使用者介面頁面上方顯示的通知。系統管理員、組織內的使用者或所有組織中的使用者可以看到這些訊息。

在建立建議之後，無法對其進行編輯。

程序

1 從頂部導覽列中，選取**管理**。

2 在左面板中的**設定**下，選取**建議**，然後按一下**新增**。

3 在說明方塊中，新增通知的文字。

您可以使用基本 Markdown 將連結新增至通知。

4 選取訊息的優先順序。

不同的優先順序訊息顯示為不同的色彩。通知會按照其優先順序顯示。無法關閉或延遲必要的建議。

5 選取您希望在使用者介面中顯示通知的時段。

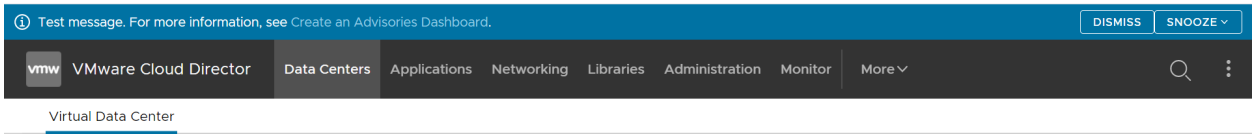
您可以在**建議**索引標籤中檢視所有建議，但僅在所選期間內向選取的使用者群組顯示這些建議。

6 選取希望只有系統管理員看到通知，還是組織內或跨組織的所有使用者都看到通知。

7 按一下**確定**。

結果

通知隨即顯示在所選入口網站的頂部導覽列上方。



後續步驟

透過選取通知旁邊的選項按鈕，然後按一下**刪除**，刪除通知。即使在到期之後，這些建議仍會顯示在**建議**索引標籤中。若要將其從清單中移除，則必須將其刪除。

設定和監控封鎖工作及通知

您可以使用封鎖工作和通知，將 VMware Cloud Director 設定為傳送特定事件所觸發的 AMQP 訊息。

有些訊息只是用於告知有事件發生，其他訊息會發佈資訊至指定的 AMQP 端點，指出請求的動作已遭封鎖，並且正在等待由繫結至該端點的用戶端應用程式進行處理。這些訊息稱為封鎖工作。

系統管理員可以設定一組系統範圍的封鎖工作，具體取決於 AMQP 用戶端所執行的程式化動作。

設定 AMQP Broker

如果您想要 VMware Cloud Director 傳送特定事件所觸發的 AMQP 訊息，則必須設定 AMQP Broker。您可以使用 AMQP 訊息自動處理基礎使用者請求。

程序

1 從頂部導覽列中，選取**管理**。

2 在**設定**下，選取**擴充性**。

AMQP Broker 索引標籤隨即開啟。

3 按一下 **AMQP Broker** 區段的**編輯**按鈕。

4 輸入 AMQP 主機的 DNS 主機名稱或 IP 位址。

RabbitMQ 伺服器主機的完整網域名稱，例如 *amqp.example.com*。

5 輸入 AMQP 連接埠。

代理接聽訊息的預設連接埠為 `5672`。

6 輸入交換。

7 輸入 vHost。

預設值為 `/`。

8 輸入首碼。

9 (選擇性) 若要使用 SSL，請開啟**使用 SSL** 切換按鈕，然後選取其中一個憑證選項。

依預設，VMware Cloud Director AMQP 服務會傳送未加密的訊息。您可以設定 AMQP 服務，以使用 SSL 加密這些訊息。此外，還可以設定服務，以使用 VMware Cloud Director 儲存格上 Java Runtime Environment 的預設 JCEKS 信任存放區 (通常位於 `$VCLOUD_HOME/jre/lib/security/cacerts`) 來驗證代理憑證。

選項	描述
接受所有憑證	憑證擁有者欄位的 CN 記錄必須符合 AMQP Broker 的主機名稱。若要使用與代理主機名稱不相符的憑證，請開啟**接受所有憑證**切換按鈕。
SSL 憑證	上傳 SSL 憑證。
SSL 金鑰儲存區 (JCEKS)	上傳 SSL 金鑰儲存區並輸入金鑰儲存區密碼。

10 輸入使用者名稱和密碼以連線至 AMQP 主機。

11 按一下**儲存**。

12 (選擇性) 若要測試設定，請按一下 **AMQP Broker** 區段下的**測試**按鈕，並提供密碼。

13 (選擇性) 若要將稽核事件發佈到 AMQP Broker，請按一下**非封鎖 AMQP 通知**區段下的**編輯**按鈕，然後開啟**啟用通知**切換按鈕。

設定封鎖工作設定

您可以將特定作業設定為封鎖工作。這些作業會暫停，直到**系統管理員**對其執行動作或預先設定的計時器到期為止。您可以指定封鎖工作的逾時設定和預設動作。這些設定會套用至安裝中的所有組織。

程序

1 從頂部導覽列中，選取**管理**。

2 在**設定**下，選取**擴充性**。

3 選取**封鎖工作**索引標籤。

4 若要編輯預設延伸逾時和預設逾時動作，請按一下**一般**區段下的**編輯**按鈕。

   a 編輯**預設封鎖工作逾時**。

   b 編輯**預設逾時動作**。

      預設逾時動作是在**預設封鎖工作逾時**到期後執行的動作。

   c 按一下**儲存**。

5 若要編輯作業清單 (視為封鎖工作)，請按一下**作業**區段下的**編輯**按鈕。

   a 從封鎖工作清單中選取或取消選取作業。

   b 按一下**儲存**。

監控封鎖的工作

在預先設定的計時器到期之前，您可以監控目前封鎖的工作，也可以手動取消工作、繼續執行工作或使工作失敗。

必要條件

設定封鎖工作設定

程序

1 從頂部導覽列的**監控**下，選取**封鎖工作**。

   此索引標籤會顯示目前已封鎖工作的清單。

2 選取您要手動編輯的工作。

3 決定取消工作、繼續執行工作還是使工作失敗，然後按一下對應的按鈕。

4 輸入訊息，然後按一下**儲存**。

   此訊息會顯示在工作詳細資料中。

設定公用位址

若要滿足負載平衡器或 Proxy 需求，您可以變更 VMware Cloud Director Web 入口網站、VMware Cloud Director API 和主控台 Proxy 的預設端點網址。

公用位址是向 VMware Cloud Director 用戶端公開的網址。安裝期間會指定這些位址的預設值。如有必要，您可以更新位址。

如果 VMware Cloud Director 由單一儲存格組成，則安裝程式會建立公用端點，這些端點通常為 API 和 Web 用戶端提供足夠的存取權。包含多個儲存格的安裝和部署通常會在儲存格和用戶端之間放置負載平衡器。用戶端會在負載平衡器的位址存取系統。負載平衡器會在可用儲存格之間散佈用戶端要求。其他包含 Proxy 或將儲存格放置到 DMZ 的網路組態也需要自訂端點。端點 URL 詳細資料專屬於您的網路組態。

VMware Cloud Director Tenant Portal 和 VMware Cloud Director Web 主控台的端點需要 SSL 憑證 (最好是已簽署)。安裝或部署 VMware Cloud Director 時，必須指定這些憑證的路徑。如果在安裝或部署後自訂其中任一端點，您可能需要安裝符合端點詳細資料 (例如 `hostname` 和 `subject alternative name`) 的新憑證。

對於 VMware Cloud Director 應用裝置，您必須設定 VMware Cloud Director 公用主控台 Proxy 位址，因為該應用裝置將具有自訂連接埠 `8443` 的單一 IP 位址用於主控台 Proxy 服務。請參閱 步驟 6。

必要條件

確認您是以**系統管理員**的身分登入。僅**系統管理員**可以自訂公用端點。

程序

1 從頂部導覽列中，選取**管理**。

2 在左面板中的**設定**下，按一下**公用位址**。

3 若要自訂公用端點，請按一下**編輯**。

4 若要自訂 VMware Cloud Director URL，請編輯 **Web 入口網站**端點。

   a 針對 HTTP (不安全) 連線輸入自訂 VMware Cloud Director 公用 URL。

   b 針對 HTTPS (安全) 連線輸入自訂 VMware Cloud Director 公用 URL，然後按一下**上傳**來上傳為該端點建立信任鏈結的憑證。

   憑證鏈結必須符合服務端點使用的憑證，該憑證是上傳到別名為 `consoleproxy` 之每個 VMware Cloud Director 儲存格金鑰儲存區的憑證。不支援對負載平衡器中的主控台 Proxy 連線進行 SSL 終止。憑證鏈結必須包含採用 `PEM` 格式且不含私密金鑰的端點憑證、中繼憑證和根憑證。

5 (選擇性) 若要自訂 Cloud Director REST API 和 OpenAPI URL，請關閉**使用 Web 入口網站設定**切換按鈕。

   a 輸入自訂 HTTP 基底 URL。

   例如，如果您將 HTTP 基底 URL 設定為 **`http://vcloud.example.com`**，您可以存取位於 `http://vcloud.example.com/api` 的 VMware Cloud Director API，並且可以存取位於 `http://vcloud.example.com/cloudapi` 的 VMware Cloud Director OpenAPI。

   b 輸入自訂 HTTPS REST API 基底 URL，然後按一下**上傳**來上傳為該端點建立信任鏈結的憑證。

   例如，如果您將 HTTPS REST API 基底 URL 設定為 **`https://vcloud.example.com`**，您可以存取位於 `https://vcloud.example.com/api` 的 VMware Cloud Director API，並且可以存取位於 `https://vcloud.example.com/cloudapi` 的 VMware Cloud Director OpenAPI。

   憑證鏈結必須符合服務端點使用的憑證，該憑證是上傳到別名為 `http` 之每個 VMware Cloud Director 儲存格金鑰儲存區的憑證或負載平衡器 VIP 憑證 (如果使用 SSL 終止)。憑證鏈結必須包含採用 `PEM` 格式且不含私密金鑰的端點憑證、中繼憑證和根憑證。

6 輸入自訂 VMware Cloud Director 公用主控台 Proxy 位址。

   - 自訂 VMware Cloud Director 應用裝置的公用主控台 Proxy 位址。

此位址是 VMware Cloud Director 應用裝置 `eth0` NIC 的完整網域名稱 (FQDN)，透過 FQDN 或 IP 位址指定，並且將自訂連接埠 `8443` 用於主控台 Proxy 服務。

- 在 Linux 公用主控台 Proxy 位址上自訂 VMware Cloud Director。

  此位址是具有連接埠號碼的 VMware Cloud Director 伺服器或負載平衡器的完整網域名稱 (FQDN)。預設連接埠為 `443`。

例如，對於具有 FQDN `vcloud.example.com` 的 VMware Cloud Director 應用裝置執行個體，輸入 **`vcloud.example.com:8443`**。

在虛擬機器上開啟遠端主控台視窗時，VMware Cloud Director 會使用主控台 Proxy 位址。

7 按一下**儲存**。

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 VMware Cloud 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。

從 10.1 版開始，VMware Cloud Director 將移至可識別承租人的集中式儲存區域，以進行憑證管理。如此一來，VMware Cloud Director 會將所有憑證集中在同一個位置，以便**系統管理員**和**組織管理員**可以檢視、稽核和管理系統中各種元件所使用的所有憑證。您可以使用 VMware Cloud Director API 在可識別承租人的新儲存區域中新增、更新或移除憑證。請參閱《VMware Cloud Director API 架構參考》。

新增或編輯新的 LDAP 伺服器端點時，VMware Cloud Director 使用者介面會探查此端點是否存在它要提供的任何憑證。VMware Cloud Director 會將任何您決定信任的憑證新增至集中式憑證儲存區域。

設定系統 LDAP 連線

若要為 VMware Cloud 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 從頂部導覽列中，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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，選取**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 VMware Cloud Director 租用戶入口網站。

4 從頂部導覽列中，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 VMware Cloud 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 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，您可以隨時將使用者和群組資訊與 LDAP 伺服器同步。

必要條件

如果您計劃連線至 LDAP over SSL (LDAPS) 伺服器，請確認 LDAP 伺服器的憑證與 Java 8 Update 181 中引入的端點識別相符。憑證的一般名稱 (CN) 或主體別名 (SAN) 必須與 LDAP 伺服器的 FQDN 相符。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 VMware Cloud Director 要連線的位置。 若要在根層級連線，請僅輸入網域元件，例如 **DC=example,DC=com**。 若要連線至網域樹狀結構中的節點，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 VMware Cloud 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**按鈕並匯入 LDAP SSL 憑證，或選取**接受所有憑證**。
驗證方法	簡單驗證包括將使用者的 DN 和密碼傳送至 LDAP 伺服器。如果您使用 LDAP，會透過網路傳送純文字形式的 LDAP 密碼。 如果您想要使用 Kerberos，則必須使用 vCloud API 設定 LDAP 連線。
使用者名稱	輸入具有網域管理員權限之服務帳戶的完整 LDAP 辨別名稱 (DN)。VMware Cloud Director 使用此帳戶來查詢 LDAP 目錄並擷取使用者資訊。 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	連線至 LDAP 伺服器之服務帳戶的密碼。 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 如果您已選取**使用 SSL** 核取方塊，並且 LDAPS 伺服器的憑證尚且不受信任，請在**信任憑證**視窗上確認您是否信任伺服器端點所提供的憑證。

6 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**。

7 若要將 VMware Cloud Director 與設定的 LDAP 伺服器同步，請按一下**同步**。

VMware Cloud 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 VMware Cloud 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。

提示 如果需要以本機使用者身分登入，則可以使用您設定的基底 URL，例如 `https://vcloud.example.com/tenant/`*`tenant_name`*`/login`。

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. 從頂部導覽列中，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 VMware Cloud 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**。

管理憑證

可以從 VMware Cloud Director 匯入、下載、編輯和刪除憑證。可以將憑證 PEM 資料複製到剪貼簿。

匯入受信任的憑證

您可以匯入 VMware Cloud Director 與之通訊的伺服器的憑證，例如 vCenter Server、NSX Manager 等。

在 FIPS 模式下使用 VMware Cloud Director 時，您必須使用 FIPS 相容的私密金鑰。可以使用 pyOpenSSL 以 FIPS 相容的 PKCS#8 格式產生私密金鑰。如果您使用 OpenSSL 產生 PKCS#8 私密金鑰，則私密金鑰不與 FIPS 相容。如需有關 FIPS 模式的詳細資訊，請參閱〈在伺服器群組中的儲存格上啟用 FIPS 模式〉或〈在 VMware Cloud Director 應用裝置上啟用或停用 FIPS 模式〉。

程序

1 從頂部導覽列中，選取**管理**。

2 在左面板中的**憑證管理**下，選取**受信任的憑證**，然後按一下**匯入**。

3 上傳包含您要匯入之憑證的 PEM 檔案，然後按一下**匯入**。

4 (選擇性) 編輯憑證名稱。

5 按一下**匯入**。

後續步驟

- 下載憑證。
- 編輯憑證名稱。
- 刪除憑證。
- 將 PEM 資料複製到剪貼簿。

將憑證匯入至憑證程式庫

在 VMware Cloud Director 憑證程式庫中，您可以匯入在建立必須保護的實體 (例如伺服器、Edge 閘道等) 時所使用的憑證。

此憑證程式庫包含單一憑證、憑證鏈結、私密金鑰、憑證到期日期、憑證保護的實體等相關資訊。

您必須分別管理每個站台的憑證程式庫。

在 FIPS 模式下使用 VMware Cloud Director 時，您必須使用 FIPS 相容的自我簽署憑證和私密金鑰。可以使用 pyOpenSSL 產生自我簽署的未加密憑證和私密金鑰。如果您使用 OpenSSL 產生自我簽署憑證和私密金鑰，則憑證和私密金鑰不與 FIPS 相容。如需有關 FIPS 模式的詳細資訊，請參閱〈在伺服器群組中的儲存格上啟用 FIPS 模式〉或〈在 VMware Cloud Director 應用裝置上啟用或停用 FIPS 模式〉。

程序

1 從頂部導覽列中，選取**管理**。

2 在左面板中的**憑證管理**下，選取**憑證程式庫**，然後按一下**匯入**。

3 為憑證程式庫中的此憑證輸入名稱，並選擇性地輸入說明，然後按**下一步**。

4 上傳包含您要匯入之憑證鏈結的 PEM 檔案，然後按**下一步**。

5 (選擇性) 上傳私密金鑰檔案。

   您的私密金鑰檔案可能不會使用複雜密碼進行保護。

6 按一下**匯入**。

結果

在建立必須保護的實體時，已匯入的憑證會出現在可用憑證清單中。

後續步驟

- 下載憑證。
- 編輯憑證的名稱和說明。
- 刪除憑證。只能刪除不保護任何實體的憑證。
- 將憑證 PEM 資料複製到剪貼簿。

管理外掛程式

VMware Cloud Director 外掛程式可延伸 Service Provider Admin Portal 和 VMware Cloud 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 VMware Cloud Director 的一部分進行安裝。

CPOM 延伸

提供使用 VMware Cloud Director Tenant Portal 檢視和管理專用 vCenter Server 執行個體與 Proxy 的功能。

自訂入口網站

提供自訂 VMware Cloud Director Service Provider Admin Portal 和 VMware Cloud Director Tenant Portal 的功能。

vCloud Availability

VMware vCloud® Availability™ 外掛程式提供可直接從 VMware Cloud 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 VMware Cloud 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. 從頂部導覽列中選取**更多 > 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 VMware Cloud Director Service Provider Admin Portal 中可用。
承租人	外掛程式功能在您所選組織的 VMware Cloud 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 從頂部導覽列中選取**更多 > 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 VMware Cloud Director Service Provider Admin Portal 移除一或多個外掛程式。

程序

1 從頂部導覽列中選取**更多 > 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 從頂部導覽列中選取**更多 > 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 VMware Cloud Director Service Provider Admin Portal 中可用。
承租人	外掛程式功能在您所選組織的 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director Service Provider Admin Portal 和每個組織的 VMware Cloud Director Tenant Portal 設定標誌和主題。此外，還可以修改和新增 VMware Cloud 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 VMware Cloud Director OpenAPI 入門，網址為：https://code.vmware.com。

入口網站商標

在安裝過程中，VMware Cloud 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 VMware Cloud Director Service Provider Admin Portal。每個組織的 VMware Cloud 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《VMware Cloud Director 安裝、設定與升級指南》。

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。

VMware Cloud Director 支援自訂連結的 `url` 值中的下列自訂變數：

表 11-2. 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 VMware Cloud Director Tenant Portal，將轉換為：

```
url: https://host:port/tenant/myorg/vdcs
```

設定密碼原則

若要防止使用者在一定次數的失敗嘗試後登入 VMware Cloud Director，您可以啟用帳戶鎖定。

對系統帳戶鎖定原則所做的變更會套用至所有新的組織。在帳戶鎖定原則變更之前所建立的組織必須在組織層級進行變更。

程序

1. 從頂部導覽列中，選取**管理**。
2. 在左面板中的**設定**下，按一下**密碼原則**。
3. 按一下**編輯**。
4. 若要啟用帳戶鎖定，請開啟**帳戶鎖定**切換按鈕。
5. 選取鎖定帳戶前接受的無效登入次數。

6 選取鎖定間隔。

7 若要啟用**系統管理員**帳戶鎖定，請開啟**可以鎖定系統管理員帳戶**切換按鈕。

8 按一下**儲存**。

設定 vSphere 服務

您可以設定並允許 VMware Cloud Director 使用 vCenter Single Sign-On，以便 vSphere 身分識別提供者對系統管理員進行驗證。

vCenter Lookup Service 包含有關 vSphere 基礎結構的拓撲資訊，使 vSphere 元件可以相互實現安全連線。

程序

1 從頂部導覽列中，選取**管理**。

2 在左窗格的**設定**下，選取 **vSphere 服務**。

3 設定 vSphere 服務。

- 若要向 vCenter Lookup Service 登錄 VMware Cloud Director，請按一下**登錄**。
- 若要從 vCenter Lookup Service 解除登錄 VMware Cloud Director，請按一下**解除登錄**。

4 輸入 vCenter Lookup Service URL，例如 `https://hostname:443/lookupservice/sdk`。

5 輸入擁有管理權限之 vCenter Single Sign-On 使用者的使用者名稱和密碼，例如，`administrator@your_domain_name` 使用者。

結果

如果已向 vCenter Lookup Service 登錄 VMware Cloud Director，則**系統管理員**必須使用其 vCenter Single Sign-On 認證登入 VMware Cloud Director。

監控 VMware Cloud Director 12

系統管理員可以監控已完成與進行中的作業，並檢視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率資訊。

從 9.1 版開始，VMware Cloud Director 不支援 VMware vCenter Chargeback Manager。請參閱《VMware 產品互通性對照表》。

本章節討論下列主題：

- VMware Cloud Director 和成本報告
- 檢視提供者虛擬資料中心的使用資訊

VMware Cloud Director 和成本報告

您可以使用 VMware vRealize Operations Tenant App for VMware Cloud Director 來設定 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director 作為服務提供者和使用 vRealize Operations Tenant App for VMware Cloud Director 作為承租人。

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 從頂部導覽列中，選取**資源**，然後按一下**雲端資源**。

2 在左面板中，選取**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

VMware Cloud 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 VMware Cloud Director 整合

您可以透過 VMware Cloud Director Service Provider Admin Portal，將 vRealize Orchestrator 與 VMware Cloud 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 VMware Cloud Director 整合以延伸 VMware Cloud Director 的基本功能。

透過 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director 登錄 vRealize Orchestrator 執行個體

若要透過 VMware Cloud Director 中的 vRealize Orchestrator 利用工作流程協調和工作自動化，您可以在 VMware Cloud 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 VMware Cloud 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 從頂部導覽列中，選取**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**新增**。

   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 443。 **備註** VMware Cloud 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 VMware Cloud 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 從頂部導覽列中，選取**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 若要建立新服務類別，請按一下**新增**。

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 從頂部導覽列中，選取**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 VMware Cloud 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 VMware Cloud 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 從頂部導覽列中，選取**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 12 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 從頂部導覽列中，選取**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 12 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 從頂部導覽列中，選取**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 12 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 VMware Cloud Director 服務時，VMware Cloud 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 VMware Cloud Director 成功驗證後收到的驗證 Token
_vcd_apiEndpoint	VMware Cloud 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 從頂部導覽列中，選取**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 12 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 從頂部導覽列中，選取**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 12 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 從頂部導覽列中，選取**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 12 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**。

管理定義的實體

14

從 VMware Cloud Director 10.2 開始，服務提供者可以使用 VMware Cloud Director API 建立延伸，以向承租人提供其他 VMware Cloud Director 功能。

服務提供者可以建立執行階段定義的實體 (RDE)，從而允許延伸在 VMware Cloud Director 中儲存及操縱延伸特定資訊。例如，Kubernetes 延伸可以在 RDE 中儲存所管理的 Kubernetes 叢集的相關資訊。然後，此延伸可提供延伸 API，從而使用 RDE 中的資訊管理這些叢集。

存取定義的實體

兩個互補機制控制 RDE 的存取權。

- 權限 - 建立 RDE 類型時，您可以為此類型建立權限服務包。若要提供對特定作業的存取權，您必須將此服務包中的權限指派給其他角色。每個服務包都有五個特定於類型的權限：**檢視：TYPE**、**編輯：TYPE**、**完全控制：TYPE**、**管理員檢視：TYPE** 和**管理員完全控制：TYPE**。

  檢視：TYPE、**編輯：TYPE** 和**完全控制：TYPE** 權限僅與 ACL 項目組合使用。

- 存取控制清單 (ACL) - ACL 資料表包含的項目定義了使用者對系統中特定實體具有的存取權。對實體提供了額外層級的控制。例如，如果**編輯：TYPE** 權限指定使用者可以修改其有權存取的實體，ACL 資料表會定義使用者可存取的實體。

  具有**檢視一般 ACL** 權限的**系統管理員**可以使用 `accessControls` API 檢視指派給特定已定義實體的 ACL。如需 VMware Cloud Director API 參考，請參閱 code.vmware.com。

  具有**管理一般 ACL** 權限的**系統管理員**可以使用 `accessControls` API 建立、修改和移除特定的 ACL。

表 14-1. RDE 作業的權限和 ACL 項目

實體作業	選項	描述
讀取	**管理員檢視：TYPE** 權限	具有此權限的使用者可以查看組織內此類型的所有 RDE。
	檢視：TYPE 權限和 ACL 項目 >= **檢視**	具有此權限和讀取層級 ACL 的使用者可以檢視此類型的 RDE。
修改	**管理員完全控制：TYPE** 權限	具有此權限的使用者可以在所有組織中建立、檢視、修改和刪除此類型的 RDE。

表 14-1. RDE 作業的權限和 ACL 項目 (續)

實體作業	選項	描述
	編輯：TYPE 權限和 ACL 項目 **>= 變更**	具有此權限和修改層級 ACL 的使用者可以建立、檢視和修改此類型的 RDE。
刪除	**管理員完全控制：TYPE** 權限	具有此權限的使用者可以在所有組織中建立、檢視、修改和刪除此類型的 RDE。
	完全控制：TYPE 權限和 ACL 項目 **= 完全控制**	具有此權限和完全控制層級 ACL 的使用者可以建立、檢視、修改和刪除此類型的 RDE。

您可以使用 VMware Cloud Director API 或使用者介面，將權限服務包發佈到要管理此類型實體的任何組織。發佈權限服務包後，您可以將服務包中的權限指派給組織內的角色。

您可以使用 VMware Cloud Director API 編輯 ACL 資料表。

本章節討論下列主題：

- 共用定義的實體
- 管理自訂實體

共用定義的實體

可以透過與其他系統管理員或承租人共用執行階段定義的實體 (RDE) 來授與對這些實體的存取權。

與其他使用者共用定義的實體

1 如果要向承租人授與已定義實體的存取權，請將已定義實體類型的權限服務包發佈到承租人組織。例如，若要建立和管理 Tanzu Kubernetes 叢集，您必須發佈 **vmware:tkgcluster 權利**權限服務包。請參閱發佈或解除發佈權限服務包。

如果要與**系統管理員**共用已定義的實體，請略過此步驟。

2 將服務包中的**檢視：TYPE**、**編輯：TYPE** 或**完全控制：TYPE** 權限指派給要對已定義實體擁有特定層級存取權的使用者角色。

例如，如果您希望具有 **tkg_viewer** 角色的使用者能夠檢視組織內的 Tanzu Kubernetes 叢集，則必須將**檢視：Tanzu Kubernetes 客體叢集**權限新增至該角色。如果您希望具有 **tkg_author** 角色的使用者能夠建立、檢視和修改此組織內的 Tanzu Kubernetes 叢集，請將**編輯：Tanzu Kubernetes 客體叢集**新增至該角色。如果您希望具有 **tkg_admin** 角色的使用者能夠建立、檢視、修改和刪除此組織內的 Tanzu Kubernetes 叢集，請將**完全控制：Tanzu Kubernetes 客體叢集**權限新增至該角色。

3 透過執行下列 REST API 呼叫，為特定使用者授與存取控制清單 (ACL)。

```
POST https://[address]/cloudapi/1.0.0/entities/urn:vcloud:entity:[vendor]:[type name]:
[version]:[UUID]/accessControls
 {
```

```
  "grantType" : "MembershipAccessControlGrant",
  "accessLevelId" : "urn:vcloud:accessLevel:[Access_level]",
  "memberId" : "urn:vcloud:user:[User_ID]"
}
```

Access_level 必須為 `ReadOnly`、`ReadWrite` 或 `FullControl`。*User_ID* 必須為要授與已定義實體之存取權的使用者識別碼。

具有 **tkg_viewer** 角色的使用者 (範例中所述) 無法授與 ACL 存取權。具有 **tkg_author** 或 **tkg_admin** 角色的使用者可以與具有 **tkg_viewer**、**tkg_author** 或 **tkg_admin** 角色的使用者共用對 VMWARE:TKGCLUSTER 實體的存取權，方法是使用 API 請求為這些使用者授與 ACL 存取權。

您也可以使用 REST API 呼叫撤銷存取權或檢視擁有實體存取權的使用者。請參閱 VMware Cloud Director REST API 說明文件，網址為 code.vmware.com。

共用對已定義實體的管理員權限

1 如果要向承租人授與已定義實體的存取權，請將已定義實體類型的權限服務包發佈到承租人組織。例如，若要建立和管理 Tanzu Kubernetes 叢集，您必須發佈 **vmware:tkgcluster 權利**權限服務包。請參閱發佈或解除發佈權限服務包。

如果要與**系統管理員**共用已定義的實體，請略過此步驟。

2 將服務包中的**管理員檢視：TYPE** 或**管理員完全控制：TYPE** 權限指派給要對已定義實體擁有特定層級存取權的使用者角色。

例如，如果您希望具有此角色的使用者能夠檢視組織內的所有 Tanzu Kubernetes 叢集，則必須將**管理員檢視：Tanzu Kubernetes 客體叢集**權限新增至該角色。如果您希望具有此角色的使用者能夠建立、檢視、修改和刪除所有組織內的 Tanzu Kubernetes 叢集，請將**管理員完全控制：Tanzu Kubernetes 客體叢集**權限新增至使用者角色。

具有**管理員完全控制：Tanzu Kubernetes 客體叢集**權限的使用者可以向任何 VMWARE:TKGCLUSTER 實體授與 ACL 存取權。

變更已定義實體的擁有者

已定義實體的擁有者或具有**管理員完全控制：TYPE** 權限的使用者，可透過更新已定義的實體模型並以新擁有者的識別碼變更擁有者欄位，將擁有權轉移給其他使用者。

管理自訂實體

VMware Cloud 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 VMware Cloud 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。

搜尋自訂實體

您可以依名稱搜尋自訂實體。

程序

1 從頂部導覽列中，選取**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 12 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 從頂部導覽列中，選取**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 12 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 從頂部導覽列中，選取**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 12 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 若要新增自訂實體，請按一下**新增**。

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 VMware Cloud 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 從頂部導覽列中，選取**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 12 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 從頂部導覽列中，選取**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 12 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**將自訂實體關聯至 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 從頂部導覽列中，選取**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 12 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 從頂部導覽列中，選取**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 12 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 從頂部導覽列中，選取**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 12 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。