VMware Cloud Director 租户门户指南

2020 年 4 月 9 日

VMware Cloud Director 10.1

您可以从 VMware 网站下载最新的技术文档：

https://docs.vmware.com/cn/。

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

威睿信息技术（中国）有限公司
北京办公室
北京市
朝阳区新源南路 8 号
启皓北京东塔 8 层 801
www.vmware.com/cn

上海办公室
上海市
淮海中路 333 号
瑞安大厦 804-809 室
www.vmware.com/cn

广州办公室
广州市
天河路 385 号
太古汇一座 3502 室
www.vmware.com/cn

目录

VMware Cloud Director™ 租户门户指南

《VMware Cloud Director™ 租户门户指南》提供了有关如何使用 VMware Cloud Director 租户门户的信息。在此版本中，您可以使用租户门户管理您的组织，以及创建和配置虚拟机、vApp 以及 vApp 中的网络。您还可以配置 VMware Cloud Director 环境中的 VMware NSX® for vSphere® 提供的高级网络连接功能。使用 VMware Cloud Director 租户门户，您还可以创建和管理目录、vApp 和 VDC 模板，以及创建和管理跨虚拟数据中心网络。

目标读者

本指南适合于要使用 VMware Cloud Director 租户门户功能的任何人。本指南的目标读者为使用租户门户管理组织、管理虚拟机、vApp、网络等的**组织管理员**。

VMware 技术出版物术语表

VMware 技术出版物术语表汇编了您可能不熟悉的术语。有关 VMware 技术文档中所使用的术语的定义，请访问 http://www.vmware.com/support/pubs。

VMware Cloud Director 租户门户入门

1

登录到租户门户时，您可以完成多项任务：从创建虚拟机和 vApp 到设置高级网络连接配置和运行 vRealize Orchestrator 工作流。

本章讨论了以下主题：

了解 VMware Cloud Director™

VMware Cloud Director™ 提供对基于 Web 的租户门户的基于角色的访问，组织成员可通过基于 Web 的租户门户与组织资源交互，从而创建并使用 vApp 和虚拟机。

VMware Cloud Director **系统管理员**必须先创建组织、分配资源并提供访问租户门户的 URL，然后您才能访问组织。每个组织包括一个或多个**组织管理员**，他们通过添加成员并设置策略和首选项来完成组织设置。设置组织之后，非管理员用户可以登录该组织，创建、使用并管理虚拟机和 vApp。

组织

组织是用于管理一批用户、组和计算资源的单元。用户将在组织级别进行身份验证，并提供在创建或导入该用户时由**组织管理员**设置的凭据。**系统管理员**可以创建并置备组织，而**组织管理员**则可管理组织用户、组和目录。

用户和组

组织可以包含任意数量的用户和组。用户可以由组织管理员本地创建，也可以从目录服务中导入。而组则必须从目录服务中导入。组织中的权限是通过为用户和组分配权限和角色来控制的。

虚拟数据中心

组织虚拟数据中心为组织提供资源。虚拟数据中心提供了一个可以存储、部署和操作虚拟系统的环境。它们还为虚拟 CD 和 DVD 媒体提供存储空间。一个组织可以有多个虚拟数据中心。

组织虚拟数据中心网络

组织虚拟数据中心网络包含在 VMware Cloud Director 组织虚拟数据中心内，并可用于组织中的所有 vApp。组织虚拟数据中心网络允许组织内的 vApp 相互通信。组织虚拟数据中心网络可以连接到外部网络，或者进行隔离，仅供组织内部使用。只有**系统管理员**才能创建组织虚拟数据中心网络，但**组织管理员**可以管理组织虚拟数据中心网络，包括其提供的网络服务。

vApp 网络

vApp 网络包含在 vApp 内，并允许 vApp 中的虚拟机相互通信。如果组织虚拟数据中心网络连接到外部网络，则您可以将 vApp 网络连接到组织虚拟数据中心网络，以允许 vApp 与组织内外的其他 vApp 通信。

目录

组织使用目录来存储 vApp 模板和媒体文件。具有目录访问权限的组织成员可以使用目录的 vApp 模板和媒体文件来创建自己的 vApp。**组织管理员**可以将公用目录中的项复制到组织目录。

专用 vCenter Server 实例 (SDDC) 和代理

软件定义的数据中心 (SDDC) 封装整个 vCenter Server 环境。一个专用 vCenter Server 实例可以包含一个或多个代理，可通过这些代理访问底层环境中的不同组件。**系统管理员**可以向您的组织发布一个或多个专用 vCenter Server 实例。您可以使用包含的代理访问代理组件的 UI 或 API。

登录到 VMware Cloud Director 租户门户

您可以使用特定于您组织的 URL 访问 VMware Cloud Director 租户门户。

如果您不知道租户门户组织 URL，请与**组织管理员**联系。有关支持的浏览器和配置的信息，请参见《VMware Cloud Director 发行说明》。

步骤

1 在 Web 浏览器中，导航到您组织的租户门户 URL。

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

2 输入您的用户名和密码，然后单击**登录**。

VMware Cloud Director 租户门户角色和权限

VMware Cloud Director 包含一组预配置的用户角色及其权限。能够访问 VMware Cloud Director 租户门户的角色是任何组织中默认创建的角色或由组织管理员创建的其他角色。

分配有以下组织角色的用户可以访问租户门户。他们看到的项目以及能够执行的操作取决于与特定角色相关联的权限。

- **组织管理员**
- **目录作者**
- **vApp 作者**
- **vApp 用户**
- **仅控制台访问权限**

有关预定义的角色及其权限的信息，请参见预定义角色及其权限。

使用 VMware Cloud Director 租户门户

如果您有多个虚拟数据中心，则在登录到 VMware Cloud Director 租户门户时，系统将导航到**数据中心**仪表板屏幕。如果您只有一个虚拟数据中心，则登录到 VMware Cloud Director 租户门户时，您会直接导航到该数据中心。

数据中心仪表板屏幕是 VMware Cloud Director 多站点功能的一部分，租户可以通过该屏幕将其分布在多个地理位置的云环境视为一个实体。有关多站点的详细信息，请参见使用多个站点。

仪表板不仅是单个组织中 VMware Cloud Director 虚拟数据中心和站点的统一视图。在多单元和多组织环境中，您还可以查看所有其他关联组织的虚拟数据中心。

注 根据所具有的权限，租户用户可以查看组织中的所有成员站点或部分站点。

在摘要功能区的顶部会显示有关组织的信息。

如果您以**组织管理员**身份登录，则可以看到：

- 站点、组织和虚拟数据中心的数量
- 正在运行的 vApp 和虚拟机总数
- 已用硬件资源，如 CPU、内存和存储

此时会以卡片视图显示虚拟数据中心。每个卡片均包含虚拟中心所属的组织、vApp 数量、虚拟机总数和处于运行状态的虚拟机数量的相关信息。卡片还显示数据中心的可用 CPU、内存和存储容量，并显示有关资源当前分配和预留的实时衡量指标。

从顶部导航区域中，可以导航到不同的菜单项。

菜单项	描述
数据中心	导航到组织中的**数据中心**、**数据中心组**和**专用 vSphere 数据中心**资源
虚拟数据中心	导航到显示组织内虚拟数据中心的**虚拟数据中心**屏幕。
数据中心组	导航到管理跨虚拟数据中心网络的**数据中心组**屏幕。默认情况下，只有**系统管理员**才可以查看此菜单项。
专用 vSphere 数据中心	导航到显示服务提供商已发布到组织的专用 vSphere 数据中心的屏幕。
应用程序	导航到组织中的**虚拟应用程序**和**虚拟机**资源。
库	将您导航到 vApp 模板、目录、媒体和其他类型文件的整合视图。使用这些模板和文件可部署虚拟机或 vApp。
管理	导航到**访问控制**、**身份提供程序**配置屏幕，以及组织的常规、电子邮件、客户机个性化、元数据、多站点和策略设置。
监控	导航到**任务**和**事件**屏幕。**任务**屏幕会显示 VMware Cloud Director 报告的任务。**事件**屏幕则显示 VMware Cloud Director 报告的事件。

您可以使用 `Branding` Cloud Director OpenAPI 来自定义 VMware Cloud Director 租户门户。有关使用 Cloud Director OpenAPI 的信息，请参见《Cloud Director OpenAPI 入门指南》文档，网址为 https://code.vmware.com。

使用 VMware Cloud Director 全局搜索

您可以使用 VMware Cloud Director 全局搜索按名称或部分名称搜索您环境中的对象名称。如果虚拟机的 IP 地址是静态的，您也可以根据其 IP 地址搜索虚拟机。

预设对象列表为：

- 数据中心
- vApp 模板
- vApp
- 虚拟机
- vApp 网络
- 目录

如果虚拟机使用由 DHCP 分配的 IP 地址，则搜索不会返回其 IP 地址。如果要搜索使用 DHCP 分配的 IP 地址的虚拟机，必须按名称进行搜索。

默认情况下，您只能搜索本地站点中的对象。如果您具有多站点环境，则可以在多个站点之间进行搜索。

步骤

1 在 VMware Cloud Director 租户门户的右上角，单击**搜索** () 图标。

2 （可选） 通过单击**固定** () 图标来固定搜索面板。

3 在**搜索**文本框中，输入作为搜索依据的符号、部分名称或 IP 地址，以搜索匹配的对象名称或虚拟机的静态 IP 地址。

4 如果使用多站点环境，请选择要在其中执行搜索的站点。

5 按 **Enter** 键。

结果

将按对象类型显示前五个匹配结果。结果按字母顺序排序。

后续步骤

- 要查看更多结果（如有），请单击每个对象类型下的**加载更多**。
- 要从搜索结果中查看有关特定对象的详细信息，请指向该对象。
- 要管理特定对象（例如，要查看或修改某个对象的设置），请单击该对象。有关对象的详细信息将在左侧显示。

查看任务

在租户门户中，您可以查看近期任务列表以及任务的详细信息和状态。此外，还可以查看所有任务列表。

默认情况下，**近期任务**面板显示在租户门户的底部，其中包含近期运行的任务列表。启动某个操作时，例如创建虚拟机，该任务将显示在此面板中。最小化**近期任务**面板后，仍能看到正在运行的或已失败的近期任务数量。单击双箭头，随时可以再次打开**近期任务**面板。

任务视图中将列出所有任务，并显示任务运行的时间，以及它们是否已成功完成。此视图是对您所在环境中的问题进行故障排除的第一步。任务视图包含长时间运行的操作，如虚拟机或 vApp 创建。

步骤

1 在顶部导航栏中，单击**监控**和**任务**。

此时将显示所有任务列表以及任务运行时间和任务状态。

2 单击编辑器图标 () 以更改您要查看的任务的详细信息。

3 （可选） 要查看任务详细信息，请单击任务名称。

任务详细信息包括失败原因、失败时间等信息。

详细信息	描述
操作	所执行操作的名称。
作业 ID	任务的 ID。
类型	在其中执行任务的对象。例如，如果您创建的是虚拟机，则类型为 vm。
组织	组织名称。
状态	任务状态，如“成功”、“正在运行”或“失败”。
启动者	启动操作的用户。
开始时间	操作开始的日期和时间。

详细信息	描述
完成时间	操作成功或失败的日期和时间。
服务名称空间	服务名称，如 *com.vmware.cloud*。
详细信息	任务失败的原因。例如，如果尝试创建虚拟机的快照，但因存储空间不足导致操作失败，任务详细信息的类型为：请求的操作将超出 VDC 的存储配额：存储策略 "*" 剩余 8,693 MB，已请求 41,472 MB (The requested operation will exceed the VDC's storage quota: storage policy "*" has 8,693 MB remaining, requested 41,472 MB)。

停止正在进行的任务

如果在应用或检查所有必要设置之前意外启动某个操作，您可以停止正在进行的任务。

默认情况下，**近期任务**面板显示在门户的底部。启动某个操作时，例如创建虚拟机，该任务将显示在此面板中。

前提条件

近期任务面板必须处于打开状态。

步骤

1 启动长时间运行的操作。

长时间运行的操作包括创建虚拟机或 vApp、在虚拟机和 vApp 上执行的电源操作等。

2 在**近期任务**面板中，单击**取消**图标 ( )。

3 在**取消任务**对话框中，单击**确定**确认取消任务。

结果

该操作将停止。

查看事件

在门户中，您可以查看所有事件的列表及其详细信息和状态。

通过事件视图可以在门户中查看事件的状态。该视图显示事件的发生时间以及成功与否。事件视图中包含一次性事件，例如用户登录和对象创建或删除。

步骤

1 在顶部导航栏中，单击**监控**和**事件**。

将显示所有事件的列表以及事件发生时间和事件状态。

2 单击编辑器图标 ( ) 以更改您要查看的有关事件的详细信息。

3 （可选） 单击事件以查看事件详细信息。

详细信息	描述
事件	事件的名称。 例如，如果您修改 vApp 以在其中包含虚拟机，启动整个操作的事件是 *Task 'Modify vApp' start*。
事件 ID	任务的 ID。
类型	在其中执行任务的对象。例如，如果您创建的是虚拟机，则类型为 *vm*。
目标	事件的目标对象。 例如，修改 vApp 以在其中包含虚拟机时，*Task 'Modify vApp' start* 事件的目标为 *vdcUpdateVapp*。
状态	事件的状态，如“成功”或“失败”。
服务名称空间	服务名称，如 *com.vmware.cloud*。
组织	组织的名称。
所有者	触发事件的用户。
发生时间	事件发生的日期和时间。

设置用户首选项

您可以设置每次登录到系统时将生效的某些显示和系统警示首选项。

要了解有关租约的更多信息，请参见了解租约。

步骤

1 在顶部导航栏中，单击您的用户名，然后选择**用户首选项**。

2 选择登录时将显示的页面。

a 选择**开始页面**旁边的单选按钮，然后单击**编辑**。

b 从下拉菜单中选择一个选项，然后单击**保存**。

3 配置运行时租约过期时使用的电子邮件通知。

a 选中**部署租约警示时间**旁边的单选按钮，然后单击**编辑**。

b 输入以秒为单位的一个值，然后单击**保存**。

4 配置存储租约过期时使用的电子邮件通知。

a 选中**存储租约警示时间**旁边的单选按钮，然后单击**编辑**。

b 输入以秒为单位的一个值，然后单击**保存**。

使用虚拟机

2

与物理机一样，虚拟机是运行操作系统和应用程序的软件计算机。虚拟机包含一组规范和配置文件，并由主机的物理资源提供支持。每个虚拟机都具有一些虚拟设备，这些设备可提供与物理硬件相同的功能，但可移植性更强、更安全且更易于管理。

除了可在物理机上运行的操作外，VMware Cloud Director 虚拟机还支持虚拟基础架构操作，如创建虚拟机状态的快照，以及将虚拟机从一台主机移到另一台主机。

从 VMware Cloud Director 9.5 开始，虚拟机支持 IPv6 连接。可以将 IPv6 地址分配给连接到虚拟机的 IPv6 网络。

重要事项 使用虚拟机的所有步骤从卡片视图进行记录，且假定您具有多个虚拟数据中心。从网格视图也可以完成同样的过程，但步骤可能会略有不同。

本章讨论了以下主题：

- 监控虚拟机
- 使用快照
- 续订虚拟机租约
- 删除虚拟机

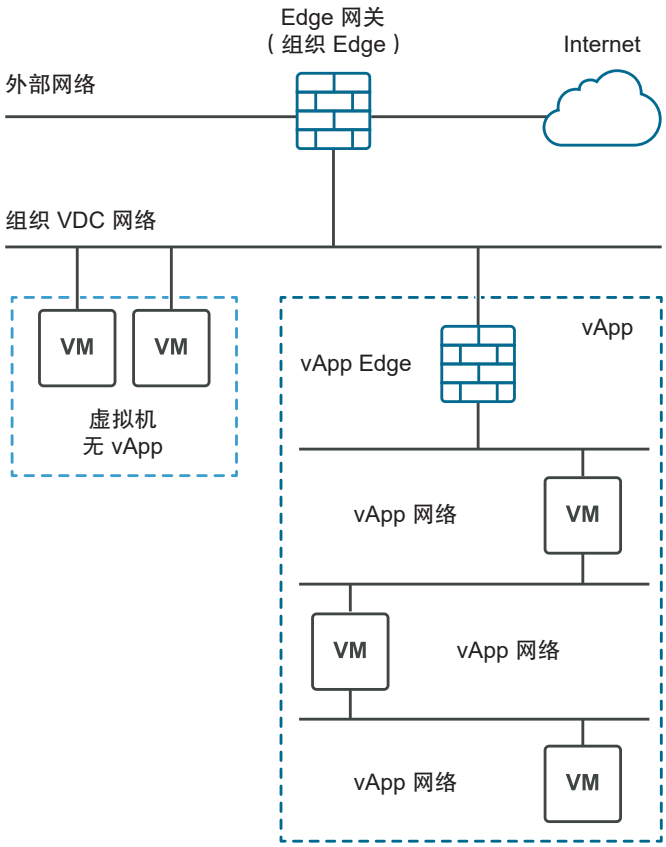
虚拟机架构

虚拟机可以作为独立计算机存在，也可以存在于 vApp 内。

与物理机一样，虚拟机是运行操作系统和应用程序的软件计算机。虚拟机包含一组规范和配置文件，并由主机的物理资源提供支持。每个虚拟机都具有一些虚拟设备，这些设备可提供与物理硬件相同的功能，但可移植性更强、更安全且更易于管理。虚拟机可以是独立计算机，也可以存在于 vApp 内。vApp 是一个或多个虚拟机以及一个或多个网络组成的复合对象。

下图显示了创建虚拟机时可供使用的不同选项。可以创建独立虚拟机，也可以在 vApp 内创建虚拟机。独立虚拟机直接连接到组织虚拟数据中心。您也可以在 vApp 内创建虚拟机。通过在 vApp 内创建虚拟机，您可以将多个虚拟机及其关联网络分组在一起。vApp 可用于构建复杂应用程序，并将其保存到目录以供将来使用。

图 2-1. 虚拟机独立存在或存在于 vApp 内



虚拟机加密

从 VMware Cloud Director 10.1 开始，可以使用 VM 加密提高数据的安全性。通过将 VM 和磁盘与具有 VM 加密功能的存储策略相关联，可对 VM 和磁盘进行加密。

加密不仅能保护虚拟机，而且还能保护虚拟机磁盘和其他文件。可以在 API 和 UI 中查看存储策略的功能以及 VM 和磁盘的加密状态。可以对相应 vCenter Server 版本中支持的加密 VM 和磁盘执行所有操作。

如果组织 VDC 使用已启用虚拟机加密的存储策略，则可以对虚拟机和磁盘进行加密。请参见《VMware Cloud Director 服务提供商管理门户指南》中的在组织虚拟数据中心的存储策略上启用 VM 加密主题。要对 VM 或磁盘进行加密，请将其与启用了 VM 加密的存储策略相关联。对于虚拟机，请参见创建新的独立虚拟机或更改虚拟机的常规属性。对于命名磁盘，请参见创建给定磁盘或编辑给定磁盘。要解密 VM 或磁盘，请将该 VM 或磁盘与未启用加密的存储策略相关联。

VM 加密限制

VMware Cloud Director 10.1 中不支持以下操作。

- 对打开电源的 VM 或其磁盘进行加密或解密。
- 导出加密 VM 的 OVF。
- 具有快照的 VM 的磁盘是快照的一部分时，对这些磁盘进行加密和解密。
- 当 VM 磁盘基于加密策略时对 VM 进行解密。
- 将加密磁盘添加到未加密 VM。
- 对未加密 VM 上的现有磁盘进行加密。
- 将已加密的给定磁盘添加到未加密 VM。
- 创建加密的链接克隆。
- 对链接克隆 VM 或其磁盘进行加密。
- 在源 VM 已加密时，跨 vCenter Server 实例实例化、移动或克隆 VM。

注 在快速置备的组织 VDC 上，如果源 VM 或目标 VM 已加密且您要创建克隆，VMware Cloud Director 始终会创建一个完整克隆。

了解 VM 加密存储功能

默认情况下，**系统管理员**和**组织管理员**具有查看组织 VDC 存储功能以及 VM 和磁盘是否已加密所需的权限。**vApp 作者**可以在虚拟机的**详细信息**页面上查看虚拟机及其磁盘的加密状态。有关角色和权限的详细信息，请参见预定义角色及其权限。

查看虚拟机

您可以查看独立的虚拟机或包含在 vApp 中的虚拟机。您可以用网格视图或卡片视图查看虚拟机。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。

2 选择以下方法之一。

- 要在网格视图中查看虚拟机，请单击 
- 要在卡片视图中查看虚拟机，请单击  。

虚拟机列表将显示在网格视图中或显示为卡片列表。

3 （可选） 从**排序依据**下拉菜单中排列虚拟机列表。

4 （可选） 在网格视图中，单击虚拟机左侧的 ，以显示可对选定虚拟机执行的操作。

例如，可以关闭虚拟机。

5 要访问虚拟机客户机操作系统的接口，请单击卡片视图右上角的桌面图标。

6 要查看和编辑虚拟机的详细信息，请单击**详细信息**。

创建新的独立虚拟机

您可以创建新的独立虚拟机。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。

2 单击  ，在卡片视图中查看列表，并（可选）从**排序依据**下拉菜单中排列虚拟机列表。

3 单击**新建虚拟机**。

4 输入虚拟机的名称和计算机名称。

重要事项 计算机名称只能包含字母数字字符和连字符。计算机名称不能仅包含数字，并且不能包含空格。

5 （可选） 输入有意义的描述。

6 选择是否要在虚拟机创建后立即打开电源。

7 选择希望部署虚拟机的方式。

选项	操作
新建	使用可自定义的设置部署新虚拟机。 a 选择操作系统系列和操作系统。 b （可选）选择引导映像。 c （可选）选择 VM 放置策略和 VM 大小调整策略。 仅当服务提供商将 VM 放置策略和 VM 大小调整策略发布到组织 VDC 时，此类策略下拉菜单才可见。 d （可选）从预定义的大小调整选项中选择虚拟机的大小，或单击**自定义大小调整选项**以手动输入虚拟 CPU 的数目、每个插槽内核数和内存设置。 如果选择定义 VM 大小的 VM 大小调整策略，则不会显示此选项。 虚拟机的预定义大小为：**小型**、**中型**和**大型**。 e 指定虚拟机的存储设置，例如存储策略和大小 (GB)。 f 指定虚拟机的网络设置，如网络、IP 模式、IP 地址和主网卡。
从模板	基于从模板目录选择的模板部署虚拟机。 a 从可用模板列表中选择一个虚拟机模板。 b （可选）选择 VM 放置策略和 VM 大小调整策略。 仅当服务提供商将 VM 放置策略和 VM 大小调整策略发布到组织 VDC 时，此类策略下拉菜单才可见。如果所选模板已分配有策略，则您可能只能使用预定义的模板策略。 c （可选）选择使用自定义存储策略，然后从**要使用的自定义存储策略**下拉菜单中选择要使用的存储策略。 d 阅读并接受最终用户许可协议（如有）。

8 单击**确定**保存虚拟机设置并启动创建过程。

目录中将显示虚拟机卡片。创建虚拟机之前，其状态显示为“忙碌”。

虚拟机快速置备

快速置备可为虚拟机置备操作使用链接克隆，从而帮助您节省时间。

链接克隆是虚拟机的副本，它使用与原始虚拟机相同的虚拟磁盘，并且有一个增量磁盘链用于跟踪原始虚拟机与克隆虚拟机之间的差异。如果禁用快速置备，则所有置备操作均会导致完整克隆。

链接克隆不能存在于不同于原始虚拟机的 vCenter Server 数据中心或数据存储上。

在快速置备 VM 时，VMware Cloud Director 会创建一个影子虚拟机，以支持跨 vCenter Server 数据中心和数据存储为与特定 vApp 模板关联的虚拟机创建链接克隆。

影子虚拟机是与原始虚拟机一模一样的副本。影子虚拟机是在创建链接克隆的数据中心和数据存储上创建的。

重要事项 利用本机快照的存储容器不支持就地整合快速置备的虚拟机。VVOL 和启用 VAAI 的数据存储使用本机快照，因此无法整合部署到这些存储容器的快速置备虚拟机。如果需要整合部署到 VVOL 或启用 VAAI 的数据存储的快速置备虚拟机，必须将其重新放置到不同的存储容器。

打开虚拟机控制台

通过访问虚拟机控制台，可以查看有关虚拟机的信息、使用客户机操作系统以及执行影响客户机操作系统的操作。

前提条件

虚拟机已启动。

在客户端上安装 VMware Remote Console

VMware Remote Console 在由 VMware Cloud Director 置备和管理的所有虚拟机中提供嵌入式用户-客户机交互。此部分详细介绍了在 Windows、 Apple OS X 和 Linux 上安装 VMware Remote Console 所需的任务。

前提条件

此操作需要预定义的 **vApp 用户**角色中包含的权限或一组等效权限。

步骤

1 下载安装程序。

- 导航到 VMware Remote Console 下载页面，然后选择与您的平台对应的链接。

  www.vmware.com/go/download-vmrc

- 在 VMware Cloud Director Tenant Portal 中的**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片。选择虚拟机，然后从**操作**菜单中选择**下载 VMRC** 。

2 运行您的平台安装。

- 如果使用的是 Windows，请双击 `.msi` 安装程序，然后按照提示进行操作。
- 如果使用的是 Linux，请使用 **root** 特权登录，运行 `.bundle` 安装程序，然后按照提示进行操作。
- 如果使用的是 Mac OS，请双击 `.dmg` 将其打开，然后双击其中的 VMware Remote Console 图标以复制到“应用程序”文件夹。

结果

安装完成后，单击以 `vmrc://` 方案开始的统一资源标识符 (Uniform Resource Identifiers, URI) 时，VMware Remote Console 即会打开。VMware Workstation、Player 和 Fusion 也会处理 `vmrc://` URI 方案。

打开虚拟机远程控制台

您可以通过 VMware Cloud Director 租户门户使用 VMware Remote Console 打开虚拟机控制台。

前提条件

- 验证 VMware Remote Console 是否已安装在本地系统上。
- 确保选定的虚拟机处于打开电源状态。

- 此操作需要预定义的 **vApp 用户**角色中包含的权限或一组等效权限。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。

2 单击  ，在卡片视图中查看列表，并（可选）从**排序依据**下拉菜单中排列虚拟机列表。

3 从虚拟机的**操作**菜单中，选择**启动虚拟机远程控制台**。

> 注 如果您没有安装 VMware Remote Console，会出现一个弹出窗口，提示您安装 VMware Remote Console 或使用 Web 控制台。

结果

虚拟机控制台将作为外部虚拟远程控制台打开。

注 使用 VMware Remote Console 连接到 VMware Cloud Director 虚拟机后，只能执行控制台交互（发送 `Ctrl+Alt+Del`）。您无法执行设备操作、电源操作或设置管理。

打开 Web 控制台

即使您的本地系统上没有安装 VMware Remote Console，也可以连接到虚拟机控制台。

前提条件

- 确认虚拟机已打开电源。
- 此操作需要预定义的 **vApp 用户**角色中包含的权限或一组等效权限。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。

2 单击  ，在卡片视图中查看列表，并（可选）从**排序依据**下拉菜单中排列虚拟机列表。

3 从虚拟机的**操作**菜单中，选择**启动 Web 控制台**。

结果

虚拟机控制台将使用 VMware HTML Console SDK 在新的浏览器选项卡中打开。

后续步骤

单击控制台窗口内的任何位置可在控制台中开始使用您的鼠标、键盘和其他输入设备。

注 有关受支持的国际键盘的信息，请参见 VMware HTML Console SDK 文档，网址为：https://www.vmware.com/support/developer/html-console/。

在虚拟机上执行电源操作

您可以在虚拟机上执行电源操作，例如打开或关闭虚拟机的电源、挂起或重置虚拟机或关闭虚拟机的客户机操作系统。

启动虚拟机

启动虚拟机相当于开启物理机的电源。

对于已启用客户机自定义的虚拟机，除非它已安装 VMware Tools 的当前版本，否则您无法启动它。

前提条件

虚拟机已关闭。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。

2 单击  ，在卡片视图中查看列表，并（可选）从**排序依据**下拉菜单中排列虚拟机列表。

3 从要打开电源的虚拟机的**操作**菜单中，选择**打开电源**。

结果

已打开电源的虚拟机显示为绿色的“已启动”状态。

关闭虚拟机

关闭虚拟机相当于关闭物理机的电源。

前提条件

虚拟机已启动。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。

2 单击  ，在卡片视图中查看列表，并（可选）从**排序依据**下拉菜单中排列虚拟机列表。

3 从要关闭电源的虚拟机的**操作**菜单中，选择**关闭电源**。

结果

已关闭电源的虚拟机显示为红色的“已关闭”状态。

关闭客户机操作系统

关闭虚拟机的客户机操作系统相当于关闭物理机的电源。

前提条件

必须已启动虚拟机和客户机操作系统。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。

2 单击  ，在卡片视图中查看列表，并（可选）从**排序依据**下拉菜单中排列虚拟机列表。

3 从虚拟机的**操作**菜单中，选择**关闭客户机操作系统**。

结果

客户机操作系统即会关闭。

重置虚拟机

重置虚拟机时将清除状态（内存和缓存等），但虚拟机仍可继续运行。重置虚拟机相当于按下物理机的重置按钮。它会启动操作系统的硬重置，但不更改虚拟机的电源状况。

前提条件

您的虚拟机已启动。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。

2 单击  ，在卡片视图中查看列表，并（可选）从**排序依据**下拉菜单中排列虚拟机列表。

3 从要重置的虚拟机的**操作**菜单中，选择**重置**。

结果

虚拟机的状态即被清除。

挂起虚拟机

挂起虚拟机会将内存写入磁盘，从而保留其当前状态。

当您要保存虚拟机的当前状态并在以后从此状态继续工作时，挂起和恢复功能将非常有用。

前提条件

虚拟机已启动。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。

2 单击  ，在卡片视图中查看列表，并（可选）从**排序依据**下拉菜单中排列虚拟机列表。

3 从要挂起的虚拟机的**操作**菜单中，选择**挂起**。

结果

虚拟机即会挂起，但其状态将保留。

放弃虚拟机的挂起状态

如果虚拟机处于挂起状态，且您不再需要继续使用该虚拟机，则可以放弃挂起状态。放弃挂起状态将释放保留的内存，并使虚拟机恢复到电源关闭状态。

前提条件

已挂起的虚拟机。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。

2 单击  ，在卡片视图中查看列表，并（可选）从**排序依据**下拉菜单中排列虚拟机列表。

3 从虚拟机的**操作**菜单中，选择**放弃挂起状态**。

结果

将放弃该状态且虚拟机电源关闭。

打开多个 VM 的电源

可以同时打开多个 VM 的电源。

对于已启用客户机自定义的虚拟机，除非它已安装 VMware Tools 的当前版本，否则您无法启动它。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。

2 启用**多选**选项。

3 选择要打开电源的 VM。

4 从**操作**菜单中，选择**启动**。

5 单击**确定**进行确认。

关闭多个虚拟机的电源

可以同时关闭多个 VM 的电源。

步骤

1. 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。
2. 启用**多选**选项。
3. 选择要关闭电源的 VM。
4. 从**操作**菜单中，选择**关闭**。
5. 单击**确定**进行确认。

放弃多个虚拟机的挂起状态

如果多个虚拟机处于挂起状态，并且您不再需要继续使用它们，则可以同时放弃这些虚拟机的挂起状态。放弃挂起状态将释放保留的内存，并使虚拟机恢复到电源关闭状态。

前提条件

确认虚拟机处于挂起状态。

步骤

1. 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。
2. 启用**多选**选项。
3. 选择要放弃其挂起状态的虚拟机。
4. 从**操作**菜单中选择**放弃已挂起状态**。
5. 单击**确定**进行确认。

重置多个虚拟机

同时重置多个 VM 将清除其状态（内存和缓存等），但 VM 仍继续运行。

重置虚拟机相当于按下物理机的重置按钮。它会启动操作系统的硬重置，但不更改虚拟机的电源状况。

前提条件

确认 VM 已打开电源。

步骤

1. 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。
2. 启用**多选**选项。
3. 选择要重置的 VM。

4 从**操作**菜单中，选择**重置**。

5 单击**确定**进行确认。

在虚拟机中安装 VMware Tools

VMware Cloud Director 凭借 VMware Tools 自定义客户机操作系统。

VMware Tools 可将通用操作系统驱动程序替换为针对虚拟硬件进行调优的 VMware 驱动程序，从而提高了虚拟机的管理和性能。VMware Tools 安装在客户机操作系统上。尽管客户机操作系统在不安装 VMware Tools 的情况下也可以运行，但这将失去重要的功能性和便利性。

前提条件

- 必须打开虚拟机的电源。
- 如果新创建的虚拟机没有客户机操作系统，则必须先安装它，然后才能安装 VMware Tools。
- 在安装 VMware Tools 之前，必须禁用客户机自定义。
- 如果 VMware Tools 的版本早于 vApp 虚拟机中的 7299，则必须升级。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。

2 单击  ，在卡片视图中查看列表，并（可选）从**排序依据**下拉菜单中排列虚拟机列表。

3 从要安装 VMware Tools 的虚拟机的**操作**菜单中，选择**安装 VMware Tools**。

VMware Tools 随即安装在目标客户机操作系统上。如果在安装期间出现错误，将显示一条错误消息。此外，还可以在**任务**窗口中查看安装操作的进度。

4 要打开虚拟机的 Web 控制台，请从**操作**菜单中选择**启动 Web 控制台**。

5 按照 VMware 知识库文章 1014294 的说明针对您特定的操作系统配置 VMware Tools。

结果

VMware Tools 即安装在客户机操作系统上并进行了相关配置。

升级虚拟机的虚拟硬件版本

您可以升级虚拟机的虚拟硬件版本。虚拟硬件版本越高，支持的功能越多。

您不能将 vApp 中虚拟机的硬件版本降级。

VMware Cloud Director 支持的硬件版本取决于支持 vSphere 资源。支持的硬件版本取决于备用提供者 VDC 中支持的最新虚拟硬件版本。**组织管理员**或**系统管理员**可以将硬件版本设置为低于基础硬件支持的最新版本。VMware Cloud Director 租户门户根据组织 VDC 或提供者 VDC 的支持硬件来动态设置可供选择的虚拟硬件版本列表。

有关通过虚拟机兼容性设置实现的硬件功能的信息，请参见《vSphere 虚拟机管理指南》。

有关 VMware 产品及其虚拟硬件版本的信息，请参见 https://kb.vmware.com/s/article/1003746。

前提条件

- 停止虚拟机或包含虚拟机的 vApp。
- 确认虚拟机上安装了最新版本的 VMware Tools。

步骤

1. 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。
2. 单击  ，在卡片视图中查看列表，并（可选）从**排序依据**下拉菜单中排列虚拟机列表。
3. 从要升级的虚拟机的**操作**菜单中选择**升级虚拟硬件版本**。
4. 单击**确定**。

结果

虚拟机即会升级到最新版本。

编辑虚拟机属性

可以编辑虚拟机的属性，其中包括虚拟机名称和描述、硬件和网络设置、客户机操作系统设置等。

更改虚拟机的常规属性

您可以查看并更改虚拟机的名称、描述和其他常规属性。

前提条件

更改操作系统等属性需要关闭计算机电源。

步骤

1. 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。
2. 单击  ，在卡片视图中查看列表，并（可选）从**排序依据**下拉菜单中排列虚拟机列表。
3. 在要编辑的虚拟机的卡中，单击**详细信息**。

4 可以在**常规**下查看或编辑的属性列表默认处于展开状态。

选项	操作
虚拟机名称	编辑虚拟机的名称。 虚拟机打开电源时，可以编辑此属性。
计算机名称	编辑在客户机操作系统中设置的用于标识网络上虚拟机的计算机名称和主机名。由于 Windows 操作系统对计算机名称的限制，此字段的长度限于 15 个字符。 虚拟机打开电源时，可以编辑此属性。
描述	编辑虚拟机的可选描述。 虚拟机打开电源时，可以编辑此属性。
操作系统系列	从下拉菜单中选择操作系统系列。 虚拟机关闭电源时，可以编辑此属性。此外，如果操作系统已存在于虚拟机上，则无法编辑此属性。
操作系统	从下拉菜单中选择操作系统。 虚拟机关闭电源时，可以编辑此属性。此外，如果操作系统已存在于虚拟机上，则无法编辑此属性。
引导延迟	指定引导操作的延迟时间（毫秒）。 启动虚拟机与其退出 BIOS 并启动客户机操作系统软件之间的时间可能非常短暂。您可以更改引导延迟，以提供更多时间。
存储策略	从下拉菜单中选择一个供虚拟机使用的存储策略。 虚拟机打开电源时，可以编辑此属性。
虚拟数据中心	查看此虚拟机所属的虚拟数据中心的名称。
VMware Tools	查看是否已在虚拟机上安装 VMware Tools。
虚拟硬件版本	查看虚拟机的虚拟硬件版本。
升级到:	要进行升级，请从下拉菜单中选择一个版本。
同步时间	选中此复选框，可以在虚拟机的客户机操作系统及其所在虚拟数据中心之间实现时间同步。
进入 BIOS 设置	选择是否强制虚拟机下次引导时进入 BIOS 设置屏幕。 虚拟机关闭电源时，可以编辑此属性。

5 更改完成后，单击**保存**。

更改虚拟机的硬件属性

可以查看和更改虚拟机的硬件属性。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。

2 单击  ，在卡片视图中查看列表，并（可选）从**排序依据**下拉菜单中排列虚拟机列表。

3 在要编辑的虚拟机的卡中，单击**详细信息**。

4 单击**硬件**以展开硬件属性列表，您可以查看和编辑该列表。

选项	描述
虚拟 CPU 的数量	编辑 CPU 的数量。 可以分配给虚拟机的最大虚拟 CPU 数量取决于主机上的逻辑 CPU 数量以及虚拟机上安装的客户机操作系统的类型。
每个插槽内核数	编辑每个插槽的内核数。 您可以根据内核数和每个插槽内核数配置虚拟 CPU 的分配方式。确定虚拟机中需要的 CPU 内核数，然后选择每个插槽中需要的内核数，具体取决于您需要单核 CPU、双核 CPU 还是三核 CPU 等等。
将硬件辅助的 CPU 虚拟化向客户机操作系统公开	可以向客户机操作系统公开整个 CPU 虚拟化，以便需要硬件虚拟化的应用程序在不需要进行二进制转换或准虚拟化的情况下可以在虚拟机上运行。
总内存	编辑虚拟机的内存资源设置。虚拟机内存大小必须是 4 MB 的倍数。 此设置确定了分配给虚拟机的 ESXi 主机内存量。虚拟硬件内存大小决定了在虚拟机中运行的应用程序可以使用的内存量。虚拟机内存资源多于配置的虚拟硬件内存大小时并不会带来优势。
内存热添加	如果启用内存热添加，则可以在虚拟机打开电源时向其添加内存资源。仅某些客户机操作系统和 7 以上的虚拟机硬件版本支持此功能。
虚拟 CPU 热添加	如果启用虚拟 CPU 热添加，则可以在虚拟机打开电源时向其添加虚拟 CPU。添加的 CPU 数量必须是每个插槽内核数的倍数。仅某些客户机操作系统和虚拟机硬件版本支持此功能。
插槽数	查看插槽数。 插槽数由可用虚拟 CPU 的数量决定。更新虚拟 CPU 数量时，此数值将更改。
可移除的媒体	查看可用的可移除媒体，如连接的 CD/DVD 和软盘驱动器。

5 在**硬盘**下，单击**添加**以添加硬盘。

选项	描述
大小	输入硬盘大小 (MB)。可以稍后增加硬盘的大小。 **注** 如果虚拟机不是链接克隆且没有快照，则可以增加现有硬盘的大小。
策略	默认使用虚拟机的存储策略。 默认情况下，连接到虚拟机的所有硬盘都使用为虚拟机指定的存储策略。创建虚拟机或修改其属性时，可以替代上述任何磁盘的默认设置。每个硬盘的“大小”列都包括一个下拉菜单，其中列出了可用于此虚拟机的所有存储策略。
IOPS	为磁盘选择特定的 IOPS。 使用此选项可限制每个磁盘每秒 I/O 操作数。
总线类型	选择总线类型。 选项包括**准虚拟 (SCSI)**、**LSI Logic 并行 (SCSI)**、**LSI Logic SAS (SCSI)**、**IDE** 和 **SATA**。有关存储控制器类型和兼容性的详细信息，请参见《vSphere 虚拟机管理指南》。
总线编号	输入总线编号。
单元编号	输入硬盘驱动器的逻辑单元号。

6 在**网卡**下，单击**添加**以添加新的网卡。

最多可以添加 10 个网卡。有关虚拟机硬件版本支持的网卡数量的信息，请参见：http://kb.vmware.com/s/article/2051652。VMware Cloud Director 支持在虚拟机运行时修改虚拟机网卡。有关受支持网络适配器类型的信息，请参见 http://kb.vmware.com/kb/1001805。

选项	描述
主网卡	选择主网卡后会显示一个标记。 选择主网卡。主网卡设置决定虚拟机的默认唯一网关。虚拟机可以使用任何网卡连接直接与网卡所在网络连接的虚拟机和物理机，但只能使用主网卡连接需要网关连接的网络上的计算机。
网卡	网卡数量。
已连接	选中该复选框以连接网卡。
网络	从下拉菜单中选择网络。
IP 模式	选择 IP 模式。 小心 如果已选择要将网卡连接到的网络，请勿将 IP 模式设置为**无**。 ■ **静态 - IP 池** 从网络 IP 池中获取静态 IP 地址。 ■ **静态 - 手动** 允许手动指定特定的 IP 地址。如果选择此选项，必须在 **IP 地址**列中键入 IP 地址。 ■ **DHCP** 从 DHCP 服务器获取 IP 地址。
MAC 地址	从下拉菜单中，选择是保留还是重置 MAC 地址。

7 单击**保存**。

更改虚拟机的客户机操作系统自定义属性

VMware Cloud Director 上的客户机操作系统自定义对于所有平台均为可选项。对于必须加入 Windows 域的虚拟机，则为必选项。

在此菜单上请求的某些信息仅适用于 Windows 平台。“客户机操作系统自定义”面板包含虚拟机加入 Windows 域所需的信息。**组织管理员**可以指定该组织中的 Windows 客户机可以加入的域的默认值。并非所有 Windows 虚拟机都必须加入域，但在大多数企业安装中，非域成员的虚拟机无法访问许多可用网络资源。

前提条件

- 此操作需要预定义的 **vApp 作者**角色中包含的权限或一组等效权限。
- 客户机自定义需要虚拟机运行 VMware Tools。
- 您的**系统管理员**必须在 VMware Cloud Director 服务器组中安装相应的 Microsoft Sysprep 文件，您才可以自定义 Windows 客户机操作系统。请参见《VMware Cloud Director 安装、配置和升级指南》。

- 自定义 Linux 客户机操作系统要求在客户机中已安装 Perl。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。

2 单击  ，在卡片视图中查看列表，并（可选）从**排序依据**下拉菜单中排列虚拟机列表。

3 在要编辑的虚拟机的卡中，单击**详细信息**。

4 单击**客户机操作系统自定义和属性**以展开客户机操作系统设置列表。

选项	描述
启用客户机自定义	选择该选项以启用客户机自定义。
更改 SID	选择该选项以更改 Windows 安全 ID (SID)。 该选项特定于运行 Windows 客户机操作系统的虚拟机。SID 在部分 Windows 操作系统中用于唯一标识系统和用户。如果您未选择此选项，则新虚拟机与它所基于的虚拟机或模板具有相同的 SID。当计算机是域的一部分，并且只使用域用户帐户时，重复 SID 不会引起问题。但是，如果计算机是工作组的一部分或者使用本地用户帐户，则重复 SID 会影响文件访问控制。有关详细信息，请参见 Microsoft Windows 操作系统的相关文档资料。
允许本地管理员密码	选择该选项以允许在客户机操作系统上设置管理员密码。 a 为本地管理员指定一个密码。 将**指定密码**文本框留空会自动生成密码。 b 指定允许自动登录的次数。 输入零值将禁用以管理员身份自动登录。
要求管理员在首次登录时更改密码	选择该选项以要求管理员在首次登录时更改客户机操作系统的密码。出于安全考虑，建议执行此操作。
自动生成密码	选择此选项以允许自动生成密码。
启用此 VM 以加入域	可以选择该选项以将虚拟机加入 Windows 域。您可以使用组织的域，或替代组织的域并输入域属性。 a 输入域名。 b 输入用户名和密码。 c 输入帐户组织单元。
脚本	可以使用自定义脚本修改虚拟机的客户机操作系统。将自定义脚本添加到虚拟机后，将仅在初始自定义和强制重新自定义时调用该脚本。如果设置 `precustomization` 命令行参数，将在客户机自定义开始前调用该脚本。如果设置 `postcustomization` 命令行参数，将在客户机自定义完成后调用该脚本。 ■ 单击脚本文本框下方的上载按钮以导航到本地计算机上的自定义脚本。 ■ 直接在**脚本文件**文本框中键入自定义脚本。 直接在**脚本文件**文本框中输入的自定义脚本不能超过 1500 个字符。有关详细信息，请参见 VMware 知识库文章 https://kb.vmware.com/kb/1026614。

5 更改完成后，单击**保存**。

了解客户机自定义

自定义客户机操作系统时，您应该了解某些设置和选项。

“启用客户机自定义”复选框

此复选框位于虚拟机**属性**页面上的**客户机操作系统自定义**选项卡中。客户机自定义的目标是根据**属性**页面上所选的选项进行配置的。如果选中此复选框，则系统将根据需要执行客户机自定义和重新自定义。

要使所有客户机自定义功能（如计算机名称、网络设置、设置管理员和 root 密码以及使其过期、Windows 操作系统 SID 更改等）正常工作，必须执行该过程。若要使**启动和强制重新自定义**正常工作，则应选中此选项。

如果已选中此复选框，且 VMware Cloud Director 中虚拟机的配置参数与客户机操作系统中的设置不同步，则虚拟机**属性**页面上的**配置文件**选项卡将显示该设置与客户机操作系统不同步，并且虚拟机需要客户机自定义。

vApp 和虚拟机的客户机自定义行为

以下复选框将会取消选中。

- **启用客户机自定义**
- **更改 SID**（在 Windows 客户机操作系统中）
- **密码重置**

如果要执行自定义（或者已对客户机操作系统中要反映的网络设置进行更改），则您可以选中**启用客户机自定义**复选框，并设置虚拟机**属性**页面的**客户机操作系统自定义**选项卡中的选项。在使用 vApp 模板中的虚拟机创建 vApp 并添加虚拟机时，vApp 模板将充当构建基块。将目录中的虚拟机添加到新 vApp 时，默认情况下，该虚拟机已启用客户机自定义。将目录中的 vApp 模板另存为 vApp 时，仅当选中**启用客户机自定义**复选框时，该虚拟机才会启用客户机自定义。

以下是客户机自定义设置的默认值：

- **启用客户机自定义**复选框与目录中的源虚拟机相同。
- 对于 Windows 客户机虚拟机，**更改 SID** 与目录中的源虚拟机相同。
- 密码重置设置与目录中的源虚拟机相同。

启动 vApp 之前，可以根据需要取消选中**启用客户机自定义**复选框。

如果将挂起客户机操作系统安装的空虚拟机添加到 vApp，则由于这些虚拟机尚未准备好进行自定义，因此默认情况下将取消选中**启用客户机自定义**复选框。

安装客户机操作系统和 VMware Tools 之后，您可以关闭虚拟机，停止 vApp，选中**启用客户机自定义**复选框，并启动 vApp 和虚拟机来执行客户机自定义。

如果虚拟机名称和网络设置在经自定义的虚拟机中已更新，则您下次启动该虚拟机时，它将重新自定义，使客户机虚拟机与 VMware Cloud Director 重新同步。

启动虚拟机并强制重新自定义

您可以打开虚拟机的电源并强制重新自定义虚拟机。

如果虚拟机中的设置与 VMware Cloud Director 不同步，或者尝试执行客户机自定义失败，则可以强制重新自定义虚拟机。

确保虚拟机中运行的应用程序支持重新自定义。如果使用 Microsoft Sysprep 更改域控制器，同时更改 SID，则虚拟机可能会损坏。要缓解损坏虚拟机的风险，请在重新自定义之前创建快照。

前提条件

- 您必须是组织管理员。
- 必须关闭虚拟机的电源。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。

2 单击  ，在卡片视图中查看列表，并（可选）从**排序依据**下拉菜单中排列虚拟机列表。

3 从要打开电源并自定义的虚拟机的**电源**菜单中选择**启动和强制重新自定义**。

结果

虚拟机随即重新自定义并启动。

更改虚拟机的高级属性

在**高级**设置中，您可以配置资源分配设置（份额、预留和限制），确定为虚拟机提供的 CPU、内存和存储资源量。

使用资源分配设置（份额、预留和限制），确定为虚拟机提供的 CPU 数量、内存数量和存储资源数量。

资源分配份额

份额用于指定虚拟机在虚拟数据中心中的相对重要性。如果某个虚拟机所拥有的资源份额是另一个虚拟机的两倍，则当这两个虚拟机抢占资源时，该虚拟机有权消耗两倍的资源。份额通常指定为“高”、“正常”或“低”，这些值分别以 4:2:1 的比率指定份额值。您还可以选择“自定义”，将特定的份额数（表示比例权重）分配给每个虚拟机。为虚拟机分配份额时，应始终指定此虚拟机相对于其他已启动虚拟机的优先级。

资源分配预留

指定保证为虚拟机分配的最少资源量。仅在有足够的未预留资源满足虚拟机的预留时，VMware Cloud Director 才允许您打开虚拟机电源。即使资源负载很重，虚拟数据中心亦能保证此资源量。预留以具体单位（兆赫或兆字节）表示。

例如，假设您有 2 GHz 可用资源，分别为虚拟机 1 和虚拟机 2 指定 1 GHz 的资源分配预留。现在，每个虚拟机均保证能获得 1GHz（如果虚拟机需要 1GHz 资源）。但是，如果虚拟机 1 仅使用 500 MHz，则虚拟机 2 可以使用 1.5 GHz。

预留默认为 0。如果需要保证虚拟机始终可以获得最低需求量的 CPU 或内存，则可以指定预留。

资源分配限制

指定可以分配给虚拟机的 CPU 和内存资源的上限。虚拟数据中心分配给虚拟机的资源可以超过预留资源，但不得超过限制，即使系统中存在未使用的资源时也是如此。限制以具体单位（兆赫或兆字节）表示。

CPU 和内存资源限制默认为无限制。当内存限制为无限制时，在大多数情况下，虚拟机创建时配置的内存数量将会生效。

大多数情况下，不必指定限制。如果指定限制，则可能浪费空闲资源。系统不允许虚拟机使用超过限制的资源，即使系统未充分利用且存在空闲资源也是如此。请仅出于合理理由指定限制。

前提条件

- 预留池虚拟数据中心。
- 确保虚拟数据中心为虚拟机提供一定量的内存。
- 保证分配给特定虚拟机的虚拟数据中心资源百分比始终高于其他虚拟机。
- 设置可以分配给虚拟机的资源上限。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。

2 单击  ，在卡片视图中查看列表，并（可选）从**排序依据**下拉菜单中排列虚拟机列表。

3 在要编辑的虚拟机的卡中，单击**详细信息**。

4 依次单击**高级**和**编辑**。

5 可通过从**优先级**下拉菜单中选择选项来设置 CPU 设置的资源分配份额。

选项	描述
低	为每个虚拟 CPU 分配 500 个份额。
正常	为每个虚拟 CPU 分配 1000 个份额。
高	为每个虚拟 CPU 分配 2000 个份额。
自定义	允许您通过输入份额数（表示比例权重），将特定数量的份额分配给每个虚拟机。为虚拟机分配份额时，应始终指定此虚拟机相对于其他已启动虚拟机的优先级。

6 通过输入预留 (MHz)，指定 CPU 设置的预留和（可选）CPU 设置的限制 (MHz)。

选项	描述
无限制	默认的 CPU 资源选项。
最高	指定可以分配给虚拟机的 CPU 资源上限 (MHz)。

7 通过从**优先级**下拉菜单中选择一个选项来设置内存设置的资源分配份额。

选项	描述
低	为已配置的虚拟机内存的每兆字节分配 5 个份额。
正常	为已配置的虚拟机内存的每兆字节分配 10 个份额。
高	为已配置的虚拟机内存的每兆字节分配 20 个份额。
自定义	允许您通过输入份额数分配特定数量的份额。

8 指定内存设置预留 (MB) 和（可选）内存设置限制 (MB)。

选项	描述
无限制	默认内存资源选项。
最高	指定可以分配给虚拟机的内存预留上限。

9 单击**保存**。

插入媒体

您可以从目录中插入 CD/DVD 映像等媒体，以便在虚拟机的客户机操作系统中使用。可以使用这些媒体文件在虚拟机、各种应用程序、驱动程序等中安装操作系统。

前提条件

您有权访问含媒体文件的目录。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。

2 单击  ，在卡片视图中查看列表，并（可选）从**排序依据**下拉菜单中排列虚拟机列表。

3 选择要在其中添加媒体的虚拟机。

4 从**操作**菜单中，选择**插入媒体**。

5 在**插入 CD** 窗口中，选择要插入到虚拟机的媒体文件。

6 单击**插入**。

弹出媒体

在虚拟机中使用完 CD 或 DVD 之后，可以弹出媒体文件。

前提条件

媒体文件已先前插入到虚拟机中。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。

2 单击  ，在卡片视图中查看列表，并（可选）从**排序依据**下拉菜单中排列虚拟机列表。

3 选择要从中弹出媒体的虚拟机。

4 从**操作**菜单中，选择**弹出媒体**。

结果

此时媒体文件将被弹出。

将虚拟机复制到其他 vApp

可以将虚拟机复制到另一个 vApp。复制虚拟机之后，原始虚拟机将保留在源 vApp 中。

复制虚拟机时，不会复制快照。

前提条件

- 此操作需要预定义的 **vApp 作者**角色中包含的权限或一组等效权限。
- 关闭虚拟机电源。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。

2 单击  ，在卡片视图中查看列表，并（可选）从**排序依据**下拉菜单中排列虚拟机列表。

3 从要复制的虚拟机的**操作**菜单中，选择**复制到**。

4 选择要将虚拟机复制到的目标 vApp，然后单击**下一步**。

5 配置资源，例如虚拟机名称和计算机名称以及（可选）存储策略和网卡，然后单击**下一步**。

重要事项 计算机名称只能包含字母数字字符和连字符。它不能仅包含数字，并且不能包含空格。

6 在**即将完成**页面上，检查设置，然后单击**完成**。

将虚拟机移动到其他 vApp

可以将虚拟机移至另一个 vApp。移动 VM 时，VMware Cloud Director 会从源 vApp 中移除原始 VM。

将虚拟机移至其他 vApp 时，所生成的快照将会丢失。

在不同 vApp 之间移动 VM 需要使用 VMware vSphere® vMotion® 和增强型 vMotion 兼容性 (EVC)。可以将 VM 移至同一组织内属于同一或其他组织 VDC 的不同 vApp。组织 VDC 可以位于相同或不同的提供者 VDC 中。

将虚拟机移至其他 vApp 时，可以执行重新配置操作，例如更改网络和存储配置文件。

表 2-1. 在虚拟机移动期间进行重新配置以及虚拟机状态

重新配置	目标 vApp 位于同一组织 VDC 时的虚拟机状态	目标 vApp 位于同一提供者 VDC 内其他组织 VDC 时的虚拟机状态
更改网络	已关闭电源	不可用
移除网络	已打开电源或已关闭电源	不可用
更改存储配置文件	已打开电源或已关闭电源	已关闭电源

前提条件

- 确认您具有 **vApp 作者**角色或一组等效权限。
- 确认底层 vSphere 资源支持 vMotion 和 EVC。有关 vMotion 和 EVC 的要求及限制的信息，请参见《vCenter Server 和主机管理》。
- 如果要更改虚拟机网络或存储配置文件，请检查是否必须关闭虚拟机的电源。请参见表虚拟机移动期间执行的重新配置操作和虚拟机状态。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。

2 单击  ，在卡片视图中查看列表，并（可选）从**排序依据**下拉菜单中排列虚拟机列表。

3 从要移动的计算机的**操作**菜单中，选择**移至**。

4 选择目标 vApp，然后单击**下一步**。

5 配置资源，例如 VM 名称和计算机名称以及（可选）存储策略和网卡，然后单击**下一步**。

重要事项 计算机名称只能包含字母数字字符和连字符。它不能仅包含数字，并且不能包含空格。

6 在**即将完成**页面上，检查设置，然后单击**完成**。

虚拟机关联性和反关联性

通过关联性和反关联性规则，您可以将一组虚拟机分布到不同的 ESXi 主机上或将一组虚拟机置于一个特定主机上。

关联性规则将一组虚拟机置于一个特定主机上，以便您可以轻松审核这些虚拟机的使用情况。反关联性规则将一组虚拟机分布在不同主机上，从而防止一个主机出现故障时所有虚拟机都发生故障。

默认情况下，关联性和反关联性规则是必需的。如果未满足关联性或反关联性规则，添加到规则的虚拟机将无法打开电源。

查看关联性和反关联性规则

您可以查看现有的关联性和反关联性规则及其属性，例如受此类规则影响的虚拟机以及是否启用规则。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**关联性规则**。

2 （可选） 单击**网格编辑器**图标 ()，然后选择要显示规则的哪些详细信息。

结果

您将看到现有关联性和反关联性规则、虚拟机以及每个规则的启用状态的列表。

创建关联性规则

创建关联性规则可在单个主机上放置一组特定虚拟机，以便可以审核这些虚拟机的使用情况。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**关联性规则**。

2 在**关联性规则**下，单击**新建**。

3 输入规则的名称。

4 取消选中**启用**以便在不启用该选项的情况下创建规则。

默认情况下，此复选框处于选中状态，规则创建后即启用。

5 将**必需**复选框保持选中状态。

默认情况下，每个关联性规则都是必需的。这意味着，如果不满足规则，添加到规则的虚拟机将不会打开电源。

6 选择要添加到关联性规则的虚拟机。

7 单击**保存**。

结果

VMware Cloud Director 将在单个主机上放置与关联性规则关联的虚拟机。

创建反关联性规则

创建反关联性规则可在多个主机上放置一组特定虚拟机，以防止在单个主机出现故障时这些虚拟机同时出现故障。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**关联性规则**。

2 在**反关联性规则**下，单击**新建**。

3 输入规则的名称。

4 取消选中**启用**以便在不启用该选项的情况下创建规则。

默认情况下，此复选框处于选中状态，规则创建后即启用。

5 将**必需**复选框保持选中状态。

默认情况下，每个反关联性规则都是必需的。这意味着，如果不满足规则，添加到规则的虚拟机将不会打开电源。

6 选择要添加到反关联性规则的虚拟机。

7 单击**保存**。

结果

VMware Cloud Director 将在多个主机上放置与反关联性规则关联的虚拟机。

编辑关联性或反关联性规则

可以编辑关联性或反关联性规则以启用或禁用规则，添加或移除虚拟机，更改规则名称或规则首选项。

前提条件

此操作需要 `Organization vDC: VM-VM Affinity Edit` 权限。预定义的**目录作者**、**vApp 作者**和**组织管理员**角色中包含此权限。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**关联性规则**。

2 单击要编辑规则的名称旁边的单选按钮，然后单击**编辑**。

3 编辑规则属性。

a 根据需要更改规则的名称。

b 选择是启用还是禁用规则。

c 将**必需**复选框保持选中状态。

d 添加多个虚拟机或移除虚拟机。

4 单击**保存**。

删除关联性或反关联性规则

如果不再需要使用关联性规则或反关联性规则，可以将其删除。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**关联性规则**。

2 单击要删除的规则的名称旁边的单选按钮，然后单击**删除**。

3 要确认删除该规则，请单击**确定**。

结果

VMware Cloud Director 将删除关联性规则或反关联性规则。

监控虚拟机

如果 VMware Cloud Director 管理员启用了虚拟机监控功能，您可以从租户门户查看监控图表。

使用此功能可了解指定虚拟机在一段时间（数天、数周或数月）内的状态。

前提条件

只有当 VMware Cloud Director 管理员启用了此功能后，您才能使用此功能。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。

2 单击  ，在卡片视图中查看列表，并（可选）从**排序依据**下拉菜单中排列虚拟机列表。

3 选择要监控的虚拟机并单击**详细信息**。

4 单击**监控图表**以展开监控视图。

监控图表随即显示。

5

6 选择用于监控虚拟机的衡量指标选项。

衡量指标下拉菜单中的列表会因所选择的**系统管理员**而异。您将看到以下选项的一部分或全部。

衡量指标	描述
最新置备的磁盘	以 KB 为单位指定。 可从天、周或月视图中选择。
平均磁盘读取量	以百分比指定。 可从天、周或月视图中选择。
平均磁盘写入量	以百分比指定。 可从天、周或月视图中选择。
平均 CPU 使用情况	以百分比指定。 可从天、周或月视图中选择。
平均 CPU 使用情况 MHz	以 MHz 为单位指定。 可从天、周或月视图中选择。
最大 CPU 使用情况	以百分比指定。 可从天、周或月视图中选择。

衡量指标	描述
平均内存使用情况	以百分比指定。 可从天、周或月视图中选择。
最新使用的磁盘	以 KB 为单位指定。 可从天、周或月视图中选择。

每次从列表中选择不同的值都会显示新图表。

7 （可选） 更改衡量指标收集的时间范围。

8 单击**刷新**。

9 要保存更改，请单击**保存**。

使用快照

创建快照时，快照将保留虚拟机的状态和数据。创建虚拟机的快照时，仅复制和存储给定状态的虚拟机的映像，虚拟机不受影响。在需要多次恢复至相同虚拟机状态而又不想创建多个虚拟机时，快照会很有用。

作为测试软件是否具有未知或潜在不利影响的短期解决方案，快照非常有用。例如，您可以将快照用作线性或迭代过程（如安装更新包）或分支过程（如安装不同版本的程序）中的还原点。

升级虚拟机的操作系统时，您可能希望使用快照。例如，在升级虚拟机之前，创建一个快照以保留升级前的时间点。如果升级期间无任何问题，您可以选择移除此快照，提交您在升级期间所做的更改。但是，如果您遇到问题，则可以恢复到快照，返回到升级前已保存的虚拟机状态。

使用 VMware Cloud Director 时您只能拥有一个虚拟机快照。每次尝试创建虚拟机的新快照都会删除之前的快照。

创建虚拟机快照

您可以创建虚拟机的快照。创建快照后，可以将虚拟机恢复到快照，也可以移除快照。

前提条件

确认虚拟机未连接到给定磁盘。

注 快照不会捕获网卡配置。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。

2 单击  ，在卡片视图中查看列表，并（可选）从**排序依据**下拉菜单中排列虚拟机列表。

3 从要创建快照的虚拟机的**操作**菜单中，选择**创建快照**。

创建虚拟机的快照将替换现有快照（如果有）。

4 （可选） 选择是否创建虚拟机内存的快照。

捕获虚拟机内存状况时，快照会保留虚拟机的实时状况。内存快照可以创建某一精确时间点的快照（例如，升级仍在运行的软件）。生成了内存快照后，如果升级未按预期完成，或软件不符合您的预期，则可将虚拟机恢复到其以前的状态。

捕获内存状况时，虚拟机的文件无需静默。如果未捕获内存状况，快照就不会保存虚拟机的实时状况，除非静默磁盘，否则磁盘就是崩溃一致的。

5 （可选） 选择是否静默客户机文件系统。

此操作要求已在虚拟机上安装 VMware Tools。当静默虚拟机时，VMware Tools 会静默虚拟机的文件系统。静默操作可确保快照磁盘表示客户机文件系统的一致状况。静默快照适用于自动备份或定期备份。例如，如果您无法识别虚拟机的活动，但希望恢复为多个最近的备份，则可以静默文件。

您无法静默包含大容量磁盘的虚拟机。

6 单击**确定**。

结果

通过快照，可以将虚拟机恢复到最新的快照。

将虚拟机恢复到快照

您可以将虚拟机恢复到它在创建快照时所处的状态。

前提条件

虚拟机有一个快照。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。

2 单击  ，在卡片视图中查看列表，并（可选）从**排序依据**下拉菜单中排列虚拟机列表。

3 从要恢复到快照的虚拟机的**操作**菜单中，选择**恢复到快照**。

4 单击**确定**。

结果

虚拟机即会恢复到已保存的快照。

移除虚拟机的快照

您可以移除虚拟机的快照。

移除快照时，会删除所保留的虚拟机的状态，而且无法再次返回到该状态。移除快照不会影响虚拟机的当前状态。

前提条件

具有已存储快照的虚拟机。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。

2 单击  ，在卡片视图中查看列表，并（可选）从**排序依据**下拉菜单中排列虚拟机列表。

3 从要移除快照的虚拟机的**操作**菜单中，选择**移除快照**。

4 单击**确定**。

续订虚拟机租约

如果租约即将过期，您可以更新虚拟机租约。

前提条件

此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。

2 单击  ，在卡片视图中查看列表，并（可选）从**排序依据**下拉菜单中排列虚拟机列表。

3 从租约即将过期的虚拟机的**操作**菜单中，选择**更新租约**。

结果

租约即会更新。您可以在**租约**字段中查看新租约的时间范围。

删除虚拟机

您可以从组织中删除虚拟机。

前提条件

必须将虚拟机关闭。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。

2 单击  ，在卡片视图中查看列表，并（可选）从**排序依据**下拉菜单中排列虚拟机列表。

3 从要删除的虚拟机的**操作**菜单中，选择**删除**。

4 确认该删除操作。

结果

该虚拟机将被删除。

使用 vApp

3

vApp 由一个或多个通过网络进行通信，并且使用已部署环境中的资源和服务的虚拟机组成。一个 vApp 可以包含多个虚拟机。

从 VMware Cloud Director 9.5 开始，vApp 支持 IPv6 连接。可以将 IPv6 地址分配给连接到 IPv6 网络的虚拟机。

重要事项 使用 vApp 的所有步骤从卡片视图进行记录，且假定您具有多个虚拟数据中心。从网格视图也可以完成同样的过程，但步骤可能会略有不同。

本章讨论了以下主题：

- 将 vApp 作为 OVF 软件包下载
- 续订 vApp 租约
- 删除 vApp
- 删除多个 vApp

查看 vApp

您可以用网格视图或卡片视图查看 vApp。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 要在网格视图中查看 vApp，请单击  。要在卡片视图中查看 vApp，请单击  。

vApp 的列表将以网格形式显示或显示为一列卡片。

3 （可选） 配置网格视图以包含要查看的详细信息。

a 在网格视图中，单击**网格编辑器**图标 ()。

b 通过选中要查看的每个详细信息旁边的复选框，选择要包含在网格视图中的 vApp 详细信息。

c 要保存更改，请单击**确定**。

选定详细信息将显示为每个 vApp 的列。

4 （可选） 在网格视图中，单击 vApp 左侧的 ，以显示可对选定 vApp 执行的操作。

例如，可以关闭 vApp。

构建新 vApp

可以使用目录中的虚拟机和/或新虚拟机创建 vApp，而不是基于 vApp 模板创建 vApp。

构建 vApp 需要提供 vApp 的名称和可选描述。您可以稍后返回并将虚拟机添加到 vApp。

前提条件

此操作需要预定义的 **vApp 作者**角色中包含的权限或一组等效权限。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 选择**新建 vApp**。

3 输入 vApp 的名称和可选描述。

4 （可选） 如果您希望 vApp 在部署时打开电源，请选中**打开电源**复选框。

注 仅当 vApp 中存在虚拟机时，才能打开电源。

5 （可选） 搜索目录中要添加到此 vApp 的虚拟机或通过单击**添加虚拟机**添加新的空虚拟机。

如果目录中没有任何虚拟机，请创建一个虚拟机并将其添加到 vApp。

a 输入虚拟机的名称和计算机名称。

重要事项 计算机名称只能包含字母数字字符和连字符。计算机名称不能仅包含数字，并且不能包含空格。

b （可选） 输入有意义的描述。

c 选择希望部署虚拟机的方式。

选项	操作
新建	使用可自定义的设置部署新虚拟机。 1 选择操作系统系列和操作系统。 2 （可选）选择引导映像。 3 （可选）选择 VM 放置策略和 VM 大小调整策略。 仅当服务提供商将 VM 放置策略和 VM 大小调整策略发布到组织 VDC 时，此类策略下拉菜单才可见。 4 选择虚拟机的大小，或单击**自定义大小调整选项**以手动输入计算、内存和存储设置。 预定义的虚拟机大小为小型、中型或大型。 5 指定存储选项，例如存储策略和大小 (GB)。 6 指定虚拟机的网络设置，如网络、IP 模式、IP 地址和主网卡。
从模板	基于从模板目录选择的模板部署虚拟机。 1 从目录中选择虚拟机模板。 2 （可选）选择 VM 放置策略和 VM 大小调整策略。 仅当服务提供商将 VM 放置策略和 VM 大小调整策略发布到组织 VDC 时，此类策略下拉菜单才可见。如果所选模板已分配有策略，则您可能只能使用预定义的模板策略。 3 （可选）选择使用自定义存储策略，然后从**要使用的自定义存储策略**中选择策略。 4 如果提供了最终用户许可协议，您必须查看并接受该协议。

d 要将虚拟机添加到 vApp，请单击**确定**。

此时，目录中将显示添加的虚拟机。

6 （可选） 针对要在 vApp 内创建的每个其他虚拟机重复步骤 5。

7 要完成 vApp 创建，请单击**创建**。

结果

此时 vApp 创建完成。打开 vApp 电源时，其中的虚拟机将完成创建并且也处于打开电源状态。

从 OVF 软件包创建 vApp

可以直接从 OVF 软件包创建和部署 vApp，而无需创建 vApp 模板和对应的目录项。

VMware Cloud Director 对 OVF 部署具有自己的限制，这与 vCenter Server 中的限制不同。因此，vCenter Server 中的成功部署 OVF 在 VMware Cloud Director 中可能会失败。

VMware Cloud Director 支持 OVF 1.1，但不支持 OVF 1.1 架构的所有部分。例如，不支持 OVF 中的 `DeploymentOptions` 部分。

VMware Cloud Director 中的 OVF 部署涉及许多组件，例如 `TransferService`、NFS 挂载上的 spool 区域、与 vCenter Server 的 NFC 连接、校验和验证等。其中任何组件出现故障都会导致 OVF 上载失败。

如果上载包含清单文件的 OVF 软件包，VMware Cloud Director 会将 OVF 描述符文件和所有 VMDK 文件的 SHA-1 哈希验证为 `manifest.mf` 文件中的值。如果任何哈希值不匹配，上载将失败。**系统管理员**可以通过将 `CONFIG` 属性设置为 `ovf.manifest.check.disabled` 来禁用此检查。

前提条件

- 确认有要上载的 OVF 软件包，并且您有权上载 OVF 软件包和部署 vApp。
- 确认 OVF 描述符文件中的 OVF 版本不是 0.9。
- VMware Cloud Director 中 OVF 描述符文件默认支持的最大大小为 12 MB。您可以通过编辑 `CONFIG` 属性 `ovf.descriptor.size.max` 来替代此设置。
- 确认清单文件（.mf 扩展名）默认允许的最大大小为 1 MB。
- 确认 OVF 软件包符合 OVF XSD 架构。
- 如果 OVF 描述符文件的 `VirtualSystemType` 元素中提供了硬件版本，请确认其低于上载 OVF 的 VDC 中支持的最高硬件版本。
- 如果 OVF 描述符文件包含 `ExtraConfig` 元素，请确认您的**系统管理员**将这些元素包含在 `extraConfigs` 元素的 `AllowedList` 中。未包含在 `AllowedList` 中的元素会导致 OVF 上载失败，并显示验证错误。

步骤

1. 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择 **vApp**。
2. 单击**从 OVF 添加 vApp**。
3. 单击**上载** (↑) 按钮，浏览到您的计算机可访问的位置，然后选择 OVF/OVA 模板文件。

   位置可能为本地硬盘驱动器、网络共享或 CD/DVD 驱动器。受支持的文件扩展名包括 `.ova`、`.ovf`、`.vmdk`、`.mf`、`.cert` 和 `.strings`。如果选择上载 OVF 文件，而其引用的文件多于您要上载的文件（例如，VMDK 文件），则必须浏览并选择所有文件。
4. 单击**下一步**。
5. 验证将部署的 OVF/OVA 模板的详细信息，然后单击**下一步**。

6 输入 vApp 的名称和可选描述，然后单击**下一步**。

7 （可选） 更改 vApp 的计算机名称，使其仅包含字母数字字符。

仅当 vApp 名称包含空格或特殊字符时，才需要执行此步骤。默认情况下，使用虚拟机的名称预填充了计算机名称。但是，计算机名称只能包含字母数字字符。

8 从**存储策略**下拉菜单中，为 vApp 中的每个虚拟机选择存储策略，然后单击**下一步**。

9 选择每个虚拟机要连接的网络。

- 从**网络**下拉菜单中为每个虚拟机选择一个网络。
- 您可以选择**切换到高级网络连接工作流程**复选框，并为 vApp 中的每个虚拟机手动输入主网卡、网络适配器类型、网络、IP 分配和 IP 地址设置等网络设置。

完成向导之后，您可以配置虚拟机的其他属性。

10 单击**下一步**。

11 自定义 vApp 中虚拟机的硬件，然后单击**下一步**。

选项	描述
虚拟 CPU 的数量	输入 vApp 中每个虚拟机的虚拟 CPU 的数量。 可以分配给虚拟机的最大虚拟 CPU 数量取决于主机上的逻辑 CPU 数量以及虚拟机上安装的客户机操作系统的类型。
每个插槽内核数	为 vApp 中的每个虚拟机输入每个插槽内核数。 您可以根据内核数和每个插槽内核数配置虚拟 CPU 的分配方式。确定虚拟机中需要的 CPU 内核数，然后选择每个插槽中需要的内核数，具体取决于您需要单核 CPU、双核 CPU 还是三核 CPU 等等。
内核数	查看 vApp 中每个虚拟机的内核数。 更新虚拟 CPU 数量时，此数值将更改。
总内存 (MB)	输入 vApp 中每个虚拟机的内存 (MB)。 此设置确定了分配给虚拟机的 ESXi 主机内存量。虚拟硬件内存大小决定了在虚拟机中运行的应用程序可以使用的内存量。虚拟机内存资源多于配置的虚拟硬件内存大小时并不会带来优势。

12 在“即将完成”页面上，检查设置，然后单击**完成**。

结果

新的 vApp 将显示在卡视图中。

从目录添加 vApp

如果您有权访问目录，则可以使用目录中的 vApp 模板创建 vApp。

vApp 模板可以基于 OVF 文件，其中包含用于自定义 vApp 虚拟机的属性。vApp 可以继承这些属性。如果其中任一属性为用户可配置属性，则您可以指定相应属性的值。

前提条件

- 要访问公用目录中的 vApp 模板，请确认您是**组织管理员**或 **vApp 作者**。
- 要访问共享给您的组织目录中的 vApp 模板，请确认您至少是 **vApp 用户**。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择 **vApp**。

2 单击**新建**，然后选择**从目录添加 vApp**。

3 选择要导入的模板，然后单击**下一步**。

4 输入 vApp 的名称和可选描述。

5 输入 vApp 的运行时租约和存储租约，然后单击**下一步**。

6 从**存储策略**下拉菜单中，为 vApp 中的每个虚拟机选择存储策略，然后单击**下一步**。

7 如果 vApp 中虚拟机的放置策略和大小调整策略可配置，请从下拉菜单中为每个虚拟机选择一个策略。

8 如果 vApp 中虚拟机的计算属性可配置，请进行自定义，然后单击**下一步**。

选项	描述
虚拟 CPU	输入 vApp 中每个虚拟机的虚拟 CPU 的数量。 可以分配给虚拟机的最大虚拟 CPU 数量取决于主机上的逻辑 CPU 数量以及虚拟机上安装的客户机操作系统的类型。
每个插槽内核数	为 vApp 中的每个虚拟机输入每个插槽内核数。 您可以根据内核数和每个插槽内核数配置虚拟 CPU 的分配方式。确定虚拟机中需要的 CPU 内核数，然后选择每个插槽中需要的内核数，具体取决于您需要单核 CPU、双核 CPU 还是三核 CPU 等等。
内核数	查看 vApp 中每个虚拟机的内核数。 更新虚拟 CPU 数量时，此数值将更改。
内存	输入 vApp 中每个虚拟机的内存 (MB)。 此设置确定了分配给虚拟机的 ESXi 主机内存量。虚拟硬件内存大小决定了在虚拟机中运行的应用程序可以使用的内存量。虚拟机内存资源多于配置的虚拟硬件内存大小时并不会带来优势。

9 如果 vApp 中虚拟机的硬件属性可配置，请自定义虚拟机硬盘的大小，然后单击**下一步**。

10 如果 vApp 中虚拟机的网络连接属性可配置，请进行自定义，然后单击**下一步**。

   a 在**配置网络**页面上，选择每个虚拟机要连接的网络。

   b （可选） 选中复选框以切换到高级网络连接工作流，并为 vApp 中的虚拟机配置其他网络连接设置。

11 检查 vApp 设置，然后单击**完成**。

从 vApp 模板创建 vApp

您可以根据有权访问的目录中存储的 vApp 模板创建新 vApp。

如果 vApp 模板以 OVF 文件为基础，而该文件包括用于自定义其虚拟机的 OVF 属性，则这些属性将传递至 vApp。如果其中任一属性为用户可配置属性，则您可以指定值。

前提条件

- 只有组织管理员和 vApp 作者才能访问公用目录中的 vApp 模板。
- vApp 用户和上述人员可访问组织目录中与其共享的 vApp 模板。

步骤

1. 在顶部导航栏中，单击**库**，然后在左侧面板中选择 **vApp 模板**。

   此时将以网格视图显示模板列表。

2. 单击要部署为 vApp 的 vApp 模板左侧的列表栏 (⋮)，然后选择**创建 vApp**。
3. 在该向导的**接受许可协议**页面中，请阅读“最终用户许可协议”，然后单击**接受**。
4. 单击**下一步**。
5. 输入 vApp 的名称和可选描述。
6. 指定此 vApp 在自动停止前可以运行的时间（小时或天）。
7. 指定停止的 vApp 在自动清理前保持可用的时间（小时或天）。
8. 单击**下一步**。
9. 选择要在其中创建 vApp 的虚拟数据中心。
10. 选择存储策略。
11. 单击**下一步**。
12. 选择每个虚拟机要连接的网络。
    - 从**网络**下拉菜单中为每个虚拟机选择一个网络。
    - 您可以选择**切换到高级网络连接工作流程**复选框，并为 vApp 中的每个虚拟机手动输入主网卡、网络适配器类型、网络、IP 分配和 IP 地址设置等网络设置。

    完成向导之后，您可以配置虚拟机的其他属性。
13. 单击**下一步**。

14 自定义 vApp 中虚拟机的硬件，然后单击**下一步**。

选项	描述
虚拟 CPU 的数量	输入 vApp 中每个虚拟机的虚拟 CPU 的数量。 可以分配给虚拟机的最大虚拟 CPU 数量取决于主机上的逻辑 CPU 数量以及虚拟机上安装的客户机操作系统的类型。
每个插槽内核数	为 vApp 中的每个虚拟机输入每个插槽内核数。 您可以根据内核数和每个插槽内核数配置虚拟 CPU 的分配方式。确定虚拟机中需要的 CPU 内核数，然后选择每个插槽中需要的内核数，具体取决于您需要单核 CPU、双核 CPU 还是三核 CPU 等等。
内核数	查看 vApp 中每个虚拟机的内核数。 更新虚拟 CPU 数量时，此数值将更改。
总内存 (MB)	输入 vApp 中每个虚拟机的内存 (MB)。 此设置确定了分配给虚拟机的 ESXi 主机内存量。虚拟硬件内存大小决定了在虚拟机中运行的应用程序可以使用的内存量。虚拟机内存资源多于配置的虚拟硬件内存大小时并不会带来优势。
硬盘属性	输入虚拟机硬盘的大小 (MB)。

15 在“即将完成”页面上，检查设置，然后单击**完成**。

结果

新的 vApp 将显示在卡视图中。

将 vCenter Server 中的虚拟机作为 vApp 导入

如果您具有**系统管理员**权限，则可以将 vCenter Server VM 作为 vApp 导入到 VMware Cloud Director。

导入虚拟机不会保留在 vCenter Server 中配置的虚拟机预留、限制和份额设置。导入的虚拟机会从所驻留的组织虚拟数据中心获取其资源分配设置。

前提条件

要从 vCenter Server 查看和导入虚拟机，请确认您具有**系统管理员**权限。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 单击**新建**，然后选择**从 vCenter 导入**。

3 从下拉菜单中，选择要从中导入虚拟机的 vCenter Server 实例。

4 选择要导入的虚拟机。

5 输入 vApp 的名称和可选描述。

6 从下拉菜单中，选择要在其中存储并运行 vApp 的虚拟数据中心。

7 （可选） 从下拉菜单中，选择 vApp 的存储策略。

8 （可选） 要删除源虚拟机，请启用**移动虚拟机**选项。

9 单击**导入**。

在 vApp 上执行电源操作

您可以在 vApp 上执行电源操作，例如打开或关闭 vApp 的电源、挂起或重置 vApp。

打开 vApp 的电源

打开 vApp 的电源将启动 vApp 中尚未启动的所有虚拟机。

前提条件

您至少是 vApp 作者。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 单击  ，以在卡片视图中查看 vApp。

3 从要打开电源的 vApp 的**操作**菜单中，选择**打开电源**。

结果

vApp 即会启动。

关闭 vApp 电源

关闭 vApp 的电源将关闭 vApp 中所有虚拟机的电源。要执行某些操作（如将 vApp 添加到目录、复制或移动到其他 VDC），首先必须关闭 vApp 的电源。

前提条件

必须启动 vApp。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 单击  ，以在卡片视图中查看 vApp。

3 从要停止的 vApp 的**操作**菜单中选择**关闭电源**。

4 单击**确定**。

结果

vApp 中的所有虚拟机和 vApp 本身都已关闭。

重置 vApp

重置 vApp 时将清除状态（内存和缓存等），但 vApp 仍可继续运行。

前提条件

将启动您的 vApp 并打开其中的虚拟机的电源。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 单击  ，以在卡片视图中查看 vApp。

3 从要重置的 vApp 的**操作**菜单中，选择**重置**。

结果

状态即被清除，vApp 仍继续运行。

挂起 vApp

挂起 vApp 会将内存写入磁盘，从而保留其当前状态。

前提条件

vApp 正在运行。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 单击  ，以在卡片视图中查看 vApp。

3 从要挂起的 vApp 的**操作**菜单中，选择**挂起**。

结果

vApp 将挂起并保留其状态。

放弃 vApp 的挂起状态

如果 vApp 处于挂起状态，并且您不再需要继续使用该 vApp，则可以放弃挂起状态。放弃挂起状态将释放保留的内存，并使 vApp 恢复到电源关闭状态。

前提条件

vApp 必须处于挂起状态。

步骤

1. 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。
2. 单击  ，以在卡片视图中查看 vApp。
3. 从挂起的 vApp 的**操作**菜单中，选择**放弃挂起状态**。

结果

将放弃该状态且 vApp 电源被关闭。

打开多个 vApp 的电源

可以同时打开多个 vApp 的电源。此操作将打开 vApp 中尚未打开电源的所有虚拟机的电源。

前提条件

确认您至少是 **vApp 作者**。

步骤

1. 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。
2. 启用**多选**选项。
3. 选择要打开电源的 vApp。
4. 从**操作**菜单中，选择**启动**。
5. 单击**确定**进行确认。

关闭多个 vApp 的电源

可以同时关闭多个 vApp 的电源。此操作将关闭 vApp 中所有虚拟机的电源。要执行某些操作（如将 vApp 添加到目录、复制或移动到其他虚拟数据中心），首先必须关闭 vApp 的电源。

前提条件

- 确认 vApp 已启动。
- 确认您至少是 **vApp 作者**。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 启用**多选**选项。

3 选择要关闭电源的 vApp。

4 从**操作**菜单中，选择**关闭**。

5 单击**确定**进行确认。

放弃多个 vApp 的挂起状态

如果多个 vApp 处于挂起状态，并且您不再需要继续使用它们，则可以同时放弃这些 vApp 的挂起状态。放弃挂起状态将释放保留的内存，并使 vApp 恢复到电源关闭状态。

前提条件

- 确认 vApp 处于挂起状态。
- 确认您至少是 **vApp 作者**。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 启用**多选**选项。

3 选择要关闭电源的已挂起 vApp。

4 从**操作**菜单中选择**放弃已挂起状态**。

结果

vApp 将关闭电源。

重置多个 vApp

重置多个 vApp 将同时清除其状态（包括内存、缓存等），但 vApp 仍可继续运行。

前提条件

- 确认 vApp 已启动并打开其中虚拟机的电源。
- 确认您至少是 **vApp 作者**。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 启用**多选**选项。

3 选择要重置的 vApp。

4 从**操作**菜单中，选择**重置**，然后单击**确定**进行确认。

结果

每个 vApp 的状态即被清除，并且 vApp 仍继续运行。

挂起多个 vApp

挂起多个 vApp 时，通过将内存写入磁盘同时保留它们的当前状态。

前提条件

确认 vApp 正在运行。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 启用**多选**选项。

3 选择要挂起的 vApp。

4 从要挂起的 vApp 的**操作**菜单中，选择**挂起**，然后单击**确定**进行确认。

结果

这些 vApp 将挂起并保留其状态。

打开 vApp

可以打开 vApp，查看所含的虚拟机和网络。此外，还可以查看显示虚拟机和网络连接情况的图表。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 单击  ，以在卡片视图中查看 vApp。

在卡视图中，您可以查看每个 vApp 的常规信息，例如其名称、电源状况、租约信息、创建日期、所有者、与 vApp 关联的虚拟机数量、CPU 总数、存储和内存总量以及关联的网络。

3 要查看所选 vApp 的详细设置，请单击 vApp 视图上的**详细信息**。

编辑 vApp 属性

可以编辑现有 vApp 的属性，包括 vApp 名称和描述、租约设置、vApp 中虚拟机的启动顺序、共享设置和网络设置。

编辑 vApp 常规属性

您可以查看并更改 vApp 的名称、描述和其他常规属性。

前提条件

确认 vApp 已关闭电源。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 单击  ，以在卡片视图中查看 vApp。

3 在所选 vApp 对应的视图中，单击**详细信息**以查看并编辑 vApp 属性。

4 查看并根据需要更改属性，然后单击**保存**。

选项	操作
名称	输入 vApp 的新名称。
描述	键入 vApp 的可选描述。
虚拟数据中心	vApp 所属的数据中心的名称。
快照	如果有快照，则会显示其详细信息。
租约	选择**续订**以续订租约。 a 调度运行时租约（以小时数或天数为单位）。 定义 vApp 在自动停止之前可以运行的时间。 b 调度存储租约（以小时数或天数为单位）。 定义 vApp 在被自动删除之前保持可用的时间。

结果

此时将保存常规设置。

编辑 vApp 中虚拟机的启动和停止顺序

您可以在 vApp 中配置虚拟机的启动和停止顺序。如果在必须按特定顺序启动和停止的虚拟机中安装了应用程序，请配置启动和停止顺序。

如果您需要按特定顺序启动和停止虚拟机，则这些设置非常有用。例如，一台虚拟机托管数据库服务器，另一台虚拟机托管应用程序服务器，最后一台虚拟机托管 Web 服务器。为了使相关功能正常工作，必须首先启动数据库服务器，其次必须启动应用程序服务器，最后必须启动 Web 服务器。

前提条件

确认 vApp 已关闭电源。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 单击  ，以在卡片视图中查看 vApp。

3 在所选 vApp 的卡片中，单击**详细信息**。

4 单击**启动和停止顺序**选项卡，然后单击**编辑**。

5 编辑每个虚拟机的启动和停止顺序属性，然后单击**确定**。

选项	操作
启动顺序	输入希望虚拟机启动的顺序。必须为序列中的每个计算机输入一个值。
启动操作	选择启动操作。 启动操作可确定启动包含虚拟机的 vApp 时该虚拟机所执行的操作。默认情况下，此选项设置为**启动**。
启动等待	输入启动等待时间。 启动等待时间是 VMware Cloud Director 启动序列中的下一台计算机之前需要等待的时间（秒）。
停止操作	选择停止操作。 停止操作是停止包含虚拟机的 vApp 时该虚拟机所执行的操作。如果您选择**关闭电源**，则 VM 会关闭电源但不执行确保稳定性的关机操作（相当于从插座拔下插头）。如果尚未安装 VMware Tools，请选择此操作。否则，请选择**关机**，以确保在关机时具有稳定性。
停止等待	输入停止等待时间。 停止等待时间是 VMware Cloud Director 关闭序列中的下一台虚拟机之前需要等待的时间（秒）。

编辑 vApp 的客户机属性

如果 vApp 包括用户可配置的 OVF 属性，则可以查看并修改这些属性。

如果 vApp 中的虚拟机包括具有相同名称的用户可配置属性的值，则虚拟机值优先。

前提条件

确认 vApp 已停止，并且其客户机属性是用户可配置属性。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**虚拟机**。

2 单击  ，在卡片视图中查看列表，并（可选）从**排序依据**下拉菜单中排列虚拟机列表。

3 在要编辑的虚拟机的卡中，单击**详细信息**。

4 单击**客户机属性**，然后单击**编辑**。

5 修改 vApp 的客户机属性，然后单击**确定**。

共享 vApp

您可以与组织中的其他组或用户共享您的 vApp。您设置的访问控制权限确定可以在共享 vApp 中完成的操作。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 单击  ，以在卡片视图中查看 vApp。

3 在所选 vApp 对应的视图中，单击**详细信息**，然后向下滚动到 vApp 的共享属性。

4 选择要与其共享 vApp 的用户，然后单击**保存**。

选项	操作
与组织中的每个人共享	选择此选项以与组织中的所有用户共享，并选择访问级别。 ■ 要授予完全控制权限，请选择**完全控制**。 组织中的所有用户均可打开和启动 vApp 以及将 vApp 另存为 vApp 模板，将模板添加到目录，更改 vApp 的所有者，复制到目录和修改属性。 ■ 要授予只读访问权限，请选择**只读**。
与特定用户和组共享	选择此选项仅与指定的用户共享。 a 从**没有访问权限的用户和组**面板中选择名称，将其移至**具有访问权限的用户和组**面板。 b 为指定的用户和组选择访问级别。 ■ 要授予完全控制权限，请选择**完全控制**。 具有完全控制权限的用户可以打开和启动 vApp 以及将 vApp 另存为 vApp 模板，将模板添加到目录，更改 vApp 的所有者，复制到目录和修改属性。 ■ 要授予只读访问权限，请选择**只读**。

结果

您的 vApp 将与指定的用户或组共享。

显示 vApp 网络图

vApp 网络图显示了 vApp 中虚拟机和网络的图形视图。

前提条件

要查看 vApp 网络图，您的 vApp 包含的虚拟机必须少于 40 个。如果 vApp 包含的虚拟机超过 40 个，则该图不可用。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择 **vApp**。

2 单击  ，以在卡片视图中查看 vApp。

3 在所选 vApp 的卡片中，单击**详细信息**。

4 单击**网络图**选项卡。

将出现一个图表，其中显示 vApp 中虚拟机和网络的连接方式。星号表示主网卡。如果网卡已连接，则显示绿色；如果网卡未连接，则显示白色。

5 （可选） 要突出显示已连接的虚拟机和网络，单击网络或虚拟机。

已连接的对象及其之间的连接将突出显示。

后续步骤

您可以在此页面中添加虚拟机或网络。

使用 vApp 中的网络

vApp 中的虚拟机可以连接到 vApp 网络（隔离网络或路由网络）和组织虚拟数据中心网络（直连或防护）。您可以将不同类型的网络添加到 vApp，以实现多种网络连接方案。

vApp 中的虚拟机可以连接到 vApp 中的可用网络。如果要将虚拟机连接到另一个不同网络，则必须先将其添加到 vApp。

vApp 可以包括 vApp 网络和组织虚拟数据中心网络。vApp 网络可以是隔离或路由网络。隔离 vApp 网络包含在 vApp 内。您还可以将 vApp 网络路由到组织虚拟数据中心网络，以便与 vApp 外部的虚拟机连接。对于路由 vApp 网络，您可以配置网络服务，例如，防火墙和静态路由。

您可以将 vApp 直接连接到组织虚拟数据中心网络。如果多个 vApp 均含有连接到同一组织虚拟数据中心网络的相同虚拟机，并且要同时启动这些 vApp，则可以防护 vApp。通过防护 vApp，可以隔离其 MAC 和 IP 地址，使您能够在不发生冲突的情况下启动虚拟机。

添加到 vApp 的网络使用与您在其中创建 vApp 的组织虚拟数据中心关联的网络池。

查看 vApp 网络

您可以访问和查看 vApp 中的网络。

前提条件

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择 **vApp**。

2 单击  ，以在卡片视图中查看 vApp。

3 在所选 vApp 的卡片中，单击**详细信息**。

4 单击**网络**选项卡。

此时将显示网络列表（如有）。您可以查看每个网络的信息，例如名称、网关、网络掩码、连接，并保留 IP 和 NAT 资源。

5 （可选） 要编辑要查看的列，请单击**网格编辑器**图标 ( )，然后分别选中或取消选中要显示或隐藏的列对应的复选框。

防护 vApp 网络

打开包含在不同 vApp 中的相同虚拟机的电源可能会引起冲突。 要允许打开不同 vApp 中相同虚拟机的电源且不发生冲突，您必须防护 vApp。

防护 vApp 会隔离虚拟机的 MAC 和 IP 地址，并将组织 VDC 网络的连接类型从直连更改为防护。在防护网络上，将自动启用和配置防火墙，以仅允许出站流量。在防护 vApp 时，还可以在防护网络上配置 NAT 和防火墙规则。

前提条件

- 您只能防护直连 vApp 网络。如果 vApp 使用多个网络，而其他网络是（例如）路由网络，则只防护直连网络。
- 必须停止 vApp 中使用直连网络的虚拟机，以确保直连 vApp 网络当前未在使用中。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 单击 ，以在卡片视图中查看 vApp。

3 在所选 vApp 的卡片中，单击**详细信息**。

4 单击**网络**选项卡。

5 如果 vApp 未受到防护，请单击**编辑**按钮。

6 打开**防护 vApp** 选项，然后单击**确定**。

结果

虚拟机的 IP 和 MAC 地址将被隔离。您可以打开不同 vApp 中相同虚拟机的电源且不会发生冲突。

将网络添加到 vApp

可以将网络添加到 vApp，使该网络可用于 vApp 中的虚拟机。可以将 vApp 网络或组织虚拟数据中心网络添加到 vApp。

连接可以是直接连接或防护连接。通过隔离虚拟机的 MAC 和 IP 地址，防护可以在不引起冲突的情况下启动不同 vApp 中相同的虚拟机。

如果已启用防护且 vApp 已打开电源，则会从组织虚拟数据中心网络池创建一个隔离网络。系统会创建一个 Edge 网关并将其连接到隔离网络和组织虚拟数据中心网络。进出虚拟机的流量会经过该 Edge 网关，该网关将使用 NAT 和代理 AR 转换 IP 地址。这样，路由器可以使用相同的 IP 空间在两个网络之间传递流量。

前提条件

要添加组织虚拟数据中心网络，您的管理员必须已创建此类网络。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 单击  ，以在卡片视图中查看 vApp。

3 在所选 vApp 对应的卡片视图中，单击**操作**，然后选择**添加网络**。

4 选择要添加的网络类型。

选项	操作
组织 VDC 网络	从可用网络列表中选择一个组织虚拟数据中心网络。
vApp 网络	a 输入网络的名称和可选描述。 b 输入网络网关 CIDR。 c （可选）输入主 DNS 和辅助 DNS 以及 DNS 后缀。 d （可选）选择是否允许客户机 VLAN。 e （可选）输入静态 IP 池设置，如 IP 范围。 f （可选）要能够连接到组织虚拟数据中心网络，请打开**连接到组织 VDC 网络**选项，然后从列表中选择一个网络。

5 单击**添加**。

结果

网络将添加到 vApp。

后续步骤

vApp 中的虚拟机即连接到该网络。

配置 vApp 网络的网络服务

您可以为某些 vApp 网络配置网络服务，例如，DHCP、防火墙和网络地址转换 (NAT) 和静态路由。

可用的网络服务取决于 vApp 网络的类型。

表 3-1. 各网络类型提供的网络服务

vApp 网络类型	DHCP	防火墙	NAT	静态路由
直接				
路由	X	X	X	X
已隔离	X			

查看和编辑常规网络详细信息

您可以查看和编辑常规 vApp 网络详细信息，例如网络名称和描述。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 单击  ，以在卡片视图中查看 vApp。

3 在所选 vApp 的卡片中，单击**详细信息**。

4 在**网络**选项卡中，单击网络以查看网络详细信息。

5 在**常规**选项卡中，查看网络信息。

6 单击**编辑**。

7 编辑 vApp 网络名称和描述。

8 单击**保存**。

编辑 vApp 网络的静态 IP 池设置

您可以配置 vApp 网络，通过从 IP 地址的静态池中拖动静态 IP 地址将其提供给 vApp 中的虚拟机。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 单击  ，以在卡片视图中查看 vApp。

3 在所选 vApp 的卡片中，单击**详细信息**。

4 在**网络**选项卡中，单击网络以查看网络详细信息。

5 在 **IP 管理**选项卡中，单击**静态池**。

6 单击**编辑**。

7 输入 IP 范围，然后单击**添加**。

8 单击**保存**。

编辑 vApp 网络的 DNS 设置

创建 vApp 网络后，您可以随时查看和编辑 DNS 设置。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 单击  ，以在卡片视图中查看 vApp。

3 在所选 vApp 的卡片中，单击**详细信息**。

4 在**网络**选项卡中，单击网络以查看网络详细信息。

5 在 **IP 管理**选项卡中，单击 **DNS**。

此时将显示 DNS 设置。

6 单击**编辑**。

7 编辑主 DNS 和辅助 DNS 以及 DNS 后缀。

8 单击**保存**。

为 vApp 网络配置 DHCP

您可以配置某些 vApp 网络，以便为 vApp 中的虚拟机提供 DHCP 服务。

为 vApp 网络启用 DHCP 时，请将 vApp 中虚拟机上的网卡连接到该网络，并选择 DHCP 作为该网卡的 IP 模式。打开虚拟机的电源时，VMware Cloud Director 将向虚拟机分配 DHCP IP 地址。

前提条件

- 确认 vApp 网络为路由网络或隔离网络。
- 确认 vApp 位于受 NSX Data Center for vSphere 支持的组织虚拟数据中心中。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 单击  ，以在卡片视图中查看 vApp。

3 在所选 vApp 的卡片中，单击**详细信息**。

4 在**网络**选项卡中，单击网络以查看网络详细信息。

5 在 **IP 管理**选项卡上，单击 **DHCP**。

此时将显示 DHCP 状态。

6 单击**编辑**。

7 单击**已启用**。

8 在 **IP 池**文本框中，输入 IP 地址范围。

VMware Cloud Director 将使用这些地址来满足 DHCP 请求。DHCP IP 地址的范围不能与 vApp 网络的静态 IP 池重叠。

9 设置默认和最长租约时间（以秒为单位）。

10 单击**保存**。

显示 vApp 网络的 IP 分配

您可以检查 vApp 中网络的 IP 分配。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择 **vApp**。

2 单击  ，以在卡片视图中查看 vApp。

3 在所选 vApp 的卡片中，单击**详细信息**。

4 在**网络**选项卡中，单击网络以查看网络详细信息。

5 在 **IP 管理**选项卡中，单击 **IP 分配**。

此时将显示已分配的 IP 地址。

为 vApp 网络配置静态路由

可以将某些 vApp 网络配置为提供静态路由服务，以允许不同 vApp 网络上的虚拟机进行通信。

所创建的任何静态路由将自动启用。

前提条件

一个路由 vApp 网络。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择 **vApp**。

2 单击  ，以在卡片视图中查看 vApp。

3 在所选 vApp 的卡片中，单击**详细信息**。

4 在**网络**选项卡中，单击网络以查看网络详细信息。

5 在**路由**选项卡上，单击**编辑**。

您可以对网络启用或禁用静态路由。

为 vApp 网络添加静态路由

您可以在路由到同一组织虚拟数据中心网络的两个 vApp 网络之间添加静态路由。两个网络之间可通过静态路由传输流量。

您无法将静态路由添加到已防护的 vApp 或在重叠的网络之间添加静态路由。将静态路由添加到 vApp 网络之后，请配置网络防火墙规则，使其允许在静态路由上传输流量。对于采用静态路由的 vApp，请选择使用已分配的 IP 地址，直至删除此 vApp 或关联网络为止。

仅当包含静态路由的 vApps 处于运行状态时，静态路由才起作用。如果更改 vApp 的父网络、删除 vApp 或删除 vApp 网络，且该 vApp 包括静态路由，则这些路由将无法起作用，而且您必须手动删除它们。

前提条件

- 两个 vApp 网络路由到同一组织虚拟数据中心网络。
- 这两个 vApp 网络处于至少已启动一次的 vApp 中。
- 两个 vApp 网络均已启用静态路由。

步骤

1. 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。
2. 单击  ，以在卡片视图中查看 vApp。
3. 在所选 vApp 的卡片中，单击**详细信息**。
4. 在**网络**选项卡中，单击网络以查看网络详细信息。
5. 在**路由**选项卡的“静态路由”下，单击**添加**。

   此时将显示已分配的 IP 地址。
6. 输入静态路由的名称。
7. 以 CIDR 格式输入网络地址。

   该网络地址将用于要添加静态路由的 vApp 网络。
8. 输入下一跳 IP 地址。

   下一跳 IP 地址是该 vApp 网络的路由器的外部 IP 地址。
9. 单击**保存**。
10. 对第二个 vApp 网络重复相同的过程。

示例： 静态路由示例

vApp 网络 1 和 vApp 网络 2 均路由到共享的组织网络。您可以在每个 vApp 网络上创建静态路由，以允许在网络之间传输流量。可以使用 vApp 网络信息来创建静态路由。

表 3-2. 网络信息

网络名称	网络规范	路由器外部 IP 地址
vApp 网络 1	192.168.1.0/24	192.168.0.100
vApp 网络 2	192.168.2.0/24	192.168.0.101
共享的组织网络	192.168.0.0/24	不适用

在 vApp 网络 1 上，创建指向 vApp 网络 2 的静态路由。在 vApp 网络 2 上，创建指向 vApp 网络 1 的静态路由。

表 3-3. 静态路由设置

vApp 网络	路由名称	网络	下一跳 IP 地址
vApp 网络 1	tovapp2	192.168.2.0/24	192.168.0.101
vApp 网络 2	tovapp1	192.168.1.0/24	192.168.0.100

将端口转发规则添加到 vApp 网络

通过添加 NAT 映射规则，您可以配置某些 vApp 网络以提供端口转发。

端口转发能让用户从外部访问在 vApp 网络上虚拟机中运行的服务。

配置端口转发之后，VMware Cloud Director 会将外部端口映射到在专用于入站流量的虚拟机上运行的服务。

将端口转发规则添加到 vApp 网络之后，它将显示在 NAT 映射规则列表的底部。有关如何设置端口转发规则实施顺序的信息，请参见

前提条件

- 确认 vApp 网络已路由。
- 确认 vApp 网络上的防火墙已启用。如果禁用防火墙，则 NAT 映射规则将不再应用于 vApp 网络。

步骤

1. 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。
2. 单击  ，以在卡片视图中查看 vApp。
3. 在所选 vApp 的卡片中，单击**详细信息**。
4. 在**网络**选项卡中，单击网络以查看网络详细信息。
5. 依次单击**服务**和**编辑**。
6. 要启用 NAT，请启用“NAT”选项。
7. 从 **NAT 类型**下拉菜单中，选择**端口转发**，然后单击**添加**。

8 （可选） 要启用 IP 伪装，请选中该复选框。

9 配置端口转发规则。

a 选择外部端口。

b 选择要转发到的端口。

c 选择虚拟机接口。

d 针对要转发的流量类型选择协议。

10 单击**保存**。

后续步骤

如有必要，使用**上移**或**下移**按钮重新排列端口转发规则。

将 IP 转换规则添加到 vApp 网络

通过添加 NAT 映射规则，您可以将某些 vApp 网络配置为提供 IP 转换。

创建网络的 IP 转换规则时，vCloud Director 会将 DNAT 和 SNAT 规则添加到与网络的端口组相关联的 Edge 网关。DNAT 规则会将入站流量的外部 IP 地址转换为内部 IP 地址。SNAT 规则会将出站流量的内部 IP 地址转换为外部 IP 地址。

前提条件

- 确认 vApp 网络已路由。
- 确认 vApp 网络上的防火墙已启用。如果禁用防火墙，则 NAT 映射规则将不再应用于 vApp 网络。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 单击  ，以在卡片视图中查看 vApp。

3 在所选 vApp 的卡片中，单击**详细信息**。

4 在**网络**选项卡中，单击网络以查看网络详细信息。

5 依次单击**服务**和**编辑**。

6 要启用 NAT，请启用“NAT”选项。

7 从 **NAT 类型**下拉菜单中，选择 **IP 转换**，然后单击**添加**。

8 选择虚拟机接口，然后单击**保留**。

9 选择映射模式。

10 如果选择**手动**映射模式，则输入外部 IP 地址。

11 单击**保存**。

后续步骤

如有必要，使用**上移**或**下移**按钮重新排列 IP 转换规则。

删除 vApp 网络

如果您不再需要 vApp 中的某个网络，则可以将其删除。

前提条件

vApp 已停止，且 vApp 中的任何虚拟机均未与该网络相连。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 单击  ，以在卡片视图中查看 vApp。

3 在所选 vApp 的卡片中，单击**详细信息**。

4 在**网络**选项卡上，选择要删除的网络，单击**删除**，然后确认删除。

使用快照

创建快照会保留 vApp 内的虚拟机在某个特定时间点的状态和数据。快照并不供长期使用，也不能代替 vApp 备份。

升级 vApp 中的虚拟机时，您可能希望使用快照。例如，在升级虚拟机之前，您创建一个快照以保留升级前的时间点。为此，您在升级之前保存一个快照，然后执行升级。如果升级期间无任何问题，您可以选择移除此快照，提交您在升级期间所做的更改。但是，如果您遇到问题，则可以恢复快照，返回到升级前已保存的 vApp 状态。

创建 vApp 的快照

通过创建 vApp 的快照，会创建该 vApp 中所有虚拟机的快照。创建快照后，可以将 vApp 中的所有虚拟机恢复到快照，也可以在不需要时移除快照。

vApp 快照具有一些限制。

- vApp 快照不会捕获网卡配置。
- 如果 vApp 中有任何虚拟机连接到给定磁盘，则无法创建 vApp 快照。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 单击  ，以在卡片视图中查看 vApp。

3 从要创建快照的 vApp 的**操作**菜单中，选择**创建快照**。

创建 vApp 的快照将替换现有快照（如果有）。

4 （可选） 选择是否创建 vApp 内存的快照。

捕获 vApp 内存状况时，快照会保留 vApp 以及 vApp 中的虚拟机的实时状况。内存快照可以创建某一精确时间点的快照（例如，升级仍在运行的软件）。生成了内存快照后，如果升级未按预期完成，或软件不符合您的预期，则可将虚拟机恢复到其以前的状态。

捕获内存状况时，vApp 的文件无需静默。如果未捕获内存状况，快照就不会保存 vApp 的实时状况，除非静默磁盘，否则磁盘就是崩溃一致的。

5 （可选） 选择是否静默客户机文件系统。

此操作要求已在 vApp 上安装 VMware Tools。当静默虚拟机时，VMware Tools 会静默虚拟机的文件系统。静默操作可确保快照磁盘表示客户机文件系统的一致状况。静默快照适用于自动备份或定期备份。例如，如果您无法识别虚拟机的活动，但希望恢复为多个最近的备份，则可以静默文件。

您无法静默包含大容量磁盘的 vApp。

6 单击**确定**。

结果

将创建 vApp 的快照。

后续步骤

您可以将 vApp 中的所有虚拟机恢复到最近的快照。

将 vApp 恢复到快照

您可以将 vApp 中的所有虚拟机恢复到创建 vApp 快照时所处的状态。

前提条件

验证 vApp 是否具有现有快照。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 单击  ，以在卡片视图中查看 vApp。

3 从要恢复的 vApp 的**操作**菜单中，选择**恢复到快照**。

4 单击**确定**。

结果

vApp 中的所有虚拟机均恢复到快照状态。

移除 vApp 的快照

您可以移除 vApp 的快照。

移除 vApp 快照时，会删除该 vApp 快照中的虚拟机的状态，而且无法再次返回到该状态。移除快照不会影响 vApp 的当前状态。

前提条件

您已创建 vApp 的快照。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 单击  ，以在卡片视图中查看 vApp。

3 从要移除快照的 vApp 的**操作**菜单中，选择**移除快照**。

4 单击**确定**。

结果

快照已被移除。

生成多个 vApp 的快照

通过生成多个 vApp 的快照，可以生成这些 vApp 中所有虚拟机的快照。生成快照后，可以将 vApp 中的所有虚拟机恢复到快照，也可以在不需要时移除快照。

vApp 快照具有一些限制。

- vApp 快照不会捕获网卡配置。
- 如果 vApp 中有任何虚拟机已连接到指定磁盘，则无法生成 vApp 快照。
- 生成多个 vApp 的快照不会创建 vApp 内存的快照，并且不会静默 vApp 的客户机文件系统。如果要创建 vApp 内存的快照或静默客户机文件系统，必须为每个 vApp 创建单独的快照。请参见创建 vApp 的快照。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 启用**多选**选项。

3 选择要为其生成快照的 vApp。

4 从**操作**菜单中，选择**创建快照**，然后单击**确定**进行确认。

后续步骤

- 您可以将 vApp 中的所有虚拟机恢复到最近的快照。请参见将多个 vApp 恢复到快照。

- 您可以移除 vApp 的快照。请参见移除多个 vApp 的快照。

移除多个 vApp 的快照

如果您不需要多个 vAapp 的快照，可以同时移除这些快照。

移除 vApp 快照时，会删除该 vApp 快照中的虚拟机的状态，而且无法再次返回到该状态。移除快照不会影响 vApp 的当前状态。

步骤

1. 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。
2. 启用**多选**选项。
3. 选择要移除其快照的 vApp。
4. 从**操作**菜单中，选择**移除快照**。

将多个 vApp 恢复到快照

可以将多个 vApp 中的所有虚拟机恢复到创建 vApp 快照时所处的状态。

前提条件

验证要恢复的 vApp 是否存在现有快照。

步骤

1. 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。
2. 启用**多选**选项。
3. 选择要恢复到其最近快照的 vApp。
4. 从**操作**菜单中，选择**恢复到快照**。
5. 单击**确定**进行确认。

更改 vApp 所有者

您可以更改 vApp 的所有者，例如，当 vApp 所有者离开公司或在公司内发生角色更改时。

前提条件

此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。

步骤

1. 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 单击  ，以在卡片视图中查看 vApp。

3 从要更改其所有者的 vApp 的**操作**菜单中，选择**更改所有者**。

4 从列表中选择一个用户。

5 单击**确定**。

结果

将更改 vApp 的所有者。

将 vApp 移至另一个虚拟数据中心

将 vApp 移至另一个虚拟数据中心时，将从源虚拟数据中心内删除该 vApp。

前提条件

- 您至少是 **vApp 作者**。
- vApp 已关闭电源。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 单击  ，以在卡片视图中查看 vApp。

3 从要移动的 vApp 的**操作**菜单中，选择**移至**。

4 选择要向其移动 vApp 的虚拟数据中心并单击**确定**。

5 （可选） 选择存储策略。

6 单击**确定**。

结果

vApp 即从源数据中心移除并移动到目标数据中心。

将停止的 vApp 复制到另一个虚拟数据中心

将 vApp 复制到另一个虚拟数据中心时，原始 vApp 保留在源虚拟数据中心。

前提条件

- 您至少是 **vApp 作者**。
- vApp 已关闭电源。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 单击  ，以在卡片视图中查看 vApp。

3 从要复制的 vApp 的**操作**菜单中，选择**复制到**。

4 键入名称和描述。

5 选择要在其中创建 vApp 副本的虚拟数据中心。

6 （可选） 选择存储策略。

7 单击**确定**。

结果

将使用提供的名称和描述将 vApp 复制到指定的虚拟数据中心。

复制已启动的 vApp

要基于现有 vApp 创建一个 vApp，可以复制 vApp，并更改复制的副本使之符合需求。复制 vApp 之前，无需关闭 vApp 中的虚拟机。运行中的虚拟机的内存状态保留在复制的 vApp 中。

前提条件

验证是否满足以下条件：

- 您至少是 **vApp 用户**。
- vCenter Server 5.5 或更高版本支持组织虚拟数据中心。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。

2 单击  ，以在卡片视图中查看 vApp。

3 从要复制的 vApp 的**操作**菜单中，选择**复制到**。

4 键入名称和描述。

5 选择要在其中创建 vApp 副本的虚拟数据中心。

6 （可选） 选择存储策略。

7 单击**确定**。

结果

将创建 vApp 副本且该 vApp 副本处于挂起状态。启用复制的 vApp 以实现网络防护。

后续步骤

修改新的 vApp 的网络属性，或启动 vApp。

将虚拟机添加到 vApp

您可以将虚拟机添加到 vApp。

前提条件

要访问公用目录中的虚拟机，您必须成为**组织管理员**或 **vApp 作者**。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择 **vApp**。

2 单击  ，以在卡片视图中查看 vApp。

3 从要向其添加虚拟机的 vApp 的**操作**菜单中，选择**添加 VM**。

将在**添加 VM** 窗口中显示与 vApp 关联的虚拟机的列表。

4 要创建新的虚拟机并自动将其与 vApp 关联，则单击**添加虚拟机**。

5 输入虚拟机的名称和计算机名称。

重要事项 计算机名称只能包含字母数字字符和连字符。计算机名称不能仅包含数字，并且不能包含空格。

6 （可选） 输入有意义的描述。

7 选择是否要在虚拟机创建后立即打开电源。

8 选择希望部署虚拟机的方式。

选项	操作
新建	使用可自定义的设置部署新虚拟机。 a 选择操作系统系列和操作系统。 b （可选）选择引导映像。 c 选择计算策略。 d 选择虚拟机的大小，或单击**自定义大小调整选项**以手动输入计算、内存和存储设置。 预定义的大小调整选项为小、中或大。 e 指定虚拟机的存储设置，例如存储策略和大小 (GB)。 f 指定虚拟机的网络设置，如网络、IP 模式、IP 地址和主网卡。
从模板	基于从模板目录选择的模板部署虚拟机。 a 从目录中选择虚拟机模板。 b （可选）选择使用自定义存储策略，然后从**要使用的自定义存储策略**中选择策略。 c 如果提供了最终用户许可协议，必须查看并接受该协议。

9 单击**确定**以创建虚拟机。

10 单击**添加**以将虚拟机添加到 vApp。

将 vApp 作为 vApp 模板保存到目录

通过将 vApp 添加到目录，您可以将特定 vApp 转换为 vApp 模板。

前提条件

- 此操作需要预定义的 **vApp 作者**角色中包含的权限或一组等效权限。
- 您的组织必须已有目录和具有可用空间的虚拟数据中心。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择 **vApp**。

2 单击  ，以在卡片视图中查看 vApp。

3 从要添加到目录的 vApp 的**操作**菜单中，选择**添加到目录**。

注 即使属于 vApp 的虚拟机处于运行状态，您也可以向目录中添加 vApp。但是，如果您选择某个正在运行的 vApp，它将作为 vApp 模板添加到目录中，且所有虚拟机将处于挂起状态。

4 从**目录**下拉菜单中选择目标目录。

5 输入 vApp 模板的名称和可选描述。

6 （可选）选择**覆盖目录项**（如果希望新目录项覆盖任何现有 vApp 模板），并选择要覆盖的目录项。

例如，将新版本的 vApp 上载到目录时，可能希望覆盖旧版本。

7 指定模板的使用方式。

基于 vApp 模板创建 vApp 时，此设置适用。使用此模板中的单个虚拟机构建 vApp 时，将忽略此设置。

选项	描述
制作相同副本	选择此选项将在从 vApp 模板创建 vApp 时制作 vApp 的相同副本。
自定义 VM 设置	选择此选项将在从 vApp 模板创建 vApp 时对虚拟机设置进行自定义。

8 单击**确定**以完成 vApp 模板创建。

结果

vApp 另存为 vApp 模板并显示在指定的目录中。

将 vApp 作为 OVF 软件包下载

可以将 vApp 作为 OVF 软件包或作为 OVA（这是同一 OVF 文件软件包的单个文件分发版）进行下载。

前提条件

- 此操作需要预定义的 **vApp 作者**角色中包含的权限或一组等效权限。
- 验证 vApp 是否已关闭且未部署。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择 **vApp**。

2 单击  ，以在卡片视图中查看 vApp。

3 从要下载的 vApp 的**操作**菜单中，选择**下载**。

4 选择下载 vApp 时要使用的格式。

5 （可选）选择**保留身份信息**以在下载的 OVF 软件包中包括 vApp 中驻留的虚拟机的 UUID 和 MAC 地址。

这限制了该软件包的可移植性，只有必要时才应使用。

6 单击**确定**以确认所选内容并开始下载。

结果

默认情况下，该软件包将下载到您的浏览器的 `Downloads` 文件夹中。

续订 vApp 租约

如果 vApp 的租约已过期或即将过期，则可以进行续订。

前提条件

确认已为您分配预定义角色 **vApp 用户**或一组等效权限。

步骤

1. 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。
2. 选择要更新的 vApp。
3. 从**操作**菜单中，选择**更新租约**。
4. 续订 vApp 的运行时租约。
   a. 选中**运行时租约**复选框。
   b. 从下拉菜单中，为运行时租约选择一个值。
      可以选择以小时、天为单位的值，也可以将租约设置为**从不过期**。
5. 续订 vApp 的存储租约。
   a. 选中**存储租约**复选框。
   b. 从下拉菜单中，为存储租约选择一个值。
      可以选择以小时、天为单位的值，也可以将租约设置为**从不过期**。

删除 vApp

将 vApp 从组织中移除之后，您便可以将其删除。

前提条件

必须将 vApp 停止。

您至少必须是 **vApp 作者**。

步骤

1. 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**vApp**。
2. 选择要删除的 vApp。
3. 从**操作**菜单中，选择**删除**。
4. 单击**确定**。

结果

该 vApp 将被删除。

删除多个 vApp

要从您的组织中移除多个 vApp，可以同时将其删除。

前提条件

- 确认您的 vApp 已停止。
- 确认您至少是 **vApp 作者**。

步骤

1. 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择 **vApp**。
2. 启用**多选**选项。
3. 选择要删除的 vApp。
4. 从**操作**菜单中，选择**删除**。
5. 单击**删除**，确认删除。

使用 VMware Cloud Director 网络 4

为了在多用途云环境中提供高度灵活的安全网络基础架构，VMware Cloud Director 使用包含三类网络的分层网络架构 - 外部网络、组织虚拟数据中心网络和 vApp 网络。大多数类型的 VMware Cloud Director 网络都需要额外的基础架构对象，如 Edge 网关和网络池。

外部网络

外部网络提供上行链路接口，将 VMware Cloud Director 环境中的网络和虚拟机连接到外部网络，例如 VPN、企业内部网或公共 Internet。

外部网络由单个 vSphere 网络、多个 vSphere 网络或 NSX-T Data Center 第 0 层逻辑路由器提供支持。

只有**系统管理员**才能创建外部网络。有关外部网络的详细信息，请参见《VMware Cloud Director 服务提供商管理门户指南》。

网络池

网络池是隔离的第 2 层网络分段的集合，您可以使用这些分段按需创建 vApp 网络和特定类型的组织虚拟数据中心网络。

必须先创建网络池，然后才能创建组织虚拟数据中心网络和 vApp 网络。如果不存在网络池，组织唯一可用的网络选项是直接连接到外部网络。

只有**系统管理员**才能创建网络池。

有关网络池的详细信息，请参见《VMware Cloud Director 服务提供商管理门户指南》。

组织虚拟数据中心网络

组织虚拟数据中心网络使 vApp 能够相互通信或与组织外部的外部网络进行通信。

有多种类型的组织虚拟数据中心网络，具体取决于组织虚拟数据中心网络与外部网络的连接。

组织虚拟数据中心网络提供直接或路由连接到外部网络，或者也可以与外部网络和其他组织虚拟数据中心网络相隔离。路由连接要求组织虚拟数据中心具有 Edge 网关和网络池。

组织虚拟数据中心网络由**系统管理员**或**组织管理员**创建并分配给组织虚拟数据中心。

新创建的组织虚拟数据中心内没有网络。**系统管理员**创建所需的网络基础架构后，**组织管理员**可以创建和管理大多数类型的组织虚拟数据中心网络。

vApp 网络

vApp 网络允许虚拟机相互通信，或者通过连接到组织虚拟数据中心网络与其他 vApp 中的虚拟机通信。

vApp 网络包含在 vApp 内。vApp 网络可以与其他网络隔离，也可以连接到组织虚拟数据中心网络。

每个 vApp 包含一个 vApp 网络。部署 vApp 时将创建该网络，取消部署 vApp 时将删除该网络。

vApp 网络由**组织管理员**设置和控制。

vApp 中的网络类型

vApp 中的虚拟机可以连接到 vApp 网络（可能是隔离、直连或路由网络），也可以连接到组织虚拟数据中心网络。

注 NSX Data Center for vSphere 支持的组织虚拟数据中心支持路由、隔离和直连 vApp 网络。

NSX-T Data Center 支持的组织虚拟数据中心支持隔离和直连 vApp 网络。

您可以将不同类型的网络添加到 vApp，以实现多种网络连接方案。

vApp 中的虚拟机可以连接到 vApp 中的可用网络。如果要将虚拟机连接到不同网络，必须先将此网络添加到 vApp。

vApp 可以包括 vApp 网络和组织虚拟数据中心网络。隔离 vApp 网络包含在 vApp 内。

您还可以将 vApp 网络路由到组织虚拟数据中心网络，以便与 vApp 外部的虚拟机连接。对于路由 vApp 网络，您可以配置网络服务，例如，防火墙和静态路由。

您可以将 vApp 直接连接到组织虚拟数据中心网络。

如果多个 vApp 均含有连接到同一组织虚拟数据中心网络的相同虚拟机，并且要同时启动这些 vApp，则可以防护 vApp。通过防护 vApp，可以隔离其 MAC 和 IP 地址，使您能够在不发生冲突的情况下启动虚拟机。

有关详细信息，请参见使用 vApp 中的网络。

Edge 网关

Edge 网关可为路由组织虚拟数据中心网络提供外部网络连接，并可提供负载均衡 、网络地址转换和防火墙等服务。VMware Cloud Director 支持 IPv4 和 IPv6 Edge 网关。

Edge 网关需要 NSX Data Center for vSphere 或 NSX-T Data Center。

本章讨论了以下主题：

- 管理组织虚拟数据中心网络
- 管理跨虚拟数据中心网络

- 管理 NSX Data Center for vSphere Edge 网关服务
- 管理 NSX-T Data Center Edge 网关

管理组织虚拟数据中心网络

组织 VDC 网络由**系统管理员**或**组织管理员**创建并分配给组织 VDC。**组织管理员**可以查看有关网络的信息、配置网络服务等。

可以使用受 NSX Data Center for vSphere 支持的直连、路由、隔离或跨 VDC 组织虚拟数据中心网络。

可以使用受 NSX-T Data Center 支持的路由、隔离和已导入组织虚拟数据中心网络。

表 4-1. 组织 VDC 网络的类型

数据中心网络类型	描述
直接	能够直接连接到由**系统管理员**置备并由 vSphere 资源提供支持的外部网络之一的组织 VDC 网络。 NSX Data Center for vSphere 支持的组织 VDC 才支持直连网络。 可由多个组织 VDC 访问。属于不同组织 VDC 的虚拟机可连接到该网络并可查看该网络上的流量。 该网络提供与组织 VDC 外虚拟机的直接第 2 层连接。此组织 VDC 外的虚拟机可以直接连接到组织 VDC 中的虚拟机。 注 只有**系统管理员**才能添加直接组织 VDC 网络。 可以是 IPv4 或 IPv6。
隔离（内部）	只能由同一组织 VDC 访问。只有此组织 VDC 中的虚拟机才能连接到内部组织 VDC 网络并查看该网络上的流量。 NSX-T Data Center 支持的组织 VDC 和 NSX Data Center for vSphere 支持的组织 VDC 支持隔离网络。 隔离的组织 VDC 网络为组织 VDC 提供了一个隔离的专用网络，多个虚拟机和 vApp 都可以连接到该网络。该网络不提供与组织 VDC 外部虚拟机的连接。组织 VDC 外的计算机无法连接到组织 VDC 内的计算机。
路由	只能由同一组织 VDC 访问。只有此组织 VDC 中的虚拟机才能连接到该网络。 此网络还提供对外部网络的受控访问。作为**系统管理员**或**组织管理员**，您可以配置网络地址转换 (NAT)、防火墙和 VPN 设置，以便可从外部网络访问特定的虚拟机。 可以是 IPv4 或 IPv6。
已导入	此网络使用现有的 NSX-T 逻辑交换机。只有**系统管理员**才能导入网络。
跨 VDC	此网络是跨数据中心组的延伸网络的一部分。一个数据中心组可在单个或多站点 VMware Cloud Director 部署中包含 2 到 16 个组织虚拟数据中心。 连接到该网络的虚拟机将连接到底层延伸网络。 跨 VDC 网络需要 NSX Data Center for vSphere。 只能是 IPv4。 有关跨 VDC 网络的信息，请参见管理跨虚拟数据中心网络。

记录的管理组织 VDC 网络的所有步骤假定您的环境中有多个虚拟数据中心。

查看可用的组织 VDC 网络

您可以查看可用的组织虚拟数据中心网络。

前提条件

此操作需要预定义的**组织管理员**或**系统管理员**角色或包含一组等效权限的角色。

步骤

- 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**网络**。

结果

您会看到可按名称排序的可用网络列表。

后续步骤

您可以添加新的网络。您还可以编辑、删除或重置现有网络。

添加隔离组织虚拟数据中心网络

可以添加隔离组织 VDC 网络，该网络只能由该组织进行访问。该网络没有为组织外的虚拟机提供连接。此组织外的虚拟机无法连接到组织内的虚拟机。

可以混合添加隔离和路由组织 VDC 网络以满足组织的需求。例如，您可以隔离包含敏感信息的网络，同时使用单独的网络与 Edge 网关相关联并连接到 Internet。

您可以创建网络池支持的隔离 VDC 网络。此外，您的服务提供商还可以创建 NSX-T 逻辑交换机支持的隔离 VDC 网络。

您只能创建 IPv4 隔离组织 VDC 网络。

前提条件

此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。

步骤

1. 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**网络**。
2. 单击**添加**。
3. 在**选择网络类型**页面上，选择**隔离**，然后单击**下一步**。
4. 为您的组织 VDC 网络输入有意义的名称。
5. 输入隔离网络的无类别域间路由 (CIDR) 设置。

   使用格式 *network_gateway_IP_address/subnet_prefix_length*，例如 **`192.167.1.1/24`**。
6. （可选） 输入组织 VDC 网络的描述。

7 （可选） 要使组织 VDC 网络可供同一组织内的其他组织 VDC 使用，请打开**共享**选项。

如果应用程序所在的组织 VDC 将预留或分配池设置为分配模型，则可能会用到此选项。在这种情况下，它可能没有足够的空间运行更多虚拟机。作为解决方案，您可以通过即付即用方法创建一个辅助组织 VDC，临时在该网络上运行更多虚拟机。

注 这些组织 VDC 必须由同一提供者 VDC 提供支持。

8 单击**下一步**。

9 （可选） 要预留一个或多个 IP 地址以分配给需要静态 IP 地址的虚拟机，请为此网络配置**静态 IP 池**。

a 输入 IP 地址或 IP 地址范围，然后单击**添加**。

b 要添加多个静态 IP 地址或范围，请重复此步骤。

c （可选） 要修改或移除 IP 地址和范围，请单击**修改**或**移除**。

10 单击**下一步**。

11 （可选） 配置 DNS 设置。

选项	操作
主 DNS	输入主 DNS 服务器的 IP 地址。
辅助 DNS	输入辅助 DNS 服务器的 IP 地址。
DNS 后缀	输入 DNS 后缀。DNS 后缀是不包括主机名的 DNS 名称。

12 单击**下一步**。

13 在**即将完成**页面上，检查您提供的组织 VDC 网络设置，然后单击**完成**。

添加路由组织虚拟数据中心网络

要控制对外部网络的访问，您可以添加路由组织 VDC 网络。**系统管理员**和**组织管理员**可以配置网络地址转换 (NAT)、防火墙和 VPN 设置，以便可从外部网络访问特定的虚拟机。

可以混合添加路由和隔离组织 VDC 网络以满足组织的需求。例如，您可以添加与 Edge 网关相关联且连接到 Internet 的网络，同时使用包含敏感信息的隔离网络。

您可以添加 IPv4 或 IPv6 路由组织 VDC 网络。

前提条件

此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**网络**。

2 单击**添加**。

3 在**选择网络类型**页面上，选择**路由**，然后单击**下一步**。

4 为您的组织 VDC 网络输入有意义的名称。

5 输入路由组织 VDC 网络的无类别域间路由 (CIDR) 设置。

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

6 （可选） 输入组织 VDC 网络的描述。

7 （可选） 要使组织 VDC 网络可供同一组织内的其他组织 VDC 使用，请打开**共享**选项。

如果组织 VDC 内的应用程序将预留或分配池设置为分配模型，则可能会用到此选项。在这种情况下，它可能没有足够的空间运行更多虚拟机。作为解决方案，您可以通过即付即用方法创建一个辅助组织 VDC，临时在该网络上运行更多虚拟机。

注 组织 VDC 必须共享同一个网络池。

8 单击**下一步**。

9 在 **Edge 连接**页面上，选择要与组织 VDC 网络关联的 Edge 网关。

如果组织 VDC 包含多个 Edge 网关，必须选择一个要连接此网络的 Edge 网关。要支持其他路由网络，Edge 网关必须在“可用网络数”列中显示一个至少为 1 的值。

10 从**接口类型**下拉菜单中，选择接口类型。

选项	描述
内部	连接到 Edge 网关的一个内部接口。 允许的最大网络数为 9。
分布式	在连接到此 Edge 网关的分布式逻辑路由器上创建网络。 允许的最大网络数为 400。
子接口	扩展组织 VDC 网络。VMware Cloud Director 会标识要通过 L2 VPN 进行扩展的网络。 借助 NSX 网络虚拟化，VMware Cloud Director 为此网络创建中继接口类型。允许的最大网络数为 200。

11 （可选） 要在此网络上启用客户机 VLAN 标记，请打开**允许的客户机 VLAN** 选项。

12 单击**下一步**。

13 （可选） 要预留一个或多个 IP 地址以分配给需要静态 IP 地址的虚拟机，请为此网络配置**静态 IP 池**。

a 输入 IP 地址或 IP 地址范围，然后单击**添加**。

b 要添加多个静态 IP 地址或范围，请重复此步骤。

c （可选） 要修改或移除 IP 地址和范围，请单击**修改**或**移除**。

14 单击**下一步**。

15 （可选） 配置 DNS 设置。

选项	操作
主 DNS	输入主 DNS 服务器的 IP 地址。
辅助 DNS	输入辅助 DNS 服务器的 IP 地址。
DNS 后缀	输入 DNS 后缀。DNS 后缀是不包括主机名的 DNS 名称。

16 单击**下一步**。

17 在**即将完成**页面上，检查您提供的组织 VDC 网络设置，然后单击**完成**。

添加直连组织虚拟数据中心网络

要通过直连路由连接到外部网络，**系统管理员**可以设置直接连接。

如果您以**组织管理员**身份登录到 VMware Cloud Director 租户门户并尝试创建直连组织虚拟数据中心网络，您将收到一条警告消息，指出您没有足够的权限。

前提条件

此操作仅限于系统管理员。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**网络**。

2 单击**添加**。

3 在**选择网络类型**页面上，选择**直连**，然后单击**下一步**。

4 为您的组织 VDC 网络输入有意义的名称。

5 （可选） 输入组织 VDC 网络的描述。

6 （可选） 要使组织 VDC 网络可供同一组织内的其他组织 VDC 使用，请打开**共享**选项。

7 在**外部网络连接**页面上，选择要将新组织虚拟数据中心网络直接连接到的外部网络，然后单击**下一步**。

8 在**即将完成**页面上，检查您提供的组织 VDC 网络设置，然后单击**完成**。

通过导入的 NSX-T 逻辑交换机添加组织 VDC 网络

系统管理员可以通过从关联的 NSX-T Manager 实例导入逻辑交换机来创建组织 VDC 网络。

注 使用 NSX-T 逻辑交换机，只能创建 IPv4 隔离组织网络。无法基于 NSX-T 逻辑交换机创建直连组织网络。

前提条件

- 此操作仅限于**系统管理员**。
- 支持目标组织虚拟数据中心的提供者虚拟数据中心必须与 NSX-T Manager 实例相关联。
- **系统管理员**必须至少创建一个未被其他组织虚拟数据中心网络使用的 NSX-T 逻辑交换机。

有关创建和配置 NSX-T 逻辑交换机的信息，请参见《NSX-T Data Center 管理指南》。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**网络**。

2 单击**添加**。

3 在**选择网络类型**页面上，选择**导入**，然后单击**下一步**。

4 输入新组织 VDC 网络的名称和可选描述，然后单击**下一步**。

5 从可用 NSX-T 逻辑交换机列表中，单击交换机名称旁边的单选按钮以选择目标交换机，然后单击**下一步**。

6 输入网络无类别域间路由 (CIDR) 设置。

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

如果交换机配置了子网，系统会预填充此信息。

7 （可选） 配置 DNS 设置和静态 IP 池。

您可以添加多个 IP 地址和 IP 范围。

8 单击**下一步**。

9 检查**即将完成**页面，然后单击**完成**。

编辑组织虚拟数据中心网络的常规设置

您可以修改组织 VDC 网络的属性。

前提条件

这些操作需要预定义的**组织管理员**或**系统管理员**角色或包含一组等效权限的角色。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**网络**。

2 单击要查看或编辑的组织 VDC 网络的名称。

3 在**常规**选项卡上，单击**编辑**。

a 编辑网络的名称和描述。

b 打开或关闭**共享**选项，以便与同一组织内的其他虚拟数据中心共享或不共享组织 VDC 网络。

4 单击**保存**。

将组织虚拟数据中心网络连接到 Edge 网关

创建组织 VDC 网络后，可以将该网络连接到 Edge 网关。

从版本 10.1 开始，VMware Cloud Director 支持连接到 NSX Data Center for vSphere 或 NSX-T Data Center 提供支持的组织 VDC 网络的 Edge 网关。

前提条件

此操作要求有一个预定义的**组织管理员**或**系统管理员**角色，或包含**组织 VDC 网络：编辑属性**权限的角色。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**网络**。

2 单击要连接到 Edge 网关的组织 VDC 网络的名称。

3 在**常规**选项卡上，单击**编辑**。

4 单击**连接**。

5 将网络连接到 Edge 网关。

   a 打开**连接到 Edge 网关**选项。

   b 从可用 Edge 网关的列表中选择要连接到的 Edge 网关。

   c 选择接口类型。

   d 要允许客户机 VLAN，请打开**允许的客户机 VLAN** 选项。

6 单击**保存**。

结果

组织 VDC 网络将连接到 Edge 网关，并从隔离转换为路由。

断开组织 VDC 网络与 Edge 网关的连接

通过断开组织 VDC 网络与 Edge 网关的连接，可以将其从路由网络转换为隔离网络。

从版本 10.1 开始，对于由 NSX Data Center for vSphere 或 NSX-T Data Center 提供支持的组织 VDC 网络，支持连接到 Edge 网关以及与 Edge 网关断开连接。

前提条件

此操作要求有一个预定义的**组织管理员**或**系统管理员**角色，或包含**组织 VDC 网络：编辑属性**权限的角色。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**网络**。

2 单击要断开连接的组织 VDC 网络的名称。

3 在**常规**选项卡上，单击**编辑**。

4 单击**连接**。

5 要断开网络与 Edge 网关的连接，请关闭**连接到 Edge 网关**选项。

6 单击**保存**。

结果

您已断开组织 VDC 网络与 Edge 网关的连接。组织 VDC 网络已从路由网络转换为隔离网络。

转换路由组织 VDC 网络的接口

您可以将网络接口从内部更改为子接口或分布式路由，例如，通过编辑网络属性。

注 无法转换跨 VDC 网络。

前提条件

此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**网络**。

2 单击要转换的网络的名称。

3 单击要编辑的组织 VDC 网络的名称。

4 在**常规**选项卡上，单击**编辑**。

5 单击**连接**。

6 从**接口类型**下拉菜单中，选择接口类型。

选项	描述
内部	连接到 Edge 网关的一个内部接口。 允许的最大网络数为 9。
分布式	在连接到此 Edge 网关的分布式逻辑路由器上创建网络。 允许的最大网络数为 400。
子接口	扩展组织 VDC 网络。VMware Cloud Director 会标识要通过 L2 VPN 进行扩展的网络。 借助 NSX 网络虚拟化，VMware Cloud Director 为此网络创建中继接口类型。允许的最大网络数为 200。

7 单击**保存**。

查看用于组织虚拟数据中心网络的 IP 地址

您可以从组织虚拟数据中心网络 IP 池中查看当前正在使用的 IP 地址的列表。

前提条件

- 这些操作需要预定义的**组织管理员**或**系统管理员**角色或包含一组等效权限的角色。
- 确认您的网络是隔离组织虚拟数据中心网络还是路由组织虚拟数据中心网络。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**网络**。

2 单击要查看已用 IP 地址的网络的名称。

3 单击 **IP 管理**选项卡。

4 单击 **IP 分配**以查看当前正在使用的 IP 地址。

将 IP 地址添加到组织虚拟数据中心网络的 IP 池中

如果组织虚拟数据中心网络的 IP 地址已用尽，可在其 IP 池中添加更多地址。

您无法将 IP 地址添加到具有直接连接的外部组织虚拟数据中心网络。

前提条件

- 这些操作需要预定义的**组织管理员**或**系统管理员**角色或包含一组等效权限的角色。
- 确认您的网络是隔离组织虚拟数据中心网络还是路由组织虚拟数据中心网络。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**网络**。

2 单击要编辑的网络的名称。

3 单击 **IP 管理**选项卡。

默认情况下，**静态 IP 池**选项处于选中状态。

4 单击右侧的**编辑**按钮。

在**编辑网络**窗口中，您会看到网关 CIDR 和 IP 地址范围（如有）。

5 在**静态 IP 池**文本框中，输入 IP 地址或 IP 地址范围，然后单击**添加**。

注 对于跨 VDC 网络，IP 地址不得与分配给同一延伸网络中其他组织 VDC 网络的 IP 地址重叠。

6 单击**保存**。

结果

此时将 IP 地址或 IP 地址范围添加到网络 IP 池。

编辑或移除组织虚拟数据中心网络中使用的 IP 范围

如果组织虚拟数据中心网络包含不再需要的 IP 地址，您可以编辑这些地址或将其从 IP 池中删除。

前提条件

- 这些操作需要预定义的**组织管理员**或**系统管理员**角色或包含一组等效权限的角色。
- 确认您的网络是隔离组织虚拟数据中心网络还是路由组织虚拟数据中心网络。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**网络**。

2 单击要编辑的网络的名称。

3 单击 **IP 管理**选项卡。

默认情况下，**静态 IP 池**选项处于选中状态。

4 单击右侧的**编辑**按钮。

- 要修改 IP 范围，请选择范围并进行必要的编辑，然后单击**修改**。
- 要移除 IP 范围，请选择范围，然后单击**移除**。

5 单击**保存**。

编辑组织虚拟数据中心网络的 DNS 设置

您可以编辑组织虚拟数据中心网络的 DNS 设置。

前提条件

- 这些操作需要预定义的**组织管理员**或**系统管理员**角色或包含一组等效权限的角色。
- 确认您的网络是隔离组织虚拟数据中心网络还是路由组织虚拟数据中心网络。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**网络**。

2 单击要编辑的网络的名称。

3 单击 **IP 管理**选项卡。

4 选择 **DNS**，然后单击右侧的**编辑**按钮。

5 根据需要编辑主 DNS、辅助 DNS 和 DNS 后缀信息。

6 单击**保存**。

为隔离组织虚拟数据中心网络配置 DHCP 设置

您可以编辑 NSX Data Center for vSphere 支持的隔离组织 VDC 网络的 DHCP 设置。组织 VDC 网络的 DHCP 服务从其地址池中向已配置为从 DHCP 请求地址的虚拟机网卡提供 IP 地址。该服务在虚拟机打开电源时提供地址。VMware Cloud Director 支持对 IPv4 使用 DHCP 设置。

前提条件

- 这些操作需要预定义的**组织管理员**或**系统管理员**角色或包含一组等效权限的角色。
- 确认您的网络是隔离组织虚拟数据中心网络。
- 确认您的网络由 NSX Data Center for vSphere 提供支持。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**网络**。

2 单击要编辑的网络的名称。

3 单击 **IP 管理**选项卡。

4 选择 **DHCP**。

右侧将显示 DHCP 设置。

5 要启用 DHCP，请单击 **DHCP 池服务**右侧的**编辑**。

6 打开 **DHCP 池服务**，然后单击**保存**。

将从 DHCP 池中提取 DHCP 客户端请求的地址。

7 为该网络创建 DHCP 池。

a 单击**添加**。

b 输入池的 IP 地址范围。

指定的 IP 地址范围不能与组织虚拟数据中心的静态 IP 地址池重叠。

c 指定 DHCP 地址的默认租约时间（以秒为单位）。

默认值为 3,600 秒。

d 指定 DHCP 地址的最大租约时间（以秒为单位）。

这是将 DHCP 分配的 IP 地址租给虚拟机的最长时间。默认值为 7,200 秒。

8 单击**保存**。

将 DHCP 池添加到 NSX-T Data Center 支持的路由组织虚拟数据中心网络

可以将 DHCP 池添加到 NSX-T Data Center 支持的路由组织 VDC 网络。

注 NSX-T Data Center 支持的组织 VDC 网络不支持删除或更新 DHCP 池。

前提条件

- 这些操作需要预定义的**组织管理员**或**系统管理员**角色或包含一组等效权限的角色。
- 确认您的网络是路由组织虚拟数据中心网络。
- 确认您的网络由 NSX-T Data Center 提供支持。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**网络**。

2 单击要编辑的网络的名称。

3 在 **IP 管理**部分中，单击“DHCP”。

4 要添加 DHCP 池，请单击**新建**。

5 输入池的 IPv4 地址范围。

6 单击**保存**。

编辑或删除 NSX Data Center for vSphere 支持的隔离组织虚拟数据中心网络的现有 DHCP 池

如果由 NSX Data Center for vSphere 支持的隔离组织虚拟数据中心网络不再需要 DHCP 池，则可以删除或编辑该池。

前提条件

- 这些操作需要预定义的**组织管理员**或**系统管理员**角色或包含一组等效权限的角色。
- 确认您的网络是隔离组织虚拟数据中心网络。
- 确认组织虚拟数据中心网络由 NSX Data Center for vSphere 提供支持。

步骤

1. 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**网络**。
2. 单击要编辑的网络的名称。
3. 单击 **IP 管理**选项卡。
4. 选择 **DHCP**。

   右侧将显示 DHCP 设置。
5. 编辑或删除现有的 DHCP 池。

选项	操作
编辑 DHCP 池。	1 选择要编辑的 DHCP 池。 2 单击**编辑**按钮。 3 更新池的 IP 地址范围。 4 编辑 DHCP 地址的默认租约时间（以秒为单位）。 5 编辑 DHCP 地址的最大租约时间（以秒为单位）。 6 单击**保存**。
删除 DHCP 池。	1 选择要删除的 DHCP 池。 2 单击**删除**按钮。

重置组织虚拟数据中心网络

如果 DHCP 设置、防火墙设置等与组织虚拟数据中心网络相关联的网络服务未按预期运行，您可以重置网络。

重置组织虚拟数据中心网络时，将强制重新部署网络 DHCP 服务网关。此操作将导致 DHCP 服务临时中断，并且在重置网络时无可用的网络服务。

前提条件

- 此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。
- 网络未连接到任何虚拟机、vApp 或其他网络。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**网络**。

2 选择组织 VDC 网络。

3 单击 **重置**并确认重置操作。

删除组织虚拟数据中心网络

如果您不再需要组织虚拟数据中心网络，则可以删除该网络。

前提条件

- 此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。
- 网络未连接到虚拟机、vApp 或其他网络。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**网络**。

2 单击目标网络名称旁边的单选按钮，然后单击**删除**。

3 单击**确定**以进行确认。

管理跨虚拟数据中心网络

要创建跨多个组织虚拟数据中心的网络，请先将虚拟数据中心分组，然后在数据中心组中创建延伸网络。

跨虚拟数据中心网络需要 NSX Data Center for vSphere。

从版本 10.1 开始，VMware Cloud Director 支持单个网络故障域同时具有活动和备用输出点的数据中心组。

数据中心组可以具有公用输出点配置、每个网络故障域一个输出点配置或者具有本地组配置。

数据中心组

数据中心组作为跨虚拟数据中心路由器，可实现集中式网络连接管理，并可在多个虚拟数据中心中配置多个输出点，同时在该组的所有网络之间提供东西向流量。一个数据中心组可以包含 1 到 16 个虚拟数据中心，这些虚拟数据中心配置为共享多个输出点。数据中心组可以具有以下输出点配置之一：

输出点配置类型	描述
公用输出点配置	您可以为数据中心组配置一个活动输出点和一个备用输出点。这两个输出点通用于数据中心组内所有网络故障域中的所有参与虚拟数据中心。 具有此配置的数据中心组最多可以包括四个网络故障域中的数据中心。
每个故障域的输出点配置	您可以将数据中心组配置为数据中心组中的每个网络故障域具有一个活动输出点和一个备用输出点。 具有此配置的数据中心组最多可以包括四个网络故障域中的数据中心。
本地组配置	本地数据中心组中的组织虚拟数据中心由单个 vCenter Server 实例提供支持。您可以将本地数据中心组配置为单个网络故障域具有一个活动输出点和一个备用输出点。

一个组织可以有多个数据中心组。一个组织虚拟数据中心可以参与多个数据中心组。

参与组织虚拟数据中心可以属于不同的 VMware Cloud Director 站点。请参见配置和管理多站点部署。

网络故障域

网络提供商范围，通常表示具有关联 NSX Manager 的底层 vCenter Server 实例。

输出点

将数据中心组或网络故障域连接到 Internet 的 Edge 网关。Edge 网关必须属于数据中心组内的虚拟数据中心。系统将在表示输出点的 Edge 网关以及虚拟数据中心组或网络故障域的通用路由器上配置 BGP 路由。Edge 网关上的现有路由不受影响。

延伸网络

延伸到数据中心组中所有虚拟数据中心的第 2 层网络。只能是 IPv4。

管理数据中心组

创建数据中心组后，可以编辑数据中心组的网络拓扑。可以在该组中添加和移除虚拟数据中心。可以交换、替换以及移除输出点。可以通过执行不同的同步任务修复配置故障。

无法将公用输出配置转换为每个故障域的输出配置，反之亦然。

由 NSX Data Center for vSphere 提供支持的组织虚拟数据中心支持创建和管理数据中心组。

创建和配置具有通用输出配置的数据中心组

您可以使用通用输出配置创建和配置虚拟数据中心组，您可以在该组中为所有参与虚拟数据中心设置一对 Edge 网关，分别用作活动和备用输出点。

前提条件

- 此操作需要**系统管理员**角色，或者具有发布给组织的 **VDC 组：配置 VDC 组**权限的角色。

- **系统管理员**必须为目标虚拟数据中心启用跨虚拟数据中心网络连接。

步骤

1 创建具有公用输出配置的数据中心组

可以将 1 到 16 个虚拟数据中心分组到一个具有公用输出配置的数据中心组中。

2 添加活动输出点

要将数据中心组连接到 Internet，必须向其网络拓扑添加一个活动输出点。

3 添加备用输出点

在具有通用输出配置的虚拟数据中心组内，可以添加辅助输出点并将其用作容错场景中的备用输出点。

创建具有公用输出配置的数据中心组

可以将 1 到 16 个虚拟数据中心分组到一个具有公用输出配置的数据中心组中。

步骤

1 在顶部导航栏中，单击**数据中心**和**数据中心组**。

此时将以卡视图显示数据中心组列表。

2 单击**新建数据中心组**。

3 输入新数据中心组的名称，并且可以选择输入一个描述。

4 选择**公用输出点**，然后单击**下一步**。

5 在**虚拟数据中心**页面中，为新数据中心组选择最少 1 个最多 16 个数据中心，并单击**下一步**。

数据中心页面将包含**系统管理员**启用以实现跨虚拟数据中心网络的虚拟数据中心列表。

6 查看数据中心组的详细信息，然后单击**完成**。

结果

新创建的虚拟数据中心组将显示在**数据中心组**视图中。

添加活动输出点

要将数据中心组连接到 Internet，必须向其网络拓扑添加一个活动输出点。

前提条件

系统管理员已在加入数据中心组的任何一个虚拟数据中心上都创建了至少一个 Edge 网关。

步骤

1 在顶部导航栏中，单击**数据中心**和**数据中心组**。

此时将以卡视图显示数据中心组列表。

2 在目标数据中心组的卡片中，单击**详细信息**。

此时将打开该数据中心组的**网络拓扑**视图。当前网络拓扑图将显示参与虚拟数据中心及其网络故障域、输出点（如果已配置）和流量路由。

3 单击**添加输出点**。

添加活动输出点页面随即打开，其中提供了属于参与虚拟数据中心的 Edge 网关的列表。

4 选择要用作此数据中心组的活动输出点的 Edge 网关，然后单击**添加**。

结果

系统将在表示输出点的 Edge 网关和虚拟数据中心组的通用路由器上配置 BGP 路由。Edge 网关上的现有路由不受影响。

网络拓扑图将更新，以包含新添加的输出点。从参与虚拟数据中心到 Internet 的流量使用蓝色实线表示。

添加备用输出点

在具有通用输出配置的虚拟数据中心组内，可以添加辅助输出点并将其用作容错场景中的备用输出点。

前提条件

除了用作活动输出点的 Edge 网关之外，您还必须在加入该组的任何虚拟数据中心中至少再配置一个 Edge 网关。

步骤

1 在顶部导航栏中，单击**数据中心**和**数据中心组**。

此时将以卡视图显示数据中心组列表。

2 在目标数据中心组的卡片中，单击**详细信息**。

此时将打开该数据中心组的**网络拓扑**视图。当前网络拓扑图将显示参与虚拟数据中心及其网络故障域、输出点（如果已配置）和流量路由。

3 单击**添加备用输出点**。

此时将打开**添加备用输出点**页面，其中显示了加入该组的虚拟数据中心中未使用的 Edge 网关列表。此虚拟数据中心组内的活动输出点正在使用的 Edge 网关并未显示。

4 选择要用作此数据中心组的备用输出点的 Edge 网关，然后单击**添加**。

结果

系统将在表示输出点的 Edge 网关和网络故障域的通用路由器上配置 BGP 路由。该配置不会影响 Edge 网关上的现有路由。

网络拓扑图将更新，以包含新添加的输出点。在容错场景中，从参与虚拟数据中心到 Internet 的流量使用蓝色虚线表示。

使用故障域输出配置创建和配置数据中心组

您可以使用故障域输出配置创建和配置虚拟数据中心组，从而为组中的每个网络故障域配置用作活动输出点的 Edge 网关。无法在具有故障域输出配置的数据中心组中创建备用输出。

前提条件

此操作需要**系统管理员**角色，或者具有发布给组织的 **VDC 组：配置 VDC 组**权限的角色。

步骤

1 使用故障域输出配置创建数据中心组

您可以使用故障域输出配置将 1 个到 16 个虚拟数据中心分组到一个数据中心组。

2 为故障域添加输出点

要将数据中心组中网络故障域内的虚拟数据中心连接到 Internet，必须向此网络故障域添加一个输出点。可以向数据中心组中的每个网络故障域添加一个输出点。具有故障域输出配置的数据中心组不支持备用输出点。

使用故障域输出配置创建数据中心组

您可以使用故障域输出配置将 1 个到 16 个虚拟数据中心分组到一个数据中心组。

前提条件

系统管理员已为目标虚拟数据中心启用了跨虚拟数据中心网络。

步骤

1 在顶部导航栏中，单击**数据中心**和**数据中心组**。

此时将以卡视图显示数据中心组列表。

2 单击**新建数据中心组**。

3 输入新数据中心组的名称，并且可以选择输入一个描述。

4 选择**每个故障域的输出点**，然后单击**下一步**。

5 在**虚拟数据中心**页面中，为新数据中心组选择最少 1 个最多 16 个数据中心，并单击**下一步**。

数据中心页面将包含**系统管理员**启用以实现跨虚拟数据中心网络的虚拟数据中心列表。

6 查看数据中心组的详细信息，然后单击**完成**。

结果

新创建的虚拟数据中心组将显示在**数据中心组**视图中。

为故障域添加输出点

要将数据中心组中网络故障域内的虚拟数据中心连接到 Internet，必须向此网络故障域添加一个输出点。可以向数据中心组中的每个网络故障域添加一个输出点。具有故障域输出配置的数据中心组不支持备用输出点。

前提条件

除了在此数据中心组中用作输出点的 Edge 网关外，在任何参与虚拟数据中心上都必须至少还有一个未使用的 Edge 网关。

步骤

1 在顶部导航栏中，单击**数据中心**和**数据中心组**。

此时将以卡视图显示数据中心组列表。

2 在目标数据中心组的卡片中，单击**详细信息**。

此时将打开该数据中心组的**网络拓扑**视图。当前网络拓扑图将显示参与虚拟数据中心及其网络故障域、输出点（如果已配置）和流量路由。

3 在网络拓扑图中，单击目标网络故障域。

网络故障域使用实线表示，其名称显示在此图的底部。

选定的故障域标记为蓝色。

4 单击**添加输出点**。

添加活动输出点页面随即打开，其中提供了属于参与虚拟数据中心的 Edge 网关的列表。

5 选择要用作此故障域的输出点的 Edge 网关，然后单击**添加**。

结果

系统将在表示输出点的 Edge 网关和网络故障域的通用路由器上配置 BGP 路由。Edge 网关上的现有路由不受影响。

网络拓扑图将更新，以包含新添加的输出点。从网络故障域中的虚拟数据中心传输到 Internet 的流量使用连续的蓝线表示。

创建并配置本地虚拟数据中心组

从版本 10.1 开始，VMware Cloud Director 支持单个网络故障域同时具有活动和备用输出点的数据中心组。

本地组中的组织虚拟数据中心由单个 vCenter Server 实例提供支持。

在本地数据中心组中，可以设置一对 Edge 网关（一个活动输出点和一个备用输出点），以在同一个网络故障域中支持高可用性和灾难恢复方案。

前提条件

此操作需要**系统管理员**角色，或者具有发布给组织的 **VDC 组：配置 VDC 组**权限的角色。

步骤

1 创建本地数据中心组

您可以使用故障域输出配置将 1 个到 16 个虚拟数据中心 (VDC) 分组到一个数据中心组。

2 为本地数据中心组添加活动输出点

要将本地数据中心组内的数据中心连接到 Internet，必须向网络故障域添加一个活动输出点。

3 为本地数据中心组添加备用输出点

在本地数据中心组配置中，可以添加辅助输出点并将其用作容错场景中的备用输出点。

创建本地数据中心组

您可以使用故障域输出配置将 1 个到 16 个虚拟数据中心 (VDC) 分组到一个数据中心组。

前提条件

系统管理员已为目标虚拟数据中心启用了跨虚拟数据中心网络。

步骤

1 在顶部导航栏中，单击**数据中心**和**数据中心组**。

此时将以卡视图显示数据中心组列表。

2 单击**新建数据中心组**。

3 输入新数据中心组的名称，并且可以选择输入一个描述。

4 要使创建的组仅包含单个网络故障域中的虚拟数据中心，请启用**创建本地组**选项。

5 单击**下一步**。

6 为本地数据中心组的网络故障域选择 VXLAN 网络池。

只有使用所选 VXLAN 网络池的组织 VDC 才能成为本地数据中心组的成员。

7 在**虚拟数据中心**页面中，为新数据中心组选择最少 1 个最多 16 个数据中心，并单击**下一步**。

数据中心页面将包含**系统管理员**启用以实现跨虚拟数据中心网络的虚拟数据中心列表。

8 查看数据中心组的详细信息，然后单击**完成**。

结果

新创建的虚拟数据中心组将显示在**数据中心组**视图中。

为本地数据中心组添加活动输出点

要将本地数据中心组内的数据中心连接到 Internet，必须向网络故障域添加一个活动输出点。

步骤

1 在顶部导航栏中，单击**数据中心**和**数据中心组**。

此时将以卡视图显示数据中心组列表。

2 在目标数据中心组的卡片中，单击**详细信息**。

此时将打开该数据中心组的**网络拓扑**视图。当前网络拓扑图将显示参与虚拟数据中心及其网络故障域、输出点（如果已配置）和流量路由。

3 在**网络拓扑**视图中，单击**添加输出点**。

4 从参与虚拟数据中心内的 Edge 网关列表中，选择一个 Edge 网关作为此数据中心组的活动输出点，然后单击**添加**。

结果

系统将在表示输出点的 Edge 网关和网络故障域的通用路由器上配置 BGP 路由。该配置不会影响 Edge 网关上的现有路由。

新添加的活动输出点将显示在网络拓扑图中。蓝色实线表示从网络故障域中的虚拟数据中心到 Internet 的流量。

后续步骤

要允许输出点容错，请为本地数据中心组添加备用输出点。

为本地数据中心组添加备用输出点

在本地数据中心组配置中，可以添加辅助输出点并将其用作容错场景中的备用输出点。

前提条件

除了用作活动输出点的 Edge 网关之外，您还必须在加入该组的任何虚拟数据中心中至少再配置一个 Edge 网关。

步骤

1 在顶部导航栏中，单击**数据中心**和**数据中心组**。

此时将以卡视图显示数据中心组列表。

2 在目标数据中心组的卡片中，单击**详细信息**。

此时将打开该数据中心组的**网络拓扑**视图。当前网络拓扑图将显示参与虚拟数据中心及其网络故障域、输出点（如果已配置）和流量路由。

3 单击**添加备用输出点**。

此时将打开**添加备用输出点**页面，其中显示了加入该组的虚拟数据中心中未使用的 Edge 网关列表。此虚拟数据中心组内的活动输出点使用的 Edge 网关将灰显。

4 选择要用作此数据中心组的备用输出点的 Edge 网关，然后单击**添加**。

结果

系统将在表示输出点的 Edge 网关和网络故障域的通用路由器上配置 BGP 路由。该配置不会影响 Edge 网关上的现有路由。

新添加的输出点将显示在网络拓扑图中。蓝色虚线表示从参与虚拟数据中心到容错场景中 Internet 的流量。

查看数据中心组

您可以查看所在组织中的数据中心组以及有关其当前配置的详细信息。

前提条件

此操作需要**系统管理员**角色，或者具有发布给组织的 **VDC 组：查看 VDC 组**权限的角色。

步骤

1 在顶部导航栏中，单击**数据中心**和**数据中心组**。

此时将以卡视图显示数据中心组列表。

2 在目标数据中心组的卡片中，单击**详细信息**。

此时将打开该数据中心组的**网络拓扑**视图。当前网络拓扑图将显示参与虚拟数据中心及其网络故障域、输出点（如果已配置）和流量路由。

将虚拟数据中心添加到数据中心组

您可以将虚拟数据中心添加到数据中心组，以便将现有网络延伸到新的虚拟数据中心。

前提条件

- 此操作需要**系统管理员**角色，或者具有发布给组织的 **VDC 组：配置 VDC 组**权限的角色。
- 数据中心组包含的虚拟数据中心不超过四个。

步骤

1 在顶部导航栏中，单击**数据中心**和**数据中心组**。

此时将以卡视图显示数据中心组列表。

2 在目标数据中心组的卡片中，单击**详细信息**。

此时将打开该数据中心组的**网络拓扑**视图。当前网络拓扑图将显示参与虚拟数据中心及其网络故障域、输出点（如果已配置）和流量路由。

3 单击**添加数据中心**。

4 在**数据中心**页面上，选择要添加到数据中心组的数据中心，然后单击**完成**。

数据中心页面包含系统管理员为跨虚拟数据中心网络启用的虚拟数据中心列表。

注 一个数据中心组最多只能包含四个虚拟数据中心。

从数据中心组移除虚拟数据中心

您可以从数据中心组移除虚拟数据中心，这样将不会延伸此虚拟数据中心中的现有网络。

前提条件

- 此操作需要**系统管理员**角色，或者具有发布给组织的 **VDC 组：配置 VDC 组**权限的角色。
- 数据中心组必须至少包含三个虚拟数据中心。
- 您无法删除向数据中心组提供输出点的虚拟数据中心。

步骤

1 在顶部导航栏中，单击**数据中心**和**数据中心组**。

此时将以卡视图显示数据中心组列表。

2 在目标数据中心组的卡片中，单击**详细信息**。

此时将打开该数据中心组的**网络拓扑**视图。当前网络拓扑图将显示参与虚拟数据中心及其网络故障域、输出点（如果已配置）和流量路由。

3 在目标虚拟数据中心对应的卡片的右上角，单击三个圆点，然后单击**移除**。

4 单击**移除**，确认移除。

结果

此虚拟数据中心将从数据中心组的网络拓扑图中移除。

同步数据中心组

要重新应用数据中心组的网络配置并确保所有参与虚拟数据中心都处于活动状态，可以同步该数据中心组。

注 在数据中心组同步过程中，由于通用路由器会在 NSX 中进行同步，因此数据中心组将有几秒钟不可用。

前提条件

此操作需要**系统管理员**角色，或者具有发布给组织的 **VDC 组：配置 VDC 组**权限的角色。

步骤

1 在顶部导航栏中，单击**数据中心**和**数据中心组**。

此时将以卡视图显示数据中心组列表。

2 在目标数据中心组的卡片中，单击**详细信息**。

此时将打开该数据中心组的**网络拓扑**视图。当前网络拓扑图将显示参与虚拟数据中心及其网络故障域、输出点（如果已配置）和流量路由。

3 单击**同步数据中心组**。

4 单击**确定**以进行确认。

交换具有公用输出配置的数据中心组中的输出点

在具有公用输出配置的数据中心组中配置活动和备用输出点后，可以交换这些输出点的角色。活动输出点可以成为备用输出点，备用输出点也可以成为活动输出点。

前提条件

此操作需要**系统管理员**角色，或者具有发布给组织的 **VDC 组：配置 VDC 组**权限的角色。

步骤

1 在顶部导航栏中，单击**数据中心**和**数据中心组**。

此时将以卡视图显示数据中心组列表。

2 在目标数据中心组的卡片中，单击**详细信息**。

此时将打开该数据中心组的**网络拓扑**视图。当前网络拓扑图将显示参与虚拟数据中心及其网络故障域、输出点（如果已配置）和流量路由。

3 单击**交换输出点**。

4 单击**确定**以进行确认。

结果

此时，网络拓扑图将使用新流量路由进行更新。流向 Internet 的流量现在会被重定向到新的活动输出点。

替换输出点的 Edge 网关

您可以替换表示数据中心组中活动或备用输出点的 Edge 网关。

前提条件

- 此操作需要**系统管理员**角色，或者具有发布给组织的 **VDC 组：配置 VDC 组**权限的角色。
- 新 Edge 网关不得由数据中心组中的其他输出点使用。

步骤

1 在顶部导航栏中，单击**数据中心**和**数据中心组**。

此时将以卡视图显示数据中心组列表。

2 在目标数据中心组的卡片中，单击**详细信息**。

此时将打开该数据中心组的**网络拓扑**视图。当前网络拓扑图将显示参与虚拟数据中心及其网络故障域、输出点（如果已配置）和流量路由。

3 如果要替换网络拓扑图上的网络故障域配置中的输出点，请选择目标输出点的网络故障域。

网络故障域使用实线表示，域名显示在图的底部。

选定的网络故障域标记为蓝色。

4 在目标输出点对应卡片的右上角，单击三个圆点，然后单击**替换**。

此时将打开**替换输出点**页面，其中显示了属于参与虚拟数据中心的 Edge 网关列表。

5 选择此新 Edge 网关，然后单击**替换**。

结果

BGP 路由将从旧 Edge 网关中移除，并在表示输出点的新 Edge 网关和虚拟数据中心组的通用路由器上配置。

网络拓扑图将使用新 Edge 网关的名称进行更新。

移除输出点

要将数据中心组或网络故障域与 Internet 断开连接，您可以移除它的输出点。

前提条件

- 此操作需要**系统管理员**角色，或者具有发布给组织的 **VDC 组：配置 VDC 组**权限的角色。
- 如果要移除与备用输出点配对的活动输出点，您必须交换这些输出点或移除该备用输出点。

步骤

1 在顶部导航栏中，单击**数据中心**和**数据中心组**。

此时将以卡视图显示数据中心组列表。

2 在目标数据中心组的卡片中，单击**详细信息**。

此时将打开该数据中心组的**网络拓扑**视图。当前网络拓扑图将显示参与虚拟数据中心及其网络故障域、输出点（如果已配置）和流量路由。

3 如果要从网络拓扑图上的网络故障域配置中移除某个输出点，请选择该目标输出点的网络故障域。

网络故障域使用实线表示，域名显示在图的底部。

选定的网络故障域标记为蓝色。

4 在目标输出点对应卡片的右上角，单击三个圆点，然后单击**删除**。

5 单击**确定**以进行确认。

结果

如果表示输出点的 Edge 网关未由其他通用路由器使用，BGP 路由将从中移除。

此输出点将从网络拓扑图中移除。

同步路由和输出点

通过同步路由，可以将动态路由配置重新应用到数据中心组或网络故障域及其关联的输出点。通过同步某个输出点，可以确保该输出点正确连接到数据中心组。

前提条件

- 此操作需要**系统管理员**角色，或者具有发布给组织的 **VDC 组：配置 VDC 组**权限的角色。
- 您已为目标数据中心组或网络故障域配置了输出点。

步骤

1 在顶部导航栏中，单击**数据中心**和**数据中心组**。

此时将以卡视图显示数据中心组列表。

2 在目标数据中心组的卡片中，单击**详细信息**。

此时将打开该数据中心组的**网络拓扑**视图。当前网络拓扑图将显示参与虚拟数据中心及其网络故障域、输出点（如果已配置）和流量路由。

3 如果要在网络拓扑图上同步数据中心组中的网络故障域，请选择该目标网络故障域。

网络故障域使用实线表示，域名显示在图的底部。

选定的网络故障域标记为蓝色。

4 要将动态路由配置重新应用到组或网络故障域及其关联输出点，请单击**同步路由**，然后单击**确定**。

5 要将输出点与其数据中心组进行同步，请单击目标输出点对应卡片右上角的三个圆点，再依次单击**同步**和击**确定**。

管理延伸网络

创建并配置数据中心组后，您可以创建和管理跨参与虚拟数据中心的第 2 层延伸网络。

在虚拟数据中心级别，延伸网络将显示为跨 VDC 路由类型的组织虚拟数据中心网络。

添加延伸网络

您可以创建跨加入数据中心组的所有虚拟数据中心的延伸网络。

只能添加 IPv4 延伸网络。

前提条件

此操作需要预定义的**组织管理员**角色，或者具有**组织 VDC 网络：编辑属性**权限的角色。

步骤

1 在顶部导航栏中，单击**数据中心**和**数据中心组**。

此时将以卡视图显示数据中心组列表。

2 在目标数据中心组的卡片中，单击**详细信息**。

此时将打开该数据中心组的**网络拓扑**视图。当前网络拓扑图将显示参与虚拟数据中心及其网络故障域、输出点（如果已配置）和流量路由。

3 在左侧面板中，单击**延伸网络**。

此时将以网格视图显示延伸网络列表。

4 单击**添加**。

5 输入新延伸网络的名称和可选描述。

6 输入网络无类别域间路由 (CIDR) 设置，然后单击**创建**。

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

结果

此时将在该数据中心组的延伸网络列表中显示此新创建的网络。

将为每个参与虚拟数据中心创建一个跨 VDC 路由类型的组织虚拟数据中心网络。通过单击参与虚拟数据中心的卡视图，然后单击**网络**，可以查看参与虚拟数据中心的延伸网络。如果虚拟机或 vApp 连接到此类组织虚拟数据中心网络，此虚拟机或 vApp 将连接到延伸网络。

后续步骤

对于每个相应的跨 VDC 组织虚拟数据中心网络，均可以分配静态 IP 地址和 IP 池。请参见将 IP 地址添加到组织虚拟数据中心网络的 IP 池中。

对于连接到延伸网络的虚拟机的 DNS 和 DHCP 配置，可以使用 Cloud Director OpenAPI。要查看 Cloud Director OpenAPI 文档，请访问 `https://Cloud_Director_IP_address_or_host_name/docs`。要查看代码示例和测试 Cloud Director OpenAPI 调用，请访问 `https://Cloud_Director_IP_address_or_host_name/api-explorer?scope=organization_name`。

查看或编辑延伸网络

您可以查看延伸网络的名称、描述和 CIDR 设置。您只能编辑延伸网络的名称和描述。

有关在虚拟数据中心级别编辑延伸网络的静态 IP 池分配的信息，请参见将 IP 地址添加到组织虚拟数据中心网络的 IP 池中。

前提条件

- 查看延伸网络需要预定义的**组织管理员**角色，或者具有**组织 VDC 网络：查看属性**权限的角色。
- 编辑延伸网络需要预定义的**组织管理员**角色，或者具有**组织 VDC 网络：编辑属性**权限的角色。

步骤

1 在顶部导航栏中，单击**数据中心**和**数据中心组**。

此时将以卡视图显示数据中心组列表。

2 在目标数据中心组的卡片中，单击**详细信息**。

此时将打开该数据中心组的**网络拓扑**视图。当前网络拓扑图将显示参与虚拟数据中心及其网络故障域、输出点（如果已配置）和流量路由。

3 在左侧面板中，单击**延伸网络**。

此时将以网格视图显示延伸网络列表。

4 单击目标网络名称旁边的单选按钮，然后单击**编辑**。

5 编辑网络详细信息，然后单击**保存**。

删除延伸网络

您可以移除不再使用的延伸网络。

前提条件

- 此操作需要预定义的**组织管理员**角色，或者具有**组织 VDC 网络：编辑属性**权限的角色。
- 相应的组织虚拟数据中心网络不得连接到任何虚拟机或 vApp。

步骤

1 在顶部导航栏中，单击**数据中心**和**数据中心组**。

此时将以卡视图显示数据中心组列表。

2 在目标数据中心组的卡片中，单击**详细信息**。

此时将打开该数据中心组的**网络拓扑**视图。当前网络拓扑图将显示参与虚拟数据中心及其网络故障域、输出点（如果已配置）和流量路由。

3 在左侧面板中，单击**延伸网络**。

此时将以网格视图显示延伸网络列表。

4 单击目标网络名称旁边的单选按钮，然后单击**删除**。

5 单击**删除**，确认删除。

结果

将从所有参与虚拟数据中心移除相应的组织虚拟数据中心网络。

同步延伸网络

要确保所有参与虚拟数据中心均可访问其延伸网络，可以同步该延伸网络。

前提条件

此操作需要预定义的**组织管理员**角色，或者具有**组织 VDC 网络：编辑属性**权限的角色。

步骤

1 在顶部导航栏中，单击**数据中心**和**数据中心组**。

此时将以卡视图显示数据中心组列表。

2 在目标数据中心组的卡片中，单击**详细信息**。

此时将打开该数据中心组的**网络拓扑**视图。当前网络拓扑图将显示参与虚拟数据中心及其网络故障域、输出点（如果已配置）和流量路由。

3 在左侧面板中，单击**延伸网络**。

此时将以网格视图显示延伸网络列表。

4 单击目标网络名称旁边的单选按钮，然后单击**同步**。

5 单击**确定**以进行确认。

管理 NSX Data Center for vSphere Edge 网关服务

VMware Cloud Director 提供由 NSX Data Center for vSphere 网络虚拟化软件支持的高级网络连接功能，可在云环境中提供增强型安全控制及路由和扩展功能。

使用这些网络功能，您可以在组织虚拟数据中心内实现最高级别的安全和隔离。这些功能提供以下优势：

- 动态路由。VMware Cloud Director 环境中的 NSX Data Center for vSphere 功能支持边界网关协议 (BGP) 和开放式最短路径优先 (OSPF) 等路由协议，用于简化系统之间的网络集成，并在云托管的应用程序部署中提供冗余和连续性。
- 精细的网络安全和隔离。VMware Cloud Director 环境中的 NSX Data Center for vSphere 功能支持使用基于对象的规则定义提供有状态网络流量隔离，而无需多个虚拟网络。此零信任安全模型可防止在入侵者破解应用程序或虚拟机时获得全部网络访问权限。使用相同的网络安全策略可以保护应用程序（无论它们实际位于 VMware Cloud Director 环境中的哪个位置）并扩展您的零信任安全模型以实现可移植安全（无论将应用程序部署在哪里），从而简化网络配置。
- NSX Data Center for vSphere 提供的其他功能包括：点到站点 (IPsec VPN) 和用户 (SSL VPN-Plus) 连接的增强型 VPN 支持、HTTPS 的增强型负载平衡以及扩展的网络可扩展性。

您可以配置两种类型的防火墙：Edge 网关防火墙和分布式防火墙。有关这些防火墙之间差异的详细信息，请参见使用租户门户配置防火墙。

您可以使用 VMware Cloud Director 租户门户或 VMware Cloud Director Service Provider Admin Portal 访问这些高级网络功能。必须先将 Edge 网关转换为高级 Edge 网关。请参见将 Edge 网关转换为高级 Edge 网关。

重要事项 IPv6 Edge 网关支持有限的服务。IPv6 Edge 网关支持 Edge 防火墙、分布式防火墙和静态路由。

VMware Cloud Director 高级网络连接入门

使用 VMware Cloud Director 高级网络连接对 VMware Cloud Director 系统中的组织执行管理任务。您可以管理分布式防火墙和 VMware Cloud Director 系统管理员提供给组织的 VMware NSX® 软件组件提供的其他高级网络连接功能。

高级网络连接的典型用户包括：

- VMware Cloud Director **系统管理员**，此类用户可能会使用租户门户来为组织配置分布式防火墙和其他高级网络连接功能。
- **组织管理员**，此类用户会使用租户门户管理分布式防火墙和**系统管理员**为该组织提供的其他高级网络连接功能。

使用租户门户配置防火墙

使用租户门户，您可以配置 VMware Cloud Director 组织虚拟数据中心中的 NSX 软件提供的防火墙功能。您可以为分布式防火墙创建防火墙规则以便在组织虚拟数据中心中的虚拟机之间提供安全性，也可以

创建应用于 Edge 网关防火墙的防火墙规则，以保护组织虚拟数据中心中的虚拟机不会受到外部网络流量的攻击。

注 在租户门户中，能够配置 Edge 网关防火墙和分布式防火墙。

NSX 逻辑防火墙技术由两个组件组成，可满足不同的部署用例需求。Edge 网关防火墙专注于南北向流量执行，而分布式防火墙专注于东西向访问控制。

Edge 网关防火墙和分布式防火墙之间的主要区别

Edge 网关防火墙监控南北向流量，以提供边界安全保护功能，包括防火墙、网络地址转换 (NAT) 以及点对点 IPSec 和 SSL VPN 功能。

分布式防火墙能够隔离和保护每个虚拟机及应用程序，且隔离和保护深度能达到第 2 层 (L2) 级别。配置分布式防火墙可有效隔离任何外部或内部网络安全危害，从而隔离同一网段上虚拟机之间的东西向流量。安全策略集中管理，可以继承，也可嵌套使用，因此网络和安全管理员可以大规模进行管理。此外，一经部署，定义的安全策略将在虚拟机或应用程序在不同虚拟数据中心之间移动时跟随这些虚拟机或应用程序。

关于防火墙规则

如 NSX 产品文档中所述，在 NSX 中，集中定义的防火墙规则称为预定义规则。您还可以在单个 Edge 网关级别添加规则，这些规则称为本地规则。

在向下移动到防火墙表中的后续规则之前，将根据表中的顶部规则检查每个通信会话。表中第一个匹配流量参数的规则会强制实施。将按照以下顺序显示规则：

1 用户定义的预定义规则具有最高优先级，按照从上到下的顺序强制实施，且在每个虚拟网卡级别优先实施。

2 自动探究的规则（使控制流量能够传输来实现各种 Edge 网关服务的规则）。

3 在 Edge 网关级别定义的本地规则。

4 默认分布式防火墙规则

有关 NSX 软件如何强制实施防火墙规则的详细信息，请参见《NSX 管理》文档中的“更改防火墙规则的顺序”。

Edge 网关防火墙

Edge 网关的防火墙可以帮助您满足关键边界安全保护要求，例如基于 IP/VLAN 构造、多租户虚拟数据中心中的租户到租户隔离、网络地址转换 (NAT)、合作伙伴（外联网）VPN 以及基于用户的 SSL VPN 构建 DMZ。

VMware Cloud Director 环境中的 Edge 网关防火墙功能由 NSX 软件提供。在 NSX 中，该防火墙功能也称为 Edge 防火墙。Edge 网关防火墙监控南北向流量，以提供边界安全保护功能，包括防火墙、网络地址转换 (NAT) 以及点对点 IPSec 和 SSL VPN 功能。

有关 NSX 软件的 Edge 网关防火墙提供的功能的更多详细信息，请参见《NSX 管理》文档。

管理 NSX Data Center for vSphere Edge 网关防火墙

要保护进出 Edge 网关的通信，可以在该 Edge 网关上创建和管理防火墙规则。

有关保护组织虚拟数据中心虚拟机之间的通信的信息，请参见使用租户门户管理分布式防火墙规则。

在分布式防火墙屏幕上创建并在“应用对象”列中指定了高级 Edge 网关的规则不会显示在该高级 Edge 网关的“防火墙”屏幕中。

Edge 网关的 Edge 网关防火墙规则显示在**防火墙**屏幕中，并按以下顺序强制实施：

1. 内部规则，也称为自动检测到的规则。这些内部规则使控制流量能够传输来实现各种 Edge 网关服务。
2. 用户定义的规则。
3. 默认规则。

默认规则设置应用于与任何用户定义的防火墙规则均不匹配的流量。默认规则将显示在“防火墙”屏幕上规则的底部。

在租户门户中，使用 Edge 网关“防火墙规则”屏幕上的**启用**开关禁用或启用 Edge 网关防火墙。

将 Edge 网关转换为高级 Edge 网关

要在租户门户中使用 Edge 网关，您需要将其转换为高级 Edge 网关。将其转换为高级 Edge 网关后，就可以使用租户门户配置由 NSX 软件为这些高级 Edge 网关提供的静态和动态路由功能。

前提条件

您现有一个 Edge 网关。

步骤

1. 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中选择**Edge**。
2. 选择要编辑的 Edge 网关。
3. 单击**转换为高级**。

结果

您的 Edge 网关将转换为高级 Edge 网关。

后续步骤

转换为高级 Edge 网关后，可以通过选择网关并单击**服务**来配置设置。

添加 NSX Data Center for vSphere Edge 网关防火墙规则

您可以使用 Edge 网关的**防火墙**选项卡为该 Edge 网关添加防火墙规则。您可以将多个 NSX Edge 接口和多个 IP 地址组添加为这些防火墙规则的源和目标。

为规则的源或目标指定**内部**表示允许连接到 NSX Edge 网关的端口组上所有子网的流量。如果您选择**内部**作为源，则在 NSX 网关上配置其他内部接口时，该规则将自动更新。

注 为动态路由配置 Edge 网关时，内部接口上的 Edge 网关防火墙规则将不起作用。

步骤

1 打开 Edge 网关服务。

   a 导航到**网络** > **Edge**。

   b 选择要编辑的 Edge 网关，然后单击**服务**。

2 如果**防火墙规则**屏幕尚不可见，请单击**防火墙**选项卡。

3 要将某个规则添加到防火墙规则表中的现有规则下方，请单击现有行，然后单击**创建**按钮。

   新规则行将添加到选定规则下方，并且默认情况下将为其分配任何目标、任何服务以及**允许**操作。如果系统定义的默认规则是防火墙表中的唯一规则，则新规则将添加到默认规则的上方。

4 单击**名称**单元格，然后键入一个名称。

5 单击**源**单元格，然后使用现在可见图标选择要添加到该规则中的源：

选项	描述
单击 IP 图标	键入要使用的源值。有效值为 IP 地址、CIDR、IP 范围或关键字 **any**。Edge 网关防火墙同时支持 IPv4 和 IPv6 格式。
单击 + 图标	使用 **+** 图标可将源指定为特定 IP 地址以外的对象： ■ 使用**选择对象**窗口添加与您的选择匹配的对象，然后单击**保留**将其添加到规则中。 ■ 要从规则中排除某个源，请使用**选择对象**窗口将此源添加到此规则中，然后选择切换排除图标从此规则中排除此源。 在对此源选择切换排除后，此规则将应用于来自您排除的源以外的所有源的流量。如果未选择切换排除，则此规则将应用于来自**选择对象**窗口中指定的源的流量

6 单击**目标**单元格，然后执行以下选项之一：

选项	描述
单击 IP 图标	键入要使用的目标值。有效值为 IP 地址、CIDR、IP 范围或关键字 **any**。Edge 网关防火墙同时支持 IPv4 和 IPv6 格式。
单击 + 图标	使用 **+** 图标可将源指定为特定 IP 地址以外的对象： ■ 使用**选择对象**窗口添加与您的选择匹配的对象，然后单击**保留**将其添加到规则中。 ■ 要从规则中排除某个源，请使用“选择对象”窗口将此源添加到此规则中，然后选择切换排除图标从此规则中排除此源。 在对此源选择切换排除后，此规则将应用于来自您排除的源以外的所有源的流量。如果未选择切换排除，则此规则将应用于来自**选择对象**窗口中指定的源的流量

7 单击新规则的**服务**单元格，然后单击 **+** 图标，将服务指定为端口协议组合：

a 选择服务协议。

b 键入源和目标端口的端口号，或指定 **any**。

c 单击**保留**。

8 在新规则的**操作**单元格中，为此规则配置相应操作。

选项	描述
接受	允许来自或流向指定源、目标和服务的流量。
拒绝	阻止来自或流向指定源、目标和服务的流量。

9 单击**保存更改**。

保存操作可能需要一分钟才能完成。

修改 NSX Data Center for vSphere Edge 网关防火墙规则

您只能编辑和删除已添加到 Edge 网关的用户定义的防火墙规则。除了可以更改默认规则的操作设置之外，您不能编辑或删除自动生成的规则或默认规则的其他内容。您可以更改用户定义的规则的优先级顺序。

有关规则的各种单元格的可用设置的详细信息，请参见添加 NSX Data Center for vSphere Edge 网关防火墙规则。

步骤

1 打开 Edge 网关服务。

a 导航到**网络** > **Edge**。

b 选择要编辑的 Edge 网关，然后单击**服务**。

2 单击**防火墙**选项卡。

3 管理防火墙规则。

- 单击规则的**编号**单元格中的绿色复选标记，禁用该规则。绿色复选标记将变成红色已禁用图标。如果规则已禁用，您想要启用该规则，请单击红色已禁用图标。
- 通过双击规则的**名称**单元格并键入新名称来编辑规则的名称。
- 通过选择相应的单元格并使用显示的控件修改规则的设置，例如源或操作设置。
- 选择一条规则并单击规则表上方的**删除**按钮以删除该规则。
- 使用**仅显示用户定义的规则**开关隐藏系统生成的规则。
- 通过选择相应规则并单击规则表上方的向上和向下箭头按钮，将规则在规则表中上移或下移。

4 单击**保存更改**。

分布式防火墙

通过分布式防火墙，您可以基于虚拟机名称和属性将组织虚拟数据中心实体（例如虚拟机）分段。

VMware Cloud Director 支持在受 NSX Data Center for vSphere 支持的组织虚拟数据中心上使用分布式防火墙服务。如《NSX 管理》文档中所述，此分布式防火墙是一种嵌入内核的虚拟化管理程序防火墙，用于查看和控制虚拟化工作负载和网络。您可以基于像虚拟机名称这样的对象以及像 IP 地址或 IP 集地址这样的网络构造创建访问控制策略。在每个虚拟机的虚拟网卡级别强制实施防火墙规则，以便即使 vSphere vMotion 将虚拟机移至新 ESXi 主机时也能够提供一致的访问控制。此分布式防火墙支持微分段安全模型，从而能够以近线速率处理检查东西向流量。

如《NSX 管理》文档中所述，对于第 2 层 (L2) 数据包，分布式防火墙会创建一个缓存来提升性能。第 3 层 (L3) 数据包按以下顺序进行处理：

1 检查所有数据包的现有状态。

2 如果发现状态匹配，则处理数据包。

3 如果未发现状态匹配，则通过规则处理数据包，直到发现匹配。

- 对于 TCP 数据包，仅为带有 SYN 标记的数据包设置状态。但是，未指定协议的规则（服务于任何项）可以匹配带有任何标记组合的 TCP 数据包。
- 对于 UDP 数据包，从数据包中提取五元组详细信息。如果状态表中不存在状态，将使用已提取的五元组详细信息创建新状态。随后接收的数据包将根据刚刚创建的状态进行匹配。
- 对于 ICMP 数据包，使用 ICMP 类型、代码和数据包方向创建状态。

分布式防火墙也可以帮助您创建基于身份的规则。管理员可以基于在企业 Active Directory (AD) 中定义的用户组成员资格强制实施访问控制。可能使用基于身份的防火墙规则的一些用例有：

- 用户使用笔记本电脑或移动设备访问虚拟应用程序，且这些设备使用 AD 进行用户身份验证
- 用户使用 VDI 基础架构访问虚拟应用程序，且虚拟机基于 Microsoft Windows

有关 NSX 软件的分布式防火墙所提供功能的更多详细信息，请参见《NSX 管理》文档。

使用租户门户在组织虚拟数据中心上启用分布式防火墙

在通过租户门户使用组织虚拟数据中心上的分布式防火墙功能之前，必须为该组织虚拟数据中心启用分布式防火墙。VMware Cloud Director 系统管理员或具有 ORG_VDC_DISTRIBUTED_FIREWALL_ENABLE 权限的用户可以在组织虚拟数据中心上启用分布式防火墙。

您可以使用租户门户中的“分布式防火墙”屏幕为组织虚拟数据中心启用分布式防火墙。

前提条件

VMware Cloud Director 支持在受 NSX Data Center for vSphere 支持的组织虚拟数据中心上使用分布式防火墙服务。

确认已向组织虚拟数据中心所属的组织分配以下权限：

- 组织 vDC 分布式防火墙: 启用/禁用
- 组织 vDC 分布式防火墙: 配置规则
- 组织 vDC 分布式防火墙: 查看规则

VMware Cloud Director 系统管理员向组织分配权限。要使用租户门户的用户界面启用分布式防火墙，需要具有“组织 vDC 分布式防火墙: 启用/禁用”权限。要查看租户门户中的防火墙规则，需要具有“组织 vDC 分布式防火墙: 查看规则”权限；要使用租户门户配置防火墙规则，需要具有“组织 vDC 分布式防火墙: 配置规则”权限。

确认您被分配的角色具有名为“组织 vDC 分布式防火墙: 启用/禁用”的权限。在 VMware Cloud Director 系统的预定义角色中，只有“系统管理员”角色默认具有该权限。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后在**网络**下选择**安全**。

2 选择要为其配置分布式防火墙规则的组织虚拟数据中心。

3 单击**配置服务**。

4 在**分布式防火墙**选项卡上启用分布式防火墙。

后续步骤

有关默认分布式防火墙规则的描述，请参见使用租户门户管理分布式防火墙规则。

使用租户门户管理分布式防火墙规则

如《NSX 管理指南》中所述，默认防火墙设置适用于与用户定义的任何防火墙规则均不匹配的流量。在 VMware Cloud Director Tenant Portal 中，默认分布式防火墙规则标记为默认允许规则。

必须先在组织虚拟数据中心上启用分布式防火墙功能，才能使用 VMware Cloud Director Tenant Portal 管理分布式防火墙设置。

默认分布式防火墙规则配置为允许所有第 3 层和第 2 层流量通过组织虚拟数据中心。用户界面“操作”列中设置的“允许”表明了此设置。默认规则始终位于规则表的底部。

重要事项 您不能删除或修改默认的分布式防火墙规则。

添加分布式防火墙规则

可以首先在组织虚拟数据中心范围内添加分布式防火墙规则。然后，可以缩小要应用规则的范围。分布式防火墙允许您在源级别和目标级别为每个规则添加多个对象，以帮助减少要添加的防火墙规则的总数。

有关可在规则中使用的预定义服务和服务组的信息，请参见查看可用于防火墙规则的服务和查看可用于防火墙规则的服务组。

前提条件

- 使用租户门户在组织虚拟数据中心上启用分布式防火墙
- 如果要使用 IP 集作为规则中的源或目标，请参见创建供防火墙规则和 DHCP 中继配置使用的 IP 集。
- 如果要使用 MAC 集作为规则中的源或目标，请参见创建供防火墙规则使用的 MAC 集。
- 如果要使用安全组作为规则中的源或目标，请参见创建安全组。

步骤

1. 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后在**网络**下选择**安全**。
2. 选择要为其修改防火墙规则的安全服务 VDC 网络，然后单击**配置服务**。

   此时将显示“安全服务”屏幕。
3. 选择要创建的规则类型。您可以选择创建常规规则或以太网规则。

   第 3 层 (L3) 规则将在**常规**选项卡上配置。第 2 层 (L2) 规则将在**以太网**选项卡上配置。
4. 要将某个规则添加到防火墙表中的现有规则下方，请单击现有行，然后单击**创建** () 按钮。

   新规则行将添加到选定规则下方，并且默认情况下将为其分配任何目标、任何服务以及**允许**操作。如果系统定义的“默认允许”规则是防火墙表中的唯一规则，则新规则将添加到默认规则的上方。
5. 单击**名称**单元格，然后键入一个名称。

6 单击**源**单元格，然后使用现在可见图标选择要添加到该规则中的源：

操作	描述
单击 IP 图标	适用于在**常规**选项卡上定义的规则。 键入要使用的源值。有效值为 IP 地址、CIDR、IP 范围或关键字 **any**。分布式防火墙仅支持 IPv4 格式。
单击 + 图标	使用 **+** 图标可将源指定为特定 IP 地址以外的对象： ■ 使用**选择对象**窗口添加与您的选择匹配的对象，然后单击**保留**将其添加到规则中。 ■ 要从规则中排除某个源，请使用**选择对象**窗口将此源添加到此规则中，然后选择切换排除图标从此规则中排除此源。 在对此源选择切换排除后，此规则将应用于来自您排除的源以外的所有源的流量。如果未选择切换排除，则此规则将应用于来自**选择对象**窗口中指定的源的流量

7 单击**目标**单元格，然后执行以下操作之一：

操作	描述
单击 IP 图标	适用于在**常规**选项卡上定义的规则。 键入要使用的目标值。有效值为 IP 地址、CIDR、IP 范围或关键字 **any**。分布式防火墙仅支持 IPv4 格式。
单击 + 图标	使用 **+** 图标可将源指定为特定 IP 地址以外的对象： ■ 使用**选择对象**窗口添加与您的选择匹配的对象，然后单击**保留**将其添加到规则中。 ■ 要从规则中排除某个源，请使用“选择对象”窗口将此源添加到此规则中，然后选择切换排除图标从此规则中排除此源。 在对此源选择切换排除后，此规则将应用于来自您排除的源以外的所有源的流量。如果未选择切换排除，则此规则将应用于来自**选择对象**窗口中指定的源的流量

8 单击此新规则对应的**服务**单元格，然后执行以下操作之一：

操作	描述
单击 IP 图标	将服务指定为端口 - 协议组合： a 选择服务协议。 b 键入源和目标端口的端口号或指定 **any**，然后单击**保留**。
单击 + 图标	选择预定义的服务或服务组，或者定义一个新服务或服务组： a 选择一个或多个对象，然后将其添加到筛选器。 b 单击**保留**。

9 在新规则的**操作**单元格中，为此规则配置相应操作。

选项	描述
允许	允许来自或流向指定源、目标和服务的流量。
拒绝	阻止来自或流向指定源、目标和服务的流量。

10 在新规则的**方向**单元格中，选择此规则是应用于入站流量、出站流量还是同时应用于这两种流量。

11 如果此规则在**常规**选项卡上，则在此新规则的**数据包类型**单元格中选择**任何**、**IPV4** 或 **IPV6** 数据包类型。

12 选择**应用对象**单元格，并使用 **+** 图标定义此规则所适用的对象范围。

如果此规则在**源**和**目标**单元格中均包含虚拟机，则您必须将源和目标虚拟机均添加到此规则**应用对象**中，此规则才能正常起作用。

重要事项 IP 地址组（IP 集）、MAC 地址组（MAC 集）和包含 IP 集或 MAC 集的安全组不是有效的输入参数。

13 单击**保存更改**。

编辑分布式防火墙规则

在 VMware Cloud Director 环境中，要修改组织虚拟数据中心的现有分布式防火墙规则，请使用**分布式防火墙**屏幕。

有关规则的各种单元格的可用设置的详细信息，请参见添加分布式防火墙规则。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后在**网络**下选择**安全**。

2 选择要为其修改防火墙规则的安全服务 VDC 网络，然后单击**配置服务**。

此时将显示“安全服务”屏幕。

3 执行以下任一操作以管理分布式防火墙规则：

- 单击规则的**编号**单元格中的绿色复选标记，禁用该规则。

  绿色复选标记将变成红色已禁用图标。如果规则已禁用，您想要启用该规则，请单击红色已禁用图标。

- 通过双击规则的**名称**单元格并键入新名称来编辑规则的名称。
- 通过选择相应的单元格并使用显示的控件修改规则的设置，例如源或操作设置。
- 选择一个规则并单击规则表上方的**删除** () 按钮以删除该规则。
- 通过选择相应规则并单击规则表上方的向上和向下箭头按钮，将规则在规则表中上移或下移。

4 单击**保存更改**。

管理 NSX Data Center for vSphere Edge 网关 DHCP

您可以配置 Edge 网关，以便为连接到关联组织虚拟数据中心网络的虚拟机提供动态主机配置协议 (DHCP) 服务。

如 NSX 文档所述，NSX Edge 网关功能包括 IP 地址池化、一对一静态 IP 地址分配以及外部 DNS 服务器配置。静态 IP 地址绑定基于请求客户端虚拟机的受管对象 ID 和接口 ID。

适用于 NSX Edge 网关的 DHCP 服务：

- 侦听 Edge 网关内部接口以发现 DHCP。

- 将 Edge 网关内部接口的 IP 地址用作所有客户端的默认网关地址。
- 将内部接口的广播和子网掩码值用于容器网络。

在以下情况下，您需要在具有 DHCP 分配的 IP 地址的客户端虚拟机上重新启动 DHCP 服务：

- 您更改或删除了一个 DHCP 池、默认网关或 DNS 服务器。
- 您更改了 Edge 网关实例的内部 IP 地址。

注 如果启用了 DHCP 的 Edge 网关上的 DNS 设置发生改变，则 Edge 网关可能停止提供 DHCP 服务。如果出现这种情况，请使用“DHCP 池”屏幕上的 **DHCP 服务状态**开关禁用并重新启用该 Edge 网关上的 DHCP。请参见添加 DHCP IP 池。

添加 DHCP IP 池

您可以配置 NSX Data Center for vSphere Edge 网关的 DHCP 服务所需的 IP 池。DHCP 自动向连接到组织虚拟数据中心网络的虚拟机分配 IP 地址。

如《NSX 管理》文档中所述，DHCP 服务需要一个 IP 地址池。IP 池是网络中连续的 IP 地址范围。通过该池将 IP 地址分配给未绑定任何地址的受 Edge 网关保护的虚拟机。IP 池的范围不得互相交叉，因此一个 IP 地址只能属于一个 IP 池。

注 必须至少配置一个 DHCP IP 池才能启用 DHCP 服务状态。

步骤

1 打开 Edge 网关服务。

   a 导航到**网络** > **Edge**。

   b 选择要编辑的 Edge 网关，然后单击**服务**。

2 导航到 **DHCP** > **池**。

3 如果当前未启用 DHCP 服务，请启用 **DHCP 服务状态**。

   注 启用 **DHCP 服务状态**后，至少添加一个 DHCP IP 池再保存更改。如果屏幕上未列出任何 DHCP IP 池时打开 **DHCP 服务状态**选项开关并保存更改，屏幕将显示为关闭该开关。

4 在“DHCP 池”下，单击**创建** () 按钮，指定 DHCP 池的详细信息，然后单击**保留**。

选项	描述
IP 范围	键入 IP 地址范围。
域名	DNS 服务器的域名。
自动配置 DNS	打开该开关可为此 IP 池的 DNS 绑定使用 DNS 服务配置。 如果启用，**主名称服务器**和**辅助名称服务器**将设置为**自动**。
主名称服务器	如果未启用**自动配置 DNS**，请键入主 DNS 服务器的 IP 地址。 将使用此 IP 地址进行主机名到 IP 地址解析。

选项	描述
辅助名称服务器	如果未启用**自动配置 DNS**，请键入辅助 DNS 服务器的 IP 地址。 将使用此 IP 地址进行主机名到 IP 地址解析。
默认网关	键入默认网关地址。 如果未指定默认网关 IP 地址，则会将 Edge 网关实例的内部接口作为默认网关。
子网掩码	键入 Edge 网关接口的子网掩码。
租约从不过期	启用该开关将使从此池分配的 IP 地址永远绑定到其已分配的虚拟机。 选择此选项时，**租约时间**将设置为无限。
租约时间 (秒)	将 DHCP 分配的 IP 地址租给客户端的时间长度（以秒为单位）。 默认租约时间为一天（86400 秒）。 注 选择**租约从不过期**时，您无法指定租约时间。

5 单击**保存更改**。

结果

VMware Cloud Director 将更新 Edge 网关，以提供 DHCP 服务。

添加 DHCP 绑定

如果您有服务在虚拟机上运行，并且不希望更改 IP 地址，可以将虚拟机 MAC 地址绑定到该 IP 地址。绑定的 IP 地址不得与 DHCP IP 池重叠。

前提条件

您具有要为其设置绑定的虚拟机的 MAC 地址。

步骤

1 打开 Edge 网关服务。

a 导航到**网络** > **Edge**。

b 选择要编辑的 Edge 网关，然后单击**服务**。

2 在 **DHCP** > **绑定**选项卡上，单击**创建** (+) 按钮，指定绑定详细信息，然后单击**保留**。

选项	描述
MAC 地址	键入要绑定到 IP 地址的虚拟机的 MAC 地址。
主机名称	键入虚拟机请求 DHCP 租约时要为该虚拟机设置的主机名称。
IP 地址	键入要绑定到 MAC 地址的 IP 地址。
子网掩码	键入 Edge 网关接口的子网掩码。
域名	键入 DNS 服务器的域名。
自动配置 DNS	启用该开关可为此 DNS 绑定使用 DNS 服务配置。 如果启用，**主名称服务器**和**辅助名称服务器**将设置为**自动**。

选项	描述
主名称服务器	如果您未选择**自动配置 DNS**，请键入主 DNS 服务器的 IP 地址。 将使用此 IP 地址进行主机名到 IP 地址解析。
辅助名称服务器	如果您未选择**自动配置 DNS**，请键入辅助 DNS 服务器的 IP 地址。 将使用此 IP 地址进行主机名到 IP 地址解析。
默认网关	键入默认网关地址。 如果未指定默认网关 IP 地址，则会将 Edge 网关实例的内部接口作为默认网关。
租约从不过期	启用该开关可使 IP 地址永远绑定到该 MAC 地址。 选择此选项时，**租约时间**将设置为无限。
租约时间 (秒)	将 DHCP 分配的 IP 地址租给客户端的时间长度（以秒为单位）。 默认租约时间为一天（86400 秒）。 注 选择**租约从不过期**时，您无法指定租约时间。

3 单击**保存更改**。

为 NSX Data Center for vSphere Edge 网关配置 DHCP 中继

通过 VMware Cloud Director 环境中 NSX 所提供的 DHCP 中继功能，可以利用 VMware Cloud Director 环境中现有的 DHCP 基础架构，而不会中断现有 DHCP 基础架构中的 IP 地址管理。DHCP 消息从虚拟机中继到物理 DHCP 基础架构中的指定 DHCP 服务器，这使得由 NSX 软件控制的 IP 地址可以继续与受 DHCP 控制的其余环境中的 IP 地址同步。

Edge 网关的 DHCP 中继配置可以列出多个 DHCP 服务器。请求会发送到列出的所有服务器。中继来自虚拟机的 DHCP 请求时，Edge 网关会将网关 IP 地址添加到该请求。外部 DHCP 服务器使用此网关地址来匹配池以及为该请求分配 IP 地址。网关地址必须属于 Edge 网关接口的子网。

您可以为每个 Edge 网关指定不同的 DHCP 服务器，并可以在每个 Edge 网关上配置多个 DHCP 服务器，从而为多个 IP 域提供支持。

注

- DHCP 中继不支持重叠的 IP 地址空间。
- DHCP 中继和 DHCP 服务不能同时运行于同一个虚拟网卡上。如果在虚拟网卡上配置了中继代理，则不能在该虚拟网卡的子网上配置 DHCP 池。有关详细信息，请参见《NSX 管理指南》。

为 NSX Data Center for vSphere Edge 网关指定 DHCP 中继配置

VMware Cloud Director 环境中的 NSX 软件让 Edge 网关能够将 DHCP 消息中继到 VMware Cloud Director 组织虚拟数据中心外部的 DHCP 服务器。您可以配置 Edge 网关的 DHCP 中继功能。

如《NSX 管理》文档中所述，可以使用现有 IP 集、IP 地址块、域或所有这些项的组合来指定 DHCP 服务器。DHCP 消息将中继到指定的每个 DHCP 服务器。

您还必须至少配置一个 DHCP 中继代理。DHCP 中继代理是 Edge 网关上的一个接口，从这里将 DHCP 请求中继到外部 DHCP 服务器。

前提条件

如果您要使用 IP 集指定 DHCP 服务器，请确认该 IP 集作为 Edge 网关可用的分组对象存在。请参见创建供防火墙规则和 DHCP 中继配置使用的 IP 集。

步骤

1 打开 Edge 网关服务。

a 导航到**网络** > **Edge**。

b 选择要编辑的 Edge 网关，然后单击**服务**。

2 导航到 **DHCP** > **中继**。

3 使用屏幕上的字段，通过 IP 地址、域名或 IP 集指定 DHCP 服务器。

您可以使用**添加** () 按钮浏览可用的 IP 集，然后从现有 IP 集中选择。

4 配置 DHCP 中继代理，然后将其配置添加到屏幕上的表中：单击**添加** () 按钮，选择虚拟网卡及其网关 IP 地址，然后单击**保留**。

默认情况下，网关 IP 地址与选定虚拟网卡的主地址相匹配。您可以保留默认地址或选择备用地址（如果该虚拟网卡上有一个可用）。

5 单击**保存更改**。

使用租户门户管理网络地址转换

VMware Cloud Director 环境中的 NSX 软件支持 Edge 网关提供网络地址转换 (NAT) 服务。使用该功能可减少组织必须使用的公用 IP 地址数，从而实现经济性并确保安全。

Edge 网关的 NAT 服务能够将公用地址分配给专用网络中的虚拟机或虚拟机组。要让 Edge 网关能够访问组织虚拟数据中心中专门寻址的虚拟机上运行的服务，您必须在 Edge 网关上配置 NAT 规则。在最常见的情况下，您将 NAT 服务与 VMware Cloud Director 环境中 Edge 网关上的上行链路接口相关联，以便不在外部网络上公开组织虚拟数据中心网络上的地址。

NAT 服务配置分为源 NAT (SNAT) 和目标 NAT (DNAT) 规则。在 VMware Cloud Director 环境中的 Edge 网关上配置 SNAT 或 DNAT 规则时，请始终从您组织虚拟数据中心的角度来配置此规则。具体来说，这意味着按照下列方式配置规则：

- SNAT：流量通过 Internet 从组织虚拟数据中心内部网络上的虚拟机（源）传输到外部网络（目标）。SNAT 规则用于转换从组织虚拟数据中心网络发送到外部网络或其他组织虚拟数据中心网络的出站数据包的源 IP 地址。
- DNAT：流量从 Internet（源）传输到您的组织虚拟数据中心内的虚拟机（目标）。DNAT 规则用于转换某个组织虚拟数据中心网络中从外部网络或其他组织虚拟数据中心网络收到的数据包的 IP 地址，也可以选择转换其端口。

您可以配置 NAT 规则以在组织虚拟数据中心内部创建专用 IP 地址空间。此配置能够将专用 IP 地址空间从一个组织虚拟数据中心移植到另一个组织虚拟数据中心。配置 NAT 规则后，可以对位于一个组织虚拟数据中心中而在另一个组织虚拟数据中心中使用的虚拟机使用相同的专用 IP 地址。

VMware Cloud Director 环境中的 NAT 规则功能支持：

- 在专用 IP 地址空间内创建子网
- 为一个 Edge 网关创建多个专用 IP 地址空间
- 在多个 Edge 网关接口上配置多个 NAT 规则

重要事项 您必须在 Edge 网关上同时配置防火墙和 NAT 规则，才能访问 Edge 网关网络上的虚拟机。默认情况下，Edge 网关部署时配置了防火墙规则，可拒绝出入 Edge 网关网络上虚拟机的所有网络流量。此外，默认情况下在 Edge 网关上禁用 NAT，以便 Edge 网关无法转换入站和出站流量的 IP 地址，除非在 Edge 网关上配置 NAT。而且，如果不添加防火墙规则以允许相应的流量，那么配置 NAT 规则后尝试对网络上的虚拟机执行 ping 操作会失败。

添加 SNAT 或 DNAT 规则

您可以创建源 NAT (SNAT) 规则，以便将源 IP 地址从公用 IP 地址更改为专用 IP 地址，或者相反。您可以创建目标 NAT (DNAT) 规则，以便将目标 IP 地址从公用 IP 地址更改为专用 IP 地址，或者相反。

在创建 NAT 规则时，您可以使用以下格式指定原始和转换后的 IP 地址：

- IP 地址：例如，192.0.2.0
- IP 地址范围：例如，192.0.2.0-192.0.2.24
- IP 地址/子网掩码：例如，192.0.2.0/24
- `any`

在 VMware Cloud Director 环境中的 Edge 网关上配置 SNAT 或 DNAT 规则时，请始终从您组织虚拟数据中心的角度来配置此规则。SNAT 规则用于转换从一个组织虚拟数据中心网络发送到外部网络或其他组织虚拟数据中心网络的数据包的源 IP 地址。DNAT 规则用于转换某个组织虚拟数据中心网络中从外部网络或其他组织虚拟数据中心网络收到的数据包的 IP 地址，也可以选择转换其端口。

前提条件

必须已将此公用 IP 地址添加到要添加规则的 NSX Data Center for vSphere Edge 网关接口。对于 DNAT 规则，必须已将原始（公用）IP 地址添加到 Edge 网关接口，对于 SNAT 规则，必须已将转换后的（公用）IP 地址添加到该接口。

步骤

1 打开 Edge 网关服务。

   a 导航到**网络** > **Edge**。

   b 选择要编辑的 Edge 网关，然后单击**服务**。

2 单击 **NAT** 以查看“NAT 规则”屏幕。

3 根据要创建的 NAT 规则类型，单击 **DNAT 规则**或 **SNAT 规则**。

4 配置目标 NAT 规则（入站）。

选项	描述
应用于	选择要应用规则的接口。
原始 IP/范围	键入所需的 IP 地址，或从列表中选择分配的 IP 地址。 此地址必须为您要为其配置 DNAT 规则的 Edge 网关的公用 IP 地址。在所检查的数据包中，此 IP 地址或范围将显示为此数据包的目标 IP 地址。这些数据包目标地址即为通过此 DNAT 规则转换的地址。
协议	选择要应用此规则的协议。要对所有协议应用此规则，请选择**任何**。
原始端口	（可选）选择入站流量为连接到连接虚拟机的内部网络而在 Edge 网关上使用的端口或端口范围。如果**协议**设置为 **ICMP** 或**任何**，则此选项不可用。
ICMP 类型	如果您对**协议**选择 **ICMP**（一种在设备之间传达错误信息的错误报告和诊断实用程序），请从下拉菜单中选择 **ICMP 类型**。 ICMP 消息可通过类型字段来识别。默认情况下，ICMP 类型设置为“任何”。
转换的 IP/范围	键入要将入站数据包上的目标地址转换到的 IP 地址或 IP 地址范围。 这些地址即为您要为其配置 DNAT 以使其可从外部网络接收流量的一个或多个虚拟机的 IP 地址。
转换的端口	（可选）选择入站流量要通过内部网络上的虚拟机连接到的端口或端口范围。这些端口即为 DNAT 规则要为虚拟机入站数据包转换到的端口。
源 IP 地址	如果您希望将规则仅应用于来自特定域的流量，请输入此域的 IP 地址或 CIDR 格式的 IP 地址范围。如果将此文本框留空，则 DNAT 规则将应用于本地子网中的所有 IP 地址。
源端口	（可选）输入源的端口号。
描述	（可选）为 DNAT 规则输入有意义的描述。
已启用	启用此选项可启用此规则。
启用日志记录	启用此选项可记录此规则执行的地址转换操作。

5 配置源 NAT 规则（出站）。

选项	描述
应用于	选择要应用规则的接口。
原始源 IP/范围	键入要应用于此规则的原始 IP 地址或 IP 地址范围，或从列表中选择分配的 IP 地址。 这些地址即为您要为其配置 SNAT 规则以使其可以向外部网络发送流量的一个或多个虚拟机的 IP 地址。
转换的源 IP/范围	键入所需 IP 地址。 此地址始终为您要为其配置 SNAT 规则的网关的公用 IP 地址。指定出站数据包上的源地址（虚拟机）在向外部网络发送流量时要转换到 IP 地址。
目标 IP 地址	（可选）如果您希望将规则仅应用到流向特定域的流量，请输入此域的 IP 地址或 CIDR 格式的 IP 地址范围。如果将此文本框留空，则 SNAT 规则将应用于本地子网外的所有目标。
目标端口	（可选）输入目标的端口号。
描述	（可选）为 SNAT 规则输入有意义的描述。

选项	描述
已启用	启用此选项可启用此规则。
启用日志记录	启用此选项可记录此规则执行的地址转换操作。

6 单击**保留**以将此规则添加到屏幕上的表中。

7 重复这些步骤以配置其他规则。

8 单击**保存更改**将规则保存到系统。

后续步骤

为您刚刚配置的 SNAT 或 DNAT 规则添加相应的 Edge 网关防火墙规则。请参见添加 NSX Data Center for vSphere Edge 网关防火墙规则。

高级路由配置

您可以为 NSX Data Center for vSphere Edge 网关配置 NSX 软件提供的静态和动态路由功能。

要启用动态路由，请使用边界网关协议 (BGP) 或开放式最短路径优先 (OSPF) 协议配置高级 Edge 网关。

有关 NSX 提供的路由功能的详细信息，请参见《NSX 管理》文档中的“路由”。

您可以为每个高级 Edge 网关指定静态和动态路由。动态路由功能提供了第 2 层广播域之间所必需的转发信息，从而减少了第 2 层广播域并提高了网络效率和规模。NSX 将此智能扩展到东西向路由的工作负载位置。利用此功能后，虚拟机到虚拟机之间的通信更加直接，而不会增加扩展跃点所需的成本或时间。

为 NSX Data Center for vSphere Edge 网关指定默认路由配置

可以为 Edge 网关指定静态路由和动态路由的默认设置。

注 要移除所有已配置的路由设置，请使用**路由配置**屏幕底部的**清除全局配置**。此操作将删除子屏幕上当前指定的所有路由设置：默认路由设置、静态路由、OSPF、BGP 和路由重新分发。

步骤

1 打开 Edge 网关服务。

a 导航到**网络** > **Edge**。

b 选择要编辑的 Edge 网关，然后单击**服务**。

2 导航到**路由** > **路由配置**。

3 要为此 Edge 网关启用等价多路径 (Equal Cost Multipath, ECMP)，请打开 **ECMP** 开关。

如《NSX 管理》文档中所述，ECMP 是一种路由策略，该策略允许通过多条最佳路径将下一跳数据包转发到单个目标。NSX 以静态方式、使用配置的静态路由或者通过 OSPF 或 BGP 之类的动态路由协议进行度量计算来确定这些最佳路径。可通过在“静态路由”屏幕上指定多个下一跳来为静态路由指定多个路径。

有关 ECMP 和 NSX 的更多详细信息，请参见《NSX 故障排除指南》中的路由主题。

4 指定默认路由网关的设置。

a 使用**应用于**下拉列表选择一个接口，通过该接口可以到达朝向目标网络的下一跳。

要查看有关所选接口的详细信息，请单击蓝色信息图标。

b 键入网关 IP 地址。

c 键入 MTU。

d （可选） 键入可选描述。

e 单击**保存更改**。

5 指定默认动态路由设置。

注 如果已在环境中配置了 IPsec VPN，则不应使用动态路由。

a 选择路由器 ID。

您可以在列表中选择一个路由器 ID，也可以使用 **+** 图标输入一个新 ID。此路由器 ID 是将路由推送到内核以实现动态路由的 Edge 网关的第一个上行链路 IP 地址。

b 打开**启用日志记录**开关并选择日志级别，以此来配置日志记录。

c 单击**确定**。

6 单击**保存更改**。

后续步骤

添加静态路由。请参见添加静态路由。

配置路由重新分发。请参见配置路由重新分发。

配置动态路由。请参见以下主题：

- 配置 BGP
- 配置 OSPF

添加静态路由

您可以为目标子网或主机添加静态路由。

如果在默认路由配置中已启用 ECMP，您可以在静态路由中指定多个下一跳。有关如何启用 ECMP 的步骤，请参见为 NSX Data Center for vSphere Edge 网关指定默认路由配置。

前提条件

正如 NSX 文档中所述，静态路由的下一跳 IP 地址必须存在于与 NSX Data Center for vSphere Edge 网关的一个接口关联的子网中。否则，该静态路由的配置将失败。

步骤

1 打开 Edge 网关服务。

a 导航到**网络** > **Edge**。

b 选择要编辑的 Edge 网关，然后单击**服务**。

2 导航到**路由** > **静态路由**。

3 单击**创建** () 按钮。

4 为静态路由配置以下选项：

选项	描述
网络	采用 CIDR 表示法键入网络。
下一跳	键入下一跳的 IP 地址。 下一跳 IP 地址必须存在于与 Edge 网关的一个接口关联的子网中。 如果已启用 ECMP，您可以键入多个下一跳。
MTU	编辑数据包的最大传输值。 该 MTU 值不能高于选定 Edge 网关接口上设置的 MTU 值。默认情况下，您可以在“路由配置”屏幕上查看 Edge 网关接口上设置的 MTU。
接口	（可选）选择要添加静态路由的 Edge 网关接口。默认情况下，会选择匹配下一跳地址的接口。
描述	（可选）键入静态路由的描述。

5 单击**保存更改**。

后续步骤

配置静态路由的 NAT 规则。请参见添加 SNAT 或 DNAT 规则。

添加防火墙规则以允许流量遍历静态路由。请参见添加 NSX Data Center for vSphere Edge 网关防火墙规则。

配置 OSPF

可以为 NSX Data Center for vSphere Edge 网关的动态路由功能配置开放式最短路径优先 (OSPF) 路由协议。在 VMware Cloud Director 环境中，OSPF 在 Edge 网关上的常见应用是在 VMware Cloud Director 中的 Edge 网关之间交换路由信息。

NSX Edge 网关支持 OSPF，它是仅在单个路由域中路由 IP 数据包的内部网关协议。如《NSX 管理》文档中所述，在 NSX Edge 网关上配置 OSPF 可以使 Edge 网关知悉和通告路由。Edge 网关使用 OSPF 从可用 Edge 网关收集链路状态信息，并构建网络的拓扑图。该拓扑确定呈现给 Internet 层的路由表，它根据在 IP 数据包中找到的目标 IP 地址制定路由决策。

因此，OSPF 路由策略在等成本路由之间提供动态的流量负载平衡过程。一个 OSPF 网络被划分为多个路由区域，以优化流量并限制路由表的大小。一个区域是具有相同区域标识的 OSPF 网络、路由器和链路的逻辑集合。区域由区域 ID 进行标识。

前提条件

必须配置路由器 ID。为 NSX Data Center for vSphere Edge 网关指定默认路由配置。

步骤

1 打开 Edge 网关服务。

a 导航到**网络** > **Edge**。

b 选择要编辑的 Edge 网关，然后单击**服务**。

2 导航到**路由** > **OSPF**。

3 如果当前未启用 OSPF，请使用 **OSPF 已启用**开关启用它。

4 根据您组织的需求配置 OSPF 设置。

选项	描述
启用正常重新启动	指定在重新启动 OSPF 服务时数据包转发保持不中断。
启用默认源	允许 Edge 网关将自己作为默认网关播发到其 OSPF 对等方。

5 （可选） 可以单击**保存更改**，也可以继续配置区域定义和接口映射。

6 单击**添加** (+) 按钮，在对话框中指定映射的详细信息，然后单击**保留**，以添加 OSPF 区域定义。

注 默认情况下，系统会配置区域 ID 为 51 的次末节区域 (NSSA)，此区域会自动显示在 OSPF 屏幕上的区域定义表中。可以修改或删除 NSSA 区域。

选项	描述
区域 ID	采用 IP 地址或十进制数字的形式键入区域 ID。
区域类型	选择**正常**或 **NSSA**。 NSSA 可防止 AS 外部链接状态通告 (LSA) 涌入 NSSA。它们依赖于到外部目标的默认路由。因此，必须将 NSSA 放在 OSPF 路由域的边缘。NSSA 可以将外部路由导入到 OSPF 路由域中，从而为不属于 OSPF 路由域的小型路由域提供传送服务。
区域身份验证	选择让 OSPF 在区域级别执行的身份验证类型。 区域内的所有 Edge 网关必须配置有相同的身份验证和相应的密码。要使 MD5 身份验证正常工作，接收方和发送方必须具有相同的 MD5 密钥。 选项包括： ■ **无** 无需进行身份验证。 ■ **密码** 如果使用此选项，则在**区域身份验证值**字段中指定的密码将包含在传输的数据包中。 ■ **MD5** 如果使用此选项，身份验证将使用 MD5（消息摘要类型 5）加密。MD5 校验和将包含在传输的数据包中。在**区域身份验证值**字段中键入 MD5 密钥。

7 单击**保存更改**，以便在添加接口映射时可以选择新配置的区域定义。

8 单击**添加** () 按钮，在对话框中指定映射的详细信息，然后单击**保留**，以添加接口映射。

这些映射用于将 Edge 网关的接口映射到区域。

a 在对话框中，选择您要映射到区域定义的接口。

该接口指定这两个 Edge 网关连接到的外部网络。

b 选择要映射到选定接口的区域的区域 ID。

c （可选） 将 OSPF 设置从默认值更改为其他值，以便针对此接口映射自定义它们。

当配置新映射时，将显示这些设置的默认值。在大多数情况下，建议保留默认设置。如果更改这些设置，请确保 OSPF 对等方使用相同的设置。

选项	描述
呼叫间隔	在接口上发送的呼叫数据包之间的间隔（以秒为单位）。
失效间隔	在声明邻居关闭之前必须从该邻居接收至少一个呼叫数据包的间隔（以秒为单位）。
优先级	接口的优先级。优先级最高的接口是指定的 Edge 网关路由器。
成本	在该接口上发送数据包所需的开销。接口的成本与该接口的带宽成反比。带宽越大，成本越低。

d 单击**保留**。

9 在 OSPF 屏幕中单击**保存更改**。

后续步骤

在要与其交换路由信息的其他 Edge 网关上配置 OSPF。

添加一个防火墙规则，以允许启用 OSPF 的 Edge 网关之间的流量。请参见添加 NSX Data Center for vSphere Edge 网关防火墙规则。

确保路由重新分发和防火墙配置允许播发正确的路由。请参见配置路由重新分发。

配置 BGP

可以为 NSX Data Center for vSphere Edge 网关的动态路由功能配置边界网关协议 (BGP)。

如《NSX 管理指南》所述，BGP 使用 IP 网络或前缀表（指定多个自主系统之间的网络可访问性）做出核心路由决策。在网络连接字段中，术语 BGP 发言方指的是运行 BGP 的网络连接设备。两个 BGP 发言方建立连接，然后再交换任何路由信息。术语 BGP 邻居指的是已经建立此类连接的 BGP 发言方。建立连接后，设备交换路由并同步其表。每台设备发送保持活动消息，确保此关系保持活动状态。

步骤

1 打开 Edge 网关服务。

a 导航到**网络** > **Edge**。

b 选择要编辑的 Edge 网关，然后单击**服务**。

2 导航到**路由** > **BGP**。

3 如果当前未启用 BGP，请使用**启用 BGP** 开关进行启用。

4 根据您组织的需求配置 BGP 设置。

选项	描述
启用正常重新启动	指定重新启动 BGP 服务时数据包转发保持不中断。
启用默认源	允许 Edge 网关将自己作为默认网关播发到其 BGP 邻居。
本地 AS	必需。指定要用于协议本地 AS 功能的自主系统 (AS) ID 编号。指定的值必须是介于 1 和 65534 之间的全局唯一数字。 本地 AS 是 BGP 的功能。系统将本地 AS 编号分配到您配置的 Edge 网关。Edge 网关在与其他自主系统中的 BGP 邻居建立对等关系时播发此 ID。选择通往目标的最佳路径时，路由将遍历的自主系统路径将用作动态路由算法中的一个衡量指标。

5 可以单击**保存更改**，也可以继续配置 BGP 路由邻居的设置。

6 单击**添加** () 按钮，在对话框中指定邻居的详细信息，然后单击**保留**，以添加 BGP 邻居配置。

选项	描述
IP 地址	键入此 Edge 网关的 BGP 邻居的 IP 地址。
远程 AS	键入此 BGP 邻居所属自主系统介于 1-65534 的全局唯一编号。此远程 AS 编号用于系统 BGP 邻居表中的 BGP 邻居条目中。
权重	邻居连接的默认权重。根据组织需求进行适当调整。
保持活动状态时间	软件将保持活动消息发送到其对等方的频率。默认频率为 60 秒。根据您组织的需求进行相应调整。
保持关闭时间	软件在未收到保持活动消息后到声明对等方失效的间隔。此间隔必须是保持活动间隔的三倍。默认间隔为 180 秒。根据您组织的需求进行相应调整。 在两个 BGP 邻居之间建立对等关系后，Edge 网关将启动保持关闭定时器。它从邻居接收的每个保持活动消息都会将保持关闭定时器重置为 0。如果 Edge 网关连续三次未收到保持活动消息，保持关闭定时器将达到保持活动间隔的三倍，此时 Edge 网关会认为邻居已关闭并从此邻居删除路由。

选项	描述
密码	如果此 BGP 邻居需要身份验证，请键入身份验证密码。 在邻居间连接上发送的每一段都会被验证。必须在两个 BGP 邻居上使用相同的密码配置 MD5 身份验证，否则，将不会建立连接。
BGP 筛选器	使用此表，通过此 BGP 邻居中的前缀列表指定路由筛选。 小心 在筛选器的末尾强制执行“全部阻止”规则。 通过单击 + 图标并配置选项，将筛选器添加到表中。单击**保留**，保存每个筛选器。 ■ 选择方向以指示是筛选发送到邻居还是发自邻居的流量。 ■ 选择操作以指示允许或拒绝流量。 ■ 键入要筛选发送到或发自邻居的网络。键入 ANY 或以 CIDR 格式键入网络。 ■ 键入 **IP 前缀 GE** 和 **IP 前缀 LE**，在 IP 前缀列表中使用 le 和 ge 关键字。

7 单击**保存更改**将配置保存到系统。

后续步骤

在要交换路由信息的其他 Edge 网关上配置 BGP。

添加一个防火墙规则，以便允许发送到和发自 BGP 配置的 Edge 网关的流量。请参见添加 NSX Data Center for vSphere Edge 网关防火墙规则了解相关信息。

配置路由重新分发

默认情况下，路由器仅与运行相同协议的其他路由器共享路由。配置多协议环境后，必须配置路由重新分发才能实现跨协议路由共享。可以为 NSX Data Center for vSphere Edge 网关配置路由重新分发。

步骤

1 打开 Edge 网关服务。

a 导航到**网络** > **Edge**。

b 选择要编辑的 Edge 网关，然后单击**服务**。

2 导航到**路由** > **路由重新分发**。

3 使用协议开关打开您要为其启用路由重新分发的那些协议。

4 将 IP 前缀添加到屏幕上的表中。

a 单击**添加** () 按钮。

b 以 CIDR 格式键入网络的名称和 IP 地址。

c 单击**保留**。

5 单击**添加** () 按钮，在对话框中指定条件，然后单击**保留**，以指定每个 IP 前缀的重新分发条件。

表中的条目将按顺序进行处理。使用向上和向下箭头可调整顺序。

选项	描述
前缀名称	选择要将此条件应用到的特定 IP 前缀，或者选择**任何**以将此条件应用到所有网络路由。
学习者协议	选择根据此重新分发条件从其他协议获知路由的协议。
允许通过以下方式学习	选择可以从中为**学习者协议**列表中选定的协议获知路由的网络类型。
操作	选择是允许还是拒绝从所选类型的网络重新分发。

6 单击**保存更改**。

负载平衡

负载平衡器采用负载分配对用户透明的方式，在多个服务器中分发入站服务请求。负载平衡可以帮助实现最优的资源利用率、最大吞吐量、最短响应时间，并可以避免出现超载的情况。

负载平衡

负载平衡器采用负载分配对用户透明的方式，在多个服务器中分发入站服务请求。负载平衡可以帮助实现最优的资源使用、最大吞吐量、最短响应时间，并可以避免出现超载的情况。

NSX 负载平衡器支持两个负载平衡引擎。第 4 层负载平衡器基于数据包，提供快速路径处理。第 7 层负载平衡器基于套接字，支持高级流量管理策略和对后端服务的 DDOS 缓解。

在外部接口上配置 NSX Data Center for vSphere Edge 网关的负载平衡，因为 Edge 网关对来自外部网络的入站流量进行负载平衡。在为虚拟服务器配置负载平衡时，请指定您在组织 VDC 中具有的一个可用 IP 地址。

负载平衡策略和概念

在 TCP 和 UDP 层实施基于数据包的负载平衡策略。基于数据包的负载平衡不会停止连接或缓冲整个请求，而是在处理数据包后将其直接发送到选定的服务器。TCP 和 UDP 会话会在负载平衡器中进行维护，以便将单个会话的数据包传送到同一服务器。您可以在全局配置和相关虚拟服务器配置中选择“已启用加速”，以启用基于数据包的负载平衡。

在套接字接口上实施基于套接字的负载平衡策略。会为单个请求建立两个连接 - 面向客户端的连接和面向服务器的连接。选择服务器后建立面向服务器的连接。对于基于 HTTP 套接字的实施，会在通过可选 L7 处理发送到选定服务器之前接收整个请求。对于基于 HTTPS 套接字的实施，会在面向客户端的连接或面向服务器的连接上交换身份验证信息。基于套接字的负载平衡是 TCP、HTTP 和 HTTPS 虚拟服务器的默认模式。

NSX 负载平衡器的主要概念有虚拟服务器、服务器池、服务器池成员和服务监控器。

虚拟服务器

应用程序服务的抽象形式，由 IP、端口、协议和应用程序配置文件（如 TCP 或 UDP）的唯一组合表示。

服务器池

后端服务器组。

服务器池成员

作为池中的成员表示后端服务器。

服务监控器

定义如何探测后端服务器的运行状况。

应用程序配置文件

表示给定应用程序的 TCP、UDP、持久性和证书配置。

设置概述

首先设置负载平衡器的全局选项。现在，创建由后端服务器成员组成的服务器池，并将服务监控器与该池关联，以便有效地管理和共享后端服务器。

其次，创建应用程序配置文件，以定义负载平衡器中的常见应用程序行为，如客户端 SSL、服务器 SSL、X-Forwarded-For 或持久性。持久性使用类似特性（例如，需要将源 IP 或 cookie 分派到同一个池成员）发送后续请求，而无需运行负载平衡算法。可以在虚拟服务器之间重复使用应用程序配置文件。

然后，创建一个可选应用程序规则，以配置应用程序特定的流量处理设置，例如匹配某个 URL 或主机名，从而可以由不同的池处理不同的请求。接下来，创建特定于应用程序的服务监控器，或者如果现有服务监控器满足您的需求，也可以使用此现有服务监控器。

（可选）您可以创建应用程序规则以支持 L7 虚拟服务器的高级功能。应用程序规则的某些用例包括内容切换、标头处理、安全规则和 DOS 防护。

最后，创建虚拟服务器，将服务器池、应用程序配置文件和任何潜在的应用程序规则连接在一起。

虚拟服务器收到请求时，负载平衡算法将考虑池成员配置和运行时状态。然后，算法计算相应的池（包含一个或多个成员）以分发流量。池成员配置包括权重、最大连接数和条件状态等设置。运行时状态包括当前连接数、响应时间以及运行状况检查状态信息。计算方法可以是循环、加权循环、最少连接、源 IP 哈希、加权最少连接、URL、URI 或 HTTP 标头。

每个池都由相关联的服务监控器监控。当负载平衡器检测到池成员出现问题时，会将其标记为关闭。从服务器池中选择池成员时，仅选择正常运行的服务器。如果服务器池未配置服务监控器，那么将认为所有池成员均正常运行。

配置负载平衡器服务

全局负载平衡器配置参数包括整体实现、第 4 层或第 7 层引擎的选择以及要记录的事件类型的指定。

步骤

1 打开 Edge 网关服务。

a 导航到**网络** > **Edge**。

b 选择要编辑的 Edge 网关，然后单击**服务**。

2 导航到**负载平衡器** > **全局配置**。

3 选择要启用的选项：

选项	操作
状态	通过单击开关图标启用负载平衡器。 启用**已启用加速**以将负载平衡器配置为使用更快的 L4 引擎而不是 L7 引擎。L4 TCP VIP 在 Edge 网关防火墙之前处理，因此不需要“允许”防火墙规则。 **注** 适用于 HTTP 和 HTTPS 的 L7 VIP 在防火墙之后处理，因此，当未启用加速时，必须存在一个 Edge 网关防火墙规则，以便允许访问这些协议的 L7 VIP。如果启用加速并且服务器池处于非透明模式，则添加 SNAT 规则，因此您必须确保在 Edge 网关上启用防火墙。
启用日志记录	启用日志记录，以便 Edge 网关负载平衡器收集流量日志。
日志级别	选择要在日志中收集的事件严重程度。

4 单击**保存更改**。

保存操作可能需要一分钟才能完成。

后续步骤

为负载平衡器配置应用程序配置文件。请参见创建应用程序配置文件。

创建应用程序配置文件

应用程序配置文件用于为特定类型的网络流量定义负载均衡器的行为。在配置配置文件后，需要将其与虚拟服务器相关联。之后，虚拟服务器将根据配置文件中指定的值来处理流量。使用配置文件可以更好地控制对网络流量的管理，并使流量管理任务更轻松、更高效。

在为 HTTPS 流量创建配置文件时，允许使用以下 HTTPS 流量模式：

- 客户端 -> HTTPS -> LB (终止 SSL) -> HTTP -> 服务器
- 客户端 -> HTTPS -> LB (终止 SSL) -> HTTPS -> 服务器
- 客户端 -> HTTPS-> LB (SSL 直通) -> HTTPS -> 服务器
- 客户端 -> HTTP-> LB -> HTTP -> 服务器

步骤

1 打开 Edge 网关服务。

a 导航到**网络** > **Edge**。

b 选择要编辑的 Edge 网关，然后单击**服务**。

2 导航到**负载均衡器** > **应用程序配置文件**。

3 单击**创建** () 按钮。

4 输入配置文件的名称。

5 配置应用程序配置文件。

选项	描述
类型	选择用于向服务器发送请求的协议类型。所需参数列表取决于您选择的协议。不能输入不适用于您所选协议的参数。所有其他参数都是必需的。
启用 SSL 直通	单击此选项可通过直通直接向虚拟服务器进行 SSL 身份验证。 否则，将在目标地址进行 SSL 身份验证。
HTTP 重定向 URL	（HTTP 和 HTTPS）输入应将传输到目标地址的流量重定向到的 URL。
持久	指定配置文件的持久机制。 持久功能可跟踪和存储会话数据，例如处理客户端请求的特定池成员。这样可确保客户端请求在整个会话生命周期或后续会话期间定向到同一池成员。选项包括： ■ **源 IP** 源 IP 持久功能会根据源 IP 地址跟踪会话。当客户端请求连接到支持源地址关联性持久功能的虚拟服务器时，负载均衡器会检查该客户端是否先前连接过，如果是，则会将该客户端返回到同一池成员。 ■ **MSRDP** （仅限 TCP）Microsoft 远程桌面协议 (MSRDP) 持久功能会在 Windows 客户端和运行 Microsoft 远程桌面协议 (RDP) 服务的服务器之间保持持久会话。启用 MSRDP 持久功能的推荐方案是：创建一个负载均衡 池，其中包含运行 Windows Server 客户机操作系统的成员，而所有成员都属于一个 Windows 集群并加入一个 Windows 会话目录。 ■ **SSL 会话 ID** 启用 SSL 直通时，可以使用 SSL 会话 ID 持久功能。SSL 会话 ID 持久功能可确保将来自同一客户端的重复连接发送到同一服务器。会话 ID 持久功能允许使用 SSL 会话恢复，从而可节省客户端和服务器的处理时间。
Cookie 名称	（HTTP 和 HTTPS）如果指定了 **Cookie** 作为持久机制，请输入 Cookie 名称。Cookie 持久功能将在客户端首次访问站点时使用 Cookie 唯一地标识会话。在连接会话中的后续请求时，负载均衡器会引用此 Cookie，以便它们都会转到同一虚拟服务器。

选项	描述
模式	选择插入 Cookie 应采用的模式。以下是受支持的模式： ■ **插入** Edge 网关会发送一个 Cookie。如果服务器发送了一个或多个 Cookie，则客户端会收到一个额外的 Cookie（即服务器 Cookie 加上 Edge 网关 Cookie）。如果服务器未发送任何 Cookie，则客户端只会收到 Edge 网关 Cookie。 ■ **前缀** 如果您的客户端不支持多个 Cookie，请选择此选项。 注 所有浏览器都接受多个 Cookie。但是，您可能会使用一个专有应用程序，该应用程序使用仅支持一个 Cookie 的专有客户端。Web 服务器会照常发送其 Cookie。Edge 网关会在服务器 Cookie 值中（作为前缀）注入其 Cookie 信息。当 Edge 网关将此 Cookie 添加的信息发送到服务器时，此信息将被移除。 ■ **应用程序会话**对于此选项，服务器不发送 Cookie，而是将用户会话信息作为 URL 发送。例如 `http://example.com/admin/UpdateUserServlet;jsessionid=OI24B9ASD7BSSD`，其中 `jsessionid` 是用户会话信息，用于实现持久性。无法查看应用程序会话持久表进行故障排除。
过期时间 (秒)	输入持久功能保持有效的时间长度（以秒为单位）。必须是介于范围 1-86400 之间的正整数。 注 对于使用 TCP 源 IP 持久功能进行的 L7 负载均衡 ，如果在一段时间内没有建立新的 TCP 连接，则持久条目将超时，即使现有连接仍处于活动状态也是如此。
插入 X-Forwarded-For HTTP 标头	（HTTP 和 HTTPS）选择**插入 X-Forwarded-For HTTP 标头**以标识通过负载均衡器连接到 Web 服务器的客户端的发起 IP 地址。 注 如果启用了 SSL 直通，则不支持使用此标头。
启用池端 SSL	（仅限 HTTPS）选择**启用池端 SSL** 以在“池证书”选项卡中定义用于从服务器端对负载均衡器进行身份验证的证书、CA 或 CRL。

6 （仅限 HTTPS）配置要与应用程序配置文件一起使用的证书。如果您需要的证书不存在，则可以从**证书**选项卡创建它们。

选项	描述
虚拟服务器证书	选择用于解密 HTTPS 流量的证书、CA 或 CRL。
池证书	定义用于从服务器端对负载均衡器进行身份验证的证书、CA 或 CRL。 注 选择**启用池端 SSL** 以启用此选项卡。
密码	选择在 SSL/TLS 握手期间协商的密码算法（或密码套件）。
客户端身份验证	指定是忽略客户端身份验证还是需要客户端身份验证。 注 如果设置为**必需**，则客户端必须在此请求之后提供一个证书，否则握手将被取消。

7 单击**保存留**以保留更改。

该操作可能需要一分钟才能完成。

后续步骤

为负载均衡器添加服务监视器，以便为不同类型的网络流量定义运行状况检查。请参见创建服务监视器。

创建服务监视器

可以创建服务监视器，以便为特定类型的网络流量定义运行状况检查参数。将服务监视器与池关联后，将根据服务监视器参数监控池成员。

步骤

1 打开 Edge 网关服务。

a 导航到**网络** > **Edge**。

b 选择要编辑的 Edge 网关，然后单击**服务**。

2 导航到**负载平衡器** > **服务监控**。

3 单击**创建** () 按钮。

4 输入服务监视器的名称。

5 （可选） 为服务监视器配置以下选项：

选项	描述
间隔	输入使用指定**方法**监控服务器的间隔。
超时	输入必须接收来自服务器的响应的最长时间（以秒为单位）。
最大重试次数	输入在声明服务器关闭之前指定的监控**方法**必须连续失败的次数。
类型	选择要将运行状况检查请求发送到服务器的方式 - HTTP、HTTPS、TCP、ICMP 或 UDP。 根据所选的类型，将启用或禁用**新建服务监视器**对话框中的其余选项。
预期	（HTTP 和 HTTPS）输入监视器希望在 HTTP 或 HTTPS 响应的状态行中匹配的字符串（例如 HTTP/1.1）。
方法	（HTTP 和 HTTPS）选择用于检测服务器状态的方法。
URL	（HTTP 和 HTTPS）输入要在服务器状态请求中使用的 URL。 注 如果选择 POST 方法，则必须为**发送**指定一个值。
发送	（HTTP、HTTPS、UDP）输入要发送的数据。
接收	（HTTP、HTTPS 和 UDP）输入要在响应内容中匹配的字符串。 注 如果**预期**不匹配，则监视器不会尝试匹配**接收**内容。

扩展	（全部）以键=值对的形式输入高级监视器参数。例如，warning=10 表示当服务器未在 10 秒内响应时其状态将设置为警告。所有扩展项都应使用回车符分隔。例如：
	`<extension>delay=2`
	`critical=3`
	`escape</extension>`

6 单击**保存留**以保留更改。

该操作可能需要一分钟才能完成。

示例： 为每个协议支持的扩展

表 4-2. 适用于 HTTP/HTTPS 协议的扩展

监视器扩展	描述
no-body	不等待文档正文，并且在 HTTP/HTTPS 标头后停止读取。 注 仍会发送 HTTP GET 或 HTTP POST；而非 HEAD 方法。
max-age=*SECONDS*	当文档存在时间超过 SECONDS 时发出警告。该数字可以采用以下形式：10m 表示分钟数，10h 表示小时数或 10d 表示天数。
content-type=*STRING*	在 POST 调用中指定 Content-Type 标头媒体类型。
linespan	允许正则表达式跨换行符（前面必须加 -r 或 -R）。
regex=*STRING* 或 ereg=*STRING*	在页面中搜索正则表达式 STRING。
eregi=*STRING*	在页面中搜索不区分大小写的正则表达式 STRING。
invert-regex	找到时返回 CRITICAL，未找到时返回 OK。
proxy-authorization=*AUTH_PAIR*	在具有基本身份验证的代理服务器上指定 username:password。
useragent=*STRING*	以 `User Agent` 的形式发送 HTTP 标头中的字符串。
header=*STRING*	发送 HTTP 标头中的任何其他标记。多次用于其他标头。
onredirect=ok|warning|critical|follow|sticky|stickyport	指示如何处理重定向的页面。 `sticky` 与 `follow` 类似，但遵循指定的 IP 地址。 `stickyport` 可确保端口保持不变。
pagesize=*INTEGER:INTEGER*	指定所需的最小和最大页面大小（以字节为单位）。
warning=DOUBLE	指定导致警告状态的响应时间（以秒为单位）。
critical=DOUBLE	指定导致严重状态的响应时间（以秒为单位）。

表 4-3. 仅适用于 HTTPS 协议的扩展

监视器扩展	描述
sni	启用 SSL/TLS 主机名扩展支持 (SNI)。
certificate=**INTEGER**	指定证书必须有效的最小天数。端口默认为 443。如果使用此选项，则不检查 URL。
authorization=AUTH_PAIR	在具有基本身份验证的站点上指定 username:password。

表 4-4. 适用于 TCP 协议的扩展

监视器扩展	描述
escape	允许在 send 或 quit 字符串中使用 \n、\r、\t 或 \。必须位于 send 或 quit 选项之前。默认情况下，不会向 send 添加任何内容，并向 quit 末尾添加 \r\n。
all	指定在服务器响应中需要出现所有预期字符串。默认情况下使用 any。
quit=*STRING*	将字符串发送到服务器，以便完全关闭连接。
refuse=ok|warn|crit	以状态 ok、warn 或 criti 接受 TCP 拒绝。默认情况下，使用状态 crit。
mismatch=ok|warn|crit	以状态 ok、warn 或 crit 接受预期字符串不匹配。默认情况下，使用状态 warn。
jail	隐藏 TCP 套接字的输出。
maxbytes=*INTEGER*	当收到超过指定字节数的字节数时，关闭连接。
delay=*INTEGER*	在发送字符串和轮询响应之间等待指定的秒数。
certificate=*INTEGER*[,*INTEGER*]	指定证书必须有效的最小天数。第一个值是表示警告的 #days，第二个值是表示严重的天数（如果未指定，则为 0）。
ssl	使用 SSL 进行连接。
warning=DOUBLE	指定导致警告状态的响应时间（以秒为单位）。
critical=DOUBLE	指定导致严重状态的响应时间（以秒为单位）。

后续步骤

为负载平衡器添加服务器池。请参见添加服务器池进行负载平衡。

添加服务器池进行负载平衡

您可以添加服务器池，以灵活高效地管理和共享后端服务器。池管理负载平衡器分配方法，并连接一个服务监控器以监控运行状况检查参数。

步骤

1 打开 Edge 网关服务。

   a 导航到**网络** > **Edge**。

   b 选择要编辑的 Edge 网关，然后单击**服务**。

2 导航到**负载平衡器** > **池**。

3 单击**创建** (+) 按钮。

4 键入负载平衡器池的名称和可选描述。

5 从**算法**下拉菜单中选择服务的平衡方法：

选项	描述
ROUND-ROBIN	将根据分配的权重来轮流使用每个服务器。当服务器处理时间平均分布时，这是最平稳最合理的算法。
IP-HASH	根据每个数据包的源和目标 IP 地址的哈希选择一个服务器。
LEASTCONN	根据服务器上已打开的连接数将客户端请求分配到多个服务器。新连接将被发送到打开连接数最少的服务器。
URI	将对 URI 的左侧部分（问号之前）进行哈希计算并除以正在运行的服务器的总权重。结果会指出哪个服务器将接收请求。此选项确保只要服务器没有出现故障，URI 就会始终定向到同一服务器。
HTTPHEADER	在每个 HTTP 请求中查找 HTTP 标头名称。圆括号中的标头名称不区分大小写，类似于 ACL ‘hdr()’ 函数。如果标头不存在或不包含任何值，将应用 ROUND-ROBIN 算法。HTTP HEADER 算法参数有一个选项 `headerName=<name>`。例如，您可以使用 **`host`** 作为 HTTP HEADER 算法参数。
URL	在每个 HTTP GET 请求的查询字符串中查找参数中指定的 URL 参数。如果参数后跟等号 = 和一个值，则对该值进行哈希计算并除以正在运行的服务器的总权重。结果会指出哪个服务器接收请求。此过程用于跟踪请求中的用户标识符，并确保只要没有服务器开启或关闭，就始终将同一用户 ID 发送到同一服务器。如果未找到任何值或参数，则应用 ROUND-ROBIN 算法。URL 算法参数有一个选项 `urlParam=<url>`。

6 向池添加成员。

a 单击**添加** () 按钮。

b 输入池成员的名称。

c 输入池成员的 IP 地址。

d 输入成员用于接收来自负载平衡器的流量的端口。

e 输入成员用于接收运行状况监控器请求的监控器端口。

f 在**权重**文本框中，键入该成员将处理的流量比例。必须是 1-256 范围内的整数。

g （可选） 在**最大连接数**文本框中，键入成员可以处理的最大并发连接数。

当入站请求数超过最大值时，请求将排队，然后负载平衡器等待释放连接。

h （可选） 在**最小连接数**文本框中，键入成员必须始终接受的最小并发连接数。

i 单击**保留**将新成员添加到池。

该操作可能需要一分钟才能完成。

7 （可选） 要使后端服务器可以看到客户端 IP 地址，请选择**透明**。

未选择**透明**（默认值）时，后端服务器会将流量源的 IP 地址视为负载平衡器的内部 IP 地址。

选择**透明**时，源 IP 地址将是客户端的实际 IP 地址，并且必须将 Edge 网关设置为默认网关，以确保返回数据包通过 Edge 网关。

8 单击**保存留**以保留更改。

该操作可能需要一分钟才能完成。

后续步骤

为负载平衡器添加虚拟服务器。虚拟服务器有一个公共 IP 地址，为所有入站客户端请求提供服务。请参见添加虚拟服务器。

添加应用程序规则

您可以编写应用程序规则，以便直接操作和管理 IP 应用程序流量。

步骤

1 打开 Edge 网关服务。

a 导航到**网络** > **Edge**。

b 选择要编辑的 Edge 网关，然后单击**服务**。

2 导航到**负载平衡器** > **应用程序规则**。

3 单击**添加** () 按钮。

4 输入应用程序规则的名称。

5 输入应用程序规则的脚本。

有关应用程序规则语法的信息，请参见 http://cbonte.github.io/haproxy-dconv/2.2/configuration.html。

6 单击**保存留**以保留更改。

该操作可能需要一分钟才能完成。

后续步骤

将新应用程序规则关联到为负载平衡器添加的虚拟服务器。请参见 添加虚拟服务器。

添加虚拟服务器

将 NSX Data Center for vSphere Edge 网关内部或上行链路接口作为虚拟服务器进行添加。虚拟服务器有一个公共 IP 地址，为所有入站客户端请求提供服务。

默认情况下，负载平衡器会在每个客户端请求后关闭服务器 TCP 连接。

步骤

1 打开 Edge 网关服务。

a 导航到**网络** > **Edge**。

b 选择要编辑的 Edge 网关，然后单击**服务**。

2 导航到**负载平衡器** > **虚拟服务器**。

3 单击**添加** () 按钮。

4 在**常规**选项卡上，配置虚拟服务器的以下选项：

选项	描述
启用虚拟服务器	单击启用虚拟服务器。
启用加速	单击启用加速。
应用程序配置文件	选择要与虚拟服务器相关联的应用程序配置文件。
名称	键入虚拟服务器的名称。
描述	键入虚拟服务器的可选描述。
IP 地址	键入或浏览选择负载平衡器侦听的 IP 地址。
协议	选择虚拟服务器接受的协议。您必须选择选定**应用程序配置文件**使用的相同协议。
端口	键入负载平衡器侦听的端口号。
默认池	选择负载平衡器将使用的服务器池。
连接限制	（可选）键入虚拟服务器可以处理的最大并发连接数。
连接速率限制 (CPS)	（可选）键入每秒最大新入站连接请求数。

5 （可选） 要将应用程序规则与虚拟服务器相关联，请单击**高级**选项卡，然后完成以下步骤：

a 单击**添加** () 按钮。

此时将显示为负载平衡器创建的应用程序规则。如有必要，为负载平衡器添加应用程序规则。请参见添加应用程序规则。

6 单击**保存留**以保留更改。

该操作可能需要一分钟才能完成。

后续步骤

创建 Edge 网关防火墙规则，以允许流向新虚拟服务器（目标 IP 地址）的流量。请参见添加 NSX Data Center for vSphere Edge 网关防火墙规则

使用虚拟专用网络保证访问安全

您可以为 NSX Data Center for vSphere Edge 网关配置由 NSX 软件提供的 VPN 功能。可使用 SSL VPN-Plus 通道、IPsec VPN 通道或 L2 VPN 通道配置与组织虚拟数据中心之间的 VPN 连接。

如《NSX 管理指南》中所述，NSX Edge 网关支持以下 VPN 服务：

- SSL VPN-Plus，允许远程用户访问专用的企业应用程序。
- IPsec VPN，提供 NSX Edge 网关和另外具有 NSX 或者第三方硬件路由器或 VPN 网关的远程站点之间的站点到站点连接。
- L2 VPN，允许虚拟机跨地域界限保留同一 IP 地址，同时又保持网络连接，从而实现组织虚拟数据中心的扩展。

在 VMware Cloud Director 环境中，您可以在下列项之间创建 VPN 通道：

- 同一组织的组织虚拟数据中心网络之间
- 不同组织的组织虚拟数据中心网络之间
- 组织虚拟数据中心网络与外部网络之间

注 VMware Cloud Director 不支持在相同的两个 Edge 网关之间创建多个 VPN 通道。如果两个 Edge 网关之间已存在一个通道，并且您想要将另外一个子网添加到该通道，则需要删除现有的 VPN 通道并创建一个包括新子网的新通道。

为某个 Edge 网关配置 VPN 通道后，您可以使用远程位置中的 VPN 客户端连接到该 Edge 网关支持的组织虚拟数据中心。

配置 SSL VPN-Plus

通过 VMware Cloud Director 环境中 NSX Data Center for vSphere Edge 网关的 SSL VPN-Plus 服务，远程用户可以安全地连接到该 Edge 网关支持的组织虚拟数据中心中的专用网络和应用程序。您可以在 Edge 网关上配置各种 SSL VPN-Plus 服务。

在 VMware Cloud Director 环境中，Edge 网关的 SSL VPN-Plus 功能支持网络访问模式。远程用户必须安装 SSL 客户端才能建立安全连接并访问 Edge 网关后面的网络和应用程序。在 Edge 网关的 SSL VPN-Plus 配置中，您可以添加适用于操作系统的安装软件包并配置某些参数。有关详细信息，请参见添加 SSL VPN-Plus 客户端安装软件包。

配置 Edge 网关上的 SSL VPN-Plus 是一个多步骤过程。

前提条件

确认已将 SSL VPN-Plus 所需的所有 SSL 证书都添加到**证书**屏幕中。请参见 SSL 证书管理。

注 在 Edge 网关上，端口 443 是 HTTPS 的默认端口。对于 SSL VPN 功能，Edge 网关的 HTTPS 端口必须可从外部网络访问。SSL VPN 客户端要求可从客户端系统访问在 **SSL VPN-Plus** 选项卡的“服务器设置”屏幕中配置的 Edge 网关 IP 地址和端口。请参见配置 SSL VPN 服务器设置。

步骤

1 导航到 SSL-VPN Plus 屏幕

您可以导航到“SSL-VPN Plus”屏幕，以便开始为 NSX Data Center for vSphere Edge 网关配置 SSL-VPN Plus 服务。

2 配置 SSL VPN 服务器设置

这些服务器设置可配置 SSL VPN 服务器，例如服务侦听的 IP 地址和端口、服务的密码列表及其服务证书。连接到 NSX Data Center for vSphere Edge 网关时，远程用户会指定您在这些服务器设置中设置的相同 IP 地址和端口。

3 创建 IP 池以与 NSX Data Center for vSphere Edge 网关上的 SSL VPN-Plus 配合使用

将从使用 **SSL VPN-Plus** 选项卡上的 **IP 池**屏幕配置的静态 IP 池中为远程用户分配虚拟 IP 地址。

4 添加专用网络以与 NSX Data Center for vSphere Edge 网关上的 SSL VPN-Plus 配合使用

使用 **SSL VPN-Plus** 选项卡上的“专用网络”屏幕配置专用网络。当远程用户使用自己的 VPN 客户端和 SSL VPN 通道连接时，专用网络是您希望 VPN 客户端有权访问的网络。启用的专用网络将安装在 VPN 客户端的路由表中。

5 为 NSX Data Center for vSphere Edge 网关上的 SSL VPN-Plus 配置身份验证服务

使用 **SSL VPN-Plus** 选项卡上的**身份验证**屏幕为 Edge 网关 SSL VPN 服务设置本地身份验证服务器，然后选择性启用客户端证书身份验证。使用此身份验证服务器对连接的用户进行身份验证。将对本地身份验证服务器中配置的所有用户进行身份验证。

6 将 SSL VPN-Plus 用户添加到本地 SSL VPN-Plus 身份验证服务器

可使用 **SSL VPN-Plus** 选项卡上的**用户**屏幕，将远程用户的帐户添加到 NSX Data Center for vSphere Edge 网关 SSL VPN 服务的本地身份验证服务器。

7 添加 SSL VPN-Plus 客户端安装软件包

使用 **SSL VPN-Plus** 选项卡上的“安装软件包”屏幕为远程用户创建 SSL VPN-Plus 客户端的指定安装软件包。

8 编辑 SSL VPN-Plus 客户端配置

使用 **SSL VPN-Plus** 选项卡上的**客户端配置**屏幕自定义 SSL VPN 客户端通道在远程用户登录到 SSL VPN 时的响应方式。

9 自定义 NSX Data Center for vSphere Edge 网关的常规 SSL VPN-Plus 设置

默认情况下，系统会在 VMware Cloud Director 环境中的 Edge 网关上设置一些 SSL VPN-Plus 设置。您可以使用 VMware Cloud Director 租户门户 **SSL VPN-Plus** 选项卡上的**常规设置**屏幕自定义这些设置。

导航到 SSL-VPN Plus 屏幕

您可以导航到“SSL-VPN Plus”屏幕，以便开始为 NSX Data Center for vSphere Edge 网关配置 SSL-VPN Plus 服务。

步骤

1 打开 Edge 网关服务。

a 导航到**网络** > **Edge**。

b 选择要编辑的 Edge 网关，然后单击**服务**。

2 单击 **SSL VPN-Plus** 选项卡。

后续步骤

在**常规**屏幕上，配置默认 SSL VPN-Plus 设置。请参见自定义 NSX Data Center for vSphere Edge 网关的常规 SSL VPN-Plus 设置。

配置 SSL VPN 服务器设置

这些服务器设置可配置 SSL VPN 服务器，例如服务侦听的 IP 地址和端口、服务的密码列表及其服务证书。连接到 NSX Data Center for vSphere Edge 网关时，远程用户会指定您在这些服务器设置中设置的相同 IP 地址和端口。

如果您的 Edge 网关在其外部接口上配置了多个覆盖 IP 地址网络，则您为 SSL VPN 服务器选择的 IP 地址可以不同于 Edge 网关的默认外部接口。

配置 SSL VPN 服务器设置时，必须选择要为 SSL VPN 通道使用哪个加密算法。可以选择一个或多个密码。请根据所选择加密算法的优缺点谨慎选择密码。

默认情况下，系统使用系统为每个 Edge 网关生成的默认自签名证书作为 SSL VPN 通道的默认服务器身份证书。可以选择使用在**证书**屏幕上添加到系统的数字证书来代替此默认证书。

前提条件

- 确认您已满足配置 SSL VPN-Plus 中所述的必备条件。
- 如果您选择使用不同于默认服务证书的证书，请将所需的证书导入到系统。请参见将服务证书添加到 Edge 网关。
- 导航到 SSL-VPN Plus 屏幕。

步骤

1 在 **SSL VPN-Plus** 屏幕上，单击**服务器设置**。

2 单击**已启用**。

3 从下拉菜单中选择 IP 地址。

4 （可选） 输入 TCP 端口号。

此 TCP 端口号由 SSL 客户端安装软件包使用。默认情况下，系统使用端口 443，它是 HTTPS/SSL 流量的默认端口。即使需要提供端口号，您也可以设置任何 TCP 端口进行通信。

> **注** SSL VPN 客户端需要可从远程用户的客户端系统访问在此处配置的 IP 地址和端口。如果您要更改默认端口号，请确保可从目标用户的系统访问该 IP 地址和端口组合。

5 从密码列表中选择一种加密方法。

6 配置服务的 Syslog 日志记录策略。

默认情况下启用日志记录。您可以更改要记录的消息级别或禁用日志记录。

7 （可选） 如果要使用服务证书，而非系统生成的默认自签名证书，请单击**更改服务器证书**，选择证书，然后单击**确定**。

8 单击**保存更改**。

后续步骤

注 您设置的 Edge 网关 IP 地址和 TCP 端口号必须可由您的远程用户访问。添加 Edge 网关防火墙规则，以允许访问在此过程中配置的 SSL VPN-Plus IP 地址和端口。请参见添加 NSX Data Center for vSphere Edge 网关防火墙规则。

添加 IP 池，以便在远程用户使用 SSL VPN-Plus 连接时向他们分配 IP 地址。请参见创建 IP 池以与 NSX Data Center for vSphere Edge 网关上的 SSL VPN-Plus 配合使用。

创建 IP 池以与 NSX Data Center for vSphere Edge 网关上的 SSL VPN-Plus 配合使用

将从使用 **SSL VPN-Plus** 选项卡上的 **IP 池**屏幕配置的静态 IP 池中为远程用户分配虚拟 IP 地址。

在此屏幕中添加的每个 IP 池都会导致在 Edge 网关上配置一个 IP 地址子网。在这些 IP 池中使用的 IP 地址范围必须不同于在 Edge 网关上配置的所有其他网络。

注 SSL VPN-Plus 会根据 IP 池在屏幕上的表中显示的顺序将 IP 池中的 IP 地址分配给远程用户。将 IP 池添加到屏幕上的表中后，您可以使用向上和向下箭头调整它们在表中的位置。

前提条件

- 导航到 SSL-VPN Plus 屏幕。
- 配置 SSL VPN 服务器设置。

步骤

1 在 **SSL VPN-Plus** 选项卡上，单击 **IP 池**。

2 单击**创建** () 按钮。

3 配置 IP 池设置。

选项	操作
IP 范围	输入此 IP 池的 IP 地址范围，例如 `127.0.0.1-127.0.0.9`。 当 VPN 客户端在进行身份验证后连接到 SSL VPN 通道时，将向它们分配这些 IP 地址。
网络掩码	输入 IP 池的网络掩码，例如 `255.255.255.0`。
网关	输入您要让 Edge 网关创建并分配为此 IP 池的网关地址的 IP 地址。 创建 IP 池后，将在 Edge 网关虚拟机上创建一个虚拟适配器，并在该虚拟接口上配置此 IP 地址。此 IP 地址可以是子网内的任何 IP，但同时不属于 **IP 范围**字段中的范围内。
描述	（可选）输入此 IP 池的描述。
状态	选择是启用还是禁用此 IP 池。
主 DNS	（可选）输入将用于对这些虚拟 IP 地址进行名称解析的主 DNS 服务器的名称。
辅助 DNS	（可选）输入要使用的辅助 DNS 服务器的名称。

选项	操作
DNS 后缀	（可选）输入托管客户端系统的域的 DNS 后缀，用于按域解析主机名。
WINS 服务器	（可选）根据组织需求输入 WINS 服务器地址。

4 单击**保留**。

结果

IP 池配置将添加到屏幕上的表中。

后续步骤

添加您希望使用 SSL VPN-Plus 连接的远程用户可以访问的专用网络。请参见添加专用网络以与 NSX Data Center for vSphere Edge 网关上的 SSL VPN-Plus 配合使用。

添加专用网络以与 NSX Data Center for vSphere Edge 网关上的 SSL VPN-Plus 配合使用

使用 **SSL VPN-Plus** 选项卡上的“专用网络”屏幕配置专用网络。当远程用户使用自己的 VPN 客户端和 SSL VPN 通道连接时，专用网络是您希望 VPN 客户端有权访问的网络。启用的专用网络将安装在 VPN 客户端的路由表中。

专用网络是 Edge 网关后面您要加密 VPN 客户端的流量，或者拒绝加密的所有可访问 IP 网络的列表。必须将需要通过 SSL VPN 通道访问的每个专用网络添加为单独的条目。您可以使用路由汇总技术限制条目数。

- 通过 SSL VPN-Plus，远程用户将基于 IP 池在屏幕上的表中显示的自上而下的顺序访问专用网络。将专用网络添加到屏幕上的表后，您可以使用向上和向下箭头调整它们在表中的位置。
- 如果您选择为某个专用网络启用 TCP 优化，则某些应用程序（例如主动模式下的 FTP）可能无法在该子网中正常运行。要添加在主动模式下配置的 FTP 服务器，必须为该 FTP 服务器添加其他专用网络并针对该专用网络禁用 TCP 优化。此外，适用于该 FTP 服务器的专用网络必须启用并显示在屏幕上的表中的 TCP 优化专用网络上方。

前提条件

- 导航到 SSL-VPN Plus 屏幕。
- 创建 IP 池以与 NSX Data Center for vSphere Edge 网关上的 SSL VPN-Plus 配合使用。

步骤

1 在 **SSL VPN-Plus** 选项卡上，单击**专用网络**。

2 单击**添加** () 按钮。

3 配置此专用网络设置。

选项	操作
网络	采用 CIDR 格式键入专用网络 IP 地址，例如 **192.169.1.0/24**。
描述	（可选）键入网络描述。

选项	操作
发送流量	指定希望 VPN 客户端发送专用网络和 Internet 流量的方式。 ■ **通过通道** VPN 客户端将通过启用了 SSL VPN-Plus 的 Edge 网关发送专用网络和 Internet 流量。 ■ **绕过通道** VPN 客户端绕过 Edge 网关，直接将流量发送到专用服务器。
启用 TCP 优化	（可选）要更好地优化 Internet 速度，则在选择**通过通道**发送流量的同时，也必须选择**启用 TCP 优化** 选择此选项可提高 VPN 通道内 TCP 数据包的性能，但不会提高 UDP 流量的性能。 常规完全访问 SSL VPN 通道会借助于第二个 TCP/IP 堆栈发送 TCP/IP 数据以通过 Internet 进行加密。此常规方法将应用程序层数据封装在两个单独的 TCP 流中。丢失数据包（在最佳的 Internet 条件下也会发生）时，将发生性能降级影响，称为 TCP-over-TCP 危机。在 TCP-over-TCP 危机中，两个 TCP 设备更正同一个 IP 数据包，这会削弱网络吞吐量，并导致连接超时。选择**启用 TCP 优化**可消除发生此 TCP-over-TCP 问题的风险。 注 启用 TCP 优化时： ■ 必须输入要针对其优化 Internet 流量的端口号。 ■ SSL VPN 服务器会代表 VPN 客户端打开 TCP 连接。SSL VPN 服务器打开 TCP 连接时，将应用第一个自动生成的 Edge 防火墙规则，以允许从 Edge 网关打开的所有连接通过。未优化的流量将通过常规 Edge 防火墙规则进行评估。默认生成的 TCP 规则将允许任何连接。
端口	选择**通过通道**后，键入希望打开的端口号范围以便远程用户访问内部服务器，例如 **20-21**（适用于 FTP 流量），**80-81**（适用于 HTTP 流量）。 要向用户授予无限制访问权限，请将此字段留空。
状态	启用或禁用专用网络。

4 单击**保留**。

5 单击**保存更改**将配置保存到系统。

后续步骤

添加身份验证服务器。请参见为 NSX Data Center for vSphere Edge 网关上的 SSL VPN-Plus 配置身份验证服务。

重要事项 添加相应的防火墙规则，以允许流入在此屏幕中添加的专用网络的网络流量。请参见添加 NSX Data Center for vSphere Edge 网关防火墙规则。

为 NSX Data Center for vSphere Edge 网关上的 SSL VPN-Plus 配置身份验证服务

使用 **SSL VPN-Plus** 选项卡上的**身份验证**屏幕为 Edge 网关 SSL VPN 服务设置本地身份验证服务器，然后选择性启用客户端证书身份验证。使用此身份验证服务器对连接的用户进行身份验证。将对本地身份验证服务器中配置的所有用户进行身份验证。

您只能在 Edge 网关上配置一个本地 SSL VPN-Plus 身份验证服务器。如果单击 **+ 本地**并指定其他身份验证服务器，则尝试保存配置时会显示一条错误消息。

通过 SSL VPN 进行身份验证的最长时间为三 (3) 分钟。此最大值由非身份验证超时确定，该超时值默认为 3 分钟且无法进行配置。因此，如果您一连串的授权中有多个身份验证服务器，且用户身份验证用时超过 3 分钟，那么将不会对该用户进行身份验证。

前提条件

- 导航到 SSL-VPN Plus 屏幕。
- 添加专用网络以与 NSX Data Center for vSphere Edge 网关上的 SSL VPN-Plus 配合使用。
- 如果您打算启用客户端证书身份验证，请确认已将 CA 证书添加到 Edge 网关。请参见将 CA 证书添加到 Edge 网关进行 SSL 证书信任验证。

步骤

1 单击 **SSL VPN-Plus** 选项卡和**身份验证**。

2 单击**本地**。

3 配置身份验证服务器设置。

a （可选） 启用和配置密码策略。

选项	描述
启用密码策略	启用您在此处配置的密码策略设置的实施。
密码长度	输入密码长度允许的最少和最多字符数。
最少字母数	（可选）键入密码中需要的最少字母字符数。
最少数字数	（可选）键入密码中需要的最少数字字符数。
最少特殊字符数	（可选）键入密码中需要的最少特殊字符数，如与号 (&)、井号 (#)、百分号 (%) 等。
密码不应包含用户 ID	（可选）启用后可以强制密码不得包含用户 ID。
密码到期时间	（可选）键入用户必须更改密码前密码可存在的最大天数。
到期通知时间	（可选）键入**密码到期时间**前的天数，在该日期会向用户发送密码即将到期通知。

b （可选） 启用和配置帐户锁定策略。

选项	描述
启用帐户锁定策略	启用您在此处配置的帐户锁定策略设置的实施。
重试次数	输入用户可以尝试访问其帐户的次数。
重试持续时间	输入登录尝试失败后锁定用户帐户的时间段（以分钟为单位）。 例如，如果将**重试次数**指定为 5，将**重试持续时间**指定为 1 分钟，则当用户在 1 分钟内尝试登录 5 次均失败后，其帐户将被锁定。
锁定持续时间	输入用户帐户保持锁定的时间段。 在此时间过后，该帐户将自动解锁。

c 在“状态”部分中，启用此身份验证服务器。

d （可选）配置辅助身份验证。

选项	描述
使用此服务器进行辅助身份验证	（可选）指定是否使用此服务器作为第二级身份验证。
如果身份验证失败，则终止会话	（可选）指定在身份验证失败时是否结束 VPN 会话。

e 单击**保留**。

4 （可选）要启用客户端证书身份验证，请单击**更改证书**，然后打开启用开关，选择要使用的 CA 证书并单击**确定**。

后续步骤

将本地用户添加到本地身份验证服务器，以便他们可以使用 SSL VPN-Plus 连接。请参见将 SSL VPN-Plus 用户添加到本地 SSL VPN-Plus 身份验证服务器。

创建包含 SSL 客户端的安装软件包，以便远程用户可以在自己的本地系统上进行安装。请参见添加 SSL VPN-Plus 客户端安装软件包。

将 SSL VPN-Plus 用户添加到本地 SSL VPN-Plus 身份验证服务器

可使用 **SSL VPN-Plus** 选项卡上的**用户**屏幕，将远程用户的帐户添加到 NSX Data Center for vSphere Edge 网关 SSL VPN 服务的本地身份验证服务器。

注 如果尚未配置本地身份验证服务器，则在**用户**屏幕上添加用户会自动使用默认值添加本地身份验证服务器。然后，可以使用**身份验证**屏幕上的编辑按钮查看和编辑默认值。有关使用**身份验证**屏幕的信息，请参见为 NSX Data Center for vSphere Edge 网关上的 SSL VPN-Plus 配置身份验证服务。

前提条件

导航到 SSL-VPN Plus 屏幕。

步骤

1 在 **SSL VPN-Plus** 选项卡上，单击**用户**。

2 单击**创建** () 按钮。

3 为用户配置以下选项。

选项	描述
用户 ID	输入用户 ID。
密码	输入用户的密码。
重新键入密码	重新输入密码。
名	（可选）输入用户的名字。
姓	（可选）输入用户的姓氏。
描述	（可选）输入用户描述。
已启用	指定是启用还是禁用此用户。

选项	描述
密码永不过期	（可选）指定是否始终对此用户使用相同的密码。
允许更改密码	（可选）指定是否允许用户更改密码。
下次登录时更改密码	（可选）指定是否希望此用户在下次用户登录时更改密码。

4 单击**保留**。

5 重复这些步骤以添加其他用户。

后续步骤

将本地用户添加到本地身份验证服务器，以便他们可以使用 SSL VPN-Plus 连接。请参见将 SSL VPN-Plus 用户添加到本地 SSL VPN-Plus 身份验证服务器。

创建包含 SSL 客户端的安装软件包，以便远程用户可以在自己的本地系统上进行安装。请参见添加 SSL VPN-Plus 客户端安装软件包。

添加 SSL VPN-Plus 客户端安装软件包

使用 **SSL VPN-Plus** 选项卡上的“安装软件包”屏幕为远程用户创建 SSL VPN-Plus 客户端的指定安装软件包。

可以将 SSL VPN-Plus 客户端安装软件包添加到 NSX Data Center for vSphere Edge 网关。新用户首次登录使用 VPN 连接时，会收到下载并安装此软件包的提示。添加后，这些客户端安装软件包可从 Edge 网关公共接口的 FQDN 进行下载。

您可以创建在 Windows、Linux 和 Mac 操作系统上运行的安装软件包。如果每个 SSL VPN 客户端需要不同的安装参数，请为每个配置创建一个安装软件包。

前提条件

导航到 SSL-VPN Plus 屏幕

步骤

1 在租户门户的 **SSL VPN-Plus** 选项卡上，单击**安装软件包**。

2 单击**添加** () 按钮。

3 配置安装软件包的设置。

选项	描述
配置文件名称	输入此安装软件包的配置文件名称。 此名称将显示给远程用户，以标识与 Edge 网关的此 SSL VPN 连接。
网关	输入 Edge 网关公共接口的 IP 地址或 FQDN。 所输入的 IP 地址或 FQDN 将绑定到 SSL VPN 客户端。在远程用户的本地系统上安装客户端后，该 IP 地址或 FQDN 将显示在此 SSL VPN 客户端上。 要将其他 Edge 网关上行链路接口绑定到此 SSL VPN 客户端，请单击**添加** () 按钮添加行，然后键入其接口 IP 地址或 FQDN 以及端口。

选项	描述
端口	（可选）要修改显示的默认端口值，请双击该值并输入一个新值。
Windows Linux Mac	选择操作系统以创建适用的安装软件包。
描述	（可选）为用户键入描述。
已启用	指定是启用还是禁用此软件包。

4 选择适用于 Windows 的安装参数。

选项	描述
登录时启动客户端	远程用户登录到自己的本地系统时启动 SSL VPN 客户端。
允许记住密码	让客户端记住用户密码。
启用静默模式安装	向远程用户隐藏安装命令。
隐藏 SSL 客户端网络适配器	隐藏与 SSL VPN 客户端安装软件包一起安装在远程用户计算机上的 VMware SSL VPN-Plus 适配器。
隐藏客户端系统托盘图标	隐藏指示 VPN 连接是否处于活动状态的 SSL VPN 托盘图标。
创建桌面图标	在用户桌面上创建一个用于调用 SSL 客户端的图标。
启用静默模式操作	隐藏指示安装已完成的窗口。
服务器安全证书验证	在建立安全连接前，SSL VPN 客户端会验证 SSL VPN 服务器证书。

5 单击**保留**。

后续步骤

编辑客户端配置。请参见编辑 SSL VPN-Plus 客户端配置。

编辑 SSL VPN-Plus 客户端配置

使用 **SSL VPN-Plus** 选项卡上的**客户端配置**屏幕自定义 SSL VPN 客户端通道在远程用户登录到 SSL VPN 时的响应方式。

前提条件

导航到 SSL-VPN Plus 屏幕

步骤

1 在 **SSL VPN-Plus** 选项卡上，单击**客户端配置**。

2 选择**通道模式**。

- 在拆分通道模式中，只有 VPN 流量会流过 Edge 网关。
- 在全通道模式中，Edge 网关将成为远程用户的默认网关，且所有流量（例如 VPN、本地和 Internet）都将流过 Edge 网关。

3 如果选择全通道模式，请输入远程用户的客户端使用的默认网关的 IP 地址，并且可以选择是否阻止本地子网流量流过 VPN 通道。

4 （可选） 禁用自动重新连接。

默认情况下启用**启用自动重新连接**。如果已启用自动重新连接，SSL VPN 客户端将在用户断开连接时自动重新连接这些用户。

5 （可选）（可选）启用可以升级客户端时客户端通知远程用户的功能。

默认情况下禁用此选项。如果您启用此选项，远程用户可以选择安装升级。

6 单击**保存更改**。

自定义 NSX Data Center for vSphere Edge 网关的常规 SSL VPN-Plus 设置

默认情况下，系统会在 VMware Cloud Director 环境中的 Edge 网关上设置一些 SSL VPN-Plus 设置。您可以使用 VMware Cloud Director 租户门户 **SSL VPN-Plus** 选项卡上的**常规设置**屏幕自定义这些设置。

前提条件

导航到 SSL-VPN Plus 屏幕。

步骤

1 在 **SSL VPN-Plus** 选项卡上，单击**常规设置**。

2 根据组织需求编辑常规设置。

选项	描述
禁止使用相同用户名进行多次登录	开启后可将远程用户限制为使用同一用户名仅能建立一个活动登录会话。
压缩	开启后可启用基于 TCP 的智能数据压缩并提高数据传输速度。
启用日志记录	启用后可维护通过 SSL VPN 网关的流量日志。 默认情况下启用日志记录。
强制使用虚拟键盘	启用后可要求远程用户仅使用虚拟（屏幕）键盘输入登录信息。
使虚拟键盘的按键随机排列	启用后可让虚拟键盘使用随机键布局。
会话空闲超时	输入会话空闲超时（以分钟为单位）。 如果用户会话在指定时间段内没有任何活动，系统将断开用户会话的连接。系统默认值为 10 分钟。
用户通知	键入要在远程用户登录后为其显示的消息。
启用公用 URL 访问	启用后可允许远程用户访问您没有显式配置为让远程用户访问的站点。
启用强制超时	启用后可让系统在**强制超时**字段中指定的时间段结束后断开远程用户的连接。
强制超时	键入超时期限（以分钟为单位）。 打开**启用强制超时**开关时显示此字段。

3 单击**保存更改**。

配置 IPsec VPN

VMware Cloud Director 环境中的 NSX Data Center for vSphere Edge 网关支持站点到站点 Internet 协议安全性 (IPsec)，以保护组织虚拟数据中心网络之间以及组织虚拟数据中心网络和外部 IP 地址之间的 VPN 通道。您可以在 Edge 网关上配置 IPsec VPN 服务。

最常见的方案是设置从远程网络到组织虚拟数据中心的 IPsec VPN 连接。NSX 软件提供了 Edge 网关的 IPsec VPN 功能，包括支持证书身份验证、预共享密钥模式以及自身与远程 VPN 路由器之间的 IP 单播通信。您还可以配置多个子网，以便通过 IPsec 通道连接到 Edge 网关后的内部网络。配置多个子网通过 IPsec 通道连接到内部网络时，这些子网和 Edge 网关后的内部网络不能具有重叠地址范围。

注 如果 IPsec 通道的本地和远程对等方具有重叠 IP 地址，则跨通道的流量转发可能会不一致，具体取决于是否存在本地连接的路由和自动检测到的路由。

支持以下 IPsec VPN 算法：

- AES (AES128-CBC)
- AES256 (AES256-CBC)
- Triple DES (3DES192-CBC)
- AES-GCM (AES128-GCM)
- DH-2（Diffie-Hellman 组 2）
- DH-5（Diffie-Hellman 组 5）
- DH-14（Diffie-Hellman 组 14）

注 IPsec VPN 不支持动态路由协议。在组织虚拟数据中心的 Edge 网关与远程站点的物理网关 VPN 之间配置 IPsec VPN 通道时，无法为该连接配置动态路由。Edge 网关上行链路上的动态路由无法获知该远程站点的 IP 地址。

如《NSX 管理指南》中的“IPSec VPN 概览”主题所述，Edge 网关上支持的最大通道数取决于为其配置的大小：紧凑、大型、超大型、四倍大。

要查看 Edge 网关配置的大小，请导航到该 Edge 网关，然后单击该 Edge 网关名称。

在 Edge 网关上配置 IPsec VPN 是一个多步骤过程。

注 如果通道端点之间存在防火墙，那么在配置 IPsec VPN 服务后，请更新防火墙规则，以便允许以下 IP 协议和 UDP 端口：

- IP 协议 ID 50 (ESP)
- IP 协议 ID 51 (AH)
- UDP 端口 500 (IKE)
- UDP 端口 4500

步骤

1 导航到“IPsec VPN”屏幕

在 **IPsec VPN** 屏幕中，可以开始为 NSX Data Center for vSphere Edge 网关配置 IPsec VPN 服务。

2 为 NSX Data Center for vSphere Edge 网关配置 IPsec VPN 站点连接

使用 VMware Cloud Director 租户门户中的 **IPsec VPN 站点**屏幕，配置通过 Edge 网关 IPsec VPN 功能在您的组织虚拟数据中心和另一站点之间创建 IPsec VPN 连接所需的设置。

3 在 NSX Data Center for vSphere Edge 网关上启用 IPsec VPN 服务

配置了至少一个 IPsec VPN 连接时，您可以在 Edge 网关上启用 IPsec VPN 服务。

4 指定全局 IPsec VPN 设置

可以使用**全局配置**屏幕在 Edge 网关级别配置 IPsec VPN 身份验证设置。在此屏幕上，您可以设置全局预共享密钥，并启用证书身份验证。

导航到“IPsec VPN”屏幕

在 **IPsec VPN** 屏幕中，可以开始为 NSX Data Center for vSphere Edge 网关配置 IPsec VPN 服务。

步骤

1 打开 Edge 网关服务。

a 导航到**网络** > **Edge**。

b 选择要编辑的 Edge 网关，然后单击**服务**。

2 导航到 **VPN** > **IPsec VPN**。

后续步骤

使用 **IPsec VPN 站点**屏幕配置 IPsec VPN 连接。必须配置至少一个连接，才能在 Edge 网关上启用 IPsec VPN 服务。请参见为 NSX Data Center for vSphere Edge 网关配置 IPsec VPN 站点连接。

为 NSX Data Center for vSphere Edge 网关配置 IPsec VPN 站点连接

使用 VMware Cloud Director 租户门户中的 **IPsec VPN 站点**屏幕，配置通过 Edge 网关 IPsec VPN 功能在您的组织虚拟数据中心和另一站点之间创建 IPsec VPN 连接所需的设置。

当配置站点之间的 IPsec VPN 连接时，可以从当前位置的角度配置连接。设置连接要求您了解 VMware Cloud Director 环境上下文中的概念，以便正确配置 VPN 连接。

- 本地和对等子网指定 VPN 连接到的网络。在 IPsec VPN 站点配置中指定这些子网时，输入网络范围而不是特定的 IP 地址。请使用 CIDR 格式，例如 **`192.168.99.0/24`**。
- 对等 ID 是唯一标识终止 VPN 连接的远程设备的标识符，通常是其公用 IP 地址。对于使用证书身份验证的对等站点，此 ID 必须是对等站点证书中设置的标识名。对于 PSK 对等站点，此 ID 可以是任何字符串。NSX 最佳做法是，使用远程设备的公用 IP 地址或 FQDN 作为对等 ID。如果对等 IP 地址来自其他组织虚拟数据中心网络，则请输入对等站点的本地 IP 地址。如果为对等站点配置了 NAT，则输入对等站点的专用 IP 地址。
- 对等端点指定您要连接到的远程设备的公用 IP 地址。如果不能从 Internet 直接访问对等站点的网关，而是通过另一个设备连接，则对等端点的地址可能与对等 ID 的地址不同。如果为对等站点配置了 NAT，则输入设备用于 NAT 的公用 IP 地址。
- 本地 ID 指定组织虚拟数据中心的 Edge 网关的公用 IP 地址。您可以输入 IP 地址或主机名以及 Edge 网关的防火墙。
- 本地端点指定在您的组织虚拟数据中心中 Edge 网关在其上传输数据的网络。通常情况下，Edge 网关的外部网络是本地端点。

前提条件

- 导航到“IPsec VPN”屏幕。
- 配置 IPsec VPN。
- 如果要使用全局证书作为身份验证方法，请确认在**全局配置**屏幕上已启用证书身份验证。请参见指定全局 IPsec VPN 设置。

步骤

1 打开 Edge 网关服务。

   a 导航到**网络** > **Edge**。

   b 选择要编辑的 Edge 网关，然后单击**服务**。

2 在 **IPsec VPN** 选项卡上，单击 **IPsec VPN 站点**。

3 单击**添加** () 按钮。

4 配置 IPsec VPN 连接设置。

选项	操作
已启用	在两个 VPN 端点之间启用此连接。
启用完全向前保密 (PFS)	启用此选项可以使系统为用户启动的所有 IPsec VPN 会话生成唯一的公钥。 启用 PFS 可确保系统不会在 Edge 网关的私钥和每个会话密钥之间创建链接。 会话密钥的泄露不会影响由该特定密钥保护的特定会话中交换的数据以外的数据。服务器私钥的泄露不能用于解密存档的会话或未来的会话。 启用 PFS 后，与此 Edge 网关的 IPsec VPN 连接会遇到轻微的处理开销。 **重要事项** 唯一的会话密钥不得用于派生任何其他密钥。此外，IPsec VPN 通道的两端都必须支持 PFS，它才能正常工作。
名称	（可选）输入此连接的名称。
本地 ID	输入 Edge 网关实例的外部 IP 地址，它是 Edge 网关的公用 IP 地址。 此 IP 地址将用于远程站点上 IPsec VPN 配置中的对等 ID。
本地端点	输入此连接的本地端点网络。 本地端点指定在您的组织虚拟数据中心中 Edge 网关在其上传输数据的网络。通常情况下，外部网络是本地端点。 如果您使用预共享密钥添加 IP 到 IP 通道，则本地 ID 和本地端点 IP 可以相同。
本地子网	输入要在站点之间共享的网络，并使用逗号作为分隔符输入多个子网。 通过使用 CIDR 格式输入 IP 地址来输入网络范围（而不是特定 IP 地址）；例如 **192.168.99.0/24**。
对等 ID	输入对等 ID 以唯一标识对等站点。 对等 ID 是唯一标识终止 VPN 连接的远程设备的标识符，通常是其公用 IP 地址。 对于使用证书身份验证的对等站点，ID 必须是对等站点证书中的标识名。对于 PSK 对等站点，此 ID 可以是任何字符串。NSX 最佳做法是，使用远程设备的公用 IP 地址或 FQDN 作为对等 ID。 如果对等 IP 地址来自其他组织虚拟数据中心网络，则请输入对等站点的本地 IP 地址。如果为对等站点配置了 NAT，则输入对等站点的专用 IP 地址。
对等端点	输入对等站点的 IP 地址或 FQDN，即您要连接的远程设备的公用地址。 **注** 如果为对等站点配置了 NAT，则输入设备用于 NAT 的公用 IP 地址。
对等子网	输入 VPN 连接的远程网络，并使用逗号作为分隔符输入多个子网。 通过使用 CIDR 格式输入 IP 地址来输入网络范围（而不是特定 IP 地址）；例如 **192.168.99.0/24**。
加密算法	从下拉菜单中选择加密算法类型。 **注** 您选择的加密类型必须与远程站点 VPN 设备上配置的加密类型相匹配。
身份验证	选择身份验证。选项包括： ■ **PSK** 预共享密钥 (Pre Shared Key, PSK) 指定在 Edge 网关和对等站点之间共享的密钥将用于身份验证。 ■ **证书** 证书身份验证指定在全局级别定义的证书将用于身份验证。除非您在 **IPsec VPN** 选项卡的**全局配置**屏幕上配置了全局证书，否则此选项不可用。

选项	操作
更改共享密钥	（可选）当您更新现有连接的设置时，可以启用此选项以使**预共享密钥**字段可用，以便可以更新共享密钥。
预共享密钥	如果您选择 **PSK** 作为身份验证类型，请键入一个字母数字密码字符串，该字符串的最大长度不得超过 128 字节。 **注** 共享密钥必须与远程站点 VPN 设备上配置的密钥相匹配。最佳做法是在匿名站点连接到 VPN 服务时配置共享密钥。
显示共享密钥	（可选）启用此选项以使共享密钥在屏幕中可见。
Diffie-Hellman 组	选择将允许对等站点和此 Edge 网关通过不安全的通信通道建立共享密钥的加密方案。 **注** Diffie-Hellman 组必须与远程站点 VPN 设备上的配置相匹配。
扩展	（可选）键入以下选项之一： ■ `securelocaltrafficbyip=`*IPAddress*，用于通过 IPsec VPN 通道重定向 Edge 网关本地流量。 这是默认值。 ■ `passthroughSubnets=`*PeerSubnetIPAddress*，支持重叠的子网。

5 单击**保留**。

6 单击**保存更改**。

保存操作可能需要一分钟才能完成。

后续步骤

配置远程站点的连接。您必须在连接的两端（您的组织虚拟数据中心和对等站点）配置 IPsec VPN 连接。

在此 Edge 网关上启用 IPsec VPN 服务。在配置了至少一个 IPsec VPN 连接时，您可以启用该服务。请参见在 NSX Data Center for vSphere Edge 网关上启用 IPsec VPN 服务。

在 NSX Data Center for vSphere Edge 网关上启用 IPsec VPN 服务

配置了至少一个 IPsec VPN 连接时，您可以在 Edge 网关上启用 IPsec VPN 服务。

前提条件

- 导航到“IPsec VPN”屏幕。
- 确认为此 Edge 网关配置了至少一个 IPsec VPN 连接。请参见为 NSX Data Center for vSphere Edge 网关配置 IPsec VPN 站点连接中所述的步骤。

步骤

1 在 **IPsec VPN** 选项卡上，单击**激活状态**。

2 单击 **IPsec VPN 服务状态**以启用 IPsec VPN 服务。

3 单击**保存更改**。

结果

Edge 网关 IPsec VPN 服务即处于活动状态。

指定全局 IPsec VPN 设置

可以使用**全局配置**屏幕在 Edge 网关级别配置 IPsec VPN 身份验证设置。在此屏幕上，您可以设置全局预共享密钥，并启用证书身份验证。

全局预共享密钥用于对等端点设置为**任何**的站点。

前提条件

- 如果要启用证书身份验证，请确认您至少具有一个服务证书，且在**证书**屏幕中具有相应的 CA 签名证书。自签名证书不能用于 IPsec VPN。请参见将服务证书添加到 Edge 网关。
- 导航到“IPsec VPN”屏幕。

步骤

1 打开 Edge 网关服务。

   a 导航到**网络** > **Edge**。

   b 选择要编辑的 Edge 网关，然后单击**服务**。

2 在 **IPsec VPN** 选项卡上，单击**全局配置**。

3 （可选） 设置全局预共享密钥：

   a 启用**更改共享密钥**选项。

   b 输入预共享密钥。

      全局预共享密钥 (PSK) 由对等端点设置为 `any` 的所有站点共享。如果已设置全局 PSK，则将 PSK 更改为空值并保存不会对现有设置产生任何影响。

   c （可选）（可选）启用**显示共享密钥**，以显示此预共享密钥。

   d 单击**保存更改**。

4 配置证书身份验证：

   a 打开**启用证书身份验证**。

   b 选择相应的服务证书、CA 证书和 CRL。

   c 单击**保存更改**。

后续步骤

您可以选择对 Edge 网关的 IPsec VPN 服务启用日志记录。请参见 Edge 网关的统计信息和日志。

配置 L2 VPN

VMware Cloud Director 环境中的 NSX Data Center for vSphere Edge 网关支持 L2 VPN。通过 L2 VPN，可以使虚拟机跨地域界限保留同一 IP 地址，同时又保持网络连接，从而扩展组织虚拟数据中心。可以在 Edge 网关上配置 L2 VPN 服务。

NSX Data Center for vSphere 为 Edge 网关提供了 L2 VPN 功能。通过 L2 VPN，可以在两个站点之间配置通道。尽管虚拟机在这些站点之间移动，但其仍在同一子网中，因此您可以通过使用 L2 VPN 延伸网络来扩展您的组织虚拟数据中心。一个站点上的 Edge 网关可以为另一个站点上的虚拟机提供所有服务。

要创建 L2 VPN 通道，需要配置 L2 VPN 服务器和 L2 VPN 客户端。如《NSX 管理指南》中所述，L2 VPN 服务器是目标 Edge 网关，L2 VPN 客户端是源 Edge 网关。配置每个 Edge 网关上的 L2 VPN 设置后，您必须启用服务器和客户端上的 L2 VPN 服务。

注 创建为子接口的路由组织虚拟数据中心网络必须存在于 Edge 网关上。

导航到“L2 VPN”屏幕

要开始为 NSX Data Center for vSphere Edge 网关配置 L2 VPN 服务，必须导航到 **L2 VPN** 屏幕。

步骤

1 打开 Edge 网关服务。

   a 导航到**网络** > **Edge**。

   b 选择要编辑的 Edge 网关，然后单击**服务**。

2 导航到 **VPN** > **L2 VPN**。

后续步骤

配置 L2 VPN 服务器。请参见将 NSX Data Center for vSphere Edge 网关配置为 L2 VPN 服务器。

将 NSX Data Center for vSphere Edge 网关配置为 L2 VPN 服务器

L2 VPN 服务器是 L2 VPN 客户端将连接到的目标 NSX Edge。

如《NSX 管理指南》中所述，您可以将多个对等站点连接到此 L2 VPN 服务器。

注 更改站点配置设置会导致 Edge 网关断开连接并重新连接所有现有连接。

前提条件

- 确认 Edge 网关具有一个路由组织虚拟数据中心网络，并且该网络已配置为此 Edge 网关的子接口。
- 导航到“L2 VPN”屏幕。
- 如果您要将服务证书绑定到 L2 VPN 连接，请确认已将服务器证书上载到 Edge 网关。请参见将服务证书添加到 Edge 网关。
- 启用 L2 VPN 服务之前，您必须配置服务器的侦听器 IP、侦听器端口、加密算法及至少一个对等站点。

步骤

1 在 **L2 VPN** 选项卡上，选择**服务器**作为 L2 VPN 模式。

2 在**服务器全局**选项卡上，配置 L2 VPN 服务器的全局配置详细信息。

选项	操作
侦听器 IP	选择 Edge 网关的外部接口的主或辅助 IP 地址。
侦听器端口	根据组织需求编辑显示的值。 L2 VPN 服务的默认端口是 443。
加密算法	选择服务器和客户端之间通信的加密算法。
服务证书详细信息	单击**更改服务器证书**，选择要绑定到 L2 VPN 服务器的证书。 在**更改服务器证书**窗口中，启用**验证服务器证书**，从列表中选择服务器证书，并单击**确定**。

3 要配置对等站点，请单击**服务器站点**选项卡。

4 单击**添加** () 按钮。

5 配置 L2 VPN 对等站点的设置。

选项	操作
已启用	启用此对等站点。
名称	输入对等站点的唯一名称。
描述	（可选）键入描述。
用户 ID **密码** **确认密码**	输入用于对对等站点进行身份验证的用户名和密码。 对等站点上的用户凭据必须与客户端上的凭据相同。
延伸接口	至少选择一个要使用客户端延伸的子接口。 可供选择的子接口是 Edge 网关上配置为子接口的组织虚拟数据中心网络。
输出优化网关地址	（可选）如果虚拟机的默认网关在两个站点上相同，请输入您希望通过 L2 VPN 通道在本地路由或阻止流量的子接口的网关 IP 地址。

6 单击**保留**。

7 单击**保存更改**。

保存操作可能需要一分钟才能完成。

后续步骤

在此 Edge 网关上启用 L2 VPN 服务。请参见在 NSX Data Center for vSphere Edge 网关上启用 L2 VPN 服务。

将 NSX Data Center for vSphere Edge 网关配置为 L2 VPN 客户端

L2 VPN 客户端是源 NSX Edge，它发起与目标 NSX Edge（即 L2 VPN 服务器）的通信。

前提条件

- 导航到“L2 VPN”屏幕。

- 如果此 L2 VPN 客户端连接到使用服务器证书的 L2 VPN 服务器，请确认已将相应的 CA 证书上载到 Edge 网关，以针对此 L2 VPN 客户端启用服务器证书验证。请参见将 CA 证书添加到 Edge 网关进行 SSL 证书信任验证。

步骤

1 在 **L2 VPN** 选项卡上，选择**客户端**作为 L2 VPN 模式。

2 在**客户端全局**选项卡上，配置 L2 VPN 客户端的全局配置详细信息。

选项	描述
服务器地址	输入要将此客户端连接到的 L2 VPN 服务器的 IP 地址。
服务器端口	输入客户端应连接到的 L2 VPN 服务器端口。 默认端口为 443。
加密算法	选择用于与服务器通信的加密算法。
延伸接口	选择要延伸到服务器的子接口。 可供选择的子接口是 Edge 网关上配置为子接口的组织虚拟数据中心网络。
输出优化网关地址	（可选）如果虚拟机在两个站点上的默认网关相同，请键入子接口的网关 IP 地址或流量不应通过通道流入的 IP 地址。
用户详细信息	输入用于向该服务器进行身份验证的用户 ID 和密码。

3 单击**保存更改**。

保存操作可能需要一分钟才能完成。

4 （可选） 要配置高级选项，请单击**客户端高级**选项卡。

5 如果此 L2 VPN 客户端 Edge 无法直接访问 Internet，而必须使用代理服务器访问 L2 VPN 服务器 Edge，请指定代理设置。

选项	描述
启用安全代理	选择后可启用安全代理。
地址	输入代理服务器的 IP 地址。
端口	输入代理服务器的端口。
用户名 **密码**	输入代理服务器的身份验证凭据。

6 要启用服务器证书验证，请单击**更改 CA 证书**，然后选择相应的 CA 证书。

7 单击**保存更改**。

保存操作可能需要一分钟才能完成。

后续步骤

在此 Edge 网关上启用 L2 VPN 服务。请参见在 NSX Data Center for vSphere Edge 网关上启用 L2 VPN 服务。

在 NSX Data Center for vSphere Edge 网关上启用 L2 VPN 服务

配置所需的 L2 VPN 设置后，可以在 Edge 网关上启用 L2 VPN 服务。

注 如果已在此 Edge 网关上配置 HA，请确保此 Edge 网关上配置了多个内部接口。如果只存在一个接口，并且已由 HA 功能使用，则在同一内部接口上配置 L2 VPN 将失败。

前提条件

- 如果此 Edge 网关是 L2 VPN 服务器，即目标 NSX Edge，请确认已配置所需的 L2 VPN 服务器设置以及至少一个 L2 VPN 对等站点。请参见将 NSX Data Center for vSphere Edge 网关配置为 L2 VPN 服务器中所述的步骤。
- 如果此 Edge 网关是 L2 VPN 客户端，即源 NSX Edge，请确认已配置 L2 VPN 客户端设置。请参见将 NSX Data Center for vSphere Edge 网关配置为 L2 VPN 客户端中所述的步骤。
- 导航到“L2 VPN”屏幕。

步骤

1 在 **L2 VPN** 选项卡上，单击**启用**开关。

2 单击**保存更改**。

结果

Edge 网关的 L2 VPN 服务将处于活动状态。

后续步骤

在面向 Internet 的防火墙端创建 NAT 或防火墙规则，从而让 L2 VPN 服务器能够连接到 L2 VPN 客户端。

从 NSX Data Center for vSphere Edge 网关中移除 L2 VPN 服务配置

您可以移除 Edge 网关的现有 L2 VPN 服务配置。此操作还会禁用 Edge 网关上的 L2 VPN 服务。

前提条件

导航到“L2 VPN”屏幕

步骤

1 向下滚动到 L2 VPN 屏幕底部，然后单击**删除配置**。

2 单击**确定**，确认删除。

结果

L2 VPN 服务将被禁用，配置详细信息将从 Edge 网关中移除。

SSL 证书管理

借助 VMware Cloud Director 环境中的 NSX 软件，您可以将安全套接字层 (Secure Sockets Layer, SSL) 证书与为 Edge 网关配置的 SSL VPN-Plus 和 IPsec VPN 通道搭配使用。

您的 VMware Cloud Director 环境中的 Edge 网关支持自签名证书、证书颁发机构 (Certification Authority, CA) 签名证书以及由 CA 生成和签名的证书。您可以生成证书签名请求 (CSR)、导入证书、管理已导入的证书，并创建证书撤销列表 (CRL)。

关于在组织虚拟数据中心使用证书

您可以在 VMware Cloud Director 组织虚拟数据中心中管理以下网络连接方面的证书。

- 组织虚拟数据中心网络和远程网络之间的 IPsec VPN 通道。
- 专用网络的远程用户和组织虚拟数据中心中的 Web 资源之间的 SSL VPN-Plus 连接。
- 两个 NSX Edge 网关之间的 L2 VPN 通道。
- 组织虚拟数据中心中为负载平衡配置的虚拟服务器和池服务器

如何使用客户端证书

您可以通过 CAI 命令或 REST 调用创建客户端证书。随后，您可以将此证书分发给您的远程用户，要求他们将证书安装在其 Web 浏览器上。

实施客户端证书的主要优势在于，可以保存每个远程用户各自的引用客户端证书，并将该证书与远程用户提供的客户端证书进行对照检查。为防止某位用户以后未经授权连接服务器，您可以将其引用证书从安全服务器的客户端证书列表中删除。删除证书后即可拒绝来自该用户的连接请求。

为 Edge 网关生成证书签名请求

从 CA 订购签名证书或创建自签名证书之前，必须为 Edge 网关生成证书签名请求 (CSR)。

CSR 是一种经过编码的文件，需要在要求 SSL 证书的 NSX Edge 网关上生成。使用 CSR 可标准化公司发送其公钥以及用来标识其公司名称和域名的信息的方式。

您使用匹配的私钥文件（必须保留在 Edge 网关上）生成 CSR。CSR 包含匹配的公钥和其他信息，例如您组织的名称、位置和域名。

步骤

1 打开 Edge 网关服务。

   a 导航到**网络** > **Edge**。

   b 选择要编辑的 Edge 网关，然后单击**服务**。

2 单击**证书**选项卡。

3 在**证书**选项卡中，单击 **CSR**。

4 为 CSR 配置以下选项：

选项	描述
公用名称	输入要使用该证书的组织的完全限定域名 (FQDN)（例如 `www.example.com`）。 请勿在公用名称中包含 `http://` 或 `https://` 前缀。
组织单位	使用此字段可区分与此证书关联的 VMware Cloud Director 组织内的部门。例如，工程部门或销售部门。
组织名称	输入您公司合法注册的名称。 列出的组织必须是证书请求中域名的合法注册人。
地点	输入您公司合法注册的城市或地点。
省/市/自治区名称	输入您公司合法注册的省/市/自治区、地区或领地的完整名称（不要使用缩写）。
国家/地区代码	输入您公司合法注册的国家/地区名称。
私钥算法	键入证书的密钥类型，RSA 或 DSA。 通常使用 RSA。密钥类型定义在主机之间通信的加密算法。 **注** SSL VPN-Plus 仅支持 RSA 证书。
密钥大小	输入密钥大小（位）。 最小值为 2048 位。
描述	（可选）输入证书描述。

5 单击**保留**。

系统将生成 CSR，并将类型为“CSR”的一个新条目添加到屏幕上的列表中。

结果

在屏幕列表中，选择类型为“CSR”的条目时，将在屏幕上显示 CSR 详细信息。您可以复制 CSR 显示的 PEM 格式数据并将其提交给证书颁发机构 (CA) 以获取 CA 签名证书。

后续步骤

使用 CSR 通过以下两种方法之一创建服务证书：

- 将 CSR 传输到 CA 以获取 CA 签名证书。CA 向您发送签名证书后，将该签名证书导入到系统。请参见导入与为 Edge 网关生成的 CSR 对应的 CA 签名证书。
- 使用 CSR 创建自签名证书。请参见配置自签名服务证书。

导入与为 Edge 网关生成的 CSR 对应的 CA 签名证书

在生成证书签名请求 (CSR) 并根据该 CSR 获取 CA 签名证书后，您可以导入该 CA 签名证书，以供 Edge 网关使用。

前提条件

确认您已获取与 CSR 对应的 CA 签名证书。如果 CA 签名证书中的私钥与用于所选 CSR 的私钥不匹配，则导入过程将失败。

步骤

1 打开 Edge 网关服务。

   a 导航到**网络** > **Edge**。

   b 选择要编辑的 Edge 网关，然后单击**服务**。

2 单击**证书**选项卡。

3 从屏幕上的表中选择 CSR 以导入与其对应的 CA 签名证书。

4 导入签名证书。

   a 单击**已为 CSR 生成签名证书**。

   b 提供 CA 签名证书的 PEM 数据。

      - 如果此数据位于系统上您可以导航到的某个 PEM 文件中，请单击**上载**按钮以浏览到该文件并选择。
      - 如果您可以复制和粘贴 PEM 数据，请将其粘贴到**签名证书 (PEM 格式)** 字段中。

        包括 **-----BEGIN CERTIFICATE-----** 和 **-----END CERTIFICATE-----** 行。

   c （可选）键入描述。

   d 单击**保留**。

   注 如果 CA 签名证书中的私钥与用于在“证书”屏幕上选择的 CSR 的私钥不匹配，则导入过程将失败。

结果

类型为“服务证书”的 CA 签名证书将显示在屏幕上的列表中。

后续步骤

根据需要将 CA 签名证书连接到您的 SSL VPN-Plus 或 IPsec VPN 通道。请参见配置 SSL VPN 服务器设置和指定全局 IPsec VPN 设置。

配置自签名服务证书

您可以对 Edge 网关配置自签名服务证书，以便在其 VPN 相关功能中使用。您可以创建、安装和管理自签名证书。

如果“证书”屏幕上存在服务证书，则可以在配置 Edge 网关的 VPN 相关设置时指定该服务证书。VPN 会将指定的服务证书提供给访问 VPN 的客户端。

前提条件

确认在 Edge 网关的**证书**屏幕上至少有一个 CSR 可用。请参见为 Edge 网关生成证书签名请求。

步骤

1 打开 Edge 网关服务。

a 导航到**网络** > **Edge**。

b 选择要编辑的 Edge 网关，然后单击**服务**。

2 单击**证书**选项卡。

3 从列表中选择要用于此自签名证书的 CSR，然后单击**自签名 CSR**。

4 键入自签名证书的有效天数。

5 单击**保留**。

系统将生成自签名证书，并将一个类型为“服务证书”的新条目添加到屏幕上的列表中。

结果

自签名证书可用于 Edge 网关。在屏幕上的列表中，当您选择类型为“服务证书”的条目时，将在屏幕上显示其详细信息。

将 CA 证书添加到 Edge 网关进行 SSL 证书信任验证

将 CA 证书添加到 Edge 网关可以对提供给 Edge 网关进行身份验证的 SSL 证书进行信任验证，通常为 Edge 网关的 VPN 连接中使用的客户端证书。

通常将公司或组织的根证书作为 CA 证书添加。一个典型用途是用于 SSL VPN，即需要使用证书对 VPN 客户端进行身份验证。可以将客户端证书分发到 VPN 客户端，当 VPN 客户端连接时，将根据 CA 证书验证其客户端证书。

注 添加 CA 证书时，通常可以配置相关的证书吊销列表 (Certificate Revocation List, CRL)。CRL 可防止客户端提供已吊销的证书。请参见将证书吊销列表添加到 Edge 网关。

前提条件

确认您的 CA 证书数据采用 PEM 格式。在用户界面中，可以粘贴 CA 证书的 PEM 数据，或者浏览到包含该数据且可从本地系统的网络中获得的文件。

步骤

1 打开 Edge 网关服务。

a 导航到**网络** > **Edge**。

b 选择要编辑的 Edge 网关，然后单击**服务**。

2 单击**证书**选项卡。

3 单击 **CA 证书**。

4 提供 CA 证书数据。

- 如果此数据位于系统上您可以导航到的某个 PEM 文件中，请单击**上载**按钮以浏览到该文件并选择。

- 如果您可以复制和粘贴 PEM 数据，请将其粘贴到 **CA 证书 (PEM 格式)** 字段中。

  包括 **-----BEGIN CERTIFICATE-----** 和 **-----END CERTIFICATE-----** 行。

5 （可选）键入描述。

6 单击**保留**。

结果

类型为“CA 证书”的 CA 证书将显示在屏幕上的列表中。现在，您可以在配置 Edge 网关的 VPN 相关设置时指定该 CA 证书。

将证书吊销列表添加到 Edge 网关

证书吊销列表 (CRL) 是指证书颁发机构 (CA) 声明要吊销的数字证书列表，以便可以在更新系统后不再信任提供这些已吊销证书的用户。可以将 CRL 添加到 Edge 网关。

如《NSX 管理指南》中所述，CRL 包含以下各项：

- 已吊销证书以及吊销原因
- 证书颁发日期
- 颁发证书的实体
- 下一个版本的计划日期

当潜在用户尝试访问服务器时，服务器会根据针对该特定用户的 CRL 条目允许或拒绝访问。

步骤

1 打开 Edge 网关服务。

  a 导航到**网络** > **Edge**。

  b 选择要编辑的 Edge 网关，然后单击**服务**。

2 单击**证书**选项卡。

3 单击 **CRL**。

4 提供 CRL 数据。

  - 如果此数据位于系统上您可以导航到的某个 PEM 文件中，请单击**上载**按钮以浏览到该文件并选择。
  - 如果您可以复制和粘贴 PEM 数据，请将其粘贴到 **CRL (PEM 格式)** 字段中。

    包括 **-----BEGIN X509 CRL-----** 和 **-----END X509 CRL-----** 行。

5 （可选）键入描述。

6 单击**保留**。

结果

CRL 将显示在屏幕上的列表中。

将服务证书添加到 Edge 网关

将服务证书添加到 Edge 网关后，在配置 Edge 网关的 VPN 相关设置时可以使用这些证书。您可以将服务证书添加到**证书**屏幕中。

前提条件

确认您拥有服务证书以及 PEM 格式的专用密钥。在用户界面中，可以粘贴 PEM 数据，或者浏览到包含该数据且可从本地系统的网络中获得的文件。

步骤

1 打开 Edge 网关服务。

   a 导航到**网络** > **Edge**。

   b 选择要编辑的 Edge 网关，然后单击**服务**。

2 单击**证书**选项卡。

3 单击**服务证书**。

4 输入服务证书的 PEM 格式数据。

   - 如果此数据位于系统上您可以导航到的某个 PEM 文件中，请单击**上载**按钮以浏览到该文件并选择。
   - 如果您可以复制和粘贴 PEM 数据，请将其粘贴到**服务证书 (PEM 格式)** 字段中。

     包括 **-----BEGIN CERTIFICATE-----** 和 **-----END CERTIFICATE-----** 行。

5 输入证书私钥的 PEM 格式数据。

   - 如果此数据位于系统上您可以导航到的某个 PEM 文件中，请单击**上载**按钮以浏览到该文件并选择它。
   - 如果您可以复制和粘贴 PEM 数据，请将其粘贴到**私钥 (PEM 格式)** 字段中。

     包括 **-----BEGIN RSA PRIVATE KEY-----** 和 **-----END RSA PRIVATE KEY-----** 行。

6 输入专用密钥密码短语并进行确认。

7 （可选） 键入描述。

8 单击**保留**。

结果

类型为“服务证书”的证书将显示在屏幕上的列表中。现在，您可以在配置 Edge 网关的 VPN 相关设置时选择该服务证书。

自定义分组对象

VMware Cloud Director 环境中的 NSX 软件提供了定义特定实体的集和组的功能，随后您可以在指定其他网络相关配置时使用这些集和组（例如在防火墙规则中）。

创建供防火墙规则和 DHCP 中继配置使用的 IP 集

IP 集是一组可在组织虚拟数据中心级别创建的 IP 地址。您可以在防火墙规则或 DHCP 中继配置中使用 IP 集作为源或目标。

您可以使用 VMware Cloud Director 租户门户的**分组对象**页面创建 IP 集。“服务”和“Edge 网关”屏幕上都提供了**分组对象**页面。

步骤

1 打开“分组对象”页面。

选项	操作
通过 Edge 网关服务打开	a 导航到**网络 > Edge**。 b 选择要编辑的 Edge 网关，然后单击**配置服务**。 c 单击**分组对象**。
通过安全服务打开	a 导航到**网络 > 安全**。 b 选择要编辑的安全服务，然后单击**配置服务**。 c 单击**分组对象**。

2 单击 **IP 集**选项卡。

在屏幕上将显示已定义的 IP 集。

3 要添加 IP 集，请单击**创建**（  ）按钮。

4 输入 IP 集的名称和（可选）描述，以及要包含在此集中的 IP 地址。

5 （可选） 如果要使用“服务”屏幕上的**分组对象**页面指定 IP 集，请使用**继承**开关以启用继承并允许在底层范围内查看。

默认情况下启用继承。

6 要保存此 IP 集，单击**保留**。

结果

新的 IP 集可在防火墙规则或 DHCP 中继配置中作为源或目标供选择。

创建供防火墙规则使用的 MAC 集

MAC 集是一组可在组织虚拟数据中心级别创建的 MAC 地址。可以将 MAC 集用作防火墙规则中的源或目标。

您可以使用 VMware Cloud Director 租户门户的**分组对象**页面创建 MAC 集。**服务**和 **Edge 网关**屏幕均提供有“分组对象”页面。

步骤

1 打开“分组对象”页面。

选项	操作
通过 Edge 网关服务打开	a 导航到**网络 > Edge**。 b 选择要编辑的 Edge 网关，然后单击**配置服务**。 c 单击**分组对象**。
通过安全服务打开	a 导航到**网络 > 安全**。 b 选择要编辑的安全服务，然后单击**配置服务**。 c 单击**分组对象**。

2 单击 **MAC 集**选项卡。

在屏幕上将显示已定义的 MAC 集。

3 要添加 MAC 集，请单击**创建** () 按钮。

4 输入 MAC 集的名称、可选描述，以及 MAC 集中要包含的 MAC 地址。

5 （可选） 如果您要使用**服务**屏幕上的**分组对象**页面指定 MAC 集，请使用**继承**开关启用继承，以便可在底层范围查看到。

默认情况下启用继承。

6 要保存 MAC 集，请单击**保留**。

结果

新 MAC 集可作为防火墙规则中的源或目标供选择。

查看可用于防火墙规则的服务

可以查看可在防火墙规则中使用的服务列表。在此环境下，服务是协议与端口的组合。

您可以使用 VMware Cloud Director 租户门户的“分组对象”页面查看可用的服务。“服务”和“Edge 网关”屏幕均提供有“分组对象”页面。

您无法使用租户门户向列表中添加新服务。可供您使用的一组服务由您的 VMware Cloud Director 系统管理员进行管理。

步骤

1 打开“分组对象”页面。

选项	操作
通过 Edge 网关服务打开	a 导航到**网络 > Edge**。 b 选择要编辑的 Edge 网关，然后单击**配置服务**。 c 单击**分组对象**。
通过安全服务打开	a 导航到**网络 > 安全**。 b 选择要编辑的安全服务，然后单击**配置服务**。 c 单击**分组对象**。

2 单击**服务**选项卡。

结果

可用的服务将显示在屏幕上。

查看可用于防火墙规则的服务组

可以查看可在防火墙规则中使用的服务组列表。在此环境下，服务是协议与端口的组合，服务组为一组服务或其他服务组。

您可以使用 VMware Cloud Director 租户门户的“分组对象”页面查看可用的服务组。“服务”和“Edge 网关”屏幕均提供有“分组对象”页面。

您无法使用租户门户创建服务组。可供您使用的一组服务组由您的 VMware Cloud Director 系统管理员进行管理。

步骤

1 打开“分组对象”页面。

选项	操作
通过 Edge 网关服务打开	a 导航到**网络 > Edge**。 b 选择要编辑的 Edge 网关，然后单击**配置服务**。 c 单击**分组对象**。
通过安全服务打开	a 导航到**网络 > 安全**。 b 选择要编辑的安全服务，然后单击**配置服务**。 c 单击**分组对象**。

2 单击**服务组**选项卡。

结果

可用的服务组将显示在屏幕上。“描述”列显示每个服务组中已分组的服务。

Edge 网关的统计信息和日志

您可以查看 Edge 网关的统计信息和日志。

查看统计信息

可以在 **Edge 网关服务**屏幕上查看统计信息。

步骤

1 打开 Edge 网关服务。

a 导航到**网络** > **Edge**。

b 选择要编辑的 Edge 网关，然后单击**服务**。

2 单击**统计信息**选项卡。

3 根据要查看的统计信息的类型浏览选项卡。

选项	描述
连接	通过“连接”屏幕可以了解运维状况。该屏幕将显示流过所选 Edge 网关的接口的流量图以及防火墙与负载平衡器服务的连接统计信息。 选择要查看统计信息的时间段。
IPsec VPN	“IPsec VPN”屏幕显示了 IPsec VPN 的状态和统计信息以及每个通道的状态和统计信息。
L2 VPN	“L2 VPN”屏幕显示 L2 VPN 状态和统计信息。

启用日志记录

您可以为 Edge 网关启用日志记录。要完成配置，除了为要收集其日志数据的功能启用日志记录外，您还必须具有 Syslog 服务器用来接收收集的日志数据。在“Edge 设置”屏幕上配置 Syslog 服务器时，您可以从该 Syslog 服务器访问已记录的日志数据。

前提条件

此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。

步骤

1 打开 Edge 网关服务。

a 导航到**网络** > **Edge**。

b 选择要编辑的 Edge 网关，然后单击**服务**。

2 在 **Edge 设置**选项卡中，单击**编辑 Syslog 服务器**按钮。

可以针对已启用日志记录的服务自定义 Edge 网关网络连接相关日志的 Syslog 服务器。

如果 VMware Cloud Director 系统管理员已为 VMware Cloud Director 环境配置了 Syslog 服务器，则系统默认使用该 Syslog 服务器，其 IP 地址将显示在 **Edge 设置**屏幕上。

3 启用每个功能的日志记录。

- 在 **NAT** 选项卡中，单击 **DNAT 规则**按钮，然后打开**启用日志记录**开关。

  记录地址转换。
- 在 **NAT** 选项卡中，单击 **SNAT 规则**按钮，然后打开**启用日志记录**开关。

  记录地址转换。
- 在**路由**选项卡中，单击**路由配置**，然后在“动态路由配置”下打开**启用日志记录**开关。

  记录动态路由活动。从**日志级别**下拉菜单中，您可以选择要记录的消息状态级别的下限。
- 在**负载平衡器**选项卡中，单击**全局配置**，然后打开**启用日志记录**开关。

  记录负载平衡器的流量。从**日志级别**下拉菜单中，您可以选择要记录的消息状态级别的下限。
- 在 **VPN** 选项卡中，导航到 **IPSec VPN > 日志记录设置**，然后打开**启用日志记录**开关。

  记录本地子网和对等子网之间的流量。从**日志级别**下拉菜单中，您可以选择要记录的消息状态级别的下限。
- 在 **SSL VPN-Plus** 选项卡中，单击**常规设置**，然后打开**启用日志记录**开关。

  保留通过 SSL VPN 网关的流量日志。
- 在 **SSL VPN-Plus** 选项卡中，单击**服务器设置**，然后打开**启用日志记录**开关。

  记录 SSL VPN 服务器上发生的 Syslog 活动。从**日志级别**下拉菜单中，您可以选择要记录的消息状态级别的下限。

启用对 Edge 网关的 SSH 命令行访问

您可以启用对 Edge 网关的 SSH 命令行访问。

步骤

1 打开 Edge 网关服务。

a 导航到**网络** > **Edge**。

b 选择要编辑的 Edge 网关，然后单击**服务**。

2 单击 **Edge 设置**选项卡。

3 配置 SSH 设置。

选项	描述
用户名 **密码** **重新键入密码**	输入对此 Edge 网关进行 SSH 访问所需的凭据。 默认情况下，SSH 用户名是 **admin**。
密码到期	输入密码的到期期限（以天为单位）
登录横幅	输入当用户开始与 Edge 网关的 SSH 连接时向用户显示的文本。

4 打开**已启用**开关。

后续步骤

配置相应的 NAT 或防火墙规则，以允许对此 Edge 网关进行 SSH 访问。

使用安全标记

安全标记是可与一台或一组虚拟机相关联的标签。安全标记旨在与安全组配合使用。创建安全标记后，可以将其与可在防火墙规则中使用的安全组相关联。您可以创建、编辑或分配用户定义的安全标记。也可以查看哪些虚拟机或安全组已应用特定的安全标记。

安全标记的常见用例是动态分组对象以简化防火墙规则。例如，您可能根据给定虚拟机上预期发生的活动类型来创建多个不同的安全标记。您为数据库服务器创建一个安全标记，为电子邮件服务器创建另一个安全标记，然后将相应的标记应用于托管数据库服务器或电子邮件服务器的虚拟机。以后，您可以将标记分配给安全组并根据其编写一个防火墙规则，根据虚拟机运行的是数据库服务器还是电子邮件服务器来应用不同的安全设置。如果您以后更改虚拟机的功能，则可以从安全标记中移除虚拟机，而无需编辑防火墙规则。

创建并分配安全标记

您可以创建安全标记，并将其分配给一台虚拟机或一组虚拟机。

您可以创建安全标记，并将其分配给一台虚拟机或一组虚拟机。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后在**网络**下选择**安全**。

2 选择一个安全服务，然后单击**配置服务**。

3 单击**安全标记**选项卡。

4 单击**创建** () 按钮，然后输入安全标记的名称。

5 （可选） 输入安全标记的描述。

6 （可选） 将安全标记分配给一台虚拟机或一组虚拟机。

在**浏览以下类型的对象**下拉菜单中，**虚拟机**默认处于选中状态。

a 从左侧面板中选择虚拟机。

b 单击向右箭头，将安全标记分配给选定的虚拟机。

该虚拟机将移至右侧面板，并获得此安全标记。

7 完成将标记分配给所选虚拟机后，单击**保留**。

结果

此时安全标记已创建，并且已分配给选定的虚拟机（如果选择）。

后续步骤

安全标记设计为与安全组配合使用。有关创建安全组的详细信息，请参见创建安全组。

更改安全标记分配

创建安全标记后，可以手动将其分配给虚拟机。还可以编辑安全标记，以将其从已分配给的虚拟机中移除。

如果已创建安全标记，则可以将其分配给虚拟机。您可以使用安全标记分组虚拟机，以便编写防火墙规则。例如，您可以将安全标记分配给一组具有高度敏感数据的虚拟机。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后在**网络**下选择**安全**。

2 选择一个安全服务，然后单击**配置服务**。

3 单击**安全标记**选项卡。

4 从安全标记列表中，选择要编辑的安全标记，然后单击**编辑** () 按钮。

5 选择左侧面板中的虚拟机，然后通过单击向右箭头为其分配安全标记。

右侧面板中的虚拟机将被分配给安全标记。

6 选择右侧面板中的虚拟机，然后通过单击向左箭头从这些虚拟机中移除该标记。

左侧面板中的虚拟机没有分配安全标记。

7 添加完更改后，单击**保留**。

结果

此时安全标记将分配给所选虚拟机。

后续步骤

安全标记设计为与安全组配合使用。有关创建安全组的详细信息，请参见创建安全组。

查看应用的安全标记

您可以查看应用于所处环境中的虚拟机的安全标记。此外，还可以查看应用于所处环境中的安全组的安全标记。

前提条件

安全标记必须已经创建完毕并已应用于虚拟机或安全组。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后在**网络**下选择**安全**。

2 选择一个安全服务，然后单击**配置服务**。

3 查看从**安全标记**选项卡分配的标记。

a 在**安全标记**选项卡上，选择要查看其分配情况的安全标记，然后单击**编辑**按钮。

b 在**分配/取消分配 VM** 下，您可以查看分配给安全标记的虚拟机的列表。

c 单击**放弃**。

4 从**安全组**选项卡查看分配的标记。

a 单击**分组对象**选项卡，然后单击**安全组**。

b 选择一个安全组。

c 从**包括成员**下的列表中，您可以查看分配给安全组的安全标记。

结果

您可以查看现有安全标记以及关联的虚拟机和安全组。这样，您可以确定一种策略来根据安全标记和安全组创建防火墙规则。

编辑安全标记

您可以编辑用户定义的安全标记。

如果您要更改虚拟机的环境或功能，则可能还需要使用其他安全标记，以便防火墙规则适用于新的虚拟机配置。例如，如果您的虚拟机不再存储敏感数据，则可能需要分配一个不同的安全标记，以便不再对该虚拟机运行适用于敏感数据的防火墙规则。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后在**网络**下选择**安全**。

2 选择一个安全服务，然后单击**配置服务**。

3 单击**安全标记**选项卡。

4 从安全标记列表中选择要编辑的安全标记。

5 单击**编辑** () 按钮。

6 编辑安全标记的名称和描述。

7 将标记分配给您选择的虚拟机或从中移除分配。

8 要保存更改，请单击**保留**。

后续步骤

如果您编辑安全标记，可能还需要编辑关联的安全组或防火墙规则。有关安全组的详细信息，请参见使用安全组

。

删除安全标记

您可以删除用户定义的安全标记。

如果虚拟机的功能或环境发生改变，则可能需要删除安全标记。例如，如果您为 Oracle 数据库设置了安全标记，但您决定使用其他数据库服务器，则可以移除该安全标记，以便不再对虚拟机运行适用于 Oracle 数据库的防火墙规则。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后在**网络**下选择**安全**。

2 选择一个安全服务，然后单击**配置服务**。

3 单击**安全标记**选项卡。

4 从安全标记列表中选择要删除的安全标记。

5 单击**删除** () 按钮。

6 单击**确定**，确认删除。

结果

安全标记将被删除。

后续步骤

如果要删除安全标记，则可能需要同时编辑关联的安全组或防火墙规则。有关安全组的详细信息，请参见使用安全组

使用安全组

安全组是指一组资产或分组对象（如虚拟机、组织虚拟数据中心网络或安全标记）。

安全组可以根据安全标记、虚拟机名称、虚拟机客户机操作系统名称或虚拟机客户机主机名称设立动态成员资格条件。例如，具有安全标记“web”的所有虚拟机将自动添加到以 Web 服务器为目标的特定安全组。创建安全组后，即会为该组应用一项安全策略。

创建安全组

您可以创建用户定义的安全组。

前提条件

如果要将安全标记与安全组配合使用，请参见创建并分配安全标记。

步骤

1 打开安全服务。

a 导航到**网络 > 安全**。

b 选择要应用安全设置的组织 VDC，然后单击**配置服务**。

租户门户将打开“安全服务”。

2 导航到**分组对象 > 安全组**

安全组页面随即打开。

3 单击**创建** () 按钮。

4 输入安全组的名称，还可以选择输入相关描述。

此描述将显示在安全组列表中，因此添加一个有意义的描述有助于一目了然地识别此安全组。

5 （可选） 添加动态成员集。

a 单击“动态成员集”下方的**添加** () 按钮。

b 选择在语句中是否匹配**任何**或**全部**条件。

c 输入要匹配的第一个对象。

选项包括**安全标记**、**VM 客户机操作系统名称**、**VM 名称**和 **VM 客户机主机名称**。

d 选择运算符，如**包含**、**开头为**或**结尾为**。

e 输入值。

f （可选） 要添加另一个语句，请使用布尔运算符**与**或者**或**。

6 （可选） 包括成员。

a 从**浏览以下类型的对象**下拉菜单中，选择对象类型，如**虚拟机**、**组织 VDC 网络**、**IP 集**、**MAC 集**或**安全标记**。

b 要在“包括成员”列表中添加一个对象，请从左侧面板中选择该对象，然后单击向右箭头，将其移到右侧面板。

7 （可选） 排除成员。

a 从**浏览以下类型的对象**下拉菜单中，选择对象类型，如**虚拟机**、**组织 VDC 网络**、**IP 集**、**MAC 集**或**安全标记**。

b 要在“排除成员”列表中包括某个对象，请从左侧面板中选择该对象，然后单击向右箭头，将其移到右侧面板。

8 单击**保存留**以保留更改。

该操作可能需要一分钟才能完成。

结果

现在，可以在规则中使用该安全组了，例如防火墙规则。

编辑安全组

您可以编辑用户定义的安全组。

步骤

1 打开安全服务。

a 导航到**网络 > 安全**。

b 选择要应用安全设置的组织 VDC，然后单击**配置服务**。

租户门户将打开“安全服务”。

2 导航到**分组对象 > 安全组**

安全组页面随即打开。

3 选择要编辑的安全组。

该安全组的详细信息将显示在安全组列表的下方。

4 （可选） 编辑安全组的名称和描述。

5 （可选） 添加动态成员集。

a 单击**动态成员集**下方的**添加** () 按钮。

b 选择在语句中是否匹配**任何**或**全部**条件。

c 输入要匹配的第一个对象。

选项包括**安全标记**、**VM 客户机操作系统名称**、**VM 名称**和 **VM 客户机主机名称**。

d 选择运算符，如**包含**、**开头为**或**结尾为**。

e 输入值。

f （可选） 要添加另一个语句，请使用布尔运算符**与**或者**或**。

6 （可选） 通过单击要编辑的成员集旁边的**编辑** (⚙) 图标编辑动态成员集。

a 将必要的更改应用到动态成员集。

b 单击**确定**。

7 （可选） 单击要删除的成员集旁边的**删除** (✖) 图标以删除此动态成员集。

8 （可选） 通过单击“包括成员”列表旁边的**编辑** (⚙) 图标编辑所包括成员的列表。

a 从**浏览以下类型的对象**下拉菜单中，选择对象类型，如**虚拟机**、**组织 VDC 网络**、**IP 集**、**MAC 集**或**安全标记**。

b 要在“包括成员”列表中添加一个对象，请从左侧面板中选择该对象，然后单击向右箭头，将其移到右侧面板。

c 要将某个对象排除在“包括成员”列表之外，请从右侧面板中选择对象，然后单击向左箭头，将其移到左侧面板。

9 （可选） 单击“排除成员”列表旁边的**编辑** (⚙) 图标以编辑排除成员列表。

a 从**浏览以下类型的对象**下拉菜单中，选择对象类型，如**虚拟机**、**组织 VDC 网络**、**IP 集**、**MAC 集**或**安全标记**。

b 要在“排除成员”列表中包括某个对象，请从左侧面板中选择该对象，然后单击向右箭头，将其移到右侧面板。

c 要将某个对象排除在“排除成员”列表之外，请从右侧面板中选择对象，然后单击向左箭头，将其移到左侧面板。

10 单击**保存更改**。

此时将保存对安全组所做的更改。

删除安全组

您可以删除用户定义的安全组。

步骤

1 打开安全服务。

a 导航到**网络 > 安全**。

b 选择要应用安全设置的组织 VDC，然后单击**配置服务**。

租户门户将打开“安全服务”。

2 导航到**分组对象 > 安全组**

安全组页面随即打开。

3 选择要删除的安全组。

4 单击**删除** (✖) 按钮。

5 单击**确定**，确认删除。

结果

安全组将被删除。

管理 NSX-T Data Center Edge 网关

NSX-T Data Center Edge 网关为路由组织 VDC 网络提供外部网络连接和 IP 管理属性。此外，还可以提供防火墙、网络地址转换 (NAT)、IPSec VPN、DNS 转发和 DHCP（默认启用）等服务。

专用外部网络

要在虚拟数据中心中提供完全路由的网络拓扑，**系统管理员**可以将外部网络专用于特定的 NSX-T Data Center Edge 网关。

在此配置中，外部网络与 NSX-T Data Center Edge 网关之间存在一对一的关系，其他 Edge 网关都无法连接到该外部网络。

与专用外部网络关联的 NSX-T Data Center 第 0 层逻辑路由器是租户网络堆栈的一部分。外部网络被视为 VMware Cloud Director 网络路由域的一部分。

专用外部网络提供额外的 Edge 网关路由服务，例如路由通告管理和边界网关协议 (BGP) 配置。

您可以决定连接到 Edge 网关的哪些网络向外部网络通告。这样可以混合使用 NAT 路由的组织虚拟数据中心网络和完全路由的组织虚拟数据中心网络。

将防火墙组添加到 NSX-T Edge 网关

要创建防火墙规则并将其添加到 NSX-T Edge 网关，必须先创建防火墙组。防火墙组是应用防火墙规则的对象组。将多个对象组合到防火墙组有助于减少要创建的防火墙规则总数。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后导航到**网络** > **Edge**。

2 单击 NSX-T Edge 网关，然后单击**安全**。

3 单击**组**选项卡，然后单击**新建**。

4 输入防火墙组的名称和可选描述。

5 输入组包含的虚拟机的 IP 地址或 IP 地址范围，然后单击**添加**。

6 要保存防火墙组，请单击**保存**。

结果

您已创建防火墙组并将其添加到 NSX-T Edge 网关。

后续步骤

添加 NSX-T Edge 网关防火墙规则

添加 NSX-T Edge 网关防火墙规则

要控制 NSX-T Edge 网关的入站和出站网络流量，请创建防火墙规则。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后导航到**网络** > **Edge**。

2 单击 Edge 网关，然后单击**服务**。

3 如果**防火墙**屏幕尚不可见，请单击**防火墙**选项卡。

4 单击**编辑规则**。

5 选择防火墙规则，然后单击**在上方添加**按钮。

将在所选规则的上方添加一行表示新规则。

6 配置防火墙规则。

选项	描述
名称	输入规则的名称。
状态	要在创建时启用规则，请打开**状态**开关。
应用程序	（可选）要选择应用规则的特定端口配置文件，请打开**应用程序**开关，然后单击**保存**。
源	选择一个选项，然后单击**保留**。 ■ 要允许或拒绝来自任何源地址的流量，请打开**任何源**。 ■ 要允许或拒绝来自特定防火墙组的流量，请从列表中选择防火墙组。
目标	选择一个选项，然后单击**保留**。 ■ 要允许或拒绝流向任何目标地址的流量，请打开**任何目标**。 ■ 要允许或拒绝来自特定防火墙组的流量，请从列表中选择防火墙组。
操作	从**操作**下拉菜单中选择一个选项。 ■ 要允许来自或流向指定源、目标和服务的流量，请选择**接受**。 ■ 要阻止来自或流向指定源、目标和服务的流量，请选择**拒绝**。
IP 协议	选择是否将规则应用于 IPv4 或 IPv6 流量。
方向	选择要应用规则的流量方向。
启用日志记录。	要记录此规则执行的地址转换，请打开**启用日志记录**开关。

7 单击**保存**。

8 要配置其他规则，请重复这些步骤。

结果

创建防火墙规则后，这些规则将显示在“Edge 网关防火墙规则”列表中。您可以根据需要上移、下移、编辑或删除这些规则。

将 SNAT 或 DNAT 规则添加到 NSX-T Edge 网关

要将源 IP 地址从专用 IP 地址更改为公用 IP 地址，请创建源 NAT (SNAT) 规则。要将目标 IP 地址从公用 IP 地址更改为专用 IP 地址，请创建目标 NAT (DNAT) 规则。

在 VMware Cloud Director 环境中的 Edge 网关上配置 SNAT 或 DNAT 规则时，请始终从您组织 VDC 的角度来配置此规则。

SNAT 规则用于转换从组织 VDC 网络发送到外部网络或其他组织 VDC 网络的数据包的源 IP 地址。

NO SNAT 规则用于阻止转换从组织 VDC 发送到外部网络或其他组织 VDC 网络的数据包的内部 IP 地址。

DNAT 规则用于转换组织 VDC 网络从外部网络或其他组织 VDC 网络收到的数据包的 IP 地址，也可以选择转换其端口。

NO DNAT 规则用于阻止转换组织 VDC 从外部网络或其他组织 VDC 网络接收的数据包的外部 IP 地址。

在 NSX-T Data Center Edge 网关上使用 NAT 服务时，VMware Cloud Director 支持自动路由重新分发。

前提条件

必须已将此公用 IP 地址添加到您要添加规则的 Edge 网关接口。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后导航到**网络** > **Edge**。

2 单击 Edge 网关，然后单击 **NAT**。

3 要添加规则，请单击**新建**。

4 配置 SNAT 或 NO SNAT 规则（内部到外部）。

选项	描述
名称	为规则输入一个有意义的名称。
描述	（可选）为规则输入描述。
状态	要在创建时启用规则，请打开**状态**选项。
接口类型	从下拉菜单中，选择 SNAT 或 NO SNAT。
外部 IP	根据要创建的规则的类型，选择其中一个选项。 ■ 如果要创建 SNAT 规则，请输入要配置 SNAT 规则的 Edge 网关的公用 IP 地址。 ■ 如果要创建 NO SNAT 规则，请将此文本框留空。
内部 IP	输入要配置 SNAT 的虚拟机的 IP 地址或 IP 地址范围，以便它们可以向外部网络发送流量。
目标 IP	（可选）如果您希望将规则仅应用到流向特定域的流量，请输入此域的 IP 地址或 CIDR 格式的 IP 地址范围。如果将此文本框留空，则 SNAT 规则将应用于本地子网外的所有目标。
日志记录	要记录此规则执行的地址转换，请打开**日志记录**选项。

5 配置 DNAT 或 NO DNAT 规则（外部到内部）。

选项	描述
名称	为规则输入一个有意义的名称。
描述	（可选）为规则输入描述。
状态	要在创建时启用规则，请打开**状态**开关。
接口类型	从下拉菜单中，选择 DNAT 或 NO DNAT。
外部 IP	输入要配置 DNAT 规则的 Edge 网关的公用 IP 地址。 所输入的 IP 地址必须属于 Edge 网关的二次分配 IP 范围。
应用程序	（可选）选择要应用规则的特定应用程序端口配置文件。 应用程序端口配置文件包含入站流量在 Edge 网关上用于连接到内部网络的端口和协议。

选项	描述
内部 IP	根据要创建的规则的类型，选择其中一个选项。 ■ 如果要创建 DNAT 规则，请输入要配置 DNAT 的虚拟机的 IP 地址或 IP 地址范围，以便它们可以从外部网络接收流量。 ■ 如果要创建 NO DNAT 规则，请将该文本框留空。
内部端口	（可选）选择 DNAT 规则要针对虚拟机入站数据包转换到的端口或端口范围。
日志记录	要记录此规则执行的地址转换，请打开**日志记录**选项。

6 单击**保存**。

7 要配置其他规则，请重复这些步骤。

在 NSX-T Edge 网关上配置 DNS 转发器服务

要将 DNS 查询转发到外部 DNS 服务器，请配置 DNS 转发器。

在配置 DNS 转发器服务时，还可以添加条件转发器区域。条件转发器区域配置为一个最多包含 5 个 FQDN DNS 区域的列表。如果 DNS 查询与该列表中的某个域名匹配，则会将该查询转发到相应转发器区域中的服务器。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后导航到**网络** > **Edge**。

2 单击 Edge 网关，然后单击**服务**。

3 单击 **DNS**，然后在 **DNS 转发器**部分中，单击**编辑**。

4 要启用 DNS 转发器服务，请打开**状态**开关。

5 输入默认 DNS 区域的名称和可选描述。

6 输入一个或多个用逗号分隔的上游服务器 IP 地址。

7 单击**保存**。

8 （可选） 添加条件转发器区域。

a 在**条件转发器区域**部分中，单击**添加**。

b 输入转发器区域的名称。

c 输入一个或多个用逗号分隔的上游服务器 IP 地址。

d 输入一个或多个用逗号分隔的域名，然后单击**保存**。

创建自定义应用程序端口配置文件

要创建防火墙规则和 NAT 规则，可以使用预配置的应用程序端口配置文件和自定义的应用程序端口配置文件。

应用程序端口配置文件包括协议和端口或端口组的组合，用于 Edge 网关上的防火墙和 NAT 服务。除了为 NSX-T Data Center 预配置的默认端口配置文件之外，还可以创建自定义应用程序端口配置文件。

在 Edge 网关上创建自定义应用程序端口配置文件时，该配置文件将对位于同一组织 VDC 中的其他所有 NSX-T Data Center Edge 网关可见。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后导航到**网络** > **Edge**。

2 单击 Edge 网关，然后单击**安全**选项卡。

3 单击**应用程序端口配置文件**。

4 在**自定义应用程序**部分中，单击**新建**。

5 输入应用程序端口配置文件的名称和可选描述。

6 从下拉菜单中选择协议。

7 输入端口或用逗号分隔的端口范围，然后单击**保存**。

后续步骤

使用应用程序端口配置文件创建防火墙规则和 NAT 规则。请参见添加 NSX-T Edge 网关防火墙规则和将 SNAT 或 DNAT 规则添加到 NSX-T Edge 网关。

用于 NSX-T Data Center Edge 网关的基于 IPsec 策略的 VPN

从版本 10.1 开始，VMware Cloud Director 支持在 NSX-T Data Center Edge 网关实例与远程站点之间建立基于站点到站点策略的 IPSec VPN。

IPSec VPN 在 Edge 网关和远程站点之间提供站点到站点连接，后者也使用 NSX-T Data Center 或具有支持 IPSec 的第三方硬件路由器或 VPN 网关。

基于策略的 IPSec VPN 要求将 VPN 策略应用于数据包，确定哪些流量受到 IPSec 保护，然后再通过 VPN 通道传递。这种类型的 VPN 被视为是静态的，因为本地网络拓扑和配置发生更改时，还必须更新 VPN 策略设置以适应所做的更改。

NSX-T Data Center Edge 网关支持拆分通道配置，IPSec 流量优先采用路由形式。

在 NSX Edge 网关上使用 IPSec VPN 时，VMware Cloud Director 支持自动路由重新分发。

配置基于 NSX-T 策略的 IPSec VPN

可以在 NSX-T Data Center Edge 网关和远程站点之间配置站点到站点连接。远程站点必须使用 NSX-T Data Center，并具有第三方硬件路由器或支持 IPSec 的 VPN 网关。

在 NSX-T Data Center Edge 网关上配置 IPSec VPN 时，VMware Cloud Director 支持自动路由重新分发。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后导航到**网络** > **Edge**。

2 单击 Edge 网关。

3 在**服务**下，单击 **IPSec VPN**。

4 要配置 IPSec VPN 通道，请单击**新建**。

5 输入 IPSec VPN 通道的名称或可选描述。

6 选择要输入的预共享密钥。

注 此预共享密钥必须与 IPSec VPN 通道另一端的预共享密钥相同。

7 输入可用于本地端点的 Edge 网关的 IP 地址之一。

注 该 IP 地址必须是 Edge 网关的主 IP，或者是从外部网络单独分配给 Edge 网关的 IP 地址。

8 以 CIDR 表示法输入至少一个本地 IP 子网地址，以用于 IPSec VPN 通道。

9 输入远程站点的 IP 地址。

10 以 CIDR 表示法输入至少一个远程 IP 子网地址，以用于 IPSec VPN 通道。

11 （可选） 要启用日志记录，请启用**日志记录**选项。

12 单击**保存**。

13 要验证通道是否正常工作，请选择该通道，然后单击**查看统计信息**。

如果通道正常工作，**通道状态**和 **IKE 服务状态**均显示可访问。

结果

新创建的 IPSec VPN 通道将在 **IPSec VPN** 视图中列出。使用默认的安全配置文件创建 IPSec VPN 通道。

后续步骤

您可以根据需要编辑 IPSec VPN 通道设置并自定义其安全配置文件。

自定义 IPSec VPN 通道的安全配置文件

如果您决定不使用创建时分配给 IPSec VPN 通道的系统生成的安全配置文件，则可以对其进行自定义。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后导航到**网络** > **Edge**。

2 单击 Edge 网关。

3 在**服务**下，单击 **IPSec VPN**。

4 选择 IPSec VPN 通道，然后单击**安全配置文件自定义**。

5 配置 IKE 配置文件。

Internet 密钥交换 (IKE) 配置文件提供有关在建立 IKE 通道时用于在网络站点之间进行身份验证、加密和建立共享密钥的算法的信息。

a 选择 IKE 协议版本，以便在 IPSec 协议套件中设置安全关联 (SA)。

选项	描述
IKEv1	选择此选项时，IPSec VPN 将仅启动并响应 IKEv1 协议。
IKEv2	默认选项。选择此版本时，IPSec VPN 将仅启动并响应 IKEv2 协议。
IKE-Flex	选择此选项时，如果使用 IKEv2 协议建立通道失败，源站点不会回退并使用 IKEv1 协议发起连接。相反，如果远程站点使用 IKEv1 协议发起连接，则会接受连接。

b 选择要在 Internet 密钥交换 (IKE) 协商期间使用的受支持加密算法。

c 从**摘要**下拉菜单中，选择要在 IKE 协商期间使用的安全哈希算法。

d 从 **Diffie-Hellman 组**下拉菜单中，选择允许对等站点和 Edge 网关通过不安全的通信通道建立共享密钥的一种加密方案。

e （可选） 在**关联生命周期**文本框中，修改需要重新建立 IPSec 通道之前的默认秒数。

6 配置 IPSec VPN 通道。

a 要启用完美前向保密，请启用此选项。

b 选择碎片整理策略。

碎片整理策略有助于处理内部数据包中存在的碎片整理位。

选项	描述
复制	将碎片整理位从内部 IP 数据包复制到外部数据包。
清除	忽略内部数据包中存在的碎片整理位。

c 选择要在 Internet 密钥交换 (IKE) 协商期间使用的受支持加密算法。

d 从**摘要**下拉菜单中，选择要在 IKE 协商期间使用的安全哈希算法。

e 从 **Diffie-Hellman 组**下拉菜单中，选择允许对等站点和 Edge 网关通过不安全的通信通道建立共享密钥的一种加密方案。

f （可选） 在**关联生命周期**文本框中，修改需要重新建立 IPSec 通道之前的默认秒数。

7 （可选） 在**探测间隔**文本框中，修改对等方失效检测的默认秒数。

8 单击**保存**。

结果

在 IPSec VPN 视图中，IPSec VPN 通道的安全配置文件显示为**用户定义**。

配置专用外部网络服务

要在虚拟数据中心提供完全路由的网络拓扑，**系统管理员**可以为特定的 NSX-T Data Center Edge 网关提供专用的外部网络。

使用专用外部网络时，可以配置额外的路由服务，例如路由通告管理和边界网关协议 (BGP) 配置。

步骤

1 管理路由通告

使用路由通告，可以在组织虚拟数据中心 (VDC) 中创建完全路由的网络环境。

2 配置 BGP 常规设置

可以在具有专用外部网络的 NSX-T Data Center Edge 网关与物理基础架构中的路由器之间配置外部或内部边界网关协议（eBGP 或 iBGP）连接。

3 创建 IP 前缀列表

您可以创建包含单个或多个 IP 地址的 IP 前缀列表。您可以使用 IP 前缀列表向 BGP 邻居分配访问路由通告的权限。

4 添加 BGP 邻居

您可以在添加 BGP 路由邻居时为其配置单独的设置。

管理路由通告

使用路由通告，可以在组织虚拟数据中心 (VDC) 中创建完全路由的网络环境。

您可以决定连接到 NSX-T Data Center Edge 网关的哪些网络子网向专用外部网络通告。

如果未将某个子网添加到通告筛选器，则不会将其路由通告到外部网络，并且该子网将保持专用状态。

注 VMware Cloud Director 通告位于通告路由内的任何组织 VDC 网络。因此，无需为通告网络中的每个子网创建筛选器。

将在 NSX-T Data Center Edge 网关上自动配置路由通告。

在 NSX-T Edge 网关上使用路由通告时，VMware Cloud Director 支持自动路由重新分发。将在表示专用外部网络的第 0 层逻辑路由器上自动配置路由重新分发。

前提条件

- 验证**系统管理员**是否将外部网络专用于组织中的 NSX-T Data Center Edge 网关。
- 确认您是**组织管理员**，或者您具有一组等效权限。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后导航到**网络** > **Edge**。

2 单击 Edge 网关。

3 在**路由**下，单击**路由通告**和**编辑**。

4 要添加要通告的子网，请单击**添加**。

5 添加 IPv4 或 IPv6 子网。

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

配置 BGP 常规设置

可以在具有专用外部网络的 NSX-T Data Center Edge 网关与物理基础架构中的路由器之间配置外部或内部边界网关协议（eBGP 或 iBGP）连接。

BGP 通过使用 IP 网络表或前缀（用于在自治系统 (AS) 之间指定多个路由）来制定核心路由决策。

术语 BGP 发言方指的是运行 BGP 的网络连接设备。两个 BGP 发言方建立连接，然后再交换任何路由信息。

术语 BGP 邻居指的是已经建立此类连接的 BGP 发言方。建立连接后，设备交换路由并同步其表。每个设备发送保持活动消息，确保此关系保持活动状态。

前提条件

-
- 验证您是否具有预定义**组织管理员**角色中包括的权限，或者一组与之等效的权限。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后导航到**网络** > **Edge**。

2 单击 Edge 网关。

3 在**路由**下，单击 **BGP**，然后在**配置**下单击**编辑**。

4 启用**状态**选项以启用 BGP。

5 输入要用于协议本地 AS 功能的自治系统 (AS) ID 编号。

VMware Cloud Director 将本地 AS 编号分配给 Edge 网关。Edge 网关在与其他自治系统中的 BGP 邻居连接时通告此 ID。

6 从下拉菜单中，选择**正常重新启动模式**选项。

选项	描述
帮助程序和正常重新启动	在 Edge 网关上启用正常重新启动功能并不是最佳做法，因为所有网关的 BGP 对等关系始终处于活动状态。 在发生故障切换情况下，正常重新启动功能会增加远程邻居选择备用的第 0 层网关所需的时间。这会延迟基于 BFD 的融合。 注 Edge 网关配置将应用于所有 BGP 邻居，除非特定于邻居的配置覆盖该配置。
仅帮助程序	能够有效减少或消除与从能够正常重新启动的邻居中发现的路由关联的流量的中断情况。邻居必须能够在重新启动时保留其转发表。
禁用	在 Edge 网关上禁用正常重新启动模式。

7 （可选） 更改正常重新启动定时器的默认值。

8 （可选） 更改失效路由定时器的默认值。

9 启用 **ECMP** 选项以启用 ECMP。

10 单击**保存**。

后续步骤

- 创建 IP 前缀列表
- 添加 BGP 邻居

创建 IP 前缀列表

您可以创建包含单个或多个 IP 地址的 IP 前缀列表。您可以使用 IP 前缀列表向 BGP 邻居分配访问路由通告的权限。

可以通过 BGP 邻居筛选器引用 IP 前缀列表，以便限制在 BGP 对等方之间交换的 BGP 更新数量。通过使用路由筛选，可以减少 BGP 更新所需的系统资源量。

例如，您可以将 IP 地址 192.168.100.3/27 添加到 IP 前缀列表，并拒绝将路由重新分发到 Edge 网关。

还可以向 IP 地址附加 `less than or equal to` (le) 及 `greater than or equal to` (ge) 修饰符，以允许或限制路由重新分发。例如，192.168.100.3/27 ge 26 le 32 修饰符与长度大于或等于 26 位且小于或等于 32 位的子网掩码相匹配。

前提条件

-
- 配置 BGP 常规设置。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后导航到**网络** > **Edge**。

2 单击 Edge 网关。

3 在**路由**下，单击 **BGP** 和 **IP 前缀列表**。

4 要添加 IP 前缀列表，请单击**新建**。

5 输入前缀列表的名称或可选描述。

6 单击**新建**，然后添加用于前缀的 CIDR 表示法。

7 从下拉菜单中，选择要应用于前缀的操作。

8 （可选）输入 `greater than or equal to` 和 `less than or equal to` 修饰符以允许或限制路由重新分发。

后续步骤

- 您可以根据需要编辑或删除 IP 前缀列表。
- 配置路由筛选。请参见添加 BGP 邻居。

添加 BGP 邻居

您可以在添加 BGP 路由邻居时为其配置单独的设置。

前提条件

-
- 验证是否已为 Edge 网关配置全局 BGP 设置。请参见配置 BGP 常规设置。
- 如果使用路由筛选，请验证是否已创建 IP 前缀列表。请参见创建 IP 前缀列表。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后导航到**网络** > **Edge**。

2 单击 Edge 网关。

3 在**路由**下，单击 **BGP** 和**邻居**。

4 要添加新的 BGP 邻居，请单击**新建**。

5 为新的 BGP 邻居输入常规设置。

a 为新的 BGP 邻居输入 IPv4 或 IPv6 地址。

b 以 ASPLAIN 格式输入远程自治系统 (Autonomous System, AS) 编号。

c 输入向 BGP 对等方发送保持活动状态消息的时间间隔。

d 输入一个时间间隔，在此时间间隔后将声明 BGP 对等方进入不活动状态。

e 从下拉菜单中，为此邻居选择**正常重新启动模式**选项。

选项	描述
禁用	覆盖全局 Edge 网关设置，并针对此邻居禁用“正常重新启动模式”。
仅帮助程序	覆盖全局 Edge 网关设置，并针对此邻居将“正常重新启动模式”配置为**仅帮助程序**。
正常重新启动和帮助程序	覆盖全局 Edge 网关设置，并将此邻居的“正常重新启动模式”配置为**正常重新启动和帮助程序**。

f 打开 **AllowAS** 开关，以便能够使用同一 AS 接收路由。

g 如果 BGP 邻居需要身份验证，请输入 BGP 邻居的密码。

6 配置新 BGP 邻居的双向转发检测 (BFD) 设置。

a （可选） 启用 **BFD** 选项以便 BFD 执行故障检测。

b 在“BFD 时间间隔”文本框中，定义发送检测信号数据包的时间间隔。

c 在**失效倍数**文本框中，输入 BGP 邻居在 BFD 声明其已关闭之前发送检测信号数据包失败的次数。

7 （可选） 配置路由筛选。

a 从 **IP 地址系列**下拉菜单中，选择 IP 地址系列。

b 要配置入站筛选器，请选择 IP 前缀列表。

c 要配置出站筛选器，请选择 IP 前缀列表。

8 单击**保存**。

后续步骤

您可以查看每个 BGP 邻居的状态，并根据需要编辑或删除 BGP 邻居。

使用给定磁盘和查看存储策略

5

可以通过 VMware Cloud Director 租户门户创建和管理给定磁盘并查看组织虚拟数据中心存储策略。

本章讨论了以下主题：

- 创建并使用给定磁盘
- 查看存储策略属性

创建并使用给定磁盘

给定磁盘是在组织 VDC 中创建的独立虚拟磁盘。**组织管理员**和具有相应权限的用户可以创建、移除和更新给定磁盘并将其连接到虚拟机。

创建给定磁盘时，它与组织 VDC 相关联，而不是与虚拟机相关联。在 VDC 中创建磁盘后，磁盘所有者或管理员可以将其连接到在 VDC 中部署的任何虚拟机。此外，磁盘所有者还可以修改磁盘属性，将磁盘与虚拟机分离，以及将磁盘从 VDC 中移除。**系统管理员**和**组织管理员**具有与磁盘所有者相同的磁盘使用和修改权限。

如果组织 VDC 具有启用了虚拟机加密的存储策略，则可以通过将虚拟机和磁盘与具有虚拟机加密功能的存储策略相关联来对这些虚拟机和磁盘进行加密。请参见虚拟机加密。

创建给定磁盘

可以创建给定磁盘并在后面阶段连接到虚拟机。

要创建给定磁盘，必须指定其名称和大小。可以选择包含描述，并选择磁盘要使用的存储配置文件。

前提条件

您必须具有**组织管理员**角色或磁盘所有者权限。

步骤

1. 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中的**存储**下选择**给定磁盘**。
2. 单击**新建**。
3. 输入磁盘的名称和可选描述。
4. 从**存储策略**下拉菜单中选择存储策略。

5 输入给定磁盘的大小（以字节为单位）。

6 分别从**总线类型**和**总线子类型**下拉菜单中选择总线类型和子类型，然后单击**保存**。

后续步骤

使用 vCloud API 将独立磁盘连接到虚拟机。请参见 VMware {code} 上的《VMware Cloud Director API 编程指南》。

编辑给定磁盘

创建磁盘后，可以修改其名称、描述、存储策略和大小。

前提条件

您必须具有**组织管理员**角色或磁盘所有者权限。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中的**存储**下选择**给定磁盘**。

2 选择要修改的磁盘，然后单击**编辑**。

3 编辑设置，例如名称、描述、存储策略和大小（字节）。

4 单击**保存**。

将给定磁盘连接到虚拟机

在 VDC 中创建给定磁盘后，可以将其连接到在 VDC 中部署的任何虚拟机。

前提条件

您必须具有**组织管理员**角色或磁盘所有者权限。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中的**存储**下选择**给定磁盘**。

2 单击要连接到虚拟机的给定磁盘名称旁边的单选按钮，然后单击**连接**。

3 从下拉菜单中，选择给定磁盘要连接的虚拟机，然后单击**应用**。

结果

给定磁盘将连接到虚拟机。

后续步骤

可以将更多给定磁盘连接到 VM，也可以根据需要将其分离。

删除给定磁盘

如果不需要给定磁盘，可以将其删除。

前提条件

您必须具有**组织管理员**角色或磁盘所有者权限。

步骤

1. 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片，然后从左侧面板中的**存储**下选择**给定磁盘**。
2. 选择要删除的磁盘，然后单击**删除**。
3. 单击**确定**。

查看存储策略属性

可以查看存储策略和存储策略详细信息。

前提条件

此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。

步骤

1. 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片。
2. 在**存储**下，单击**存储策略**。

   将显示可用存储策略列表。
3. 要查看有关存储策略的详细信息，请单击存储策略的名称。
4. 查看**常规**和**元数据**选项卡上的详细信息，然后单击**确定**。

查看和编辑虚拟数据中心属性

6

作为**组织管理员**，您可以查看虚拟数据中心属性。您还可以控制组织中的用户和组对组织 VDC 的访问。

本章讨论了以下主题：

- 查看虚拟数据中心属性
- 查看虚拟数据中心元数据
- 仅限组织中的特定用户和组访问组织 VDC

查看虚拟数据中心属性

可以查看分配给组织的虚拟数据中心的属性。

前提条件

此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片。

2 在**设置**下，单击**常规**。

结果

可以查看虚拟数据中心的属性，如名称、描述和状态。数据中心的衡量指标信息包括分配模型、vCPU、CPU 和内存使用情况。

查看虚拟数据中心元数据

VMware Cloud Director 提供了一个用于将用户定义的元数据与对象关联起来的通用工具。如果您的系统管理员为组织虚拟数据中心创建了元数据，则您可以查看组织数据中心元数据。

前提条件

此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要浏览的虚拟数据中心对应的卡片。

2 在**设置**下，单击**元数据**。

将显示可用元数据列表。

仅限组织中的特定用户和组访问组织 VDC

作为**组织管理员**，您可以仅限特定的用户和组访问组织中的每个组织 VDC。

默认情况下，组织 VDC 与具有的角色包括**允许访问所有组织 VDC** 权限的所有用户和组共享。

如果您的组织具有多个组织 VDC，并且您希望单独对其进行管理，则可以创建一个可充当组织 VDC 管理员的自定义角色，并将其分配给组织中的特定用户或组，从而可以只允许这些用户或组访问特定 VDC 的计算资源和网络资源。

前提条件

1 确认您是**组织管理员**。

2 为要向其提供特定组织 VDC 访问权限的用户和组创建自定义角色。此角色必须排除**允许访问所有组织 VDC** 权限。请参见第 12 章 管理用户、组和角色。

步骤

1 在**虚拟数据中心**仪表板屏幕上，单击要仅限对其进行访问的虚拟数据中心对应的卡视图。

2 在**设置**下，单击**共享**。

此时将显示组织中有权访问该 VDC 的用户和组列表。

3 要更改组织 VDC 的访问设置，请单击**编辑**。

4 选择**特定用户和组**。

5 从**用户**列表中，选择要为其提供 VDC 访问权限的用户。

6 从**组**列表中，选择要为其提供 VDC 访问权限的组。

7 要与选定的用户和组共享 VDC，请单击**共享**。

结果

对组织 VDC 的访问仅限于您选择的用户和组。

使用专用 vCenter Server 实例和代理

7

从 VMware Cloud Director 9.7 开始，可以从 VMware Cloud Director 访问专用 vCenter Server 环境。

专用 vSphere 数据中心

在 VMware Cloud Director 中，软件定义的数据中心 (SDDC) 封装整个专用 vCenter Server 环境。

VMware Cloud Director 中的专用 vCenter Server 实例消除了 vCenter Server 实例需可公开访问的要求。

一个专用 vCenter Server 实例可以包含一个或多个代理，可通过这些代理访问底层环境中的不同组件。

系统管理员可以向您的组织发布一个或多个专用 vCenter Server 实例。可以使用代理访问代理组件的 UI 或 API。

代理

VMware Cloud Director 可以充当 HTTPS 代理服务器，并支持访问专用 vCenter Server 实例以及用于备份环境的共享或专用 vCenter Server 实例的不同组件。

代理提供数据中心组件（如 vCenter Server 实例、ESXi 主机、NSX Manager 实例或 NSX-T Manager 实例）的访问点。

您可以使用您的 VMware Cloud Director 帐户登录到代理组件的 UI 或 API。

要访问代理组件，必须使用 Chrome Browser Extension for VMware Cloud Director，或者使用代理设置手动配置浏览器。

本章讨论了以下主题：

- 使用 Chrome Browser Extension for VMware Cloud Director
- 为浏览器配置代理设置
- 登录代理组件的 UI

使用 Chrome Browser Extension for VMware Cloud Director

可以使用 Chrome Browser Extension for VMware Cloud Director 登录到环境中被代理的 vSphere 组件。

Chrome Browser Extension for VMware Cloud Director 提供代理配置和身份验证。

Chrome Browser Extension for VMware Cloud Director 支持多站点环境。

可以通过 Chrome Web Store 将该扩展添加到 Chrome 浏览器。

为浏览器配置代理设置

必须设置发布到组织的代理，然后才能访问代理 vSphere 组件的 UI。

要将浏览器配置为使用已发布的代理，请将代理自动配置 (PAC) 文件的 URL 复制到您的浏览器。

注 当**系统管理员**向您的组织发布专用 vSphere 数据中心，或者将代理添加到一个专用 vSphere 数据中心时，浏览器可能需要几分钟的时间才能从提供的 URL 重新获取 PAC。要强制刷新浏览器，可以重复此过程。

前提条件

- 确认**系统管理员**至少已将一个已启用的专用 vCenter Server 实例发布到您的组织。
- 确认**系统管理员**已将 **SDDC_VIEW** 和**令牌：管理**权限发布到您的组织，并且您的角色包括这些权限。
- 确认**系统管理员**已将 **CPOM 扩展**插件发布到您的组织并已启用。此插件提供了在 VMware Cloud Director Tenant Portal 中查看和使用专用 vSphere 数据中心的功能。

步骤

1. 在顶部导航栏中，单击**数据中心**和**虚拟数据中心**。
2. 在**专用 vSphere 数据中心**窗格中，单击**单击此处查看代理配置指南**。
3. 复制 PAC URL，然后单击**下一步**。
4. 按照说明配置浏览器以指向此 PAC URL。
5. 如果代理组件使用的是自签名证书，则将证书导入到浏览器。
   a. 在目标 vSphere 数据中心卡上，单击**操作**，然后单击**导入证书**。
   b. 下载证书和证书吊销列表 (CRL)。
   c. 将下载的证书导入到您的浏览器中。

      请参见您的浏览器对应的用户说明。

登录代理组件的 UI

可以使用您的 VMware Cloud Director 帐户访问代理组件的 UI。

前提条件

为浏览器配置代理设置，或使用 Chrome Browser Extension for VMware Cloud Director 到 Google Chrome。

步骤

1. 在顶部导航栏中，单击**数据中心**和**虚拟数据中心**。
2. 单击**专用 vSphere 数据中心**选项卡。
3. 打开专用 vCenter Server 实例的代理。
   - 要打开默认代理，请单击**打开 vSphere**。
   - 要打开非默认代理，请执行以下步骤：
     - 单击**操作**，然后单击**查看代理**。
     - 单击代理 URL。

   此时将打开包含您代理凭据的新的卡视图。
4. 复制用户名和密码。
5. 要激活代理，请单击**打开**。

   此时将打开一个新卡视图，提示您对代理进行身份验证。
6. 在**用户名**文本框中，粘贴复制的用户名。
7. 在**密码**文本框中，粘贴复制的密码，然后单击**确定**。

结果

代理组件的 UI 随即打开。

使用 vApp 模板

8

vApp 模板是已经加载了操作系统、应用程序和数据的虚拟机映像。这些模板可确保虚拟机配置在整个组织中是一致的。vApp 模板添加到目录中。

本章讨论了以下主题：

- 查看 vApp 模板
- 从 OVF 文件创建 vApp 模板
- 将 vCenter Server 中的虚拟机作为 vApp 模板导入
- 将 VM 放置策略和 VM 大小调整策略分配给 vApp 模板
- 下载 vApp 模板
- 删除 vApp 模板

查看 vApp 模板

您可以查看自己有权访问的目录中的 vApp 模板的列表。可以查看 vApp 模板及其所含的虚拟机。

您只能访问已共享给您的目录项中包含的 vApp 模板。有关共享目录的详细信息，请参见共享目录。

前提条件

此操作需要预定义的 **vApp 作者**角色中包含的权限或一组等效权限。

步骤

1 在顶部导航栏中，单击**库**，然后在左侧面板中选择 **vApp 模板**。

此时将以网格视图显示模板列表。

2 （可选） 配置网格视图以包含要查看的元素。

a 在网格视图中，单击 vApp 模板列表下方的网格编辑器图标 ( )。

b 选择要包含在网格视图中的元素，例如版本、状态、目录、所有者等。

c 单击**确定**。

网格会以列表显示您为每个 vApp 模板选择的元素。

3 要查看 vApp 模板中包含的虚拟机，请单击 vApp 模板名称。

vApp 模板中包含虚拟机将显示在网格中。

4 （可选） 要选择要在网格视图中查看的元素，请单击虚拟机列表下方的网格编辑器图标 ( )。

a 选择要包含在网格视图中的元素。

b 单击**确定**。

从 OVF 文件创建 vApp 模板

您可以上载 OVF 软件包，以在目录中创建 vApp 模板。

VMware Cloud Director 支持开放式虚拟化格式 (OVF) 和开放式虚拟化设备 (OVA) 规范。如果上载的 OVF 文件包括用于自定义其虚拟机的 OVF 属性，则 vApp 模板中将保留这些属性。有关创建 OVF 软件包的信息，请参见《OVF 工具用户指南》和《VMware vCenter Converter 用户指南》

前提条件

此操作需要预定义的**目录作者**角色中包含的权限或一组等效权限。

步骤

1 在顶部导航栏中，单击**库**，然后在左侧面板中选择 **vApp 模板**。

此时将以网格视图显示模板列表。

2 单击**新建**。

3 输入 OVF 文件的 URL 地址，或单击**上载**图标 ( ) 浏览到可从您的计算机访问的位置，然后选择 OVF/OVA 模板文件。

位置可能为本地硬盘驱动器、网络共享或 CD/DVD 驱动器。受支持的文件扩展名包括 `.ova`、`.ovf`、`.vmdk`、`.mf`、`.cert` 和 `.strings`。如果选择上载 OVF 文件，而其引用的文件多于您要上载的文件（例如，VMDK 文件），则必须浏览并选择所有文件。

4 验证将部署的 OVF/OVA 模板的详细信息，然后单击**下一步**。

5 输入 vApp 模板的名称和可选描述，然后单击**下一步**。

6 从**目录**下拉菜单中，选择要将模板添加到的目录。

7 检查 vApp 模板设置，然后单击**完成**。

结果

新的 vApp 模板将显示在模板网格视图中。

将 vCenter Server 中的虚拟机作为 vApp 模板导入

如果您具有**系统管理员**权限，则可以将 vCenter Server VM 作为目录中的 vApp 模板导入到 VMware Cloud Director。

前提条件

要将 vCenter Server 中的 VM 作为 vApp 模板查看和导入，请确认您具有**系统管理员**权限。

步骤

1 在顶部导航栏中，单击**库**，然后在左侧面板中选择 **vApp 模板**。

此时将以网格视图显示模板列表。

2 单击**从 vCenter 导入**。

3 从下拉菜单中，选择要从中导入 vApp 模板的 vCenter Server 实例。

4 从虚拟机列表中选择一个模板。

5 输入 vApp 模板的名称和可选描述。

6 从下拉菜单中，选择要向其添加 vApp 模板的目录。

7 （可选） 要删除源虚拟机，请启用**移动虚拟机**选项。

8 （可选） 将此 vApp 模板标记为目录中的首选模板。

9 单击**导入**。

将 VM 放置策略和 VM 大小调整策略分配给 vApp 模板

要将 vApp 模板的 VM 与特定 VM 放置策略和 VM 大小调整策略相关联，可以使用要分配的策略标记 vApp 模板的各个 VM。

从 VMware Cloud Director 10.0 开始，您可以允许用户在编辑 VM 时更改预定义的 VM 放置策略或 VM 大小调整策略。

注 升级到 VMware Cloud Director 10.0 或更高版本后，所有预先存在的模板标记都将变为可修改。如果要禁止对预定义的 VM 放置策略或 VM 大小调整策略进行更改，则必须取消选中要使其不可更改的策略对应的**可修改**复选框。

前提条件

- 此操作需要 vApp 模板的编辑权限。
- 确认您的 VMware Cloud Director 环境中至少有一个 vApp 模板。

步骤

1 在顶部导航栏中，单击**库**，然后在左侧面板中选择 **vApp 模板**。

此时将以网格视图显示模板列表。

2 选择要标记的 vApp 模板旁边的单选按钮，然后单击**使用计算策略进行标记**。

3 如果要将 VM 放置策略分配给 vApp 模板中的 VM，请从该 VM 对应的行上的 **VM 放置策略**下拉菜单中选择一个策略。

4 如果要将 VM 大小调整策略分配给 vApp 模板中的 VM，请从该 VM 对应的行上的 **VM 大小调整策略**下拉菜单中选择一个策略。

5 （可选） 要允许用户在编辑 VM 时更改预定义的 VM 放置策略或 VM 大小调整策略，请选中策略下拉菜单下的**可修改**复选框。

6 单击**标记**。

下载 vApp 模板

您可以将 vApp 模板以 OVA 文件的形式从目录下载到您的本地计算机。

前提条件

此操作需要预定义的**目录作者**角色中包含的权限或一组等效权限。

步骤

1 在顶部导航栏中，单击**库**，然后在左侧面板中选择 **vApp 模板**。

此时将以网格视图显示模板列表。

2 单击要下载的 vApp 模板左侧的列表栏 (⋮)，然后选择**下载**。

注 可以从组织目录下载 vApp 模板。如果您是组织管理员，则可以从公用目录下载 vApp 模板。否则，**下载**按钮灰显。

3 （可选） 要在下载的 OVA 软件包中保留虚拟机的 UUID 和 MAC 地址，请选中**保存身份信息**复选框。

4 单击**确定**并等待下载完成。

OVA 文件会保存到 Web 浏览器的默认下载位置。

删除 vApp 模板

您可以从组织目录中删除 vApp 模板。如果该目录已发布，则还会从公用目录中删除该 vApp 模板。

前提条件

此操作需要预定义的 **vApp 作者**角色中包含的权限或一组等效权限。

步骤

1 在顶部导航栏中，单击**库**，然后在左侧面板中选择 **vApp 模板**。

此时将以网格视图显示模板列表。

2 单击要删除的 vApp 模板左侧的列表栏 (⋮)，然后选择**删除**。

3 确认该删除操作。

已删除的 vApp 模板将从网格视图中移除。

使用媒体文件

9

目录支持您上载、复制、移动媒体文件和编辑媒体文件的属性。

本章讨论了以下主题：

- 上载媒体文件
- 删除媒体文件
- 下载媒体文件

上载媒体文件

您可以将新的媒体文件或新版现有媒体文件上载到目录。具有目录访问权限的用户可以打开媒体文件及其虚拟机。

前提条件

此操作需要预定义的**目录作者**角色中包含的权限或一组等效权限。

步骤

1. 在顶部导航栏中，单击**库**，然后在左侧面板中选择**媒体和其他**。

   此时将以网格视图显示媒体文件列表。

2. 单击**添加**。
3. 从**目录**下拉菜单中，选择要上载媒体文件的目录。
4. 输入媒体文件的名称。

   如果未输入名称，则会在媒体文件名称后自动填充名称文本框。

5. 单击上载图标 (↑)，浏览并选择磁盘映像文件，例如 `.iso` 文件。
6. 单击**确定**。

   上载开始后，媒体文件将显示在网格视图中。

后续步骤

根据文件大小，可能需要一些时间才能完成上载。您可以在**近期任务**视图中监控上载状态。有关详细信息，请参见查看任务。

删除媒体文件

可以从目录中删除不再使用的媒体文件。

前提条件

此操作需要预定义的**目录作者**角色中包含的权限或一组等效权限。

步骤

1 在顶部导航栏中，单击**库**，然后在左侧面板中选择**媒体和其他**。

此时将以网格视图显示媒体文件列表。

2 单击要删除的媒体文件左侧的列表栏 (⋮)，然后选择**删除**。

3 确认该删除操作。

已删除的媒体文件将从网格视图中移除。

下载媒体文件

您可以从目录下载媒体文件。

前提条件

此操作需要预定义的**目录作者**角色中包含的权限或一组等效权限。

步骤

1 在顶部导航栏中，单击**库**，然后在左侧面板中选择**媒体和其他**。

此时将以网格视图显示媒体文件列表。

2 单击要下载的媒体文件左侧的列表栏 (⋮)，然后选择**下载**。

下载任务将启动，并将文件保存到 Web 浏览器的默认下载位置。

后续步骤

根据文件大小，可能需要一些时间才能完成下载。您可以在**近期任务**面板中监控下载状态。有关详细信息，请参见查看任务。

使用目录

10

目录是组织中的 vApp 模板和媒体文件的容器。组织管理员和目录作者均可在组织中创建目录。目录内容可以与 VMware Cloud Director 安装中的其他用户或组织共享，或者在外部发布，以供 VMware Cloud Director 安装之外的组织访问。

VMware Cloud Director 包含专用目录、共享目录和外部可访问的目录。专用目录包括可以与组织中其他用户共享的 vApp 模板和媒体文件。如果系统管理员为您的组织启用目录共享，则您可以共享组织目录，以创建可由 VMware Cloud Director 安装中的其他组织访问的目录。如果系统管理员为您的组织启用外部目录发布，则您可以发布组织目录，以供 VMware Cloud Director 安装外部的组织访问。VMware Cloud Director 安装之外的组织必须订阅外部发布的目录才能访问其内容。

可以将 OVF 软件包直接上载到目录，将 vApp 另存为 vApp 模板，或者从 vSphere 导入 vApp 模板。请参见从 OVF 文件创建 vApp 模板和将 vApp 作为 vApp 模板保存到目录。

组织成员可以访问他们所拥有或与他们共享的 vApp 模板和媒体文件。组织管理员和系统管理员可以与组织中的每位成员或组织中的特定用户和组共享目录。请参见共享目录。

本章讨论了以下主题：

查看目录

您可以访问组织内与您共享的目录。如果组织管理员已将公用目录设置为可在组织内进行访问，那么您可以访问这些公用目录。

目录访问通过目录共享进行控制，而不是通过角色中的权限。您只能访问与您共享的目录或目录项。有关详细信息，请参见共享目录。

步骤

1 在顶部导航栏中，单击**库**，然后在左侧面板中选择**目录**。

此时将以网格视图显示目录列表。

2 （可选）配置网格视图以包含您要查看的元素。

a 在网格视图中，单击目录列表下方显示的网格编辑器图标 ()。

b 选择要包含在网格视图中的元素，例如版本、描述、状态等。

c 单击**确定**。

网格将显示您为每个目录选择的元素。

3 （可选）从网格视图中，使用列表栏 (⋮) 显示您可以对每个目录执行的操作。

例如，您可以共享或删除目录。

创建目录

可以创建新目录并将其与存储策略相关联。

前提条件

此操作需要预定义的**目录作者**角色中包含的权限或一组等效权限。

步骤

1 在顶部导航栏中，单击**库**，然后在左侧面板中选择**目录**。

此时将以网格视图显示目录列表。

2 单击**新建**以创建新目录。

3 输入目录的名称和可选描述。

4 （可选） 选择是否要将存储策略分配给目录，并选择一个存储策略。

5 单击**确定**。

结果

新目录将显示在**目录**选项卡上的网格视图中。

共享目录

您可以与组织的所有成员或者与特定成员共享目录。

前提条件

- 此操作需要预定义的**目录作者**角色中包含的权限或一组等效权限。
- 您必须是目录的所有者。

步骤

1 在顶部导航栏中，单击**库**，然后在左侧面板中选择**目录**。

此时将以网格视图显示目录列表。

2 单击要共享的目录左侧的列表栏 (⋮)，然后选择**共享**。

能够访问目录的用户列表显示在**共享目录**窗口的网格视图中。

3 单击 **添加**以与其他用户共享目录。

选项	描述
与组织中的每个人共享	向组织中的所有用户和组授予访问权限。
与特定用户和组共享	选择要向其授予目录访问权限的用户或组，然后单击**添加**。

4 选择访问级别。

选项	描述
只读	有权访问此目录的用户能够对此目录的 vApp 模板和 ISO 文件进行读取。
读/写	有权访问此目录的用户能够对此目录的 vApp 模板和 ISO 文件进行读取，并能向此目录中添加 vApp 模板和 ISO 文件。
完全控制	有权访问此目录的用户可以完全控制此目录的内容和设置。

5 单击**确定**。

当前有权访问此目录的用户或组将显示在**共享目录**对话框的网格视图中。

6 （可选） 进行选择将只读访问权限共享给其他所有组织的管理员

7 单击**保存**。

结果

在**目录**选项卡上，网格视图中此目录的“已共享”状态会发生变化。

删除目录

您可以从组织中删除目录。

前提条件

此操作需要预定义的**目录作者**角色中包含的权限或一组等效权限。

注 目录不得包含任何 vApp 模板或媒体文件。您可以将这些项目移至不同目录或删除它们。

步骤

1 在顶部导航栏中，单击**库**，然后在左侧面板中选择**目录**。

此时将以网格视图显示目录列表。

2 单击要删除的目录左侧的列表栏 (⋮)，然后选择**删除**。

3 确认该删除操作。

已删除的目录项将从网格视图中移除。

更改目录的所有者

组织管理员可以更改目录的所有者。

删除拥有目录的用户之前，您必须先更改所有者或删除该目录。

前提条件

此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。

步骤

1 在顶部导航栏中，单击**库**，然后在左侧面板中选择**目录**。

此时将以网格视图显示目录列表。

2 单击目录左侧的列表栏 (⋮)，并选择**更改所有者**。

能够访问目录的用户列表将显示在**更改所有者**窗口的网格视图中。

3 选择要作为新目录所有者的用户，然后单击**确定**。

结果

在**目录**选项卡上，网格视图中此目录的所有者名称将发生变化。

管理目录的元数据

作为**组织管理员**或**目录所有者**，您可以创建或更新所拥有的目录的元数据。

步骤

1 在顶部导航栏中，单击**库**，然后在左侧面板中选择**目录**。

此时将以网格视图显示目录列表。

2 单击目录左侧的列表栏 (⋮)，并选择**元数据**。

将在网格视图中显示所选目录的元数据。

3 （可选） 要添加元数据，请单击**添加**。

a 输入元数据名称。

该名称在附加到此对象的元数据名称内必须唯一。

b 选择元数据类型，例如，**文本**、**数字**、**日期和时间**或**是或否**。

c 输入元数据值。

d 单击**保存**。

4 （可选） 更新现有元数据。

无法更新元数据名称。

a 更新元数据类型。

b 输入新的元数据值。

c 单击**保存**。

5 （可选） 删除现有元数据。

a 单击删除图标。

b 单击**保存**。

发布目录

如果**系统管理员**已授予您目录访问权限，则您可以在外部发布目录，以使其 vApp 模板和媒体文件可供 VMware Cloud Director 安装外部的组织订阅。

前提条件

验证**系统管理员**是否为组织启用了外部目录发布以及是否授予您目录访问权限。

步骤

1 在顶部导航栏中，单击**库**，然后在左侧面板中选择**目录**。

此时将以网格视图显示目录列表。

2 单击要发布的目录左侧的列表栏 (⋮)，然后选择**发布设置**。

3 选择**启用发布**和（可选）输入目录访问的密码。

仅支持 ASCII 字符。

4 单击**保存**。

订阅外部目录

可以订阅外部目录，从而创建外部发布目录的只读副本。无法修改订阅目录。

前提条件

- 此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。
- **系统管理员**必须向您的组织授予订阅外部目录的权限。

步骤

1 在顶部导航栏中，单击**库**，然后在左侧面板中选择**目录**。

此时将以网格视图显示目录列表。

2 单击**新建**以创建新目录。

3 输入目录的名称和可选描述。

4 选择订阅外部目录并提供订阅 URL。

5 输入用于访问目录的可选密码。

6 选择是否要自动从外部目录下载内容。

7 单击**确定**。

更新订阅目录的位置 URL 和密码

创建订阅目录后，可以更新订阅目录的位置 URL 和密码。

前提条件

- 此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。
- 必须已创建订阅目录。
- **系统管理员**必须向您的组织授予订阅外部目录的权限。

步骤

1 在顶部导航栏中，单击**库**，然后在左侧面板中选择**目录**。

此时将以网格视图显示目录列表。

2 单击订阅目录左侧的列表栏 (⋮)，并选择**订阅设置**。

如果目录不是订阅目录，该选项将灰显。

3 更新此订阅目录的位置 URL 和密码。

4 选择是否要自动从外部目录下载内容。

5 单击**保存**。

同步订阅目录

创建订阅目录后，可以将其与原始目录同步以查看是否有任何更改。例如，如果原始目录的元数据有所更改，则执行同步时，订阅目录的元数据会更新。

前提条件

- 此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。
- 必须已创建订阅目录。
- **系统管理员**必须向您的组织授予订阅外部目录的权限。

步骤

1 在顶部导航栏中，单击**库**，然后在左侧面板中选择**目录**。

此时将以网格视图显示目录列表。

2 单击订阅目录左侧的列表栏 (⋮)，并选择**同步**。

如果目录不是订阅目录，该选项将灰显。

订阅目录将与原始目录同步。

使用组织虚拟数据中心模板

11

组织管理员或有权查看和实例化组织虚拟数据中心模板的任何角色均可创建其他组织虚拟数据中心。

组织虚拟数据中心模板可以为组织虚拟数据中心指定一种配置，也可以为 Edge 网关和组织虚拟数据中心网络指定一种配置。如果系统管理员希望组织管理员能够在其组织中创建这些资源，则可以创建组织虚拟数据中心模板并与这些组织共享模板。

通过创建并共享虚拟数据中心模板，系统管理员可以启用组织虚拟数据中心的自助置备，同时还可以对系统资源（如提供者虚拟数据中心和外部网络）的分配保留管理控制权限。

系统管理员可以创建组织虚拟数据中心模板，并向不同组织提供模板的访问权限。

如果您的组织已具有虚拟数据中心模板的访问权限，您可以使用 VMware Cloud Director Tenant Portal 从可用的模板创建虚拟数据中心。

本章讨论了以下主题：

查看可用虚拟数据中心模板

您可以查看系统管理员为您创建的组织虚拟数据中心模板。

先查看虚拟数据中心模板，然后再从虚拟数据中心模板创建新组织虚拟数据中心。

前提条件

此操作需要预定义的**组织管理员**角色或有权查看和实例化组织虚拟数据中心模板的角色中包含的权限。

步骤

- 在顶部导航栏中，单击**库**，然后在左侧面板中选择**组织 VDC 模板**。

  此时将以网格视图显示虚拟数据中心模板列表。

后续步骤

查看组织虚拟数据中心模板的描述，然后选择要用于创建新组织虚拟数据中心的模板。

从模板创建虚拟数据中心

您可以从系统管理员已创建的虚拟数据中心模板创建组织虚拟数据中心。

前提条件

此操作需要预定义的**组织管理员**角色或有权查看和实例化组织虚拟数据中心模板的角色中包含的权限。

步骤

1. 在顶部导航栏中，单击**库**，然后在左侧面板中选择**组织 VDC 模板**。

   此时将以网格视图显示虚拟数据中心模板列表。
2. 选择一个模板，然后单击**新建 VDC**。
3. 输入虚拟数据中心的名称和（可选）描述。
4. 单击**创建**。

结果

此时将实例化新组织虚拟数据中心的创建，此操作可能需要几分钟的时间。您可以在**近期任务**面板中查看任务进度。

后续步骤

您可以通过创建虚拟机、vApp 以及管理网络和安全设置等操作管理新创建的组织虚拟数据中心。

管理用户、组和角色

12

可以单独将组织管理员添加到 VMware Cloud Director，也可以将其作为 LDAP 组的一部分添加。您还可以添加并修改决定用户在其组织内所拥有权限的角色。

重要事项 只有**组织管理员**能够管理组织内的用户、组和角色。**系统管理员**可以向您的租户发布一个或多个全局租户角色，而**组织管理员**则可在角色列表中查看这些角色。此类角色包括**目录作者**、**vApp 作者**、**vApp 用户**、**组织管理员**等等。您不能修改预定义的全局租户角色，但可以创建和更新类似的自定义租户角色并将其分配给租户中的用户。

本章讨论了以下主题：

管理用户

可以从租户门户创建、编辑、导入和删除用户。此外，还可以在用户尝试使用错误密码登录而导致锁定自己的用户帐户的情况下，解除用户帐户锁定。

创建用户

可以在您的 VMware Cloud Director 组织内创建用户。

前提条件

此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。

步骤

1. 在顶部导航栏中，单击**管理**。
2. 在左侧面板中的**访问控制**下，单击**用户**。

   此时将显示用户列表。
3. 单击**创建**。
4. （可选） 输入用户的用户名和密码设置。

   最小密码长度为 6 个字符。

5 选择是否在创建时启用用户。

6 选择要分配给用户的角色。

可用角色菜单包含一系列预定义角色以及您或系统管理员可能创建的任何自定义角色。

预定义角色	描述
vApp 作者	与预定义的 **vApp 作者**角色关联的权限允许用户使用目录并创建 vApp。
仅控制台访问权	与预定义的**仅控制台访问权**角色关联的权限允许用户查看虚拟机状态和属性并使用客户机操作系统。
vApp 用户	与预定义的 **vApp 用户**角色关联的权限允许用户使用现有 vApp。
组织管理员	具有预定义**组织管理员**角色的用户可以使用 VMware Cloud Director 租户门户或 Cloud Director OpenAPI 管理其组织中的用户和组，并为其分配角色（包括预定义的**组织管理员**角色）。**组织管理员**可以使用 Cloud Director OpenAPI 创建或更新组织的本地角色对象。某个**组织管理员**创建或修改的角色对其他组织不可见。
遵从身份提供者	与预定义的**遵从身份提供程序**角色相关联的权限根据从用户的 OAuth 或 SAML 身份提供程序收到的信息确定。为用户分配了**遵从身份提供程序**角色时，要符合包含条件，身份提供程序提供的角色名称必须与组织中定义的角色名称完全匹配且大小写一致。
目录作者	与预定义的**目录作者**角色关联的权限允许用户创建和发布目录。

7 （可选） 输入联系人信息，例如姓名、电子邮件地址、电话号码和即时消息 ID。

8 （可选） 输入用户的虚拟机配额。

配额确定了用户可以管理的虚拟机数量以及正在运行的虚拟机数量。如果希望为用户提供无限数量的虚拟机，请选择**无限制**。

9 单击**保存**。

导入用户

可以通过导入 LDAP 用户或 SAML 用户并为其分配特定角色来将用户添加到您的组织。

前提条件

- 此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。
- 确认您具有与 LDAP 服务器的有效连接，或者为组织启用 SAML 身份提供者支持。

步骤

1 在顶部导航栏中，单击**管理**。

2 在左侧面板中的**访问控制**下，单击**用户**。

此时将显示用户列表。

3 单击**导入用户**。

4 选择要从其导入用户的源。

您只能查看源 LDAP 服务器或配置为身份提供者的 SAML 服务器。

源	操作
LDAP	从 LDAP 服务器导入用户。 a 在文本框中输入全称或部分名称，然后单击**搜索**。 b 选择要导入的用户，然后单击**添加**。
SAML	从 SAML 服务器导入用户。输入要导入的用户的用户名。 用户名必须使用为此组织配置的 SAML 身份提供者所支持的名称标识符格式。 **注** 如果使用 vCenter Single Sign-On 作为 SAML 身份提供者，则从 vCenter Single Sign-On 域导入的用户名必须采用用户主体名称 (UPN) 格式，例如 jdoe@mydomain.com。 每个用户名使用一个新行。

5 选择要为导入的用户分配的角色。

6 单击**保存**。

修改用户

作为组织管理员，您可以修改现有用户的密码、联系信息和虚拟机配额设置。此外，还可以更改用户的角色。

前提条件

此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。

步骤

1 在顶部导航栏中，单击**管理**。

2 在左侧面板中的**访问控制**下，单击**用户**。

此时将显示用户列表。

3 单击要编辑的用户名称旁边的单选按钮，然后单击**修改**。

4 更新要修改的设置。

a 根据需要更改密码。

b 选择是启用还是禁用用户。

c 更新用户角色。

d 更新联系人信息，例如姓名、电子邮件地址、电话号码和即时消息 ID。

e 编辑用户的虚拟机配额。

5 单击**保存**。

禁用或启用用户帐户

可以禁用用户帐户以阻止该用户登录到 VMware Cloud Director。要删除用户，必须先禁用其帐户。

前提条件

此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。

步骤

1 在顶部导航栏中，单击**管理**。

2 在左侧面板中的**访问控制**下，单击**用户**。

此时将显示用户列表。

3 要禁用用户帐户，请单击用户名旁边的单选按钮，单击**禁用**，并确认您要禁用该帐户。

4 要启用已禁用的用户帐户，请单击用户名旁边的单选按钮，然后单击**启用**。

删除用户

可以通过删除用户帐户来从 VMware Cloud Director 组织中移除用户。

前提条件

- 此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。
- 禁用要删除的帐户。

步骤

1 在顶部导航栏中，单击**管理**。

2 在左侧面板中的**访问控制**下，单击**用户**。

此时将显示用户列表。

3 单击要删除的用户的名称旁边的单选按钮，然后单击**删除**。

4 要确认删除该用户帐户，请单击**确定**。

解锁锁定的用户帐户

如果已在 VMware Cloud Director 组织中启用锁定策略，那么将在一定次数的无效登录尝试后锁定用户帐户。您可以解锁锁定的用户帐户。最佳做法是更改用户的密码，然后解锁该帐户。

前提条件

此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。

步骤

1 在顶部导航栏中，单击**管理**。

2 在左侧面板中的**访问控制**下，单击**用户**。

此时将显示用户列表。

3 单击用户名旁边的单选按钮，单击**解锁**。

管理组

如果您具有与 LDAP 服务器的有效连接，或者已使您的组织使用 SAML 身份提供者，则可以导入 LDAP 组或 SAML 组。此外，还可以编辑或删除导入的组。

导入组

要添加一组用户，可以导入 LDAP 组或 SAML 组。

前提条件

- 此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。
- 确认您具有与 LDAP 服务器的有效连接，或者为组织启用 SAML 身份提供者支持。

步骤

1 在顶部导航栏中，单击**管理**。

2 在左侧面板中的**访问控制**下，单击**组**。

此时将显示用户组列表。

3 单击**导入组**。

4 选择要从其导入用户组的源。

您只能查看源 LDAP 服务器或配置为身份提供者的 SAML 服务器。

源	操作
LDAP	从 LDAP 服务器导入用户组。 a 在文本框中输入全称或部分名称，然后单击**搜索**。 b 选择要导入的用户组，然后单击**添加**。
SAML	从 SAML 服务器导入用户组。输入要导入的组的名称。 每个组名称占用一个新行。

5 选择要为导入的用户组分配的角色。

6 单击**保存**。

删除组

可以通过删除 LDAP 组来从 VMware Cloud Director 组织中移除组。

删除 LDAP 组后，那些仅凭其在该组中的成员资格而拥有 VMware Cloud Director 帐户的用户将变为无效用户且无法登录。

前提条件

此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。

步骤

1 在顶部导航栏中，单击**管理**。

2 在左侧面板中的**访问控制**下，单击**组**。

此时将显示用户组列表。

3 单击要删除的组的名称旁边的单选按钮，然后单击**删除**。

4 要确认删除该组，请单击**确定**。

编辑组

可以从 VMware Cloud Director 租户门户编辑组。

前提条件

此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。

步骤

1 在顶部导航栏中，单击**管理**。

2 在左侧面板中的**访问控制**下，单击**组**。

此时将显示用户组列表。

3 单击要编辑的组名称旁边的单选按钮，然后单击**编辑**。

4 根据需要编辑组。

a 更改描述。

b 根据需要更改组成员的角色。

5 单击**保存**。

角色和权限

VMware Cloud Director 使用角色和权限来确定用户可以在组织中执行的操作。VMware Cloud Director 包含具有特定权限的许多预定义角色。

系统管理员和**组织管理员**必须为每个用户或组分配一个角色。同一名用户在不同的组织中可以具有不同的角色。**系统管理员**可以为整个系统创建角色并修改现有角色，而**组织管理员**只能为其管理的组织创建并修改角色。

VMware Cloud Director 租户门户允许**组织管理员**管理其组织中的角色。如果**系统管理员**将一个或多个预定义的租户角色发布到您的组织，则您作为**组织管理员**可以查看这些角色，但不能进行修改。不过，您可以创建具有类似权限的自定义租户角色并将其分配给组织中的用户。

有关预定义的角色及其权限的信息，请参见预定义角色及其权限。

预定义角色及其权限

每个 VMware Cloud Director 预定义角色都包含一组执行常用工作流操作所需的默认权限。默认情况下，所有预定义全局租户角色会发布到系统中的每个组织。

预定义提供者角色

默认情况下，仅提供者组织的本地提供者角色才为**系统管理员**和**多站点系统**角色。**系统管理员**可以创建其他自定义提供者角色。

系统管理员

系统管理员角色仅在提供者组织中存在。**系统管理员**角色包括系统中的所有权限。如需仅适用于**系统管理员**角色的权限列表，请参见《VMware Cloud Director 服务提供商管理门户指南》。**系统管理员**凭据在安装和配置过程中创建。**系统管理员**可在提供者组织中创建其他系统管理员和用户帐户。

多站点系统

用于为多站点部署运行检测信号进程。该角色只有一个权限，即**多站点：系统操作**，该权限允许发出 Cloud Director OpenAPI 请求以检索站点关联的远程成员的状态。

预定义全局租户角色

默认情况下，预定义全局租户角色及其包含的权限发布到所有组织。**系统管理员**可从各个组织取消发布权限和全局租户角色。**系统管理员**可以编辑或删除预定义全局租户角色。**系统管理员**可以创建和发布其他全局租户角色。

组织管理员

创建组织后，**系统管理员**可以将**组织管理员**的角色分配给组织中的任何用户。具有预定义**组织管理员**角色的用户可以管理其组织中的用户和组，并为其分配角色（包括预定义的**组织管理员**角色）。某个**组织管理员**创建或修改的角色对其他组织不可见。

目录作者

与预定义的**目录作者**角色关联的权限允许用户创建和发布目录。

vApp 作者

与预定义的 **vApp 作者**角色关联的权限允许用户使用目录并创建 vApp。

vApp 用户

与预定义的 **vApp 用户**角色关联的权限允许用户使用现有 vApp。

仅控制台访问权限

与预定义的**仅控制台访问权限**角色关联的权限允许用户查看虚拟机状态和属性并使用客户机操作系统。

遵从身份提供者

与预定义的**遵从身份提供程序**角色相关联的权限根据从用户的 OAuth 或 SAML 身份提供程序收到的信息确定。如果为用户或组分配了**遵从身份提供程序**角色，则要符合包含条件，身份提供程序提供的角色或组名称必须与组织中定义的角色或组名称完全匹配且大小写一致。

- 如果由 OAuth 身份提供程序定义用户，则会为此用户分配此用户的 OAuth 令牌的 `roles` 数组中指定的角色。
- 如果由 SAML 身份提供程序定义用户，则会将在 SAML 属性中指定的角色分配给用户，该属性的名称显示在 `RoleAttributeName` 元素中，该元素位于组织 `OrgFederationSettings` 的 `SamlAttributeMapping` 元素中。

如果为用户分配了**遵从身份提供者**角色，但组织中没有匹配的角色或组名称，则用户可以登录组织，但没有任何权限。如果身份提供程序将用户与某个系统级角色（例如**系统管理员**）相关联，则该用户可以登录到该组织，但没有任何权限。必须手动为此类用户分配角色。

每个预定义的角色都包含一组默认权限，**遵从身份提供者**角色除外。只有**系统管理员**才能修改预定义角色中的权限。如果**系统管理员**修改了某个预定义角色，则所做修改将传播到该角色在系统中的所有实例。

预定义全局角色中的权限

多个预定义全局角色共有各种权限。这些权限默认授予所有新组织，并且可在**组织管理员**创建的其他角色中使用。如需预定义租户角色中的权限列表，请参见 预定义全局角色中的权限。

预定义全局角色中的权限

多个预定义全局角色共有各种权限。这些权限默认授予所有新组织，并且可在**组织管理员**创建的其他角色中使用。

VMware Cloud Director 全局租户角色中包含的权限

本版本新增	权限名称	组织管理员	目录作者	vApp 作者	vApp 用户	仅控制台访问权限
	访问所有组织 VDC	✓				
	目录：从我的云添加 vApp	✓	✓	✓		
	目录：更改所有者	✓				
	目录：CLSP 发布订阅	✓	✓			
	目录：创建/删除目录	✓	✓			
	目录：编辑属性	✓	✓			
	目录：发布	✓	✓			
	目录：共享	✓	✓			
	目录：查看 ACL	✓	✓			
	目录：查看专用目录和共享目录	✓	✓	✓		
	目录：查看已发布目录	✓				

本版本新增	权限名称	组织管理员	目录作者	vApp 作者	vApp 用户	仅控制台访问权限
	自定义实体：查看组织中的所有自定义实体实例	✓				
	自定义实体：查看自定义实体实例	✓				
	磁盘：更改所有者	✓	✓			
	磁盘：创建	✓	✓	✓		
	磁盘：删除	✓	✓	✓		
	磁盘：编辑属性	✓	✓	✓		
✓	磁盘：查看加密状态	✓		✓		
	磁盘：查看属性	✓	✓	✓	✓	
	常规：管理员控制	✓				
	常规：管理员查看	✓				
	常规：发送通知	✓				
	组/用户：查看	✓				
	混合云环境运维：获取控制票证	✓				
	混合云环境运维：获取云传出通道票证	✓				
	混合云环境运维：获取云传入通道票证	✓				
	混合云环境运维：创建云传出通道	✓				
	混合云环境运维：创建云传入通道	✓				
	混合云环境运维：删除云传出通道	✓				
	混合云环境运维：删除云传入通道	✓				
	混合云环境运维：更新云传出通道端点标记	✓				
	混合云环境运维：查看云传出通道	✓				
	混合云环境运维：查看云传入通道	✓				
	组织网络：编辑属性	✓				
	组织网络：查看	✓				
	组织 vDC 计算策略：查看	✓	✓	✓	✓	
	组织 vDC 分布式防火墙：配置规则	✓				
	组织 vDC 分布式防火墙：查看规则	✓				

本版本新增	权限名称	组织管理员	目录作者	vApp 作者	vApp 用户	仅控制台访问权限
	组织 vDC 网关：配置 DHCP	✓				
	组织 vDC 网关：配置 DNS	✓				
	组织 vDC 网关：配置 ECMP 路由	✓				
	组织 vDC 网关：配置防火墙	✓				
	组织 vDC 网关：配置 IPSec VPN	✓				
	组织 vDC 网关：配置负载平衡器	✓				
	组织 vDC 网关：配置 NAT	✓				
	组织 vDC 网关：配置静态路由	✓				
	组织 vDC 网关：配置 Syslog	✓				
	组织 vDC 网关：转换为高级网络连接	✓				
	组织 vDC 网关：查看	✓				
	组织 vDC 网关：查看 DHCP	✓				
	组织 vDC 网关：查看 DNS	✓				
	组织 vDC 网关：查看防火墙	✓				
	组织 vDC 网关：查看 IPSec VPN	✓				
	组织 vDC 网关：查看负载平衡器	✓				
	组织 vDC 网关：查看 NAT	✓				
	组织 vDC 网关：查看静态路由	✓				
	组织 vDC 网络：编辑属性	✓				
	组织 vDC 网络：查看属性	✓		✓		
✓	组织 vDC 存储策略：查看功能	✓				
	组织 vDC 存储配置文件：设为默认值	✓				
	组织 vDC：编辑	✓				
	组织 vDC：编辑 ACL	✓				
	组织 vDC：管理防火墙	✓				
	组织 vDC：查看	✓	✓			
	组织 vDC：查看 ACL	✓				
	组织 vDC：查看衡量指标	✓				

本版本新增	权限名称	组织管理员	目录作者	vApp 作者	vApp 用户	仅控制台访问权限
	组织 vDC：VM-VM 关联性编辑	✓	✓	✓		
	组织：编辑关联设置	✓				
	组织：编辑联合设置	✓				
	组织：编辑 LDAP 设置	✓				
	组织：编辑租约策略	✓				
	组织：编辑 OAuth 设置	✓				
	组织：编辑密码策略	✓				
	组织：编辑属性	✓				
	组织：编辑配额策略	✓				
	组织：编辑 SMTP 设置	✓				
	组织：在编辑 VDC ACL 时从 IdP 导入用户/组	✓				
	组织：查看	✓	✓	✓		
	组织：查看衡量指标	✓				
	角色：创建、编辑、删除或复制	✓				
	服务库：查看服务库	✓				
	UI 插件：查看	✓	✓	✓	✓	
	vApp 模板/媒体：复制	✓	✓	✓		
	vApp 模板/媒体：创建/上载	✓	✓			
	vApp 模板/媒体：编辑	✓	✓	✓		
	vApp 模板/媒体：查看	✓	✓	✓	✓	
	vApp 模板：更改所有者	✓	✓			
	vApp 模板：签出	✓	✓	✓	✓	
	vApp 模板：下载	✓	✓			
	vApp：更改所有者	✓				
	vApp：复制	✓	✓	✓	✓	
	vApp：创建/重新配置	✓	✓	✓		
	vApp：删除	✓	✓	✓	✓	
	vApp：下载	✓	✓	✓		

本版本新增	权限名称	组织管理员	目录作者	vApp 作者	vApp 用户	仅控制台访问权限
	vApp：编辑属性	✓	✓	✓	✓	
	vApp：编辑 VM 计算策略	✓	✓	✓		
	vApp：编辑 VM CPU	✓	✓	✓		
	vApp：编辑 VM 硬盘	✓	✓	✓		
	vApp：编辑 VM 内存	✓	✓	✓		
	vApp：编辑 VM 网络	✓	✓	✓	✓	
	vApp：编辑 VM 属性	✓	✓	✓	✓	
	vApp：管理 VM 密码设置	✓	✓	✓	✓	✓
	vApp：电源操作	✓	✓	✓	✓	
	vApp：共享	✓	✓	✓	✓	
	vApp：快照操作	✓	✓	✓	✓	
	vApp：上载	✓	✓	✓		
	vApp：使用控制台	✓	✓	✓	✓	✓
	vApp：查看 ACL	✓	✓	✓	✓	
✓	vApp：查看 VM 和 VM 的磁盘加密状态	✓		✓		
	vApp：查看 VM 衡量指标	✓		✓	✓	
	vApp：VM 引导选项	✓	✓	✓		
	vApp：VM 元数据到 vCenter	✓	✓	✓		
	VDC 模板：实例化	✓				
	VDC 模板：查看	✓				

创建自定义租户角色

组织管理员可以使用租户门户在其管理的组织中创建自定义租户角色对象。

前提条件

此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。

步骤

1 在顶部导航栏中，单击**管理**。

2 在左侧面板中的**访问控制**下，单击**角色**。

此时将显示角色列表。

3 单击**添加**。

4 输入角色的名称和可选描述。

5 展开角色的权限，然后为角色选择权限。

权限按类别和子类别进行分组，以允许查看或管理对象。

选项	描述
访问控制	用于控制查看和管理特定对象的权限。
管理	用于控制管理访问的权限。
计算	用于控制访问和管理组织和提供者虚拟数据中心、vApp、组织虚拟数据中心模板、虚拟机组和虚拟机监控的权限。
扩展	用于控制对任何其他插件和 VMware Cloud Director 扩展进行访问的权限。
基础架构	用于控制基础架构对象（如数据存储、磁盘、主机等）的访问和管理的权限。
库	用于控制访问和管理任何目录和目录项的权限。
网络	用于控制访问和管理网络设置的权限。

6 单击**保存**。

编辑自定义租户角色

组织管理员可以使用租户门户编辑其管理的组织中的自定义租户角色对象。作为组织管理员，您只能查看系统管理员发布到您组织的全局租户角色。您无法编辑全局租户角色。

前提条件

此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。

步骤

1 在顶部导航栏中，单击**管理**。

2 在左侧面板中的**访问控制**下，单击**角色**。

此时将显示角色列表。

3 单击要编辑的角色旁边的单选按钮，然后单击**编辑**。

4 根据需要修改角色设置。

a 更改角色的名称和可选描述。

b 编辑角色的权限。

5 单击**保存**。

删除角色

组织管理员可以使用租户门户在其管理的组织中删除角色对象。

前提条件

此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。

步骤

1. 在顶部导航栏中，单击**管理**。
2. 在左侧面板中的**访问控制**下，单击**角色**。

   此时将显示角色列表。
3. 单击要删除的角色旁边的单选按钮，然后单击**删除**。
4. 单击**确定**，确认删除该角色。

配置身份提供程序

13

可以将您的云与外部身份提供程序集成并将用户和组导入到您的组织中。

您可以为组织使用 SAML 身份提供程序，也可以配置 LDAP 服务器连接。

本章讨论了以下主题：

- 为组织启用 SAML 身份提供者支持
- 编辑组织的 LDAP 设置
- 配置、测试和同步 LDAP 连接

为组织启用 SAML 身份提供者支持

使您的组织能够使用安全断言标记语言 (SAML) 身份提供程序（也称为单点登录）从 SAML 身份提供程序导入用户和组，并允许导入的用户使用在 SAML 身份提供程序中建立的凭据登录到组织。

在导入用户和组时，系统会从 SAML 令牌提取一系列属性（如果有），并使用它们来解读有关尝试登录的用户的相应信息。

- `email address = "EmailAddress"`
- `user name = "UserName"`
- `full name = "FullName"`
- `user's groups = "Groups"`
- `user's roles = "Roles"`

  可以配置角色属性。

如果未直接导入用户，但用户需要通过已导入组的成员资格登录，则必须提供组信息。一个用户可能属于多个组，因此在会话期间可能具有多个角色。

如果为导入的用户或组分配了**遵从身份提供者**角色，则会根据从该令牌的“角色”属性中收集的信息分配角色。如果使用了其他属性，则只能通过使用 API 配置此属性名称，并且只能配置“角色”属性。如果使用了**遵从身份提供程序**角色，但无法提取任何角色信息，则用户可以登录，但不具有执行任何活动的权限。

前提条件

- 此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。

- 确认您有权访问符合 SAML 2.0 的身份提供者。
- 确认您可以从 SAML 身份提供者接收所需的元数据。您必须将此元数据手动或作为 XML 文件导入到 VMware Cloud Director。元数据中必须包含以下信息：
  - 单点登录服务的位置
  - 单点注销服务的位置
  - 服务的 X.509 证书的位置

  有关配置和获取 SAML 提供者元数据的信息，请参见 SAML 身份提供者文档。

步骤

1. 在顶部导航栏中，单击**管理**。
2. 在**身份提供程序**下，单击 **SAML**。
3. 单击**编辑**。
4. 在**服务提供商**选项卡中，输入实体 ID。

   实体 ID 是您的组织对于身份提供程序的唯一标识符。可以使用您组织的名称或满足 SAML 身份提供程序要求的任何其他字符串。

   重要事项 指定实体 ID 后，无法删除。要更改实体 ID，您必须对组织执行完整的 SAML 重新配置。有关实体 ID 的信息，请参见 OASIS 安全断言标记语言 (SAML) 2.0 的断言和协议。
5. 单击**元数据**链接，下载适用于组织的 SAML 元数据。

   已下载的元数据必须原样提供给您的身份提供程序。
6. 查看证书过期日期，并（可选）单击重新生成以重新生成用来对联合消息进行签名的证书。

   证书包含在 SAML 元数据中，用于加密和签名。根据组织与 SAML 身份提供程序之间建立信任的方式，可能需要加密和签名中的一个或两者都需要。
7. 在**身份提供程序**选项卡上启用**使用 SAML 身份提供程序**开关。
8. 复制您收到的来自身份提供程序的 SAML 元数据并粘贴到文本框中，或单击**上载**以浏览到 XML 文件并上载其中的元数据。
9. 单击**保存**。

后续步骤

- 使用 VMware Cloud Director 元数据配置 SAML 提供者。请参见 SAML 身份提供者文档和《VMware Cloud Director 安装、配置和升级指南》。
- 从 SAML 身份提供程序导入用户和组。请参见第 12 章 管理用户、组和角色

编辑组织的 LDAP 设置

可以将组织配置为使用系统 LDAP 连接作为用户和组的共享源。可以将组织配置为使用单独的 LDAP 连接作为用户和组的专用源。

前提条件

此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。

步骤

1 在顶部导航栏中，单击**管理**。

2 在左侧面板中的**身份提供程序**下，单击 **LDAP**。

将显示当前 LDAP 设置。

3 在 **LDAP 设置**选项卡上，单击**编辑**。

4 为组织配置用户和组的 LDAP 源，然后单击**保存**。

选项	描述
不使用 LDAP	组织不使用 LDAP 服务器作为组织用户和组的源。
VMware Cloud Director 系统 LDAP 服务	组织使用您的服务提供商配置的 VMware Cloud Director 系统 LDAP 连接。 输入组织单位的标识名。
自定义 LDAP 服务	组织将使用专用 LDAP 服务器作为组织用户和组的源。

后续步骤

如果已选择**自定义 LDAP 服务**，请单击**自定义 LDAP** 选项卡配置、测试和同步 LDAP 连接。

配置、测试和同步 LDAP 连接

要配置 LDAP 连接，请设置 LDAP 服务器的详细信息。可以通过测试连接来确保输入的设置正确且用户和组属性已正确映射。成功进行 LDAP 连接后，可以随时将用户和组信息与 LDAP 服务器进行同步。

前提条件

如果您计划通过 SSL 连接到 LDAP 服务器 (LDAPS)，请确认 LDAP 服务器的证书与 Java 8 Update 181 中引入的端点标识相容。证书的公用名称 (CN) 或主体备用名称 (SAN) 必须与 LDAP 服务器的 FQDN 相匹配。有关详细信息，请参见《Java 8 版本变更》，网址为 https://www.java.com。

此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。

步骤

1 在**连接**选项卡中，输入 LDAP 连接所需的信息。

所需信息	描述
服务器	LDAP 服务器的主机名或 IP 地址。
端口	LDAP 服务器侦听的端口号。 对于 LDAP，默认端口号为 389。对于 LDAPS，默认端口号为 636。
基本标识名	基本标识名 (DN) 是 LDAP 目录中 VMware Cloud Director 要连接的位置。 要在根级别连接，请仅输入域组件，例如 **`DC=example,DC=com`**。 要连接到域树结构中的节点，请输入该节点的标识名，例如 **`OU=ServiceDirector,DC=example,DC=com`**。 连接到一个节点将限制 VMware Cloud Director 可用的目录范围。
连接器类型	LDAP 服务器的类型。可以是 **Active Directory** 或 **OpenLDAP**。
使用 SSL	如果您的服务器为 LDAPS，请选中此复选框。
接受所有证书	如果您的服务器为 LDAPS，请选中此复选框或者上载 LDAP SSL 证书。
自定义信任存储区	如果您的服务器为 LDAPS，请单击上载图标 (⤒)，然后导入 LDAP SSL 证书或选择**接受所有证书**。
身份验证方法	简单身份验证包括将用户的 DN 和密码发送到 LDAP 服务器。如果使用的是 LDAP，则 LDAP 密码将以纯文本形式通过网络发送。 如果要使用 Kerberos，则必须使用 vCloud API 配置 LDAP 连接。
用户名	输入具有域管理员权限的服务帐户的完整 LDAP 标识名 (DN)。VMware Cloud Director 使用此帐户查询 LDAP 目录和检索用户信息。 如果对 LDAP 服务器启用了匿名读取支持，则可以将这些文本框留空。
密码	连接到 LDAP 服务器的服务帐户的密码。 如果对 LDAP 服务器启用了匿名读取支持，则可以将这些文本框留空。

2 单击**用户属性**选项卡，查看用户属性的默认值，如果您的 LDAP 目录使用其他架构，请修改这些值。

3 单击**组属性**选项卡，查看组属性的默认值，如果您的 LDAP 目录使用其他架构，请修改这些值。

4 单击**保存**。

5 如果已选中**使用 SSL** 复选框，但是 LDAPS 服务器的证书尚不受信任，请在**信任证书**窗口中确认是否信任服务器端点提供的证书。

6 要测试 LDAP 连接设置和 LDAP 属性映射，请执行以下操作：

a 单击**测试**。

b 输入您配置的 LDAP 服务器用户的密码，然后单击**测试**。

如果连接成功，将显示绿色复选标记。

检索到的用户和组属性值将显示在表中。成功映射到 LDAP 属性的值将带有绿色复选标记。未映射到 LDAP 属性的值为空，并带有红色感叹号。

c 要退出，请单击**取消**。

7 要将 VMware Cloud Director 与配置的 LDAP 服务器同步，请单击**同步**。

VMware Cloud Director 会根据您在常规系统设置中设置的同步间隔，定期将用户和组信息与 LDAP 服务器同步。

等待几分钟，使同步完成。

结果

可以从新配置的 LDAP 服务器导入用户和组。

管理您的组织

14

作为**组织管理员**，您可以修改组织内的各种设置。可以修改组织的名称、电子邮件设置、域设置、元数据和策略等。

可以使用 VMware Cloud Director API 通过 MQTT 协议订阅有关组织中的事件和任务的消息。使用《VMware Cloud Director 安装、配置和升级指南》中的 MQTT 客户端查看有关订阅事件和任务的信息。

本章讨论了以下主题：

编辑组织名称和描述

可以编辑组织的全名和描述。

前提条件

此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。

步骤

1 在顶部导航栏中，单击**管理**。

2 在**设置**下，单击**常规**。

将显示常规设置列表，如组织名称、默认 URL、全名和描述。

3 要修改组织的全名和描述，请单击**编辑**。

4 应用必要更改，然后单击**保存**。

修改电子邮件设置

可以查看并修改系统管理员创建组织时设置的默认电子邮件设置。

需要报告重要信息时（例如，数据存储空间不足时）VMware Cloud Director 将发送警示电子邮件。默认情况下，组织会使用在系统级别指定的 SMTP 服务器向系统管理员或在系统级别指定的电子邮件地址列表发送警示电子邮件。如果您希望 VMware Cloud Director 将组织警示发送至并非在系统级别指定的一组电子邮件地址，或者如果您希望组织使用并非在系统级别指定的 SMTP 服务器发送警示，则可以在组织级别修改电子邮件设置。

前提条件

此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。

步骤

1 在顶部导航栏中，单击**管理**。

2 在**设置**下，单击**电子邮件**。

将显示组织的电子邮件设置。

3 单击**编辑**。

4 在 **SMTP 服务器**选项卡上编辑 SMTP 服务器设置。

a 选择使用自定义 SMTP 服务器还是默认服务器。

b 如果选择使用自定义 SMTP 服务器，请在 **SMTP 服务器名称**文本框中输入 SMTP 服务器的 DNS 主机名或 IP 地址。

c （可选） 输入 SMTP 服务器端口。

d （可选） 选择是否需要身份验证并输入用户名和密码。

5 要编辑通知设置，请单击**通知设置**选项卡。

a 选择使用自定义通知设置。

b 输入将显示为组织电子邮件发件人的电子邮件地址。

c （可选） 输入要用作电子邮件主题前缀的文本。

d （可选） 选择是将通知发送至所有组织管理员还是特定电子邮件地址。

e （可选） 如果选择将通知发送至特定电子邮件地址，请输入以逗号分隔的电子邮件地址。

6 单击**保存**。

测试 SMTP 设置

修改组织的电子邮件设置后，可以测试 SMTP 设置。

前提条件

此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。

步骤

1 在顶部导航栏中，单击**管理**。

2 在**设置**下，单击**电子邮件**。

将显示组织的电子邮件设置。

3 单击**测试**。

4 输入目标电子邮件地址和 SMTP 服务器密码以测试 SMTP 设置，然后单击**测试**按钮。

修改组织中虚拟机的域设置

您可以设置在组织中创建的虚拟机可以加入的默认 Windows 域。无论是否指定默认域，虚拟机始终可以加入它们具有凭据的域。

前提条件

此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。

步骤

1 在顶部导航栏中，单击**管理**。

2 在**设置**下，单击**客户机个性化**。

3 选择后可为组织中的虚拟机启用域加入功能。

4 输入域名、用户名和密码。

输入的凭据适用于普通域用户，而不是域管理员。

5 （可选） 输入帐户组织单元。

6 单击**保存**。

使用多个站点

通过 VMware Cloud Director 多站点功能，分布于各个地理位置的多个 VMware Cloud Director 安装（服务器组）的服务提供商或租户可以将这些安装及其组织作为单个实体进行管理和监控。

VMware Cloud Director 组织管理员**可以通过** 租户门户将关联站点上的各个组织关联起来。

有关站点关联的详细信息，请参见《VMware Cloud Director 服务提供商管理门户指南》。

配置和管理多站点部署

在**系统管理员**关联两个站点之后，任一成员站点的**组织管理员**都可以开始关联其组织。

要在两个组织（此处称为 Org-A 和 Org-B）之间创建关联，您必须是这两个组织的**组织管理员**，这样您才可以登录到每个组织，检索其本地关联数据，并将检索到的数据提交到另一组织。

重要事项 将两个组织相关联的过程在逻辑上可以分解为两个互补的配对操作。第一个操作（在此示例中）将 Site-A 的 Org-A 与 Site-B 的 Org-B 相配对。然后，您必须将 Site-B 的 Org-B 与 Site-A 的 Org-A 相配对。在这两个配对完成之前，该关联并未完成。

前提条件

- 必须关联组织所占用的站点。
- 您必须是两个站点的**系统管理员**或两个组织的**组织管理员**。

步骤

1 登录到 Site-A 的 Org-A 的 VMware Cloud Director 租户门户以检索其本地关联数据。

   a 单击**管理**。

   b 在**设置**下，单击**多站点**。

   c 要以 XML 格式下载数据，请单击**导出本地关联数据**。

   浏览器将数据保存在其下载文件夹的文件中。

2 登录到 Site-B 的 Org-B 的 VMware Cloud Director 租户门户，以提交 Site-A 的 Org-A 中的本地关联数据。

   a 单击**管理**。

   b 在**设置**下，单击**多站点**。

   c 单击**新建组织关联**。

   通过单击**新建关联 XML** 文本框下方的上载箭头，并选择在步骤 步骤 1 中下载的本地关联数据，将在步骤 步骤 1 中下载的关联数据提交到 Org-B。

   d 单击**下一步**以确认并提交数据。

   系统将 Site-A 的 Org-A 与 Site-B 的 Org-B 配对。

   e 单击**完成**以查看关联的组织。

   f 要查看已关联组织的详细信息或删除关联，单击**组织名称**卡。

3 通过重复步骤 1 和步骤 2 完成该关联，以从 Org-B 检索本地关联数据并将其提交到 Org-A。

了解租约

创建组织时需要指定租约。 租约通过指定 vApp 可以运行的最长时间以及 vApp 和 vApp 模板可以存储的最长时间，来控制组织的存储资源和计算资源。

运行时租约旨在防止非活动的 vApp 消耗计算资源。例如，如果用户启动 vApp 并在节假日继续运行而不停止，则 vApp 将继续消耗资源。

用户启动 vApp 时运行时租约即开始。运行时租约到期时，VMware Cloud Director 将停止 vApp。

存储租约旨在防止未使用的 vApp 和 vApp 模板消耗存储资源。用户停止 vApp 时 vApp 存储租约即开始。存储租约不会影响正在运行的 vApp。当用户将 vApp 模板添加到 vApp、将 vApp 模板添加到工作区或者下载、复制或移动 vApp 模板时，vApp 模板存储租约即开始。

存储租约到期时，VMware Cloud Director 将根据您设置的组织策略将 vApp 或 vApp 模板标记为已过期，或者删除 vApp 或 vApp 模板。

修改组织内的 vApp 和 vApp 模板租约策略

可以查看并修改创建组织时系统管理员设置的默认策略。

前提条件

此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。

步骤

1 在顶部导航栏中，单击**管理**。

2 在**设置**下，单击**策略**。

您可以查看**系统管理员**设置的默认策略。

3 单击**编辑**。

4 编辑 vApp 租约。

vApp 租约通过指定 vApp 可以运行的最长时间以及 vApp 可以存储的最长时间来控制组织的存储资源和计算资源。此外，您还可以指定 vApp 存储租约到期时执行何种操作。

a 要定义 vApp 自动停止前可以运行的时间，请输入最大运行时租约。

b 选择运行时到期操作，如关闭电源或挂起。

c 要定义停止的 vApp 在自动清理前仍然可用的时间，请输入最大存储租约。

d 选择存储清理操作，例如永久删除 vApp 或将其移至过期项目。

5 编辑 vApp 模板租约。

vApp 模板租约通过指定 vApp 模板可以存储的最长时间来控制组织的存储资源和计算资源。此外，您还可以指定 vApp 模板存储租约到期时执行何种操作。

a 要定义 vApp 模板在自动清理前仍然可用的时间，请输入最大存储租约。

b 选择存储清理操作，例如永久删除 vApp 模板或将其移至过期项目。

6 单击**确定**。

修改组织中虚拟机的默认配额

可以查看并修改创建组织时系统管理员设置的默认配额策略。

配额可确定组织中的每个用户可在组织虚拟数据中心内存储并打开电源的虚拟机数量。对于添加到组织的所有新用户而言，您指定的配额将成为默认值。在用户级别设置的配额优先于在组织级别设置的配额。

前提条件

此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。

步骤

1 在顶部导航栏中，单击**管理**。

2 在**设置**下，单击**策略**。

您可以查看**系统管理员**设置的默认策略。

3 单击**编辑**。

4 在无限数量的虚拟机与指定数量之间做出选择。

5 在无限数量已打开电源的虚拟机与指定数量之间做出选择。

6 单击**确定**。

修改组织内的密码和用户帐户策略

可以查看并修改创建组织时系统管理员设置的默认密码和用户帐户策略。

密码和用户帐户策略定义了用户输入的密码无效时 VMware Cloud Director 的行为。

前提条件

此操作需要预定义的**组织管理员**角色中包含的权限或一组等效权限。

步骤

1 在顶部导航栏中，单击**管理**。

2 在**设置**下，单击**策略**。

您可以查看**系统管理员**设置的默认策略。

3 单击**编辑**。

4 启用在多次无效登录尝试之后锁定用户帐户的功能。

5 输入锁定帐户之前的无效尝试登录次数。

6 输入帐户被锁定的用户无法重新登录的时间间隔（以分钟为单位）。

7 单击**确定**。

使用服务库

15

VMware Cloud Director 中的服务库项目是 vRealize Orchestrator 工作流，可用于扩展云管理功能，并帮助提供商管理员或租户管理员监控和操作不同的服务。

本章讨论了以下主题：

搜索服务

VMware Cloud Director 租户门户中的**服务库**页面列出了导入到 VMware Cloud Director 并发布到您组织的 vRealize Orchestrator 工作流集。

前提条件

此操作要求在预定义的用户角色中包含服务库权限。

步骤

1 在顶部导航栏中，单击**库**，然后在**服务**下，选择**服务库**。

此时将以卡视图显示服务项列表，每页显示 12 项，并按名称的字母顺序排序。每个卡会显示服务的名称以及 vRealize Orchestrator 导入的服务类别所对应的标记。

2 在页面顶部的**搜索**文本框中，输入服务名称或服务类别名称的第一个单词。

a 选择是要在服务名称还是服务类别名称中搜索。

搜索结果将显示在每页 12 项的卡视图中，按名称的字母顺序排序。

执行服务

您可以从 VMware Cloud Director 租户门户中的“服务库”页面执行服务。

前提条件

此操作要求在预定义的用户角色中包含服务库权限。

步骤

1 在顶部导航栏中，单击**库**，然后在**服务**下，选择**服务库**。

此时将以卡视图显示服务项列表，每页显示 12 项，并按名称的字母顺序排序。每个卡会显示服务的名称以及 vRealize Orchestrator 导入的服务类别所对应的标记。

2 搜索要执行的服务。

3 在服务卡片上单击**执行**。

此时将打开一个新对话框。您必须输入服务的必需输入参数的值。

4 单击**完成**，确认执行服务。

后续步骤

您可以在**近期任务**视图中监控执行的状态。有关详细信息，请参见查看任务。

使用自定义实体定义

16

VMware Cloud Director 中的自定义实体定义是绑定到 vRealize Orchestrator 对象类型的对象类型。VMware Cloud Director 组织内的用户可以根据需要拥有、管理和更改这些类型。通过执行服务，组织用户可以实例化自定义实体，并将操作应用于对象实例。

本章讨论了以下主题：

搜索自定义实体

您可以搜索已发布到您组织的自定义实体。

前提条件

此操作要求在预定义的用户角色中包含自定义实体权限。

步骤

1 在顶部导航栏中，单击**库**，然后在**服务**下选择**自定义实体定义**。

此时将以卡视图显示自定义实体列表，每页显示 12 项，并按名称的字母顺序排序。每个卡会显示自定义实体的名称、实体映射到的 vRealize Orchestrator 类型、实体的类型以及描述（如果有）。

2 在页面顶部的**搜索**文本框中，输入要查找的实体名称的单词或字符。

搜索结果将显示在每页 12 项的卡视图中，按名称的字母顺序排序。

编辑自定义实体定义

您可以修改自定义实体的名称和描述。您无法更改实体的类型或实体所绑定的 vRealize Orchestrator 对象类型，这些是自定义实体的默认属性。如果要修改任何默认属性，您必须删除自定义实体定义并重新创建它。

前提条件

此操作要求在预定义的用户角色中包含自定义实体权限。

步骤

1 在顶部导航栏中，单击**库**，然后在**服务**下选择**自定义实体定义**。

此时将以卡视图显示自定义实体列表，每页显示 12 项，并按名称的字母顺序排序。每个卡会显示自定义实体的名称、实体映射到的 vRealize Orchestrator 类型、实体的类型以及描述（如果有）。

2 在所选自定义实体的卡中，选择**操作 > 编辑**。

此时将打开一个新对话框。

3 修改自定义实体定义的名称或描述。

4 单击**确定**，确认所做的更改。

添加自定义实体定义

您可以创建自定义实体，并将其映射到现有的 vRealize Orchestrator 对象类型。

前提条件

此操作要求在预定义的用户角色中包含自定义实体权限。

步骤

1 在顶部导航栏中，单击**库**，然后在**服务**下选择**自定义实体定义**。

此时将以卡视图显示自定义实体列表，每页显示 12 项，并按名称的字母顺序排序。每个卡会显示自定义实体的名称、实体映射到的 vRealize Orchestrator 类型、实体的类型以及描述（如果有）。

2 单击 ＋ 图标以添加新的自定义实体。

此时将打开一个新对话框。

3 按照**自定义实体定义**向导的步骤执行操作。

步骤	
名称和描述	输入新实体的名称和（可选）描述。 输入实体类型的名称，例如 `sshHost`。
vRO	从下拉菜单中，选择要用于映射自定义实体定义的 vRealize Orchestrator。 **注** 如果您有多个 vRealize Orchestrator 服务器，则必须分别为每个服务器创建自定义实体定义。

步骤	
类型	单击视图列表图标 ( ) 以浏览按插件分组的可用 vRealize Orchestrator 对象类型。例如，**SSH > 主机**。如果您知道类型的名称，则可以直接输入到文本框中。例如：`SSH:Host`。
检查	检查您指定的详细信息，然后单击**完成**以完成创建。

结果

新的自定义实体定义将显示在卡视图中。

自定义实体实例

使用作为 VMware Cloud Director 中已定义为自定义实体定义的对象类型的输入参数运行 vRealize Orchestrator 工作流时，会将输出参数显示为自定义实体的实例。

前提条件

此操作要求在预定义的用户角色中包含自定义实体权限。

步骤

1 在顶部导航栏中，单击**库**，然后在**服务**下选择**自定义实体定义**。

此时将以卡视图显示自定义实体列表，每页显示 12 项，并按名称的字母顺序排序。每个卡会显示自定义实体的名称、实体映射到的 vRealize Orchestrator 类型、实体的类型以及描述（如果有）。

2 在所选自定义实体的卡中，单击**实例**。

可用的实例将显示在网格视图中。

3 单击每个实体左侧的列表栏 ( ) 以显示关联的工作流。

单击工作流会发起工作流运行，这需要将实体实例作为输入参数。

将操作关联到自定义实体

通过将操作关联到自定义实体定义，您可以对特定自定义实体的实例执行一组 vRealize Orchestrator 工作流。

前提条件

此操作要求在预定义的用户角色中包含自定义实体权限。

步骤

1 在顶部导航栏中，单击**库**，然后在**服务**下选择**自定义实体定义**。

此时将以卡视图显示自定义实体列表，每页显示 12 项，并按名称的字母顺序排序。每个卡会显示自定义实体的名称、实体映射到的 vRealize Orchestrator 类型、实体的类型以及描述（如果有）。

2 在选定自定义实体的卡上，选择**操作 > 关联操作**。

此时将打开一个新对话框。

3 按照**将自定义实体关联到 VRO 工作流**向导的步骤执行操作。

步骤	详细信息
选择 VRO 工作流	选择列出的工作流之一。这些工作流是**服务库**页面中可用的工作流。
选择工作流输入参数	从列表中选择可用的输入参数。您可以将 vRealize Orchestrator 工作流的类型与自定义实体定义的类型相关联。
检查关联	检查您指定的详细信息，然后单击**完成**以完成关联。

示例

例如，如果您有一个类型为 `SSH:Host` 的自定义实体，则可以通过选择与自定义实体类型匹配的 `sshHost` 输入参数将其与 `Add a Root Folder to SSH Host` 工作流相关联。

从自定义实体定义取消关联操作

您可以从关联操作的列表中移除 vRealize Orchestrator 工作流。

前提条件

此操作要求在预定义的用户角色中包含自定义实体权限。

步骤

1 在顶部导航栏中，单击**库**，然后在**服务**下选择**自定义实体定义**。

此时将以卡视图显示自定义实体列表，每页显示 12 项，并按名称的字母顺序排序。每个卡会显示自定义实体的名称、实体映射到的 vRealize Orchestrator 类型、实体的类型以及描述（如果有）。

2 在所选自定义实体的卡中，选择**操作 > 取消关联操作**。

此时将打开一个新对话框。

3 选择您要移除的工作流，然后单击**取消关联操作**。

vRealize Orchestrator 工作流将不再与自定义实体相关联。

发布自定义实体

您必须发布自定义实体，以便其他租户或服务提供商的用户可以使用自定义实体实例作为输入参数来运行工作流。

前提条件

此操作要求在预定义的用户角色中包含自定义实体权限。

步骤

1 在顶部导航栏中，单击**库**，然后在**服务**下选择**自定义实体定义**。

此时将以卡视图显示自定义实体列表，每页显示 12 项，并按名称的字母顺序排序。每个卡会显示自定义实体的名称、实体映射到的 vRealize Orchestrator 类型、实体的类型以及描述（如果有）。

2 在所选自定义实体的卡中，选择**操作 > 发布**。

此时将打开一个新对话框。

3 选择将自定义实体定义发布到服务提供商、所有租户还是仅发布到所选租户。

4 单击**保存**，确认所做的更改。

此时自定义实体定义可供选定相关方使用。

删除自定义实体

如果自定义实体不再使用、配置不正确或者要将 vRealize Orchestrator 类型映射到不同的自定义实体，则可以删除自定义实体定义。

前提条件

此操作要求在预定义的用户角色中包含自定义实体权限。

步骤

1 在顶部导航栏中，单击**库**，然后在**服务**下选择**自定义实体定义**。

此时将以卡视图显示自定义实体列表，每页显示 12 项，并按名称的字母顺序排序。每个卡会显示自定义实体的名称、实体映射到的 vRealize Orchestrator 类型、实体的类型以及描述（如果有）。

2 在所选自定义实体的卡中，选择**操作 > 删除**。

3 确认该删除操作。

自定义实体将从卡视图中移除。