VMware Cloud Director 租用戶入口網站指南

修改日期：2021 年 4 月 4 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™ 租用戶入口網站指南

《VMware Cloud Director™ 租用戶入口網站指南》提供有關如何使用 VMware Cloud Director 租用戶入口網站的資訊。在此版本中，您可以使用租用戶入口網站管理您的組織，以及建立和設定虛擬機器、vApp 和 vApp 中的網路。您也可以設定 VMware Cloud Director 環境中的 VMware NSX® for vSphere® 提供的進階網路功能。使用 VMware Cloud Director 租用戶入口網站，您也可以建立和管理目錄、vApp 和 VDC 範本，以及建立和管理跨虛擬資料中心網路。

主要對象

本指南適用於想要使用 VMware Cloud Director 租用戶入口網站功能的任何人。此資訊主要是針對使用租用戶入口網站來管理其組織，管理虛擬機器、vApp、網路等的**組織管理員**而撰寫的。

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 http://www.vmware.com/support/pubs。

使用條款和條件

VMware 允許您根據合理需要修改本承租人使用者指南 (簡稱「指南」)，對其進行自訂以反映您的操作流程，以及將修改後的指南重新產生並發佈給您的客戶。您不得針對客戶使用修改後的指南收取任何費用。您確認，本指南免費「原樣」提供給您，不提供任何形式的擔保，並且僅用於上述目的。因此，VMware 及其供應商因向您提供本指南的存取權而產生或與之相關的總負債不得超過 100 美元。在任何情況下，VMware 或其供應商對任何間接、偶然、特殊或後果性損害 (包括但不限於業務利潤損失、業務中斷或業務資訊丟失造成的損害) 均不承擔責任，無論是由何種原因引起的，也無論依據何種責任理論，即使 VMware 或其供應商已被告知可能會發生此類損害。即使未達到任何有限補救措施的基本目的，這些限制仍然應適用。

VMware Cloud Director 租用戶入口網站入門

1

當您登入租用戶入口網站時，有大量工作可完成，從建立虛擬機器和 vApp 到設定進階網路組態和執行 vRealize Orchestrator 工作流程。

本章節討論下列主題：

瞭解 VMware Cloud Director™

VMware Cloud Director™ 提供以 Web 為基礎之租用戶入口網站的角色型存取，讓組織成員與組織資源互動，以建立與使用 vApp 和虛擬機器。

在您可以存取組織之前，VMware Cloud Director **系統管理員**必須建立組織，並為其指派資源，然後提供 URL 以存取租用戶入口網站。每個組織都會包括一或多個**組織管理員**，而組織管理員透過新增成員以及設定原則和喜好設定來完成組織的設定。設定組織之後，非管理員使用者就可以登入，以建立、使用與管理虛擬機器和 vApp。

組織

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。

使用者與群組

組織可包含任意的使用者與群組數。組織管理員可以在本機建立使用者，或從目錄服務匯入使用者。群組必須從目錄服務匯入。組織內的權限是透過對使用者與群組指定的權限與角色來控制。

虛擬資料中心數目

組織虛擬資料中心提供資源給組織。虛擬資料中心提供的環境可儲存、部署以及操作虛擬系統。它們還為虛擬 CD 和 DVD 媒體提供儲存區。一個組織可以有多個虛擬資料中心。

組織虛擬資料中心網路

組織虛擬資料中心網路包含在 VMware Cloud Director 組織虛擬資料中心內，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。組織虛擬資料中心網路可以連線至外部網路，或組織的內部隔離網路。只有**系統管理員**才能建立組織虛擬資料中心網路，但是**組織管理員**可以管理組織虛擬資料中心網路 (包括它們提供的網路服務)。

vApp 網路

vApp 網路包含在 vApp 內，而且允許 vApp 內的虛擬機器互相通訊。如果組織虛擬資料中心網路連線至外部網路，則您可以將 vApp 網路連線至組織虛擬資料中心網路，以允許 vApp 與組織中和組織外部的其他 vApp 進行通訊。

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目錄的 vApp 範本與媒體檔案來建立其專屬 vApp。**組織管理員**可以將公用目錄中的項目複製至其組織目錄。

專用 vCenter Server 執行個體 (SDDC) 和 Proxy

軟體定義資料中心 (SDDC) 封裝整個 vCenter Server 環境。一個專用 vCenter Server 執行個體可包含一或多個 Proxy，這些 Proxy 會提供對基礎環境中不同元件的存取權。**系統管理員**可以向您的組織發佈一或多個專用 vCenter Server 執行個體。您可以使用包含的 Proxy 存取代理元件的使用者介面或 API。

登入 VMware Cloud Director 租用戶入口網站

您可以透過使用組織特定的 URL 來存取 VMware Cloud Director 租用戶入口網站。

如果您不知道租用戶入口網站的組織 URL，請連絡**組織管理員**。如需支援的瀏覽器和組態的相關資訊，請參閱《VMware Cloud Director 版本說明》。

程序

1 在網頁瀏覽器中，導覽至您組織的租用戶入口網站 URL。

例如，*https://cloud.example.com/tenant/myOrg*。

2 輸入使用者名稱和密碼，然後按一下**登入**。

VMware Cloud Director 租用戶入口網站的角色與權限

VMware Cloud Director 包含預先設定的一組使用者角色及其權限。可存取 VMware Cloud Director 租用戶入口網站的角色預設為任何組織中所建立的角色，或由組織管理員建立的其他角色。

已獲指派下列組織角色的使用者可以存取租用戶入口網站。所查看的項目以及可執行的動作取決於與特定角色相關聯的權限。

- **組織管理員**
- **目錄作者**
- **vApp 作者**
- **vApp 使用者**
- **僅限主控台存取**

如需預先定義的角色及其權限的相關資訊，請參閱預先定義的角色與其權限。

使用 VMware Cloud Director 租用戶入口網站

如果您有多個虛擬資料中心，當您登入 VMware Cloud Director 租用戶入口網站時，系統會將您導覽至**資料中心**儀表板畫面。如果您只有一個虛擬資料中心，則登入 VMware Cloud Director 租用戶入口網站時，系統會將您直接導覽至該資料中心。

資料中心儀表板畫面是 VMware Cloud Director 多站台功能的一部分，可讓承租人將其分散在不同地理位置的雲端環境視為單一實體。如需有關多站台的詳細資訊，請參閱使用多個站台。

儀表板可提供 VMware Cloud Director 虛擬資料中心以及站台 (不僅僅位於單一組織) 的統一視圖。在多儲存格和多組織環境中，您也可以查看所有其他相關聯的組織的虛擬資料中心。

備註 根據其權限，租用戶使用者可以查看組織的所有成員站台或僅查看站台的子集。

在摘要功能區的頂端會顯示組織的相關資訊。

如果您以**組織管理員**身分登入，您可以看到：

- 站台、組織及虛擬資料中心的數目
- 執行中的 vApp 和虛擬機器的總數
- 已使用的硬體資源，如 CPU、記憶體和儲存區

虛擬資料中心會顯示在卡視圖中。每張卡包含虛擬中心所屬組織、vApp 數目、虛擬機器總數以及處於執行中狀態之虛擬機器數目的相關資訊。此卡也會顯示資料中心的可用 CPU、記憶體和儲存區容量，並顯示有關目前資源配置和保留的即時度量。

從頂部導覽，您可以導覽至不同的功能表項目。

功能表項目	描述
資料中心	將您導覽至組織中的**虛擬資料中心**、**資料中心群組**和**專用 vSphere 資料中心**資源
虛擬資料中心	將您導覽至顯示組織內的虛擬資料中心的**虛擬資料中心**畫面。

功能表項目	描述
專用 vSphere 資料中心	將您導覽至顯示服務提供者已發佈至您組織的專用 vSphere 資料中心的畫面。
應用程式	將您導覽至組織中的**虛擬應用程式**和**虛擬機器**資源。
程式庫	將您導覽至 vApp 範本、目錄、媒體及其他檔案類型的整併視圖。可以使用這些範本和檔案部署虛擬機器或 vApp。
網路作業	將您導覽至組織中的網路、Edge 閘道和資料中心群組。
管理	將您導覽至**存取控制**、**身分識別提供者**組態畫面，以及您組織的一般、電子郵件、客體個人化、中繼資料、多站台和原則設定。
監視器	將您導覽至**工作**和**事件**畫面。**工作**畫面顯示由 VMware Cloud Director 報告的工作。**事件**畫面顯示由 VMware Cloud Director 報告的事件。

您可以透過使用 `Branding` Cloud Director OpenAPI 自訂 VMware Cloud Director 租用戶入口網站。如需使用 Cloud Director OpenAPI 的相關資訊，請參閱《Cloud Director OpenAPI 入門》文件，網址為 https://code.vmware.com。

使用 VMware Cloud Director 全域搜尋

您可以使用 VMware Cloud Director 全域搜尋，依名稱或部分名稱搜尋環境中的物件名稱。如果虛擬機器的 IP 位址為靜態，也可以依 IP 位址搜尋虛擬機器。

預設物件清單為：

- 資料中心
- vApp 範本
- vApp
- 虛擬機器
- vApp 網路
- 目錄

如果虛擬機器使用由 DHCP 指派的 IP 位址，搜尋不會傳回其 IP 位址。如果您要搜尋的虛擬機器使用由 DHCP 指派的 IP 位址，您必須依名稱搜尋。

依預設，您只能搜尋本機站台中的物件。如果您有多站台環境，您可以在多個站台之間進行搜尋。

程序

1. 在 VMware Cloud Director 租用戶入口網站的右上角，按一下**搜尋**圖示。
2. (選擇性) 透過按一下**釘選**圖示，釘選搜尋面板。
3. 在**搜尋**文字方塊中，輸入用於搜尋相符物件名稱或虛擬機器的靜態 IP 位址的符號、部分名稱或 IP 位址。
4. 如果您使用多站台環境，請選取您要在其中執行搜尋的站台。
5. 按 **Enter** 鍵。

結果

此時會顯示每個物件類型的前五個相符結果。結果會按字母順序進行排序。

後續步驟

- 若要查看更多結果 (如有)，請按一下每個物件類型下的**載入更多**。
- 若要查看搜尋結果中有關特定物件的詳細資訊，請指向該物件。
- 若要管理某特定物件 (例如，檢視或修改物件設定)，請按一下該物件。此時會在左側顯示有關物件的詳細資料。

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

從租用戶入口網站中，您可以檢視最近的工作清單及其詳細資料和狀態。此外，還可以查看所有工作的清單。

依預設，**最近的工作**面板顯示在租用戶入口網站的底部，其中包含最近執行的工作清單。啟動作業時，例如建立虛擬機器，該工作會顯示在此面板中。在最小化**最近的工作**面板的情況下，仍會看到正在執行或已失敗的最近工作的數目。透過按一下雙箭頭，隨時可以再次開啟**最近的工作**面板。

工作視圖中會列出所有工作，並顯示執行工作的時間及其是否成功完成。此視圖是對您環境中的問題進行疑難排解的第一步。工作視圖包含長時間執行的作業，例如虛擬機器或 vApp 建立。

程序

1 在頂部導覽列中，按一下**監控**和**工作**。

此時將顯示所有工作的清單，以及工作執行時間和工作狀態。

2 按一下編輯器圖示 ( )，以變更您要檢視的工作的詳細資料。

3 (選擇性) 若要檢視工作詳細資料，請按一下工作名稱。

工作詳細資料包括失敗原因、工作失敗的時間等資訊。

詳細資料	說明
作業	所執行作業的名稱。
工作識別碼	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`。
組織	組織名稱。
狀態	工作狀態，如 [成功]、[執行中] 或 [失敗]。
啟動器	啟動作業的使用者。
開始時間	作業開始的日期和時間。
完成時間	作業成功或失敗的日期和時間。
服務命名空間	服務名稱，例如 *com.vmware.cloud*。
詳細資料	工作失敗的原因。例如，如果您嘗試建立虛擬機器的快照，但因儲存區不足而導致作業失敗，則工作詳細資料的類型為：要求的作業將會超出 `VDC` 的儲存配額：儲存區原則 `"*"` 有 `8,693 MB` 剩餘，要求 `41,472 MB`。

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**。

使用虛擬機器

2

虛擬機器是一種軟體電腦，可以像實體電腦一樣執行作業系統和應用程式。虛擬機器由一組規格和組態檔組成，並由主機實體資源支援。每台虛擬機器都擁有可提供與實體硬體功能相同的虛擬裝置，但這些裝置更易於攜帶、管理，且更加安全。

除了您可以在實體機器上執行的作業外，VMware Cloud Director 虛擬機器支援虛擬基礎結構作業，例如建立虛擬機器狀態的快照，以及將虛擬機器從一台主機移至另一台主機。

從 VMware Cloud Director 9.5 開始，虛擬機器支援 IPv6 連線。您可以將 IPv6 位址指派給連線至 IPv6 網路的虛擬機器。

重要 假設您有多個虛擬資料中心，使用虛擬機器的所有步驟均從卡視圖中進行記錄。從網格視圖也可以完成相同的程序，但步驟可能略有差別。

本章節討論下列主題：

- 虛擬機器架構
- 虛擬機器加密
- 檢視虛擬機器
- 建立新的獨立虛擬機器
- 快速佈建虛擬機器
- 開啟虛擬機器主控台
- 在虛擬機器上執行電源作業
- 在虛擬機器中安裝 VMware Tools
- 升級虛擬機器的虛擬硬體版本
- 編輯虛擬機器內容
- 插入媒體
- 退出媒體
- 將虛擬機器複製到不同的 vApp
- 將虛擬機器移動至不同的 vApp
- 虛擬機器相似性和反相似性

- 監控虛擬機器
- 使用快照
- 更新虛擬機器租用
- 刪除虛擬機器
- 自動縮放群組

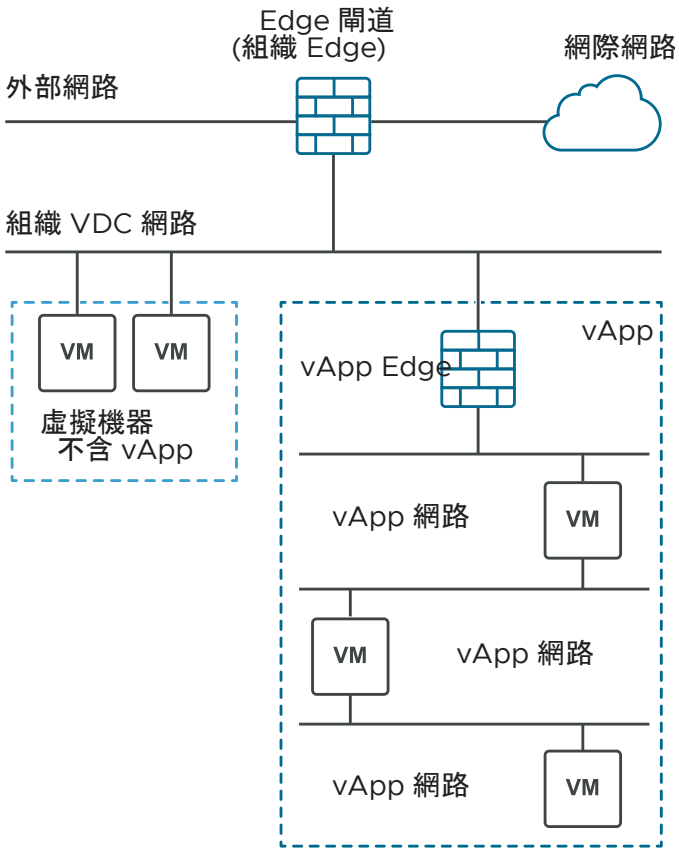
虛擬機器架構

虛擬機器可以做為獨立機器存在，也可以存在於 vApp 中。

虛擬機器是一種軟體電腦，可以像實體電腦一樣執行作業系統和應用程式。虛擬機器由一組規格和組態檔組成，並由主機實體資源支援。每台虛擬機器都擁有可提供與實體硬體功能相同的虛擬裝置，但這些裝置更易於攜帶、管理，且更加安全。虛擬機器可以是獨立的，也可以存在於 vApp 中。vApp 是複合物件，由一或多個虛擬機器以及一或多個網路組成。

建立虛擬機器時，下圖會顯示不同的選項。您可以建立獨立虛擬機器，也可以在 vApp 內建立虛擬機器。獨立虛擬機器直接連線至組織虛擬資料中心。也可以在 vApp 中建立虛擬機器。透過在 vApp 內建立虛擬機器，您可以將多個虛擬機器及其相關聯的網路歸為同一組。vApp 可讓您建立複雜的應用程式，並將其儲存至目錄以供日後使用。

圖 2-1. 虛擬機器是獨立的或位於 vApp 中



虛擬機器加密

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。您可以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，以加密虛擬機器和磁碟。

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。

如果組織 VDC 具有已啟用虛擬機器加密的儲存區原則，您可以加密虛擬機器和磁碟。請參閱《VMware Cloud Director Service Provider Admin Portal 指南》中的〈對組織虛擬資料中心的儲存區原則啟用虛擬機器加密〉主題。若要加密虛擬機器或磁碟，請將其與已啟用虛擬機器加密的儲存區原則相關聯。對於虛擬機器，請參閱建立新的獨立虛擬機器或變更虛擬機器的一般內容。對於具名磁碟，請參閱建立具名磁碟或編輯具名磁碟。若要解密虛擬機器或磁碟，請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**可以在虛擬機器的**詳細資料**頁面上，檢視虛擬機器及其磁碟的加密狀態。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。

檢視虛擬機器

您可以檢視獨立虛擬機器或做為 vApp 一部分的虛擬機器。您可以在網格視圖或卡視圖中檢視虛擬機器。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。

2 選擇下列其中一項。

- 若要在網格視圖中檢視虛擬機器，請按一下  。
- 若要在卡視圖中檢視虛擬機器，請按一下  。

虛擬機器的清單會顯示在網格視圖中或顯示為卡清單。

3 (選擇性) 從**排序依據**下拉式功能表排列虛擬機器清單。

4 (選擇性) 在網格視圖中，按一下虛擬機器的左側 ，以顯示可針對所選虛擬機器採取的動作。

例如，您可以關閉虛擬機器。

5 若要存取虛擬機器之客體作業系統的介面，請按一下卡視圖右上角的桌面圖示。

6 若要檢視和編輯虛擬機器的詳細資料，請按一下**詳細資料**。

建立新的獨立虛擬機器

您可以建立新的獨立虛擬機器。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。

2 按一下  以檢視卡視圖中的清單，並選擇性地從**排序依據**下拉式功能表排列虛擬機器清單。

3 按一下**新增虛擬機器**。

4 輸入虛擬機器的名稱和電腦名稱。

重要 電腦名稱只能包含英數字元和連字號。電腦名稱不能只包含數字，且不能包含空格。

5 (選擇性) 輸入有意義的說明。

6 選取建立虛擬機器後是否要立即開啟其電源。

7 選取您要部署虛擬機器的方式。

選項	動作
新增	使用可自訂設定部署新的虛擬機器。 a 選取作業系統系列和作業系統。 b (選擇性) 選取開機映像。 c (選擇性) 選取虛擬機器放置原則和虛擬機器大小調整原則。 僅當服務提供者已將此類原則發佈至組織 VDC 時，才會顯示虛擬機器放置和虛擬機器大小調整原則下拉式功能表。 d (選擇性) 從預先定義的大小調整選項中選取虛擬機器的大小，或按一下**自訂大小調整選項**以手動輸入虛擬 CPU 的數目、每個通訊端的核心數以及記憶體設定。 如果選取用於定義虛擬機器大小的虛擬機器大小調整原則，則不會顯示此選項。 虛擬機器的預先定義的大小為**小型**、**中型**和**大型**。 e 指定虛擬機器的儲存區設定，例如儲存區原則和大小 (GB)。 f 指定虛擬機器的網路設定，例如網路、IP 模式、IP 位址和主要 NIC。
從範本	從您從範本目錄選取的範本部署虛擬機器。 a 從可用範本清單中選取虛擬機器範本。 b (選擇性) 選取虛擬機器放置原則和虛擬機器大小調整原則。 僅當服務提供者已將此類原則發佈至組織 VDC 時，才會顯示虛擬機器放置和虛擬機器大小調整原則下拉式功能表。如果選取的範本具有已指派的原則，則可能僅限於使用預先定義的範本原則。 c (選擇性) 選取以使用自訂儲存區原則，然後從**要使用的自訂儲存區原則**下拉式功能表中選取要使用的儲存區原則。 d 閱讀並接受終端使用者授權合約 (如有)。

8 按一下**確定**以儲存虛擬機器的設定，並啟動建立程序。

您可以查看目錄中的虛擬機器卡。虛擬機器建立完成之前，其狀態會一直顯示為 [忙碌]。

快速佈建虛擬機器

快速佈建使用連結的複製進行虛擬機器佈建操作，進而節省時間。

連結複製是使用與原始機器相同虛擬磁碟的重複虛擬機器，並有一串差異磁碟以追蹤原始與複製機器間的差別。如果停用快速佈建，所有佈建作業都會產生完整複製。

連結複製無法存在於原始虛擬機器之外的不同 vCenter Server 資料中心或資料存放區上。

在快速佈建虛擬機器時，VMware Cloud Director 會為與特定 vApp 範本相關聯的虛擬機器建立陰影虛擬機器，以支援在 vCenter Server 資料中心與資料存放區上建立連結複製。

陰影虛擬機器是原始虛擬機器的完全相同複本。陰影虛擬機器會建立在用於建立連結複製的資料中心與資料存放區上。

重要 在使用原生快照的儲存區容器上不支援就地整併快速佈建的虛擬機器。已啟用 VVOL 和 VAAI 的資料存放區使用原生快照，以便無法整併已部署到其中一個儲存區容器的快速佈建虛擬機器。如果您需要整併已部署到啟用 VVOL 或 VAAI 之資料存放區的快速佈建虛擬機器，您必須將其重新放置到其他儲存區容器。

開啟虛擬機器主控台

存取虛擬機器主控台，可讓您檢視虛擬機器的相關資訊、使用客體作業系統，以及執行可影響客體作業系統的作業。

必要條件

虛擬機器已開啟電源。

在用戶端上安裝 VMware Remote Console

VMware Remote Console 在 VMware Cloud Director 佈建和管理的所有虛擬機器中提供內嵌式使用者-客體互動。本節詳述在 Windows、Apple OS X 和 Linux 上安裝 VMware Remote Console 的必要工作。

必要條件

此作業需要預先定義之 **vApp 使用者**角色中包含的權限或一組同等權限。

程序

1 下載安裝程式。

- 導覽至 VMware Remote Console 下載頁面，然後選取您的平台對應的連結。

  www.vmware.com/go/download-vmrc

- 在 VMware Cloud Director Tenant Portal 的**虛擬資料中心**儀表板畫面中，按一下您想要探索的虛擬資料中心的卡。選取虛擬機器，然後從**動作**功能表中選取**下載 VMRC**。

2 執行平台安裝。

- 如果您使用的是 Windows，請按兩下 `.msi` 安裝程式，然後依照提示進行操作。
- 如果您使用的是 Linux，請使用 **root** 權限登入，然後執行 `.bundle` 安裝程式，並依照提示進行操作。
- 如果您使用的是 Mac OS，請按兩下 `.dmg` 加以開啟，然後按兩下其中的 VMware Remote Console 圖示以複製到 Applications 資料夾。

結果

安裝完成後，會在您按一下以 `vmrc://` 配置開頭的統一資源識別元 (URI) 時開啟 VMware Remote Console。VMware Workstation、Player 和 Fusion 也可處理 `vmrc://` URI 配置。

開啟虛擬機器遠端主控台

您可以透過 VMware Cloud Director 租用戶入口網站，使用 VMware Remote Console 開啟虛擬機器主控台。

必要條件

- 確認 VMware Remote Console 已安裝在本機系統上。

- 請確保選取的虛擬機器處於已開啟電源狀態。
- 此作業需要預先定義之 **vApp 使用者**角色中包含的權限或一組同等權限。

程序

1. 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。
2. 按一下  以檢視卡視圖中的清單，並選擇性地從**排序依據**下拉式功能表排列虛擬機器清單。
3. 從虛擬機器的**動作**功能表中，選取**啟動虛擬機器遠端主控台**。

   備註 如果您沒有安裝 VMware Remote Console，快顯視窗會提示您安裝 VMware Remote Console 或使用 Web 主控台。

結果

虛擬機器主控台將會開啟，做為外部虛擬遠端主控台。

備註 使用 VMware Remote Console 連線至 VMware Cloud Director 虛擬機器時，您只能在主控台上進行互動 (傳送 `Ctrl+Alt+Del`)。您無法執行裝置作業、電源作業或設定管理。

開啟 Web 主控台

即使本機系統上未安裝 VMware Remote Console，您也可以連線至虛擬機器的主控台。

必要條件

- 確認虛擬機器已開啟電源。
- 此作業需要預先定義之 **vApp 使用者**角色中包含的權限或一組同等權限。

程序

1. 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。
2. 按一下  以檢視卡視圖中的清單，並選擇性地從**排序依據**下拉式功能表排列虛擬機器清單。
3. 從虛擬機器的**動作**功能表中，選取**啟動 Web 主控台**。

結果

透過使用 VMware HTML Console SDK，虛擬機器主控台在新的瀏覽器索引標籤中開啟。

後續步驟

按一下主控台視窗中的任一處，即可在主控台中開始使用滑鼠、鍵盤和其他輸入裝置。

備註 如需有關支援的國際鍵盤的資訊，請參閱 VMware HTML Console SDK 說明文件，網址為 https://www.vmware.com/support/developer/html-console/。

在虛擬機器上執行電源作業

您可以在虛擬機器上執行電源作業，例如開啟或關閉虛擬機器的電源、暫停或重設虛擬機器或關閉虛擬機器的客體作業系統。

開啟虛擬機器的電源

開啟虛擬機器的電源等同於開啟實體機器的電源。

除非虛擬機器已安裝最新版的 VMware Tools，否則您無法將已啟用客體自訂的虛擬機器電源開啟。

必要條件

虛擬機器已關閉電源。

程序

1. 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。
2. 按一下  以檢視卡視圖中的清單，並選擇性地從**排序依據**下拉式功能表排列虛擬機器清單。
3. 從要啟動的虛擬機器的**動作**功能表中，選取**開啟電源**。

結果

已開啟電源的虛擬機器會以綠色顯示 [已開啟電源] 狀態。

關閉虛擬機器的電源

關閉虛擬機器的電源等同於關閉實體機器的電源。

必要條件

虛擬機器已開啟電源。

程序

1. 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。
2. 按一下  以檢視卡視圖中的清單，並選擇性地從**排序依據**下拉式功能表排列虛擬機器清單。
3. 從要關閉電源的虛擬機器的**動作**功能表中，選取**關閉電源**。

結果

已關閉電源的虛擬機器會以紅色顯示 [已關閉電源] 狀態。

關閉客體作業系統

關閉虛擬機器的客體作業系統等同於關閉實體機器的電源。

必要條件

必須開啟虛擬機器和客體作業系統的電源。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。

2 按一下  以檢視卡視圖中的清單，並選擇性地從**排序依據**下拉式功能表排列虛擬機器清單。

3 從虛擬機器的**動作**功能表中，選取**關閉客體作業系統**。

結果

客體作業系統即會關閉。

重設虛擬機器

重設虛擬機器會清除狀態 (記憶體、快取等)，但虛擬機器仍會繼續執行。重設虛擬機器等同於按實體機器的重設按鈕。它會起始作業系統硬重設，且不會變更虛擬機器的電源狀態。

必要條件

虛擬機器已開啟電源。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。

2 按一下  以檢視卡視圖中的清單，並選擇性地從**排序依據**下拉式功能表排列虛擬機器清單。

3 從要重設的虛擬機器的**動作**功能表中，選取**重設**。

結果

虛擬機器的狀態即會清除。

暫停虛擬機器

暫停虛擬機器時，會透過將記憶體寫入磁碟來保留其目前狀態。

當您想要儲存虛擬機器的目前狀態，並且稍後從同一狀態繼續工作時，暫停和繼續功能非常有用。

必要條件

虛擬機器已開啟電源。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。

2 按一下  以檢視卡視圖中的清單，並選擇性地從**排序依據**下拉式功能表排列虛擬機器清單。

3 從要暫停的虛擬機器的**動作**功能表中，選取**暫停**。

結果

虛擬機器即會暫停，但其狀態會保留下來。

捨棄虛擬機器的暫停狀態

如果虛擬機器處於暫停狀態，並且您不再需要繼續使用該機器，則可以捨棄暫停狀態。捨棄暫停狀態會移除儲存的記憶體，並將機器恢復為已關閉電源狀態。

必要條件

處於暫停狀態的虛擬機器。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。

2 按一下  以檢視卡視圖中的清單，並選擇性地從**排序依據**下拉式功能表排列虛擬機器清單。

3 從虛擬機器的**動作**功能表中，選取**捨棄暫停狀態**。

結果

狀態已捨棄，並且虛擬機器的電源已關閉。

開啟多個虛擬機器的電源

您可以同時開啟多個虛擬機器的電源。

除非虛擬機器已安裝最新版的 VMware Tools，否則您無法將已啟用客體自訂的虛擬機器電源開啟。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。

2 開啟**多重選取**選項。

3 選取您要開啟電源的虛擬機器。

4 從**動作**功能表中，選取**開啟電源**。

5 按一下**確定**以進行確認。

關閉多個虛擬機器的電源

您可以同時關閉多個虛擬機器的電源。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。

2 開啟**多重選取**選項。

3 選取您要關閉電源的虛擬機器。

4 從**動作**功能表中，選取**關閉電源**。

5 按一下**確定**以進行確認。

捨棄多個虛擬機器的暫停狀態

如果多個虛擬機器處於暫停狀態，並且您不再需要繼續使用，則可以同時捨棄這些虛擬機器的暫停狀態。捨棄暫停狀態會移除儲存的記憶體，並將虛擬機器恢復為已關閉電源狀態。

必要條件

確認虛擬機器處於暫停狀態。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。

2 開啟**多重選取**選項。

3 選取您想要捨棄暫停狀態的虛擬機器。

4 從**動作**功能表中，選取**捨棄暫停狀態**。

5 按一下**確定**以進行確認。

重設多個虛擬機器

同時重設多個虛擬機器會清除其狀態 (記憶體、快取等)，但虛擬機器仍會繼續執行。

重設虛擬機器等同於按實體機器的重設按鈕。它會起始作業系統硬重設，且不會變更虛擬機器的電源狀態。

必要條件

確認虛擬機器已開啟電源。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。

2 開啟**多重選取**選項。

3 選取您要重設的虛擬機器。

4 從**動作**功能表中，選取**重設**。

5 按一下**確定**以進行確認。

在虛擬機器中安裝 VMware Tools

VMware Cloud Director 根據 VMware Tools 來自訂客體作業系統。

VMware Tools 會將一般作業系統驅動程式取代為已針對虛擬硬體調整的 VMware 驅動程式，來改善虛擬機器的管理和效能。VMware Tools 安裝在客體作業系統上。雖然客體作業系統在不安裝 VMware Tools 的情況下也可以執行，但這樣會失去重要功能和便利性。

必要條件

- 確認虛擬機器已開啟電源。
- 如果您新建立的虛擬機器沒有客體作業系統，則必須先安裝它，才能安裝 VMware Tools。
- 必須在安裝 VMware Tools 之前停用客體自訂。
- 如果 VMware Tools 的版本比 vApp 的虛擬機器中的 7299 舊，則必須予以升級。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。

2 按一下  以檢視卡視圖中的清單，並選擇性地從**排序依據**下拉式功能表排列虛擬機器清單。

3 從要安裝 VMware Tools 的虛擬機器的**動作**功能表中，選取**安裝 VMware Tools**。

將在目標客體作業系統上安裝 VMware Tools。如果在安裝期間發生錯誤，會顯示錯誤訊息。您也可以在**工作**視窗中檢視安裝作業的進度。

4 若要開啟虛擬機器的 Web 主控台，請從**動作**功能表中選取**啟動 Web 主控台**。

5 請遵循 VMware 知識庫文章 1014294 中的指示為特定作業系統設定 VMware Tools。

結果

將在客體作業系統上安裝和設定 VMware Tools。

升級虛擬機器的虛擬硬體版本

您可以升級虛擬機器的虛擬硬體版本。虛擬硬體版本越新，支援的功能就越多。

您不可以降級 vApp 中虛擬機器的硬體版本。

VMware Cloud Director 支援的硬體版本取決於支援 vSphere 資源。支援的硬體版本取決於支援提供者 VDC 中的最新支援的虛擬硬體版本。**組織管理員**或**系統管理員**可將硬體版本設定為低於基礎硬體支援的最新版本。VMware Cloud Director 租用戶入口網站根據組織或提供者 VDC 的支援硬體，以動態方式設定可選取的虛擬硬體版本的清單。

如需虛擬機器相容性設定可用的硬體功能的相關資訊，請參閱《vSphere 虛擬機器管理》。

如需 VMware 產品及其虛擬硬體版本的相關資訊，請參閱 https://kb.vmware.com/s/article/1003746。

必要條件

- 停止虛擬機器或包含此虛擬機器的 vApp。
- 確認虛擬機器上已安裝最新版本的 VMware Tools。

程序

1. 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。
2. 按一下  以檢視卡視圖中的清單，並選擇性地從**排序依據**下拉式功能表排列虛擬機器清單。
3. 從要升級的虛擬機器的**動作**功能表中，選取**升級虛擬硬體版本**。
4. 按一下**確定**。

結果

虛擬機器即會升級至最新版本。

編輯虛擬機器內容

您可以編輯虛擬機器的內容，包括虛擬機器名稱和說明、硬體和網路設定、客體作業系統設定等。

變更虛擬機器的一般內容

您可以檢閱和變更虛擬機器的名稱、描述和其他一般內容。

必要條件

變更作業系統等內容需要關閉機器電源。

程序

1. 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。
2. 按一下  以檢視卡視圖中的清單，並選擇性地從**排序依據**下拉式功能表排列虛擬機器清單。
3. 在您要編輯的虛擬機器卡中，按一下**詳細資料**。
4. 依預設，會展開可在**一般**下檢視或編輯的內容清單。

選項	動作
虛擬機器名稱	編輯虛擬機器的名稱。 當虛擬機器開啟電源時，您可以編輯此內容。
電腦名稱	編輯客體作業系統中設定的電腦和主機名稱，用來在網路上識別虛擬機器。因為 Windows 作業系統的電腦名稱限制，所以此欄位限制為 15 個字元。 當虛擬機器開啟電源時，您可以編輯此內容。

選項	動作
描述	編輯虛擬機器的選擇性說明。 當虛擬機器開啟電源時，您可以編輯此內容。
作業系統系列	從下拉式功能表中選取作業系統系列。 當虛擬機器關閉電源時，您可以編輯此內容。此外，如果作業系統已存在於虛擬機器上，則無法編輯此內容。
作業系統	從下拉式功能表中選取作業系統。 當虛擬機器關閉電源時，您可以編輯此內容。此外，如果作業系統已存在於虛擬機器上，則無法編輯此內容。
開機延遲	指定延遲開機作業的時間 (毫秒)。 虛擬機器開啟電源與結束 BIOS，並啟動客體作業系統軟體之間的間隔時間可能非常短暫。您可以變更開機延遲，以提供更多時間。
儲存空間原則	從下拉式功能表中選取虛擬機器要使用的儲存空間原則。 當虛擬機器開啟電源時，您可以編輯此內容。
虛擬資料中心	檢視此虛擬機器所屬的虛擬資料中心的名稱。
VMware Tools	檢視是否已在虛擬機器上安裝 VMware Tools。
虛擬硬體版本	檢視虛擬機器的虛擬硬體版本。
升級為：	若要升級，請從下拉式功能表中選取版本。
同步時間	選取此核取方塊，即可啟用虛擬機器客體作業系統與執行該系統之虛擬資料中心之間的時間同步。
進入 BIOS 設定	選取是否要在虛擬機器下次開機時強制進入 BIOS 設定畫面。 當虛擬機器關閉電源時，您可以編輯此內容。

5 變更完成後，按一下**儲存**。

變更虛擬機器的硬體內容

您可以檢閱和變更虛擬機器的硬體內容。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。

2 按一下  以檢視卡視圖中的清單，並選擇性地從**排序依據**下拉式功能表排列虛擬機器清單。

3 在您要編輯的虛擬機器卡中，按一下**詳細資料**。

4 按一下**硬體**以展開您可以檢視和編輯的硬體內容清單。

選項	描述
虛擬 CPU 數目	編輯 CPU 的數目。 可以指派給虛擬機器的虛擬 CPU 的數目上限，取決於主機上的邏輯 CPU 數目，以及虛擬機器上安裝的客體作業系統類型。
每個插槽的核心數	編輯每個插槽的核心數目。 您可以根據核心和每個插槽核心數設定虛擬 CPU 的指派方式。依據您要使用單核心 CPU、雙核心 CPU、三核心 CPU 等因素，判定虛擬機器需要多少 CPU 核心，然後選取應指派給每個插槽的核心數目。
向客體作業系統顯露硬體協助的 CPU 虛擬化	可以向客體作業系統公開完整的 CPU 虛擬化，以便需要硬體虛擬化的應用程式在不需要進行二進位轉譯或半虛擬化的情況下可在虛擬機器上執行。
記憶體總計	編輯虛擬機器的記憶體資源設定。虛擬機器記憶體大小必須是 4 MB 的倍數。 此設定會決定配置給虛擬機器的 ESXi 主機記憶體數量。虛擬硬體記憶體大小將決定在虛擬機器中執行的應用程式可使用的記憶體大小。虛擬機器無法獲得多於其已設定虛擬硬體記憶體大小的記憶體資源。
記憶體熱新增	如果您啟用記憶體熱新增，則可以在虛擬機器開啟電源時，將記憶體資源新增至該機器。只有特定客體作業系統和大於 7 的虛擬機器硬體版本才支援此功能。
虛擬 CPU 熱新增	如果您啟用虛擬 CPU 熱新增，則可以在虛擬機器開啟電源時，將虛擬 CPU 新增至該機器。新增的 CPU 數目必須是每個插槽核心數目的倍數。只有特定客體作業系統和虛擬機器硬體版本才支援此功能。
插槽數目	檢視通訊端數目。 通訊端數目由可用的虛擬 CPU 數目所決定。當您更新虛擬 CPU 數目時，該數目會有所變更。
卸除式媒體	檢視可用的卸除式媒體，例如連結的 CD/DVD 和軟碟機。

5 在**硬碟**下，按一下**新增**以新增硬碟。

選項	描述
大小	輸入硬碟大小 (以 MB 為單位)。您可以稍後增加硬碟的大小。 **備註** 如果虛擬機器不是連結複製且沒有快照，您可以增加現有硬碟的大小。
原則	預設會使用虛擬機器的儲存區原則。 依預設，連接至虛擬機器的所有硬碟均使用為此虛擬機器指定的儲存空間原則。您可在建立虛擬機器或修改其內容時，覆寫任一磁碟的此預設值。每個硬碟的 [大小] 資料行包含一個下拉式功能表，列出此虛擬機器可用的所有儲存區原則。
IOPS	為磁碟選取特定的 IOPS。 使用此選項可限制每個磁碟的每秒 I/O 作業數。
匯流排類型	選取匯流排類型。 選項包括 **Paravirtual (SCSI)**、**LSI Logic Parallel (SCSI)**、**LSI Logic SAS (SCSI)**、**IDE** 和 **SATA**。如需有關存放控制器類型和相容性的詳細資訊，請參閱《vSphere 虛擬機器管理指南》。
匯流排號碼	輸入匯流排號碼。
單元號碼	輸入硬碟機的邏輯單元號碼。

6 在 **NIC** 下，按一下**新增**以新增 NIC。

您可以新增最多 10 個 NIC。如需根據虛擬機器硬體版本支援的 NIC 數目的相關資訊，請參閱：http://kb.vmware.com/s/article/2051652。VMware Cloud Director 支援在虛擬機器執行時修改虛擬機器 NIC。如需支援的網路介面卡類型的相關資訊，請參閱 http://kb.vmware.com/kb/1001805。

選項	描述
主要 NIC	選取主要 NIC 時，會顯示一個旗標。 選取主要 NIC。主要 NIC 設定會決定虛擬機器的預設唯一閘道。虛擬機器可使用任何的 NIC 連線至虛擬和實體機器，這些機器則直接連線至與 NIC 相同的網路，但是只能使用主要 NIC 連線至需要閘道連線之網路上的機器。
NIC	NIC 數目。
已連線	選取核取方塊以連線 NIC。
網路	從下拉式功能表中選取網路。
IP 模式	選取 IP 模式。 **注意** 如果已選取要將 NIC 連線到的網路，請勿將 IP 模式設定為**無**。 ■ **靜態 - IP 集區** 從網路 IP 集區提取靜態 IP 位址。 ■ **靜態 - 手動** 可讓您手動指定特定的 IP 位址。如果您選取此選項，必須在 **IP 位址**資料行中輸入 IP 位址。 ■ **DHCP** 從 DHCP 伺服器中提取 IP 位址。
MAC 位址	從下拉式功能表中，選擇是保留還是重設 MAC 位址。

7 按一下**儲存**。

變更虛擬機器的客體作業系統自訂內容

VMware Cloud Director 上的客體作業系統自訂對於所有平台均為選用。對於必須加入 Windows 網域的虛擬機器，則為必要。

此功能表上要求的部分資訊僅適用於 Windows 平台。[客體作業系統自訂] 面板包含虛擬機器加入 Windows 網域所需的資訊。**組織管理員**可以指定該組織中 Windows 客體可以加入之網域的預設值。並非所有的 Windows 虛擬機器都必須加入網域，但在大多數企業安裝中，不是網域成員的虛擬機器無法存取許多可用網路資源。

必要條件

- 此作業需要預先定義之 **vApp 作者**角色中包含的權限或一組同等權限。
- 客體自訂需要虛擬機器執行 VMware Tools。

- 在可以自訂 Windows 客體作業系統之前，您的**系統管理員**必須在 VMware Cloud Director 伺服器群組上安裝適當的 Microsoft Sysprep 檔案。請參閱《VMware Cloud Director 安裝、設定與升級指南》。
- 自訂 Linux 客體作業系統要求客體中已安裝 Perl。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。

2 按一下  以檢視卡視圖中的清單，並選擇性地從**排序依據**下拉式功能表排列虛擬機器清單。

3 在您要編輯的虛擬機器卡中，按一下**詳細資料**。

4 按一下**客體作業系統自訂和內容**，以展開客體作業系統設定的清單。

選項	描述
啟用客體自訂	選取此選項可啟用客體自訂。
變更 SID	選取此選項可變更 Windows 安全性識別碼 (SID)。 此選項是執行 Windows 客體作業系統的虛擬機器所特有的。SID 在部分 Windows 作業系統中，可用於唯一識別系統和使用者。如果您未選取此選項，則新虛擬機器與其所依據的虛擬機器或範本將具有相同的 SID。如果電腦屬於網域的一部分，且僅使用網域使用者帳戶，則重複的 SID 不會引起問題。不過，如果機器是工作群組的一部分，或者使用本機使用者帳戶，則重複的 SID 可能會影響檔案存取控制。如需詳細資訊，請參閱 Microsoft Windows 作業系統的相關說明文件。
允許本機管理員密碼	選取此選項可允許設定客體作業系統的管理員密碼。 a 指定本機管理員的密碼。 將**指定密碼**文字方塊保留空白會自動產生密碼。 b 指定允許自動登入的次數。 輸入值 0 將以**管理員**身分停用自動登入。
管理員在初次登入時需變更密碼	選取此選項可要求管理員在初次登入時變更客體作業系統的密碼。為了安全起見，此為建議事項。
自動產生密碼	選取此選項可允許自動產生密碼。
啟用此虛擬機器以加入網域	您可以選取此選項，以將虛擬機器加入 Windows 網域。您可以使用組織的網域或覆寫組織的網域，然後輸入網域內容。 a 輸入網域名稱。 b 輸入使用者名稱與密碼。 c 輸入帳戶組織單位。
指令碼	您可以使用自訂指令碼修改虛擬機器的客體作業系統。將自訂指令碼新增至虛擬機器後，只在初始自訂和強制重新自訂時呼叫該指令碼。如果設定 `precustomization` 命令列參數，將在客體自訂開始之前呼叫該指令碼。如果設定 `postcustomization` 命令列參數，將在客體自訂完成之後呼叫該指令碼。 ■ 按一下指令碼文字方塊下方的上傳按鈕，以導覽至本機機器上的自訂指令碼。 ■ 直接在**指令碼檔案**文字方塊中輸入自訂指令碼。 直接在**指令碼檔案**文字方塊中輸入的自訂指令碼不能超過 1500 個字元。如需詳細資訊，請參閱 VMware 知識庫文章 https://kb.vmware.com/kb/1026614。

5 變更完成後，按一下**儲存**。

瞭解客體自訂

當您自訂客體作業系統時，有一些應該知道的設定和選項。

啟用客體自訂核取方塊

此核取方塊位於虛擬機器**內容**頁面的**客體作業系統自訂**索引標籤上。客體自訂的目標是根據**內容**頁面中選取的選項進行設定。如果選取此核取方塊，則會在必要時執行客體自訂和重新自訂。

需要此程序，所有客體自訂功能 (如電腦名稱、網路設定、管理員和根密碼的設定和到期、Windows 作業系統的 SID 變更等) 才能運作。應該選取此選項，**開啟電源並強制重新自訂**才能運作。

如果選取此核取方塊，而且 VMware Cloud Director 中虛擬機器的組態參數與客體作業系統中的設定不同步，則虛擬機器**內容**頁面上的**設定檔**索引標籤會顯示設定與客體作業系統不同步，虛擬機器需要客體自訂。

vApp 和虛擬機器的客體自訂行為

會取消選取這些核取方塊。

- **啟用客體自訂**
- 在 Windows 客體作業系統中，為**變更 SID**
- **密碼重設**

如果您想要執行自訂 (或變更了需要在客體作業系統中反映的網路設定)，則可以選取**啟用客體自訂**核取方塊，並在虛擬機器**內容**頁面的**客體作業系統自訂**索引標籤上設定選項。如果使用 vApp 範本中的虛擬機器來建立 vApp，然後新增虛擬機器，則 vApp 範本會做為建置區塊。當您將目錄中的虛擬機器新增至新的 vApp 時，預設會啟用虛擬機器以進行客體自訂。當您將目錄中的 vApp 範本儲存為 vApp 時，只有在選取**啟用客體自訂**核取方塊時，才會啟用虛擬機器以進行客體自訂。

這些是客體自訂設定的預設值：

- **啟用客體自訂**核取方塊與您目錄中的來源虛擬機器相同。
- 在 Windows 客體虛擬機器中，**變更 SID** 與您目錄中的來源虛擬機器相同。
- 密碼重設設定與您目錄中的來源虛擬機器相同。

必要時，您可以先取消選取**啟用客體自訂**核取方塊，然後啟動 vApp。

如果將會擱置客體作業系統安裝的空白虛擬機器新增至 vApp，則預設會取消選取**啟用客體自訂**核取方塊，因為這些虛擬機器尚未準備進行自訂。

在您安裝客體作業系統和 VMware Tools 之後，就可以關閉虛擬機器的電源、停止 vApp，以及選取**啟用客體自訂**核取方塊，並啟動 vApp 和虛擬機器以執行客體自訂。

如果更新已自訂的虛擬機器上的虛擬機器名稱和網路設定，則下次開啟該虛擬機器的電源時，會重新自訂該虛擬機器，以重新同步客體虛擬機器與 VMware Cloud Director。

開啟電源並強制重新自訂虛擬機器

您可以開啟虛擬機器的電源並強制重新自訂虛擬機器。

如果虛擬機器中的設定與 VMware Cloud Director 不同步，或執行客體自訂的嘗試失敗，您可以強制重新自訂虛擬機器。

確保虛擬機器中執行的應用程式支援重新自訂。如果使用 Microsoft Sysprep 變更網域控制站，且同時變更 SID，則虛擬機器可能會損毀。為了降低損毀虛擬機器的風險，請在重新自訂之前建立快照。

必要條件

- 您必須是組織管理員。
- 虛擬機器必須關閉電源。

程序

1. 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。
2. 按一下  以檢視卡視圖中的清單，並選擇性地從**排序依據**下拉式功能表排列虛擬機器清單。
3. 從要開啟電源和自訂的虛擬機器的**電源**功能表中，選取**開啟電源並強制重新自訂**。

結果

此時會重新自訂虛擬機器並開啟電源。

變更虛擬機器的進階內容

在**進階**設定中，您可以設定資源配置設定 (共用、保留及限制)，以決定提供給虛擬機器的 CPU、記憶體及儲存資源的數量。

使用資源配置設定 (共用、保留及限制)，以決定提供給虛擬機器的 CPU、記憶體及儲存資源的數量。

資源配置共用

共用可指定虛擬資料中心內虛擬機器的相對重要性。如果虛擬機器的某個資源的共用數目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資源。共用通常指定為 [高]、[一般] 或 [低]，這些值將分別按 4:2:1 的比例指定共用值。還可以選取 [自訂]，為各虛擬機器指派特定的共用數目 (表示比例權重)。當您將共用指派給虛擬機器時，一律會指定該虛擬機器相對於其他已開啟電源的虛擬機器的優先順序。

資源配置保留

指定保證為虛擬機器配置的最少資源量。僅在具有足夠的未保留資源用於滿足虛擬機器保留時，VMware Cloud Director 才允許您開啟虛擬機器電源。虛擬資料中心會保證該數量，即使它的資源已超載也是一樣。保留是以實體單位來表示 (MHz 或 MB)。

例如，假設您有 2 GHz 可用，並且指定 1 GHz 的資源配置保留給虛擬機器 1，另將 1 GHz 保留給虛擬機器 2。現在，每個虛擬機器在需要時都一定會取得 1GHz。但是，如果虛擬機器 1 僅使用 500 MHz，則虛擬機器 2 可以使用 1.5 GHz。

保留預設為 0。如果您需要保證虛擬機器一律具有最小必要 CPU 或記憶體數量，則可以指定保留。

資源配置限制

指定可配置給虛擬機器的 CPU 和記憶體資源上限。虛擬資料中心所配置的數量可以高於虛擬機器的保留，但絕不能高於限制，即使系統上具有未用的資源也是一樣。限制是以實體單位來表示 (MHz 或 MB)。

CPU 和記憶體資源限制預設為「無限制」。在大部份情況下，如果記憶體限制為無限制，則在建立虛擬機器時設定給它的記憶體數量就會變成其有效限制。

在大部份情況下，並不需要指定限制。如果您指定限制，則可能會浪費閒置資源。系統不允許虛擬機器所使用的資源高於限制，即使系統的使用量過低且有閒置資源可用也是一樣。只有在您有充分的原因需要指定限制時，才這麼做。

必要條件

- 保留集區虛擬資料中心。
- 確保虛擬資料中心已提供虛擬機器的特定記憶體數量。
- 保證特定的虛擬機器一律比其他虛擬機器配置更高百分比的虛擬資料中心資源。
- 設定可以配置給虛擬機器的資源上限。

程序

1. 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。
2. 按一下  以檢視卡視圖中的清單，並選擇性地從**排序依據**下拉式功能表排列虛擬機器清單。
3. 在您要編輯的虛擬機器卡中，按一下**詳細資料**。
4. 按一下**進階**和**編輯**。
5. 從**優先順序**下拉式功能表中選取選項，以設定 CPU 設定的資源配置共用。

選項	描述
低	每個虛擬 CPU 配置 500 個共用。
正常	每個虛擬 CPU 配置 1000 個共用。
高	每個虛擬 CPU 配置 2000 個共用。
自訂	可讓您為每個虛擬機器輸入共用數 (表示比例權重)，來指派特定數量的共用。 當您將共用指派給虛擬機器時，一律會指定該虛擬機器相對於其他已開啟電源的虛擬機器的優先順序。

6. 透過輸入保留 (以 MHz 為單位) 來指定 CPU 設定的保留，並選擇性地指定 CPU 設定的限制 (以 MHz 為單位)。

選項	描述
無限制	預設的 CPU 資源選項。
最大	指定可配置給虛擬機器的 CPU 資源上限 (以 MHz 為單位)。

7 從**優先順序**下拉式功能表中選取選項，以設定記憶體設定的資源配置共用。

選項	描述
低	每 MB 已設定虛擬機器記憶體配置 5 個共用。
正常	已設定虛擬機器記憶體的每個 MB 配置 10 個共用。
高	已設定虛擬機器記憶體的每個 MB 配置 20 個共用。
自訂	可讓您透過輸入共用數來指派特定數量的共用。

8 指定記憶體設定的保留 (以 MB 為單位)，並選擇性地指定記憶體設定的限制 (以 MB 為單位)。

選項	描述
無限制	預設的記憶體資源選項。
最大	指定可配置給虛擬機器的記憶體保留上限。

9 按一下**儲存**。

插入媒體

您可以從目錄插入要在虛擬機器客體作業系統中使用的媒體，例如 CD/DVD 映像。您可以使用這些媒體檔案在虛擬機器、各種應用程式、驅動程式等中安裝作業系統。

必要條件

您可以存取內含媒體檔案的目錄。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。

2 按一下  以檢視卡視圖中的清單，並選擇性地從**排序依據**下拉式功能表排列虛擬機器清單。

3 選取您要新增媒體的虛擬機器。

4 從**動作**功能表中，選取**插入媒體**。

5 在**插入 CD** 視窗中，選取要插入至虛擬機器的媒體檔案。

6 按一下**插入**。

退出媒體

在虛擬機器中完成使用 CD 或 DVD 之後，您可以將媒體檔案退出。

必要條件

媒體檔案先前已插入至虛擬機器。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。

2 按一下  以檢視卡視圖中的清單，並選擇性地從**排序依據**下拉式功能表排列虛擬機器清單。

3 選取您要從中退出媒體的虛擬機器。

4 從**動作**功能表中，選取**退出媒體**。

結果

隨即退出媒體檔案。

將虛擬機器複製到不同的 vApp

您可以將虛擬機器複製至另一個 vApp。當您複製虛擬機器時，原始虛擬機器會依然保留在來源 vApp 中。

當您複製虛擬機器時，快照不會包含在複本中。

必要條件

- 此作業需要預先定義之 **vApp 作者**角色中包含的權限或一組同等權限。
- 關閉虛擬機器電源。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。

2 按一下  以檢視卡視圖中的清單，並選擇性地從**排序依據**下拉式功能表排列虛擬機器清單。

3 從您要複製的虛擬機器的**動作**功能表中，選取**複製至**。

4 選取要將虛擬機器複製至的目的地 vApp，然後按**下一步**。

5 設定資源 (例如虛擬機器名稱和電腦名稱)，並選擇性地設定儲存區原則和 NIC，然後按**下一步**。

重要 電腦名稱只能包含英數字元和連字號。不能只包含數字，且不能包含空格。

6 在**即將完成**頁面上檢閱您的設定，然後按一下**完成**。

將虛擬機器移動至不同的 vApp

您可以將虛擬機器移至另一個 vApp。移動虛擬機器時，VMware Cloud Director 會從來源 vApp 中移除原始虛擬機器。

當您將虛擬機器移到不同的 vApp 時，已建立的快照會遺失。

在不同 vApp 之間移動虛擬機器需要使用 VMware vSphere® vMotion® 和增強型 vMotion 相容性 (EVC)。您可以將虛擬機器移到屬於同一組織內相同或其他組織 VDC 中的不同 vApp。組織 VDC 可位於相同的或其他的提供者 VDC 中。

將虛擬機器移到不同 vApp 時，可以執行重新設定作業 (例如，變更網路和儲存區設定檔)。

表 2-1. 虛擬機器移動期間進行的重新設定以及虛擬機器狀態

重新設定	目標 vApp 位於相同組織 VDC 時的虛擬機器狀態	目標 vApp 位於同一提供者 VDC 內其他組織 VDC 時的虛擬機器狀態
變更網路	已關閉電源	不適用
移除網路	已開啟電源或已關閉電源	不適用
變更儲存區設定檔	已開啟電源或已關閉電源	已關閉電源

必要條件

- 確認您具有 **vApp 作者**角色或一組同等權限。
- 確認基礎 vSphere 資源支援 vMotion 和 EVC。如需有關 vMotion 和 EVC 的需求和限制的相關資訊，請參閱《vCenter Server 和主機管理》。
- 如果您要變更虛擬機器網路或儲存區設定檔，請檢查是否必須關閉虛擬機器的電源。請參閱資料表虛擬機器移動期間執行的重新設定和虛擬機器狀態。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。

2 按一下  以檢視卡視圖中的清單，並選擇性地從**排序依據**下拉式功能表排列虛擬機器清單。

3 從要移動的機器的**動作**功能表中，選取**移動至**。

4 選取目的地 vAp，然後按**下一步**。

5 設定資源 (例如虛擬機器名稱和電腦名稱)，並選擇性地設定儲存區原則和 NIC，然後按**下一步**。

重要 電腦名稱只能包含英數字元和連字號。不能只包含數字，且不能包含空格。

6 在**即將完成**頁面上檢閱您的設定，然後按一下**完成**。

虛擬機器相似性和反相似性

相似性和反相似性規則可讓您將一組虛擬機器分散至不同 ESXi 主機，或將一組虛擬機器保留在特定 ESXi 主機上。

相似性規則可將一組虛擬機器置於特定主機上，以便輕鬆稽核這些虛擬機器的使用情況。反相似性規則可將一組虛擬機器置於不同主機上，以避免單一主機故障時，所有虛擬機器同時故障。

如果不符合相似性或反相似性規則，則新增至規則的虛擬機器將無法開啟電源。

檢視相似性和反相似性規則

您可以檢視現有的相似性和反相似性規則及其內容，例如受規則影響的虛擬機器以及規則是否已啟用。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**相似性規則**。

2 (選擇性) 按一下**網格編輯器**圖示 ()，然後選取要顯示規則的哪些詳細資料。

結果

您將看到現有相似性和反相似性規則、虛擬機器以及每個規則的啟用狀態的清單。

建立相似性規則

建立相似性規則可將一組特定的虛擬機器置於單一主機上，以便稽核這些虛擬機器的使用情況。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**相似性規則**。

2 在**相似性規則**下，按一下**新增**。

3 輸入規則的名稱。

4 取消選取**已啟用**可建立但不啟用規則。

依預設，已選取此核取方塊，規則建立後會加以啟用。

5 將**必要**核取方塊保留選取狀態。

依預設，每個相似性規則都是必要的。這表示如果不符合規則，則新增至規則的虛擬機器不會開啟電源。

6 選取要新增至相似性規則的虛擬機器。

7 按一下**儲存**。

結果

VMware Cloud Director 會將與此相似性規則相關聯的虛擬機器置於單一主機上。

建立反相似性規則

建立反相似性規則可將一組特定的虛擬機器置於多個主機上，以避免單一主機故障時，這些虛擬機器同時發生故障。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**相似性規則**。

2 在**反相似性規則**下，按一下**新增**。

3 輸入規則的名稱。

4 取消選取**已啟用**可建立但不啟用規則。

依預設，已選取此核取方塊，規則建立後會加以啟用。

5 將**必要**核取方塊保留選取狀態。

依預設，每個反相似性規則都是必要的。這表示如果不符合規則，則新增至規則的虛擬機器不會開啟電源。

6 選取要新增至反相似性規則的虛擬機器。

7 按一下**儲存**。

結果

VMware Cloud Director 會將與此反相似性規則相關聯的虛擬機器置於多個主機上。

編輯相似性或反相似性規則

您可以編輯相似性或反相似性規則，以啟用或停用規則、新增或移除虛擬機器，以及變更規則名稱或規則喜好設定。

必要條件

此作業需要 `Organization vDC: VM-VM Affinity Edit` 權限。此權限包含在預先定義的**目錄作者**、**vApp 作者**和**組織管理員**角色中。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**相似性規則**。

2 按一下要編輯的規則名稱旁邊的選項按鈕，然後按一下**編輯**。

3 編輯規則內容。

a 視需要變更這些規則的名稱。

b 選取是啟用還是停用規則。

c 將**必要**核取方塊保留選取狀態。

d 新增多個虛擬機器或移除虛擬機器。

4 按一下**儲存**。

刪除相似性或反相似性規則

如果您不再想要使用相似性規則或反相似性規則，則可以將其刪除。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**相似性規則**。

2 按一下要刪除的規則名稱旁邊的選項按鈕，然後按一下**刪除**。

3 若要確認您要刪除該規則，請按一下**確定**。

結果

VMware Cloud Director 會刪除相似性規則或反相似性規則。

監控虛擬機器

如果 VMware Cloud Director 管理員已啟用虛擬機器監控功能，您可以從租用戶入口網站檢視監控圖。

使用此功能以瞭解指定虛擬機器隨時間 (天、週或月) 變化的狀態。

必要條件

此功能僅在 VMware Cloud Director 管理員已啟用它的情況下可用。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。

2 按一下  以檢視卡視圖中的清單，並選擇性地從**排序依據**下拉式功能表排列虛擬機器清單。

3 選取您想要監控的虛擬機器，然後按一下**詳細資料**。

4 按一下**監控圖**以展開監控視圖。

[正在監視圖] 隨即顯示。

5

6 選取度量選項以監控虛擬機器。

度量下拉式功能表中的清單視**系統管理員**的選擇而有所不同。您會看到部分或全部選項。

度量	描述
最新佈建的磁碟	以 KB 為單位指定。 從天、週或月視圖中選擇。
平均磁碟讀取	以百分比指定。 從天、週或月視圖中選擇。
平均磁碟寫入	以百分比指定。 從天、週或月視圖中選擇。
平均 CPU 使用率	以百分比指定。 從天、週或月視圖中選擇。
平均 CPU 使用率 (MHz)	以 MHz 為單位指定。 從天、週或月視圖中選擇。
最大 CPU 使用率	以百分比指定。 從天、週或月視圖中選擇。

度量	描述
平均記憶體使用率	以百分比指定。 從天、週或月視圖中選擇。
最近使用的磁碟	以 KB 為單位指定。 從天、週或月視圖中選擇。

每次從清單中選取不同的值時，都會顯示新圖。

7 (選擇性) 變更度量收集的時間範圍。

8 按一下**重新整理**。

9 若要儲存變更，請按一下**儲存**。

使用快照

快照可保留建立時虛擬機器的狀態和資料。建立虛擬機器的快照時，虛擬機器不會受到影響，僅會複製和儲存處於指定狀態的虛擬機器之映像。如果您需要重複還原至相同的虛擬機器狀態，但不想建立多個虛擬機器，快照是很實用的功能。

快照是非常實用的暫時解決方案，可用於測試軟體是否有未知或潛在的有害影響。例如，您可將快照用作線性或反覆程序 (如安裝更新套件) 或分支程序 (如安裝不同版本的程式) 中的還原點。

您可能想要在升級虛擬機器的作業系統時使用快照。例如，升級虛擬機器之前，您可以建立快照以保留升級前的時間點。如果在升級期間未發生任何問題，您可以選擇移除快照，這會認可升級期間所做的變更。但是，如果您遇到問題，您可以還原快照，這樣便會回到升級前已儲存的虛擬機器狀態。

使用 VMware Cloud Director 時，您只能擁有一個虛擬機器快照。每次嘗試建立虛擬機器的新快照都會刪除之前的快照。

建立虛擬機器快照

您可以拍攝虛擬機器的快照。建立快照後，您可以將虛擬機器還原至快照，或是移除快照。

必要條件

確認虛擬機器未連線至具名磁碟。

備註 快照不會擷取 NIC 組態。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。

2 按一下  以檢視卡視圖中的清單，並選擇性地從**排序依據**下拉式功能表排列虛擬機器清單。

3 從您要建立快照的虛擬機器的**動作**功能表中，選取**建立快照**。

建立虛擬機器的快照將會取代現有的快照 (如有)。

4 (選擇性) 選取是否要建立虛擬機器記憶體的快照。

擷取虛擬機器的記憶體狀態時，快照會保留虛擬機器的即時狀態。記憶體快照可建立某一精確時間點的快照 (例如，升級仍在運作的軟體)。建立記憶體快照後，如果升級未如預期完成，或軟體不符合您的預期，可將虛擬機器還原到先前的狀態。

擷取記憶體狀態時，無需靜止虛擬機器的檔案。如果未擷取記憶體狀態，則快照不會儲存虛擬機器的即時狀態，除非靜止磁碟，否則磁碟就是當機一致的。

5 (選擇性) 選取是否要靜止客體檔案系統。

此作業要求在虛擬機器上安裝 VMware Tools。當您靜止虛擬機器時，VMware Tools 會靜止虛擬機器的檔案系統。靜止作業可確認快照磁碟代表客體檔案系統的一致狀態。已靜止的快照適用於自動備份或定期備份。例如，如果無法感知虛擬機器的活動，但希望還原為多個最近備份，則可以靜止檔案。

您無法靜止包含大容量磁碟的虛擬機器。

6 按一下**確定**。

結果

快照可讓您將虛擬機器還原為最新快照。

還原虛擬機器至快照

您可以將虛擬機器還原至建立快照時的當時狀態。

必要條件

虛擬機器具有快照。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。

2 按一下  以檢視卡視圖中的清單，並選擇性地從**排序依據**下拉式功能表排列虛擬機器清單。

3 從要還原至快照的虛擬機器的**動作**功能表中，選取**還原至快照**。

4 按一下**確定**。

結果

此時虛擬機器將還原為已儲存的快照。

移除虛擬機器快照

您可以移除虛擬機器的快照。

移除快照時，會刪除已保留的虛擬機器的狀態，且無法再回到該狀態。移除快照不會影響虛擬機器的目前狀態。

必要條件

具有已儲存快照的虛擬機器。

程序

1. 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。
2. 按一下  以檢視卡視圖中的清單，並選擇性地從**排序依據**下拉式功能表排列虛擬機器清單。
3. 從要移除快照的虛擬機器的**動作**功能表中，選取**移除快照**。
4. 按一下**確定**。

更新虛擬機器租用

如果租用即將到期，則可以更新虛擬機器租用。

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. 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。
2. 按一下  以檢視卡視圖中的清單，並選擇性地從**排序依據**下拉式功能表排列虛擬機器清單。
3. 從租用即將到期的虛擬機器的**動作**功能表中，選取**更新租用**。

結果

租用將會更新。您可以在**租用**欄位中查看新租用時間範圍。

刪除虛擬機器

您可以從組織中刪除虛擬機器。

必要條件

您的虛擬機器必須關閉電源。

程序

1. 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。
2. 按一下  以檢視卡視圖中的清單，並選擇性地從**排序依據**下拉式功能表排列虛擬機器清單。
3. 從您要刪除的虛擬機器的**動作**功能表中，選取**刪除**。

4 確認刪除。

結果

將會刪除虛擬機器。

自動縮放群組

從 VMware Cloud Director 10.2.2 開始，可以根據目前的 CPU 和記憶體使用情況自動縮放應用程式。

如需自動縮放解決方案組態的相關資訊，請參閱《VMware Cloud Director 安裝、設定與升級指南》中的〈自動縮放群組〉。

根據 CPU 和記憶體使用情況的預先定義準則，VMware Cloud Director 可以自動垂直擴充或縮減所選縮放群組中的虛擬機器數目。若要平衡為執行相同應用程式而設定的伺服器的負載，您可以使用 VMware NSX Advanced Load Balancer (Avi Networks)。

系統管理員和**組織管理員**角色對縮放群組中的虛擬機器擁有完全控制權。其他全域承租人角色可以檢視虛擬機器並存取虛擬機器 Web 主控台，但無法刪除、編輯、執行電源作業等。

如果刪除縮放群組，VMware Cloud Director 不會刪除縮放群組中任何現有的虛擬機器。

建立縮放群組

從 VMware Cloud Director 10.2.2 開始，您的服務提供者可授與您建立縮放群組的權限。縮放群組中的虛擬機器數量會根據您定義的條件自動變更。

您也可以從選取的組織虛擬資料中心 (VDC) 存取縮放群組。

程序

1 從頂部導覽列中，選取**應用程式**，然後選取**縮放群組**索引標籤。

2 按一下**新增縮放群組**。

3 選取要在其中建立縮放群組的組織 VDC。

4 輸入新縮放群組的名稱，並選擇性地輸入說明。

5 選取要將群組縮放到的虛擬機器數目下限和上限，然後按**下一步**。

6 為縮放群組中的虛擬機器選取虛擬機器範本和儲存區原則，然後按**下一步**。

7 為縮放群組選取網路。

- 如果您的 VDC 受 NSX-T Data Center 支援，請選取負載平衡器。
- 如果要自行管理負載平衡器或不需要負載平衡器，請選取**我的網路已完整設定**。

8 按一下**建立群組並新增規則**。

結果

VMware Cloud Director 開始對縮放群組進行初始擴充，以達到虛擬機器數目下限。

後續步驟

- 新增自動縮放規則
- 從縮放群組的詳細資料視圖中，如果選取**監控**，可以查看與此縮放群組相關的所有工作。例如，可以查看建立縮放群組的時間、群組的所有擴充或縮小工作、起始工作的規則等。
- 刪除縮放群組。如果刪除縮放群組，VMware Cloud Director 不會刪除縮放群組中任何現有的虛擬機器。如果您要減少虛擬機器數目，則必須手動將其刪除。

新增自動縮放規則

從 VMware Cloud Director 10.2.2 開始，您的服務提供者可授與您建立和管理縮放群組的權限。您可以新增用於觸發縮放群組擴充或縮小的規則。

必要條件

建立縮放群組

程序

1 從頂部導覽列中，選取**應用程式**，然後選取**縮放群組**索引標籤。

2 選取縮放群組，然後選取**規則**。

3 按一下**新增規則**。

4 輸入規則的名稱。

5 選取當規則生效時，縮放群組必須擴充還是縮小。

6 選取當規則生效時希望群組擴充或縮小的虛擬機器數目。

7 輸入在群組中每次自動縮放後的等待時間 (以分鐘為單位)。

在等待時間到期之前，條件無法觸發其他縮放。當縮放群組的任何規則生效時，等待時間將會重設。

8 新增觸發規則的條件。

持續時間是指條件必須保持有效以觸發規則的時間。若要觸發規則，則必須滿足所有條件。

9 (選擇性) 若要新增其他條件，請按一下**新增條件**。

10 按一下**新增**。

使用 vApp

3

vApp 包含的一個或多個虛擬機器透過網路進行通訊，而且在已部署的環境中使用資源和服務。vApp 可以包含多個虛擬機器。

從 VMware Cloud Director 9.5 開始，vApp 支援 IPv6 連線。您可以將 IPv6 位址指派給連線至 IPv6 網路的虛擬機器。

重要 假設您有多個虛擬資料中心，使用 vApp 的所有步驟均從卡視圖中進行記錄。從網格視圖也可以完成相同的程序，但步驟可能略有差別。

本章節討論下列主題：

- 下載 vApp 作為 OVF 套件
- 更新 vApp 租用
- 刪除 vApp
- 刪除多個 vApp

檢視 vApp

您可以在網格視圖或卡視圖中檢視 vApp。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 若要在網格視圖中檢視 vApp，請按一下 。若要在卡視圖中檢視 vApp，請按一下 。

vApp 的清單會顯示在網格中或顯示為卡清單。

3 (選擇性) 將網格視圖設定為包含您想要查看的詳細資料。

a 從網格視圖中，按一下**網格編輯器**圖示 ( )。

b 選取要查看的每個詳細資料旁邊的核取方塊，以選取要包含在網格視圖中的 vApp 詳細資料。

c 若要儲存變更，請按一下**確定**。

選取的詳細資料會顯示為每個 vApp 的資料行。

4 (選擇性) 在網格視圖中，按一下 vApp 左側的 ，以顯示可針對所選 vApp 採取的動作。

例如，您可以關閉 vApp。

建置新的 vApp

您可以決定使用目錄中的虛擬機器及/或新的虛擬機器建立 vApp，而不是根據 vApp 範本來建立 vApp。

建置 vApp 需要您提供 vApp 的名稱，並選擇性地提供其說明。您可以於稍後返回並將虛擬機器新增至 vApp。

必要條件

此作業需要預先定義之 **vApp 作者**角色中包含的權限或一組同等權限。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 選取**新增 vApp**。

3 輸入 vApp 的名稱，並選擇性地輸入其說明。

4 (選擇性) 如果您想讓 vApp 在部署時開啟電源，請選取**開啟電源**核取方塊。

備註 僅當其中包含虛擬機器時，vApp 才能開啟電源。

5 (選擇性) 搜尋目錄中要新增到此 vApp 的虛擬機器，或透過按一下**新增虛擬機器**來新增空白虛擬機器。

如果目錄中沒有任何虛擬機器，請建立虛擬機器，並將其新增至 vApp。

a 輸入虛擬機器的名稱和電腦名稱。

重要 電腦名稱只能包含英數字元和連字號。電腦名稱不能只包含數字，且不能包含空格。

b (選擇性) 輸入有意義的說明。

c 選取您要部署虛擬機器的方式。

選項	動作
新增	使用可自訂設定部署新的虛擬機器。 1 選取作業系統系列和作業系統。 2 (選擇性) 選取開機映像。 3 (選擇性) 選取虛擬機器放置原則和虛擬機器大小調整原則。 僅當服務提供者已將此類原則發佈至組織 VDC 時，才會顯示虛擬機器放置和虛擬機器大小調整原則下拉式功能表。 4 選取虛擬機器的大小，或按一下**自訂大小調整選項**手動輸入計算、記憶體和儲存區設定。 虛擬機器的預先定義的大小為小型、中型或大型。 5 指定儲存區設定，例如儲存區原則和大小 (GB)。 6 指定虛擬機器的網路設定，例如網路、IP 模式、IP 位址和主要 NIC。
從範本	從您從範本目錄選取的範本部署虛擬機器。 1 從目錄中選取虛擬機器範本。 2 (選擇性) 選取虛擬機器放置原則和虛擬機器大小調整原則。 僅當服務提供者已將此類原則發佈至組織 VDC 時，才會顯示虛擬機器放置和虛擬機器大小調整原則下拉式功能表。如果選取的範本具有已指派的原則，則可能僅限於使用預先定義的範本原則。 3 (選擇性) 選取以使用自訂儲存區原則，然後從**要使用的自訂儲存區原則**中選取原則。 4 若有終端使用者授權合約，您必須檢閱並接受此合約。

d 若要將虛擬機器新增至 vApp，請按一下**確定**。

您可以查看目錄中新增的虛擬機器。

6 (選擇性) 針對您想要在 vApp 內建立的每個其他虛擬機器，重複 步驟 5。

7 若要完成 vApp 建立，請按一下**建立**。

結果

隨即建立 vApp。當 vApp 開啟電源時，其中的虛擬機器隨即建立並且也處於開啟電源狀態。

從 OVF 套件建立 vApp

您可以直接從 OVF 套件建立並部署 vApp，而不需要建立 vApp 範本及對應的目錄項目。

VMware Cloud Director 對 OVF 部署具有自己的限制，這與 vCenter Server 中的限制不同。因此，在 vCenter Server 中成功的 OVF 部署在 VMware Cloud Director 中可能會失敗。

VMware Cloud Director 支援 OVF 1.1，但不支援 OVF 1.1 架構的所有部分。例如，不支援 OVF 中的 `DeploymentOptions` 部分。

VMware Cloud Director 中的 OVF 部署涉及許多元件，例如 `TransferService`、NFS 掛接上的 spool 區域、vCenter Server 的 NFC 連線、總和檢查碼驗證等。其中任何元件出現故障都會導致 OVF 上傳失敗。

如果上傳包含資訊清單檔案的 OVF 套件，VMware Cloud Director 會驗證 OVF 描述元檔案和所有 VMDK 檔案的 SHA-1 雜湊與 `manifest.mf` 檔案中的值是否相符。如果任何雜湊不相符，上傳將失敗。**系統管理員**可以透過將 `CONFIG` 內容設定為 `ovf.manifest.check.disabled` 來停用此檢查。

必要條件

- 請確認您有可上傳的 OVF 套件，以及擁有上傳 OVF 套件及部署 vApp 的權限。
- 確認 OVF 描述元檔案中的 OVF 版本不是 0.9。
- VMware Cloud Director 中預設支援的 OVF 描述元檔案大小上限為 12 MB。您可以透過編輯 `CONFIG` 內容 `ovf.descriptor.size.max` 來覆寫此值。
- 確認預設允許的資訊清單檔案 (副檔名為 .mf) 大小上限為 1 MB。
- 確認 OVF 套件符合 OVF XSD 架構。
- 如果 OVF 描述元檔案的 `VirtualSystemType` 元素中提供了硬體版本，請確認其低於上傳 OVF 的 VDC 中支援的最高硬體版本。
- 如果 OVF 描述元檔案包含 `ExtraConfig` 元素，請確認您的**系統管理員**將這些元素包含在 `extraConfigs` 元素的 `AllowedList` 中。未包含在 `AllowedList` 中的元素會導致 OVF 上傳失敗，並顯示驗證錯誤。

程序

1. 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。
2. 按一下**從 OVF 新增 vApp**。
3. 按一下**上傳**按鈕，瀏覽至可從電腦存取的位置，然後選取 OVF/OVA 範本檔案。

   位置可能為本機硬碟、網路共用或 CD/DVD 光碟機。支援的副檔名包括 `.ova`、`.ovf`、`.vmdk`、`.mf`、`.cert` 和 `.strings` 檔案。如果您選取上傳 OVF 檔案，而其參考的檔案超過您嘗試上傳的檔案 (例如，VMDK 檔案)，則必須瀏覽並選取所有檔案。
4. 按**下一步**。
5. 驗證即將部署的 OVF/OVA 範本的詳細資料，然後按**下一步**。
6. 輸入 vApp 的名稱，並選擇性地輸入其說明，然後按**下一步**。

7 (選擇性) 變更 vApp 的電腦名稱，使其僅包含英數字元。

僅當 vApp 名稱包含空格或特殊字元時，才需要執行此步驟。依預設，使用虛擬機器的名稱已預先填入電腦名稱。不過，電腦名稱必須僅包含英數字元。

8 在**儲存區原則**下拉式功能表中，選取 vApp 中每個虛擬機器的儲存區原則，然後按**下一步**。

9 選取每個虛擬機器要連線的網路。

- 從**網路**下拉式功能表中，選取每個虛擬機器的網路。
- 您可以選取**切換至進階網路工作流程**核取方塊，然後手動輸入 vApp 中每個虛擬機器的網路設定，例如主要 NIC、網路介面卡類型、網路、IP 指派和 IP 位址設定。

完成精靈後，您可以設定虛擬機器的其他內容。

10 按**下一步**。

11 自訂 vApp 中虛擬機器的硬體，然後按**下一步**。

選項	描述
虛擬 CPU 數目	輸入 vApp 中每個虛擬機器的虛擬 CPU 數目。 可以指派給虛擬機器的虛擬 CPU 的數目上限，取決於主機上的邏輯 CPU 數目，以及虛擬機器上安裝的客體作業系統類型。
每個插槽的核心數	為 vApp 中每個虛擬機器輸入每個插槽的核心數。 您可以根據核心和每個插槽核心數設定虛擬 CPU 的指派方式。依據您要使用單核心 CPU、雙核心 CPU、三核心 CPU 等因素，判定虛擬機器需要多少 CPU 核心，然後選取應指派給每個插槽的核心數目。
核心數目	檢視 vApp 中每個虛擬機器的核心數目。 當您更新虛擬 CPU 數目時，該數目會有所變更。
記憶體總計 (MB)	輸入 vApp 中每個虛擬機器的記憶體 (以 MB 為單位)。 此設定會決定配置給虛擬機器的 ESXi 主機記憶體數量。虛擬硬體記憶體大小將決定在虛擬機器中執行的應用程式可使用的記憶體大小。虛擬機器無法獲得多於其已設定虛擬硬體記憶體大小的記憶體資源。

12 在 [即將完成] 頁面上，檢閱設定，然後按一下**完成**。

結果

新的 vApp 會顯示在卡視圖中。

從目錄新增 vApp

如果您擁有目錄的存取權，則可以使用目錄中的 vApp 範本來建立 vApp。

vApp 範本可以基於 OVF 檔案，其中包含用於自訂 vApp 虛擬機器的內容。vApp 會繼承這些內容。如果其中任一個內容可供使用者設定，則您可以指定其值。

必要條件

- 若要存取公用目錄中的 vApp 範本，請確認您是**組織管理員**或 **vApp 作者**。

- 若要存取與您共用的組織目錄中的 vApp 範本，請確認您至少是 **vApp 使用者**。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下**新增**，然後選取**從目錄新增 vApp**。

3 選取要匯入的範本，然後按**下一步**。

4 輸入 vApp 的名稱，並選擇性地輸入其說明。

5 輸入 vApp 的執行階段租用和儲存區租用，然後按**下一步**。

6 在**儲存區原則**下拉式功能表中，選取 vApp 中每個虛擬機器的儲存區原則，然後按**下一步**。

7 如果 vApp 中虛擬機器的放置原則和大小調整原則可進行設定，請從下拉式功能表中為每個虛擬機器選取一個原則。

8 如果 vApp 中虛擬機器的計算內容可進行設定，請自訂這些內容，然後按**下一步**。

選項	描述
虛擬 CPU	輸入 vApp 中每個虛擬機器的虛擬 CPU 數目。 可以指派給虛擬機器的虛擬 CPU 的數目上限，取決於主機上的邏輯 CPU 數目，以及虛擬機器上安裝的客體作業系統類型。
每個插槽的核心數	為 vApp 中每個虛擬機器輸入每個插槽的核心數。 您可以根據核心和每個插槽核心數設定虛擬 CPU 的指派方式。依據您要使用單核心 CPU、雙核心 CPU、三核心 CPU 等因素，判定虛擬機器需要多少 CPU 核心，然後選取應指派給每個插槽的核心數目。
核心數目	檢視 vApp 中每個虛擬機器的核心數目。 當您更新虛擬 CPU 數目時，該數目會有所變更。
記憶體	輸入 vApp 中每個虛擬機器的記憶體 (以 MB 為單位)。 此設定會決定配置給虛擬機器的 ESXi 主機記憶體數量。虛擬硬體記憶體大小將決定在虛擬機器中執行的應用程式可使用的記憶體大小。虛擬機器無法獲得多於其已設定虛擬硬體記憶體大小的記憶體資源。

9 如果 vApp 中虛擬機器的硬體內容可進行設定，請自訂虛擬機器硬碟大小，然後按**下一步**。

10 如果 vApp 中虛擬機器的網路內容可進行設定，請自訂這些內容，然後按**下一步**。

   a 在**設定網路**頁面上，選取每個虛擬機器連線的網路。

   b (選擇性) 選取此核取方塊以切換至進階網路工作流程，並針對 vApp 中的虛擬機器設定其他網路設定。

11 檢閱 vApp 設定，然後按一下**完成**。

從 vApp 範本建立 vApp

您可以根據您有權存取的目錄中儲存的 vApp 範本，建立新的 vApp。

如果 vApp 範本是根據 OVF 檔案，而此檔案包括用於自訂其虛擬機器的 OVF 內容，則那些內容會傳遞至 vApp。如果使用者可以設定其中任一個內容，則您可以指定值。

必要條件

- 只有組織管理員及 vApp 作者才能存取公用目錄中的 vApp 範本。
- vApp 使用者及上述的身分可以存取組織目錄中他們共用的 vApp 範本。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在左面板中選取 **vApp 範本**。

範本清單會以網格視圖顯示。

2 按一下要使用的 vApp 範本旁邊的選項按鈕，然後按一下**建立 vApp**。

3 輸入 vApp 的名稱，並選擇性地輸入其說明。

4 指定此 vApp 自動停止前可執行的時間長度 (以小時或天為單位)。

5 指定已停止的 vApp 自動清除前保持可用的時間長度 (以小時或天為單位)。

6 按**下一步**。

7 選取要在其中建立 vApp 的虛擬資料中心。

8 選取儲存區原則。

9 按**下一步**。

10 對於 VMware Cloud Director 10.2.2 及更新版本，設定虛擬機器放置和大小調整原則。

從 10.2.2 版開始，放置原則是全域的，您可以將其發佈到多個提供者 VDC，且 vApp 範本同時包括大小調整和放置原則資訊。

11 選取每個虛擬機器要連線的網路。

- 從**網路**下拉式功能表中，選取每個虛擬機器的網路。
- 您可以選取**切換至進階網路工作流程**核取方塊，然後手動輸入 vApp 中每個虛擬機器的網路設定，例如主要 NIC、網路介面卡類型、網路、IP 指派和 IP 位址設定。

完成精靈後，您可以設定虛擬機器的其他內容。

12 按**下一步**。

13 自訂 vApp 中虛擬機器的硬體，然後按**下一步**。

選項	描述
虛擬 CPU 數目	輸入 vApp 中每個虛擬機器的虛擬 CPU 數目。 可以指派給虛擬機器的虛擬 CPU 的數目上限，取決於主機上的邏輯 CPU 數目，以及虛擬機器上安裝的客體作業系統類型。
每個插槽的核心數	為 vApp 中每個虛擬機器輸入每個插槽的核心數。 您可以根據核心和每個插槽核心數設定虛擬 CPU 的指派方式。依據您要使用單核心 CPU、雙核心 CPU、三核心 CPU 等因素，判定虛擬機器需要多少 CPU 核心，然後選取應指派給每個插槽的核心數目。

選項	描述
核心數目	檢視 vApp 中每個虛擬機器的核心數目。 當您更新虛擬 CPU 數目時，該數目會有所變更。
記憶體總計 (MB)	輸入 vApp 中每個虛擬機器的記憶體 (以 MB 為單位)。 此設定會決定配置給虛擬機器的 ESXi 主機記憶體數量。虛擬硬體記憶體大小將決定在虛擬機器中執行的應用程式可使用的記憶體大小。虛擬機器無法獲得多於其已設定虛擬硬體記憶體大小的記憶體資源。
硬碟內容	輸入虛擬機器硬碟的大小 (以 MB 為單位)。

14 在 [即將完成] 頁面上，檢閱設定，然後按一下**完成**。

結果

新的 vApp 會顯示在卡視圖中。

從 vCenter Server 匯入虛擬機器做為 vApp

如果您具有**系統管理員**權限，則可以將 vCenter Server 虛擬機器做為 vApp 匯入至 VMware Cloud Director。

匯入虛擬機器不會保留 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。

必要條件

若要從 vCenter Server 查看和匯入虛擬機器，請確認您具有**系統管理員**權限。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下**新增**，然後選取**從 vCenter 匯入**。

3 從下拉式功能表中，選取要從中匯入虛擬機器的 vCenter Server 執行個體。

4 請選取要匯入的虛擬機器。

5 輸入 vApp 的名稱，並選擇性地輸入其說明。

6 從下拉式功能表中，選取要在其中儲存和執行 vApp 的虛擬資料中心。

7 (選擇性) 從下拉式功能表中，選取 vApp 的儲存區原則。

8 (選擇性) 若要刪除來源虛擬機器，請開啟**移動虛擬機器**選項。

9 按一下**匯入**。

在 vApps 上執行電源作業

您可以在 vApp 上執行電源作業，例如開啟或關閉 vApp 的電源、暫停或重設 vApp。

開啟 vApp 電源

開啟 vApp 電源會將 vApp 中尚未開啟電源的所有虛擬機器電源開啟。

必要條件

您至少是 vApp 作者。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下 ，以在卡視圖中檢視 vApp。

3 從要開啟電源的 vApp 的**動作**功能表中，選取**開啟電源**。

結果

vApp 即會開啟電源。

關閉 vApp 電源

關閉 vApp 電源，會將 vApp 中的所有虛擬機器關閉電源。若要執行某些動作，例如將 vApp 新增至目錄、複製 vApp 或將其移至其他 VDC，必須先關閉 vApp 的電源。

必要條件

必須啟動 vApp。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下 ，以在卡視圖中檢視 vApp。

3 從要停止的 vApp 的**動作**功能表中，選取**關閉電源**。

4 按一下**確定**。

結果

vApp 中的所有虛擬機器和 vApp 本身均已關閉電源。

重設 vApp

重設 vApp 會清除狀態 (記憶體、快取等)，但 vApp 仍會繼續執行。

必要條件

已啟動您的 vApp，並已開啟其中的虛擬機器的電源。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下  ，以在卡視圖中檢視 vApp。

3 從要重設的 vApp 的**動作**功能表中，選取**重設**。

結果

狀態即會清除，而 vApp 仍繼續執行。

暫停 vApp

暫停 vApp 時，會透過將記憶體寫入磁碟來保留其目前狀態。

必要條件

vApp 執行中。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下  ，以在卡視圖中檢視 vApp。

3 從要暫停的 vApp 的**動作**功能表中，選取**暫停**。

結果

此時會暫停 vApp，並保留其狀態。

捨棄 vApp 的暫停狀態

如果 vApp 處於暫停狀態，並且您不再需要繼續使用 vApp，則可以捨棄暫停狀態。捨棄暫停狀態會移除儲存的記憶體，並將 vApp 恢復為已關閉電源狀態。

必要條件

vApp 必須處於暫停狀態。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下  ，以在卡視圖中檢視 vApp。

3 從暫停的 vApp 的**動作**功能表中，選取**捨棄暫停狀態**。

結果

狀態已捨棄，並且 vApp 的電源已關閉。

開啟多個 vApp 的電源

您可以同時開啟多個 vApp 的電源。此動作會將 vApp 中尚未開啟電源的所有虛擬機器開啟電源。

必要條件

確認您至少是 **vApp 作者**。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 開啟**多重選取**選項。

3 選取您要開啟電源的 vApp。

4 從**動作**功能表中，選取**開啟電源**。

5 按一下**確定**以進行確認。

關閉多個 vApp 的電源

您可以同時關閉多個 vApp 的電源。此動作會將 vApp 中的所有虛擬機器關閉電源。若要執行某些動作，例如將 vApp 新增至目錄、複製 vApp 或將其移至其他虛擬資料中心，必須先關閉 vApp 的電源。

必要條件

- 確認 vApp 已啟動。
- 確認您至少是 **vApp 作者**。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 開啟**多重選取**選項。

3 選取您要關閉電源的 vApp。

4 從**動作**功能表中，選取**關閉電源**。

5 按一下**確定**以進行確認。

捨棄多個 vApp 的暫停狀態

如果多個 vApp 處於暫停狀態，並且您不再需要繼續使用，則可以同時捨棄這些 vApp 的暫停狀態。捨棄暫停狀態會移除儲存的記憶體，並將 vApp 恢復為已關閉電源狀態。

必要條件

- 確認 vApp 處於暫停狀態。
- 確認您至少是 **vApp 作者**。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 開啟**多重選取**選項。

3 選取您要關閉電源的已暫停 vApp。

4 從**動作**功能表中，選取**捨棄暫停狀態**。

結果

vApp 已關閉電源。

重設多個 vApp

同時重設多個 vApp 會清除其狀態 (包括記憶體、快取等)，但 vApp 仍會繼續執行。

必要條件

- 確認 vApp 已啟動，並且其中的虛擬機器已開啟電源。
- 確認您至少是 **vApp 作者**。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。
2 開啟**多重選取**選項。
3 選取您想要重設的 vApp。
4 從**動作**功能表中，選取**重設**，然後按一下**確定**以進行確認。

結果

每個 vApp 的狀態即會清除，而 vApp 仍繼續執行。

暫停多個 vApp

同時暫停多個 vApp 時，會透過將記憶體寫入磁碟來保留其目前狀態。

必要條件

確認 vApp 正在執行中。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。
2 開啟**多重選取**選項。
3 選取要暫停的 vApp。
4 從要暫停的 vApp 的**動作**功能表中，選取**暫停**，然後按一下**確定**以進行確認。

結果

此時會暫停 vApp，並保留其狀態。

開啟 vApp

您可以開啟 vApp，檢視所含的虛擬機器和網路。此外，還可以檢視顯示虛擬機器和網路連線情況的圖表。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下  ，以在卡視圖中檢視 vApp。

在卡視圖中，您可以查看每個 vApp 的一般資訊，例如名稱、電源狀態、租用資訊、建立日期、擁有者、與 vApp 相關聯的虛擬機器數目、CPU 總數、儲存區和記憶體總計以及相關網路。

3 若要檢視所選 vApp 的詳細設定，請按一下 vApp 卡上的**詳細資訊**。

編輯 vApp 屬性

您可以編輯現有 vApp 的內容，包括 vApp 名稱和說明、租用設定、vApp 中虛擬機器的啟動順序、共用設定和網路設定。

編輯 vApp 的一般內容

您可以檢閱和變更 vApp 的名稱、描述和其他一般內容。

必要條件

請確認 vApp 已關閉電源。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下  ，以在卡視圖中檢視 vApp。

3 在所選 vApp 的卡中，按一下**詳細資料**以檢視和編輯 vApp 內容。

4 視需要檢閱和變更內容，然後按一下**儲存**。

選項	動作
名稱	輸入 vApp 的新名稱。
描述	輸入 vApp 的選擇性描述。
虛擬資料中心	vApp 所屬資料中心的名稱。

選項	動作
快照	如果存在快照，會顯示其詳細資料。
租用	選取**更新**來更新租用。 a 排程執行階段租用的時數或天數。 定義 vApp 在自動停止之前可以執行的時間長度。 b 排程儲存區租用的時數或天數。 定義 vApp 自動刪除前保持可用的時間長度。

結果

將會儲存一般設定。

編輯 vApp 中虛擬機器的啟動和停止順序

您可以設定在 vApp 內啟動和停止虛擬機器的順序。如果虛擬機器中已安裝的應用程式必須按照特定順序啟動和停止，請設定啟動和停止順序。

如果您需要以特定順序啟動和停止虛擬機器，這些設定會非常有用。例如，一個虛擬機器容納資料庫伺服器，另一個容納應用程式伺服器，最後一個容納 Web 伺服器。為了讓相關功能正常運作，必須先啟動資料庫伺服器，接著啟動應用程式伺服器，最後啟動 Web 伺服器。

必要條件

請確認 vApp 已關閉電源。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下  ，以在卡視圖中檢視 vApp。

3 在所選 vApp 的卡中，按一下**詳細資料**。

4 按一下**啟動和停止順序**索引標籤，然後按一下**編輯**。

5 編輯每個虛擬機器的啟動和停止順序內容，然後按一下**確定**。

選項	動作
啟動順序	輸入要啟動虛擬機器的順序。必須依序輸入每個機器的值。
啟動動作	選取啟動動作。 啟動動作將決定啟動含有虛擬機器的 vApp 時該虛擬機器所執行的動作。此選項預設是設定為**開啟電源**。
啟動等候	輸入啟動等候時間。 啟動等候時間是 VMware Cloud Director 依序啟動下一個機器之前要等候的時間 (以秒為單位)。

選項	動作
停止動作	選取停止動作。 停止動作是停止含有虛擬機器的 vApp 時該虛擬機器所執行的動作。如果選取**關閉電源**，虛擬機器將關閉電源而不執行關閉動作以確保穩定性 (相當於從插座拔下插頭)。如果您未安裝 VMware Tools，請選取此動作。否則，請選取**關閉**，以確保關閉時的穩定性。
停止等候	輸入停止等候時間。 停止等候時間是 VMware Cloud Director 依序關閉下一個虛擬機器之前要等候的時間 (以秒為單位)。

編輯 vApp 的客體內容

如果 vApp 包括使用者可設定的 OVF 內容，您可以檢閱和修改這些內容。

如果 vApp 中的虛擬機器包括同名的使用者可設定內容值，則會優先採用虛擬機器值。

必要條件

確認 vApp 已停止，並且其客體內容可供使用者設定。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取**虛擬機器**。

2 按一下 以檢視卡視圖中的清單，並選擇性地從**排序依據**下拉式功能表排列虛擬機器清單。

3 在您要編輯的虛擬機器卡中，按一下**詳細資料**。

4 按一下**客體內容**，然後按一下**編輯**。

5 修改 vApp 的客體內容，然後按一下**確定**。

共用 vApp

您可以與組織中的其他群組或使用者共用 vApp。您設定的存取控制會決定可在共用 vApp 上完成的作業。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下 ，以在卡視圖中檢視 vApp。

3 在所選 vApp 的卡中，按一下**詳細資料**並向下捲動至 vApp 的共用內容。

4 選取您想要共用 vApp 的使用者，然後按一下**儲存**。

選項	動作
與組織中的所有人共用	選取此選項可與組織中的所有使用者共用，然後選取存取層級。 ■ 若要授與完全控制權，請選取**完全控制**。 組織中的所有使用者都可以開啟和啟動 vApp、將 vApp 儲存為 vApp 範本、將範本新增至目錄、變更 vApp 的擁有者、複製至目錄，以及修改內容。 ■ 若要授與唯讀存取權，請選取**唯讀**。
與特定的使用者和群組共用	選取此選項可僅與您指定的使用者共用。 a 從**不具有存取權的使用者和群組**面板中選取名稱，以將其移至**具有存取權的使用者和群組**面板。 b 選取指定的使用者和群組的存取層級。 ■ 若要授與完全控制權，請選取**完全控制**。 具有完全控制權的使用者可以開啟和啟動 vApp、將 vApp 儲存為 vApp 範本、將範本新增至目錄、變更 vApp 的擁有者、複製至目錄，以及修改內容。 ■ 若要授與唯讀存取權，請選取**唯讀**。

結果

您的 vApp 已與指定的使用者或群組共用。

顯示 vApp 網路圖表

透過 vApp 網路圖表，您可以圖形形式檢視 vApp 中的虛擬機器及網路。

必要條件

若要檢視 vApp 網路圖表，您的 vApp 必須包含 40 個以下虛擬機器。如果 vApp 包含超過 40 個虛擬機器，該圖表便無法使用。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下  ，以在卡視圖中檢視 vApp。

3 在所選 vApp 的卡中，按一下**詳細資料**。

4 按一下**網路圖表**索引標籤。

此時會顯示一張圖表，指示 vApp 中的虛擬機器與網路是如何連線的。星號代表主要 NIC。如果 NIC 已連線，則星號為綠色，如果 NIC 未連線，則星號為白色。

5 (選擇性) 若要反白顯示連線的虛擬機器和網路，請按一下網路或虛擬機器。

已連線的物件和這些物件之間的連線會反白顯示。

後續步驟

在此頁面中，您可以新增虛擬機器或網路。

在 vApp 中使用網路

vApp 中的虛擬機器可以連線至 vApp 網路 (隔離或路由) 和組織虛擬資料中心網路 (直接或已納入範圍)。您可以將不同類型的網路新增至 vApp，以處理多個網路案例。

vApp 中的虛擬機器可以連線至 vApp 中的可用網路。如果您想要將虛擬機器連線至不同網路，則必須先將它新增至 vApp。

vApp 可以包括 vApp 網路和組織虛擬資料中心網路。vApp 網路可以是隔離或路由網路。隔離的 vApp 網路包含在 vApp 內。您也可以將 vApp 網路路由至組織虛擬資料中心網路，以提供與 vApp 外部的虛擬機器的連線。針對路由的 vApp 網路，您可以設定網路服務 (如防火牆和靜態路由)。

備註 NSX Data Center for vSphere 所支援的組織 VDC 支援路由、隔離和直接 vApp 網路。

NSX-T Data Center 所支援的組織 VDC 支援隔離和直接 vApp 網路。

您可以將 vApp 直接連線至組織虛擬資料中心網路。如果您有多個 vApp 包含連線至相同組織虛擬資料中心網路的相同虛擬機器，而且想要同時啟動 vApp，則可以將 vApp 納入範圍。將 vApp 納入範圍可讓您隔離虛擬機器的 MAC 和 IP 位址，以開啟其電源，而不發生衝突。

您新增至 vApp 的網路會使用與您在其中建立 vApp 之組織虛擬資料中心相關聯的網路集區。

檢視 vApp 網路

您可以存取和檢視 vApp 中的網路。

必要條件

程序

1. 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。
2. 按一下  ，以在卡視圖中檢視 vApp。
3. 在所選 vApp 的卡中，按一下**詳細資料**。
4. 按一下**網路**索引標籤。

   此時將顯示網路清單 (如有)。您可以檢視每個網路的相關資訊，例如名稱、閘道、網路遮罩、連線，並保留 IP 和 NAT 資源。

5. (選擇性) 若要編輯需查看的資料行，請按一下**網格編輯器**圖示 ()，然後分別選取或取消選取要顯示或隱藏資料行的核取方塊。

將 vApp 網路納入範圍

將不同 vApp 中包含的相同虛擬機器開啟電源可能會導致衝突。 若要允許將不同 vApp 中的相同虛擬機器開啟電源而不發生衝突，您必須將 vApp 納入範圍。

將 vApp 納入範圍會隔離虛擬機器的 MAC 和 IP 位址，並且將組織 VDC 網路的連線類型從「直接」變更為「已納入範圍」。在已納入範圍的網路上，防火牆會自動啟用並設定，以便僅允許傳出流量。將 vApp 納入範圍時，您也可以在納入範圍的網路上設定 NAT 和防火牆規則。

必要條件

- 您只能將直接 vApp 網路納入範圍。如果 vApp 使用多個網路而其他網路是路由網路 (舉例來說)，則僅將直接網路納入範圍。
- 必須停止 vApp 中使用直接網路的虛擬機器，以確保直接 vApp 網路目前未在使用。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下  ，以在卡視圖中檢視 vApp。

3 在所選 vApp 的卡中，按一下**詳細資料**。

4 按一下**網路**索引標籤。

5 如果 vApp 未納入範圍，請按一下**編輯**按鈕。

6 開啟**圍牆 vApp** 選項，然後按一下**確定**。

結果

虛擬機器的 IP 和 MAC 位址變為隔離。您可以將不同 vApp 中的相同虛擬機器開啟電源而不發生衝突。

新增網路至 vApp

新增網路至 vApp，使 vApp 中的虛擬機器可以使用該網路。您可以將 vApp 網路或組織虛擬資料中心網路新增至 vApp。

連線可以是直接或已納入範圍。圍牆會隔離虛擬機器的 MAC 和 IP 位址，讓不同 vApp 中的相同虛擬機器同時開啟而不衝突。

納入範圍功能啟用且啟動 vApp 時，會從組織虛擬資料中心的網路集區建立隔離的網路。系統會建立 Edge 閘道並連結至隔離網路以及組織虛擬資料中心網路。進入和離開虛擬機器的流量都會通過 Edge 閘道，此閘道會使用 NAT 與 Proxy-AR 轉譯 IP 位址。如此一來，路由器便可使用相同的 IP 空間在兩個網路間傳遞流量。

必要條件

若要新增組織虛擬資料中心網路，您的管理員必須已建立此類網路。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下  ，以在卡視圖中檢視 vApp。

3 在所選 vApp 的卡中，按一下**動作**，然後選取**新增網路**。

4 選取要新增的網路類型。

選項	動作
組織 VDC 網路	從可用網路清單中選取組織虛擬資料中心網路。
vApp 網路	a 輸入網路的名稱，並選擇性地輸入其說明。 b 輸入網路閘道 CIDR。 c (選擇性) 輸入主要和次要 DNS 以及 DNS 尾碼。 d (選擇性) 選取是否允許客體 VLAN。 e (選擇性) 輸入靜態 IP 集區設定，例如 IP 範圍。 f (選擇性) 若要連線至組織虛擬資料中心網路，請開啟**連線至組織 VDC 網路**選項，然後從清單中選取網路。

5 按一下**新增**。

結果

網路會新增至 vApp。

後續步驟

將 vApp 中的虛擬機器連線至網路。

設定 vApp 網路的網路服務

您可以為特定的 vApp 網路設定網路服務，例如 DHCP、防火牆、網路位址轉譯 (NAT) 及靜態路由。

可用的網路服務取決於 vApp 網路的類型。

表 3-1. 可用的網路服務 (依網路類型排序)

vApp 網路類型	DHCP	防火牆	NAT	靜態路由
直接				
路由	X	X	X	X
隔離	X			

備註 NSX Data Center for vSphere 所支援的組織 VDC 支援路由、隔離和直接 vApp 網路。

NSX-T Data Center 所支援的組織 VDC 支援隔離和直接 vApp 網路。

檢視和編輯一般網路詳細資料

您可以檢視和編輯一般 vApp 網路詳細資料，例如網路名稱和說明。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下  ，以在卡視圖中檢視 vApp。

3 在所選 vApp 的卡中，按一下**詳細資料**。

4 在**網路**索引標籤上，按一下網路以檢視網路詳細資料。

5 在**一般**索引標籤中，檢閱網路資訊。

6 按一下**編輯**。

7 編輯 vApp 網路名稱和說明。

8 按一下**儲存**。

編輯 vApp 網路的靜態 IP 集區設定

您可以設定 vApp 網路，或透過從 IP 位址的靜態集區中擷取靜態 IP 位址將其提供給 vApp 中的虛擬機器。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下  ，以在卡視圖中檢視 vApp。

3 在所選 vApp 的卡中，按一下**詳細資料**。

4 在**網路**索引標籤上，按一下網路以檢視網路詳細資料。

5 在 **IP 管理**索引標籤上，按一下**靜態集區**。

6 按一下**編輯**。

7 輸入 IP 範圍，然後按一下**新增**。

8 按一下**儲存**。

編輯 vApp 網路的 DNS 設定

建立 vApp 網路後，您可以隨時檢視和編輯 DNS 設定。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下  ，以在卡視圖中檢視 vApp。

3 在所選 vApp 的卡中，按一下**詳細資料**。

4 在**網路**索引標籤上，按一下網路以檢視網路詳細資料。

5 在 **IP 管理**索引標籤上，按一下 **DNS**。

此時會顯示 DNS 設定。

6 按一下**編輯**。

7 編輯主要和次要 DNS 以及 DNS 尾碼。

8 按一下**儲存**。

設定 vApp 網路的 DHCP

您可以設定特定的 vApp 網路，以提供 DHCP 服務給 vApp 中的虛擬機器。

為 vApp 網路啟用 DHCP 後，將 vApp 中的虛擬機器上的 NIC 連線至該網路，並選取 DHCP 做為該 NIC 的 IP 模式。VMware Cloud Director 會在虛擬機器開啟電源時為其指派 DHCP IP 位址。

必要條件

- 確認 vApp 網路已路由或已隔離。
- 確認 vApp 位於受 NSX Data Center for vSphere 支援的組織虛擬資料中心內。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下  ，以在卡視圖中檢視 vApp。

3 在所選 vApp 的卡中，按一下**詳細資料**。

4 在**網路**索引標籤上，按一下網路以檢視網路詳細資料。

5 在 **IP 管理**索引標籤上，按一下 **DHCP**。

此時會顯示 DHCP 狀態。

6 按一下**編輯**。

7 按一下**已啟用**。

8 在 **IP 集區**文字方塊中，輸入 IP 位址範圍。

VMware Cloud Director 會使用這些位址以滿足 DHCP 要求。DHCP IP 位址的範圍不能與 vApp 網路的靜態 IP 集區重疊。

9 設定預設租用時間和租用時間上限 (以秒為單位)。

10 按一下**儲存**。

顯示 vApp 網路的 IP 配置

您可以檢閱 vApp 中網路的 IP 配置。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下  ，以在卡視圖中檢視 vApp。

3 在所選 vApp 的卡中，按一下**詳細資料**。

4 在**網路**索引標籤上，按一下網路以檢視網路詳細資料。

5 在 **IP 管理**索引標籤上，按一下 **IP 配置**。

此時會顯示已配置的 IP 位址。

設定 vApp 網路的靜態路由

您可以設定特定 vApp 網路，以提供允許不同 vApp 網路上的虛擬機器進行通訊的靜態路由服務。

系統會自動啟用您建立的任何靜態路由。

必要條件

路由 vApp 網路。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下  ，以在卡視圖中檢視 vApp。

3 在所選 vApp 的卡中，按一下**詳細資料**。

4 在**網路**索引標籤上，按一下網路以檢視網路詳細資料。

5 在**路由**索引標籤上，按一下**編輯**。

您可以對網路啟用或停用靜態路由。

新增 vApp 網路的靜態路由

您可以在兩個路由至同一個組織虛擬資料中心網路的 vApp 網路之間新增靜態路由。靜態路由允許網路之間的流量。

您無法新增靜態路由至已納入範圍的 vApp，也無法在重疊網路之間新增它。在新增靜態路由至 vApp 網路之後，請設定網路防火牆規則，以允許靜態路由上的流量。若為採用靜態路由的 vApp，請選取以使用指派的 IP 位址，直到將 vApp 或相關聯的網路刪除為止。

靜態路由只在包含路由的 vApp 執行時才會運作。如果您變更 vApp 的上層網路、刪除 vApp 或刪除 vApp 網路，並且 vApp 包括靜態路由，則那些路由無法運作，且您必須手動移除它們。

必要條件

- 兩個 vApp 網路皆路由至同一個組織虛擬資料中心網路。
- vApp 網路位於至少啟動過一次的 vApp 中。
- 靜態路由已在兩個 vApp 網路上啟用。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下  ，以在卡視圖中檢視 vApp。

3 在所選 vApp 的卡中，按一下**詳細資料**。

4 在**網路**索引標籤上，按一下網路以檢視網路詳細資料。

5 在**路由**索引標籤的 [靜態路由] 下，按一下**新增**。

此時會顯示已配置的 IP 位址。

6 輸入靜態路由的名稱。

7 以 CIDR 格式輸入網路位址。

網路位址是針對要新增靜態路由的 vApp 網路。

8 輸入下一個躍點 IP 位址。

下一個躍點 IP 位址為該 vApp 網路路由器的外部 IP 位址。

9 按一下**儲存**。

10 對第二個 vApp 網路重複相同的程序。

範例： 靜態路由範例

vApp 網路 1 和 vApp 網路 2 皆路由至共用組織網路。您可以在每一個 vApp 網路上建立靜態路由，以允許網路之間的流量。您可以使用 vApp 網路的相關資訊建立靜態路由。

表 3-2. 網路資訊

網路名稱	網路規格	路由器外部 IP 位址
vApp 網路 1	192.168.1.0/24	192.168.0.100
vApp 網路 2	192.168.2.0/24	192.168.0.101
共用組織網路	192.168.0.0/24	無

在 vApp 網路 1 上，建立 vApp 網路 2 的靜態路由。在 vApp 網路 2 上，建立 vApp 網路 1 的靜態路由。

表 3-3. 靜態路由設定

vApp 網路	路由名稱	網路	下一個躍點 IP 位址
vApp 網路 1	tovapp2	192.168.2.0/24	192.168.0.101
vApp 網路 2	tovapp1	192.168.1.0/24	192.168.0.100

新增連接埠轉送規則至 vApp 網路

您可以新增 NAT 對應規則，設定特定的 vApp 網路，以提供連接埠轉送。

連接埠轉送會對 vApp 網路上執行於虛擬機器的服務提供外部存取。

當您設定連接埠轉送時，VMware Cloud Director 會將外部連接埠對應至虛擬機器上執行的專用於輸入流量的服務。

當您將連接埠轉送規則新增至 vApp 網路時，它會出現在 NAT 對應規則清單的底端。如需如何設定連接埠轉送規則強制執行順序的相關資訊，請參閱

必要條件

- 確認 vApp 網路已路由。
- 確認 vApp 網路上的防火牆已啟用。如果停用防火牆，NAT 對應規則將不再套用至 vApp 網路。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下  ，以在卡視圖中檢視 vApp。

3 在所選 vApp 的卡中，按一下**詳細資料**。

4 在**網路**索引標籤上，按一下網路以檢視網路詳細資料。

5 按一下**服務**，然後按一下**編輯**。

6 若要啟用 NAT，請開啟 NAT 選項。

7 從 **NAT 類型**下拉式功能表中，選取**連接埠轉送**，然後按一下**新增**。

8 (選擇性) 若要啟用 IP 偽裝，請選取此核取方塊。

9 設定連接埠轉送規則。

   a 選取外部連接埠。

   b 選取要轉送到的連接埠。

   c 選取虛擬機器介面。

   d 選取要轉送之流量類型的通訊協定。

10 按一下**儲存**。

後續步驟

如有必要，請使用**上移**或**下移**按鈕重新排列連接埠轉送規則。

新增 IP 轉譯規則至 vApp 網路

您可以透過新增 NAT 對應規則設定特定的 vApp 網路，以提供 IP 轉譯。

當您建立網路的 IP 轉譯規則時，vCloud Director 會將 DNAT 和 SNAT 規則新增至與該網路的連接埠群組相關聯的 Edge 閘道。DNAT 規則會將外部 IP 位址轉譯為傳入流量的內部 IP 位址。SNAT 規則會將內部 IP 位址轉譯為傳出流量的外部 IP 位址。

必要條件

- 確認 vApp 網路已路由。

- 確認 vApp 網路上的防火牆已啟用。如果停用防火牆，NAT 對應規則將不再套用至 vApp 網路。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下  ，以在卡視圖中檢視 vApp。

3 在所選 vApp 的卡中，按一下**詳細資料**。

4 在**網路**索引標籤上，按一下網路以檢視網路詳細資料。

5 按一下**服務**，然後按一下**編輯**。

6 若要啟用 NAT，請開啟 NAT 選項。

7 從 **NAT 類型**下拉式功能表中，選取 **IP 轉譯**，然後按一下**新增**。

8 選取虛擬機器介面，然後按一下**保留**。

9 選取對應模式。

10 如果已選取**手動**對應模式，則輸入外部 IP 位址。

11 按一下**儲存**。

後續步驟

如有必要，請使用**上移**或**下移**按鈕重新排列 IP 轉譯規則。

刪除 vApp 網路

如果您在 vApp 中不再需要網路，則可以刪除網路。

必要條件

vApp 已停止，而且 vApp 中沒有虛擬機器連線至網路。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下  ，以在卡視圖中檢視 vApp。

3 在所選 vApp 的卡中，按一下**詳細資料**。

4 在**網路**索引標籤上，選取要刪除的網路，按一下**刪除**，然後確認刪除。

使用快照

建立快照會保留 vApp 內的虛擬機器在特定時間點的狀態和資料。快照不適用於長時間使用或取代備份 vApp。

您可能想要在升級 vApp 中的虛擬機器時使用快照。例如，升級虛擬機器之前，您可以建立快照以保留升級前的時間點。若要執行此操作，請在升級之前儲存快照，然後再執行升級。如果在升級期間未發生任何問題，您可以選擇移除快照，這會認可升級期間所做的變更。但是，如果您遇到問題，您可以還原快照，這樣便會回到升級前已儲存的 vApp 狀態。

建立 vApp 快照

透過建立 vApp 的快照，會建立此 vApp 中所有虛擬機器的快照。建立快照後，您可以將 vApp 中的所有虛擬機器還原為快照，或是移除您不需要的快照。

vApp 快照有某些限制。

- vApp 快照不會擷取 NIC 組態。
- 如果 vApp 中的任何虛擬機器連線至具名磁碟，則無法建立 vApp 快照。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下  ，以在卡視圖中檢視 vApp。

3 從您要建立快照的 vApp 的**動作**功能表中，選取**建立快照**。

建立 vApp 的快照將會取代現有的快照 (如有)。

4 (選擇性) 選取是否要建立 vApp 記憶體的快照。

擷取 vApp 記憶體狀態時，快照會保留 vApp 以及 vApp 中的虛擬機器的即時狀態。記憶體快照可建立某一精確時間點的快照 (例如，升級仍在運作的軟體)。建立記憶體快照後，如果升級未如預期完成，或軟體不符合您的預期，可將虛擬機器還原到先前的狀態。

擷取記憶體狀態時，無需靜止 vApp 的檔案。如果未擷取記憶體狀態，則快照不會儲存 vApp 的即時狀態，除非靜止磁碟，否則磁碟就是當機一致的。

5 (選擇性) 選取是否要靜止客體檔案系統。

此作業要求在 vApp 中的虛擬機器上安裝 VMware Tools。當您靜止虛擬機器時，VMware Tools 會靜止虛擬機器的檔案系統。靜止作業可確認快照磁碟代表客體檔案系統的一致狀態。已靜止的快照適用於自動備份或定期備份。例如，如果無法感知虛擬機器的活動，但希望還原為多個最近備份，則可以靜止檔案。

您無法靜止包含大容量磁碟的 vApp。

6 按一下**確定**。

結果

vApp 的快照即會建立。

後續步驟

您可以將 vApp 中的所有虛擬機器還原為最新快照。

還原 vApp 至快照

您可以將 vApp 內的所有虛擬機器還原到建立 vApp 快照時的當時狀態。

必要條件

確認 vApp 具有現有快照。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下  ，以在卡視圖中檢視 vApp。

3 從要還原的 vApp 的**動作**功能表中，選取**還原至快照**。

4 按一下**確定**。

結果

vApp 中的所有虛擬機器即會還原為快照狀態。

移除 vApp 快照

您可以移除 vApp 的快照。

移除 vApp 快照時，會刪除 vApp 快照中虛擬機器的狀態，且無法再回到該狀態。移除快照不會影響 vApp 的目前狀態。

必要條件

您已建立 vApp 的快照。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下  ，以在卡視圖中檢視 vApp。

3 從要移除快照的 vApp 的**動作**功能表中，選取**移除快照**。

4 按一下**確定**。

結果

快照即會移除。

建立多個 vApp 的快照

透過建立多個 vApp 的快照，會建立此 vApp 中所有虛擬機器的快照。建立快照後，您可以將 vApp 中的所有虛擬機器還原為快照，或是移除您不需要的快照。

vApp 快照有某些限制。

- vApp 快照不會擷取 NIC 組態。

- 如果 vApp 中的任何虛擬機器連線至具名磁碟，則無法建立 vApp 快照。
- 建立多個 vApp 的快照不會建立 vApp 記憶體的快照，也不會靜止 vApp 的客體檔案系統。如果您想要建立 vApp 記憶體的快照或靜止客體檔案系統，則必須為每個 vApp 單獨建立快照。請參閱建立 vApp 快照。

程序

1. 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。
2. 開啟**多重選取**選項。
3. 選取您想要建立快照的 vApp。
4. 從**動作**功能表中，選取**建立快照**，然後按一下**確定**以進行確認。

後續步驟

- 您可以將 vApp 中的所有虛擬機器還原為最新快照。請參閱將多個 vApp 還原到快照。
- 您可以移除 vApp 的快照。請參閱移除多個 vApp 的快照。

移除多個 vApp 的快照

如果您不需要多個 vApp 的快照，可以同時將其移除。

移除 vApp 快照時，會刪除 vApp 快照中虛擬機器的狀態，且無法再回到該狀態。移除快照不會影響 vApp 的目前狀態。

程序

1. 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。
2. 開啟**多重選取**選項。
3. 選取要移除其快照的 vApp。
4. 從**動作**功能表中，選取**移除快照**。

將多個 vApp 還原到快照

您可以將多個 vApp 內的所有虛擬機器還原到建立 vApp 快照時其所處的狀態。

必要條件

確認要還原的 vApp 具有現有快照。

程序

1. 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。
2. 開啟**多重選取**選項。
3. 選取您要還原至其最新快照的 vApp。
4. 從**動作**功能表中，選取**還原至快照**。

5 按一下**確定**以進行確認。

變更 vApp 的擁有者

例如，vApp 擁有者離開公司或在公司內變更角色時，您可以變更 vApp 的擁有者。

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 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下  ，以在卡視圖中檢視 vApp。

3 從您要變更其擁有者的 vApp 的**動作**功能表中，選取**變更擁有者**。

4 從清單中選取使用者。

5 按一下**確定**。

結果

vApp 的擁有者即會變更。

將 vApp 移動至另一個虛擬資料中心

當您將 vApp 移動至另一個虛擬資料中心時，會從來源虛擬資料中心移除 vApp。

必要條件

- 您至少是 **vApp 作者**。
- vApp 即會關閉電源。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下  ，以在卡視圖中檢視 vApp。

3 從要移動的 vApp 的**動作**功能表中，選取**移動至**。

4 選取您要移動 vApp 的虛擬資料中心，然後按一下**確定**。

5 (選擇性) 選取儲存區原則。

6 按一下**確定**。

結果

vApp 將從來源資料中心移除並移動至目標資料中心。

將停止的 vApp 複製至另一個虛擬資料中心

當您將 vApp 複製至另一個虛擬資料中心時，原始 vApp 仍會保留在來源虛擬資料中心內。

必要條件

- 您至少是 **vApp 作者**。
- vApp 即會關閉電源。

程序

1. 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。
2. 按一下  ，以在卡視圖中檢視 vApp。
3. 從您要複製的 vApp 的**動作**功能表中，選取**複製至**。
4. 輸入名稱及描述。
5. 選取要在其中建立 vApp 複本的虛擬資料中心。
6. (選擇性) 選取儲存區原則。
7. 按一下**確定**。

結果

vApp 連同提供的名稱和說明一併會複製至指定的虛擬資料中心。

複製已開啟電源的 vApp

若要根據現有 vApp 建立新的 vApp，您可以複製 vApp，並變更複本以使該複本符合您的需求。複製 vApp 之前，不需要關閉 vApp 中的虛擬機器電源。執行中虛擬機器的記憶體狀態會保留在複製的 vApp 中。

必要條件

驗證是否符合下列條件。

- 您至少是 **vApp 使用者**。
- vCenter Server 5.5 或更新版本可支援組織虛擬資料中心。

程序

1. 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。
2. 按一下  ，以在卡視圖中檢視 vApp。
3. 從您要複製的 vApp 的**動作**功能表中，選取**複製至**。
4. 輸入名稱及描述。
5. 選取要在其中建立 vApp 複本的虛擬資料中心。

6 (選擇性) 選取儲存區原則。

7 按一下**確定**。

結果

vApp 的複本隨即建立並處於暫停狀態。複製的 vApp 會啟用，以進行網路納入範圍。

後續步驟

修改新 vApp 的網路內容或開啟 vApp 的電源。

新增虛擬機器至 vApp

您可以新增虛擬機器至 vApp。

必要條件

您必須是**組織管理員**或 **vApp 作者**，才能存取公用目錄中的虛擬機器。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下  ，以在卡視圖中檢視 vApp。

3 從您要向其新增虛擬機器的 vApp 的**動作**功能表中，選取**新增虛擬機器**。

與 vApp 相關聯的虛擬機器清單將會顯示在**新增虛擬機器**視窗中。

4 若要建立新的虛擬機器並使其自動與 vApp 建立關聯，請按一下**新增虛擬機器**。

5 輸入虛擬機器的名稱和電腦名稱。

重要 電腦名稱只能包含英數字元和連字號。電腦名稱不能只包含數字，且不能包含空格。

6 (選擇性) 輸入有意義的說明。

7 選取建立虛擬機器後是否要立即開啟其電源。

8 選取您要部署虛擬機器的方式。

選項	動作
新增	使用可自訂設定部署新的虛擬機器。 a 選取作業系統系列和作業系統。 b (選擇性) 選取開機映像。 c 選取運算原則。 d 選取虛擬機器的大小，或按一下**自訂大小調整選項**手動輸入計算、記憶體和儲存區設定。 預先定義的大小調整選項為小型、中型或大型。 e 指定虛擬機器的儲存區設定，例如儲存區原則和大小 (GB)。 f 指定虛擬機器的網路設定，例如網路、IP 模式、IP 位址和主要 NIC。
從範本	從您從範本目錄選取的範本部署虛擬機器。 a 從目錄中選取虛擬機器範本。 b (選擇性) 選取以使用自訂儲存區原則，然後從**要使用的自訂儲存區原則**中選取原則。 c 若有使用者授權合約，您必須檢閱並接受此合約。

9 按一下**確定**即可建立虛擬機器。

10 按一下**新增**將虛擬機器新增至 vApp。

將 vApp 以 vApp 範本形式儲存至目錄

透過新增 vApp 至目錄，您可以將特定的 vApp 轉換為 vApp 範本。

從 VMware Cloud Director 10.2.2 開始，新增 vApp 至目錄時，vApp 範本會將來源 vApp 的放置和大小調整原則作為不可修改的標籤包括在內。

必要條件

- 此作業需要預先定義之 **vApp 作者**角色中包含的權限或一組同等權限。
- 您的組織必須具有目錄以及含有可用空間的虛擬資料中心。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下  ，以在卡視圖中檢視 vApp。

3 從您要新增至目錄的 vApp 的**動作**功能表中，選取**新增至目錄**。

備註 即使屬於 vApp 的虛擬機器處於執行中狀態，您仍可以新增 vApp 至目錄。但是，如果您選取執行中的 vApp，則其會新增至目錄做為 vApp 範本，並且所有虛擬機器都會處於暫停狀態。

4 從**目錄**下拉式功能表中選取目的地目錄。

5 輸入 vApp 範本的名稱，並選擇性地輸入說明。

6 (選擇性) 如果您想要新目錄項目覆寫任何現有 vApp 範本，請選取**覆寫目錄項目**，然後選取要覆寫的目錄項目。

例如，當您上傳新版 vApp 至目錄時，可能想要覆寫舊版本。

7 指定必須如何使用範本。

根據 vApp 範本建立 vApp 時，會套用此設定。而在使用此範本中的個別虛擬機器建置 vApp 時，則予以忽略。

選項	描述
製作相同複本	從 vApp 範本建立 vApp 時，選取以製作 vApp 的相同複本。
自訂虛擬機器設定	從 vApp 範本建立 vApp 時，選取以啟用虛擬機器設定的自訂。

8 若要完成 vApp 範本建立，請按一下**確定**。

結果

vApp 範本隨即顯示在指定的目錄中。

下載 vApp 作為 OVF 套件

您可以將 vApp 作為 OVF 套件或 OVA (這是相同 OVF 檔案套件的單一檔案散發) 進行下載。

必要條件

- 此作業需要預先定義之 **vApp 作者**角色中包含的權限或一組同等權限。
- 請確認 vApp 已關閉電源且已解除部署。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。

2 按一下  ，以在卡視圖中檢視 vApp。

3 從您要下載的 vApp 的**動作**功能表中，選取**下載**。

4 選取下載 vApp 要採用的格式。

5 (選擇性) 選取**保留身分識別資訊**，以便在下載的 OVF 套件中包含位於 vApp 中的虛擬機器的 UUID 和 MAC 位址。

這會限制套件的可攜性，必須僅在必要時使用。

6 按一下**確定**以確認選取項目並開始下載。

結果

依預設，套件將下載到您瀏覽器的 `Downloads` 資料夾中。

更新 vApp 租用

如果 vApp 的租用已到期或即將到期，您可以更新租用。

必要條件

確認您已獲指派預先定義的 **vApp 使用者**角色或一組同等權限。

程序

1. 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。
2. 選取您想要更新的 vApp。
3. 從**動作**功能表中，選取**更新租用**。
4. 更新 vApp 的執行階段租用。
   a. 選取**執行階段租用**核取方塊。
   b. 從下拉式功能表中，選取執行階段租用的值。

      您可以選取以小時、天為單位的值，或將租用設定為**永不到期**。**系統管理員**可以限制您可選擇的長度上限。
5. 更新 vApp 的儲存區租用。
   a. 選取**儲存區租用**核取方塊。
   b. 從下拉式功能表中，選取儲存區租用的值。

      您可以選取以小時、天為單位的值，或將租用設定為**永不到期**。**系統管理員**可以限制您可選擇的長度上限。

刪除 vApp

您可以刪除 vApp，這會從組織中移除它。

必要條件

您的 vApp 必須停止。

您必須至少是 **vApp 作者**。

程序

1. 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。
2. 選取您想要刪除的 vApp。
3. 從**動作**功能表中，選取**刪除**。
4. 按一下**確定**。

結果

將會刪除此 vApp。

刪除多個 vApp

若要從您的組織移除多個 vApp，可以同時將其刪除。

必要條件

- 確認您的 vApp 已停止。
- 確認您至少是 **vApp 作者**。

程序

1. 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後從左面板中選取 **vApp**。
2. 開啟**多重選取**選項。
3. 選取您想要刪除的 vApp。
4. 從**動作**功能表中，選取**刪除**。
5. 按一下**刪除**以確認。

使用 Kubernetes 叢集

4

可以從現有的組織 VDC 原則建立不同節點大小的 Kubernetes 叢集。

Kubernetes Container Clusters 是適用於 VMware Cloud Director 的 Container Service Extension 外掛程式。可以使用 VMware Cloud Director Tenant Portal 中的 Kubernetes Container Clusters 外掛程式，部署類型為原生和 VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) 叢集的叢集。可以在不使用 Kubernetes Container Clusters 外掛程式的情況下建立 Tanzu Kubernetes 叢集。

在 vSphere 叢集上啟用後，VMware vSphere® with VMware Tanzu™ 提供在專用資源集區中建立上游 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。

當服務提供者建立提供者 VDC Kubernetes 原則並將該原則發佈至組織 VDC 時，他們會建立組織 VDC Kubernetes 原則。您可以使用 Kubernetes Container Clusters 外掛程式，透過套用其中一個組織 VDC Kubernetes 原則來建立 Tanzu Kubernetes 叢集。

Kubernetes 執行階段選項

- Tanzu Kubernetes 叢集 - 您可以使用 vSphere Kubernetes 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。
- 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。
- 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、健全狀況檢查以及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。

本章節討論下列主題：

- 建立 VMware Tanzu Kubernetes Grid Integrated Edition 叢集
- 設定對 Tanzu Kubernetes 叢集中服務的外部存取權

新增組織 VDC Kubernetes 原則

如果您擁有**系統管理員**權限，則可以使用提供者 VDC Kubernetes 原則新增組織 VDC Kubernetes 原則。您可以使用組織 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，您可以透過建立組織 VDC 原則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

- 確認您具有**系統管理員**角色或包含一組同等權限的角色。所有其他角色只能檢視組織 VDC Kubernetes 原則。
- 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 Service Provider Admin Portal 的**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《VMware Cloud Director Service Provider Admin Portal 指南》中的〈使用 VMware Cloud Director 中的 vSphere with Kubernetes〉。
- 確認您已登入 Flex 組織 VDC。
- 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. 在頂部導覽列中，按一下**資料中心**，然後按一下**虛擬資料中心**。
2. 選取組織虛擬資料中心。
3. 在左面板中的**設定**下，選取 **Kubernetes 原則**，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

- 刪除組織 VDC Kubernetes 原則。
- 透過使用 Service Provider Admin Portal，您可以管理組織資源配額。請參閱《VMware Cloud Director Service Provider Admin Portal 指南》中的〈管理組織的資源耗用量配額〉。
- 管理群組的資源配額 或 管理使用者的資源配額

編輯組織 VDC Kubernetes 原則

如果您擁有**系統管理員**權限，則可以修改組織 VDC Kubernetes 原則以變更其說明及 CPU 和記憶體限制。

必要條件

確認您具有**系統管理員**角色或包含一組同等權限的角色。所有其他角色只能檢視組織 VDC Kubernetes 原則。

程序

1 在頂部導覽列中，按一下**資料中心**，然後按一下**虛擬資料中心**。

2 選取組織虛擬資料中心。

3 在左面板中的**設定**下，選取 **Kubernetes 原則**。

4 選取您要編輯的組織 VDC Kubernetes 原則，然後按一下**編輯**。

編輯 VDC Kubernetes 原則精靈隨即顯示。

5 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。

6 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。

7 檢閱新原則詳細資料，然後按一下**儲存**。

後續步驟

- 刪除組織 VDC Kubernetes 原則。
- 透過使用 Service Provider Admin Portal，您可以變更組織資源配額。請參閱《VMware Cloud Director Service Provider Admin Portal 指南》中的〈管理組織的資源耗用量配額〉。
- 變更群組和使用者配額。請參閱 管理群組的資源配額或管理使用者的資源配額。

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，請參閱第 4 章 使用 Kubernetes 叢集。

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

- 確認您的服務提供者已向您的組織發佈 Kubernetes Container Clusters 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。
- 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。
- 確認您的服務提供者已將 **vmware:tkgcluster 權利**權限服務包發佈到您的組織，並授與您建立和修改 Tanzu Kubernetes 叢集的**編輯：Tanzu Kubernetes 客體叢集**權限。為了能夠刪除叢集，您必須擁有**完全控制：Tanzu Kubernetes 客體叢集**權限。
- 確認您的服務提供者已為您建立存取控制清單 (ACL) 項目，其中包含您的存取層級的相關資訊。

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，請參閱第 4 章 使用 Kubernetes 叢集。

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。
- 確認您的服務提供者已完成 Container Service Extension 3.0 伺服器設定，並且已將 Container Service Extension 原生放置原則發佈到組織 VDC。
- 確認您的服務提供者已將 **cse:nativeCluster 權利**權限服務包發佈到您的組織，並授與您建立和修改原生 Kubernetes 叢集的**編輯 CSE:NATIVECLUSTER** 權限。為了能夠刪除叢集，您必須擁有**完全控制 CSE:NATIVECLUSTER** 權限。
- 確認您的服務提供者已為您建立存取控制清單 (ACL) 項目，其中包含您的存取層級的相關資訊。

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，請參閱第 4 章 使用 Kubernetes 叢集。

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。
- 確認您的服務提供者已完成 Container Service Extension 3.0 伺服器設定，並且已將 Container Service Extension TKGI 啟用中繼資料發佈到組織 VDC。
- 確認您具有 **{cse}:PKS DEPLOY RIGHT** 權限。

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。

設定對 Tanzu Kubernetes 叢集中服務的外部存取權

從 VMware Cloud Director 10.2.2 開始，預設只能從建立叢集之相同組織虛擬資料中心內的網路 IP 子網路連線到 Tanzu Kubernetes 叢集。如有必要，您可以手動設定對 Tanzu Kubernetes 叢集中特定服務的外部存取權。

向組織 VDC 發佈 VDC Kubernetes 原則後，將自動在叢集 Edge 閘道上部署防火牆原則，以允許從 VDC 內的授權來源存取該叢集。此外，還會自動向組織 VDC 內的 NSX-T Data Center Edge 閘道新增系統 SNAT 規則，以確保組織 VDC 內的工作負載可連線至叢集 Edge 閘道。

備註 如果組織虛擬資料中心是 NSX-T Data Center 群組的一部分，則資料中心群組內的其他 VDC 無法連線至叢集 Edge 閘道。

除非**系統管理員**從 VDC 刪除 Kubernetes 原則，否則無法移除叢集 Edge 閘道上佈建的防火牆原則以及 NSX-T Data Center Edge 閘道上的 SNAT 規則。

如有必要，您可以手動設定從外部網路存取 Tanzu Kubernetes 叢集中的特定服務。若要執行此操作，您必須在 NSX-T Data Center Edge 閘道上建立 DNAT 規則，以確保來自外部位置的流量會轉送至叢集 Edge 閘道。

必要條件

- 確認您的雲端基礎結構受 vSphere 7.0 Update 1C、7.0 Update 2 或更新版本支援。連絡您的**系統管理員**。
- 確認您是**組織管理員**。
- 確認您的**系統管理員**已在 Tanzu Kubernetes 叢集所在的組織虛擬資料中心內建立 NSX-T Data Center Edge 閘道。
- 確認要用於服務的公用 IP 位址已配置給您要新增 DNAT 規則的 Edge 閘道介面。
- 使用 `kubectl` 命令列工具的 `get services my-service` 命令擷取要公開之服務的外部 IP。

程序

1. 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**索引標籤。
2. 按一下 Edge 閘道，然後在**服務**下，按一下 **NAT**。
3. 若要新增規則，請按一下**新增**。
4. 針對要連線至外部網路的服務設定 DNAT 規則。

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。
狀態	若要在建立時啟用規則，請開啟**狀態**切換按鈕。
介面類型	從下拉式功能表中，選取 [DNAT]。

選項	描述
外部 IP	輸入服務的公用 IP 位址。 您輸入的 IP 位址必須屬於 NSX-T Data Center Edge 閘道的子配置 IP 範圍。
應用程式	將方塊保留空白。
內部 IP	輸入從 Kubernetes 入口集區配置的服務 IP 位址。
內部連接埠	(選擇性) 輸入將輸入流量導向到的連接埠號碼。
記錄	(選擇性) 若要記錄此規則執行的位址轉譯，請開啟**記錄**選項。

5 按一下**儲存**。

後續步驟

如果您要提供從外部網路到發佈為 Kubernetes 服務之其他應用程式的存取權，則必須為每個應用程式設定其他 DNAT 規則。

使用網路

5

為了在多用途雲端環境中提供高度彈性且安全的網路基礎結構，VMware Cloud Director 將使用具有四種網路類別的分層網路架構。這些網路類別包括外部網路、組織虛擬資料中心 (VDC) 網路、資料中心群組網路和 vApp 網路。大多數類型的 VMware Cloud Director 網路需要額外的基礎結構物件，例如 Edge 閘道和網路集區。

外部網路

外部網路會提供可將 VMware Cloud Director 環境中的網路和虛擬機器連線至此環境外部網路的上行介面，例如 VPN、公司內部網路或公用網際網路。

外部網路由單一 vSphere 網路、多個 vSphere 網路或 NSX-T Data Center 第 0 層邏輯路由器提供支援。

只有**系統管理員**可以建立外部網路。如需外部網路的相關資訊，請參閱《VMware Cloud Director Service Provider Admin Portal 指南》。

網路集區

網路集區是隔離的第 2 層網路區段的集合，可用來按需建立 vApp 網路以及特定類型的組織 VDC 網路。

必須先建立網路集區，然後再建立組織 VDC 網路和 vApp 網路。如果不存在，則唯一可供組織使用的網路選項是直接連線到外部網路。

只有**系統管理員**可以建立網路集區。

如需網路集區的相關資訊，請參閱《VMware Cloud Director Service Provider Admin Portal 指南》。

組織 VDC 網路

組織虛擬資料中心 (VDC) 網路允許 vApp 相互通訊，或與組織外部的外部網路進行通訊。

存在多種不同類型的組織 VDC 網路，具體取決於組織 VDC 網路與外部網路的連線。

組織 VDC 網路可提供與外部網路的直接或路由連線，也可以與外部網路和其他組織 VDC 網路隔離。路由連線需要組織 VDC 中具有 Edge 閘道和網路集區。

系統管理員或**組織管理員**會建立組織 VDC 網路，並將其指派給您的組織。

新建立的組織 VDC 沒有可用的網路。當**系統管理員**建立所需的網路基礎結構後，**組織管理員**可以建立和管理大多數類型的組織 VDC 網路。

NSX Data Center for vSphere 支援的資料中心群組網路

NSX Data Center for vSphere 支援的跨資料中心群組的網路。一個資料中心群組可在單一或多站台 VMware Cloud Director 部署中包含 1 個到 16 個組織 VDC。

NSX-T Data Center 支援的資料中心群組網路

資料中心群組網路是一種組織 VDC 網路類型，這些網路可在一或多個 VDC 之間共用，並且 vApp 可連線到這些網路。

系統管理員或**組織管理員**會建立資料中心群組網路，並將其範圍限定為單一 VDC 群組。

VMware Cloud Director 支援 NSX-T Data Center 所支援的隔離、匯入、直接和路由的資料中心群組網路。

vApp 網路

vApp 網路允許虛擬機器相互通訊，或透過連線至組織 VDC 網路，與其他 vApp 中的虛擬機器進行通訊。

vApp 網路包含在 vApp 內。可將 vApp 網路與其他網路隔離，或連線至組織 VDC 網路。

每個 vApp 都包含 vApp 網路。部署 vApp 時，系統會建立該網路，並在取消部署 vApp 時加以刪除。

組織管理員會設定和控制 vApp 網路。

vApp 中的網路類型

vApp 中的虛擬機器能夠連線到隔離、直接或路由的 vApp 網路，以及組織 VDC 網路。

備註 NSX Data Center for vSphere 所支援的組織 VDC 支援路由、隔離和直接 vApp 網路。

NSX-T Data Center 所支援的組織 VDC 支援隔離和直接 vApp 網路。

您可以將不同類型的網路新增至 vApp，以處理多個網路案例。

vApp 中的虛擬機器可以連線至 vApp 中的可用網路。如果您想要將虛擬機器連線至不同網路，則必須先將此網路新增至 vApp。

vApp 可以包括 vApp 網路和組織 VDC 網路。隔離的 vApp 網路包含在 vApp 內。

您也可以將 vApp 網路路由至組織 VDC 網路，以提供與 vApp 外部的虛擬機器的連線。針對路由的 vApp 網路，您可以設定網路服務 (如防火牆和靜態路由)。

可以將 vApp 直接連線至組織 VDC 網路。

如果有多個 vApp 包含連線至同一個組織 VDC 網路的相同虛擬機器，而且要同時啟動 vApp，則可以將 vApp 納入範圍。將 vApp 納入範圍可讓您隔離虛擬機器的 MAC 和 IP 位址，以開啟其電源，而不發生衝突。

如需相關資訊，請參閱在 vApp 中使用網路。

Edge 閘道

Edge 閘道提供路由的組織 VDC 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。

Edge 閘道需要 NSX Data Center for vSphere 或 NSX-T Data Center。

本章節討論下列主題：

- 管理組織虛擬資料中心網路
- 使用 NSX-T Data Center 管理資料中心群組網路
- 使用 NSX Data Center for vSphere 管理資料中心群組網路
- 管理 NSX Data Center for vSphere Edge 閘道服務
- 管理 NSX-T Data Center Edge 閘道

管理組織虛擬資料中心網路

系統管理員或**組織管理員**會建立組織 VDC 網路，並將其指派給組織 VDC 或組織 VDC 群組。**組織管理員**可以檢視網路的相關資訊、設定網路服務等。

您可以使用 NSX Data Center for vSphere 支援的直接、路由、隔離或資料中心群組組織 VDC 網路。

您可以使用 NSX-T Data Center 支援的路由、隔離、匯入和直接組織 VDC 網路。此外，還可以使用 NSX-T Data Center 支援的路由、隔離和匯入的資料中心群組網路。

表 5-1. 組織 VDC 網路類型

資料中心類型網路	描述
直接	可直接連線到**系統管理員**所佈建的其中一個外部網路並由 vSphere 資源支援的組織 VDC 網路。 NSX Data Center for vSphere 支援的組織 VDC 支援直接網路，而從 VMware Cloud Director 10.2.2 開始，NSX-T Data Center 支援的組織 VDC 支援直接網路。 直接網路可供多個組織 VDC 存取。 屬於不同組織 VDC 的虛擬機器可以連線至這個網路，並查看此網路上的流量。 直接網路提供直接第 2 層連線，連線至組織 VDC 外部的虛擬機器。此組織 VDC 外部的虛擬機器可以直接連線至組織 VDC 中的虛擬機器。 **備註** 只有您的**系統管理員**可以新增直接組織 VDC 網路。 可以是 IPv4 或 IPv6。
隔離 (內部)	隔離的網路僅可供同一個組織 VDC 存取。只有此組織 VDC 中的虛擬機器可連線至內部組織 VDC 網路，並查看此網路上的流量。 NSX-T Data Center 支援的組織 VDC 和組織 VDC NSX Data Center for vSphere 支援隔離網路。 隔離的組織 VDC 網路可為組織 VDC 提供隔離的私人網路，可供多個虛擬機器和 vApp 連線。此網路無法連線至組織 VDC 外部的虛擬機器。組織 VDC 外部的機器無法連線至組織 VDC 中的機器。

表 5-1. 組織 VDC 網路類型 (續)

資料中心類型網路	描述
路由	路由的網路僅可供同一個組織 VDC 存取。只有此組織 VDC 中的虛擬機器可連線至此網路。 這個網路也提供外部網路的控制存取功能。做為**系統管理員**或**組織管理員**，您可以設定網路位址轉譯 (NAT)、防火牆和 VPN 設定，以便能夠從外部網路存取特定虛擬機器。 可以是 IPv4 或 IPv6。
匯入的 NSX-T Data Center 邏輯交換器	匯入的 NSX-T Data Center 網路是在 NSX-T Data Center 中建立並使用現有 NSX-T Data Center 邏輯交換器的邏輯區段。它們將作為組織 VDC 網路匯入特定組織中。 **備註** 只有**系統管理員**可以匯入 NSX-T Data Center 網路。
NSX Data Center for vSphere 支援的資料中心群組網路	此網路是跨資料中心群組的資料中心群組網路的一部分。一個資料中心群組可在單一或多站台 VMware Cloud Director 部署中包含 1 個到 16 個組織 VDC。 連線至此網路的虛擬機器將連線至基礎延伸網路。
NSX-T Data Center 支援的資料中心群組網路	資料中心群組網路是一種由 NSX-T Data Center 支援的組織 VDC 網路類型，這些網路可在一或多個 VDC 之間共用，並且 vApp 可連線到這些網路。 資料中心群組網路可以隔離、匯入或路由，並且需要 NSX-T Data Center。

記錄的管理組織 VDC 網路的所有步驟假設您的環境中有多個 VDC。

檢視可用的組織 VDC 網路

您可以檢視可用的組織虛擬資料中心網路。

必要條件

確認您是**組織管理員**、**系統管理員**，或者您已獲指派包含一組同等權限的角色。

程序

- 在頂部導覽列中，按一下**網路**。

結果

在**網路**索引標籤中，您會看到可依各種準則篩選的可用網路清單。

後續步驟

您可以新增組織 VDC 網路。此外，還可以編輯、增加範圍、刪除或重設現有的組織 VDC 網路。

新增隔離組織虛擬資料中心網路

您可以新增隔離組織 VDC 網路，只有此組織可以存取這個網路。這個網路不能連線至這個組織外的虛擬機器。此組織外部的虛擬機器無法連線至組織中的虛擬機器。

您可以新增一組隔離和路由組織 VDC 網路，以滿足您組織的需求。例如，您可以隔離包含敏感資訊的網路，同時具有與 Edge 閘道相關聯並連線至網際網路的單獨網路。

您可以建立受網路集區支援的隔離 VDC 網路。服務提供者也可以建立受 NSX-T 邏輯交換器支援的隔離 VDC 網路。

您只能建立 IPv4 隔離組織 VDC 網路。

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 在頂部導覽列中，按一下**網路**。

2 在**網路**索引標籤上，按一下**新增**。

3 在**範圍**頁面上，選取**組織虛擬資料中心**，選取要在其中建立網路的 VDC，然後按**下一步**。

4 在**選取網路類型**頁面上，選取**隔離**，然後按**下一步**。

5 為網路輸入有意義的名稱。

6 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**。

7 輸入組織 VDC 網路的說明。

8 (選擇性) 如果已建立網路的 VDC 由 NSX Data Center for vSphere 提供支援，請開啟**已共用**選項，使組織 VDC 網路可供相同組織內的其他組織 VDC 使用。

此選項的一種可能使用案例為，如果組織 VDC 內存在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。以下方法可做為解決方案，即透過隨收隨付建立第二個組織 VDC，並暫時在該網路上執行更多虛擬機器。

備註 組織 VDC 必須由相同的提供者 VDC 支援。

9 按**下一步**。

10 (選擇性) 若要保留一或多個 IP 位址以指派給需要靜態 IP 位址的虛擬機器，請設定此網路的**靜態 IP 集區**。

a 輸入 IP 位址或 IP 位址範圍，然後按一下**新增**。

若要新增多個靜態 IP 位址或範圍，請重複此步驟。

b (選擇性) 若要修改或移除 IP 位址和範圍，請按一下**修改**或**移除**。

11 按**下一步**。

12 (選擇性) 設定 DNS。

選項	動作
主要 DNS	輸入您的主要 DNS 伺服器的 IP 位址。
次要 DNS	輸入您的次要 DNS 伺服器的 IP 位址。
DNS 尾碼	輸入 DNS 尾碼。 DNS 尾碼為不包含主機名稱的 DNS 名稱。

13 按**下一步**。

14 在**即將完成**頁面上，檢閱設定，然後按一下**完成**。

新增路由組織虛擬資料中心網路

若要控制對外部網路的存取，您可以新增路由組織 VDC 網路。**系統管理員**和**組織管理員**可以設定網路位址轉譯 (NAT)、防火牆和 VPN 設定，以便能夠從外部網路存取特定虛擬機器。

您可以新增一組路由和隔離組織 VDC 網路，以滿足您組織的需求。例如，您可以新增與 Edge 閘道相關聯並連線至網際網路的網路，同時具有包含敏感資訊的隔離網路。

您可以新增 IPv4 或 IPv6 路由組織 VDC 網路。

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 在頂部導覽列中，按一下**網路**。

2 在**網路**索引標籤上，按一下**新增**。

3 在**範圍**頁面上，選取**組織虛擬資料中心**，選取要在其中建立網路的 VDC，然後按**下一步**。

4 在**選取網路類型**頁面上，選取**已路由**，然後按**下一步**。

5 為網路輸入有意義的名稱。

6 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**。

7 輸入組織 VDC 網路的說明。

8 (選擇性) 如果已建立網路的 VDC 由 NSX Data Center for vSphere 提供支援，請開啟**已共用**選項，使組織 VDC 網路可供相同組織內的其他組織 VDC 使用。

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。以下方法可做為解決方案，即透過隨收隨付建立第二個組織 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 按**下一步**。

10 在 **Edge 連線**頁面上，選取要與組織 VDC 網路相關聯的 Edge 閘道。

如果組織 VDC 包含多個 Edge 閘道，您必須選取此網路連線的 Edge 閘道。為了支援其他路由網路，Edge 閘道在 [可用網路數目] 資料行中必須顯示至少為 1 的值。

11 從**介面類型**下拉式功能表中，選取介面類型。

選項	描述
內部	連線到 Edge 閘道的其中一個內部介面。 允許的網路數目上限為 9。
分散式	在連線至此 Edge 閘道的分散式邏輯路由器上建立網路。 允許的網路數目上限為 400。
子介面	延伸組織 VDC 網路。VMware Cloud Director 識別要用於透過 L2 VPN 延伸的網路。 藉由 NSX 網路虛擬化的協助，VMware Cloud Director 將為此網路建立主幹介面類型。允許的網路數目上限為 200。

12 (選擇性) 若要在此網路上啟用客體 VLAN 標記，請開啟**允許的客體 VLAN** 選項。

13 按**下一步**。

14 (選擇性) 若要保留一或多個 IP 位址以指派給需要靜態 IP 位址的虛擬機器，請設定此網路的**靜態 IP 集區**。

a 輸入 IP 位址或 IP 位址範圍，然後按一下**新增**。

若要新增多個靜態 IP 位址或範圍，請重複此步驟。

b (選擇性) 若要修改或移除 IP 位址和範圍，請按一下**修改**或**移除**。

15 按**下一步**。

16 (選擇性) 設定 DNS。

選項	動作
主要 DNS	輸入您的主要 DNS 伺服器的 IP 位址。
次要 DNS	輸入您的次要 DNS 伺服器的 IP 位址。
DNS 尾碼	輸入 DNS 尾碼。 DNS 尾碼為不包含主機名稱的 DNS 名稱。

17 按**下一步**。

18 在**即將完成**頁面上，檢閱設定，然後按一下**完成**。

新增直接組織虛擬資料中心網路

若要透過直接路由連線至外部網路，**系統管理員**可以設定直接連線。

從 VMware Cloud Director 10.2.2 開始，支援在 NSX-T Data Center 和 NSX Data Center for vSphere 支援的組織 VDC 中建立直接網路。

如果您以**組織管理員**身分登入 VMware Cloud Director 租用戶入口網站，並嘗試建立直接組織虛擬資料中心網路，您會收到一條警告訊息，指示您的權限不足。

必要條件

驗證您是否具有**系統管理員**權限。

程序

1 在頂部導覽列中，按一下**網路**。

2 在**網路**索引標籤上，按一下**新增**。

3 在**範圍**頁面上，選取**組織虛擬資料中心**，選取要在其中建立網路的 VDC，然後按**下一步**。

4 在**網路類型**頁面上，選取**直接**，然後按**下一步**。

5 為網路輸入有意義的名稱。

6 輸入組織 VDC 網路的說明。

7 (選擇性) 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**選項。

8 在**外部網路連線**頁面上，選取您要將新組織虛擬資料中心網路直接連線到的外部網路，然後按**下一步**。

9 在**即將完成**頁面上，檢閱設定，然後按一下**完成**。

使用匯入的 NSX-T Data Center 邏輯交換器新增組織 VDC 網路

系統管理員可以透過從相關聯的 NSX-T Manager 執行個體匯入邏輯交換器來建立組織 VDC 網路。

必要條件

- 驗證您是否具有**系統管理員**權限。
- 確認支援目標組織虛擬資料中心的提供者虛擬資料中心是否與 NSX-T Manager 執行個體相關聯。
- 您必須建立至少一個未被其他組織虛擬資料中心網路使用的 NSX-T 邏輯交換器。

如需建立和設定 NSX-T 邏輯交換器的相關資訊，請參閱 NSX-T Data Center 管理指南。

程序

1 在頂部導覽列中，按一下**網路**。

2 在**網路**索引標籤上，按一下**新增**。

3 在**範圍**頁面上，選取**組織虛擬資料中心**，選取要在其中建立網路的 VDC，然後按**下一步**。

4 在**網路類型**頁面上，依序選取**已匯入**和 **NSX-T 邏輯交換器**，然後按**下一步**。

5 從可用 NSX-T 邏輯交換器的清單中，選取目標交換器，然後按**下一步**。

6 為網路輸入有意義的名稱。

7 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**。

如果交換器設定了子網路，系統會預先填入此資訊。

8 輸入組織 VDC 網路的說明。

9 按**下一步**。

10 (選擇性) 設定 DNS 設定和靜態 IP 集區。

您可以新增多個 IP 位址和 IP 範圍。

11 按**下一步**。

12 在**即將完成**頁面上，檢閱設定，然後按一下**完成**。

編輯組織虛擬資料中心網路的一般設定

您可以修改組織 VDC 網路的內容。

必要條件

確認您是**組織管理員**、**系統管理員**，或者您已獲指派包含一組同等權限的角色。

程序

1 在頂部導覽列中，按一下**網路**。

2 在**網路**索引標籤上，按一下您要編輯的組織 VDC 網路的名稱。

3 在**一般**索引標籤上，按一下**編輯**。

a 編輯網路的名稱和說明。

b 如果已建立網路的 VDC 由 NSX Data Center for vSphere 提供支援，請開啟或關閉**已共用**選項，使組織 VDC 網路可供相同組織內的其他組織 VDC 使用。

4 按一下**儲存**。

將組織虛擬資料中心網路連線至 Edge 閘道

建立組織 VDC 網路後，您可以將網路連線至 Edge 閘道。

從 10.1 版開始，對於 NSX Data Center for vSphere 或 NSX-T Data Center 所支援的組織 VDC 網路，VMware Cloud Director 支援連線至 Edge 閘道。

必要條件

此作業需要其中一個預先定義的**組織管理員**或**系統管理員**角色，或包含向組織發佈的**組織 VDC 網路：編輯內容**和 **VDC 群組：檢視**權限的角色。

程序

1 在頂部導覽列中，按一下**網路**。

2 按一下您要連線至 Edge 閘道的組織 VDC 網路的名稱。

3 在**一般**索引標籤上，按一下**編輯**。

4 按一下**連線**。

5 將網路連線至 Edge 閘道。

a 開啟**連線至 Edge 閘道**選項。

b 從可用 Edge 閘道清單中，選取要連線的 Edge 閘道。

c 選取介面類型。

d 若要允許客體 VLAN，請開啟**允許的客體 VLAN** 選項。

6 按一下**儲存**。

結果

組織 VDC 網路會連線至 Edge 閘道，並從隔離轉換為路由。

中斷組織 VDC 網路與 Edge 閘道的連線

透過中斷組織 VDC 網路與 Edge 閘道的連線，可以將其從路由網路轉換為隔離網路。

從 10.1 版開始，對於 NSX Data Center for vSphere 或 NSX-T Data Center 所支援的組織 VDC 網路，支援連線至 Edge 閘道以及與 Edge 閘道中斷連線。

必要條件

此作業需要其中一個預先定義的**組織管理員**或**系統管理員**角色，或是包含**組織 VDC 網路：編輯內容**權限的角色。

程序

1 在頂部導覽列中，按一下**網路**。

2 按一下您要中斷連線的組織 VDC 網路的名稱。

3 在**一般**索引標籤上，按一下**編輯**。

4 按一下**連線**。

5 若要從 Edge 閘道中斷網路連線，請關閉**連線至 Edge 閘道**選項。

6 按一下**儲存**。

結果

您已中斷組織 VDC 網路與 Edge 閘道的連線。組織 VDC 網路會從路由網路轉換為隔離網路。

轉換路由組織 VDC 網路的介面

例如，您可以透過編輯網路內容，將網路的介面從內部變更為子介面或分散式路由。

備註 無法轉換跨 VDC 網路。

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 在頂部導覽列中，按一下**網路**。

2 按一下您要編輯的組織 VDC 網路的名稱。

3 在**一般**索引標籤上，按一下**編輯**。

4 按一下**連線**。

5 從**介面類型**下拉式功能表中，選取介面類型。

選項	描述
內部	連線到 Edge 閘道的其中一個內部介面。 允許的網路數目上限為 9。
分散式	在連線至此 Edge 閘道的分散式邏輯路由器上建立網路。 允許的網路數目上限為 400。
子介面	延伸組織 VDC 網路。VMware Cloud Director 識別要用於透過 L2 VPN 延伸的網路。 藉由 NSX 網路虛擬化的協助，VMware Cloud Director 將為此網路建立主幹介面類型。允許的網路數目上限為 200。

6 按一下**儲存**。

檢視用於組織虛擬資料中心網路的 IP 位址

您可以檢視組織虛擬資料中心網路 IP 集區中目前正在使用中的 IP 位址清單。

必要條件

- 確認您是**組織管理員**、**系統管理員**，或者您已獲指派包含一組同等權限的角色。
- 確認您的網路是隔離或路由的組織虛擬資料中心網路。

程序

1 在頂部導覽列中，按一下**網路**。

2 按一下您要查看所使用 IP 位址的網路的名稱。

3 在 **IP 管理**區段中，按一下 **IP 使用量**以查看目前使用中的 IP 位址。

將 IP 位址新增至組織虛擬資料中心網路 IP 集區

如果組織虛擬資料中心網路已用完 IP 位址，則您可以其 IP 集區新增更多位址。

您無法將 IP 位址新增至具有直接連線的外部組織虛擬資料中心網路。

必要條件

- 確認您是**組織管理員**、**系統管理員**，或者您已獲指派包含一組同等權限的角色。
- 確認您的網路是隔離或路由的組織虛擬資料中心網路。

程序

1 在頂部導覽列中，按一下**網路**。

2 按一下您要編輯的網路的名稱。

3 在 **IP 管理**區段中，按一下**靜態 IP 集區**索引標籤。

4 按一下右側的**編輯**按鈕。

在**編輯網路**視窗中，您會看到閘道 CIDR 和 IP 位址範圍 (如有)。

5 在**靜態 IP 集區**文字方塊中，輸入 IP 位址或 IP 位址範圍，然後按一下**新增**。

備註 對於跨 VDC 網路，IP 位址不得與指派給相同延伸網路中其他組織 VDC 網路的 IP 位址重疊。

6 按一下**儲存**。

結果

IP 位址或 IP 位址範圍隨即新增至網路 IP 集區。

編輯或移除組織虛擬資料中心網路中使用的 IP 範圍

如果組織虛擬資料中心網路包含您不再需要的 IP 位址，您可以編輯這些位址或將其從 IP 集區中刪除。

必要條件

- 確認您是**組織管理員**、**系統管理員**，或者您已獲指派包含一組同等權限的角色。
- 確認您的網路是隔離或路由的組織虛擬資料中心網路。

程序

1 在頂部導覽列中，按一下**網路**。

2 按一下您要編輯的網路的名稱。

3 在 **IP 管理**區段中，按一下**靜態 IP 集區**。

4 按一下右側的**編輯**按鈕。

- 若要修改 IP 範圍，請選取範圍，進行必要的編輯，然後按一下**修改**。
- 若要移除 IP 範圍，請選取範圍，然後按一下**移除**。

5 按一下**儲存**。

編輯組織虛擬資料中心網路的 DNS 設定

您可以編輯組織虛擬資料中心網路的 DNS 設定。

必要條件

- 確認您是**組織管理員**、**系統管理員**，或者您已獲指派包含一組同等權限的角色。
- 確認您的網路是隔離或路由的組織虛擬資料中心網路。

程序

1 在頂部導覽列中，按一下**網路**。

2 按一下您要編輯的網路的名稱。

3 在 **IP 管理**區段中，按一下 **DNS**。

4 按一下右側的**編輯**按鈕。

5 視需要編輯主要 DNS、次要 DNS 和 DNS 尾碼資訊。

6 按一下**儲存**。

設定隔離組織虛擬資料中心網路的 DHCP 設定

您可以編輯 NSX Data Center for vSphere 支援的隔離組織 VDC 網路的 DHCP 設定。組織 VDC 網路的 DHCP 服務將其位址集區中的 IP 位址提供給設定為從 DHCP 要求位址的虛擬機器 NIC。當虛擬機器開啟電源時，此服務會提供位址。

從 10.2 版開始，VMware Cloud Director 對 IPv4 和 IPv6 支援 DHCP 設定。您可以使用 VMware Cloud Director API 進行 IPv6 設定。

必要條件

- 確認您是**組織管理員**、**系統管理員**，或者您已獲指派包含一組同等權限的角色。
- 確認您的網路是隔離組織虛擬資料中心網路。
- 確認您的網路是否受 NSX Data Center for vSphere 支援。

程序

1 在頂部導覽列中，按一下**網路**。

2 按一下您要編輯的網路的名稱。

3 在 **IP 管理**區段中，按一下 **DHCP**。

4 若要啟用 DHCP，請按一下 **DHCP 集區服務**右側的**編輯**。

5 開啟 **DHCP 集區服務**，然後按一下**儲存**。

DHCP 用戶端所要求的位址會從 DHCP 集區提取。

6 建立網路的 DHCP 集區。

a 按一下**新增**。

b 輸入集區的 IP 位址範圍。

您指定的 IP 位址範圍不能與組織虛擬資料中心的靜態 IP 位址集區重疊。

c 指定 DHCP 位址的預設租用時間 (以秒為單位)。

預設值為 3,600 秒。

d 指定 DHCP 位址的最大租用時間 (以秒為單位)。

這是 DHCP 指派的 IP 位址租用給虛擬機器的時間長度上限。預設值為 7,200 秒。

7 按一下**儲存**。

將 DHCP 集區新增到 NSX-T Data Center 支援的路由組織虛擬資料中心網路

您可以將 DHCP 集區新增到 NSX-T Data Center 支援的路由組織 VDC 網路。

備註 NSX-T Data Center 支援的組織 VDC 網路不支援刪除或更新 DHCP 集區。

必要條件

- 這些作業需要預先定義的**組織管理員**或**系統管理員**角色或包括一組同等權限的角色。
- 確認您的網路是否為路由組織虛擬資料中心網路。
- 確認您的網路是否受 NSX-T Data Center 支援。

程序

1 在頂部導覽列中，按一下**網路**。

2 按一下您要編輯的網路的名稱。

3 在 **IP 管理**區段中，按一下 [DHCP]。

4 若要新增 DHCP 集區，請按一下**新增**。

5 輸入集區的 IPv4 位址範圍。

6 按一下**儲存**。

為 NSX Data Center for vSphere 支援的隔離組織虛擬資料中心網路編輯或刪除現有 DHCP 集區

如果您的隔離組織虛擬資料中心網路內不再需要 DHCP 集區，可以刪除或編輯 NSX Data Center for vSphere 支援的集區。

必要條件

- 確認您是**組織管理員**、**系統管理員**，或者您已獲指派包含一組同等權限的角色。
- 確認您的網路是隔離組織虛擬資料中心網路。
- 確認組織虛擬資料中心網路受 NSX Data Center for vSphere 支援。

程序

1 在頂部導覽列中，按一下**網路**。

2 按一下您要編輯的網路的名稱。

3 按一下 **IP 管理**區段，按一下 **DHCP**。

4 編輯或刪除現有的 DHCP 集區。

選項	動作
編輯 DHCP 集區。	1 選取您要編輯的 DHCP 集區。 2 按一下**編輯**按鈕。 3 更新集區的 IP 位址範圍。 4 編輯 DHCP 位址的預設租用時間 (以秒為單位)。 5 編輯 DHCP 位址的最大租用時間 (以秒為單位)。 6 按一下**儲存**。
刪除 DHCP 集區。	1 選取您要刪除的 DHCP 集區。 2 按一下**刪除**按鈕。

重設組織虛擬資料中心網路

如果與組織虛擬資料中心網路相關聯的網路服務 (例如 DHCP 設定或防火牆設定) 未如預期般運作，您可以重設網路。

當您重設組織虛擬資料中心網路時，您可以強制重新部署網路 DHCP 服務閘道。此作業將導致 DHCP 服務暫時中斷，並且在重設網路時網路服務均無法使用。

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。
- 網路未連線到任何虛擬機器、vApp 或其他網路。

程序

1 在頂部導覽列中，按一下**網路**。

2 選取組織 VDC 網路。

3 按一下**重設**，並確認重設作業。

刪除組織虛擬資料中心網路

如果您不再需要組織虛擬資料中心網路，則可以刪除此網路。

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。
- 網路未連線到虛擬機器、vApp 或其他網路。

程序

1 在頂部導覽列中，按一下**網路**。

2 按一下目標網路名稱旁邊的選項按鈕，然後按一下**刪除**。

3 按一下**確定**以確認。

使用 NSX-T Data Center 管理資料中心群組網路

從版本 10.2 開始，VMware Cloud Director 支援 NSX-T Data Center 所支援的資料中心群組網路。

若要跨多個組織 VDC 建立網路，請先分組 VDC，然後建立與其共用的群組網路。

NSX-T Data Center 支援的資料中心群組網路提供了第 2 層網路共用、單一主動出口點組態，以及跨資料中心群組套用的 Distributed Firewall (DFW) 規則。

資料中心群組

資料中心群組充當跨 VDC 路由器，可提供集中式網路管理、出口點組態，以及群組內所有網路之間的東西向流量。一個資料中心群組可以包含 1 個到 16 個 VDC，這些 VDC 設定為共用一個主動出口點。

可用性區域

可用性區域表示可供網路使用的計算叢集或計算容錯網域。依預設，可用性區域為提供者 VDC。

重要 您的**系統管理員**必須透過為 vCenter Server 執行個體以及 vCenter Server 執行個體支援的提供者 VDC (可選) 設定**計算提供者範圍**，為具有 NSX-T Data Center 的群組網路設定可用性區域。依預設，提供者 VDC 的計算提供者範圍會從支援此 VDC 的 vCenter Server 執行個體複製。**系統管理員**可區分由單一 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，您可以具有範圍為 **Germany** 的 vCenter Server 執行個體以及範圍為 **Munich** 的提供者 VDC。

您的**系統管理員**也可以將可用性區域重新設定為網路提供者範圍，這通常表示具有相關聯 NSX-T Manager 的基礎 vCenter Server 執行個體。

出口點

設定為將資料中心群組連線至外部網路的現有 NSX-T Data Center Edge 閘道。

資料中心群組網路

在資料中心群組中的所有 VDC 之間共用的第 2 層網路。

管理具有 NSX-T Data Center 網路提供者類型的資料中心群組

建立具有 NSX-T Data Center 網路提供者類型的資料中心群組後，您可以將資料中心新增至該群組、移除資料中心，以及編輯群組設定。

一個資料中心群組最多可包含 16 個虛擬資料中心。

從資料中心群組中移除的 VDC 不得將工作負載連結至參與資料中心群組的任何網路。

建立具有 NSX-T Data Center 網路提供者類型的資料中心群組

您可以將 1 個到 16 個 VDC 分組至一個具有 NSX-T Data Center 網路提供者類型的資料中心群組中。

必要條件

確認您是**組織管理員**、**系統管理員**，或者您已獲指派包含一組同等權限的角色。

程序

1 在頂部導覽列中，按一下**網路**，然後按一下**資料中心群組**索引標籤。

2 按一下**新增**。

3 在**起始 VDC** 頁面上，選取 NSX-T Data Center 支援的 VDC 以啟動群組。

4 輸入新資料中心群組的名稱，並選擇性地輸入說明。

5 在**參與 VDC** 頁面上，為新的資料中心群組選取其他資料中心，然後按**下一步**。

6 檢閱資料中心群組的詳細資料，然後按一下**完成**。

結果

新建立的群組會顯示在資料中心群組清單中。

後續步驟

建立跨越具有 NSX-T Data Center 網路提供者類型的資料中心群組的網路。

檢視和編輯具有 NSX-T Data Center 網路提供者類型的資料中心群組的一般設定

您可以在組織中檢視和編輯具有 NSX-T Data Center 網路提供者類型的資料中心群組。

必要條件

確認您是**組織管理員**，或者您的角色擁有一組同等權限。

程序

1 在頂部導覽列中，按一下**網路**，然後按一下**資料中心群組**索引標籤。

資料中心群組清單隨即顯示。

2 按一下目標資料中心群組。

3 在**一般設定**窗格中，按一下**編輯**。

4 編輯資料中心群組的名稱，並選擇性地編輯其說明，然後按一下**儲存**以確認。

管理資料中心群組中的參與 VDC

可以選取將成為 VDC 群組的一部分並相互通訊的 VDC。

必要條件

確認您是**組織管理員**，或者您的角色擁有一組同等權限。

程序

1 在頂部導覽列中，按一下**網路**，然後按一下**資料中心群組**索引標籤。

資料中心群組清單隨即顯示。

2 按一下目標資料中心群組。

3 按一下**參與 VDC**，然後按一下**管理**。

4 選取要包含在群組中的 VDC，然後按一下**儲存**以確認。

同步具有 NSX-T Data Center 網路提供者類型的資料中心群組

若要確認加入資料中心群組的所有 VDC 是否仍存在並已正確設定，您可以同步資料中心群組。

程序

1 在頂部導覽列中，按一下**網路**，然後按一下**資料中心群組**索引標籤。

資料中心群組清單隨即顯示。

2 按一下目標資料中心群組。

3 按一下**同步**並進行確認。

在具有 NSX-T Data Center 網路提供者類型的資料中心群組中使用 Distributed Firewall

從 10.2 版開始，VMware Cloud Director 對於具有 NSX-T Data Center 網路提供者類型的資料中心群組支援 Distributed Firewall 服務。

針對具有 NSX-T Data Center 網路提供者類型的資料中心群組啟用 Distributed Firewall 時，您可以建立套用至資料中心群組的單一預設安全性原則。

身為**組織管理員**，您可以建立和修改與資料中心群組的預設安全性原則相關聯的其他 Distributed Firewall 規則。

依預設，不會啟用 Distributed Firewall 服務。啟用 Distributed Firewall 後，您可以建立 IP 集和安全群組，以協助建立 Distributed Firewall 規則。

備註 您建立的 Distributed Firewall 規則僅適用於連結至資料中心群組網路的工作負載。

針對具有 NSX-T Data Center 網路提供者類型的資料中心群組啟用 Distributed Firewall

透過使用 Distributed Firewall，可以在單一資料中心群組之間套用一組第 3 層防火牆規則。

依預設，不會啟用 Distributed Firewall。啟用時，您可以建立單一預設安全性原則。

必要條件

確認您是**系統管理員**。

程序

1 在頂部導覽列中，按一下**網路**，然後按一下**資料中心群組**索引標籤。

資料中心群組清單隨即顯示。

2 按一下目標資料中心群組。

3 在 **Distributed Firewall** 區段中，按一下**啟用**，並確認您要啟用 Distributed Firewall。

後續步驟

建立 Distributed Firewall 規則。

將 IP 集新增至資料中心群組

若要建立 Distributed Firewall 規則並將其新增至資料中心群組，您必須先建立 IP 集。IP 集是套用 Distributed Firewall 規則的 IP 位址和網路群組。將多個物件合併至 IP 集有助於減少要建立的 Distributed Firewall 規則總數。

程序

1 在頂部導覽列中，按一下**網路**，然後按一下**資料中心群組**索引標籤。

資料中心群組清單隨即顯示。

2 按一下目標資料中心群組。

3 在 [安全性] 下，按一下 **IP 集**。

4 按一下**新增**。

5 為新的 IP 集輸入有意義的名稱，並選擇性地輸入其說明。

6 以 CIDR 格式輸入 IPv4 位址、IPv6 位址或位址範圍，然後按一下**新增**。

7 若要修改現有的 IP 位址或範圍，請按一下**修改**並編輯值。

8 按一下**儲存**以確認。

在具有 NSX-T Data Center 網路提供者類型的資料中心群組中建立安全群組

為資料中心群組建立 Distributed Firewall 規則之前，您可以將資料中心群組網路分組到套用這些規則的安全群組中。

安全群組是指套用 Distributed Firewall 規則的一組資料中心群組網路。對網路進行分組有助於減少要建立的 Distributed Firewall 規則總數。

必要條件

確認您至少有一個資料中心群組網路受到 NSX-T Data Center 支援。

程序

1 在頂部導覽列中，按一下**網路**，然後按一下**資料中心群組**索引標籤。

資料中心群組清單隨即顯示。

2 按一下目標資料中心群組。

3 在 [安全性] 下，按一下**安全群組**，然後按一下**新增**。

4 輸入安全群組的名稱，並選擇性地輸入說明，然後按一下**儲存**。

新安全群組即顯示在清單中。

5 選取新建立的安全群組，然後按一下**管理成員**。

6 選取要新增至安全群組的資料中心群組網路。

7 按一下**儲存**。

後續步驟

將 Distributed Firewall 規則新增至具有 NSX-T Data Center 網路提供者類型的資料中心群組

將應用程式連接埠設定檔新增至資料中心群組

若要建立 Distributed Firewall 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 (用於防火牆服務)。除了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。

程序

1 在頂部導覽列中，按一下**網路**，然後按一下**資料中心群組**索引標籤。

資料中心群組清單隨即顯示。

2 按一下目標資料中心群組。

3 在 [安全性] 下，按一下**應用程式連接埠設定檔**。

4 在**自訂應用程式**窗格中，按一下**新增**。

5 輸入應用程式連接埠設定檔的名稱，並選擇性地輸入說明。

6 從**通訊協定**下拉式功能表中，選取通訊協定。

7 輸入連接埠或連接埠範圍 (以逗號分隔)，然後按一下**儲存**。

8 若要設定其他連接埠設定檔，請重複這些步驟。

後續步驟

使用應用程式連接埠設定檔建立 Distributed Firewall 規則。

將 Distributed Firewall 規則新增至具有 NSX-T Data Center 網路提供者類型的資料中心群組

您建立的 Distributed Firewall 規則僅適用於附加至資料中心群組網路的工作負載。

必要條件

確認已啟用資料中心群組的 Distributed Firewall 服務。

程序

1 在頂部導覽列中，按一下**網路**，然後按一下**資料中心群組**索引標籤。

資料中心群組清單隨即顯示。

2 按一下目標資料中心群組。

3 按一下左側的 **Distributed Firewall** 索引標籤。

4 按一下**編輯規則**。

5 若要新增防火牆規則，請按一下**在頂部新增**。

6 設定規則。

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**選項。
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**。
內容	(選擇性) 為規則選取 NSX-T Data Center 內容設定檔。
來源	選取來源流量，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 IP 集或安全群組的流量，請從清單中選取 IP 集和安全群組。
目的地	選取目的地流量，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 IP 集或安全群組的流量，請從清單中選取 IP 集和安全群組。
動作	從**動作**下拉式功能表中，選取允許還是拒絕進出特定來源的流量。 ■ 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，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。
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。

7 按一下**儲存**。

8 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 [Distributed Firewall 規則] 清單中。您可以視需要上移、下移、編輯或刪除規則。

停用預設分散式防火牆原則

如果您想要停用分散式防火牆服務，則必須先停用預設分散式防火牆原則。

停用預設原則時，您可以編輯分散式防火牆規則，但不會再套用這些規則。

程序

1 在頂部導覽列中，按一下**網路**，然後按一下**資料中心群組**索引標籤。

資料中心群組清單隨即顯示。

2 按一下目標資料中心群組。

3 按一下左側的**分散式防火牆**索引標籤。

4 在 [分散式防火牆規則] 清單上方的**預設原則**卡中，按一下**停用**並確認動作。

結果

預設原則已停用。其餘的分散式防火牆規則可以進行編輯，但不會套用。

停用分散式防火牆服務

如果您不想使用分散式防火牆服務，可以將其停用。

停用資料中心群組的分散式防火牆服務時，系統會永久刪除此群組的安全性規則組態，且無法復原。

必要條件

停用預設分散式防火牆原則

程序

1 在頂部導覽列中，按一下**網路**，然後按一下**資料中心群組**索引標籤。

資料中心群組清單隨即顯示。

2 按一下目標資料中心群組。

3 按一下**一般**。

4 在右側的**分散式防火牆**窗格中，按一下**停用**，然後確認動作。

結果

分散式防火牆服務已停用，且安全性規則組態已刪除。

管理具有 NSX-T Data Center 網路提供者類型的資料中心群組網路

建立並設定資料中心群組後，您可以建立和管理跨越參與 VDC 的資料中心群組網路。

您可以使用 NSX-T Data Center 支援的路由、隔離和匯入的組織資料中心群組網路。

資料中心群組網路的範圍只能限定為單一資料中心群組。

您可以將現有網路的範圍從組織 VDC 增加到資料中心群組。

您可以將所有類型的網路新增至資料中心群組。

重要 即使參與資料中心群組的網路已隔離，這些網路中的 IP 位址也不得重疊。

表 5-2. 資料中心群組網路的類型

資料中心群組網路類型	描述
隔離	隔離的資料中心群組網路僅供同一資料中心群組中的 VDC 存取。只有資料中心群組中的虛擬機器可以連線到並查看隔離的資料中心群組網路上的流量。
路由	路由資料中心群組網路透過屬於資料中心群組的 NSX-T Data Center Edge 閘道，提供對外部網路的控制存取權。
匯入	匯入的資料中心群組網路會使用現有的 NSX-T Data Center 邏輯交換器。只有**系統管理員**可以匯入網路。

建立 NSX-T Data Center 支援的隔離資料中心群組網路

您可以新增隔離資料中心群組網路，該網路僅供資料中心群組中的虛擬機器存取。位於此網路之外的虛擬機器無法連線到該網路，無論其是否已連線至同一資料中心群組中的其他網路。

必要條件

- 確認您是**組織管理員**。
- 確認您已建立具有 NSX-T Data Center 網路提供者類型的資料中心群組。

程序

1. 在頂部導覽列中，按一下**網路**。
2. 在**網路**索引標籤上，按一下**新增**。
3. 在**範圍**頁面上，選取**資料中心群組**，然後選取要在其中建立網路且具有 NSX-T Data Center 網路提供者的群組。
4. 在**網路類型**頁面上，選取**已隔離**，然後按**下一步**。
5. 為網路輸入有意義的名稱。
6. 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**。
7. 輸入組織 VDC 網路的說明。
8. 按**下一步**。
9. (選擇性) 若要保留一或多個 IP 位址以指派給需要靜態 IP 位址的虛擬機器，請設定此網路的**靜態 IP 集區**。
   a. 輸入 IP 位址或 IP 位址範圍，然後按一下**新增**。

      若要新增多個靜態 IP 位址或範圍，請重複此步驟。
   b. (選擇性) 若要修改或移除 IP 位址和範圍，請按一下**修改**或**移除**。
10. (選擇性) 設定 DNS。

選項	動作
主要 DNS	輸入您的主要 DNS 伺服器的 IP 位址。
次要 DNS	輸入您的次要 DNS 伺服器的 IP 位址。
DNS 尾碼	輸入 DNS 尾碼。 DNS 尾碼為不包含主機名稱的 DNS 名稱。

11. 在**即將完成**頁面上，檢閱設定，然後按一下**完成**。

建立 NSX-T Data Center 支援的路由資料中心群組網路

若要控制對外部網路的存取，您可以新增路由資料中心群組網路。

必要條件

- 確認您是**組織管理員**，或者您的角色擁有一組同等權限。
- 確認您已建立具有 NSX-T Data Center 網路提供者類型的資料中心群組。
- 確認您已將現有 NSX-T Data Center Edge 閘道的範圍限定為您想要在其中建立路由網路的資料中心群組。

程序

1 在頂部導覽列中，按一下**網路**。

2 在**網路**索引標籤上，按一下**新增**。

3 在**範圍**頁面上，選取**資料中心群組**，然後選取要在其中建立網路且具有 NSX-T Data Center 網路提供者的群組。

4 在**網路類型**頁面上，選取**已路由**，然後按**下一步**。

如果僅有一個範圍限定為資料中心群組的可用 Edge 閘道，則會自動將其指派給網路。

5 如果有多個 NSX-T Data Center 可用於資料中心群組，請從清單中選取一個 Edge 閘道，然後按**下一步**。

6 為網路輸入有意義的名稱。

7 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**。

8 輸入組織 VDC 網路的說明。

9 按**下一步**。

10 (選擇性) 若要保留一或多個 IP 位址以指派給需要靜態 IP 位址的虛擬機器，請設定此網路的**靜態 IP 集區**。

a 輸入 IP 位址或 IP 位址範圍，然後按一下**新增**。

若要新增多個靜態 IP 位址或範圍，請重複此步驟。

b (選擇性) 若要修改或移除 IP 位址和範圍，請按一下**修改**或**移除**。

11 (選擇性) 設定 DNS。

選項	動作
主要 DNS	輸入您的主要 DNS 伺服器的 IP 位址。
次要 DNS	輸入您的次要 DNS 伺服器的 IP 位址。
DNS 尾碼	輸入 DNS 尾碼。 DNS 尾碼為不包含主機名稱的 DNS 名稱。

12 在**即將完成**頁面上，檢閱設定，然後按一下**完成**。

使用已匯入的 NSX-T 邏輯交換器建立資料中心群組網路

系統管理員可以透過從相關聯的 NSX-T Manager 執行個體匯入區段來建立組織 VDC 網路。

必要條件

- 確認您是**系統管理員**。
- 確認您已建立具有 NSX-T Data Center 網路提供者類型的資料中心群組。
- 確認支援目標虛擬資料中心群組的提供者虛擬資料中心是否與 NSX-T Manager 執行個體相關聯。
- 確認至少建立一個未被其他網路使用的 NSX-T 邏輯交換器。如需建立和設定 NSX-T 邏輯交換器的相關資訊，請參閱 NSX-T Data Center 管理指南。

程序

1. 在頂部導覽列中，按一下**網路**。
2. 在**網路**索引標籤上，按一下**新增**。
3. 在**範圍**頁面上，選取**資料中心群組**，然後選取要在其中建立網路且具有 NSX-T Data Center 網路提供者的群組。
4. 在**選取網路**頁面上，選取**已匯入**，然後按**下一步**。
5. 從可用 NSX-T 邏輯交換器的清單中，選取目標交換器，然後按**下一步**。
6. 為網路輸入有意義的名稱。
7. 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**。
8. 輸入組織 VDC 網路的說明。
9. 按**下一步**。
10. (選擇性) 若要保留一或多個 IP 位址以指派給需要靜態 IP 位址的虛擬機器，請設定此網路的**靜態 IP 集區**。
    a. 輸入 IP 位址或 IP 位址範圍，然後按一下**新增**。

       若要新增多個靜態 IP 位址或範圍，請重複此步驟。
    b. (選擇性) 若要修改或移除 IP 位址和範圍，請按一下**修改**或**移除**。
11. (選擇性) 設定 DNS。

選項	動作
主要 DNS	輸入您的主要 DNS 伺服器的 IP 位址。
次要 DNS	輸入您的次要 DNS 伺服器的 IP 位址。
DNS 尾碼	輸入 DNS 尾碼。 DNS 尾碼為不包含主機名稱的 DNS 名稱。

12. 在**即將完成**頁面上，檢閱設定，然後按一下**完成**。

增加 NSX-T Data Center 支援的組織 VDC 網路的範圍

將組織 VDC 網路的範圍增加到資料中心群組網路後，可以從參與資料中心群組的所有資料中心連線工作負載。

必要條件

- 確認您是**組織管理員**，或者您的角色擁有一組同等權限。
- 確認您已建立具有 NSX-T Data Center 網路提供者類型的資料中心群組。
- 確認您已建立 NSX-T Data Center 支援的組織 VDC 網路。

程序

1. 在頂部導覽列中，按一下**網路**。
2. 按一下要增加範圍的組織 VDC 網路旁邊的選項按鈕，然後按一下**增加範圍**。
3. 從資料中心群組清單中選取資料中心群組，然後按一下**確定**以確認。

結果

網路範圍將增加到資料中心群組網路。在網路清單中，它會列為範圍限定為您選取的資料中心群組。

縮減 NSX-T Data Center 支援的資料中心群組網路的範圍

您可以將 NSX-T Data Center 支援的資料中心群組網路的範圍縮減到組織 VDC 網路。

如果您將資料中心群組網路的範圍縮減到單一組織 VDC 網路，則可以為僅屬於組織 VDC 的工作負載提供網路連線。

必要條件

- 確認您是**組織管理員**，或者您的角色擁有一組同等權限。
- 確認您已建立 VDC 網路，並將其範圍限定為具有 NSX-T Data Center 網路提供者類型的資料中心群組。

程序

1. 在頂部導覽列中，按一下**網路**。
2. 按一下要縮減範圍的資料中心群組網路旁邊的選項按鈕，然後按一下**縮減範圍**。
3. 從屬於群組網路成員的 VDC 清單中，選取要將網路範圍限定到的 VDC，然後按一下**確定**。

結果

網路範圍將縮減到單一組織 VDC 網路。

管理具有 NSX-T Data Center 網路提供者類型的資料中心群組的出口點

若要將流入和流出資料中心群組網路的流量路由至外部網路，您可以將 NSX-T Data Center Edge 閘道設定為資料中心群組的出口點。

如果將 Edge 閘道設定為資料中心群組的出口點，會將其範圍增加至資料中心群組。Edge 閘道將在參與此群組的所有資料中心之間共用。連結至 Edge 閘道的所有路由網路均連結至資料中心群組，且適用範圍為該群組。

所有 Edge 閘道服務會繼續作為 Edge 閘道功能的一部分。如需詳細資訊，請參閱管理 NSX-T Data Center Edge 閘道。

如果 VDC 是資料中心群組的成員，且沒有任何工作負載連結至不屬於目標範圍的任何路由網路，則可以從資料中心群組中移除 Edge 閘道並將其範圍限定為單一 VDC。

可以將 Edge 閘道新增至隔離的資料中心群組網路，並將其轉換為路由資料中心網路。也可以從資料中心群組網路移除與 Edge 閘道的連線，從而將路由網路轉換為隔離的資料中心群組網路。

將 NSX-T Data Center Edge 閘道新增至資料中心群組

若要將 NSX-T Data Center Edge 閘道設定為資料中心群組的出口點，請增加 Edge 閘道的範圍。然後，該閘道將在參與此群組的所有資料中心之間共用。

將 Edge 閘道範圍限定為資料中心群組時，連結至 Edge 閘道的所有路由網路均會連結至資料中心群組且適用範圍為該群組。

連結至 Edge 閘道的所有新的路由網路都屬於資料中心群組。

連結至適用範圍為 VDC 的 Edge 閘道的路由網路，只有在 Edge 的範圍增加到資料中心群組時，才可以參與此資料中心群組。

必要條件

確認您已將現有 NSX-T Data Center Edge 閘道與參與資料中心群組的其中一個 VDC 建立關聯。

程序

1 在頂部導覽列中，按一下**網路**，然後按一下**資料中心群組**索引標籤。

資料中心群組清單隨即顯示。

2 按一下目標資料中心群組。

3 按一下 **Edge 閘道**，然後按一下**新增 Edge**。

4 選取其中一個可用的 Edge 閘道，然後按一下**儲存**。

結果

Edge 閘道的範圍隨即增加到資料中心群組。範圍的變更不會影響任何現有的基礎服務或網路。

將 NSX-T Data Center Edge 閘道的範圍縮減到 VDC

您可以將 NSX-T Data Center Edge 閘道的範圍縮減到特定 VDC，方法是將 Edge 閘道從其適用範圍所在的資料中心群組中移除。

將 Edge 閘道的範圍縮減到特定 VDC 時，Edge 閘道正在使用的所有安全群組物件會隨 Edge 閘道一起保留。分散式防火牆以獨佔方式使用的安全群組會繼續作為 VDC 群組的一部分。

必要條件

- 確認要將 Edge 閘道範圍縮減到的 VDC 是資料中心群組的成員。
- 確認沒有任何工作負載連結至不屬於目標 Edge 閘道範圍的任何路由網路。
- 確認 Edge 閘道和分散式防火牆同時正在使用的資料中心群組中沒有安全群組或 IP 集。

程序

1 在頂部導覽列中，按一下**網路**，然後按一下**資料中心群組**索引標籤。

資料中心群組清單隨即顯示。

2 按一下目標資料中心群組。

3 按一下 **Edge 閘道**，然後按一下**移除 Edge**。

4 選取要將 Edge 閘道範圍縮減到的 VDC，然後按一下**儲存**。

使用 NSX Data Center for vSphere 管理資料中心群組網路

若要跨多個組織虛擬資料中心建立網路，請先分組虛擬資料中心，然後建立範圍限定為資料中心群組的 VDC 網路。

VMware Cloud Director 支援 NSX Data Center for vSphere 所支援的組織虛擬資料中心的資料中心群組網路，這些資料中心同時具有單一網路容錯網域的主動和待命出口點。

NSX Data Center for vSphere 支援的資料中心群組可擁有一般出口點組態、每個網路容錯網域的出口點組態或本機群組組態。

資料中心群組

資料中心群組充當虛擬資料中心群組路由器，可提供集中式網路管理、多個虛擬資料中心中多個出口點的組態，以及群組內所有網路之間的東西向流量。一個資料中心群組可以包含 1 個到 16 個虛擬資料中心，這些虛擬資料中心設定為共用多個出口點。資料中心群組可具有以下其中一個出口點組態：

表 5-3. NSX Data Center for vSphere 支援的資料中心群組的出口點組態類型

出口點組態類型	描述
一般出口點組態	您可以為資料中心群組設定具有一個主動出口點和一個待命出口點。這兩個出口點通用於資料中心群組中的所有網路容錯網域之間的所有參與虛擬資料中心。 具有此組態的資料中心群組可包含最多四個網路容錯網域中的資料中心。
每個容錯網域的出口點組態	對於資料中心群組中的每個網路容錯網域，可以為資料中心群組設定一個主動出口點和一個待命出口點。 具有此組態的資料中心群組可包含最多四個網路容錯網域中的資料中心。
本機群組組態	本機資料中心群組中的組織虛擬資料中心由單一 vCenter Server 執行個體所支援。對於單一網路容錯網域，可以為本機資料中心群組設定一個主動出口點和一個待命出口點。

一個組織可以有多個資料中心群組。一個組織虛擬資料中心可以參與多個資料中心群組。

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。

網路容錯網域

網路提供者範圍，通常表示有相關聯 NSX Manager 的基礎 vCenter Server 執行個體。

出口點

將資料中心群組或網路容錯網域連線至網際網路的 Edge 閘道。Edge 閘道必須屬於資料中心群組內的虛擬資料中心。系統將在代表出口點的 Edge 閘道和虛擬資料中心群組或網路容錯網域的通用路由器上設定 BGP 路由。Edge 閘道上的現有路由不受影響。

延伸網路

在資料中心群組中的所有虛擬資料中心之間延伸的第 2 層網路。只能是 IPv4。

管理具有 NSX Data Center for vSphere 網路提供者類型的資料中心群組

建立 NSX Data Center for vSphere 支援的資料中心群組後，您可以編輯資料中心群組的網路拓撲。您可以在該群組中新增和移除虛擬資料中心。您可以交換、取代以及移除出口點。您可以透過執行不同的同步工作來修正組態失敗。

無法將一般出口組態轉換為每個容錯網域的出口組態，反之亦然。

建立和設定具有一般出口組態且受 NSX Data Center for vSphere 支援的資料中心群組。

您可以建立和設定具有一般出口組態且受 NSX Data Center for vSphere 支援的虛擬資料中心群組，從而在該群組中為所有參與虛擬資料中心設定一對 Edge 閘道，分別作為主動和待命出口點。

必要條件

- 此作業需要**系統管理員**角色，或具有發佈給組織的 **VDC 群組：設定 VDC 群組**權限的角色。
- **系統管理員**必須啟用目標虛擬資料中心以取得跨虛擬資料中心網路。

程序

1. 建立具有一般出口組態且受 NSX Data Center for vSphere 支援的資料中心群組。
   您可以將 1 個到 16 個虛擬資料中心分組至一個具有一般出口組態的資料中心群組中。
2. 將主動出口點新增至具有 NSX Data Center for vSphere 網路提供者類型的資料中心群組
   若要將資料中心群組連線至網際網路，必須為其網路拓撲新增一個主動出口點。
3. 將待命出口點新增至具有 NSX Data Center for vSphere 網路提供者類型的資料中心群組
   在具有通用出口組態的虛擬資料中心群組中，您可以新增次要出口點並將其做為容錯案例中的待命出口點。

建立具有一般出口組態且受 NSX Data Center for vSphere 支援的資料中心群組。

您可以將 1 個到 16 個虛擬資料中心分組至一個具有一般出口組態的資料中心群組中。

程序

1 在頂部導覽列中，按一下**網路**，然後按一下**資料中心群組**索引標籤。

資料中心群組清單隨即顯示。

2 按一下**新增**。

3 在**起始 VDC** 頁面上，選取 VDC 以啟動 VDC 群組。

4 輸入新資料中心群組的名稱，並選擇性地輸入說明。

5 選取**一般出口點**，然後按**下一步**。

6 在**參與 VDC** 頁面上，為新的資料中心群組選取其他資料中心，然後按**下一步**。

資料中心頁面包含**系統管理員**針對跨虛擬資料中心網路啟用的 VDC 清單。

7 檢閱資料中心群組的詳細資料，然後按一下**完成**。

結果

新建立的虛擬資料中心群組會列在**資料中心群組**視圖中。

將主動出口點新增至具有 NSX Data Center for vSphere 網路提供者類型的資料中心群組

若要將資料中心群組連線至網際網路，必須為其網路拓撲新增一個主動出口點。

必要條件

系統管理員已在參與資料中心群組的任何一個虛擬資料中心上建立了至少一個 Edge 閘道。

程序

1 在頂部導覽列中，按一下**網路**，然後按一下**資料中心群組**索引標籤。

資料中心群組清單隨即顯示。

2 按一下目標資料中心群組。

此資料中心群組的**網路拓撲**視圖隨即開啟。目前網路拓撲的圖表顯示了參與 VDC 及其網路容錯網域、出口點 (如果已設定) 和流量路由。

3 按一下**新增出口點**。

新增主動出口點頁面隨即開啟，其中提供了屬於參與虛擬資料中心的 Edge 閘道的清單。

4 選取要做為此資料中心群組之主動出口點的 Edge 閘道，然後按一下**新增**。

結果

系統將在代表出口點的 Edge 閘道和虛擬資料中心群組的通用路由器上設定 BGP 路由。Edge 閘道上的現有路由不受影響。

網路拓撲圖會更新，以包含新增的出口點。從參與虛擬資料中心到網際網路的流量以藍色實線表示。

將待命出口點新增至具有 NSX Data Center for vSphere 網路提供者類型的資料中心群組

在具有通用出口組態的虛擬資料中心群組中，您可以新增次要出口點並將其做為容錯案例中的待命出口點。

必要條件

除了做為主動出口點的 Edge 閘道，您還必須在參與該群組的任何虛擬資料中心中至少再設定一個 Edge 閘道。

程序

1 在頂部導覽列中，按一下**網路**，然後按一下**資料中心群組**索引標籤。

資料中心群組清單隨即顯示。

2 按一下目標資料中心群組。

此資料中心群組的**網路拓撲**視圖隨即開啟。目前網路拓撲的圖表顯示了參與 VDC 及其網路容錯網域、出口點 (如果已設定) 和流量路由。

3 按一下**新增待命出口點**。

新增待命出口點頁面隨即開啟，其中提供了屬於參與虛擬資料中心之未使用的 Edge 閘道清單。將不會顯示正由此虛擬資料中心群組中的主動出口點使用的 Edge 閘道。

4 選取要做為此資料中心群組之待命出口點的 Edge 閘道，然後按一下**新增**。

結果

系統將在代表出口點的 Edge 閘道和網路容錯網域的通用路由器上設定 BGP 路由。此組態不會影響 Edge 閘道上的現有路由。

網路拓撲圖會更新，以包含新增的出口點。在容錯案例中，從參與虛擬資料中心到網際網路的流量以藍色虛線表示。

建立和設定具有容錯網域出口組態且受 NSX Data Center for vSphere 支援的資料中心群組。

您可以建立和設定具有容錯網域出口組態且受 NSX Data Center for vSphere 支援的虛擬資料中心群組，從而為群組中的每個網路容錯網域設定作為主動出口點的 Edge 閘道。無法在具有容錯網域出口組態的資料中心群組中建立待命出口。

必要條件

此作業需要**系統管理員**角色，或具有發佈給組織的 **VDC 群組：設定 VDC 群組**權限的角色。

程序

1 建立具有容錯網域出口組態且受 NSX Data Center for vSphere 支援的資料中心群組。

您可以將 1 個到 16 個虛擬資料中心分組至一個具有容錯網域出口組態且受 NSX Data Center for vSphere 支援的資料中心群組中。

2 為容錯網域新增出口點

若要將虛擬資料中心從 NSX Data Center for vSphere 所支援的資料中心群組中的網路容錯網域連線至網際網路，您必須為此網路容錯網域新增一個出口點。您可以向資料中心群組中的每個網路容錯網域新增一個出口點。具有容錯網域出口組態的資料中心群組不支援待命出口點。

建立具有容錯網域出口組態且受 NSX Data Center for vSphere 支援的資料中心群組。

您可以將 1 個到 16 個虛擬資料中心分組至一個具有容錯網域出口組態且受 NSX Data Center for vSphere 支援的資料中心群組中。

必要條件

系統管理員已為目標虛擬資料中心啟用跨虛擬資料中心網路。

程序

1 在頂部導覽列中，按一下**網路**，然後按一下**資料中心群組**索引標籤。

資料中心群組清單隨即顯示。

2 按一下**新增**。

3 輸入新資料中心群組的名稱，並選擇性地輸入說明。

4 選取**每個容錯網域的出口點**，然後按**下一步**。

5 在**參與 VDC** 頁面上，為新的資料中心群組選取其他資料中心，然後按**下一步**。

資料中心頁面包含**系統管理員**針對跨虛擬資料中心網路啟用的 VDC 清單。

6 檢閱資料中心群組的詳細資料，然後按一下**完成**。

結果

新建立的虛擬資料中心群組會列在**資料中心群組**視圖中。

為容錯網域新增出口點

若要將虛擬資料中心從 NSX Data Center for vSphere 所支援的資料中心群組中的網路容錯網域連線至網際網路，您必須為此網路容錯網域新增一個出口點。您可以向資料中心群組中的每個網路容錯網域新增一個出口點。具有容錯網域出口組態的資料中心群組不支援待命出口點。

必要條件

除了在此資料中心群組中做為出口點的 Edge 閘道，您還必須在任何參與虛擬資料中心中至少設定一個未使用的 Edge 閘道。

程序

1 在頂部導覽列中，按一下**網路**，然後按一下**資料中心群組**索引標籤。

資料中心群組清單隨即顯示。

2 按一下目標資料中心群組。

此資料中心群組的**網路拓撲**視圖隨即開啟。目前網路拓撲的圖表顯示了參與 VDC 及其網路容錯網域、出口點 (如果已設定) 和流量路由。

3 在網路拓撲圖中，按一下目標網路容錯網域。

網路容錯網域以實線表示，其名稱顯示在此圖的底部。

選取的容錯網域標記為藍色。

4 按一下**新增出口點**。

新增主動出口點頁面隨即開啟，其中提供了屬於參與虛擬資料中心的 Edge 閘道的清單。

5 選取要做為此容錯網域之出口點的 Edge 閘道，然後按一下**新增**。

結果

系統將在代表出口點的 Edge 閘道和網路容錯網域的通用路由器上設定 BGP 路由。Edge 閘道上的現有路由不受影響。

網路拓撲圖會更新，以包含新增的出口點。從網路容錯網域中的虛擬資料中心到網際網路的流量以連續的藍線表示。

建立和設定具有 NSX Data Center for vSphere 網路提供者類型的本機虛擬資料中心群組

從 10.1 版開始，VMware Cloud Director 支援同時具有單一網路容錯網域之主動和待命出口點且受 NSX Data Center for vSphere 支援的資料中心群組。

本機群組中的組織虛擬資料中心由單一 vCenter Server 執行個體所支援。

在本機資料中心群組中，您可以設定一對 Edge 閘道 (一個主動出口點和一個待命出口點)，以支援同一網路容錯網域中的高可用性和災難復原案例。

必要條件

此作業需要**系統管理員**角色，或具有發佈給組織的 **VDC 群組：設定 VDC 群組**權限的角色。

程序

1 建立具有 NSX Data Center for vSphere 網路提供者類型的本機資料中心群組

您可以將 1 個到 16 個虛擬資料中心 (VDC) 分組至一個具有容錯網域出口組態且受 NSX Data Center for vSphere 支援的資料中心群組中。

2 為具有 NSX Data Center for vSphere 網路提供者類型的本機資料中心群組新增主動出口點

若要將 NSX Data Center for vSphere 支援的本機資料中心群組中的資料中心連線至網際網路，您必須向網路容錯網域新增一個主動出口點。

3 為具有 NSX Data Center for vSphere 網路提供者類型的本機資料中心群組新增待命出口點

在本機資料中心群組組態中，您可以新增次要出口點以做為容錯案例中的待命出口點。

建立具有 NSX Data Center for vSphere 網路提供者類型的本機資料中心群組

您可以將 1 個到 16 個虛擬資料中心 (VDC) 分組至一個具有容錯網域出口組態且受 NSX Data Center for vSphere 支援的資料中心群組中。

必要條件

系統管理員已為目標虛擬資料中心啟用跨虛擬資料中心網路。

程序

1. 在頂部導覽列中，按一下**網路**，然後按一下**資料中心群組**索引標籤。

   資料中心群組清單隨即顯示。

2. 按一下**新增**。
3. 在**起始 VDC** 頁面上，選取 VDC 以啟動 VDC 群組。
4. 輸入新資料中心群組的名稱，並選擇性地輸入說明。
5. 若要建立僅包含單一網路容錯網域中的虛擬資料中心的群組，請開啟**建立本機群組**選項。
6. 按**下一步**。
7. 在**參與 VDC** 頁面上，為新的資料中心群組選取其他資料中心，然後按**下一步**。

   資料中心頁面包含**系統管理員**針對跨虛擬資料中心網路啟用的 VDC 清單。

8. 檢閱資料中心群組的詳細資料，然後按一下**完成**。

結果

新建立的虛擬資料中心群組會顯示在**資料中心群組**視圖中。

為具有 NSX Data Center for vSphere 網路提供者類型的本機資料中心群組新增主動出口點

若要將 NSX Data Center for vSphere 支援的本機資料中心群組中的資料中心連線至網際網路，您必須向網路容錯網域新增一個主動出口點。

程序

1. 在頂部導覽列中，按一下**網路**，然後按一下**資料中心群組**索引標籤。

   資料中心群組清單隨即顯示。

2. 按一下目標資料中心群組。

   此資料中心群組的**網路拓撲**視圖隨即開啟。目前網路拓撲的圖表顯示了參與 VDC 及其網路容錯網域、出口點 (如果已設定) 和流量路由。

3. 按一下**新增出口點**。
4. 從屬於參與虛擬資料中心的 Edge 閘道清單中，選取要充當資料中心群組之主動出口點的 Edge 閘道，然後按一下**新增**。

結果

系統將在代表出口點的 Edge 閘道和網路容錯網域的通用路由器上設定 BGP 路由。此組態不會影響 Edge 閘道上的現有路由。

新增的主動出口點會顯示在網路拓撲圖中。藍色實線表示從網路容錯網域中的虛擬資料中心到網際網路的流量。

後續步驟

若要允許出口點容錯，請為本機資料中心群組新增一個待命出口點。

為具有 NSX Data Center for vSphere 網路提供者類型的本機資料中心群組新增待命出口點

在本機資料中心群組組態中，您可以新增次要出口點以做為容錯案例中的待命出口點。

必要條件

除了作為主動出口點的 Edge 閘道，您還必須在參與本機資料中心群組的任何虛擬資料中心中至少再設定一個 Edge 閘道。

程序

1 在頂部導覽列中，按一下**網路**，然後按一下**資料中心群組**索引標籤。

資料中心群組清單隨即顯示。

2 按一下目標資料中心群組。

此資料中心群組的**網路拓撲**視圖隨即開啟。目前網路拓撲的圖表顯示了參與 VDC 及其網路容錯網域、出口點 (如果已設定) 和流量路由。

3 按一下**新增待命出口點**。

新增待命出口點頁面隨即開啟，其中提供了屬於參與虛擬資料中心之未使用的 Edge 閘道清單。將以灰色顯示正由此虛擬資料中心群組中的主動出口點使用的 Edge 閘道。

4 選取要做為此資料中心群組之待命出口點的 Edge 閘道，然後按一下**新增**。

結果

系統將在代表出口點的 Edge 閘道和網路容錯網域的通用路由器上設定 BGP 路由。此組態不會影響 Edge 閘道上的現有路由。

新增的出口點會顯示在網路拓撲圖中。藍色虛線表示 Fault Tolerance 案例中從參與虛擬資料中心到網際網路的流量。

檢視具有 NSX Data Center for vSphere 網路提供者類型的資料中心群組

您可以檢視組織中的資料中心群組，以及有關其目前組態的詳細資料。

必要條件

此作業需要**系統管理員**角色，或具有發佈給組織的 **VDC 群組：檢視 VDC 群組**權限的角色。

程序

1 在頂部導覽列中，按一下**網路**，然後按一下**資料中心群組**索引標籤。

資料中心群組清單隨即顯示。

2 按一下目標資料中心群組。

此資料中心群組的**網路拓撲**視圖隨即開啟。目前網路拓撲的圖表顯示了參與 VDC 及其網路容錯網域、出口點 (如果已設定) 和流量路由。

將虛擬資料中心新增至具有 NSX Data Center for vSphere 網路提供者類型的資料中心群組

您可以將虛擬資料中心新增至資料中心群組，以便將現有網路延伸至新的虛擬資料中心。

必要條件

- 此作業需要**系統管理員**角色，或具有發佈給組織的 **VDC 群組：設定 VDC 群組**權限的角色。
- 資料中心群組包含的虛擬資料中心不超過四個。

程序

1 在頂部導覽列中，按一下**網路**，然後按一下**資料中心群組**索引標籤。

資料中心群組清單隨即顯示。

2 按一下目標資料中心群組。

此資料中心群組的**網路拓撲**視圖隨即開啟。目前網路拓撲的圖表顯示了參與 VDC 及其網路容錯網域、出口點 (如果已設定) 和流量路由。

3 按一下**新增資料中心**。

4 在**資料中心**頁面上，選取要新增至資料中心群組的資料中心，然後按一下**完成**。

資料中心頁面包含系統管理員針對跨虛擬資料中心網路啟用的虛擬資料中心清單。

備註 一個資料中心群組最多只能包含四個虛擬資料中心。

從具有 NSX Data Center for vSphere 網路提供者類型的資料中心群組移除虛擬資料中心

您可以從資料中心群組移除虛擬資料中心，以便不會延伸此虛擬資料中心中的現有網路。

必要條件

- 此作業需要**系統管理員**角色，或具有發佈給組織的 **VDC 群組：設定 VDC 群組**權限的角色。
- 資料中心群組必須至少包含三個虛擬資料中心。
- 您想移除的虛擬資料中心不得向資料中心群組提供出口點。

程序

1 在頂部導覽列中，按一下**網路**，然後按一下**資料中心群組**索引標籤。

資料中心群組清單隨即顯示。

2 按一下目標資料中心群組。

此資料中心群組的**網路拓撲**視圖隨即開啟。目前網路拓撲的圖表顯示了參與 VDC 及其網路容錯網域、出口點 (如果已設定) 和流量路由。

3 在目標虛擬資料中心的卡的右上角，按一下三個點，然後按一下**移除**。

4 按一下**移除**以確認。

結果

此虛擬資料中心會從資料中心群組的網路拓撲圖中移除。

同步具有 NSX Data Center for vSphere 網路提供者類型的資料中心群組

若要重新套用資料中心群組的網路組態，並確保所有參與的虛擬資料中心都處於作用中狀態，您可以同步該資料中心群組。

備註 在資料中心群組同步程序中，由於通用路由器會在 NSX 中進行同步，因此資料中心群組會有幾秒無法使用。

必要條件

此作業需要**系統管理員**角色，或具有發佈給組織的 **VDC 群組：設定 VDC 群組**權限的角色。

程序

1 在頂部導覽列中，按一下**網路**，然後按一下**資料中心群組**索引標籤。

資料中心群組清單隨即顯示。

2 按一下目標資料中心群組。

此資料中心群組的**網路拓撲**視圖隨即開啟。目前網路拓撲的圖表顯示了參與 VDC 及其網路容錯網域、出口點 (如果已設定) 和流量路由。

3 按一下**同步資料中心群組**。

4 按一下**確定**以確認。

交換具有 NSX Data Center for vSphere 網路提供者類型和一般出口組態的資料中心群組中的出口點

在具有一般出口組態的資料中心群組中設定主動和待命出口點後，您可以交換這些出口點的角色。主動出口點可以成為待命出口點，待命出口點也可以成為主動出口點。

必要條件

此作業需要**系統管理員**角色，或具有發佈給組織的 **VDC 群組：設定 VDC 群組**權限的角色。

程序

1 在頂部導覽列中，按一下**網路**，然後按一下**資料中心群組**索引標籤。

資料中心群組清單隨即顯示。

2 按一下目標資料中心群組。

此資料中心群組的**網路拓撲**視圖隨即開啟。目前網路拓撲的圖表顯示了參與 VDC 及其網路容錯網域、出口點 (如果已設定) 和流量路由。

3 按一下**交換出口點**。

4 按一下**確定**以確認。

結果

此時，網路拓撲圖會使用新流量路由進行更新。網際網路的流量現在會被重新導向至新的主動出口點。

取代具有 NSX Data Center for vSphere 網路提供者類型之資料中心群組的出口點的 Edge 閘道

您可以取代代表資料中心群組中主動或待命出口點的 Edge 閘道。

必要條件

- 此作業需要**系統管理員**角色，或具有發佈給組織的 **VDC 群組：設定 VDC 群組**權限的角色。
- 新的 Edge 閘道不得由資料中心群組中的其他出口點使用。

程序

1 在頂部導覽列中，按一下**網路**，然後按一下**資料中心群組**索引標籤。

資料中心群組清單隨即顯示。

2 按一下目標資料中心群組。

此資料中心群組的**網路拓撲**視圖隨即開啟。目前網路拓撲的圖表顯示了參與 VDC 及其網路容錯網域、出口點 (如果已設定) 和流量路由。

3 如果您要取代網路拓撲圖上網路容錯網域組態中的出口點，請選取目標出口點的網路容錯網域。

網路容錯網域使用實線表示，網域名稱顯示在圖的底部。

選取的網路容錯網域標記為藍色。

4 在目標出口點的卡的右上角，按一下三個點，然後按一下**取代**。

此時將開啟**取代出口點**頁面，其中顯示了屬於參與虛擬資料中心的 Edge 閘道清單。

5 選取此新 Edge 閘道，然後按一下**取代**。

結果

BGP 路由將從舊 Edge 閘道移除，並在代表出口點的新 Edge 閘道和虛擬資料中心群組的通用路由器上設定。

網路拓撲圖會使用新的 Edge 閘道的名稱進行更新。

從具有 NSX Data Center for vSphere 網路提供者類型的資料中心群組移除出口點

若要將資料中心群組或網路容錯網域與網際網路中斷連線，您可以移除其出口點。

必要條件

- 此作業需要**系統管理員**角色，或具有發佈給組織的 **VDC 群組：設定 VDC 群組**權限的角色。
- 如果您要移除與待命出口點配對的主動出口點，則必須交換這些出口點或移除待命出口點。

程序

1. 在頂部導覽列中，按一下**網路**，然後按一下**資料中心群組**索引標籤。

   資料中心群組清單隨即顯示。

2. 按一下目標資料中心群組。

   此資料中心群組的**網路拓撲**視圖隨即開啟。目前網路拓撲的圖表顯示了參與 VDC 及其網路容錯網域、出口點 (如果已設定) 和流量路由。

3. 如果您要從網路拓撲圖上的網路容錯網域組態中移除某個出口點，請選取該目標出口點的網路容錯網域。

   網路容錯網域使用實線表示，網域名稱顯示在圖的底部。

   選取的網路容錯網域標記為藍色。

4. 在目標出口點的卡的右上角，按一下三個點，然後按一下**刪除**。
5. 按一下**確定**以確認。

結果

如果代表出口點的 Edge 閘道未由其他通用路由器使用，將從中移除 BGP 路由。

此出口點會從網路拓撲圖中移除。

同步具有 NSX Data Center for vSphere 網路提供者類型的資料中心群組的路由和出口點

透過同步路由，您可以將動態路由組態重新套用至資料中心群組或網路容錯網域及其相關聯的出口點。透過同步某個出口點，您可以確保該出口點正確連線至資料中心群組。

必要條件

- 此作業需要**系統管理員**角色，或具有發佈給組織的 **VDC 群組：設定 VDC 群組**權限的角色。
- 您已為目標資料中心群組或網路容錯網域設定出口點。

程序

1. 在頂部導覽列中，按一下**網路**，然後按一下**資料中心群組**索引標籤。

   資料中心群組清單隨即顯示。

2 按一下目標資料中心群組。

此資料中心群組的**網路拓撲**視圖隨即開啟。目前網路拓撲的圖表顯示了參與 VDC 及其網路容錯網域、出口點 (如果已設定) 和流量路由。

3 如果您想要在網路拓撲圖上同步資料中心群組中的網路容錯網域，請選取目標網路容錯網域。

網路容錯網域使用實線表示，網域名稱顯示在圖的底部。

選取的網路容錯網域標記為藍色。

4 若要將動態路由組態重新套用到群組或網路容錯網域及其相關聯的出口點，請按一下**同步路由**，然後按一下**確定**。

5 若要將出口點與其資料中心群組進行同步，請在目標出口點的卡的右上角，按一下三個點，再依序按一下**同步**和**確定**。

管理 NSX Data Center for vSphere 支援的資料中心群組網路

建立並設定資料中心群組後，您可以建立和管理跨越參與虛擬資料中心的第 2 層 VDC 群組網路。

新增 NSX Data Center for vSphere 支援的 VDC 群組網路

您可以建立跨越參與資料中心群組之所有虛擬資料中心的 VDC 群組網路。

您只能新增 NSX Data Center for vSphere 所支援的 IPv4 資料中心群組網路。

必要條件

此作業需要預先定義的**組織管理員**角色，或具有**組織 VDC 網路：編輯內容**權限的角色。

程序

1 在頂部導覽列中，按一下**網路**。

2 在**網路**索引標籤上，按一下**新增**。

3 在**範圍**頁面上，選取**資料中心群組**，然後選取要在其中建立網路的 NSX Data Center for vSphere 所支援的資料中心群組，然後按**下一步**。

4 為網路輸入有意義的名稱。

5 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**。

6 輸入組織 VDC 網路的說明。

7 按**下一步**。

8 檢閱設定，然後按一下**完成**。

結果

您可以在組織的網路清單中看到此新建立的資料中心群組網路。

其網路類型會列為跨 VDC。

將為每個參與虛擬資料中心建立跨 VDC 路由類型的組織虛擬資料中心網路。透過按一下參與虛擬資料中心的卡，然後按一下**網路**，即可查看參與虛擬資料中心的 VDC 群組網路。如果虛擬機器或 vApp 連線到此類組織虛擬資料中心網路，此虛擬機器或 vApp 將連線至 VDC 群組網路。

後續步驟

對於每個對應的跨 VDC 組織虛擬資料中心網路，您可以指派靜態 IP 位址和 IP 集區。請參閱將 IP 位址新增至組織虛擬資料中心網路 IP 集區。

對於連結至 VDC 群組網路的虛擬機器的 DNS 和 DHCP 組態，您可以使用 VMware Cloud Director OpenAPI。若要檢查 VMware Cloud Director OpenAPI 說明文件，請前往 `https://Cloud_Director_IP_address_or_host_name/docs`。若要檢視程式碼範例並測試 VMware Cloud Director OpenAPI 呼叫，請前往 `https://Cloud_Director_IP_address_or_host_name/api-explorer?scope=organization_name`。

檢視或編輯 NSX Data Center for vSphere 支援的資料中心群組網路

您可以檢視 NSX Data Center for vSphere 支援的資料中心群組網路的名稱、說明和 CIDR 設定。只能編輯 NSX Data Center for vSphere 支援的資料中心群組網路的名稱和說明。

如需在虛擬資料中心層級編輯資料中心群組網路之靜態 IP 集區配置的相關資訊，請參閱將 IP 位址新增至組織虛擬資料中心網路 IP 集區。

必要條件

確認您已獲指派預先定義的**組織管理員**角色，或包含**組織 VDC 網路：檢視內容**和**組織 VDC 網路：編輯內容**權限的角色。

程序

1. 在頂部導覽列中，按一下**網路**。
2. 按一下目標網路以檢視其詳細資料。
3. 若要編輯網路的名稱和說明，請按一下**編輯**。
4. 編輯網路詳細資料，然後按一下**儲存**。

同步 NSX Data Center for vSphere 支援的資料中心群組網路

為了確保所有參與的虛擬資料中心均可存取 NSX Data Center for vSphere 支援的資料中心群組網路，您可以同步資料中心群組網路。

必要條件

此作業需要預先定義的**組織管理員**角色，或具有**組織 VDC 網路：編輯內容**權限的角色。

程序

1. 在頂部導覽列中，按一下**網路**。
2. 在 [網路] 索引標籤中，選取目標網路名稱旁的選項按鈕，然後按一下**同步**。
3. 按一下**確定**以確認。

管理 NSX Data Center for vSphere Edge 閘道服務

VMware Cloud Director 提供由 NSX Data Center for vSphere 網路虛擬化軟體支援的進階網路功能，可在雲端環境中提供增強的安全性控制以及路由和網路調整功能。

使用這些網路功能，在組織虛擬資料中心內可以實現前所未有的安全性和隔離。這些功能提供下列優點：

- 動態路由。VMware Cloud Director 環境中的 NSX Data Center for vSphere 功能支援邊界閘道協定 (BGP) 和先開啟最短的路徑 (OSPF) 等路由通訊協定，以簡化系統之間的網路整合，從而在雲端主控的應用程式部署中提供備援和持續性。
- 更為精細的網路安全性與隔離。VMware Cloud Director 環境中的 NSX Data Center for vSphere 功能支援使用以物件為基礎的規則定義，以提供可設定狀態的網路流量隔離，且不需要多個虛擬網路。如果應用程式或虛擬機器受到危及，此零信任安全性模型可防止侵入者取得完整網路存取權。透過使用相同的網路安全性原則簡化網路組態，可保護應用程式 (無論其實際位於 VMware Cloud Director 環境中的何處) 並可擴充零信任安全性模型以取得可攜式安全性 (無論在何處部署應用程式)。
- 由 NSX Data Center for vSphere 提供的其他功能包括點到站台 (IPsec VPN) 和使用者 (SSL VPN-Plus) 連線的增強型 VPN 支援、HTTPS 的增強型負載平衡，以及擴充的網路延展性。

您可以設定兩種類型的防火牆：Edge 閘道防火牆和 Distributed Firewall。如需有關這些防火牆之間的差異的詳細資訊，請參閱 NSX Data Center for vSphere 的租用戶防火牆組態。

您可以使用 VMware Cloud Director 租用戶入口網站或 VMware Cloud Director Service Provider Admin Portal 存取這些進階網路功能。必須先將 Edge 閘道轉換為進階 Edge 閘道。請參閱將 NSX Data Center for vSphere Edge 閘道轉換為進階 Edge 閘道。

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

NSX Data Center for vSphere 的 VMware Cloud Director 進階網路入門

您可以使用 VMware Cloud Director 進階網路在 VMware Cloud Director 系統中的組織上執行管理工作。您可以管理分散式防火牆以及 NSX Data Center for vSphere 所提供的其他進階網路功能 (由 VMware Cloud Director 系統管理員提供給組織)。

NSX Data Center for vSphere 提供的進階網路的一般使用者包括：

- VMware Cloud Director **系統管理員**，可能會使用租用戶入口網站來為組織設定分散式防火牆和其他進階網路功能。
- **組織管理員**，使用租用戶入口網站來管理分散式防火牆以及**系統管理員**提供給該組織的其他進階網路功能。

NSX Data Center for vSphere 的租用戶防火牆組態

使用租用戶入口網站，您可以設定由 VMware Cloud Director 組織虛擬資料中心內的 NSX Data Center for vSphere 所提供的防火牆功能。您可以建立分散式防火牆的防火牆規則，在組織虛擬資料中心內的虛

擬機器與要套用至 Edge 閘道防火牆的防火牆規則之間提供安全性，以防組織虛擬資料中心內的虛擬機器傳入外部網路流量。

備註 租用戶入口網站提供設定 Edge 閘道防火牆和分散式防火牆的功能。

NSX Data Center for vSphere 邏輯防火牆技術包含兩個元件來處理不同的部署使用案例。Edge 閘道防火牆的重點在於南北向流量強制執行，而分散式防火牆著重於東西向存取控制。

Edge 閘道防火牆和分散式防火牆之間的主要差異

Edge 閘道防火牆會監控南北向流量，以提供周邊安全性功能，包括防火牆、網路位址轉譯 (NAT) 以及站台間 IPSec 與 SSL VPN 功能。

分散式防火牆提供用於隔離並保護每個虛擬機器和應用程式安全 (直至第 2 層 (L2)) 的功能。有效地設定分散式防火牆可以隔離任何外部或內部網路安全性危害，從而隔離位於相同網路區段上的虛擬機器之間的東西向流量。安全性原則可集中管理、繼承和嵌套，以便網路和安全管理員可進行大規模管理。此外，一旦部署已定義的安全性原則，它們便會跟隨虛擬機器或應用程式在不同的虛擬資料中心之間移動。

關於防火牆規則

如相關產品說明文件中所述，在 NSX Data Center for vSphere 中，集中式層級上所定義的防火牆規則稱為預先規則。您也可以在個別 Edge 閘道層級中新增規則，這些規則稱為本機規則。

在資料表中將後續規則向下移動之前，系統會對防火牆資料表中的頂端規則檢查每一個流量工作階段。系統會強制執行資料表中符合流量參數的第一個規則。規則按以下順序顯示：

1. 使用者定義的預先規則具有最高優先順序，並針對每個虛擬 NIC 層級優先順序以從上到下的順序強制執行。
2. 自動探索的規則 (可控制 Edge 閘道服務的流量流動的規則)。
3. 在 Edge 閘道層級定義的本機規則。
4. 預設分散式防火牆規則

如需有關 NSX Data Center for vSphere 軟體如何強制執行防火牆規則的詳細資訊，請參閱 NSX Data Center for vSphere 說明文件中的〈變更防火牆規則的順序〉。

NSX Data Center for vSphere Edge 閘道防火牆

Edge 閘道防火牆可協助您滿足主要周邊安全性需求，例如根據 IP/VLAN 建構建立 DMZ、多承租人虛擬資料中心中的租用戶間隔離、網路位址轉譯 (NAT)、合作夥伴 (外部網路) VPN 和以使用者為基礎的 SSL VPN。

VMware Cloud Director 環境中的 Edge 閘道防火牆功能由 NSX Data Center for vSphere 提供。在 NSX Data Center for vSphere 中，此防火牆功能亦稱為 Edge 防火牆。Edge 閘道防火牆會監控南北向流量，以提供周邊安全性功能，包括防火牆、網路位址轉譯 (NAT) 以及站台間 IPSec 與 SSL VPN 功能。

如需有關 NSX Data Center for vSphere 的 Edge 閘道防火牆所提供功能的更多詳細資訊，請參閱 NSX Data Center for vSphere 說明文件。

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，請參閱使用租用戶入口網站管理 NSX Data Center for vSphere 分散式防火牆規則。

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。

將 NSX Data Center for vSphere Edge 閘道轉換為進階 Edge 閘道

若要使用租用戶入口網站中的 NSX Data Center for vSphere Edge 閘道，您需要將其轉換為進階 Edge 閘道。一旦將其轉換為進階 Edge 閘道，您可以使用租用戶入口網站設定 NSX Data Center for vSphere 針對這些進階 Edge 閘道所提供的靜態和動態路由功能。

必要條件

您具有現有的 Edge 閘道。

程序

1 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**索引標籤。

2 選取要編輯的 Edge 閘道。

3 按一下**轉換成進階**。

結果

Edge 閘道隨即轉換為進階 Edge 閘道。

後續步驟

一旦轉換為進階 Edge 閘道，您可以透過選取閘道並按一下**服務**進行設定。

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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。

b 選取要編輯的 Edge 閘道，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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。

   b 選取要編輯的 Edge 閘道，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**。

NSX Data Center for vSphere 分散式防火牆

分散式防火牆可讓您根據虛擬機器名稱和屬性，分割組織虛擬資料中心實體，例如虛擬機器。

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。如 NSX Data Center for vSphere 說明文件中所述，此分散式防火牆是 Hypervisor 核心內嵌防火牆，可提供對虛擬化工作負載和網路的可見度與控制。您可以根據虛擬機器名稱等物件以及 IP 位址或 IP 集位址等網路建構，建立存取控制原則。防火牆規則會在每個虛擬機器的 vNIC 層級強制執行，以提供一致的存取控制，即使 vSphere vMotion 將虛擬機器移至新的 ESXi 主機。此分散式防火牆支援可在近線速率處理時檢查東西向流量的微分割安全性模型。

如 NSX Data Center for vSphere 說明文件中所述，對於第 2 層 (L2) 封包，分散式防火牆會建立快取以提升效能。第 3 層 (L3) 封包按下列順序進行處理：

1 檢查所有封包的現有狀態。

2 找到狀態相符項時，會處理封包。

3 找不到狀態相符項時，會透過規則處理封包，直到找到相符項。

- 對於 TCP 封包，僅針對具有 SYN 旗標的封包設定狀態。但是，未指定通訊協定 (服務 ANY) 的規則可以符合具有任意旗標組合的 TCP 封包。
- 對於 UDP 封包，會從封包擷取 5 元組詳細資料。如果狀態資料表中不存在狀態，會使用擷取的 5 元組詳細資料建立新狀態。後續接收的封包會根據剛建立的狀態進行比對。
- 對於 ICMP 封包，ICMP 類型、代碼和封包方向會用來建立狀態。

分散式防火牆同時有助於建立身分識別型規則。管理員可以根據使用者的群組成員資格 (如企業 Active Directory (AD) 中所定義)，強制執行存取控制。可以使用身分識別型防火牆規則的一些使用案例如下：

- 使用者使用膝上型電腦或行動裝置存取虛擬應用程式，其中 AD 用於使用者驗證
- 使用者使用 VDI 基礎結構存取虛擬應用程式，其中虛擬機器以 Microsoft Windows 為基礎

如需有關分散式防火牆所提供功能的更多詳細資訊，請參閱 NSX Data Center for vSphere 說明文件。

在 NSX Data Center for vSphere 支援的組織虛擬資料中心上啟用分散式防火牆

在您可以使用租用戶入口網站以搭配使用組織虛擬資料中心上 NSX Data Center for vSphere 提供的分散式防火牆功能之前，必須為組織虛擬資料中心啟用分散式防火牆。VMware Cloud Director 系統管理員或被授與 **org_vdc_distributed_firewall_enable** 權限的使用者，可以在組織虛擬資料中心上啟用分散式防火牆。

您可以使用租用戶入口網站中的 [分散式防火牆] 畫面，為組織虛擬資料中心啟用分散式防火牆。

必要條件

確認組織虛擬資料中心所屬的組織指派有下列權限：

- 組織 vDC 分散式防火牆：啟用/停用
- 組織 vDC 分散式防火牆：設定規則
- 組織 vDC 分散式防火牆：檢視規則

VMware Cloud Director **系統管理員**會指派權限給組織。使用租用戶入口網站中的使用者介面啟用分散式防火牆時，需要「組織 vDC 分散式防火牆：啟用/停用」權限。在租用戶入口網站中檢視防火牆規則時，需要「組織 vDC 分散式防火牆：檢視規則」權限；使用租用戶入口網站設定防火牆規則時，需要「組織 vDC 分散式防火牆：設定規則」權限。

確認您具有授與您「組織 vDC 分散式防火牆：啟用/停用」權限的已指派角色。在 VMware Cloud Director 系統之預先定義的角色中，預設只有系統管理員角色擁有該權限。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後在**網路**下，選取**安全性**。

2 選取您想要設定分散式防火牆規則的組織虛擬資料中心。

3 按一下**設定服務**。

4 在**分散式防火牆**索引標籤上啟用分散式防火牆。

後續步驟

如需預設分散式防火牆規則的描述，請參閱使用租用戶入口網站管理 NSX Data Center for vSphere 分散式防火牆規則。

使用租用戶入口網站管理 NSX Data Center for vSphere 分散式防火牆規則

如 NSX Data Center for vSphere 說明文件中所述，預設防火牆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。在 VMware Cloud Director Tenant Portal 中，預設分散式防火牆規則標示為「預設允許規則」。

分散式防火牆功能必須在組織虛擬資料中心上啟用，您才能使用 VMware Cloud Director Tenant Portal 管理分散式防火牆設定。

預設分散式防火牆規則設定為允許所有第 3 層和第 2 層流量通過組織虛擬資料中心。此設定由使用者介面之 [動作] 資料行中所設定的 [允許] 指示。預設規則一律位於 [規則] 資料表的底部。

重要 您無法刪除或修改預設的分散式防火牆規則。

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

- 在 NSX Data Center for vSphere 支援的組織虛擬資料中心上啟用分散式防火牆
- 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 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後在**網路**下，選取**安全性**。

2 選取您想要修改防火牆規則的安全性服務 VDC 網路，然後按一下**設定服務**。

[安全性服務] 畫面隨即顯示。

3 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。

4 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。

5 按一下**名稱**儲存格，然後輸入名稱。

6 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。

7 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。

8 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**。

9 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。

10 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。

11 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。

12 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。

13 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 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後在**網路**下，選取**安全性**。

2 選取您想要修改防火牆規則的安全性服務 VDC 網路，然後按一下**設定服務**。

[安全性服務] 畫面隨即顯示。

3 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。

4 按一下**儲存變更**。

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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。

   b 選取要編輯的 Edge 閘道，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。

選項	描述
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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。

b 選取要編輯的 Edge 閘道，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。

選項	描述
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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。

   b 選取要編輯的 Edge 閘道，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**。

管理 NSX Data Center for vSphere Edge 閘道上的網路位址轉譯

VMware Cloud Director 環境中的 NSX Data Center for vSphere 軟體可使 Edge 閘道提供網路位址轉譯 (NAT) 服務。出於經濟和安全性目的，使用此功能可減少組織必須使用的公用 IP 位址數目。

Edge 閘道的 NAT 服務提供將公用位址指派給虛擬機器或私人網路中之虛擬機器群組的功能。若要使您的 Edge 閘道提供對執行於組織虛擬資料中心內私下定址的虛擬機器之服務的存取權，您必須在 Edge 閘道上設定 NAT 規則。在大多數情況下，需將 NAT 服務與 VMware Cloud Director 環境中 Edge 閘道上的上行介面建立關聯，以便組織虛擬資料中心網路上的位址不會在外部網路上公開。

NAT 服務組態分為來源 NAT (SNAT) 和目的地 NAT (DNAT) 規則。在 VMware Cloud Director 環境中的 Edge 閘道上設定 SNAT 或 DNAT 規則時，一律從組織虛擬資料中心的角度來設定規則。具體來說，這表示您可以透過下列方式設定規則：

- SNAT：流量從組織虛擬資料中心之內部網路上的虛擬機器 (來源)，通過網際網路傳輸至外部網路 (目的地)。SNAT 規則會轉譯組織虛擬資料中心網路的傳出封包 (傳送至外部網路或另一個組織虛擬資料中心網路) 的來源 IP 位址。
- DNAT：流量從網際網路 (來源) 傳輸至組織虛擬資料中心內的虛擬機器 (目的地)。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。

您可以設定 NAT 規則，以在組織虛擬資料中心內部建立私人 IP 位址空間。此組態提供將私人 IP 位址空間從一個組織虛擬資料中心移植到另一個組織虛擬資料中心的功能。透過設定 NAT 規則，可讓您為某個組織虛擬資料中心內的虛擬機器使用曾在另一個組織虛擬資料中心使用的相同私人 IP 位址。

VMware Cloud Director 環境中的 NAT 規則功能支援：

- 在私人 IP 位址空間內建立子網路
- 為 Edge 閘道建立多個私人 IP 位址空間
- 在多個 Edge 閘道介面上設定多個 NAT 規則

重要 您必須在 Edge 閘道上設定防火牆和 NAT 規則，才能使 Edge 閘道網路上的虛擬機器可供存取。依預設，Edge 閘道已部署防火牆規則，這些規則設定為拒絕 Edge 閘道網路上虛擬機器的所有傳入和傳出網路流量。此外，NAT 在 Edge 閘道上預設為停用，以便 Edge 閘道無法轉譯傳入和傳出流量的 IP 位址，除非您在 Edge 閘道上設定 NAT。在設定 NAT 規則後嘗試對網路上的虛擬機器執行 Ping 動作會失敗，除非您新增防火牆規則以允許對應流量。

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. 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。
   b. 選取要編輯的 Edge 閘道，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。
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。

選項	描述
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。

NSX Data Center for vSphere Edge 閘道的進階路由組態

可以在 NSX Data Center for vSphere Edge 閘道上設定靜態和動態路由。

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 Data Center for vSphere 提供的路由功能的詳細資訊，請參閱 NSX Data Center for vSphere 說明文件。

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 Data Center for vSphere 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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。

   b 選取要編輯的 Edge 閘道，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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。

   b 選取要編輯的 Edge 閘道，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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。

   b 選取要編輯的 Edge 閘道，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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。

b 選取要編輯的 Edge 閘道，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。
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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。

   b 選取要編輯的 Edge 閘道，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**。

NSX Data Center for vSphere 的負載平衡

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。負載平衡可提供應用程式高可用性並協助達到最佳的資源使用率、最大化輸送量、最小化回應時間並避免超載。

關於負載平衡

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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。

   b 選取要編輯的 Edge 閘道，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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。

   b 選取要編輯的 Edge 閘道，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。

選項	描述
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。
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。

選項	描述
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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。

b 選取要編輯的 Edge 閘道，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 5-4. HTTP/HTTPS 通訊協定的延伸

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

表 5-4. HTTP/HTTPS 通訊協定的延伸 (續)

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

表 5-5. 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 5-6. 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)。

表 5-6. TCP 通訊協定的延伸 (續)

監控器延伸	描述
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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。

   b 選取要編輯的 Edge 閘道，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。

選項	描述
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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。

b 選取要編輯的 Edge 閘道，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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。

b 選取要編輯的 Edge 閘道，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。

選項	描述
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

在 NSX Data Center for vSphere Edge 閘道上使用 VPN 設定安全存取

您可以設定由 NSX Data Center for vSphere Edge 閘道上的 NSX Data Center for vSphere 軟體提供的 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 NSX Data Center for vSphere Edge 閘道上的 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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。

b 選取要編輯的 Edge 閘道，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。
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。
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。

選項	動作
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。
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。
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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。

b 選取要編輯的 Edge 閘道，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 開啟 Edge 閘道服務。

   a 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。

   b 選取要編輯的 Edge 閘道，然後按一下**服務**。

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

3 按一下**新增** () 按鈕。

4 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`。

選項	動作
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。
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。

5 按一下**保留**。

6 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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。

   b 選取要編輯的 Edge 閘道，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 NSX Data Center for vSphere 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。

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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。

b 選取要編輯的 Edge 閘道，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。

NSX Data Center for vSphere Edge 閘道上的 SSL 憑證管理

VMware Cloud Director 環境中的 NSX Data Center for vSphere 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 Data Center for vSphere 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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。

   b 選取要編輯的 Edge 閘道，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。 **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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。
   b 選取要編輯的 Edge 閘道，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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。

   b 選取要編輯的 Edge 閘道，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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。

b 選取要編輯的 Edge 閘道，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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。

b 選取要編輯的 Edge 閘道，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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。

   b 選取要編輯的 Edge 閘道，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。

NSX Data Center for vSphere Edge 閘道的自訂群組物件

VMware Cloud Director 環境中的 NSX Data Center for vSphere 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 VMware Cloud Director 租用戶入口網站的**群組物件**頁面來建立 IP 集。**群組物件**頁面在 [服務] 和 [Edge 閘道] 畫面上均可使用。

程序

1 開啟**群組物件**頁面。

選項	動作
透過 Edge 閘道服務開啟	a 導覽至**網路 > Edge**。 b 選取要編輯的 Edge 閘道，然後按一下**設定服務**。 c 按一下**群組物件**。
透過安全性服務開啟	a 導覽至**網路 > 安全性**。 b 選取要編輯的安全性服務，然後按一下**設定服務**。 c 按一下**群組物件**。

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 (選擇性) 如果使用 [服務] 畫面上的**群組物件**頁面指定 IP 集，請使用**繼承**切換按鈕啟用繼承，並允許基礎範圍內的可見度。

預設會啟用繼承。

6 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 VMware Cloud Director 租用戶入口網站的**群組物件**頁面來建立 MAC 集。[群組物件] 頁面在**服務**和 **Edge 閘道**畫面上均可使用。

程序

1 開啟**群組物件**頁面。

選項	動作
透過 Edge 閘道服務開啟	a 導覽至**網路 > Edge**。 b 選取要編輯的 Edge 閘道，然後按一下**設定服務**。 c 按一下**群組物件**。
透過安全性服務開啟	a 導覽至**網路 > 安全性**。 b 選取要編輯的安全性服務，然後按一下**設定服務**。 c 按一下**群組物件**。

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 (選擇性) 如果使用**服務**畫面上的**群組物件**頁面指定 MAC 集，請使用**繼承**切換按鈕啟用繼承，並允許基礎範圍內的可見度。

預設會啟用繼承。

6 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 VMware Cloud Director 租用戶入口網站的 [群組物件] 頁面檢視可用服務。[群組物件] 頁面在 [服務] 和 [Edge 閘道] 畫面上均可使用。

無法使用租用戶入口網站將服務新增至清單。可供您使用的一組服務由 VMware Cloud Director 系統管理員進行管理。

程序

1 開啟**群組物件**頁面。

選項	動作
透過 Edge 閘道服務開啟	a 導覽至**網路 > Edge**。 b 選取要編輯的 Edge 閘道，然後按一下**設定服務**。 c 按一下**群組物件**。
透過安全性服務開啟	a 導覽至**網路 > 安全性**。 b 選取要編輯的安全性服務，然後按一下**設定服務**。 c 按一下**群組物件**。

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 VMware Cloud Director 租用戶入口網站的 [群組物件] 頁面檢視可用服務群組。[群組物件] 頁面在 [服務] 和 [Edge 閘道] 畫面上均可使用。

您無法使用租用戶入口網站建立服務群組。可供您使用的一組服務群組由 VMware Cloud Director 系統管理員進行管理。

程序

1 開啟**群組物件**頁面。

選項	動作
透過 Edge 閘道服務開啟	a 導覽至**網路 > Edge**。 b 選取要編輯的 Edge 閘道，然後按一下**設定服務**。 c 按一下**群組物件**。
透過安全性服務開啟	a 導覽至**網路 > 安全性**。 b 選取要編輯的安全性服務，然後按一下**設定服務**。 c 按一下**群組物件**。

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。

NSX Data Center for vSphere Edge 閘道的統計資料和記錄

您可以檢視 NSX Data Center for vSphere 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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。

b 選取要編輯的 Edge 閘道，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

- 確認您是**組織管理員**，或者您已獲指派包含一組同等權限的角色。
- 驗證您的角色是否包含**設定系統記錄**權限。

程序

1 開啟 Edge 閘道服務。

a 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。

b 選取要編輯的 Edge 閘道，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 NSX Data Center for vSphere 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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**。

   b 選取要編輯的 Edge 閘道，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。

使用 NSX Data Center for vSphere Edge 閘道的安全性標籤

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 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後在**網路**下，選取**安全性**。

2 選取安全性服務，然後按一下**設定服務**。

3 按一下**安全性標籤**索引標籤。

4 按一下**建立** () 按鈕，然後輸入安全性標籤的名稱。

5 (選擇性) 輸入安全性標記的描述。

6 (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。

7 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 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後在**網路**下，選取**安全性**。

2 選取安全性服務，然後按一下**設定服務**。

3 按一下**安全性標籤**索引標籤。

4 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。

5 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。

6 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。

7 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 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後在**網路**下，選取**安全性**。

2 選取安全性服務，然後按一下**設定服務**。

3 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**。

4 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 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後在**網路**下，選取**安全性**。

2 選取安全性服務，然後按一下**設定服務**。

3 按一下**安全性標籤**索引標籤。

4 從安全性標籤清單中，選取您要編輯的安全性標籤。

5 按一下**編輯**按鈕。

6 編輯安全性標籤的名稱和說明。

7 將標籤指派給所選的虛擬機器或從中移除指派。

8 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 NSX Data Center for vSphere Edge 閘道的安全群組

。

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 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後在**網路**下，選取**安全性**。

2 選取安全性服務，然後按一下**設定服務**。

3 按一下**安全性標籤**索引標籤。

4 從安全性標籤清單中，選取您要刪除的安全性標籤。

5 按一下**刪除**按鈕。

6 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 NSX Data Center for vSphere Edge 閘道的安全群組。

使用 NSX Data Center for vSphere Edge 閘道的安全群組

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 開啟安全性服務。

   a 導覽至**網路 > 安全性**。

   b 選取您想要套用安全性設定的組織 VDC，然後按一下**設定服務**。

   租用戶入口網站隨即開啟安全性服務。

2 導覽至**群組物件 > 安全群組**

   安全群組頁面隨即開啟。

3 按一下**建立** () 按鈕。

4 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。

5 (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**。

6 (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。

7 (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。

8 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 開啟安全性服務。

a **導覽至網路 > 安全性**。

b 選取您想要套用安全性設定的組織 VDC，然後按一下**設定服務**。

租用戶入口網站隨即開啟安全性服務。

2 **導覽至群組物件 > 安全群組**

安全群組頁面隨即開啟。

3 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。

4 (選擇性) 編輯安全群組的名稱和說明。

5 (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。

6 (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**。

7 (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。

8 (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。

9 (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。

10 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 開啟安全性服務。

a **導覽至網路 > 安全性**。

b 選取您想要套用安全性設定的組織 VDC，然後按一下**設定服務**。

租用戶入口網站隨即開啟安全性服務。

2 **導覽至群組物件 > 安全群組**

安全群組頁面隨即開啟。

3 選取您要刪除的安全群組。

4 按一下**刪除**按鈕。

5 按一下**確定**以確認刪除。

結果

將會刪除安全群組。

管理 NSX-T Data Center Edge 閘道

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。

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，您的**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。

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，其他 Edge 閘道無法連線至外部網路。

與專用外部網路相關聯的 NSX-T Data Center 第 0 層邏輯路由器或 VRF 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。

專用外部網路提供其他 Edge 閘道路由服務，例如，路由通告管理和邊界閘道通訊協定 (BGP) 組態。

您可以決定將哪個連結至 Edge 閘道的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。

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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**索引標籤。

2 按一下 NSX-T Edge 閘道。

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

4 輸入 IP 集的名稱，並選擇性地輸入其說明。

5 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**。

6 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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**索引標籤。

2 按一下 Edge 閘道。

3 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。

4 按一下**編輯規則**。

5 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。

6 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。
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。

選項	描述
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。

7 按一下**儲存**。

8 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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**索引標籤。

2 按一下 Edge 閘道，然後在**服務**下，按一下 **NAT**。

3 若要新增規則，請按一下**新增**。

4 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。
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**。

5 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。

選項	描述
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。
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**。

6 按一下**儲存**。

7 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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**索引標籤。

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

3 在 **DNS 轉寄站**區段中，按一下**編輯**。

4 若要啟用 DNS 轉寄站服務，請開啟**狀態**切換按鈕。

5 輸入預設 DNS 區域的名稱，並選擇性地輸入說明。

6 輸入一或多個上游伺服器的 IP 位址，以逗號分隔。

7 按一下**儲存**。

8 (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**。

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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**索引標籤。

2 按一下 Edge 閘道。

3 在**安全性**下，按一下**應用程式連接埠設定檔**。

4 在**自訂應用程式**區段中，按一下**新增**。

5 輸入應用程式連接埠設定檔的名稱，並選擇性地輸入說明。

6 從下拉式功能表中選取通訊協定。

7 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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**索引標籤。

2 按一下 Edge 閘道。

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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**索引標籤。

2 按一下 Edge 閘道。

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。

程序

1 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。

2 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。

3 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。

4 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。

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**系統管理員**已將外部網路專用於您組織中的 NSX-T Data Center Edge 閘道。
- 確認您是**組織管理員**，或者您已獲指派包含一組同等權限的角色。

程序

1. 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**索引標籤。
2. 按一下 Edge 閘道。
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。您的**系統管理員**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**系統管理員**已將外部網路專用於您組織中的 NSX-T Data Center Edge 閘道。

- 確認您是**組織管理員**，或者您已獲指派包含一組同等權限的角色。

程序

1. 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**索引標籤。
2. 按一下 Edge 閘道。
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**系統管理員**已將外部網路專用於您組織中的 NSX-T Data Center Edge 閘道。
- 確認您是**組織管理員**，或者您已獲指派包含一組同等權限的角色。
- 設定 BGP 一般設定.

程序

1. 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**索引標籤。
2. 按一下 Edge 閘道。
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**系統管理員**已將外部網路專用於您組織中的 NSX-T Data Center Edge 閘道。
- 確認您是**組織管理員**，或者您已獲指派包含一組同等權限的角色。
- 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. 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**索引標籤。
2. 按一下 Edge 閘道。
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。

使用 NSX Advanced 負載平衡

身為**組織管理員**，您可以透過設定在多個伺服器集區之間散佈流量的虛擬服務，在 NSX-T Data Center 支援的資料中心內平衡工作負載。

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

VMware Cloud Director 支援可在 NSX-T Data Center Edge 閘道上設定的 L4 和 L7 負載平衡。

層級 4 負載平衡 (L4) 根據網路和傳輸層通訊協定 (例如 IP 位址和 TCP 連接埠) 中的資料導向流量。

層級 7 負載平衡 (L7) 根據屬性 (例如 HTTP 標頭、統一資源識別元、SSL 工作階段識別碼和 HTML 表單資料) 散佈流量。

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. 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**索引標籤。
2. 按一下要在其上啟用負載平衡的 NSX-T Data Center Edge 閘道。
3. 在 [負載平衡器] 下，按一下**一般設定**。
4. 按一下**編輯**，然後開啟**負載平衡器狀態**選項。
5. 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。
6. 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. 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**索引標籤。

2 按一下要為其指派服務引擎群組的 NSX-T Data Center Edge 閘道。

3 在 [負載平衡器] 下，按一下**服務引擎群組**。

4 按一下**新增**。

5 從清單中選取可用的服務引擎群組。

6 輸入可放置在 Edge 閘道上的虛擬服務數目上限。

7 輸入可供 Edge 閘道使用的保證虛擬服務數目。

8 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 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**索引標籤。

2 按一下已獲指派服務引擎群組的 NSX-T Data Center Edge 閘道。

3 在 [負載平衡器] 下，按一下**服務引擎群組**。

4 按一下**編輯**。

5 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。

6 編輯可供 Edge 閘道使用的保證虛擬服務數目。

7 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

- 確認您是**組織管理員**。
- 確認您的**系統管理員**已在 NSX-T Edge 閘道上啟用負載平衡。
- 確認您的**系統管理員**至少將一個服務引擎群組指派給 Edge 閘道。

程序

1 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**索引標籤。

2 按一下要為其設定負載平衡器集區的 NSX-T Data Center Edge 閘道。

3 在 [負載平衡器] 下，按一下**集區**，然後按一下**新增**。

4 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。

5 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。

6 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。

7 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。

8 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

- 確認您是**組織管理員**。
- 確認您的**系統管理員**已在 NSX-T Edge 閘道上啟用負載平衡。
- 確認您的**系統管理員**至少將一個服務引擎群組指派給 Edge 閘道。
- 新增負載平衡器伺服器集區。

程序

1 在頂部導覽列中，按一下**網路**，然後按一下 **Edge 閘道**索引標籤。

2 按一下要在其上建立虛擬服務的 NSX-T Data Center Edge 閘道。

3 在 [負載平衡器] 下，按一下**虛擬服務**，然後按一下**新增**。

4 為虛擬服務輸入有意義的名稱，並選擇性地輸入說明。

5 若要在建立時啟動虛擬服務，請開啟**已啟用**選項。

6 為虛擬服務選取服務引擎群組。

7 為虛擬服務選取負載平衡器集區。

8 輸入虛擬服務的 IP 位址。

9 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。

10 按一下**儲存**。

使用具名磁碟和檢閱儲存區原則

6

您可以透過使用 VMware Cloud Director 租用戶入口網站建立和管理具名磁碟，以及檢閱組織虛擬資料中心儲存區原則。

本章節討論下列主題：

- 建立和使用具名磁碟
- 檢閱儲存區原則內容

建立和使用具名磁碟

具名磁碟是在組織 VDC 中建立的獨立虛擬磁碟。**組織管理員**和具有相應權限的使用者可以建立、移除和更新具名磁碟，並將其連線至虛擬機器。

建立具名磁碟時，它與組織 VDC 相關聯，而不與虛擬機器相關聯。在 VDC 中建立磁碟後，磁碟擁有者或管理員可將其連結至 VDC 中部署的任何虛擬機器。如果您具有**建立共用磁碟**權限，則可以建立可連結至多個虛擬機器的共用具名磁碟。此外，磁碟擁有者還可以修改磁碟內容、將其與虛擬機器中斷連結，以及將其從 VDC 中移除。**系統管理員**與**組織管理員**具有與磁碟擁有者相同的使用和修改磁碟的權限。

備註 雖然 vSphere 支援 Windows Server 容錯移轉叢集 (WSFC) 等組態，並且您可以透過實體 SCSI 匯流排共用建立共用磁碟，但 VMware Cloud Director 10.2 不支援此功能。在 VMware Cloud Director 中建立共用磁碟時，僅在啟用多寫入器模式的情況下在 vSphere 中建立基礎獨立持續性磁碟。

如果連結具名磁碟，則無法建立虛擬機器快照。如果將共用磁碟連結至虛擬機器，則無法從虛擬機器詳細資料視圖中編輯其硬碟設定。

如果組織 VDC 具有已啟用虛擬機器加密的儲存區原則，您可以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，以加密這些虛擬機器和磁碟。請參閱虛擬機器加密。

建立具名磁碟

您可以建立具名磁碟，並在之後階段中將其連結到一或多個虛擬機器。

若要建立具名磁碟，您必須指定其名稱及大小。您可以選擇性地包含說明，並選取磁碟要使用的儲存區設定檔。您可以建立能夠連結至多個虛擬機器的共用磁碟。

備註 雖然 vSphere 支援 Windows Server 容錯移轉叢集 (WSFC) 等組態，並且您可以透過實體 SCSI 匯流排共用建立共用磁碟，但 VMware Cloud Director 10.2 不支援此功能。在 VMware Cloud Director 中建立共用磁碟時，僅在啟用多寫入器模式的情況下在 vSphere 中建立基礎獨立持續性磁碟。

必要條件

1 您必須具有**組織管理員**角色或磁碟擁有者權限。

2 如果您想要建立共用磁碟，則必須具有**建立共用磁碟**權限。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後在**儲存區**下，從左面板中選取**具名磁碟**。

2 按一下**新增**。

3 輸入磁碟的名稱，並選擇性地輸入其說明。

4 從**儲存區原則**下拉式功能表中，選取儲存區原則。

5 輸入具名磁碟的大小。

6 分別從**匯流排類型**和**匯流排子類型**下拉式功能表中選取匯流排類型和子類型。

7 如果您想要將具名磁碟連結至多個虛擬機器，請選取**可共用**核取方塊。

稍後無法編輯此設定。

8 按一下**儲存**。

後續步驟

使用 VMware Cloud Director API 將獨立磁碟連結至虛擬機器。請參閱 VMware {code} 上的 VMware Cloud Director API 程式設計指南。

編輯具名磁碟

建立磁碟後，您可以修改其名稱、說明、儲存區原則和大小。

您無法編輯具名磁碟的**可共用**設定。

必要條件

1 您必須具有**組織管理員**角色或磁碟擁有者權限。

程序

1 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後在**儲存區**下，從左面板中選取**具名磁碟**。

2 選取要修改的磁碟，然後按一下**編輯**。

3 編輯設定，例如名稱、說明、儲存區原則和大小。

4 按一下**儲存**。

將具名磁碟連結至虛擬機器

在 VDC 中建立具名磁碟之後，您可以將其連結至 VDC 中部署的任何虛擬機器。您可以將共用的具名磁碟連結至多個虛擬機器。

必要條件

您必須具有**組織管理員**角色或磁碟擁有者權限。

程序

1. 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後在**儲存區**下，從左面板中選取**具名磁碟**。
2. 按一下要連結至虛擬機器之具名磁碟名稱旁邊的選項按鈕，然後按一下**連結**。
3. 從下拉式功能表中，選取要連結具名磁碟的虛擬機器，然後按一下**套用**。
4. 如果您想要將其他虛擬機器連結至共用磁碟，請重複步驟 2 和步驟 3。

後續步驟

您可以將更多具名磁碟連結至虛擬機器，也可以視需要將其中斷連結。

刪除具名磁碟

如果不需要具名磁碟，可將其刪除。

必要條件

您必須具有**組織管理員**角色或磁碟擁有者權限。

程序

1. 在**虛擬資料中心**儀表板畫面上，按一下您想要探索的虛擬資料中心的卡，然後在**儲存區**下，從左面板中選取**具名磁碟**。
2. 選取要刪除的磁碟，然後按一下**刪除**。
3. 按一下**確定**。

檢閱儲存區原則內容

您可以檢閱儲存區原則和儲存區原則詳細資料。

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. 在**虛擬資料中心**儀表板畫面中，按一下您想要探索的虛擬資料中心的卡。
2. 在**儲存區**下，按一下**儲存區原則**。

   將顯示可用儲存區原則的清單。
3. 若要檢視有關儲存區原則的詳細資料，請按一下儲存區原則的名稱。
4. 在**一般**和**中繼資料**索引標籤上檢閱詳細資料，然後按一下**確定**。

   您可以檢閱儲存區原則的名稱、限制、IOPS 設定和中繼資料詳細資料。

檢閱和編輯虛擬資料中心內容 7

作為**組織管理員**，您可以檢閱虛擬資料中心內容。您還可以控制組織中的使用者和群組對組織 VDC 的存取。

本章節討論下列主題：

- 檢閱虛擬資料中心內容
- 檢閱虛擬資料中心中繼資料
- 僅限組織中特定的使用者和群組存取組織 VDC

檢閱虛擬資料中心內容

您可以檢閱指派給組織的虛擬資料中心內容。

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 在**虛擬資料中心**儀表板畫面中，按一下您想要探索的虛擬資料中心的卡。

2 在**設定**下，按一下**一般**。

結果

您可以檢閱虛擬資料中心的內容，例如名稱、說明和狀態。資料中心的相關度量資訊包括配置模型、vCPU、CPU 和記憶體使用量。

檢閱虛擬資料中心中繼資料

VMware Cloud Director 提供一般目的功能，用於將使用者定義的中繼資料與物件相關聯。如果您的系統管理員已針對組織虛擬資料中心建立中繼資料，您可以檢閱組織資料中心中繼資料。

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 在**虛擬資料中心**儀表板畫面中，按一下您想要探索的虛擬資料中心的卡。

2 在**設定**下，按一下**中繼資料**。

將顯示可用中繼資料的清單。

僅限組織中特定的使用者和群組存取組織 VDC

作為**組織管理員**，您可以僅限特定的使用者和群組存取組織中的每個組織 VDC。

依預設，組織 VDC 與具有包括**允許存取所有組織 VDC** 權限之角色的所有使用者和群組共用。

如果您的組織具有多個組織 VDC，並且您希望單獨對其進行管理，則可以建立一個可充當組織 VDC 管理員的自訂角色，並將其指派給組織中的特定使用者和群組，從而可以只允許這些使用者和群組存取特定 VDC 的計算資源和網路資源。

必要條件

1 確認您是**組織管理員**。

2 為要向其提供特定組織 VDC 存取權的使用者和群組建立自訂角色。此角色必須排除**允許存取所有組織 VDC** 權限。請參閱第 13 章 管理使用者、群組和角色。

程序

1 在**虛擬資料中心**儀表板畫面中，按一下您想要限制其存取的虛擬資料中心的卡。

2 在**設定**下，按一下**共用**。

此時將顯示組織中有權存取該 VDC 的使用者和群組清單。

3 若要變更組織 VDC 的存取設定，請按一下**編輯**。

4 選取**特定的使用者和群組**。

5 從**使用者**清單中，選取要為其提供 VDC 存取權的使用者。

6 從**群組**清單中，選取要為其提供 VDC 存取權的群組。

7 若要與所選使用者和群組共用 VDC，請按一下**共用**。

結果

對組織 VDC 的存取僅限於所選使用者和群組。

使用專用 vCenter Server 執行個體、端點和 Proxy

8

您可以從 VMware Cloud Director Tenant Portal 存取專用 vCenter Server 環境或 vCenter Server 元件。

專用 vSphere 資料中心

在 VMware Cloud Director 中，軟體定義資料中心 (SDDC) 封裝了整個專用 vCenter Server 環境。

VMware Cloud Director 中的專用 vCenter Server 執行個體移除了 vCenter Server 執行個體可供公開存取的需求。

系統管理員可以向您的組織發佈一或多個專用 vCenter Server 執行個體。您可以使用端點存取代理元件或非代理元件的使用者介面或 API。

端點

一個專用 vCenter Server 執行個體可包含一或多個端點，這些端點會提供對基礎環境中不同元件的存取權。端點可提供資料中心元件的存取點，例如 vCenter Server 執行個體、ESXi 主機、NSX Manager 執行個體或 NSX-T Manager 執行個體。

端點可能會，也可能不會連線至 Proxy。

Proxy

VMware Cloud Director 可以充當 HTTPS Proxy 伺服器，並提供對專用 vCenter Server 執行個體的存取權，以及用於備份環境的共用或專用 vCenter Server 執行個體之不同元件的存取權。

您可以使用 VMware Cloud Director 帳戶登入代理元件的使用者介面或 API。

若要存取代理元件，您必須使用 Chrome Browser Extension for VMware Cloud Director，或使用 Proxy 設定手動設定您的瀏覽器。

本章節討論下列主題：

- 使用 Chrome Browser Extension for VMware Cloud Director
- 為瀏覽器設定 Proxy 設定
- 使用端點登入元件的使用者介面

使用 Chrome Browser Extension for VMware Cloud Director

您可以使用 Chrome Browser Extension for VMware Cloud Director 登入環境中代理的 vSphere 元件。

Chrome Browser Extension for VMware Cloud Director 提供 Proxy 組態和驗證。

Chrome Browser Extension for VMware Cloud Director 支援多站台環境。

您可以透過 Chrome 線上應用程式商店將延伸新增至 Chrome 瀏覽器。

為瀏覽器設定 Proxy 設定

您必須設定發佈到您組織的 Proxy，才能存取代理的 vSphere 元件的使用者介面。

若要將瀏覽器設定為使用已發佈的 Proxy，您可以將 Proxy 自動組態 (PAC) 檔案的 URL 複製到瀏覽器中。

備註 當**系統管理員**將專用的 vSphere 資料中心發佈到您的組織，或將 Proxy 新增至其中一個專用的 vSphere 資料中心時，瀏覽器可能需要幾分鐘的時間從提供的 URL 重新擷取 PAC。若要強制重新整理瀏覽器，您可以重複此程序。

必要條件

- 確認**系統管理員**已將至少一個已啟用的專用 vCenter Server 執行個體發佈到您的組織。
- 確認**系統管理員**已將 **SDDC_VIEW** 和 **Token: 管理**權限發佈到您的組織，並且您的角色包含這些權限。
- 確認**系統管理員**已將 **CPOM 延伸**外掛程式發佈到您的組織並已啟用。此外掛程式提供在 VMware Cloud Director Tenant Portal 中檢視和使用專用 vSphere 資料中心的功能。

程序

1. 在頂部導覽列中，按一下**資料中心**，然後按一下**虛擬資料中心**。
2. 在**專用 vSphere 資料中心**窗格上，按一下**按一下這裡以檢視 Proxy 組態指南**。
3. 複製 PAC URL，然後按**下一步**。
4. 依照指示將瀏覽器設定為指向 PAC URL。
5. 如果代理元件使用自我簽署憑證，請將憑證匯入至您的瀏覽器。
   a. 在目標 vSphere 資料中心卡上，按一下**動作**，然後按一下**匯入憑證**。
   b. 下載憑證和憑證撤銷清單 (CRL)。
   c. 將已下載的憑證匯入您的瀏覽器中。

      請參閱瀏覽器的使用者指示。

使用端點登入元件的使用者介面

您可以使用端點，透過 VMware Cloud Director 帳戶存取代理元件或非代理元件的使用者介面。

必要條件

如果您想要存取代理的元件，請為瀏覽器設定 Proxy 設定或使用 Chrome Browser Extension for VMware Cloud Director 新增至 Google Chrome。

程序

1. 在頂部導覽列中，按一下**資料中心**，然後按一下**虛擬資料中心**。
2. 選取**專用 vSphere 資料中心**索引標籤。
3. 開啟專用 vCenter Server 執行個體的端點。
   - 若要開啟預設端點，請按一下**開啟 vSphere**。
   - 若要開啟非預設端點，請遵循下列步驟：
     - 按一下**動作**功能表，然後按一下**檢視端點**。
     - 按一下端點 URL。

   如果您要存取代理元件，則會開啟含 Proxy 認證的新卡。
4. 如果您要登入代理元件，請使用您的認證存取元件。
   a. 複製使用者名稱和密碼。
   b. 若要啟動 Proxy，請按一下**開啟**。

      新卡隨即開啟，並提示您對 Proxy 進行驗證。
   c. 在**使用者名稱**文字方塊中，貼上複製的使用者名稱。
   d. 在**密碼**文字方塊中，貼上複製的密碼，然後按一下**確定**。

使用 vApp 範本

9

vApp 範本是與作業系統、應用程式和資料一起載入的虛擬機器映像。這些範本確保虛擬機器在整個組織中的設定一致。vApp 範本會新增至目錄。

本章節討論下列主題：

- 檢視 vApp 範本
- 從 OVF 檔案建立 vApp 範本
- 從 vCenter Server 匯入虛擬機器做為 vApp 範本
- 將虛擬機器放置原則和虛擬機器大小調整原則指派給 vApp 範本
- 下載 vApp 範本
- 刪除 vApp 範本

檢視 vApp 範本

您可以查看目錄中可用並且您具有存取權的 vApp 範本清單。您可以檢視 vApp 範本並探索其中包含的虛擬機器。

您只能存取與您共用的目錄項目中所包含的 vApp 範本。如需有關共用目錄的詳細資訊，請參閱共用目錄。

必要條件

此作業需要預先定義之 **vApp 作者**角色中包含的權限或一組同等權限。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在左面板中選取 **vApp 範本**。

範本清單會以網格視圖顯示。

2 (選擇性) 將網格視圖設定為包含您想要查看的元素。

a 從網格視圖中，按一下 vApp 範本清單下方的網格編輯器圖示 ( )。

b 選取要包含在網格視圖中的元素，例如版本、狀態、目錄、擁有者等。

c 按一下**確定**。

網格會顯示您為清單中的每個 vApp 範本選取的元素。

3 若要檢視 vApp 範本中包含的虛擬機器，請按一下 vApp 範本名稱。

vApp 範本所包含的虛擬機器會顯示在網格中。

4 (選擇性) 若要選取要在網格視圖中查看的元素，請按一下虛擬機器清單下方的網格編輯器圖示 ( )。

a 選取要包含在網格視圖中的元素。

b 按一下**確定**。

從 OVF 檔案建立 vApp 範本

您可以上傳 OVF 套件，以在目錄中建立 vApp 範本。

VMware Cloud Director 支援開放虛擬化格式 (OVF) 和開放虛擬化應用裝置 (OVA) 規格。如果您上傳的 OVF 檔案包括用於自訂其虛擬機器的 OVF 內容，則那些內容會保留在 vApp 範本中。如需有關建立 OVF 套件的資訊，請參閱《OVF Tool 使用者指南》和《VMware vCenter Converter 使用者指南》

必要條件

此作業需要預先定義之**目錄作者**角色中包含的權限或一組同等權限。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在左面板中選取 **vApp 範本**。

範本清單會以網格視圖顯示。

2 按一下**新增**。

3 輸入 OVF 檔案的 URL 位址，或按一下**上傳**圖示瀏覽至可從電腦存取的位置，然後選取 OVF/OVA 範本檔案。

位置可能為本機硬碟、網路共用或 CD/DVD 光碟機。支援的副檔名包括 `.ova`、`.ovf`、`.vmdk`、`.mf`、`.cert` 和 `.strings`。如果您選取上傳 OVF 檔案，而其參考的檔案超過您嘗試上傳的檔案 (例如，VMDK 檔案)，則必須瀏覽並選取所有檔案。

4 驗證即將部署的 OVF/OVA 範本的詳細資料，然後按**下一步**。

5 輸入 vApp 範本的名稱，並選擇性地輸入說明，然後按**下一步**。

6 從**目錄**下拉式功能表中，選取您想要新增範本的目錄。

7 檢閱 vApp 範本設定，然後按一下**完成**。

結果

新的 vApp 範本會顯示在範本網格視圖中。

從 vCenter Server 匯入虛擬機器做為 vApp 範本

如果您具有**系統管理員**權限，則可以將 vCenter Server 虛擬機器做為目錄中的 vApp 範本匯入至 VMware Cloud Director。

必要條件

若要從 vCenter Server 查看和匯入做為 vApp 範本的虛擬機器，請確認您具有**系統管理員**權限。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在左面板中選取 **vApp 範本**。

範本清單會以網格視圖顯示。

2 按一下**從 vCenter 匯入**。

3 從下拉式功能表中，選取要從中匯入 vApp 範本的 vCenter Server 執行個體。

4 從虛擬機器清單中選取範本。

5 輸入 vApp 範本的名稱，並選擇性地輸入說明。

6 從下拉式功能表中，選取要向其中新增 vApp 範本的目錄。

7 (選擇性) 若要刪除來源虛擬機器，請開啟**移動虛擬機器**選項。

8 (選擇性) 將 vApp 範本標記為目錄中的慣用範本。

9 按一下**匯入**。

將虛擬機器放置原則和虛擬機器大小調整原則指派給 vApp 範本

若要將 vApp 範本的虛擬機器與特定虛擬機器放置和虛擬機器大小調整原則相關聯，您可以使用要指派的原則來標記 vApp 範本的個別虛擬機器。

從 VMware Cloud Director 10.0 開始，您可以允許使用者在編輯虛擬機器時變更預先定義的虛擬機器放置或虛擬機器大小調整原則。

備註 升級到 VMware Cloud Director 10.0 或更新版本後，所有既存的範本標記都會變得可修改。如果您想要禁止變更預先定義的虛擬機器放置或虛擬機器大小調整原則，則必須取消選取想要禁止變更之原則的**可修改**核取方塊。

必要條件

- 此作業需要編輯 vApp 範本的權限。
- 確認您的 VMware Cloud Director 環境中至少有一個 vApp 範本。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在左面板中選取 **vApp 範本**。

範本清單會以網格視圖顯示。

2 選取要標記的 vApp 範本旁邊的選項按鈕，然後按一下**使用運算原則標記**。

3 如果您想要在 vApp 範本中將虛擬機器放置原則指派給虛擬機器，請從與虛擬機器對應的資料列上的**虛擬機器放置原則**下拉式功能表中選取一個原則。

4 如果您想要在 vApp 範本中將虛擬機器大小調整原則指派給虛擬機器，請從與虛擬機器對應的資料列上的**虛擬機器大小調整原則**下拉式功能表中選取一個原則。

5 (選擇性) 若要允許使用者在編輯虛擬機器時變更預先定義的虛擬機器放置或虛擬機器大小調整原則，請在原則下拉式功能表下方選取**可修改**核取方塊。

6 按一下**標記**。

下載 vApp 範本

您可以從目錄以 OVA 檔案形式將 vApp 範本下載到本機機器。

必要條件

此作業需要預先定義之**目錄作者**角色中包含的權限或一組同等權限。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在左面板中選取 **vApp 範本**。

範本清單會以網格視圖顯示。

2 按一下要下載的 vApp 範本左側的清單列 (⋮)，然後選取**下載**。

備註 您可以從組織目錄下載 vApp 範本。如果您是組織管理員，可以從公用目錄下載 vApp 範本。否則，**下載**按鈕會顯示為灰色。

3 (選擇性) 若要在下載的 OVA 套件中保留虛擬機器的 UUID 和 MAC 位址，請選取**保留身分識別資訊**核取方塊。

4 按一下**確定**，然後等待下載完成。

OVA 檔案會儲存到您的網頁瀏覽器的預設下載位置。

刪除 vApp 範本

您可以從組織目錄中刪除 vApp 範本。如果已發佈目錄，則也會從公用目錄中刪除 vApp 範本。

必要條件

此作業需要預先定義之 **vApp 作者**角色中包含的權限或一組同等權限。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在左面板中選取 **vApp 範本**。

範本清單會以網格視圖顯示。

2 按一下要刪除的 vApp 範本左側的清單列 (⋮)，然後選取**刪除**。

3 確認刪除。

刪除的 vApp 範本會從網格視圖中移除。

使用媒體檔案

10

目錄可讓您上傳、複製、移動和編輯媒體檔案的內容。

本章節討論下列主題：

- 上傳媒體檔案
- 刪除媒體檔案
- 下載媒體檔案

上傳媒體檔案

您可以上傳新的媒體檔案或新版本的現有媒體檔案至目錄。具有目錄存取權限的使用者可以透過其虛擬機器開啟媒體檔案。

必要條件

此作業需要預先定義之**目錄作者**角色中包含的權限或一組同等權限。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在左面板中選取**媒體及其他**。

媒體檔案清單會以網格視圖顯示。

2 按一下**新增**。

3 從**目錄**下拉式功能表中，選取您想要上傳媒體檔案的目錄。

4 輸入媒體檔案的名稱。

如果您未輸入名稱，則名稱文字方塊中會自動填入媒體檔案的名稱。

5 按一下上傳圖示瀏覽並選取磁碟映像檔，例如 `.iso` 檔案。

6 按一下**確定**。

開始上傳後，媒體檔案會顯示在網格中。

後續步驟

上傳可能需要一段時間才能完成，具體取決於檔案大小。您可以在**最近的工作**視圖中監控下載狀態。如需詳細資訊，請參閱檢視工作。

刪除媒體檔案

您可以從目錄中刪除不再使用的媒體檔案。

必要條件

此作業需要預先定義之**目錄作者**角色中包含的權限或一組同等權限。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在左面板中選取**媒體及其他**。

媒體檔案清單會以網格視圖顯示。

2 按一下要刪除的媒體檔案左側的清單列（ ⋮ ），然後選取**刪除**。

3 確認刪除。

刪除的媒體檔案會從網格視圖中移除。

下載媒體檔案

您可以從目錄下載媒體檔案。

必要條件

此作業需要預先定義之**目錄作者**角色中包含的權限或一組同等權限。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在左面板中選取**媒體及其他**。

媒體檔案清單會以網格視圖顯示。

2 按一下要下載的媒體檔案左側的清單列（ ⋮ ），然後選取**下載**。

下載工作隨即啟動，並且檔案儲存到網頁瀏覽器的預設下載位置。

後續步驟

下載可能需要一段時間才能完成，具體取決於檔案大小。您可以在**最近的工作**面板中監控下載狀態。如需詳細資訊，請參閱檢視工作。

使用目錄

11

目錄是組織中 vApp 範本和媒體檔案的容器。組織管理員和目錄作者可以在組織中建立目錄。目錄內容可以與 VMware Cloud Director 安裝內的其他使用者或組織共用，也可以在外部發佈以供 VMware Cloud Director 安裝外的組織存取。

VMware Cloud Director 包含私人目錄、共用目錄，以及外部可存取的目錄。私人目錄包括您可與組織中其他使用者共用的 vApp 範本和媒體檔案。如果系統管理員啟用組織的目錄共用功能，您便可以共用組織目錄，以建立目錄供 VMware Cloud Director 安裝內的其他組織存取。如果系統管理員啟用組織的外部目錄發佈功能，您便可以發佈組織目錄，供 VMware Cloud Director 安裝外的組織存取。在 VMware Cloud Director 安裝之外的組織必須訂閱外部發佈目錄，才能存取其內容。

您可以將 OVF 套件直接上傳至目錄、將 vApp 儲存為 vApp 範本，或是從 vSphere 匯入 vApp 範本。請參閱從 OVF 檔案建立 vApp 範本與將 vApp 以 vApp 範本形式儲存至目錄。

組織成員可以存取他們所擁有或共用的 vApp 範本和媒體檔案。組織管理員和系統管理員可以與組織中的所有人共用目錄，或與組織中的特定使用者和群組共用目錄。請參閱共用目錄。

本章節討論下列主題：

- 檢視目錄
- 建立目錄
- 共用目錄
- 刪除目錄
- 變更目錄的擁有者
- 管理目錄的中繼資料
- 發佈目錄
- 訂閱外部目錄
- 更新訂閱目錄的位置 URL 和密碼
- 同步訂閱目錄

檢視目錄

您可以存取在組織內與您共用的目錄。如果組織管理員已使公用目錄在組織內可存取，則您可以存取這些公用目錄。

目錄存取透過目錄共用控制，而不是透過您角色中的權限控制。您只能存取與您共用的目錄或目錄項目。如需詳細資訊，請參閱共用目錄。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在左面板中選取**目錄**。

目錄清單會以網格視圖顯示。

2 (選擇性) 將網格視圖設定為包含您想要查看的元素。

a 從網格視圖中，按一下目錄清單下方顯示的網格編輯器圖示 ( )。

b 選取要包含在網格視圖中的元素，例如版本、說明、狀態等。

c 按一下**確定**。

網格會顯示您為每個目錄選取的元素。

3 (選擇性) 從網格視圖中，使用清單列 ( ) 顯示您可以為每個目錄所採取的動作。

例如，您可以共用或刪除目錄。

建立目錄

您可以建立新目錄並將其與儲存區原則相關聯。

必要條件

此作業需要預先定義之**目錄作者**角色中包含的權限或一組同等權限。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在左面板中選取**目錄**。

目錄清單會以網格視圖顯示。

2 按一下**新增**以建立新目錄。

3 輸入目錄的名稱，並選擇性地輸入其說明。

4 (選擇性) 選取是否要將儲存區原則指派給目錄，然後選取一個儲存區原則。

5 按一下**確定**。

結果

新目錄將會出現在**目錄**索引標籤上的網格視圖中。

共用目錄

您可以與組織的所有成員或特定成員共用目錄。

必要條件

- 此作業需要預先定義之**目錄作者**角色中包含的權限或一組同等權限。
- 您必須是目錄的擁有者。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在左面板中選取**目錄**。

目錄清單會以網格視圖顯示。

2 按一下要共用的目錄左側的清單列（ ⋮ ），然後選取**共用**。

可存取目錄之使用者的清單會顯示在**共用目錄**視窗的網格視圖中。

3 按一下**新增**，與其他使用者共用目錄。

選項	描述
與此組織中的所有人共用	為組織中的所有使用者和群組授與存取權。
與特定的使用者和群組共用	選取要授與目錄存取權的使用者或群組，然後按一下**新增**。

4 選取存取層級。

選項	描述
唯讀	具有此目錄存取權的使用者擁有目錄的 vApp 範本和 ISO 檔案的讀取存取權。
讀/寫	具有此目錄存取權的使用者擁有目錄的 vApp 範本和 ISO 檔案的讀取存取權，並且可以將 vApp 範本和 ISO 檔案新增至目錄。
完全控制	具有此目錄存取權的使用者擁有目錄內容和設定的完全控制權。

5 按一下**確定**。

現在具有目錄存取權的使用者或群組會顯示在**共用目錄**對話方塊的網格視圖中。

6 (選擇性) 選取以共用對所有其他組織管理員的唯讀存取權

7 按一下**儲存**。

結果

在**目錄**索引標籤上，網格視圖中此目錄的共用狀態會發生變更。

刪除目錄

您可以從組織中刪除目錄。

必要條件

此作業需要預先定義之**目錄作者**角色中包含的權限或一組同等權限。

備註 目錄不得包含任何 vApp 範本或媒體檔案。您可以將這些項目移動至不同的目錄或加以刪除。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在左面板中選取**目錄**。

目錄清單會以網格視圖顯示。

2 按一下要刪除的目錄左側的清單列（ ⋮ ），然後選取**刪除**。

3 確認刪除。

刪除的目錄項目會從網格視圖中移除。

變更目錄的擁有者

組織管理員可以變更目錄的擁有者。

在可以刪除擁有目錄的使用者之前，您必須變更擁有者或刪除目錄。

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 在頂部導覽列中，按一下**程式庫**，然後在左面板中選取**目錄**。

目錄清單會以網格視圖顯示。

2 按一下目錄左側的清單列（ ⋮ ），然後選取**變更擁有者**。

可存取目錄之使用者的清單會顯示在**變更擁有者**視窗的網格視圖中。

3 選取要成為目錄之新擁有者的使用者，然後按一下**確定**。

結果

在**目錄**索引標籤上，網格視圖中此目錄擁有者的名稱會發生變更。

管理目錄的中繼資料

做為**組織管理員**或**目錄擁有者**，您可以建立或更新所擁有目錄的中繼資料。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在左面板中選取**目錄**。

目錄清單會以網格視圖顯示。

2 按一下目錄左側的清單列（ ⋮ ），然後選取**中繼資料**。

將在網格視圖中顯示所選目錄的中繼資料。

3 (選擇性) 若要新增中繼資料，請按一下**新增**。

a 輸入中繼資料名稱。

在連結至此物件的中繼資料名稱中，該名稱必須是唯一的。

b 選取中繼資料類型，例如，**文字**、**數字**、**日期和時間**或**是或否**。

c 輸入中繼資料值。

d 按一下**儲存**。

4 (選擇性) 更新現有中繼資料。

無法更新中繼資料名稱。

a 更新中繼資料類型。

b 輸入新的中繼資料值。

c 按一下**儲存**。

5 (選擇性) 刪除現有中繼資料。

a 按一下刪除圖示。

b 按一下**儲存**。

發佈目錄

如果**系統管理員**已授與您目錄存取權，您就可以在外部發佈目錄，使其 vApp 範本與媒體檔案可供 VMware Cloud Director 安裝外的組織訂閱。

必要條件

請確認**系統管理員**已啟用組織的外部目錄發佈功能，並且已授與您目錄存取權。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在左面板中選取**目錄**。

目錄清單會以網格視圖顯示。

2 按一下要發佈的目錄左側的清單列 (⋮)，然後選取**發佈設定**。

3 選取**啟用發佈**，然後選擇性地輸入用於目錄存取的密碼。

僅支援 ASCII 字元。

4 按一下**儲存**。

訂閱外部目錄

您可以訂閱外部目錄，以建立外部發佈目錄的唯讀複本。無法修改訂閱目錄。

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。
- **系統管理員**必須授與您的組織訂閱外部目錄的權限。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在左面板中選取**目錄**。

目錄清單會以網格視圖顯示。

2 按一下**新增**以建立新目錄。

3 輸入目錄的名稱，並選擇性地輸入其說明。

4 選取以訂閱外部目錄並提供訂閱 URL。

5 輸入選擇性密碼來存取目錄。

6 選取是否要自動從外部目錄下載內容。

7 按一下**確定**。

更新訂閱目錄的位置 URL 和密碼

建立訂閱目錄後，您可以更新訂閱目錄的位置 URL 和密碼。

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。
- 必須已建立訂閱目錄。
- **系統管理員**必須授與您的組織訂閱外部目錄的權限。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在左面板中選取**目錄**。

目錄清單會以網格視圖顯示。

2 按一下訂閱目錄左側的清單列 (⋮)，然後選取**訂閱設定**。

如果目錄不是已訂閱目錄，此選項會顯示為灰色。

3 更新這個已訂閱目錄的位置 URL 和密碼。

4 選取是否要自動從外部目錄下載內容。

5 按一下**儲存**。

同步訂閱目錄

建立訂閱目錄後，您可以將其與原始目錄同步以查看是否有任何變更。例如，如果原始目錄的中繼資料有所變更，則執行同步時，訂閱目錄的中繼資料會進行更新。

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。
- 必須已建立訂閱目錄。
- **系統管理員**必須授與您的組織訂閱外部目錄的權限。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在左面板中選取**目錄**。

目錄清單會以網格視圖顯示。

2 按一下訂閱目錄左側的清單列（ ⋮ ），然後選取**同步**。

如果目錄不是已訂閱目錄，此選項會顯示為灰色。

訂閱目錄將與原始目錄同步。

使用組織虛擬資料中心範本

12

組織管理員或有權檢視和具現化組織虛擬資料中心範本的任何角色可建立其他組織虛擬資料中心。

組織虛擬資料中心範本會為組織虛擬資料中心指定組態，並選擇性地為 Edge 閘道和組織虛擬資料中心網路指定組態。透過建立組織虛擬資料中心範本並與這些組織共用這些範本，系統管理員可讓組織管理員在其組織中建立這些資源。

透過建立和共用虛擬資料中心範本，系統管理員可以在保留對系統資源 (例如提供者虛擬資料中心和外部網路) 配置的管理控制時，啟用組織虛擬資料中心的自助佈建。

系統管理員可以建立組織虛擬資料中心範本，並為不同組織提供範本的存取權。

如果您的組織已有虛擬資料中心範本的存取權，您可以使用 VMware Cloud Director Tenant Portal 從可用的範本建立虛擬資料中心。

本章節討論下列主題：

- 檢視可用的虛擬資料中心範本
- 從範本具現化虛擬資料中心

檢視可用的虛擬資料中心範本

您可以檢視系統管理員已為您建立的組織虛擬資料中心範本。

檢視虛擬資料中心範本，然後再從虛擬資料中心範本建立新的組織虛擬資料中心。

必要條件

此作業需要預先定義的**組織管理員**角色或有權檢視和具現化組織虛擬資料中心範本的角色中包含的權限。

程序

- 在頂部導覽列中，按一下**程式庫**，然後在左面板中選取**組織 VDC 範本**。

  虛擬資料中心範本清單會以網格視圖顯示。

後續步驟

檢閱組織虛擬資料中心範本的說明，然後選取要用於建立新組織虛擬資料中心的範本。

從範本具現化虛擬資料中心

當系統管理員建立組織虛擬資料中心 (VDC) 範本並將範本發佈到您的組織時，您可以從該範本建立組織 VDC。

必要條件

此作業需要預先定義的**組織管理員**角色或有權檢視和具現化組織 VDC 範本的角色中包含的權限。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在左面板中選取**組織 VDC 範本**。

虛擬資料中心範本清單會以網格視圖顯示。

2 選取一個範本，然後按一下**新增 VDC**。

從 VMware Cloud Director 10.2.2 開始，必須在選取範本後按一下**具現化 VDC**。

3 輸入 VDC 的名稱，並選擇性地輸入說明。

4 按一下**建立**。

結果

此時將具現化新組織虛擬資料中心的建立，此作業可能需要幾分鐘的時間。您可以在**最近的工作**面板中查看工作的進度。

後續步驟

您可以透過建立虛擬機器、vApp 和管理網路與安全性設定等作業，管理新建立的組織虛擬資料中心。

管理使用者、群組和角色 13

您可以將組織管理員個別新增至 VMware Cloud Director，或是當作 LDAP 群組的一部分進行新增。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。

重要 您必須是**組織管理員**，才能管理您組織中的使用者、群組和角色。**系統管理員**可以為您的承租人發佈一或多個全域承租人角色，而您可以**組織管理員**身分在角色清單中查看這些角色。例如，此類角色包括**目錄作者**、**vApp 作者**、**vApp 使用者**、**組織管理員**等。您無法修改預先定義的全域承租人角色，但您可以建立和更新類似的自訂承租人角色並將其指派給承租人中的使用者。

本章節討論下列主題：

管理使用者

您可以從租用戶入口網站建立、編輯、匯入和刪除使用者。此外，也可以在使用者嘗試使用錯誤密碼登入而導致鎖定其自己的使用者帳戶的情況下，解除鎖定使用者帳戶。

建立使用者

您可以在您的 VMware Cloud Director 組織內建立使用者。

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. 在頂部導覽列中，按一下**管理**。
2. 在左面板中的**存取控制**下，按一下**使用者**。

   使用者清單隨即顯示。
3. 按一下**新增**。
4. 輸入使用者的使用者名稱和密碼設定。

   最小密碼長度為 6 個字元。

5 選取是否要在建立時啟用使用者。

6 如果您想要對可供使用者使用的資源設定特定限制，請開啟**設定使用者的配額**切換按鈕。

如果開啟此切換按鈕，當您完成此精靈時，VMware Cloud Director 會將您重新導向至**配額**頁面。可以對 Tanzu Kubernetes 叢集數目、使用者管理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配額。如果您希望使用者擁有所選類型的無限制資源，請選取**無限制**。

7 選擇要指派給使用者的角色。

可用角色功能表包含預先定義的角色清單，以及您或系統管理員可能已建立的任何自訂角色。

預先定義的角色	說明
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。
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。
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。
組織管理員	具有預先定義之**組織管理員**角色的使用者可以使用 VMware Cloud Director 租用戶入口網站或 Cloud Director OpenAPI，來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。**組織管理員**可使用 Cloud Director OpenAPI 建立或更新組織的本機角色物件。其他組織不會看見由**組織管理員**建立或修改的角色。
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。當為使用者指派**遵從身分識別提供者**角色時，若要取得加入的資格，身分識別提供者提供的角色名稱必須與在組織中定義的角色或名稱完全相符 (區分大小寫)。
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。

8 (選擇性) 輸入連絡人資訊 (例如，名稱、電子郵件地址、電話號碼和即時訊息識別碼)。

9 按一下**儲存**。

後續步驟

如果您已為使用者啟用配額組態，並且 VMware Cloud Director 將您重新導向至**配額**頁面，請參閱管理使用者的資源配額。

匯入使用者

您可以透過匯入 LDAP 使用者或 SAML 使用者並為其指派特定角色，來將使用者新增至您的組織。

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。
- 請確認您擁有與 LDAP 伺服器的有效連線，或允許您的組織使用 SAML 身分識別提供者。

程序

1 在頂部導覽列中，按一下**管理**。

2 在左面板中的**存取控制**下，按一下**使用者**。

使用者清單隨即顯示。

3 按一下**匯入使用者**。

4 選取要從中匯入使用者的來源。

您將只能檢視已設定為身分識別提供者的來源 LDAP 伺服器或 SAML 伺服器。

來源	動作
LDAP	從 LDAP 伺服器匯入使用者。 a 在文字方塊中輸入完整或部分名稱，然後按一下**搜尋**。 b 選取要匯入的使用者，然後按一下**新增**。
SAML	從 SAML 伺服器匯入使用者。輸入要匯入之使用者的使用者名稱。 使用者名稱必須採用針對此組織設定的 SAML 身分識別提供者支援的名稱識別碼格式。 **備註** 如果您使用 vCenter Single Sign-On 做為 SAML 身分識別提供者，則從 vCenter Single Sign-On 網域匯入的使用者名稱必須採用使用者主體名稱 (UPN) 格式，例如 jdoe@mydomain.com。 為每個使用者名稱使用一個新行。

5 選取您想要指派給所匯入的使用者的角色。

6 按一下**儲存**。

修改使用者

身為組織管理員，您可以修改現有使用者的密碼、連絡人和虛擬機器配額設定。此外，也可以變更使用者的角色。

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 在頂部導覽列中，按一下**管理**。

2 在左面板中的**存取控制**下，按一下**使用者**。

使用者清單隨即顯示。

3 按一下要編輯的使用者名稱旁邊的選項按鈕，然後按一下**修改**。

4 更新要修改的設定。

a 視需要變更密碼。

b 選取是啟用還是停用使用者。

c 更新使用者角色。

d 更新連絡人資訊 (例如，名稱、電子郵件地址、電話號碼和即時訊息識別碼)。

e 編輯使用者的虛擬機器配額。

5 按一下**儲存**。

停用或啟用使用者帳戶

您可以停用使用者帳戶，以阻止使用者登入 VMware Cloud Director。若要刪除使用者，您必須先停用其帳戶。

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 在頂部導覽列中，按一下**管理**。

2 在左面板中的**存取控制**下，按一下**使用者**。

使用者清單隨即顯示。

3 若要停用使用者帳戶，請按一下使用者名稱旁邊的選項按鈕，然後按一下**停用**並確認。

4 若要啟用已停用的使用者帳戶，請按一下使用者名稱旁邊的選項按鈕，然後按一下**啟用**。

刪除使用者

您可以透過刪除使用者帳戶，來從 VMware Cloud Director 組織中移除使用者。

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。
- 停用要刪除的帳戶。

程序

1 在頂部導覽列中，按一下**管理**。

2 在左面板中的**存取控制**下，按一下**使用者**。

使用者清單隨即顯示。

3 按一下要刪除的使用者名稱旁邊的選項按鈕，然後按一下**刪除**。

4 若要確認您要刪除該使用者帳戶，請按一下**確定**。

解除鎖定鎖定的使用者帳戶

如果已在 VMware Cloud Director 組織中啟用鎖定原則，則在特定次數的無效登入嘗試之後會鎖定使用者帳戶。您可以解除鎖定鎖定的使用者帳戶。最佳做法是變更使用者的密碼，然後解除鎖定該帳戶。

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 在頂部導覽列中，按一下**管理**。

2 在左面板中的**存取控制**下，按一下**使用者**。

使用者清單隨即顯示。

3 按一下使用者名稱旁邊的選項按鈕，然後按一下**解除鎖定**。

管理使用者的資源配額

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

使用者可以查看僅與其使用者類型相關的配額。使用者將從所屬群組繼承配額。如果使用者從其群組繼承資源配額，並且已為該資源定義明確的使用者層級配額，則使用者層級配額會優先於群組層級配額。

如需建立或匯入使用者的相關資訊，請參閱建立使用者或匯入使用者。

必要條件

確認您擁有新增、編輯和刪除資源配額的必要權限。依預設，**組織管理員**可以變更使用者的配額。

程序

1 在頂部導覽列中，按一下**管理**。

2 在左面板中的**存取控制**下，按一下**使用者**。

3 選取使用者的名稱，然後選取**配額**索引標籤。

依預設，使用者沒有任何配額。屬於群組的所有使用者都會繼承群組的配額。如果使用者屬於具有資源配額的群組，則配額會在該使用者的配額清單中顯示為不可編輯。

4 按一下**編輯**。

5 修改所選使用者的配額。

可以對 Tanzu Kubernetes 叢集數目、使用者管理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。如果您希望使用者擁有所選類型的無限制資源，請選取**無限制**。

6 按一下**儲存**。

管理群組

如果您擁有與 LDAP 伺服器的有效連線，或允許組織使用 SAML 身分識別提供者，則可以匯入 LDAP 群組或 SAML 群組。此外，也可以編輯或刪除已匯入的群組。

匯入群組

若要新增使用者群組，您可以匯入 LDAP 群組或 SAML 群組。

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。
- 請確認您擁有與 LDAP 伺服器的有效連線，或允許您的組織使用 SAML 身分識別提供者。

程序

1. 在頂部導覽列中，按一下**管理**。
2. 在左面板中的**存取控制**下，按一下**群組**。

   使用者群組清單隨即顯示。
3. 按一下**匯入群組**。
4. 選取要從中匯入使用者群組的來源。

   您只能檢視已設定為身分識別提供者的來源 LDAP 伺服器或 SAML 伺服器。

來源	動作
LDAP	從 LDAP 伺服器匯入使用者群組。 a 在文字方塊中輸入完整或部分名稱，然後按一下**搜尋**。 b 選取要匯入的使用者群組，然後按一下**新增**。
SAML	從 SAML 伺服器匯入使用者群組。輸入要匯入之群組的名稱。 為每個群組名稱使用一個新行。

5. 選取您想要指派給所匯入的使用者群組的角色。
6. 按一下**儲存**。

後續步驟

如果您已為群組啟用配額組態，並且 VMware Cloud Director 將您重新導向至**配額**頁面，請參閱管理群組的資源配額。

刪除群組

您可以透過刪除其 LDAP 群組從 VMware Cloud Director 組織中移除群組。

刪除 LDAP 群組時，該群組內僅根據其成員資格而擁有 VMware Cloud Director 帳戶的使用者就無法再被利用，也無法登入。

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. 在頂部導覽列中，按一下**管理**。
2. 在左面板中的**存取控制**下，按一下**群組**。

   使用者群組清單隨即顯示。

3 按一下要刪除之群組名稱旁邊的選項按鈕，然後按一下**刪除**。

4 若要確認您要刪除該群組，請按一下**確定**。

編輯群組

您可以從 VMware Cloud Director 租用戶入口網站編輯該群組。

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 在頂部導覽列中，按一下**管理**。

2 在左面板中的**存取控制**下，按一下**群組**。

使用者群組清單隨即顯示。

3 按一下要刪除之群組名稱旁邊的選項按鈕，然後按一下**編輯**。

4 視需要編輯群組。

a 變更說明。

b 視需要變更群組成員的角色。

5 按一下**儲存**。

管理群組的資源配額

透過直接對群組設定配額，您可以管理其中每個使用者的整體資源耗用量限制。您可以新增、編輯和移除群組的虛擬機器、Tanzu Kubernetes 叢集、CPU、記憶體或儲存區配額。群組中的每個成員都會套用該群組的配額。

使用者將從所屬群組繼承配額。如果使用者從其群組繼承資源配額，並且已為該資源定義明確的使用者層級配額，則使用者層級配額會優先於群組層級配額。

如需匯入群組的相關資訊，請參閱匯入群組。

必要條件

確認您擁有新增、編輯和刪除資源配額的必要權限。依預設，**組織管理員**可以變更群組的配額。

程序

1 在頂部導覽列中，按一下**管理**。

2 在左面板中的**存取控制**下，按一下**群組**。

3 選取群組的名稱，然後選取**配額**索引標籤。

依預設，群組沒有任何配額。屬於群組的所有使用者都會繼承群組的配額。如果使用者屬於具有資源配額的群組，則配額會在該使用者的配額清單中顯示為不可編輯。

4 按一下**編輯**。

5 修改所選群組的配額。

可以對 Tanzu Kubernetes 叢集數目、群組管理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。如果您希望使用者群組擁有所選類型的無限制資源，請選取**無限制**。

6 按一下**儲存**。

角色與權限

VMware Cloud Director 使用角色和權限來決定使用者可以在組織中執行的動作。VMware Cloud Director 包含具有特定權限的許多預先定義的角色。

系統管理員與**組織管理員**必須為每個使用者或群組指派角色。同一個使用者在不同組織中角色可能不同。**系統管理員**可以為整個系統建立角色並修改現有角色，而**組織管理員**只能為其所管理的組織建立和修改角色。

VMware Cloud Director 租用戶入口網站可讓**組織管理員**管理其組織中的角色。如果**系統管理員**將一或多個預先定義的承租人角色發佈至您的組織，則您做為**組織管理員**可以檢視這些角色，但無法進行修改。不過，您可以建立具有類似權限的自訂承租人角色，並將其指派給組織中的使用者。

如需預先定義的角色及其權限的相關資訊，請參閱預先定義的角色與其權限。

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《VMware Cloud Director Service Provider Admin Portal 指南》。**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

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。

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：CLSP 發佈訂閱	✓	✓			
	目錄：建立/刪除目錄	✓	✓			
	目錄：編輯內容	✓	✓			
	目錄：發佈	✓	✓			
	目錄：共用	✓	✓			
	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	✓				
	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	✓				
	磁碟：變更擁有者	✓	✓			
	磁碟：建立	✓	✓	✓		
	磁碟：刪除	✓	✓	✓		
	磁碟：編輯內容	✓	✓	✓		
	磁碟：檢視加密狀態	✓		✓		
	磁碟：檢視內容	✓	✓	✓	✓	
	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	✓				
	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	✓				

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：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	✓				
	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	✓				

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 NAT	✓				
	組織 vDC 閘道：檢視靜態路由	✓				
	組織 vDC 網路：編輯內容	✓				
	組織 vDC 網路：檢視內容	✓		✓		
	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	✓				
	組織 vDC：編輯 ACL	✓				
	組織 vDC：管理防火牆	✓				
	組織 vDC：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 LDAP 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	✓				
	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	✓				

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
	服務程式庫：檢視服務程式庫	✓				
	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：變更擁有者	✓	✓			
	vApp 範本：簽出	✓	✓	✓	✓	
	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	✓	✓	✓		
	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	✓	✓	✓	✓	

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：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：檢視	✓				
✓	VDC 群組：設定記錄	✓				
	VDC 範本：具現化	✓				
	VDC 範本：檢視	✓				

建立自訂承租人角色

組織管理員可使用租用戶入口網站在其管理的組織中建立自訂承租人角色物件。

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. 在頂部導覽列中，按一下**管理**。
2. 在左面板中的**存取控制**下，按一下**角色**。

   角色清單隨即顯示。
3. 按一下**新增**。
4. 輸入角色的名稱，並選擇性地輸入其說明。
5. 展開角色的權限，然後為角色選取權限。

   權限依類別和子類別分組，以允許檢視或管理物件。

選項	描述
存取控制	用於控制檢視及管理特定物件的存取的權限。
管理	用於控制管理存取的權限。
計算	用於控制組織和提供者虛擬資料中心、vApp、組織虛擬資料中心範本、虛擬機器群組之存取和管理，以及虛擬機器監控的權限。
延伸	用於控制對任何其他外掛程式和 VMware Cloud Director 延伸的存取權限。
基礎結構	用於控制基礎結構物件 (如資料存放區、磁碟、主機等) 之存取和管理的權限。

選項	描述
程式庫	用於控制任何目錄和目錄項目之存取和管理的權限。
網路作業	用於控制網路設定之存取和管理的權限。

6 按一下**儲存**。

編輯自訂承租人角色

組織管理員可以使用租用戶入口網站，在其管理的組織中編輯自訂承租人角色物件。做為組織管理員，您只能檢視系統管理員發佈至您組織的全域承租人角色。無法編輯全域承租人角色。

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 在頂部導覽列中，按一下**管理**。

2 在左面板中的**存取控制**下，按一下**角色**。

角色清單隨即顯示。

3 按一下要編輯的角色旁邊的選項按鈕，然後按一下**編輯**。

4 視需要修改角色設定。

a 變更角色的名稱，並選擇性地變更其說明。

b 編輯該角色的權限。

5 按一下**儲存**。

刪除角色

組織管理員可以使用租用戶入口網站，在其管理的組織中刪除角色物件。

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 在頂部導覽列中，按一下**管理**。

2 在左面板中的**存取控制**下，按一下**角色**。

角色清單隨即顯示。

3 按一下要刪除的角色旁邊的選項按鈕，然後按一下**刪除**。

4 按一下**確定**，即可確認您要刪除該角色。

設定身分識別提供者

14

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。

可以讓您的組織使用 SAML 身分識別提供者，也可以設定 LDAP 伺服器連線。

本章節討論下列主題：

- 允許您的組織使用 SAML 身分識別提供者
- 編輯組織的 LDAP 設定
- 設定、測試和同步 LDAP 連線

允許您的組織使用 SAML 身分識別提供者

允許您的組織使用安全性聲明標記語言 (SAML) 身分識別提供者 (亦稱為單一登入)，以從 SAML 身分識別提供者匯入使用者與群組，並允許匯入的使用者使用在 SAML 身分識別提供者中建立的認證登入組織。

在匯入使用者和群組時，系統會從 SAML Token 擷取一系列屬性 (如果有)，並使用它們來解譯嘗試登入之使用者的相關資訊。

- `email address = "EmailAddress"`
- `user name = "UserName"`
- `full name = "FullName"`
- `user's groups = "Groups"`
- `user's roles = "Roles"`

  您可以設定角色屬性。

如果沒有直接匯入使用者，但仍期望可以憑藉已匯入群組的成員資格登入，則必須提供群組資訊。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，則僅可透過 API 設定此屬性名稱，並且僅可設定 [角色] 屬性。如果使用**遵從身分識別提供者**角色，但沒有可擷取的角色資訊，則使用者可以登入，但沒有執行任何活動的權限。

必要條件

- 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。

- 確認您具有 SAML 2.0 相容身分識別提供者的存取權。
- 確認您收到來自 SAML 身分識別提供者的必要中繼資料。您必須將此中繼資料手動或以 XML 檔案形式匯入 VMware Cloud Director。此中繼資料必須包含下列資訊：
  - 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 身分識別提供者的說明文件。

程序

1 在頂部導覽列中，按一下**管理**。

2 在**身分識別提供者**下，按一下 **SAML**。

3 按一下**編輯**。

4 在**服務提供者**索引標籤上，輸入實體識別碼。

  實體識別碼是您的組織針對身分識別提供者的唯一識別碼。您可以使用您的組織名稱，或符合 SAML 身分識別提供者需求的任何其他字串。

  重要 一旦指定實體識別碼，您便無法將其刪除。若要變更實體識別碼，您必須對組織執行完整的 SAML 重新設定。如需實體識別碼的相關資訊，請參閱《OASIS Security Assertion Markup Language (SAML) 2.0 適用的判斷提示和通訊協定》。

5 按一下**中繼資料**連結下載您組織的 SAML 中繼資料。

  必須按原樣將已下載的中繼資料提供給您的身分識別提供者。

6 檢閱憑證到期日期，然後選擇性地按一下重新產生來重新產生用於簽署同盟訊息的憑證。

  此憑證包含在 SAML 中繼資料中，可同時用於加密和簽署。根據您組織與 SAML 身分識別提供者之間建立信任的方式，可能需要加密和簽署中的一個或兩者都需要。

7 在**身分識別提供者**索引標籤上，啟用**使用 SAML 身分識別提供者**切換按鈕。

8 複製您收到的來自身分識別提供者的 SAML 中繼資料並貼到文字方塊中，或按一下**上傳**以瀏覽至 XML 檔案並上傳其中的中繼資料。

9 按一下**儲存**。

後續步驟

- 使用 VMware Cloud Director 中繼資料設定 SAML 提供者。請參閱 SAML 身分識別提供者說明文件和《VMware Cloud Director 安裝、設定與升級指南》。
- 從 SAML 身分識別提供者匯入使用者與群組。請參閱第 13 章 管理使用者、群組和角色

編輯組織的 LDAP 設定

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。

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 在頂部導覽列中，按一下**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。

3 在 **LDAP 設定**索引標籤上，按一下**編輯**。

4 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。
VMware Cloud Director 系統 LDAP 服務	組織將使用由您的服務提供者設定的 VMware Cloud Director 系統 LDAP 連線。 輸入組織單位的辨別名稱。
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。

後續步驟

如果您已選取**自訂 LDAP 服務**，請按一下**自訂 LDAP** 索引標籤以設定、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。

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 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。

管理憑證

15

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。

本章節討論下列主題：

- 匯入受信任的憑證
- 將憑證匯入至憑證程式庫

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〉。

必要條件

確認您是以**系統管理員**或**組織管理員**的身分登入。

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。

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〉。

必要條件

確認您是以**系統管理員**或**組織管理員**的身分登入。

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。

管理您的組織

16

做為**組織管理員**，您可以修改組織內的各種設定。您可以修改組織名稱、電子郵件設定、網域設定、中繼資料、原則等。

您可以使用 VMware Cloud Director API，透過 MQTT 通訊協定來訂閱有關組織中的事件和工作的訊息。請參閱《VMware Cloud Director 安裝、設定與升級指南》中使用 MQTT 用戶端來訂閱事件和工作的相關資訊。

本章節討論下列主題：

- 編輯組織名稱和說明
- 修改電子郵件設定
- 測試 SMTP 設定
- 修改組織中虛擬機器的網域設定
- 使用多個站台
- 設定和管理多站台部署
- 瞭解租用
- 修改組織內的 vApp 和 vApp 範本租用原則
- 修改組織中的密碼和使用者帳戶原則
- 建立建議儀表板

編輯組織名稱和說明

您可以編輯組織的全名和說明。

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 在頂部導覽列中，按一下**管理**。

2 在**設定**下，按一下**一般**。

此時會顯示一般設定清單，例如組織名稱、預設 URL、全名和說明。

3 若要修改組織的全名和說明，請按一下**編輯**。

4 套用必要的變更，然後按一下**儲存**。

修改電子郵件設定

您可以檢閱和修改系統管理員在建立您組織時所設定的預設電子郵件設定。

需要報告重要資訊時 (例如，資料存放區空間不足時)，VMware Cloud Director 會傳送警示電子郵件。依預設，組織會使用在系統層級指定的 SMTP 伺服器，傳送電子郵件警示給系統管理員或傳送在系統層級指定的電子郵件地址清單。如果您想要 VMware Cloud Director 將組織的警示傳送至與在系統層級所指定的電子郵件地址不同的電子郵件地址組，或者您想要組織使用與在系統層級指定的伺服器不同的 SMTP 伺服器來傳送警示，則您可以在組織層級修改電子郵件設定。

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 在頂部導覽列中，按一下**管理**。

2 在**設定**下，按一下**電子郵件**。

此時會顯示組織的電子郵件設定。

3 按一下**編輯**。

4 在 **SMTP 伺服器**索引標籤上編輯 SMTP 伺服器設定。

a 選取使用自訂 SMTP 伺服器還是預設伺服器。

b 如果您選取使用自訂 SMTP 伺服器，請在 **SMTP 伺服器名稱**文字方塊中輸入 SMTP 伺服器的 DNS 主機名稱或 IP 位址。

c (選擇性) 輸入 SMTP 伺服器連接埠。

d (選擇性) 選取是否需要驗證，然後輸入使用者名稱和密碼。

5 若要編輯通知設定，請按一下**通知設定**索引標籤。

a 選取此項可使用自訂通知設定。

b 輸入將顯示為組織電子郵件寄件者的電子郵件地址。

c (選擇性) 輸入要用作電子郵件主旨前置詞的文字。

d (選擇性) 選取將通知傳送到所有組織管理員還是特定電子郵件地址。

e (選擇性) 如果您選取將通知傳送至特定電子郵件地址，請輸入電子郵件地址 (以逗號分隔)。

6 按一下**儲存**。

測試 SMTP 設定

修改組織的電子郵件設定後，您可以測試 SMTP 設定。

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 在頂部導覽列中，按一下**管理**。

2 在**設定**下，按一下**電子郵件**。

此時會顯示組織的電子郵件設定。

3 按一下**測試**。

4 輸入目的地電子郵件地址和 SMTP 伺服器密碼以測試 SMTP 設定，然後按一下**測試**按鈕。

修改組織中虛擬機器的網域設定

您可以設定組織中所建立之虛擬機器可加入的預設 Windows 網域。無論是否指定預設網域，虛擬機器始終可以加入它們具有認證的網域。

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 在頂部導覽列中，按一下**管理**。

2 在**設定**下，按一下**客體個人化**。

3 選取此項可為組織中的虛擬機器啟用網域加入功能。

4 輸入網域名稱、使用者名稱和密碼。

輸入的認證適用於一般網域使用者，而不是網域管理員。

5 (選擇性) 輸入帳戶組織單位。

6 按一下**儲存**。

使用多個站台

VMware Cloud Director 多站台功能可讓有多個 VMware Cloud Director 安裝 (伺服器群組) 分散在不同地理位置的服務提供者或承租人，以單一實體形式管理和監控這些安裝及其組織。

VMware Cloud Director 租用戶入口網站可讓**組織管理員**在相關聯站台中關聯組織。

如需有關站台關聯的詳細資訊，請參閱《VMware Cloud Director Service Provider Admin Portal 指南》。

設定和管理多站台部署

在**系統管理員**關聯兩個站台後，任何成員站台上的**組織管理員**均可開始關聯其組織。

若要建立兩個組織之間的關聯 (以下稱為 Org-A 和 Org-B)，您必須是這兩個組織的**組織管理員**，以便您可以登入每個組織、擷取其本機關聯資料，以及提交擷取的資料至其他組織。

重要 關聯兩個組織的程序可以邏輯方式分解為兩次互補配對作業。第一次作業 (在此範例中) 將 Site-A 中的 Org-A 與 Site-B 中的 Org-B 配對。然後，必須將 Site-B 中的 Org-B 與 Site-A 中的 Org-A 配對。直到這兩個配對完成為止，關聯程序才算完成。

必要條件

- 組織佔用的站台必須相關聯。
- 您必須是兩個站台的**系統管理員**或兩個組織的**組織管理員**。

程序

1 登入 Site-A 中的 Org-A 的 VMware Cloud Director 租用戶入口網站以擷取其本機關聯資料。
   a 按一下**管理**。
   b 在**設定**下，按一下**多站台**。
   c 若要以 XML 格式下載資料，請按一下**匯出本機關聯資料**。
      瀏覽器會將檔案中的資料儲存到下載資料夾中。
2 登入 Site-B 中的 Org-B 的 VMware Cloud Director 租用戶入口網站，從 Site-A 中的 Org-A 提交本機關聯資料。
   a 按一下**管理**。
   b 在**設定**下，按一下**多站台**。
   c 按一下**建立新組織關聯**。
      透過按一下**新的關聯 XML** 文字方塊下的上傳箭頭並選取步驟 步驟 1 中所下載的本機關聯資料，將在步驟 步驟 1 中所下載的關聯資料提交至 Org-B。
   d 按**下一步**以確認並提交資料。
      系統將 Site-A 中的 Org-A 與 Site-B 中的 Org-B 配對。
   e 按一下**完成**，以檢視相關聯的組織。
   f 若要檢視相關聯組織的詳細資料或刪除關聯，請按一下**組織名稱**卡。
3 透過重複步驟 1 和步驟 2 完成關聯，以從 Org-B 擷取本機關聯資料並將其提交至 Org-A。

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，如果某使用者啟動 vApp 後外出度假，但未停止 vApp，該 vApp 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。

修改組織內的 vApp 和 vApp 範本租用原則

您可以檢閱和修改系統管理員在建立您組織時所設定的預設原則。

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 在頂部導覽列中，按一下**管理**。

2 在**設定**下，按一下**原則**。

您可以檢視**系統管理員**設定的預設原則。

3 按一下**編輯**。

4 編輯 vApp 租用。

vApp 租用藉由指定可執行 vApp 以及可儲存 vApp 的時間量上限，為組織的儲存與計算資源提供控制層級。您也可以指定 vApp 儲存區租用到期時對 vApp 的影響。

a 若要定義 vApp 自動停止前可執行的時間長度，請輸入執行階段租用上限。

b 選取執行階段到期動作，例如關閉電源或暫停。

c 若要定義已停止的 vApp 自動清除前保持可用的時間長度，請輸入儲存區租用上限。

d 選取儲存區清理動作，例如永久刪除 vApp 或將其移至到期項目。

5 編輯 vApp 範本租用。

vApp 範本租用藉由指定 vApp 範本可儲存的時間量上限，為組織的儲存與計算資源提供控制層級。您也可以指定 vApp 範本儲存區租用到期時對 vApp 範本的影響。

a 若要定義 vApp 範本自動清除前保持可用的時間長度，請輸入儲存區租用上限。

b 選取儲存區清理動作，例如永久刪除 vApp 範本或將其移至到期項目。

6 按一下**確定**。

修改組織中的密碼和使用者帳戶原則

您可以檢閱和修改系統管理員在建立您組織時所設定的預設密碼和使用者帳戶原則。

密碼和使用者帳戶原則定義在使用者輸入無效密碼時 VMware Cloud Director 的行為。

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 在頂部導覽列中，按一下**管理**。

2 在**設定**下，按一下**原則**。

您可以檢視**系統管理員**設定的預設原則。

3 按一下**編輯**。

4 在若干次無效的登入嘗試之後，啟用使用者帳戶鎖定。

5 輸入在帳戶鎖定前的無效登入嘗試次數。

6 輸入帳戶被鎖定的使用者無法重新登入的時間間隔 (以分鐘為單位)。

7 按一下**確定**。

建立建議儀表板

您可以建立顯示在 Tenant Portal 使用者介面頁面上方的通知。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。

必要條件

確認您是以**系統管理員**的身分登入。

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。

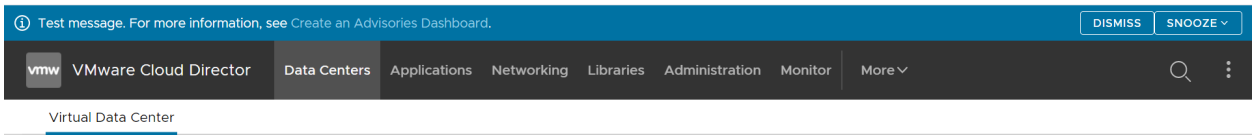
5 選取您希望在使用者介面中顯示通知的時段。

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 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。

使用服務程式庫

17

VMware Cloud Director 中的服務程式庫項目是 vRealize Orchestrator 工作流程，可延伸雲端管理功能，並讓提供者或承租人管理員能夠監控和操作各種服務。

本章節討論下列主題：

搜尋服務

VMware Cloud Director 租用戶入口網站中的**服務程式庫**頁面會列出一組已匯入 VMware Cloud Director 並發佈至您組織的 vRealize Orchestrator 工作流程。

必要條件

此作業要求服務程式庫權限包含在預先定義的使用者角色中。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在**服務**下，選取**服務程式庫**。

服務項目清單會以卡視圖顯示，每頁 12 個項目，根據名稱按字母順序排序。每張卡片會顯示服務的名稱以及對應匯入 vRealize Orchestrator 之服務類別的標籤。

2 在頁面頂部的**搜尋**文字方塊中，輸入服務名稱或服務所屬類別之名稱的第一個字組。

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

您可以從 VMware Cloud Director 租用戶入口網站的 [服務程式庫] 頁面執行服務。

必要條件

此作業要求服務程式庫權限包含在預先定義的使用者角色中。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在**服務**下，選取**服務程式庫**。

服務項目清單會以卡視圖顯示，每頁 12 個項目，根據名稱按字母順序排序。每張卡片會顯示服務的名稱以及對應匯入 vRealize Orchestrator 之服務類別的標籤。

2 搜尋您要執行的服務。

3 在服務卡上，按一下**執行**。

新的對話方塊隨即開啟。您必須輸入服務的必要輸入參數的值。

4 按一下**完成**以確認執行服務。

後續步驟

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。

管理定義的實體

18

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。如果服務提供者授與您存取權，您可以管理已定義的實體並與其他承租人共用這些實體。

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 - 當服務提供者建立 RDE 類型時，會為此類型建立權限服務包。服務提供者必須為您指派以下五個特定於類型的權限中的一或多個：**檢視：TYPE**、**編輯：TYPE**、**完全控制：TYPE**、**管理員檢視：TYPE** 以及**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。

表 18-1. 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。
	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。

表 18-1. RDE 作業的權限和 ACL 項目 (續)

實體作業	選項	描述
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。

與其他使用者共用定義的實體

如果**系統管理員**為已定義的實體類型發佈了權限服務包並授與您 `ReadWrite` 或 `FullControl` 權限，或者您是已定義實體的擁有者，則您可以與其他使用者共用這些實體的存取權。

1 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。

備註 您必須以**系統管理員**或**組織管理員**的身分登入以指派權限。

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。

2 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。

您必須對實體具有 `ReadWrite` 或 `FullControl` 權限，才能向該實體授與 ACL 存取權。

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。

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。

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。

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。

本章節討論下列主題：

- 使用自訂實體定義

使用自訂實體定義

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。VMware Cloud Director 組織內的使用者可以根據需要擁有、管理和變更這些類型。透過執行服務，組織使用者可以個體化自訂實體，並對物件的執行個體套用動作。

搜尋自訂實體

您可以搜尋已發佈至您組織的自訂實體。

必要條件

此作業要求自訂實體權限包含在預先定義的使用者角色中。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在**服務**下，選取**自訂實體定義**。

自訂實體清單會以卡視圖顯示，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。您無法變更實體類型或實體繫結到的 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。

必要條件

此作業要求自訂實體權限包含在預先定義的使用者角色中。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在**服務**下，選取**自訂實體定義**。

自訂實體清單會以卡視圖顯示，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。

必要條件

此作業要求自訂實體權限包含在預先定義的使用者角色中。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在**服務**下，選取**自訂實體定義**。

自訂實體清單會以卡視圖顯示，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。

必要條件

此作業要求自訂實體權限包含在預先定義的使用者角色中。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在**服務**下，選取**自訂實體定義**。

自訂實體清單會以卡視圖顯示，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。

必要條件

此作業要求自訂實體權限包含在預先定義的使用者角色中。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在**服務**下，選取**自訂實體定義**。

自訂實體清單會以卡視圖顯示，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定義的關聯

您可以從相關聯的動作清單中移除 vRealize Orchestrator 工作流程。

必要條件

此作業要求自訂實體權限包含在預先定義的使用者角色中。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在**服務**下，選取**自訂實體定義**。

自訂實體清單會以卡視圖顯示，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。

必要條件

此作業要求自訂實體權限包含在預先定義的使用者角色中。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在**服務**下，選取**自訂實體定義**。

自訂實體清單會以卡視圖顯示，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。

必要條件

此作業要求自訂實體權限包含在預先定義的使用者角色中。

程序

1 在頂部導覽列中，按一下**程式庫**，然後在**服務**下，選取**自訂實體定義**。

自訂實體清單會以卡視圖顯示，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。