vCloud Director 安全

VMware Cloud Director 9.5
vCloud Director 9.1

vmware®

您可以从 VMware 网站下载最新的技术文档：

https://docs.vmware.com/cn/。

如果您对本文档有任何意见或建议，请将反馈信息发送至：

docfeedback@vmware.com

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

版权所有 © 2010-2020 VMware, Inc. 保留所有权利。 版权和商标信息

目录

简介

1

VMware vCloud Director 是用于提供云计算服务的灵活系统。它利用并扩展了 VMware 核心虚拟化和管理技术来支持云环境。

由于系统的开发和测试考虑到多租户架构、可扩展性和其他安全问题，因此它的部署方式会对整个系统的安全造成巨大影响。本文档介绍了系统可能面临的一些威胁、整个 VMware 软件堆栈安全功能及其使用的相关组，例如数据库。

没有任何准则集能够涵盖所有可能的客户用例。每个 vCloud Director 部署都有自己的 IT 环境，但网络拓扑、内部安全系统和标准、客户要求以及用例存在差异。将提供一些常规准则，以提高系统的整体安全性。在适用的情况下，还会考虑提供更具体的使用情况，以及针对这些特定用例量身定制的准则。不过，您选择遵守本指南中的哪些具体建议要视您的独特部署环境以及您认为组织面临并希望缓解的风险而定。

一般情况下，对 vCloud Director 的威胁分为两类：内部威胁和外部威胁。内部威胁通常涉及多租户架构问题、以托管云环境为目标的外部威胁，但是这些威胁通常不严重且不紧急。例如，存在攻击托管环境安全的内部威胁。

除了本文档中的以下指南，您还应注意查看 http://www.vmware.com/security/advisories.html 中的安全建议，并使用该页面上的表单注册电子邮件警示。有关 vCloud Director 的其他安全指导和最新建议也将在此页面上发布。

建议范围

本指南中提供的建议仅限特定于 vCloud Director 的安全管理问题。对于在 Linux 平台上托管的 Web 应用程序，vCloud Director 中存在这两个类别的安全漏洞，这些信息记录在其他位置。

请务必记住，软件的安全部署只是整体安全过程的一部分，该过程中还包括物理安全、培训、运维过程、修补程序策略、升级和响应计划、灾难恢复和以及许多其他主题。这些辅助主题中的大部分都不在本指南讨论范围内。

威胁

2

vCloud Director 的安全威胁大致可以归类为来自系统及其租户内部的内部威胁或来自系统外部的外部威胁。外部威胁包括对为托管 vCloud Director 服务器组而创建的基础架构造成的威胁，以及对已安装的 vCloud Director 软件造成的威胁。

多租户和内部威胁

vCloud Director 旨在使租户能够对 VMware vSphere ® 网络、计算和存储资源执行受管访问。租户用户可以登录到 vCloud Director，且通常获得部署和/或使用虚拟机、使用存储、运行应用程序以及（在有限范围内）与其他用户共享资源的权限。

vCloud Director 的一个主要功能是，不支持非管理用户直接查看或访问大多数系统级资源，包括物理主机信息，例如 IP 地址、MAC 地址、CPU 类型、ESXi 访问权限、物理存储位置等。但是，用户仍然可以试图访问运行已启用云的应用程序的系统基础架构相关信息。如果他们能够执行此操作，则可以更便利地针对系统的较低级别发动攻击。

即使在虚拟化资源级别，用户仍可以试图使用其合法访问权限对本来无权访问的系统部分进行未经授权访问，如属于其他组织的资源。他们可能会试图升级特权，特别是，获取为管理员预留的操作的访问权限。无论有意还是无意，用户也可能会试图执行破坏系统整体可用性和性能的操作，个别情况下可能会导致对其他用户“拒绝服务”。

此外，通常存在各种各样的管理用户。这些管理用户包括 vCloud Director 站点的系统管理员、租户组织管理员、数据库和网络管理员以及有权访问 ESXi、vCenter 以及运行管理工具的客户机操作系统的用户。这些用户比普通用户具有更高的特权，且通常能够直接登录到内部系统。但是，其特权没有限制。因此，他们有可能也会试图升级特权或执行有害操作。

显然，保护 vCloud Director 免受这些威胁不仅需要确保 vCloud Director、vSphere 和 VMware NSX® 的架构、设计和实施安全，而且还需为其他安全系统以及部署这些安全系统的基础架构提供安全保障。由于这些系统的灵活性和动态性质，遵循所有这些组件的适用安全配置指南极为重要。

安全托管和外部威胁

外部威胁来自云外部的系统和用户，包括 Internet、通过其 API 和 Web 界面（vCloud Director Web 控制台和 vCloud Director 租户门户）攻击 vCloud Director，以及 vApp 传输服务和虚拟机远程控制台。无法访问系统的远程用户可能会试图以授权用户身份进行访问。这些接口的经身份验证的用户也可能会被视为外部威胁的来源，因为他们可能会试图利用未经身份验证的用户无法访问的系统中的漏洞。

通常情况下，为了获取信息，访问服务，或仅仅是通过破坏系统可用性或系统和信息完整性来中断云操作，这些参与者会试图利用系统实施或其部署中的缺陷。正如这些攻击描述所表明的那样，其中一些攻击会违反 vCloud Director 尝试强制实施的租户边界和硬件抽象层。尽管系统不同层的部署会影响这些威胁的缓解，但面向外部的接口（包括防火墙、路由器、VPN 等）是最关键的问题。

vCloud Director 架构和安全功能

3

vCloud Director 提供 VMware vSphere ® 和 VMware NSX® 基础架构即服务，从而支持在云环境中执行要求的租户隔离。

vCloud Director 服务器组由一台或多台 Linux 服务器组成。该组中的每台服务器均运行名为 vCloud Director 单元的服务集合。所有单元共享一个 vCloud Director 数据库，并连接到多个 vCenter Server 系统及其管理的 ESXi 主机以及提供网络服务的 NSX Manager。

图 3-1. vCloud Director 架构图

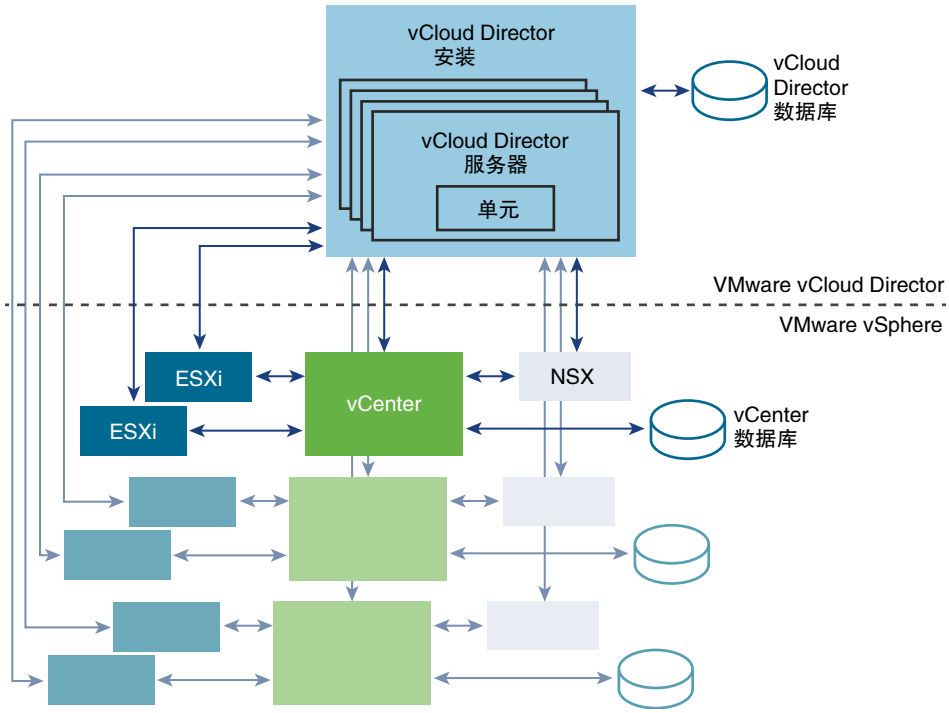


图 图 3-1. vCloud Director 架构图 显示了一个 vCloud Director 服务器组（安装）。在该服务器组中，可能有多个 vCloud Director 服务器主机，每个主机运行一个单元。服务器组一起共享 vCloud Director 数据库和 NFS 文件共享（未显示）。云抽象使用 vCloud Director 软件并利用 vCenter 和 NSX 中的功能构建，它在图中显示为连接到服务器组。vCloud Director 组织及其用户在创建和管理工作负载时不直接与 vCenter 和 NSX 交互。系统管理员以外的任何用户与 vCenter 和 NSX 的所有交互都显示为 vCloud Director 对象上的 vCloud Director 操作。访问和操作 vCloud Director 对象的权限是基于角色的。预定义的角色提供常见任务的基准访问权限。组织管理员还可以创建自定义角色，以便利用具有细化权限的数组。

后续小节中介绍了虚拟计算层、云抽象和虚拟网络连接层的安全性。

本章讨论了以下主题：

- 虚拟机安全和隔离
- 安全性和 vCloud Director 抽象
- 安全性和虚拟网络连接层

虚拟机安全和隔离

本文档介绍了安全性和网络隔离，我们希望评估网络隔离和流量隔离控制不足带来的风险并选择建议的纠正措施。

了解网络分段时，我们将了解信任区域的概念。信任区域是一种主动安全控制，可控制对网络流量的访问。从广义定义来讲，信任区域是数据相对自由流动的网络分段，而数据流入和流出信任区域会受到更强的限制。信任区域示例包括：

- 外围网络（也称为隔离区或 DMZ）
- 支付卡行业 (PCI) 持卡人数据环境
- 站点特定的区域，如根据部门或职能的分段
- 应用程序定义的区域，如某 Web 应用程序的三层

安全性和底层虚拟化层

vCloud Director 安全性，尤其是保护云租户免受内部威胁，很大程度上通过安全性设计和底层虚拟化层的特定配置来实现，包括 vSphere 的设计和配置、vCloud Director 软件定义的网络的安全性增强、NSX 技术的利用以及 ESXi 主机自身的安全性。

安全性和 vCloud Director 抽象

vCloud Director 在 vSphere 操作与租户日常运维需求之间实施严格隔离。

vCloud Director 抽象允许服务提供商将 vApp 的创建、管理和使用委派给租户组织（或 IT 部门将这些功能委派给业务团队）。租户组织管理员和用户不对 vMotion、vSAN 等 vCenter 功能进行操作或管理。租户只负责将工作负载 (vApp) 部署到资源池和存储配置文件并将其连接到组织拥有的组织 VDC 网络中。由于组织管理员和用户从不登录到 vCenter，因此不可能存在授予用户过多权限的 vCenter 权限配置错误。此外，提供商可以随意更改资源池和存储配置文件的构成，而无需组织执行任何修改。

更重要的是，该抽象会将不同的组织相互隔离。即使碰巧为他们分配了公共网络、数据存储或资源池，他们也不能相互修改或甚至查看 vApp。（连接到同一外部网络的 vApp 属于例外情况，因为它们共享同一个 vSwitch。）为每个租户组织提供自己的专用数据存储、网络和资源池，虽然系统没有此要求，但此操作可使服务提供商在组织之间更好地进行隔离。

限制租户对系统信息的访问

尽管 vCloud Director 旨在向租户隐藏系统级操作，但系统的某些功能可以配置为提供可能被恶意租户滥用的信息。

禁止向客户机发送主机性能数据。

在安装了 VMware Tools 的 Windows 操作系统中，vSphere 会包含虚拟机性能计数器。默认情况下，vSphere 不会向客户机虚拟机公开主机信息。由于物理主机相关信息可能会被恶意租户滥用，因此您应确认已配置此默认行为。有关详细信息，请参见《vSphere 安全性》中的确认已禁止向客户机发送主机性能数据。

限制虚拟机衡量指标的收集

vCloud Director 可收集提供有关虚拟机性能和资源消耗的最新信息和历史信息的衡量指标。由于其中的某些衡量指标包含物理主机相关信息，而这些信息可能会被恶意租户滥用，因此您应考虑将衡量指标收集子系统配置为仅收集不会遭受恶意使用的衡量指标。有关详细信息，请参见《vCloud Director 管理员指南》中的配置衡量指标收集。

使用扩展要小心谨慎

vCloud Director 支持一系列可扩展性方法。尽管这些方法旨在防止任何扩展获取未授予租户用户的权限或升级安装时分配给他们的特权，但扩展会提供（无论有意还是无意）额外的攻击面，而了解该扩展的人员会利用这些攻击面。服务提供商和租户管理员在提供、查看或安装扩展时应格外小心。此外，仔细管理允许的扩展以及使用适当的安全措施（如 `X-Content-Type-Options: nosniff` 标头）可以防止插件加载恶意内容。

安全性和虚拟网络连接层

vCloud Director 网络连接利用 vSphere 和 NSX 的软件定义的网络连接功能为租户提供共享网络资源的安全访问。服务提供商只负责提供外部连接和确保这些连接可供租户使用所需的网络连接基础架构，以及将系统级网络连接资源分配给网络池，以便可供租户使用。

vCloud Director 简要概述旨在建立一个上下文环境，并从安全配置角度讨论提供商级和租户级网络连接要求。vCloud Director 文档详细介绍了这些功能，网址：http://docs.vmware.com。

提供商级网络资源

在典型情况下，服务提供商负责在 vCloud Director 与外部网络（如 Internet）或客户的企业网络之间创建一个或多个连接。此类网络实质上是商用 IP 网络连接。如果此类网络上的数据包在物理级别被拦截，则不会提供保密性，而且不提供任何 vCloud Director VLAN 或 VXLAN 网络隔离功能。

要启用租户组织网络连接，服务提供商必须创建一个或多个网络池，并以可供租户组织使用的形式聚合来自 ESXi Dvswitch 和端口组的资源。（外部网络不使用网络池中的资源。）VXLAN 支持的网络池或 VLAN 支持的网络池使用 VLAN 在整个 vNetwork Distributed Switch 内提供隔离。vCloud Director VXLAN 网络也可以通过在 ESXi 内核中将第 2 层数据包封装在其他第 2 层数据包中 (MAC-in-MAC) 提供隔离，这样取消封装数据包时，内核能够将这些数据包传输到正确的客户机虚拟机（连接到在这种池外部创建的网络）。

服务提供商还负责创建和管理位于租户为自己创建的网络与系统级资源（例如 ESXi 提供的交换机和端口组）之间的 NSX 基础架构。通过这些资源，租户组织可以创建自己的网络。

组织 VDC 网络

组织 VDC 网络允许组织 VDC 中的虚拟机相互通信以及访问其他网络，包括组织 VDC 网络和外部网络，可以直接通信，也可以通过提供防火墙和 NAT 服务的 Edge 网关通信。

- 直连组织 VDC 网络可以直接连接到外部网络。只有系统管理员才可以创建直连组织 VDC 网络。
- 路由组织 VDC 网络可以通过 Edge 网关连接到外部网络。路由组织 VDC 网络还需要使用包含的 VDC 才能包含网络池。系统管理员使用 Edge 网关置备组织 VDC 并将其与网络池关联后，组织管理员或系统管理员可以在该 VDC 中创建路由组织 VDC 网络。
- 隔离组织 VDC 网络不需要 Edge 网关或外部网络，但要求包含的 VDC 与网络池相关联。系统管理员使用网络池创建组织 VDC 后，组织管理员或系统管理员可以在该 VDC 中创建隔离组织 VDC 网络。

表 3-1. 组织 VDC 网络的类型及其要求

组织 VDC 网络连接	描述	要求
直接连接到外部网络。	提供与组织 VDC 外部的计算机和网络的直接第 2 层连接。此组织 VDC 外部的计算机可以直接连接到组织 VDC 中的计算机。	云必须包含外部网络。
路由连接到外部网络。	通过 Edge 网关提供对组织 VDC 外部的计算机和网络的受控访问。系统管理员和组织管理员可以在网关上配置网络地址转换 (NAT) 和防火墙设置，以便可从外部网络访问 VDC 中的特定虚拟机。	VDC 必须包含 Edge 网关和网络池。
未连接到外部网络。	提供组织 VDC 中的计算机可连接的专用隔离网络。此组织 VDC 外部的计算机无法与该网络进行入站或出站连接。	VDC 必须包含网络池。

默认情况下，只有包含网络的组织 VDC 中的虚拟机可以使用该网络。创建组织 VDC 网络时，可以将其指定为共享网络。共享组织 VDC 网络可供组织中的所有虚拟机使用。

vApp 网络

每个 vApp 包含一个 vApp 网络。vApp 网络是逻辑网络，可以控制 vApp 中的虚拟机相互连接以及与组织 VDC 网络连接的方式。用户可以创建和更新 vApp 网络并将其连接到组织 VDC 网络，可以直接连接，也可以使用 NAT 和防火墙保护连接。

基础架构安全

4

本指南的大部分内容都与保护 vCloud Director 自身有关，但是整体系统安全还要求保护 vCloud Director 所依赖的基础架构，包括 vSphere、NSX、单元 Linux 平台和 vCloud Director 数据库。

安装前将最新安全修补程序应用于每个基础架构组件是一个关键步骤，持续监控以确保这些组件处于最新修补程序级别也至关重要。

保护 VMware 基础架构

保护 vSphere 和 NSX 是保护 vCloud Director 的关键第一步。管理员应查看 https://www.vmware.com/security/hardening-guides.html 中提供的检查表指南，另外还要参见以下文档中提供的更详细的安全信息：

vSphere 安全	《vSphere 安全性》。https://docs.vmware.com/cn/VMware-vSphere/6.0/com.vmware.vsphere.security.doc/GUID-52188148-C579-4F6A-8335-CFBCE0DD2167.html
NSX 安全	《保护 VMware NSX for vSphere》。https://communities.vmware.com/docs/DOC-27674 和 https://communities.vmware.com/docs/DOC-28142。

保护单元平台

vCloud Director 单元在基于 Linux 的操作系统上使用安装期间创建的非特权用户 (`vcloud.vcloud`) 身份运行。《vCloud Director 发行说明》中包含受支持的单元平台操作系统的列表。保护单元平台（无论是物理还是虚拟单元平台）是保护 vCloud Director 的关键部分。

应向单元平台应用标准安全强化过程，包括禁用不必要的网络服务、移除不必要的软件包、限制远程 root 用户访问和强制使用强密码策略。尝试使用集中式身份验证服务，例如 Kerberos。考虑安装监控和入侵检测工具。

可以在单元 OS 实例上安装其他应用程序和置备其他用户，但不建议您这么做。扩大单元操作系统的访问权限可能会降低安全性。

安装后保护敏感文件

安装期间，vCloud Director 会将包括密码在内的安装数据写入单元 Linux 主机的本地文件系统的文件中。这些文件（即 `global.properties` 和 `responses.properties`）均在 `$VCLOUD_HOME/etc` 下，其中包含您向服务器组添加更多服务器时必须重用的敏感信息。`Responses.properties` 文件包含运行配置脚本时管理员提供的响应。该文件包含 vCloud Director 数据库密码和系统密钥库密码的加密版本。如果对该文件进行未授权访问，将使攻击者能够使用与配置脚本中指定的数据库用户相同的权限访问 vCloud Director 数据库。`Global.properties` 文件中还包含除单元管理员以外的其他任何人均不能访问的加密凭据。

创建时，`responses.properties` 和 `global.properties` 文件受到 `$VCLOUD_HOME/etc` 文件夹和文件本身的访问控制的保护。请勿更改文件或文件夹的权限，因为可能会授予过多的访问权限，这会降低安全性，或过度限制访问权限，导致 vCloud Director 软件无法正常使用。为了确保访问控制正常运行，vCloud Director 服务器的物理和逻辑访问权限必须严格限于需要登录且具有所需最低访问级别的用户。这需要通过 `sudo` 和其他最佳做法限制 root 帐户的使用，这些内容不在本文档讨论范围内。此外，必须使用从备份自身单独管理的密钥严格保护和加密服务器的所有备份。

有关更多详细信息，请参见《vCloud Director 安装和升级指南》中的保护和重用响应文件。

管理凭据

确保用于对单元、vSphere、vCloud Director 数据库、外部防火墙和其他设备进行管理访问的所有凭据都遵守相应的密码复杂性标准。请尽可能考虑对密码使用过期和轮换策略。不过请注意，数据库过期或更改后，vSphere 或 NSX 密码导致使部分或整个云基础架构无法正常工作，直到使用新密码更新 vCloud Director。

务必从“深度防御”角度出发，更改 vCloud Director 环境中不同服务器的管理密码，包括 vCloud Director 单元、vCloud Director 数据库、vSphere 服务器和 NSX Manager。这样，即使一组凭据遭到入侵（例如，来自于从组织离职的心怀不满的员工），也不会自动入侵其他基础架构中的其他系统。

有关管理员和租户的帐户与凭据管理的详细信息，请参见用户帐户管理

本章讨论了以下主题：

- 数据库安全

数据库安全

总的来说，数据库安全不在本文档讨论范围内。与云环境中的所有其他系统一样，您应采用行业最佳做法妥善保护 vCloud Director 数据库。

vCloud Director 数据库用户帐户应仅具有《vCloud Director 安装和升级指南》的相应数据库配置指南中列出的系统特权。不应为 vCloud Director 数据库用户授予该服务器上其他数据库的特权或其他系统管理特权。否则将违反数据库服务器的“最小特权原则”，授予用户不必要的权限。

建议您查看以下文档以获取数据库安全信息。

Microsoft SQL Server	《SQL Server Security Best Practices》，网址：http://download.microsoft.com/download/8/f/a/8fabacd7-803e-40fc-adf8-355e7d218f4c/sql_server_2012_security_best_practice_whitepaper_apr2012.docx。 注 vCloud Director 不支持通过 SSL 连接到 Microsoft SQL Server 数据库。
Oracle	《Oracle Database Security Guide》，网址：https://docs.oracle.com/cd/B28359_01/network.111/b28531.pdf。 注 vCloud Director 9.5 不支持 Oracle 数据库。 vCloud Director 9.1 支持 Oracle 数据库，但不支持通过 HTTPS 和 SSL 连接到 Oracle 数据库。
PostgreSQL	除了为 PostgreSQL 连接启用 SSL，我们建议您查看 IBM developerWorks 中的 PostgreSQL 服务器管理文档和 PostgreSQL 数据库总体安全性。

系统安全性

5

服务提供商和系统管理员负责每个 vCloud Director 服务器组的安全。

要保护 vCloud Director 服务器组免遭外部攻击者的攻击，您需要采取针对所有基于 Web 的服务通用的防御措施，包括使用签名证书并保护 HTTPS 端点以及将 Web 应用程序防火墙置于系统和 Internet 之间。此外，您还必须确保配置 vCloud Director 依赖的服务，包括 RabbitMQ AMQP 代理和一个可选的 Apache Cassandra 数据库，且配置方式需最大限度地降低外部参与者破坏这些系统的可能性。

本章讨论了以下主题：

网络安全要求

vCloud Director 的安全操作需要拥有一个安全的网络环境。在开始安装 vCloud Director 之前，必须先配置和测试此网络环境。

将所有 vCloud Director 服务器连接到受保护和监控的网络。vCloud Director 网络连接还具有以下几个要求：

- 请勿将 vCloud Director 直接连接到公共 Internet。始终使用防火墙保护 vCloud Director 网络连接。对于入站连接，仅必须打开端口 443 (HTTPS)。如果需要，也可以为入站连接打开端口 22 (SSH) 和 80 (HTTP)。此外，`cell-management-tool` 需要访问单元的 loopback 地址。防火墙必须拒绝来自公共网络的所有其他入站流量，包括发送到 JMX 的请求（端口 8999）。

表 5-1. 必须支持来自 vCloud Director 主机的入站软件包的端口

端口	协议	注释
111	TCP 和 UDP	由传输服务使用的 NFS portmapper
920	TCP 和 UDP	由传输服务使用的 NFS rpc.statd
61611	TCP	AMQP
61616	TCP	AMQP

- 不要将用于出站连接的端口连接到公共网络。

表 5-2. 必须支持来自 vCloud Director 主机的出站软件包的端口

端口	协议	注释
25	TCP 和 UDP	SMTP
53	TCP 和 UDP	DNS
111	TCP 和 UDP	由传输服务使用的 NFS portmapper
123	TCP 和 UDP	NTP
389	TCP 和 UDP	LDAP
443	TCP	使用标准端口的 vCenter、NSX Manager 和 ESXi 连接。如果您为这些服务选择了其他端口，请禁用端口 443 的连接并为所选端口启用这些服务。
514	UDP	可选。启用 syslog。
902	TCP	vCenter 和 ESXi 连接。
903	TCP	vCenter 和 ESXi 连接。
920	TCP 和 UDP	由传输服务使用的 NFS rpc.statd。
1433	TCP	默认的 Microsoft SQL Server 数据库端口。
5672	TCP 和 UDP	可选。任务延期的 AMQP 消息。
61611	TCP	AMQP
61616	TCP	AMQP

- 通过专用网络路由 vCloud Director 服务器与以下服务器之间的流量。
  - vCloud Director 数据库服务器
  - RabbitMQ
  - Cassandra
- 如果可能，通过专用网络路由 vCloud Director 服务器、vSphere 和 NSX 之间的流量。
- 支持提供商网络的虚拟交换机和分布式虚拟交换机必须相互隔离。它们不能共享相同的第 2 层物理网络分段。
- 使用 NFSv4 传输服务存储。最常见的 NFS 版本 NFSv3 不提供传输加密，对于某些配置，这可能会导致正在传输的数据被嗅探或篡改。SANS 白皮书受信任与不受信任环境中的 NFS 安全中介绍了 NFSv3 中固有的威胁。有关配置和保护 vCloud Director 传输服务的其他信息可从 VMware 知识库文章 2086127 获取。

证书

vCloud Director 使用 HTTPS（TLS 或 SSL）保护流向所有外部端点的网络流量。许多内部端点也支持 HTTPS，包括 AMQP 和 LDAP。特别重要的一点是，务必为外部端点提供公认证书颁发机构 (CA) 签名的证书。内部端点不太容易受到攻击，在大多数情况下，使用企业证书甚至是自签名证书足以提供充分的保护。

所有证书应具有与安装所在服务器的完全限定域名 (FQDN) 匹配的公用名称 (CN) 字段。这通常意味着服务器已注册到 DNS，因此具有充分定义的唯一 FQDN，同时也意味着您通过 FQDN（而不是 IP 地址）与之连接。如果一定要使用 IP 地址连接，那么证书应包括与主机的 IP 地址匹配的 `subjectAltName` 字段。

其他信息请参见 (RFC 6125) 和 (RFC 5280)。您还应咨询您的 CA。

公用端点证书

对于向企业网络或 Internet 等其他公共网络公开的端点，应使用由公认的根 CA 签名的证书进行保护。这些端点包括：

- 单元 HTTPS 地址和控制台代理地址。您必须配置这两个地址，并在安装过程中提供相应的证书和密钥库详细信息。
- SSL 终止负载平衡器。请参见负载平衡器和 SSL 终止。

一般情况下，无需导入已签名的证书，因为任何 SSL 客户端都可以验证信任链，一直验证到 root。您的本地安全团队创建的级别较低的证书（企业 CA 或自签名）不能以这种方式检查，安全团队会告知您这些证书的导入位置。

专用（内部）端点证书

专用网络上的端点可以使用企业 CA 签名的证书，必要时甚至可以使用自签名证书，这些端点无法从公共网络访问且通常是针对数据库和 AMQP 等 vCloud Director 组件专门创建的。这些端点包括：

- 指向 vSphere 和 NSX 的内部连接。

- 连接 vCloud Director 和 RabbitMQ 的 AMQP 端点。
- PostgreSQL 数据库连接（可选）。

拥有签名证书可以降低恶意应用程序伪装成合法 vCloud Director 组件访问专用网络的风险。

支持的协议和密码套件

vCloud Director 支持若干 HTTPS 协议，包括 TLS 和 SSL。默认情况下不支持 TLS v1.0，因为它存在已知漏洞。安装完成后，您可以使用单元管理工具配置系统支持用于 HTTPS 连接的协议集和密码套件。有关详细信息，请参见《vCloud Director 发行说明》。

配置 vSphere 证书

在 vSphere 6.0 及更高版本中，VMware Certificate Authority (VMCA) 默认使用由 VMCA 签名的证书置备每个 ESXi 主机和每个 vCenter Server 服务。您可以将现有证书替换为新的 VMCA 签名证书，将 VMCA 设为辅助 CA，或将所有证书替换为自定义证书。有关创建和替换 vCenter 和 ESXi 所用证书的详细信息，请参见《vSphere 安全性》指南中的 vSphere 安全性证书。

配置 vCloud Director 以检查 vCenter 证书

要配置 vCloud Director 以检查 vCenter 证书，请使用 JCEKS 格式创建一个 Java 密钥库，其中包含用于对 vCenter 证书进行签名的受信任证书。（用于各个 vCenter 服务器的证书不在此存储区中，仅存储用于对它们进行签名的 CA 证书。）

类似以下内容的命令将 PEM 编码证书从 `/tmp/cacert.pem` 导入到名为 `myca.ks` 的密钥库：

```
$ keytool –import –alias default –keystore myca.ks –file /tmp/cacert.pem –storepass password –
storetype JCEKS
```

类似以下内容的命令将另一个证书（本例中为 `/tmp/cacert2.pem`）添加到同一个密钥库：

```
$ keytool –importcert–keystore myca.ks –storepass password –file /tmp/cacert2.pem –storetype JCEKS
```

创建密钥库后，以系统管理员身份登录到 vCloud Director。在**管理**选项卡的**系统设置**部分，单击**常规**，然后导航到页面底部。

选择**验证 vCenter 和 vSphere SSO** 证书和**验证 NSX Manager 证书**。单击**浏览**按钮以搜索 Java 密钥库，然后单击**打开**。输入密钥库密码，然后单击**应用**。

操作完成后，您的受信任证书和其他信息将上载到 vCloud Director 数据库。因此，您只需针对所有单元执行一次此操作。

启用此选项后，所有 vCenter 和 NSX Manager 证书将处于选中状态，因此每个 vCenter 和 NSX Manager 都必须具有正确的证书链以及与其 FQDN 相匹配的证书。否则，指向 vCenter 和 NSX 的连接将失败。

重要事项 如果将 vCloud Director 和 vCenter 添加到 NSX Manager 后更改了证书，则必须强制重新连接到服务器。

更新 vCloud Director 单元的证书和密钥

每个 vCloud Director 服务器均需在 Java 密钥存储文件中提供两个 SSL 证书，一个用于 HTTP 服务，一个用于控制台代理服务。安装 vCloud Director 时，必须提供这些密钥库的路径名。签名证书将提供最高级别的信任。

单元管理工具的 `certificates` 命令会自动将现有证书替换为新证书。使用 `certificates` 命令将自签名证书替换为签名证书，或将过期证书替换为新证书。要创建包含签名证书的 JCEKS 密钥库，请参见《vCloud Director 安装和升级指南》中的创建和导入签名 SSL 证书。

要替换一个或两个端点的 SSL 证书，请使用以下形式的命令：

```
cell-management-tool certificates options
```

有关详细信息，请参见《vCloud Director 管理员指南》中的替换 HTTP 和控制台代理端点的证书。

防火墙

vCloud Director 单元必须可供租户和系统管理员访问，他们通常从服务提供商网络外围的外部与其连接。确保 vCloud Director 服务可供外部访问的建议方法是在 Internet（或其他企业网络）与每个 vCloud Director 公用端点之间放置 Web 应用程序防火墙。

网络防火墙会对物理和/或虚拟网络进行分段，以便只有特定端口上一组明确定义的有限流量可在它们之间通过。总的来说，本文不会定义防火墙部署的基本原理，也不详细介绍防火墙的设置。这些主题不在本指南讨论范围内。本指南只介绍相对于 vCloud Director 部署的不同组件放置网络防火墙的建议位置。

注 通过网络或每租户 VPN 中的 IP 地址限制可以进一步限制管理连接。该级别的保护可能适用于某些部署，但不在本文档讨论范围内。

因为 vCloud Director 单元在 DMZ 中，因此它们对所需服务的访问也应由网络防火墙传递。具体来说，建议仅限从防火墙公共端无法访问的内部网络访问 vCloud Director 数据库、vCenter Server、ESXi 主机、AMQP 和任何备份或类似服务。有关该防火墙中必须打开的端口的列表，请参见网络安全要求。

阻止恶意流量

建议采用的防火墙规则有多个，它们都可以帮助系统防御网络威胁：

- 丢弃来自不可路由地址（IP 欺骗）的数据包
- 丢弃格式不正确的 TCP 数据包
- 限制请求速率，尤其是 SYN 请求，防止出现 SYN 洪水攻击（拒绝服务攻击）
- 考虑拒绝非来自入站请求的防火墙出站流量

Web 应用程序防火墙一般应用这些规则和其他规则，您选择部署的网络防火墙可能会默认应用这些规则和其他规则。有关具体配置说明和默认功能，请参见所选防火墙的文档。

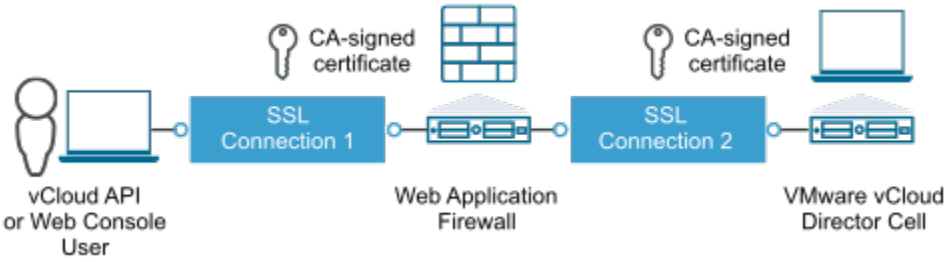
负载平衡器和 SSL 终止

您应使用 Web 应用程序防火墙 (WAF) 保护 vCloud Director 公用端点。与负载平衡器结合使用时，配置 WAF 以允许检查恶意流量和通过在 WAF 上终止 HTTPS 连接来阻止恶意流量，从而允许 WAF 使用自己的证书完成握手并将带有 `X-Forwarded-For` 标头的可接受请求转发给单元。

必须向 HTTPS 端点发送 vCloud Director 的客户端请求。（HTTP 到单元的连接受支持，但并不安全）即使远程客户端与 WAF 之间的通信使用 HTTPS 进行保护，也要求通过 HTTPS 完成 WAF 与单元的通信。

下图十分简单，省去了负载平衡器，展示了使用 TLS 或 SSL 终止时存在的两个 TLS 或 SSL 连接，一个在计算机与 WAF 之间，另一个在防火墙与 vCloud Director 单元之间。

图 5-1. WAF 的 TLS/SSL 配置



TLS/SSL 终止和证书

配置 TLS 或 SSL 终止时，重要的一点是，不仅要在 WAF 上安装 CA 签名的证书，以便 vCloud API 和 Web 控制台等客户端应用程序可以识别服务器的身份，还要在单元上使用 CA 签名的证书，即使这些单元仅为 WAF 可见。即使 WAF 接受自签名证书，也仅在部署时手动接受每个证书的情况下适用；不过，这限制了 vCloud Director 服务器组的灵活性，因为必须手动配置每个单元（续订证书时必须重新配置）。

最后，如果负载平衡器独立于 WAF，它也应使用 CA 签名的证书。有关添加负载平衡器端点证书链路径的过程，请参见《vCloud Director 管理员指南》中的自定义公用端点。

X-Forwarded-For 标头

`X-Forwarded-For` 是广泛使用的标头，受多个代理和防火墙的支持。如有可能，建议在防火墙上启用此标头生成。

当防火墙在单元前面时，单元可以查询客户端的 IP 地址进行记录，但它通常会获取防火墙的地址。但是，如果单元接收到的请求中存在 `X-Forwarded-For` 标头，则会在日志中将该地址记录为客户端地址，并将防火墙地址记录为单独的 `proxyAddress` 字段。

保护 AMQP (RabbitMQ)

高级消息队列协议 (Advanced Message Queuing Protocol, AMQP) 是消息队列的开放式标准，支持企业系统进行灵活的消息传输。vCloud Director 使用 RabbitMQ AMQP 代理提供可供扩展服务、对象扩展和阻塞任务通知使用的消息总线。

发布到 RabbitMQ 的消息包含敏感信息。公开 vCloud Director 单元之间的 AMQP 流量对系统及其租户而言是一种安全威胁。AMQP 端点应配置为使用 SSL。应在系统防火墙上阻止 AMQP 端口。必须允许使用 AMQP 消息的第三方客户端在 DMZ 中运行。使用 vCloud Director 消息的任何代码均应接受服务提供商安全团队的审核。

有关 RabbitMQ 及其如何用于 vCloud Director 的详细信息，请参见 VCAT-SP 博客内容，网址为：https://blogs.vmware.com/vcat/2015/08/vcloud-director-for-service-providers-vcd-sp-and-rabbitmq-security.html

使用 SSL 保护 AMQP 服务

若要对 vCloud Director AMQP 服务使用 SSL，请在 vCloud Director Web 控制台的**扩展性**页面的 **AMQP 代理设置**部分选择**使用 SSL**，并提供以下任一内容：

- SSL 证书路径名
- JCEKS 信任存储路径名、用户名和密码

有关完整的过程，请参见《vCloud Director 管理员指南》中的配置 AMQP 代理。

重要事项 虽然**接受所有证书**选项可用，但是我们不建议在存在安全问题时选择该选项。在不进行检查的情况下接受所有证书，容易受到中间人攻击。

在系统防火墙上阻止 AMQP 端口

管理网络上必须有多个 AMQP 端口可供访问，如网络安全要求中所述。但是，不应通过公共或企业网络访问任何 AMQP 端点。

保护 Cassandra（虚拟机衡量指标数据库）

Cassandra 是开源数据库，您可以使用该数据库为可扩展的高性能解决方案提供备用存储，以便收集虚拟机衡量指标等时间序列数据。发送到并存储在 Cassandra 群集中的数据可能是敏感数据，应受到保护。

除了放置在专用管理网络上，还应使用 SSL 保护 Cassandra 基础架构。

启用 Cassandra 客户端到节点加密

有关安装 SSL 证书以及启用加密的信息，请参见 Cassandra 客户端到节点加密页面。

我们建议使用由公认 CA 签名的证书。执行此操作时，不需要在 vCloud Director 中执行其他任何配置。如果您使用的自签名证书，则必须将其手动导入到 vCloud Director。使用单元管理工具的 `import-trusted-certificates` 命令，如《vCloud Director 管理员指南》中的从外部服务导入 SSL 证书所示

安全访问 JMX

如《vCloud Director 管理员指南》中所述，每个 vCloud Director 单元均通过 JMX 公开了大量 MBean，允许对服务器进行运维管理并支持访问内部统计信息。由于此接口可以公开关于正在运行的系统的敏感信息并影响其运维，因此必须严格控制对 JMX 的访问。

JMX 身份验证

只允许 vCloud Director 系统管理员访问 JMX 接口，他们必须使用访问 vCloud Director 的相同凭据向 JMX 进行身份验证。此功能不可配置。

限制与 JMX 的连接

由于 JMX 是仅供系统管理员访问的管理接口，因此没有理由在 vCloud Director 的管理网络之外公开。如果系统分配了专门用于管理的第三个 IP 地址，请将 JMX 直接绑定到此 IP 地址。默认情况下，vCloud Director JMX 连接器绑定到在系统配置期间指定的主 IP 地址。通过在 `/opt/vmware/vcloud-service-director/etc/global.properties` 中插入以下属性可以替代此默认值：

```
vcloud.cell.ip.management=IP or hostname for the management network to which the JMX connector should bind
```

最安全的配置是将 JMX 连接器绑定到本地主机地址：

```
vcloud.cell.ip.management=127.0.0.1
```

无论采用哪种路由和防火墙设备，分配给此管理网络的 IP 地址和 JMX 端口（默认为 8999）都不应允许遍历 Internet 或组织用户的网络边界。

在 `global.properties` 中使用此设置时，只能从本地 vCloud Director 系统访问 JMX。无论网络的路由配置如何，与 JMX 端口的任何外部连接都不会成功。

保护 JMX 通信

如果 JMX 仅公开给 localhost 地址 (`127.0.0.1`)，您可以将 SSH 用作隧道机制进行任意 JMX 访问以保护 JMX 通信。

如果您的管理要求不允许使用此配置且 JMX 必须在 vCloud Director 单元之外公开，则应使用 HTTPS 保护 JMX，您可以通过设置以下环境变量进行配置：

```
# export VCLOUD_JAVA_OPTS="-Dcom.sun.management.jmxremote.ssl=true \
-Djavax.net.keyStore=pathTokeystore \
-Djavax.net.sll.keyStorePassword=password \
-Djavax.net.ssl.keyStoreType=storeType"
```

然后，必须重新启动 vCloud Director。

JMX 客户端现在必须使用 HTTPS 连接，但它们必须有权访问 CA 证书。例如，对于 `jconsole`，应将 CA 证书导入到将运行 `jconsole` 的计算机上的密钥库中。然后，使用以下命令行参数启动 `jconsole`：

```
# jconsole -J-Djavax.net.ssl.trustStoreType=store type \
-J-Djavax.net.ssl.trustStore=pathTokeystore \
-J-Djavax.net.ssl.trustStorePassword=password
```

自签名证书（不建议用于生产部署）将导致此过程难以管理，因为您需要每个自签名证书位于运行 JMX 客户端的计算机上的密钥库中。CA 签名证书在此情况下更易于支持，因为 JMX 客户端计算机仅需要 CA 证书。

管理网络配置

vCloud Director 管理网络是专用网络，为云基础架构提供服务，并为用于在 vCloud Director 上执行管理功能的客户端系统提供访问权限。

连接到管理网络的系统包括 vCloud Director 数据库服务器、用于传输存储的 NFS 服务器、vCenter 服务器、用于对提供商管理员进行身份验证的可选 LDAPv3 目录、提供商保存用于对组织用户进行身份验证的任何 LDAPv3 目录以及 NSX Manager。此网络上的 vCenter 服务器还需要访问自己的 Active Directory 服务器。

虚拟基础架构管理网络配置要求

隔离管理网络与虚拟机数据网络非常重要，对于提供商和租户来自不同组织的云环境则更为重要。因为您不希望打开提供商的管理网络，以防从组织的 vApp 对其进行攻击。同样，管理网络必须与提供组织管理员访问权限的 DMZ 隔离开。即使它们可以使用提供商系统管理员的身份访问相同的接口，DMZ 概念对于隔离专用网络与公共网络以及提供深度防御也非常重要。

从物理连接角度而言，虚拟机数据网络必须与管理网络隔离。这是防止管理网络遭受恶意虚拟机的唯一方法。同样，vCloud Director 单元以物理方式存在于 DMZ 中。在物理部署图中，管理容器中连接到云容器的服务器通过单独的物理网络实现这一点，特定的防火墙规则将允许此流量通过。

从网络架构角度来看，需要使用内部防火墙将 vCenter 和 vCloud Director 连接传递到 vSphere（和其他网络）。这不是单个主机上不同虚拟机能否同时连接到 DMZ 和专用网络的问题，而是该管理容器（云单元）中存在连接到这两个网络的虚拟机。虽然 vCloud Director 软件的设计和实施符合以下 VMware 产品安全策略并考虑到了安全要求，但它并不是防火墙，因此不应用于在 DMZ 和专用管理网络之间传递流量。这是防火墙的角色。

其他相关网络

如物理和逻辑部署图所示，存储网络也是物理隔离的。这遵循 vSphere 最佳做法，可以保护租户和提供商存储免于恶意虚拟机的危害。该做法同样适用于备份网络。从技术角度来看，备份网络是管理网络的一个分支。它的特定要求和配置取决于使用的备份软件和配置。

vMotion 并非始终放置与管理网络隔离的网络上；但在云中，从职责分离的角度来看，应始终将 vMotion 放置在与管理网络隔离的网络上。vMotion 通常在清除时进行，如果将其放置在管理网络上，提供商管理员或其他有权访问该网络的用户将可以“嗅探”vMotion 流量，而这一行为侵犯了组织隐私。因此，您应为云工作负载的 vMotion 创建单独的物理网络。

审核和日志记录

记录和监控用户活动是确保整个系统安全的重要部分。大多数组织都实施了相应的规则，用于管理谁可以访问和更改软件及相关的硬件资源。通过保留重大活动的审核日志，组织可以验证规则合规性，发现任何违规行为，并启动修复活动。一些业务需要遵守外部法律法规中有关持续监控和验证访问及授权规则的规定。

审核日志还有助于检测非法访问系统、探查系统信息或中断系统操作的尝试，而不论这些尝试是否成功。了解有人尝试攻击以及攻击尝试的详细信息，有利于减轻危害并预防未来攻击。

无论是否有要求，定期检查日志并查看是否存在可疑、异常或未经授权的活动都是一种良好的安全做法。例行日志分析也有利于确定系统配置错误和故障，并有助于确保遵守 SLA。

vCloud Director 包括两种类型的日志：

诊断日志	在每个单元的日志目录中维护的诊断日志。诊断日志对于解决问题非常有用，但它不会保留为重大系统交互的审核记录。每个 vCloud Director 单元都会创建若干诊断日志文件，如《vCloud Director 管理员指南》的查看 vCloud Director 日志中所述。
审核日志	审核日志记录登录和注销等重大操作。系统审核日志保存在 vCloud Director 数据库中，可通过 Web UI 进行监控。每个组织管理员和系统管理员都可以查看各自控制范围内的日志。

我们建议使用 `syslog` 实用程序来保留这些日志和其他 vCloud Director 日志。此外，您应考虑使用 vRealize Log Insight，该应用程序支持远程收集其他不基于 `log4j` 的日志，如请求日志。

将 Syslog 与 vCloud Director 配合使用

可以在安装期间设置 `syslog` 服务器，请参见《vCloud Director 安装和升级指南》，了解详细信息。建议将日志导出到 `syslog` 服务器，原因如下：

- 数据库日志只能保留 90 天，但通过 `syslog` 传输的日志可以根据需要保留任意时间。
- 可以在一个中央位置同时查看所有单元的审核日志。
- 可以防止本地系统因故障、磁盘空间不足、遭到入侵等原因丢失审核日志。
- 支持在遇到上述问题时执行取证操作。
- 许多日志管理与安全信息和事件管理 (SIEM) 系统都使用此方法与 vCloud Director 集成。这样可以：
  - 将 vCloud Director、vSphere、NSX 甚至堆栈的物理硬件层上的事件和活动关联起来。
  - 横跨物理、虚拟和云基础架构，将云安全操作与云提供商或企业的其余安全操作集成起来。
- 将日志记录到远程系统，而不是部署单元的系统，可防止日志遭到篡改。单元受到破坏并不一定就能够访问或更改审核日志信息。

如果初始安装时没有为日志记录设置 `syslog` 目标，稍后可以进行此配置，方法是转到每个单元，编辑 `$VCLOUD_HOME/etc/global.properties` 文件，然后重新启动单元。

有关从 vCloud Director 主机到 `syslog` 服务器必须保持打开状态的端口的列表，请参见网络安全要求。`syslog` 服务器配置详细信息特定于系统，这不属于本文档的讨论范围。建议为 `syslog` 服务器配置冗余，确保重要事件始终可以记录到日志中。

上述讨论仅涉及将审核日志发送到 `syslog` 服务器。安全运维和 IT 运维组织也可以受益于上述集中聚合和管理的诊断日志。收集这些日志的方法有很多，包括调度作业以定期将日志复制到中央位置，在 `log4j.properties` 文件 (`$VCLOUD_HOME/etc/log4j.properties`) 中额外设置一个日志记录器并将其指向中央 syslog 服务器，或者使用 vRealize Log Insight 等日志收集实用程序来监控日志文件并将日志文件复制到中央位置。这些选项的配置取决于您希望在环境中使用的系统，但这不属于本文档的讨论范围。

重要事项 我们建议使用启用了 TLS 的 `syslog` 基础架构。默认 (UDP) `syslog` 协议不提供传输过程加密功能或传输控制/确认功能。如果不加密，日志数据容易被嗅探到（日志中的信息可能会被用于发动进一步攻击）；如果没有传输控制，攻击者将能够篡改日志记录数据。有关详细信息，请参见 RFC 5426 的第 4 部分。

诊断日志记录和日志滚动

Jetty 请求日志文件 (`$VCLOUD_HOME/logs/`*`yyyy_mm_dd`*`.request.log`) 由 Jetty (HTTP) 服务器以编程方式控制，但未设置大小上限。因此日志文件存在无限制增长的风险。Jetty 每处理一个 HTTP 请求时，都会将一个日志条目添加到当前文件。鉴于这一点，我们建议使用 `logrotate` 或类似方法来控制日志大小和保留的旧日志文件数量。

其他诊断日志文件的上限为 400 MB。确保有足够的可用磁盘空间来容纳这些文件，同时提供足够空间供 Jetty 请求日志使用。如上所述，使用集中化日志记录可确保日志文件达到 400 MB 上限并导致文件轮换和删除时，您也不会丢失重要的诊断信息。

NTP 和日志

《vCloud Director 安装和升级指南》将 NTP 标识为所有 vCloud Director 单元的要求。使用 NTP 有一个附带好处，即所有单元的日志消息具有同步时间戳。当然，日志管理工具和 SIEM 系统会使用自己的时间戳协调来自多个来源的日志，但这些时间戳只表示系统接收日志的时间，并非最初记录事件的时间。

其他日志

vCloud Director 连接并使用的其他系统将创建应整合到审核流程的审核日志。其中包括来自 NSX Manager、vCloud Director 数据库、vCenter Server 和 vSphere 主机的日志。每个系统的日志文件及其用途的详细信息不在本文档讨论范围内，请在这些产品的相关文档中查找相应信息。

租户安全

6

服务提供商、系统管理员和组织管理员负责每个 vCloud Director 租户组织的安全。

要保护 vCloud Director 租户组织免遭外部攻击，在很大程度上需要提供良好的系统级安全性，以便外部攻击者无法访问租户资源。服务提供商还需要注意可能会出现一个租户攻击（或只是干扰）另一个租户的情况。可能的租户间攻击途径包括侦听计算、存储和网络资源的系统级详细信息。无论蓄意与否，在租户（可能会相互怀疑）之间共享系统资源且一个租户设法充分占用这些资源以拒绝其他租户获得预期的服务级别时，就会出现干扰。这种情况通常称为“嘈杂邻居”问题。

如第 3 章 vCloud Director 架构和安全功能 中所述，vCloud Director 旨在使大量租户可以透明地共享系统资源。一般情况下，服务提供商可随意部署系统资源，但是部署时应尽可能地提高系统效率同时最大限度地减少停机时间。只要在租户组织之间共享资源，服务提供商就应考虑此类共享可能会对各种租户操作造成的影响，还应考虑是否可能会引起租户间攻击。

本章讨论了以下主题：

- 租户组织的网络安全
- 资源分配和隔离
- 用户帐户管理

租户组织的网络安全

尽管 vCloud Director 组织的网络安全由其自行负责，但服务提供商应使用防火墙保护外部网络。

在 vCloud Director 系统中，VXLAN 和 VLAN 网络会强制隔离数据包流量，等同于使用独立物理网络实现的效果。它们还提供了一系列路由和防火墙选项，使组织能够精细控制外部系统工作负载以及组织内工作负载的访问。vCloud Director 文档详细介绍了这些功能，网址：http://docs.vmware.com。大多数情况下，为系统本身设计了有效保护机制（包括 Web 应用程序防火墙、SSL 终止负载平衡器和正确签名的数字证书）的服务提供商不需要主动建立或维护组织 VDC 网络的安全性。

租户工作负载的外部访问

配置从 Internet 或企业网络访问组织工作负载 (vApp) 时，服务提供商应牢记 vCloud Director 部署和使用的 vSphere 基础架构的防火墙要求。最可能的情况是，某些 vApp 将需要访问 Internet 或需要被远程访问，无论是通过 RDP、SSH 等（针对管理），还是通过 HTTP 或其他协议（针对这些服务的最终用户）。因此，建议使用两个不同的虚拟机数据网络（如资源分配和隔离中的架构图所示）实现不同的用途，这两个网络都需要网络防火墙保护。

需要从云外部进行访问（例如从 Internet）的虚拟机将通过针对所公开服务配置的端口转发连接到公共网络或专用的 NAT 路由网络。这些组织 VDC 网络所连接的外部网络要求保护防火墙允许商定的流量进入此 DMZ 网络。也就是说，服务提供商应确保并非每个端口和协议都能发起与外部 DMZ 网络的连接。同时，必须确保组织的 vApp 能够向所需的服务提供足够的流量。这通常包括端口 80/TCP 和 443/TCP，但也可能包括其他端口和协议。服务提供商必须确定如何最佳实现此平衡，同时应了解从安全角度而言，应阻止不必要的端口和协议。

一般情况下，建议将需要访问 Internet 和从 Internet 访问的 vApp 连接到配置为仅允许所需类型的入站和出站连接的路由组织 VDC 网络。组织将能够控制 NSX 防火墙和端口转发规则。使用此类配置时，仍然需要使用网络防火墙来隔离这些组织 VDC 网络使用的外部网络；这是因为公共组织 VDC 网络没有任何 vCloud Director 防火墙保护。创建 DMZ 需要单独的防火墙（但是，通过单独的 NSX Edge 实例即可执行此功能）。

同样，将对允许虚拟机访问 Internet 的虚拟机数据网络使用一个专用的 NAT 路由组织 VDC 网络。如上所述，NSX Edge 可为此内部虚拟机数据网络提供 NAT 和防火墙功能。再次强调，此路由网络的外部网络部分应位于 DMZ 中，以便单独的网络防火墙将 DMZ 与 Internet 连接隔离开。

资源分配和隔离

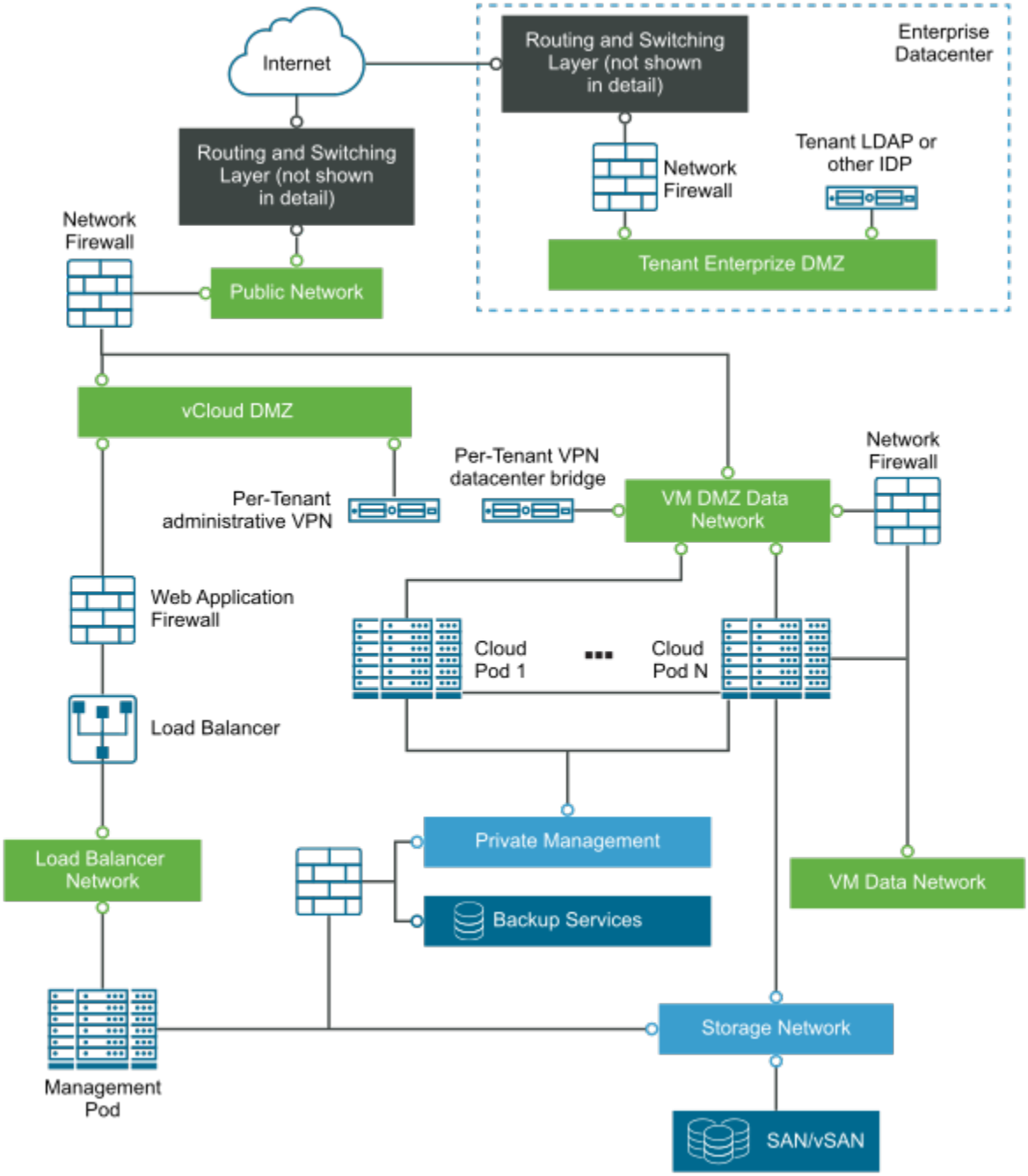
vCloud Director 的标准服务提供商部署假设在多个租户组织间共享 vSphere 资源。这为组织提供了最大的灵活性，使得提供商可以最大限度地利用已置备的计算、网络和存储资源。逻辑和物理部署图示例如下。

本小节的其他内容将简略介绍组件，后面各个小节将介绍有关资源池、数据存储、网络和其他组件配置的具体建议。

共享资源部署

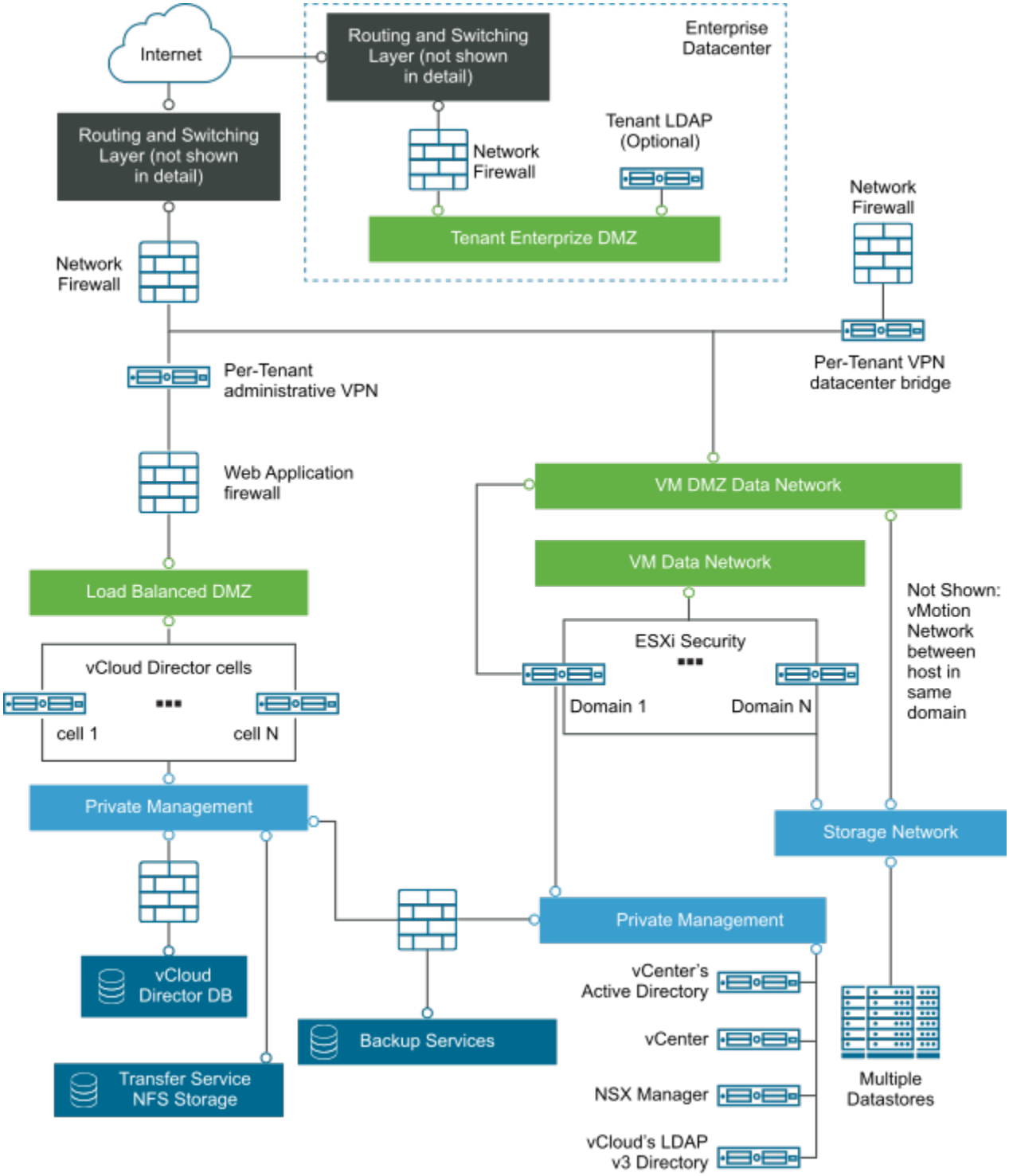
图 6-1. 物理部署图 和图 6-2. 逻辑部署图 是同一个 vCloud Director 安装的两个视图。在这些图中，我们使用术语“容器”来表示专门用于系统管理（“管理容器”）或租户工作负载（“云容器”）的一组资源（物理或虚拟机）。

图 6-1. 物理部署图



在图 6-2. 逻辑部署图 中，左侧显示负载平衡 DMZ 中的 vCloud Director 单元。DMZ 还包含 WAF 和每租户管理 VPN（可选）。服务提供商可为每个组织配置此 VPN，以便更严格地限制哪些用户和 IP 地址可以访问通过 WAF 公开的服务。此外，租户可以配置 VPN，以便将其内部部署工作负载和数据连接到云中的虚拟机。此类 VPN 的配置不在本文档讨论范围内。

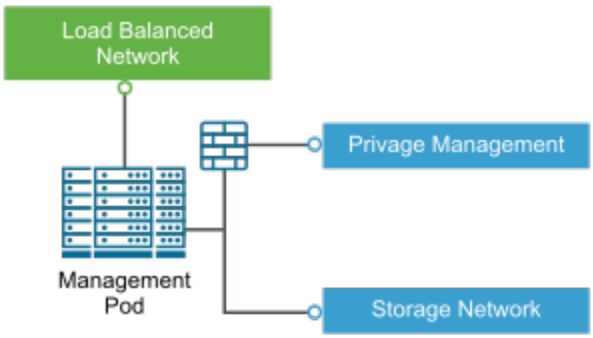
图 6-2. 逻辑部署图



单元的后面是 vCloud Director 所需的专用管理元素，包括 vCenter、NSX、vCloud Director 数据库等。图中的防火墙会严格控制它们的连接，因为不应从 DMZ 上的其他计算机或直接从 Internet 访问这些服务。

图 图 6-3. 管理容器网络 仅重点展示管理容器。图中显示，即使不需要三个，至少也需要两个单独的物理网络与管理容器连接。这包括负载平衡 DMZ 网络、专用管理网络和可选的专用存储网络，以及特定于提供商的配置。

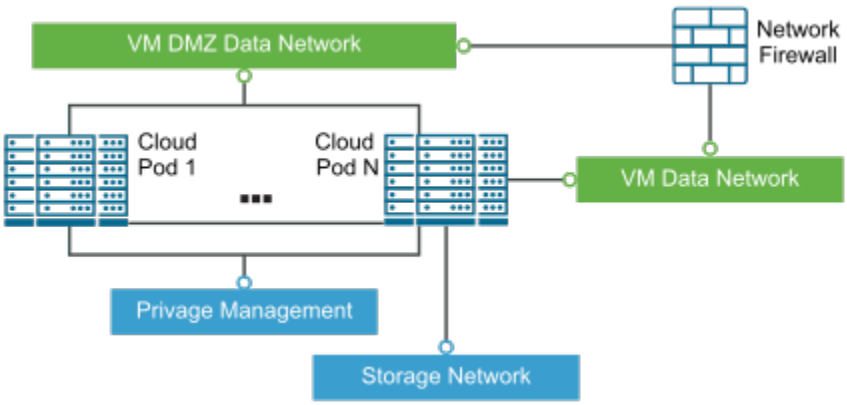
图 6-3. 管理容器网络



对于分组到不同安全域的 vSphere 主机，每个主机都有一个作为虚拟机 DMZ 数据网络公开且用作公共组织 VDC 网络的外部网络和一个用作专用组织 VDC 网络且可以路由到外部网络的虚拟机数据网络。

图 图 6-4. 云容器网络 重点展示云容器。图中显示了四个物理网络；但是，存储网络特定于所选的特定硬件和存储技术。如果资源池未跨群集，您可能无需提供物理虚拟机数据网络。否则（如果资源池跨群集），本文档建议将单独的物理网络用于 vMotion 流量。

图 6-4. 云容器网络



它还假定典型的数据中心安全技术（如 IDS/IPS、SIEM、配置管理、修补程序管理、漏洞管理、防病毒和 GRC 管理系统）将应用于 vCloud Director 及其关联系统、vSphere 及其关联系统，以及支持它们的网络和存储基础架构。这些系统的详细信息不在本文档讨论范围内。

资源共享和隔离建议

正常情况下，服务提供商可以在多个租户组织之间共享计算、存储和网络资源。系统在管理程序和 vCloud Director 软件堆栈中强制通过抽象、安全的工程做法执行隔离。

租户组织共享通过单个提供者 VDC 提供的底层资源池、数据存储和外部网络，而不会影响（或甚至不会感知）不属于自己的资源。正确管理 vApp 存储和运行时租约、vApp 配额、资源密集型操作的限制以及组织 VDC 分配模型可确保租户无法无意或有意地拒绝为其他租户提供服务。例如，非常保守的配置将在预留池分配模型下设置所有组织 VDC，且永远不会过度分配资源。本文档未涵盖全部情况；但是，以下各小节提到了几点。

安全域和提供者 VDC

尽管在软件中适当隔离且具有适当的组织配置，有时候租户组织也可能不希望在特定计算、网络或存储资源上运行或存储不同的工作负载。这不会将整个系统提升到“高安全性环境”（对此方面的讨论不属于本文档范围内），但确实需要将云分为多个安全域。需要此类处理的工作负载的特定示例包括：

- 受隐私法约束的数据，隐私法要求在规定的地理位置内存储并处理数据。
- 国家/地区或组织拥有的数据和资源，尽管这些国家/地区或组织信任云隔离，但出于谨慎考虑和加强深度防御，要求其 VDC 不能与其他特定租户（例如，竞争公司）共享资源。

在这些情形及其他情形中，应使用不同的提供者 VDC 将资源池、网络和数据存储分割到不同的安全域，以便对具有相似问题的 vApp 进行分组（或隔离）。例如，您可能明确确定某些提供者 VDC 在某些国家/地区存储和处理数据。

资源池

在单个提供者 VDC 中，您可以具有聚合底层 vSphere 基础架构提供的 CPU 和内存资源的多个资源池。从保密性和完整性角度来看，不需要在不同资源池间分配不同的组织。但从可用性角度来看，有必要这么做。此资源管理问题与组织 VDC 分配模型、预期工作负载、应用于这些组织的配额和限制以及提供者可联机增加计算资源的速度有关。本指南未定义不同资源分配模型及对每个组织使用资源池的影响，而是说明了每当允许过度分配多个组织所用池中的资源时，便会出现导致一个或多个组织的服务质量下降的风险。要避免一个组织导致的拒绝服务，必须正确监控服务级别，但安全性不要求对组织进行特定隔离来实现此目标。

限制共享资源的共享使用

在默认配置中，所有租户可以无限使用许多 vCloud Director 计算和存储资源。系统提供了多种方法，可帮助系统管理员管理和监控这些资源的使用。仔细检查以下方面非常重要，可在一定程度上限制“嘈杂邻居”影响 vCloud Director 所提供服务级别的可能性。

限制资源密集型操作	请参见《vCloud Director 管理员指南》中的配置系统限制。
实施合理配额	请参见《vCloud Director 管理员指南》中的配置组织租约、配额和限制设置和（要限制租户可以创建的 VDC 数量以及限制每个虚拟机的同时连接数）配置系统限制。
管理存储和运行时租约	租约可以在一定程度上控制租户对存储和计算资源的使用。限制 vApp 打开电源的时长或关闭电源的 vApp 可以使用存储的时长是管理共享资源的关键一步。请参见《vCloud Director 管理员指南》中的了解租约。

外部网络

服务提供商创建外部网络，并使其可供租户访问。可以安全地在多个公共网络之间共享外部网络，因为按照定义这些网络是公共网络。租户应注意，外部网络上的流量会遭到拦截，因此如果需要，应在这些网络上采取应用程序级或传输级安全性，以确保保密性和完整性。

在相同情况下（用于连接到公共网络时），专用路由网络可以共享这些外部网络。有时，组织 VDC 网络可能会使用外部网络连接两个不同的 vApp 及其网络或将 vApp 网络连接回企业数据中心。在这些情况下，不应在组织之间共享外部网络。

当然，不能期望每个组织都有一个单独的物理网络。建议使用共享物理网络连接到明确确定为 DMZ 网络的单个外部网络。因此，组织将了解它不提供保密保护。对于遍历外部网络但要求保密保护的通信（例如，vApp 到企业数据中心连接或通过公共网络的 vApp 到 vApp 网桥），可以部署 VPN。这是因为，要确保专用路由网络上的 vApp 可以访问，必须通过可在该外部网络上路由的 IP 地址利用 IP 地址转发。连接到该物理网络的任何其他 vApp 可以将数据包发送到该 vApp，即使是连接到其他外部网络的其他组织也可如此。为了防止出现这种情况，服务提供商可以使用 NSX 分布式防火墙和分布式逻辑路由强制隔离来自单个外部网络上多个租户的流量。请参见《VMware vCloud® Architecture Toolkit™ for Service Providers (VCAT-SP)》中的 NSX 分布式防火墙和逻辑路由

不同租户拥有的组织 VDC 网络可以共享同一外部网络（作为 Edge 网关的上行链路），只要不允许通过 NAT 和 IP 伪装访问内部即可。

重要事项 vCloud Director 高级网络连接允许租户和服务提供商采用动态路由协议，例如 OSPF。在不进行身份验证的情况下使用 OSPF 自动发现机制，可能会在属于不同租户的 Edge 网关之间建立对等关系，并启动交换路由。为了防止出现这种情况，请不要在公共共享接口上启用 OSPF，除非同时启用了 OSPF 身份验证以防止与未经身份验证的 Edge 网关建立对等关系。

网络池

多个租户可以使用一个网络池，只要池中的所有网络都适当隔离即可。VXLAN 支持的网络池（默认设置）依赖于配置为允许在一个 VXLAN 内建立连接以及在不同 VXLAN 之间隔离的物理和虚拟交换机。端口组支持的网络池必须配置相互隔离的端口组。这些端口组可以通过 VXLAN 进行物理隔离。

在三种类型的网络池（端口组、VLAN 和 VXLAN）中，共享 vCloud Director VXLAN 网络池最容易。VXLAN 池支持的网络比 VLAN 支持的网络池或端口组支持的网络池多很多，并且在 vSphere 内核层强制实施隔离。尽管物理交换机在不使用 VXLAN 时不会隔离流量，VXLAN 也不易受到硬件层配置错误的影响。从上文可以看到，任何网络池中的网络都不会为拦截的数据包提供保密保护（例如，物理层）。

存储配置文件

vCloud Director 存储配置文件聚合数据存储时，服务提供商能够提供按容量、性能和其他属性分层的存储功能。租户组织无法访问每个数据存储。租户可以从服务提供商提供的一组存储配置文件中进行选择。如果底层数据存储配置为只能从 vSphere 管理网络进行访问，则与计算资源一样，共享数据存储时只存在可用性风险。一个组织最终使用的存储可能比预期多，这限制了其他组织可使用的存储量。使用即付即用分配模型和“无限制存储”默认设置的组织尤为如此因此，如果您共享数据存储，则应设置存储限制，启用精简置备（如果可能）并仔细监控存储使用情况。此外，还应精心管理您的存储租约，如限制共享资源的共享使用中所述。或者，如果您不共享数据存储，则必须正确地将存储专门用于您提供给每个组织的存储配置文件，这可能会因将存储分配给不需要的组织而导致存储浪费。

vSphere 数据存储对象是存储 VMDK 的逻辑卷。虽然 vSphere 管理员可以查看从中创建这些数据存储的物理存储系统，但也需要 vCloud Director 管理员或租户不可用的权限。创建和上载 vApp 的租户用户只需在所用组织 VDC 中的一个可用存储配置文件上存储 vApp 的 VMDK。

因此，虚拟机永远无法访问其 VMDK 所用存储外部的任何存储，除非它们与这些存储系统建立了网络连接。本指南建议不建立连接；提供商可以网络服务形式为 vApp 提供外部存储访问，但必须与分配给支持云的 vSphere 主机的 LUN 隔离开。

同样，租户组织只能查看自己的组织 VDC 中可用的存储配置文件，即便如此，视图也限于 vCloud Director 抽象。他们无法浏览系统的数据存储。只能查看目录中发布的内容或其管理的 vApp 使用的内容。如果组织 VDC 存储配置文件不共享数据存储，则组织不会影响其他组织的存储（除非可能为存储 I/O 使用过多的网络带宽）。即使组织这样做，上述限制和抽象也可以确保组织之间正确隔离。vCloud Director 管理员可以在特定数据存储上启用 vSphere Storage I/O Control，以限制租户过度使用存储 I/O 带宽。请参见《vCloud Director 管理员指南》中的在提供者 VDC 中配置 Storage I/O Control 支持。

用户帐户管理

用户及其凭据的管理对于任何系统的安全性都非常重要。由于对 vCloud Director 系统的所有身份验证都通过用户名和密码执行，因此遵循最佳做法管理用户及其密码至关重要。

本主题旨在定义在 vCloud Director 中管理用户及密码的功能和限制，并提供有关在这些给定限制条件下如何安全地进行管理和使用的建议。

本地用户帐户的限制

vCloud Director 为在 vCloud Director 数据库中创建和维护的用户帐户提供了独立的身份提供程序。尽管在配置了数据库有限网络访问权限（请参见管理网络配置）的系统中不易受到攻击，但这些帐户未提供某些行业（如 PCI 数据安全标准）要求的各种密码管理功能。要阻止暴力攻击，本地帐户应遵守密码重试限制次数和帐户锁定规则的规定。

服务提供商应仔细权衡继续为系统管理员使用本地帐户的优势和风险，还应严格控制配置本地系统管理员帐户的情况下可以使用哪些源 IP 地址向组织的云 URL 进行身份验证。我们强烈建议，避免或至少限制针对系统管理员帐户使用此身份提供程序。

新安装的 vCloud Director 会创建一个本地系统管理员帐户。在默认配置中，vCloud Director 至少需要一个系统管理员帐户为本地帐户。已支持系统组织使用 vSphere SSO 服务 (SAML IDP) 或 LDAP 的服务提供商可以通过以下步骤将 vCloud Director 配置为不使用本地系统管理员帐户即可运行：

1 在 vSphere SSO 服务 (SAML IDP) 或 LDAP 中为您的系统管理员创建一个或多个帐户。

2 将这些帐户导入系统组织。

3 运行单元管理工具 `manage-config` 命令重新配置系统，以便不需要本地系统管理员帐户以及具有本地帐户的系统管理员无法向系统进行身份验证。

```
./cell-management-tool manage-config -n local.sysadmin.disabled -v true
```

请注意，这不会禁用其他组织的本地帐户。

注 在没有本地系统管理员帐户的系统中，要求您指定系统管理员凭据的单元管理工具命令必须改为使用 `-i -pid` 选项，以便在 *pid* 中提供单元的进程 ID。请参见《vCloud Director 管理员指南》中的单元管理工具参考。

4 您可以使用类似单元管理工具命令行撤消此更改，使得具有本地帐户的系统管理员能够重新访问。

```
./cell-management-tool manage-config -n local.sysadmin.disabled -v false
```

密码管理

大多数 LDAP、OAUTH 和 SAML IDP 提供各种功能或与系统集成来处理用户忘记密码的情况。这些不在本文档讨论范围内。vCloud Director 单元管理工具包括可用于恢复丢失的系统管理员密码的 `recover-password` 命令。没有任何 vCloud Director 原生功能可用于为其他本地用户处理此情况。建议按照经 IT 安全部门批准的方式安全存储所有本地帐户密码。一些组织将密码锁在保管库中。一些组织使用市售或免费的密码存储程序。本文档不会建议特定方法。

密码强度

IDP 用户的密码强度取决于该 IDP 和/或管理目录中的用户所用工具提供的控制。例如，如果将 vCloud Director 连接到 Active Directory，会在目录内强制执行与 Microsoft Active Directory 关联的典型 Active Directory 密码长度、复杂性和历史记录控制。其他 IDP 往往支持类似的功能。有关密码强度控制的具体详细信息是根据目录而定的，在此不做更详细地介绍。

vCloud Director 要求本地用户的密码长度至少为 6 个字符。此要求不可配置，无其他密码复杂性或历史记录控制要求。建议任何用户，尤其是系统管理员或组织管理员，谨慎选择密码，以抵御暴力攻击（请参见下面的帐户锁定问题）。

用户密码保护

从不在 vCloud Director 数据库中存储由 IDP 管理的用户的凭据。使用 IDP 选择的方法传输这些凭据。有关保护此信息通道的详细信息，请参见配置身份提供程序 。

将本地用户的密码存储在 vCloud Director 数据库中之前将对其进行加盐和哈希处理。无法从数据库恢复纯文本密码。将通过对提供的密码进行哈希处理并将其与数据库中的密码字段内容进行比较来对本地用户进行身份验证。

其他密码

除了本地用户的凭据之外，vCloud Director 数据库还存储已连接的 vCenter Server 和 NSX Manager 的密码。对这些密码所做的更改不会在系统中自动更新。您将需要使用 vCloud Director 配置脚本（适用于 vCloud Director 数据库密码）或 Web UI（适用于 vCenter 和 NSX）手动对其进行更改。

vCloud Director 还维护用于访问与其 TLS/SSL 证书关联的私钥的密码，以及上文提及的 vCloud Director 数据库、vCenter Server 和 NSX Manager 的密码。这些密码使用每个 vCloud Director 安装一个唯一密钥的机制进行加密并存储在 `$VCLOUD_HOME/etc/global.properties` 文件中。如安装后保护敏感文件中所述，应仔细保护包含该文件的任何备份。

基于角色的访问控制

vCloud Director 实现了基于角色的授权模型。本节讨论 vCloud Director 中的各种身份源、用户类型、身份验证控制、角色和权限。只有了解此信息才能恰当保证系统安全，为相应用户提供正确的访问权限。

vCloud Director 租户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，也可以从外部目录服务 (LDAP) 或身份提供程序 (OAUTH、SAML) 导入。导入的用户可以是一个或多个组的成员。如果用户是多个组的成员，他/她将获得分配给这些组的所有角色。创建的每个组织都有一组默认权限和一组包括这些权限的任意组合的预定义角色。系统管理员可向组织授予其他权限，组织管理员可以使用这些权限创建组织本地的自定义角色。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。

不允许任何未经身份验证的用户通过 Web 控制台、租户门户或 vCloud API 访问任何 vCloud Director 功能。每个用户都使用用户名和密码进行身份验证。可以全局配置密码重试和帐户锁定策略，也可以按组织配置。

角色是指为分配了该角色的用户提供功能的权限组。预定义的角色包括：

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

《vCloud Director 管理员指南》中还介绍了分配给每个角色的权限。本部分是为了帮助您为每个类型的用户选择适当的角色。例如，vApp 用户角色可能适合需要开启和关闭虚拟机电源的管理员，但是如果他们也需要编辑分配给虚拟机的内存量，那么 vApp 作者将是一个更合适的角色。这些角色的权限与客户组织中的权限可能并非完全吻合，因此组织管理员也可以创建自定义角色。有关可以组合起来创建有用的自定义角色的具体权限的说明不在本文的讨论范畴。

配置身份提供程序

vCloud Director 租户组织可以定义与其他应用程序或企业共享的身份提供程序。用户对身份提供程序进行身份验证，获取稍后用来登录组织的令牌。通过这一策略，企业能够使用一组凭据提供对多个不相关服务的访问权限，包括 vCloud Director，这一安排通常称为单点登录。

关于身份提供程序

vCloud Director 支持以下类型的身份提供程序：

OAuth	组织可以定义支持 OAuth 身份验证的外部身份提供程序，如 RFC 6749 (http://tools.ietf.org/html/rfc6749) 中所定义。
SAML	组织可以定义支持安全断言标记语言 (SAML) 2.0 标准的外部身份提供程序。
集成	集成身份提供程序是对本地创建或从 LDAP 导入的用户进行身份验证的 vCloud Director 服务。

OAuth

在任何 OAuth 实施中，大部分安全决策都在 OAuth 授权服务器层制定。vCloud Director 的作用是资源服务器，是令牌的使用者，仅负责验证令牌的完整性。

为了保护 vCloud Director 会话和底层敏感资产，OAuth 授权服务器必须安全设置并安装其最新的安全修补程序。

如果 OAuth 授权服务器可以设置为将用户重定向到查询参数指定的任意 URL，则必须将 OAuth 授权服务器设置为验证 URL，以防止攻击者控制重定向到第三方应用程序。必须使用合法应用程序白名单（如可用）进行验证。

LDAP

vCloud Director 集成身份提供程序支持多个常用的 LDAP 服务。

有关支持的 LDAP 服务的列表，请参见《vCloud Director 发行说明》。

vCloud Director 允许系统管理员定义可供所有租户使用的系统范围 LDAP 服务。租户用户帐户被导入到分配有 vCloud Director 角色的 vCloud Director 数据库。在 LDAP 目录中保存和管理 LDAP 用户密码，将使用 LDAP 配置屏幕中指定的设置对该目录进行身份验证。LDAP 目录中对身份验证和密码的所有控制都保留了下来，包括身份验证失败锁定、密码过期、历史记录、复杂性等等，而且这些控制都特定于所选的 LDAP 服务。如果一个组织配置为使用系统 LDAP，那么它的用户来自该组织的 vCloud Director 系统 LDAP 服务设置中专门配置的 OU。

云提供商可能允许租户组织在系统 LDAP 内使用 OU 或者托管自己的 LDAP 目录服务。在这两种情况下，必须提供目录的适当管理访问权限，以便组织管理员可以管理用户。如果缺乏这样的控制，则会为系统管理员带来额外的负担，并且使组织无法轻松恰当地控制对虚拟数据中心的访问。如果缺乏这样的管理控制，那么组织应该只使用他们自己托管和管理的专用 LDAP 目录。

必须为该软件启用从 vCloud Director 单元到系统 LDAP 服务器以及任何组织 LDAP 服务器的连接，才能正确地对用户进行身份验证。本文档建议系统 LDAP 服务器必须位于专用管理网络中，并通过防火墙与 DMZ 隔离。有些云提供商和大多数 IT 组织会运行所需的任何组织 LDAP 服务器，这些服务器也应位于专用网络，而不是 DMZ 中。使用组织 LDAP 服务器的另一个方案是将其置于云提供商环境之外进行托管和管理，并由组织进行控制。在这种情况下，必须向 vCloud Director 单元公开，而这可能要通过企业数据中心自身的 DMZ 来实现。

在所有这些情形下，都需要通过各种防火墙为单元和 LDAP 服务器之间的路径打开恰当的端口，如 LDAP over TLS/LDAP over SSL 中所述。此外，组织在托管自己的 LDAP 服务器时会带来一个问题：通过自己的 DMZ 公开该服务器。公众不需要访问这项服务，因此应当采取措施，仅限 vCloud Director 单元访问该服务。为此可采取一种简单的配置方法，将 LDAP 服务器和/或外部防火墙配置为仅允许从属于云提供商报告的 vCloud Director 单元的 IP 地址访问。此外也可以选择其他方案，包括为每个组织配置站点到站点 VPN 来将两套系统连接起来、强化 LDAP 代理或虚拟目录等，这些都不在本文档讨论范围内。

相反，云提供商应该认识到，如果组织托管的 LDAP 服务器由不法客户管理，则可能会被用来攻击其他组织。例如，有人虚构了一个组织，并请求很容易与另一个组织的名称混淆的组织名称，而且在钓鱼攻击中使用十分相似的登录 URL。提供商可以采取措施防止此类或类似攻击，包括在条件允许时，限制请求的源 IP 地址，从而避免跨组织登录尝试，以及确保分配的组织名称不会与其他组织名称过于相似。

LDAP over TLS/LDAP over SSL

强烈建议您配置 LDAPv3 目录进行用户身份验证。必须将 vCloud Director 配置为通过 SSL 连接到 LDAP 服务器，以妥善保护用于验证这些服务器的密码。有关详细信息，请参见《vCloud Director 管理员指南》中的“配置 LDAP 连接”。最安全的 LDAP 配置指定**使用 SSL**，并需要 LDAP 服务提供的 SSL 证书。

如果 LDAP 服务器的签名证书不可用，则必须将对 LDAP 服务器证书进行签名的 CA 的证书导入到系统或组织 JCE 密钥库 (JCEKS) 中。指定 JCEKS 密钥库的 LDAP 配置也很安全，但如果信任的 CA 证书过多（或者特定的服务器证书很多），可能会导致配置错误。此外，最好选择支持 Kerberos 身份验证的 LDAP 提供程序。

无需连接到 LDAP 服务器。尽管纯（非 SSL）LDAP 在端口 389/TCP 上运行，但支持 LDAP over SSL 的计算机默认使用端口 636/TCP；不过，此端口也是可配置的。请注意，vCloud Director 支持旧版 LDAP over SSL (LDAPS) 方法，但不支持使用 StartTLS 命令在 LDAP 连接中协商 TLS。

最后，必须使用 SSL 证书正确配置启用了 LDAP 的目录服务器。配置方法不在本文档讨论范围内...

导入组

将组导入到 vCloud Director，是为了避免手动分别导入具有相同角色的所有用户。当 LDAP 用户登录时，其会话将获得映射到其所在组的分配角色。当用户的组成员资格根据他们在组织内的职责变动而发生更改时，分配给这些用户的角色也会根据组与角色的映射关系自动更改。因此，组织可以轻松将云角色与内部组织组/角色以及置备和管理它们的系统集成。

例如，组织可能决定最初只授予 LDAP 用户“仅控制台访问权限”角色来限制用户的权限。为此，请将需要此基本角色的所有用户添加到一个 LDAP 组，导入该组后，组织管理员向其分配“仅控制台访问权限”角色。然后，将需要履行其他工作职责的用户添加到其他 LDAP 组，并在导入到 vCloud Director 后分配具有更多特权的角色。例如，可以将需要创建目录的用户添加到组织 LDAP 服务器中的“云 A 目录作者”组。然后，组织 A 的组织管理员可以导入“组织 A 目录作者”组，并将其映射到 vCloud Director 中预定义的“目录作者”角色。有关操作步骤，请参见《vCloud Director 用户指南》中的“导入组”说明。

检查表

7

此检查表汇总了本文档中所述的主要安全配置任务。

- 除了本文档中的指导，您还应注意 http://www.vmware.com/security/advisories/ 中的安全建议，并使用该页面上的表单注册电子邮件警示。有关 vCloud Director 的其他安全指导和最新建议也将在此页面上发布。
- 管理员应遵循《vSphere 安全性》(https://docs.vmware.com/cn/VMware-vSphere/6.0/com.vmware.vsphere.security.doc/GUID-52188148-C579-4F6A-8335-CFBCE0DD2167.html)、《保护 VMware NSX for vSphere》(https://communities.vmware.com/docs/DOC-27674) 和《NSX-v 6.3.x 安全配置指南》(https://communities.vmware.com/docs/DOC-28142) 中建议的步骤，确保安全安装这些产品。
- 安装前将当前的安全修补程序应用到单元 Linux 平台、vCloud Director 数据库和虚拟基础架构；持续监控以确保这些组件处于最新修补程序级别，这一点也至关重要。
- 应向单元 Linux 平台应用标准安全强化过程，包括禁用不必要的网络服务、移除不必要的软件包、限制远程 root 用户访问和强制使用强密码策略。如果可能，使用集中式身份验证服务，例如 Kerberos。考虑安装监控和入侵检测工具。
- 可以在单元 Linux 平台上安装其他应用程序和置备其他用户，但不建议您这么做。扩大单元操作系统的访问权限可能会降低安全性。
- 请仅允许有需要的用户访问 `responses.properties` 文件。如果它正在使用中（向服务器组添加单元时），请针对所有目标主机均可访问的位置设置适当的访问控制。应严格控制所有备份，如果备份软件支持加密，还应对备份进行加密。在所有服务器主机上安装该软件后，应删除这些可访问位置中 `responses.properties` 文件的所有副本。
- `responses.properties` 和 `global.properties` 文件受 `$VCLOUD_ HOME/etc` 文件夹和文件本身的访问控制保护。请勿更改文件或文件夹的权限。
- vCloud Director 服务器的物理和逻辑访问必须严格限于需要登录且具有所需最低访问级别的用户。这涉及通过 `sudo` 和其他最佳做法限制 root 帐户的使用。必须使用从备份自身单独管理的密钥严格保护和加密服务器的所有备份。
- 有关数据库安全要求，请参阅所选的 vCloud Director 数据库软件的安全指南。
- 不应为 vCloud Director 数据库用户授予该服务器上其他数据库的特权或其他系统管理特权。
- 确保用于对单元、连接 vCenter Server、vCloud Director 数据库、防火墙和其他设备进行管理访问的所有凭据都遵循密码复杂性标准。

- 务必从深度防御角度出发，更改 vCloud Director 环境中不同服务器的管理密码，包括单元、vCloud Director 数据库、vCenter Server 和 NSX。
- 有关创建和替换 vCenter 和 ESXi 所用证书的信息，请参见 https://docs.vmware.com/cn/VMware-vSphere/6.0/com.vmware.vsphere.security.doc/GUID-779A011D-B2DD-49BE-B0B9-6D73ECF99864.html。强烈建议您了解此信息。
- vCenter 证书应具有与 vCenter 安装所在服务器的完全限定域名 (FQDN) 匹配的公用名称 (CN) 字段。
- 配置 vCloud Director 以检查 vCenter 证书。
- vCenter 证书应由 CA 签名，并且具有与单元安装所在主机的 FQDN 相匹配的 CN。
- 确保 vCloud Director 服务可供外部使用的建议方法是将单元放置在 DMZ 中，并使用网络防火墙将 Internet 与 DMZ 上的 vCloud Director 单元相隔离。唯一需允许通过 Internet 侧防火墙的端口是 443/TCP。
- 因为 vCloud Director 单元在 DMZ 中，因此它们对所需服务的访问也应由网络防火墙传递。具体来说，建议在将 DMZ 和内部网络隔离的防火墙的另一端访问 vCloud Director 数据库、vCenter Server、vSphere 主机、IDP（包括 LDAP）以及任何备份或类似服务。
- 需要从云外部进行访问（例如从 Internet）的虚拟机将通过针对所公开服务配置的端口转发连接到公共网络或专用的 NAT 路由网络。这些组织 VDC 网络所连接的外部网络要求保护防火墙允许商定的流量进入此 DMZ 网络。
- 一般情况下，建议将需要从 Internet 进行访问的 vApp 放置在专用的路由网络中。租户将能够控制防火墙和 NSX 提供的端口转发规则。您选择部署的网络防火墙可能会默认应用这些规则和其他规则。有关具体配置说明和默认功能，请参见所选防火墙的文档。
- 深度防御原则要求在对单元所连接的 DMZ 实施保护的网络防火墙上阻止 JMX（端口 8999/TCP）和 JMS（端口 61611/TCP 和 61616/TCP）。
- 为 WAF 或负载平衡器后面的多单元云设置公共 Web URL、公共控制台代理地址和公共 REST API 基本 URL。
- Web 应用程序防火墙 (WAF) 应部署在 vCloud Director 单元的前面。
- 在此类部署中，建议配置 WAF 以允许检查和正确阻止恶意流量。通常通过 TLS 或 SSL 终止来实现。
- 配置 TLS 或 SSL 终止时，重要的一点是，不仅要在 Web 应用程序防火墙 (WAF) 上安装 CA 签名的证书，以便 vCloud API 和 Web 控制台等客户端应用程序可以识别服务器的身份，还要在单元上使用 CA 签名的证书，即使这些单元仅为 WAF 可见。
- 最后，如果负载平衡器独立于 WAF，它也应使用 CA 签名的证书。
- 如有可能，建议在防火墙上启用 `X-Forwarded-For` 标头生成。
- 如果 vCloud Director 服务器分配了专门用于管理的第三个 IP 地址，请将 JMX 直接绑定到此 IP 地址。默认情况下，vCloud Director JMX 连接器将绑定到配置期间指定的主 IP 地址。通过在 /opt/vmware/vcloud-service-director/etc/global.properties 中插入以下属性可以覆盖此默认值：
  `vcloud.cell.ip.management=` *`JMX 连接器应绑定的管理网络的 IP 或主机名.`*

- 更安全的建议配置需要将 JMX 连接器绑定到 localhost 地址：`vcloud.cell.ip.management=127.0.0.1`。如果 JMX 仅公开给 localhost，则将 SSH 用作隧道机制进行任意 JMX 访问以保护 JMX 通信。如果您的管理要求不允许使用这种 localhost 配置且 JMX 必须在 vCloud Director 服务器之外公开，则应使用 TLS 或 SSL 保护 JMX。
- 单元后面的是 vCloud Director 所需的专用管理元素：其数据库、NSX、vCenter Server、系统 LDAP 服务器（如有）、vCenter 使用的 Active Directory 服务器以及 vSphere 主机的管理接口。防火墙会严格控制它们的连接，因为不应从 DMZ 上的其他虚拟机或直接从 Internet 访问这些服务。
- 它还假定典型的数据中心安全技术（如 IDS/IPS、SIEM、配置管理、修补程序管理、漏洞管理、防病毒和 GRC 管理系统）将应用于 vCloud Director 及其关联系统、vSphere 及其关联系统，以及支持它们的网络和存储基础架构。
- 正确管理租约、配额、限制和分配模型可以确保租户组织不会无意或有意拒绝其他租户组织的服务。
- 在这些情形及其他情形中，应使用不同的提供者 VDC 将资源池、网络和数据存储分割到不同的安全域，以便对具有相似问题的 vApp 进行分组（或隔离）。
- 如果允许过度分配由多个租户组织使用的池中的资源，则其他租户的服务质量可能会降低。要避免“嘈杂邻居”租户导致的拒绝服务，必须正确监控服务级别，但安全性不要求将租户隔离到各个资源池中来实现此目标。
- 有时，组织 VDC 网络可能会使用外部网络连接两个不同的 vApp 及其网络或将 vApp 网络连接回企业数据中心。在这些情况下，不应在租户组织之间共享外部网络。
- 对于遍历外部网络同时要求保密保护的通信（例如，vApp 到企业数据中心的连接或 vApp 到 vApp 的网桥），建议在组织 VDC 网络中部署 NSX Edge 或其他 VPN 虚拟设备。
- 如果必须在租户之间共享网络池，最安全的做法是共享 VXLAN 支持的池。相较于 VLAN 支持的池，VXLAN 支持的池可以支持更多网络，并且会在 ESXi 内核层强制实施隔离。
- 如果在存储配置文件之间共享数据存储，则应设置存储限制、启用精简配置（如果可能），并仔细监控存储使用情况。此外，还应非常谨慎地管理 vApp 存储租约。
- 虚拟机永远无法访问其 VMDK 外部的任何存储，除非它们与这些存储系统建立了网络连接。本指南不建议进行此连接；提供商可以网络服务形式为 vApp 提供外部存储访问，但必须与分配给支持云的 vSphere 主机的 LUN 隔离开。
- 隔离管理网络与虚拟机数据网络非常重要，如《vSphere 安全性》(https://docs.vmware.com/cn/VMware-vSphere/6.0/com.vmware.vsphere.security.doc/GUID-52188148-C579-4F6A-8335-CFBCE0DD2167.html) 中所述。
- 同样，管理网络必须与提供组织管理员访问权限的 DMZ 隔离开。
- 存储网络也进行物理隔离。这遵循 vSphere 最佳做法，可以保护租户组织和提供商存储免于恶意虚拟机的危害。
- vMotion 并非始终放置与管理网络隔离的网络上；但在云中，从职责分离的角度来看，应始终将 vMotion 放置在与管理网络隔离的网络上。vMotion 通常在清除时进行，如果将其放置在管理网络上，提供商管理员或其他有权访问该网络的用户将可以“嗅探”vMotion 流量，而这一行为侵犯了租户隐私。因此，您应为云工作负载的 vMotion 创建单独的物理网络。

- 定期检查日志并查看是否存在可疑、异常或未经授权的活动是一种良好的安全做法。例行日志分析也有利于确定系统配置错误和故障，并有助于确保遵守 SLA。
- 安装期间可以设置 Syslog 服务器。我们建议使用启用了 TLS 的 Syslog 基础架构。基于多重原因考虑，建议将日志导出到 Syslog 服务器。建议为 `syslog` 服务器配置冗余，确保重要事件始终可以记录到日志中。安全运维和 IT 运维组织也可以受益于集中聚合和管理的诊断日志。我们建议使用 `logrotate` 或类似方法来控制日志大小和保留的旧日志文件数量。
- 请确保有足够的可用磁盘空间来容纳诊断日志和 Jetty 请求日志。使用集中化日志记录可确保日志文件达到 400 MB 上限并导致文件轮换和删除时，您也不会丢失重要的诊断信息。
- vCloud Director 连接并使用的其他系统将创建应整合到审核流程的审核日志。其中包括来自 NSX、vCloud Director 数据库、vCenter Server 和 vSphere 主机的日志。
- 创建初始本地系统管理员帐户后，强烈建议由 LDAP 或 vSphere SSO 服务等身份提供程序管理所有系统管理员帐户。
- 一些云提供商可能允许组织使用系统 LDAP 内的 OU 或者托管组织的 LDAP 目录。在这两种情况下，必须提供目录的适当管理访问权限，以便组织管理员可以管理用户。如果缺少此类管理控制，租户组织应只使用他们自己托管和管理的专用 LDAP 目录。
- 组织托管自己的 LDAP 服务器时会带来另一个问题：服务器会在 DMZ 外部公开。公众不需要访问这项服务，因此应当采取措施，仅限 vCloud Director 单元访问该服务。为此可采取一种简单的配置方法，将 LDAP 服务器和/或外部防火墙配置为仅允许从属于 vCloud Director 单元的 IP 地址访问。
- 供商可以采取措施防止类似攻击，包括在条件允许时，限制请求的源 IP 地址，以及确保分配的组织名称不会与其他组织名称过于相似。
- 必须将 vCloud Director 配置为通过 SSL 连接到 LDAP 服务器，以妥善保护用于验证这些服务器的密码。配置 LDAP over SSL 时，请勿接受所有证书。
- 务必了解并应用管理用户及其密码的最佳做法。
- 应使用日志管理、安全信息和事件管理 (SIEM) 或其他监控系统来监控试图通过暴力攻击破解密码的行为。
- 建议使用 IT 安全部门批准的方式安全地存储系统管理员和组织管理员的密码。