VMware Cloud Director Security

VMware Cloud Director 10.1
vCloud Director 10.0
vCloud Director 9.7

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

Contents

Introduction

1

VMware Cloud Director™ is a flexible system for providing cloud computing services. It leverages and extends the core virtualization and management technologies of VMware for support of cloud environments.

Because the system was developed and tested with multitenancy, scalability, and other security concerns in mind, how you deploy VMware Cloud Director can have a significant impact on the security of the overall system. This document describes some possible threats that the system faces, as well the security features provided by the overall VMware software stack and the related components it uses, such as its underlying database.

No set of guidelines can cover all possible customer use cases. Each deployment of VMware Cloud Director can have its own IT environment, with differences in network topology, internal security systems and standards, customer requirements, and use cases. Some general guidelines are given to increase the overall security of the system. Where appropriate, more specific usage scenarios are also considered with guidance tailored to those particular cases. Nevertheless, the specific recommendations from this guide that you choose to follow ultimately depend on your unique deployment environment and the threats you determine to be a risk for your organization and want to mitigate.

In general, threats to VMware Cloud Director fall into two separate baskets: internal threats and external threats. Internal threats typically involve issues of multitenancy, and external threats target the security of the hosted cloud environment, but those lines are not hard and fast. There are internal threats that attack the security of the hosting environment, for example.

In addition to following the guidance in this document, you should monitor the security advisories at http://www.vmware.com/security/advisories.html and sign up for email alerts using the form on that page. You can find additional security guidance and late-breaking advisories for VMware Cloud Director there.

You can report security issues with VMware Cloud Director at security@vmware.com.

Scope of Recommendations

Recommendations provided in this guide are limited to the management of security issues specific to VMware Cloud Director. As a Web application hosted on a Linux platform, VMware Cloud Director is subject to the security vulnerabilities present in those two categories, all of which are documented elsewhere. VMware Cloud Director 9.7 and later versions can be deployed alternately as an appliance cluster hosted on the Photon OS platform. Compared to the Linux deployments, the appliance deployment generally provides more a secure out-of-the-box configuration.

It is also important to remember that secure deployment of software is only part of an overall security process, which includes physical security, training, operational procedures, patch strategy, escalation and response plans, disaster recovery, and many other topics. Most of these additional topics are not discussed in this guide.

Threats 2

Security threats to VMware Cloud Director can be broadly categorized as either internal threats that originate within the system and its tenants, or external threats that originate outside the system. This latter category includes threats to the infrastructure created to host a VMware Cloud Director server group and threats to the installed VMware Cloud Director software.

Multitenancy and Internal Threats

With VMware Cloud Director, tenants have managed access to VMware vSphere ® network, computing, and storage resources. Tenant users can log into VMware Cloud Director to deploy and use virtual machines, use storage, run applications, and share resources with other users.

One of the key features of VMware Cloud Director is that it does not provide direct visibility or access to most system-level resources, including physical host information such as IP addresses, MAC addresses, CPU type, ESXi access, physical storage locations, and so on, to non-administrative users. However, users might still attempt to gain access to information about the system infrastructure on which their cloud-enabled applications run. If they can do so, they might be able to initiate better attacks against the lower levels of the system.

Even at the level of virtualized resources, users can attempt to use their legitimate access to obtain unauthorized access to parts of the system they are not entitled to. For example, users can try to access resources that belong to another organization. They might attempt a privilege escalation, in particular, obtaining access to actions reserved for administrators. Users might also attempt actions that, intentionally or not, disrupt the overall availability and performance of the system, in extreme cases resulting in a "denial of service" for other users.

In addition, various administrative users generally exist. These users include the system administrator for a VMware Cloud Director site, tenant organization administrators, administrators of databases and networks, and users with access rights to ESXi, vCenter Server, and guest operating systems that run management tools. These users have higher privileges compared to ordinary users, and usually have a direct login to internal systems. Nevertheless, their privileges are not unlimited. There is a potential threat that they too might attempt privilege escalation or take harmful actions.

As discussed in this guide, the security of VMware Cloud Director from these threats comes from the architecture, design, and implementation of VMware Cloud Director, vSphere, VMware NSX®, other security systems, and the infrastructure on which these systems are deployed. Due to the flexibility and dynamic nature of these systems, it is critical to follow the applicable security configuration guidance for all these components.

Secure Hosting and External Threats

The sources of external threats are systems and users from outside the cloud, including the Internet. Those sources can attack VMware Cloud Director through its APIs and Web interfaces, like the VMware Cloud Director Tenant Portal and Service Provider Admin Portal, the vApp transfer service, the virtual machine remote console, or the proxying capability of VMware Cloud Director 10.0 and later. A remote user who has no access rights to the system can attempt to gain access as an authorized user. Authenticated users of those interfaces can also be the sources of external threats, as they might try to exploit vulnerabilities in the system not available to unauthenticated users.

Typically, these actors attempt to exploit flaws in the system implementation or its deployment to obtain information, acquire access to services, or simply to disrupt the operation of the cloud through the loss of system availability or system and information integrity. As the description of these attacks implies, some of these attacks violate the tenant boundaries and hardware abstraction layers that VMware Cloud Director attempts to enforce. While the deployment of the different layers of the system affects the mitigation of these threats, the externally facing interfaces, including firewalls, routers, VPNs, and so on, are of utmost concern.

VMware Cloud Director Architecture and Security Features

3

VMware Cloud Director provides vSphere and NSX infrastructure as a service, enabling the tenant isolation required in a cloud environment.

You can deploy VMware Cloud Director as a server group of Photon OS-based appliances or as a server group of one or more Linux servers.

VMware Cloud Director Appliance Deployment

The appliance-based deployment consists of VMware Cloud Director servers installed on Photon OS-based hosts. A high availability embedded PostgreSQL database cluster is optionally installed on a minimum of three of the servers. The cluster consists of a primary database and two standby databases which are synchronous replicas. In addition to the three database cells, stateless application cells can be added for horizontal scaling. All cells connect to the embedded PostgreSQL primary database. All cells connect to multiple vCenter Server systems, the ESXi hosts that they manage, and the NSX Manager instances that provide networking services. A non-high availability PostgreSQL configuration of a single database cell can also be deployed. For more information, see the *VMware Cloud Director Installation, Configuration, and Upgrade Guide*.

Figure 3-1. VMware Cloud Director Appliance Architecture Diagram
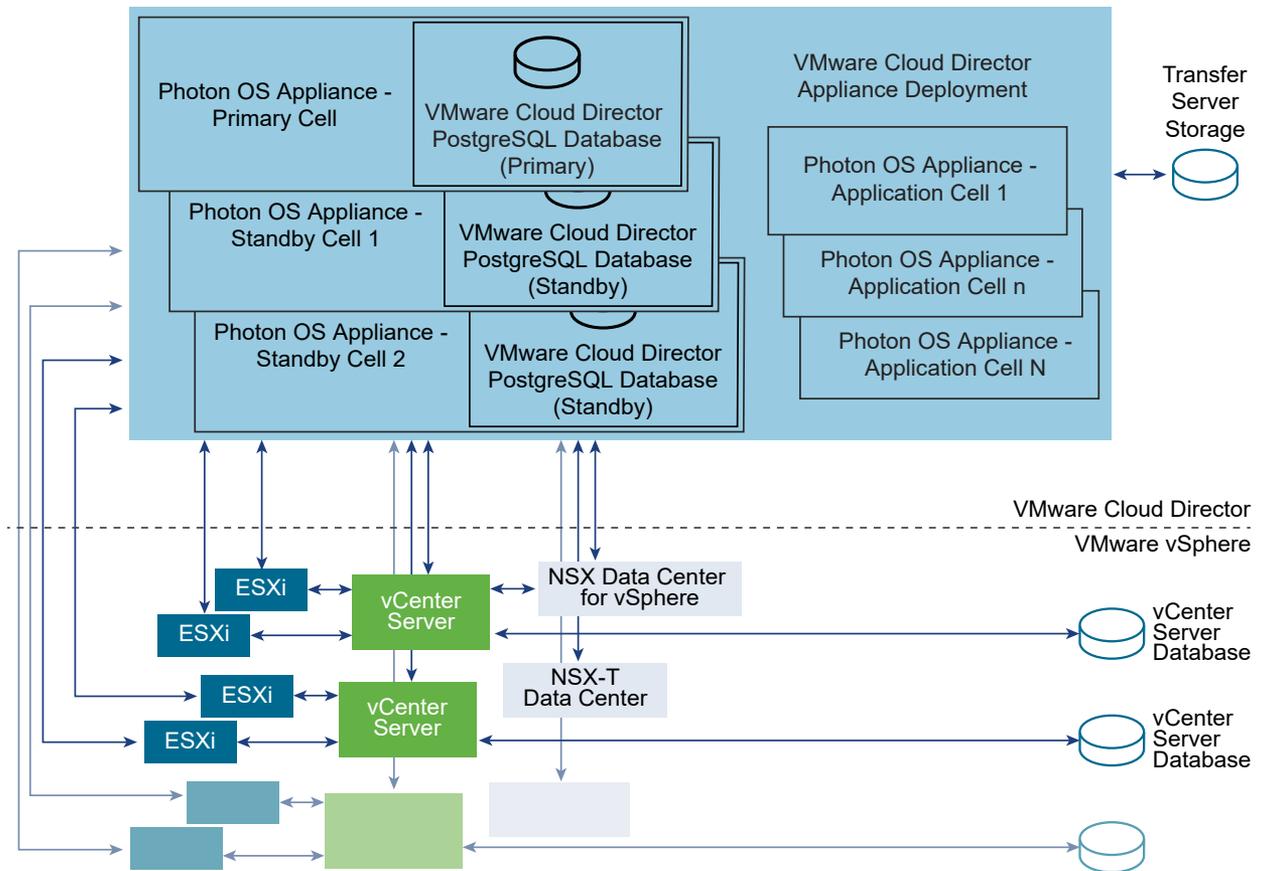
VMware Cloud Director on Linux Installation

For the Linux-based installation, each server in the group runs a collection of services called a VMware Cloud Director cell. All cells share a single VMware Cloud Director database, and connect to multiple vCenter Server systems, the ESXi hosts that they manage, and the NSX Manager instances that provide networking services.

Figure 3-2. VMware Cloud Director Linux Installation Architecture Diagram
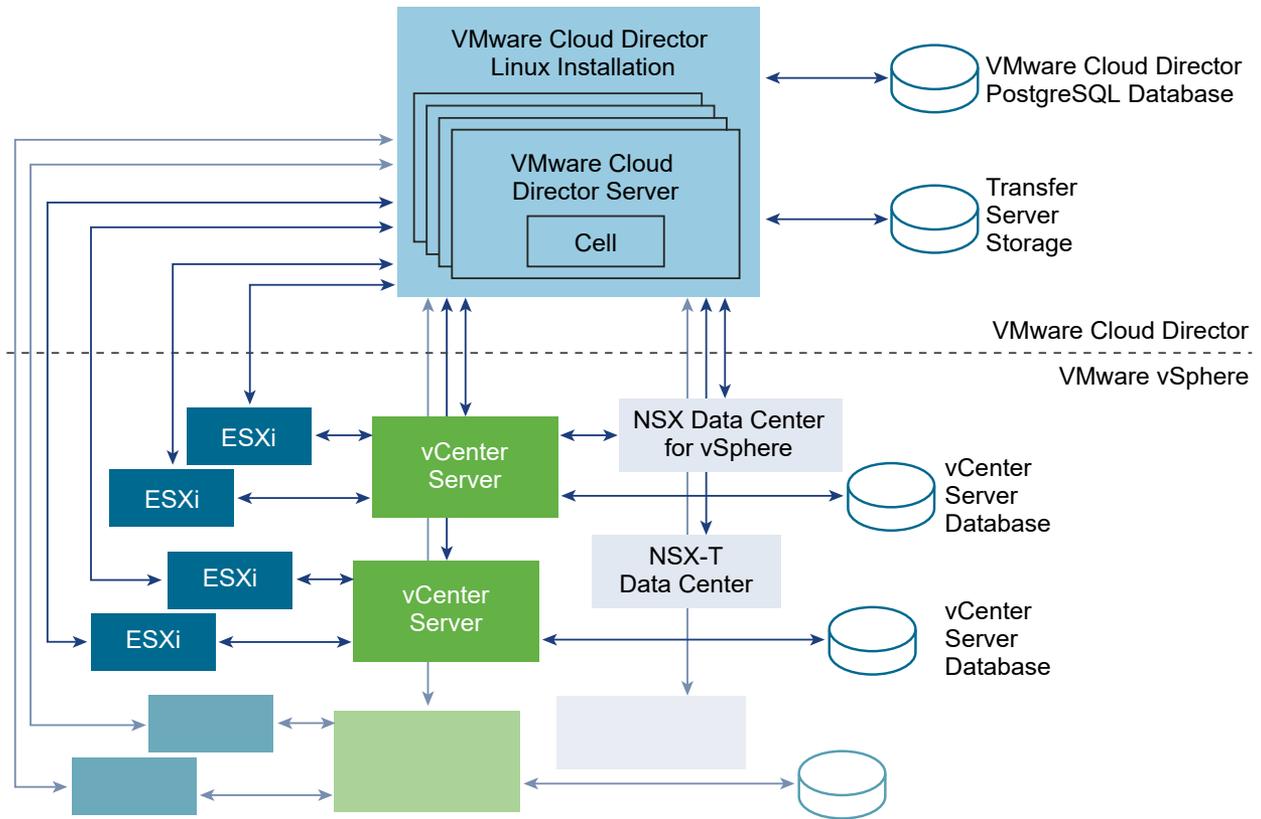
The appliance and Linux diagrams show a single VMware Cloud Director server group deployment or installation. Within the server group there might be many VMware Cloud Director server hosts, each with a single cell running. Together, the server group shares the VMware Cloud Director database and an NFS file share. The cloud abstraction is built using the VMware Cloud Director software and leveraging capabilities in both vCenter Server and NSX, shown in the diagram as connecting to the server group.

Dedicated and Shared vCenter Server Instances

Starting with VMware Cloud Director 9.7, you can select to dedicate a vCenter Server instance to a tenant or to use the vCenter Server instance to back a provider virtual data center.

For dedicated vCenter Server instances, the infrastructure of an attached vCenter Server instance is encapsulated as a Software-Defined Data Center (SDDC) and is fully dedicated to a single tenant.

After you enable the tenant access for a vCenter Server instance, you can publish the dedicated instance to a tenant. Tenant users can then view the vCenter Server instances within the tenant portal and access them through VMware Cloud Director acting as a proxy.

Figure 3-3. Dedicated and Shared vCenter Server Architecture Diagram
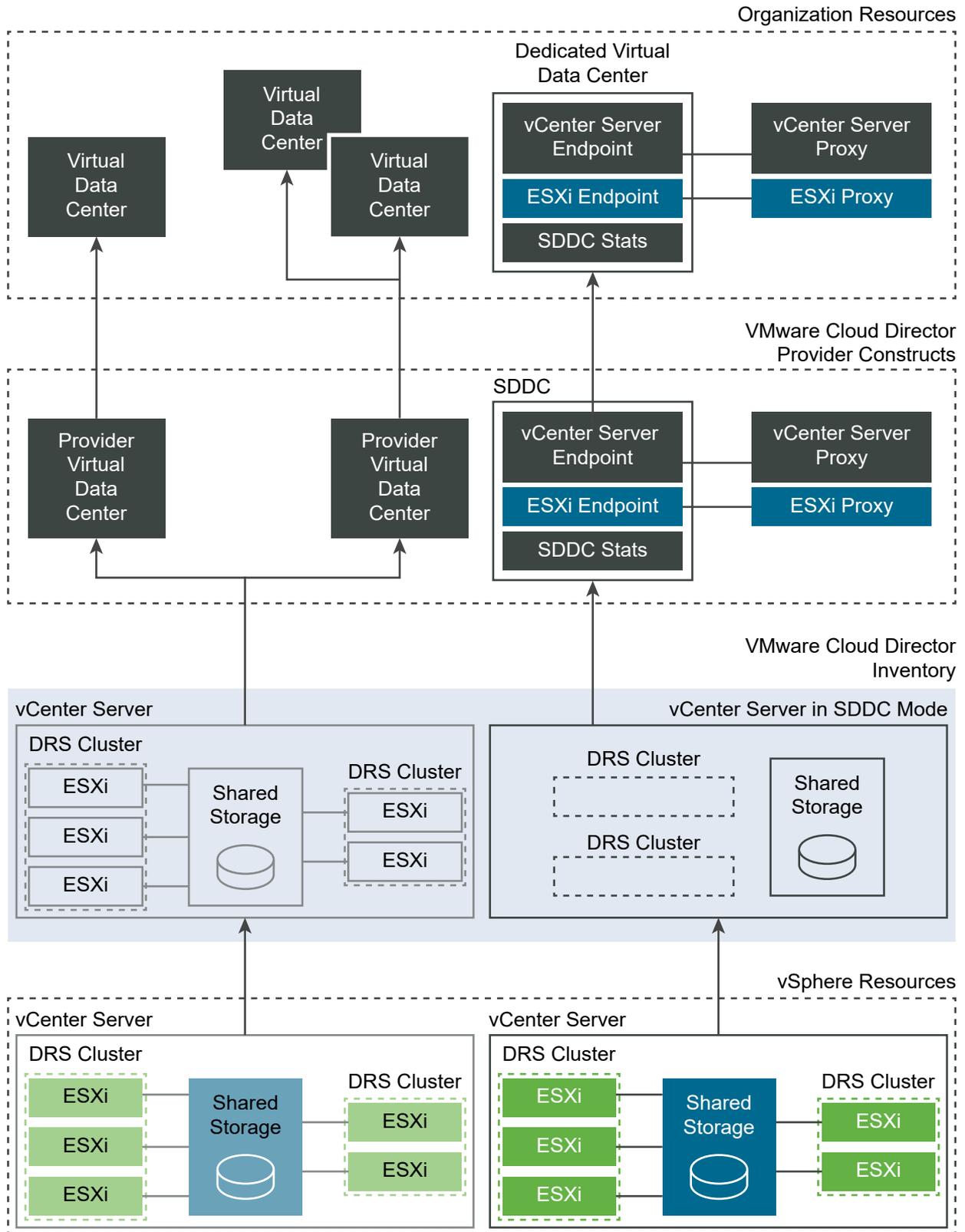
The shared vCenter Server instance model represents the legacy use of vCenter Server instances where they back one or more provider virtual data centers. The provider can use different resource pools of the vCenter Server instance across multiple provider VDCs and then allocate those resource pools to different tenants.

VMware Cloud Director organizations and their users do not interact directly with vCenter Server and NSX to create and manage their workloads. For anyone other than a **system administrator**, all interactions with vCenter Server and NSX are presented as VMware Cloud Director operations on VMware Cloud Director objects. Permission to access and operate on VMware Cloud Director objects is role-based. Predefined roles provide baseline access to common tasks. Organization administrators can also create custom roles that take advantage of an array of fine-grained rights.

The subsequent subsections describe security at the virtual computing layer, the cloud abstraction, and the virtual networking layer.

This chapter includes the following topics:

■ Virtual Machine Security and Isolation

■ Security and the VMware Cloud Director Abstraction

■ Security and the Virtual Networking Layer

Virtual Machine Security and Isolation

When we examine security and network isolation in this document, we are looking to assess the risk that network separation and traffic isolation controls are insufficient, and to choose the recommended corrective actions.

When looking at network segmentation, we have a notion of a trust zone. Trust zones are a proactive security control to control access to network traffic. A trust zone is loosely defined as a network segment within which data flows relatively freely, whereas data flowing in and out of the trust zone is subject to stronger restrictions. Examples of trust zones include:

■ Perimeter networks (also called demilitarized zones or DMZs)

■ Payment-card industry (PCI) cardholder data environment

■ Site-specific zones, such as segmentation according to department or function

■ Application-defined zones, such as the three tiers of a Web application

Security and the Underlying Virtualization Layer

A significant portion of VMware Cloud Director security, especially in protecting cloud tenants from internal threats, comes from the security design and the specific configuration of the underlying virtualization layer. This includes the design and configuration of vSphere, the additional security of VMware Cloud Director software-defined networks, the leveraging of NSX technology, and the security of the ESXi hosts themselves.

Security and the VMware Cloud Director Abstraction

VMware Cloud Director imposes a strict separation between vSphere operations and the day-to-day operational needs of tenants.

The VMware Cloud Director abstraction enables a service provider to delegate the vApp creation, management, and use to tenant organizations or an IT department can delegate these capabilities to line-of-business teams. Tenant organization administrators and users do not operate on or manage vCenter Server features like vMotion, vSAN. Tenants deal only with deploying their workloads like vApps to resource pools and storage profiles, and connecting them to organization VDC networks owned by their organization. Since organization administrators and users never log in to vCenter Server, there is no chance of a misconfigured vCenter Server permission giving the user too many rights. Moreover, the provider is free to change the composition of resource pools and storage profiles without the organization needing to change anything.

More important, this abstraction separates different organizations from each other. Even if they happen to be assigned common networks, datastores, or resource pools, they cannot modify or even see each other's vApps. The exception is vApps connected to the same External Network, because they are sharing a vSwitch. Providing each tenant organization with their own dedicated datastores, networks, and resource pools, while not a requirement of the system, enables the service provider to enforce even greater separation between the organizations.

Limiting Tenant Access to System Information

Although VMware Cloud Director hides system-level operations from tenants, certain features of the system can be configured to provide information that a malicious tenant might misuse.

Disable sending host performance data to guests.

> vSphere includes virtual machine performance counters on Windows operating systems where VMware Tools is installed. By default, vSphere does not expose host information to the guest virtual machine. Because a malicious tenant might misuse the information about the physical host, you must verify that this default behavior is in place. See Verify That Sending Host Performance Data to Guests is Disabled in *vSphere Security* for details.

Limit the collection of VM metrics

> VMware Cloud Director can collect metrics that provide current and historic information about the virtual machine performance and resource consumption. Some of these metrics include information about the physical host that a malicious tenant might misuse. You must consider configuring the metrics collection subsystem to collect only those metrics that are not subject to a malicious use. See Configuring Metrics Collection in the *VMware Cloud Director Installation, Configuration, and Upgrade Guide* for details.

Exercise Caution with Extensions

VMware Cloud Director supports various extensibility methods. These methods are all designed to prevent any extension from acquiring rights not granted to tenant users or escalating the privileges assigned to tenants at installation. However, an extension can provide, intentionally or not, additional attack surfaces that someone with knowledge of the extension might exploit. Service providers and tenant administrators must exercise caution when offering, reviewing, or installing extensions. In addition, careful management of allowed extensions and use of appropriate safeguards such as the `X-Content-Type-Options: nosniff` header can prevent plugins from loading malicious content.

Security and the Virtual Networking Layer

VMware Cloud Director networking leverages the software-defined networking capabilities of vSphere and NSX to provide tenants with secure access to shared network resources. The service provider's responsibilities are limited to providing external connections and the networking infrastructure required to make those connections usable by tenants and allocation of system-level networking resources to network pools so that tenants can use them.

This brief overview of VMware Cloud Director establishes the context in which we can discuss provider-level and tenant-level networking requirements from a security configuration standpoint. These features are described in detail in the VMware Cloud Director documentation.

Provider-Level Network Resources

In the typical case, a service provider is responsible for creating one or more connections between VMware Cloud Director and an external network such as the Internet or a customer's enterprise network. This sort of network is essentially a commodity IP network connection. It does not provide confidentiality if packets on it are intercepted at the physical level, and provides no VMware Cloud Director VLAN or VXLAN network isolation features.

To enable tenant organization networking, the service provider must create one or more network pools that aggregate resources from ESXi DVswitches and port groups in a form that can be made available to tenant organizations. An external network does not consume resources from a network pool. A VXLAN- or VLAN-backed network pool provides isolation using VLANs across a vNetwork Distributed Switch. A VMware Cloud Director VXLAN network can also provide isolation by encapsulating Layer 2 packets in other Layer 2 packets (MAC-in-MAC) in the ESXi kernel. This isolation allows the kernel when de-encapsulating packets to direct them to the correct guest VMs connected to the networks created out of this sort of pool. Starting with version 10.0, you can create Geneve network pools to provide the overlay capability for NSX-T Data Center resources.

The service provider is also responsible for creating and managing the NSX infrastructure that stands between the networks that tenants create for themselves and the system-level resources such as switches and port groups provided by ESXi. From these resources, tenant organizations can create their own networks.

To provide a fully routed network topology in a virtual data center, a **system administrator** can dedicate an external network to a specific NSX-T Data Center edge gateway. In this configuration, there is a one-to-one relationship between the external network and the NSX-T Data Center edge gateway, and other edge gateways cannot connect to the external network. Dedicating an external network can cause disruptions. You must remove the tenants attached to the network before dedicating it to a specific NSX-T Data Center edge gateway. You must also remove tenants from a dedicated external network before removing the dedicated status because the tenants might have traffic through the network between their private clouds when MPLS is deployed.

Organization VDC Networks

An organization VDC network allows VMs in the organization VDC to communicate with each other and to access other networks. The VMs can access organization VDC networks and external networks, either directly or through an edge gateway that can provide firewall and NAT services.

Table 3-1. Types of Organization VDC Networks and Their Requirements

Organization VDC Network Connection	Description	Requirements
Direct connection to an external network.	Provides direct layer 2 connectivity to machines and networks outside of the organization VDC. Machines outside of this organization VDC can connect directly to machines within the organization VDC. Only a **system administrator** can create a direct organization VDC network. Direct networks are only supported for organization VDCs that are backed by NSX Data Center for vSphere.	The cloud must contain an external network.
Routed connection to an external network.	Provides controlled access to machines and networks outside of the organization VDC through an edge rateway. **System administrators** and **organization administrators** can configure network address translation (NAT) and firewall settings on the gateway to make specific virtual machines in the VDC accessible from an external network.	The VDC must contain an edge gateway and a network pool.
No connection to an external network.	Provides an isolated, private network that machines in the organization VDC can connect to. This network provides no incoming or outgoing connectivity to machines outside this organization VDC.	The VDC must contain a network pool.
Imported NSX-T Data Center logical switch	This network uses an existing NSX-T Data Center logical switch. Only a **system administrator** can import a network.	The provider virtual data center that backs the target organization virtual data center must be associated with an NSX-T Manager instance. The **system administrator** must create at least one NSX-T Data Center logical switch that is not in use by other organization virtual data center networks.

By default, only virtual machines in the organization VDC that contains the network can use it. When you create an organization VDC network, you can specify that it is shared. All virtual machines in the organization can use a shared organization VDC network.

vApp Networks

A vApp network is contained within a vApp. A vApp network is a logical network that controls how the virtual machines in a vApp connect to each other and to organization VDC networks. Users can create and update vApp networks and connect them to organization VDC networks, either directly or with NAT and Firewall protection.

Infrastructure Security

4

Much of this guide focuses on protecting VMware Cloud Director itself. However, overall system security also requires securing the infrastructure on which VMware Cloud Director depends, including vSphere, NSX, the cell Linux platform, the VMware Cloud Director database, and the NFS server providing shared NFS resources to the VMware Cloud Director server group.

Applying current security patches to each of these infrastructure components before installation is a key step and ongoing monitoring to keep these components at a current patch level is also crucial.

Securing Your VMware Infrastructure

Securing vSphere and NSX is a critical first step in securing VMware Cloud Director. Administrators must review the checklists guides available on https://www.vmware.com/security/hardening-guides.html and also consult the more detailed security information available in the following documents:

vSphere security

vSphere Security

- vSphere 7.0 Security Guide

- vSphere 6.7 Security Guide

- vSphere 6.5 Security Guide

NSX security

Securing VMware NSX for vSphere. For more information, see the VMware Technology Network.

Securing Your Cell Platforms

VMware Cloud Director can be installed on a customer supplied Linux-based system, or deployed as an appliance, running Photon OS 2.0. In either case, VMware Cloud Director cells run as an unprivileged user `vcloud.vcloud` created during installation. The list of supported cell platform operating systems is included in the *VMware Cloud Director Release Notes*. Securing the cell platform, whether it is physical or virtual, is a key part of securing VMware Cloud Director.

Standard security hardening procedures must be applied to the cell platform, including disabling unnecessary network services, removing unnecessary packages, restricting remote root access, and enforcing strong password policies. Try to use a centralized authentication service such as Kerberos. Consider installation of monitoring and intrusion detection tools.

It is possible to install additional applications and provision additional users on the cell OS instance, but it is recommended that you do not do this. Widening access to the cell OS might decrease the security.

Most of these hardening procedures are implemented in the VMware Cloud Director appliance.

Protecting Sensitive Files After Installation

During installation, VMware Cloud Director writes installation data, including passwords, to files in the local file system of the cell Linux host. These files, `global.properties` and `responses.properties`, both found under `$VCLOUD_HOME/etc`, contain sensitive information that you must reuse when you add more servers to a server group. The `responses.properties` file contains responses provided by the administrator when running the configuration script. That file contains an encrypted version of the VMware Cloud Director database password and system keystore passwords. Unauthorized access to that file might give an attacker access to the VMware Cloud Director database with the same permissions as the database user specified in the configuration script. The `global.properties` file also contains encrypted credentials that must not be made accessible to anyone but a cell administrator.

At creation, the `responses.properties` and `global.properties` files are protected by access controls on the `$VCLOUD_HOME/etc` folder and the files themselves. Do not change the permissions on the files or folder as it might either give too much access, reducing security, or restrict access too much, stopping the VMware Cloud Director software from working. In order for the access controls to work properly, physical and logical access to the VMware Cloud Director servers must be strictly limited to those with a need to log in and only with the minimal levels of access required. This involves limiting the use of the root account through `sudo` and other best practices that are outside the scope of this document. Moreover, any backups of the servers must be strictly protected and encrypted, with the keys managed separately from the backups themselves.

In the case of the VMware Cloud Director appliance, the `responses.properties` file is also copied to the NFS shared transfer service storage mounted at `$VCLOUD_HOME/data/transfer` to make it available to configure automatically other appliances joining that server group. Therefore, the NFS server and the access to the NFS shared transfer service storage used by VMware Cloud Director must also be protected.

For more details, see Protecting and Reusing the Response File in the *VMware Cloud Director Installation, Configuration, and Upgrade Guide*.

Administrative Credentials

Ensure that any credentials used for administrative access to the cell, vSphere, the VMware Cloud Director database, to external firewalls and other devices, follow standards for the adequate password complexity. Consider an expiration and rotation policy for passwords wherever possible. Be aware, however, that an expired or changed database, vSphere, or NSX password makes a part or all of the cloud infrastructure nonfunctional until VMware Cloud Director is updated with the new passwords.

It is important from a "defense in depth" perspective to vary the administrative passwords for the different servers in the VMware Cloud Director environment, including the VMware Cloud Director cells, the VMware Cloud Director database, vSphere servers, and NSX manager. The passwords must vary because if one set of credentials is compromised, for example, through a disgruntled employee leaving the organization, other systems are not automatically compromised across the rest of the infrastructure.

For the VMware Cloud Director appliances, password complexity rules and yearly account password expiration for the **root** account are enforced. However, deviating from the "defense in depth" approach mentioned above, the VMware Cloud Director appliances in the same server group must use the same **root** credentials during the initial deployment. The credentials must be identical because the initial **root** password becomes the appliance keystore password and all appliances must have matching keystore passwords. After the initial configuration of the appliance, you can change the **root** password on each appliance to make the passwords unique.

For more information about account and credential management for administrators and tenants, see User Account Management

This chapter includes the following topics:

- Database Security

Database Security

In general, database security is outside the scope of this document. Like all other systems used in your cloud deployment, you are expected to secure properly the VMware Cloud Director database per industry best practices.

The VMware Cloud Director database user account must have only the system privileges listed in the appropriate database configuration guidance in the *VMware Cloud Director Installation, Configuration, and Upgrade Guide*. The VMware Cloud Director database user must not be given privileges over other databases on that server or other system administration privileges. Providing such privileges can violate the Principle of Least Privilege on the database server and give the user more rights than necessary.

Consult the following documents for database security information.

PostgreSQL

In addition to enabling SSL for PostgreSQL connections, review the PostgreSQL Server Administration documents.

The VMware Cloud Director appliance has an embedded PostgreSQL database in the primary appliance. For VMware Cloud Director appliances comprising an embedded database High Availability cluster, the VMware Cloud Director database is replicated to two standby VMware Cloud Director appliance instances, to achieve an HA solution. You can grant external access to the embedded PostgreSQL database. See Configure External Access to the VMware Cloud Director Appliance.

System Security

<div style="text-align: right; font-size: 3em; color: #999;">5</div>

The service provider and system administrators are responsible for the security of each VMware Cloud Director server group.

Securing a VMware Cloud Director server group from outside attackers requires you to take the kinds of defensive measures common to all Web-based services. Such measures include securing HTTPS endpoints with signed certificates and placing a Web application firewall between the system and the Internet. In addition, you must configure the services on which VMware Cloud Director depends, including the RabbitMQ AMQP broker and an optional Apache Cassandra database, in a way that minimizes opportunities for external actors to compromise these systems.

This chapter includes the following topics:

- VMware Cloud Director Appliance OS

- Network Security Requirements

- Certificates

- Firewalls

- Load Balancers and SSL Termination

- Using VMware Cloud Director as a Proxy Server

- Securing MQTT

- Securing RabbitMQ AMQP

- Securing a Cassandra Metrics Database

- Securing Access to JMX

- Configuring the Management Network of VMware Cloud Director

- Auditing and Logging

VMware Cloud Director Appliance OS

The VMware Cloud Director appliance is based on VMware Photon OS 2.0 and features some OS hardening, which might require a periodic user action.

Accounts

The **root** account password for the appliance OS has a one-year expiration. When changing the **root** password, you must do so for the OS of each appliance in the cluster separately. You can use different passwords for the different **root** accounts.

You can disable the **root** SSH access to the appliance. See Enable or Disable SSH Access to the VMware Cloud Director Appliance. Even with **root** SSH access disabled, if the appliance is deployed using a database High Availability (HA) function, then SSH access is still possible for the **postgres** user. The **postgres** user can use SSH access through the public-private key authentication that was automatically established between the cluster nodes. This access is necessary to support the database HA function.

The VMware Cloud Director appliance takes advantage of two non-root accounts, **vcloud** and **postgres**, to ensure that critical processes are running with unprivileged permissions. This follows the principle of least privilege and ensures that the accounts are separated, so that each account can only access the resources that it needs.

Neither of these accounts have passwords and do not expire. The **vcloud** user cannot be logged into. The VMware Cloud Director service and appliance management UI run as the **vcloud** user. You can switch to the **postgres** user from the **root** account using `su - postgres`. The embedded PostgreSQL database runs as the **postgres** user.

OS Package Updates

Installing new versions of the appliance ensures uptaking Photon OS updates.

Embedded PostgreSQL

It is possible to grant external access to the embedded PostgreSQL database. See Configure External Access to the VMware Cloud Director Database.

Network Security Requirements

Secure operation of VMware Cloud Director requires a secure network environment. Configure and test this network environment before you begin installing VMware Cloud Director.

Connect all VMware Cloud Director servers to a network that is secured and monitored.

For information on the network ports and protocols used by VMware Cloud Director, see VMware Ports and Protocols.

VMware Cloud Director network connections have several additional requirements:

- Do not connect VMware Cloud Director directly to the public Internet. Always protect VMware Cloud Director network connections with a firewall. Only port 443 (HTTPS) must be open to incoming connections. Ports 22 (SSH) and 80 (HTTP) can also be opened for incoming connections if needed. In addition, the `cell-management-tool` requires access to the cell's loopback address. All other incoming traffic from a public network, including requests to JMX (port 8999) must be rejected by the firewall.

Table 5-1. Ports That Must Allow Incoming Packets from VMware Cloud Director Hosts

Port	Protocol	Comments
111	TCP, UDP	NFS portmapper used by transfer service
920	TCP, UDP	NFS rpc.statd used by transfer service
61611	TCP	AMQP
61616	TCP	AMQP

- Do not connect the ports used for outgoing connections to the public network.

Table 5-2. Ports That Must Allow Outgoing Packets from VMware Cloud Director Hosts

Port	Protocol	Comments
25	TCP, UDP	SMTP
53	TCP, UDP	DNS
111	TCP, UDP	NFS portmapper used by transfer service
123	TCP, UDP	NTP
389	TCP, UDP	LDAP
443	TCP	vCenter Server, NSX Manager, and ESXi connections using the standard port. If you have chosen a different port for these services, disable connection to port 443 and enable them for the port you have chosen.
514	UDP	Optional. Enables syslog use.
902	TCP	vCenter Server and ESXi connections.
903	TCP	vCenter Server and ESXi connections.
920	TCP, UDP	NFS rpc.statd used by transfer service.
5432	TCP	Default PostgreSQL database port
5672	TCP, UDP	Optional. AMQP messages for task extensions.
61611	TCP	AMQP
61616	TCP	AMQP

- Starting with version 10.1, service providers and tenants can use the VMware Cloud Director API to test connections to remote servers, and to verify server identity as part of an SSL handshake. To protect VMware Cloud Director network connections, configure a deny list of internal hosts that are unreachable to tenants who are using the VMware Cloud Director API for connection testing. Configure the deny list after VMware Cloud Director installation or upgrade and before granting tenants access to VMware Cloud Director. See Configure a Test Connection Deny List.

- Route traffic between VMware Cloud Director servers and the following servers over a dedicated private network.

  - VMware Cloud Director database server

  - RabbitMQ

  - Cassandra

- If possible, route traffic between VMware Cloud Director servers, vSphere, and NSX over a dedicated private network.

- Virtual switches and distributed virtual switches that support provider networks must be isolated from each other. They cannot share the same layer 2 physical network segment.

- Use NFSv4 for transfer service storage. The most common NFS version, NFSv3, does not offer on transit encryption which in some configurations might enable in-flight sniffing or tampering with data being transferred. Threats inherent in NFSv3 are described in the SANS white paper NFS Security in Both Trusted and Untrusted Environments. Additional information about configuring and securing the VMware Cloud Director transfer service is available lin VMware Knowledge Base article 2086127.

Certificates

VMware Cloud Director uses HTTPS (TLS or SSL) to secure all network traffic to all external endpoints. HTTPS is also supported for many internal endpoints, including AMQP and LDAP. It is especially important to provide a certificate signed by a well-known certificate authority (CA) for external endpoints. Internal endpoints are less vulnerable, and in most cases can be adequately secured with enterprise or even self-signed certificates.

All certificates must have a common name (CN) field that matches the Fully Qualified Domain Name (FQDN) of the server on which they are installed. Usually this implies that the server is registered in DNS, so it has a well-defined and unique FQDN, and also it implies that you are connecting to it by FQDN, not an IP address. If you do intend to connect using the IP address, then the certificate must include subjectAltName field that matches the host's IP address.

Additional information is available in RFC 6125 and RFC 5280. You can also consult your CA.

Certificates for Public Endpoints

Endpoints exposed to an enterprise network or other public network such as the Internet should be protected with a certificate signed by a well-known root CA. These endpoints include:

- The cell HTTPS address and console proxy address. You must configure both addresses and supply their certificate and keystore details during installation.

- SSL-terminating load balancers. See Load Balancers and SSL Termination.

In general, well-signed certificates do not need to be imported, since any SSL client can verify the trust chain all the way up to the root. Your local security team creates lower-level certificates, like enterprise-CA or self-signed, that cannot be checked in this way. Your local security team can tell you from where to import the lower-level certificates.

Certificates for Private/Internal Endpoints

The endpoints on private networks are unreachable from public networks and are usually created specifically for use by VMware Cloud Director components such as the database and AMQP. Those endpoints can use certificates signed by an enterprise CA, or even use self-signed certificates if necessary. These endpoints include:

- Internal connections to vSphere and NSX.

- AMQP endpoints connecting VMware Cloud Director and RabbitMQ.

- PostgreSQL database connections (optional).

Having a signed certificate reduces the chance that a malicious application that manages to gain access to a private network can masquerade as a legitimate VMware Cloud Director component.

Centralized Management of Certificates from vSphere Resources

Starting with version 10.1, VMware Cloud Director changes the way it manages SSL certificates provided by vSphere infrastructure resources. Because of that, if you do not import your certificates into VMware Cloud Director before the upgrade, the vCenter Server and NSX connections might show failed connection errors due to SSL verification issues. In this case, after upgrading, use the Service Provider Admin Portal to select each vCenter Server and NSX instance, reenter the credentials for it and verify the certificate that it provides.

Supported Protocols and Cipher Suites

VMware Cloud Director supports several HTTPS protocols, including TLS and SSL. TLS v1.0 and v1.1 are unsupported by default because they have known vulnerabilities. After installation, you can use the cell management tool to configure the set of protocols and cipher suites that the system supports for HTTPS connections. For details, see *VMware Cloud Director Release Notes*.

Support for Connections to vCenter Server and NSX Through an HTTP Proxy

VMware Cloud Director 10.1 supports the HTTP Proxy protocol for connections to vSphere, NSX Manager and NSX-T Manager.

When such a proxy configuration is defined and assigned to a vCenter Server or NSX-T Manager connection, VMware Cloud Director attempts to connect through that proxy with basic authentication. To do that, VMware Cloud Director uses the user name and password that are configured on the corresponding proxy configuration.

VMware Cloud Director connects to the proxy in plain text over HTTP. After the basic authentication with the proxy, VMware Cloud Director uses the proxy connection to initiate tunneled SSL traffic to vCenter Server, NSX Manager or NSX-T Manager.

This deployment configuration is only recommended if your proxy host and VMware Cloud Director instances are behind a load balancer.

For more information about the security implications of using an HTTP proxy configuration, see Using VMware Cloud Director as a Proxy Server.

Configuring vSphere Certificates

In vSphere 6.0 and later, the VMware Certificate Authority (VMCA) provisions each ESXi host and each vCenter Server instance with a certificate that is signed by VMCA by default. You can replace the existing certificates with new VMCA-signed certificates, make VMCA a subordinate CA, or replace all certificates with custom certificates. See vSphere Security Certificates in *vSphere Security* for more information about creating and replacing certificates used by vCenter Server and ESXi.

Configuring VMware Cloud Director to Check vCenter Server Certificates

To configure VMware Cloud Director to check vCenter Server certificates, create a Java keystore in JCEKS format that contains one or more trusted certificates used to sign vCenter Server certificates. Certificates for the individual vCenter Server instances are not in this store, only the CA certificates that are used to sign them.

A command such as this one imports a PEM-encoded certificate from `/tmp/cacert.pem` into a keystore named `myca.ks`:

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

A command such as this one adds another certificate to the same keystore, like `/tmp/cacert2.pem` in this example:

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

Once you create the keystore, follow the instructions for the version of VMware Cloud Director that you are using.

VMware Cloud Director version	Steps
VMware Cloud Director 10.1 and 10.0	1 Log in to the VMware Cloud Director Service Provider Admin Portal as **system administrator**. 2 In the top navigation bar, click **Administration**. 3 Under **Settings** section of the tab, click **General** and navigate to the **Certificates** section of the page. 4 Toggle on the **Verify vCenter Server and vSphere Single Sign-On** and **Verify NSX Manager** options. 5 Click **Edit** and click the **Upload** button. 6 Browse to your Java keystore, then click **Open**. 7 Enter the keystore password and click **Save**.
vCloud Director 9.7	1 Log in to the VMware Cloud Director Web Console (Flex-based UI) as **system administrator**. 2 In the **System Settings** section of the **Administration** tab, click **General**. 3 Navigate to the **Certificates** section of the page. 4 Select the check boxes **Verify vCenter and vSphere SSO certificates** and **Verify NSX Manager certificates**. 5 Click **Browse** and navigate to your Java keystore. 6 Click **Open**. 7 Enter the keystore password and click **Apply**.

When the operation completes, your trusted certificates and other information are uploaded to the VMware Cloud Director database. So you only need to do this operation once for all cells.

Once this option is turned on, all vCenter Server and NSX Manager certificates are checked, so every vCenter Server and NSX Manager must have a correct certificate chain and a certificate that matches its FQDN. If it does not, connections to vCenter Server and NSX Manager will fail.

Important   If you are using VMware Cloud Director 10.0 or 9.7 and you have changed certificates after adding vCenter Server and NSX Manager instances to VMware Cloud Director, you must force reconnection to the servers.

Updating Certificates and Keys for VMware Cloud Director Cells

Each VMware Cloud Director server requires two SSL certificates, one for the HTTP service and one for the console proxy service, in a Java keystore file. You must provide the pathname to these keystores when you install VMware Cloud Director. Signed certificates provide the highest level of trust.

The `certificates` command of the cell management tool automates the process of replacing existing certificates with new ones. Use the `certificates` command to replace self-signed certificates with signed ones or replace expiring certificates with new ones. To create a JCEKS keystore containing signed certificates, see Create an CA-Signed SSL Certificate Keystore for VMware Cloud Director on Linux or Create and Import CA-Signed SSL Certificates to the VMware Cloud Director Appliance in the *VMware Cloud Director Installation, Configuration, and Upgrade Guide*.

To replace SSL certificates for one or both endpoints use a command with the following form:

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

For more information on certificate creation and management for VMware Cloud Director on Linux and for the VMware Cloud Director appliance, see *VMware Cloud Director Installation, Configuration, and Upgrade Guide*.

Firewalls

VMware Cloud Director cells must be accessible by tenants and system administrators, who typically connect to them from outside the service provider's network perimeter. To make VMware Cloud Director services available to the outside, you must place a Web application firewall (WAF) between the Internet or other enterprise network and each VMware Cloud Director public endpoint.

Network firewalls segment physical and virtual networks so that only a limited, well-defined set of traffic on specific ports and protocols passes between them. This document does not define the rationale for a firewall deployment in general or cover the details of firewall setup. Those topics are outside the scope of this guide. Rather, this guide identifies the locations where you must place network firewalls in relation to the different components of a VMware Cloud Director deployment.

Note Management connections can be further limited through IP address restrictions in the network or per-tenant VPNs. This level of protection might be appropriate in certain deployments, but is outside the scope of this document.

As the VMware Cloud Director cells are in the DMZ, you must mediate their access to the services that they need by using a network firewall. Restrict the access to the VMware Cloud Director database, vCenter Server, ESXi hosts, AMQP and any backup or similar services to an internal network that is unreachable from the public side of the firewall. See Network Security Requirements for a list of ports that must be opened in that firewall.

Blocking Malicious Traffic

You must use firewall rules to protect the system against network threats, such as:

- Dropping packets that appear to originate from nonroutable addresses (IP spoofing)

- Dropping malformed TCP packets

- Limiting the rate of requests, especially of SYN requests – to protect against a SYN flood attack (an attempted denial of service)

- Consider denying outbound traffic from the firewall that does not originate from an incoming request.

You can apply these and other rules by using Web Application Firewall or the network firewall you choose to deploy. See your firewall's documentation for specific configuration instructions and default capabilities.

Load Balancers and SSL Termination

You protect VMware Cloud Director public endpoints by using a Web Application Firewall (WAF). When you use it with a load balancer, configure the WAF to allow inspection and blocking of malicious traffic by terminating the HTTPS connection at the WAF. This enables the WAF to carry out the handshake using its own certificate and to forward acceptable requests to the cell with an `X-Forwarded-For` header.

Client requests to VMware Cloud Director must be made to an HTTPS endpoint. An HTTP connection to the cell is supported but is not secure. Even when communications between the remote client and the WAF are secured with HTTPS, WAF-to-cell communication is also carried out over HTTPS.

The following simple diagram, leaving out the load balancer, illustrates the two TLS or SSL connections that exist when using TLS or SSL termination, one between the user's computer and the WAF, and one between the firewall and the VMware Cloud Director cell.

Figure 5-1. TLS/SSL Configuration with WAF
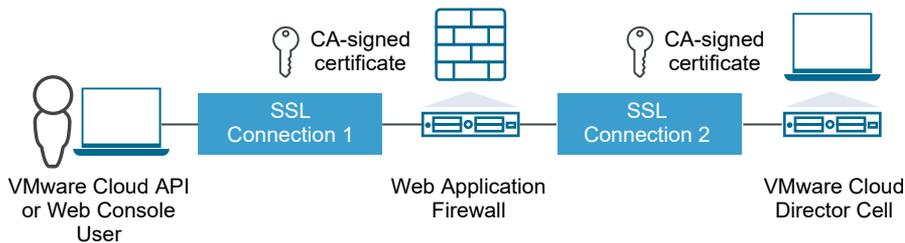
TLS/SSL Termination and Certificates

When configuring TLS or SSL termination, it is important not only to install a CA-signed certificate at the WAF so that client applications such as the VMware Cloud Director API and the Web Console can be assured of the identity of the server, but also to use a CA-signed certificate on the cells even though they are only seen by the WAF. Self-signed certificates, even if the WAF accepts them, are only appropriate if each certificate is manually accepted at deployment time. However, this limits the flexibility of the VMware Cloud Director server group, as each cell must be manually configured (and reconfigured when certificates are renewed).

Finally, if the load balancer is independent of the WAF, it too should use a CA-signed certificate. Procedures for adding certificate chain paths for load-balancer endpoints are documented in Customize Public Endpoints in the *VMware Cloud Director Installation, Configuration, and Upgrade Guide*.

X-Forwarded-For Header

`X-Forwarded-For` is a widely used header, supported by many proxies and firewalls. If possible, you must enable generation of this header at the firewall.

When a firewall is present in front the cell, the cell may query for the client's IP address in order to log it, but it generally gets the address of the firewall instead. However, if the `X-Forwarded-For` header is present in the request the cell receives, it will log this address as the client address and it will log the firewall address as a separate `proxyAddress` field in the log.

Using VMware Cloud Director as a Proxy Server

VMware Cloud Director can act as an HTTP proxy server between tenants and the underlying vSphere environment. With dedicated vCenter Server instances, you can use VMware Cloud Director as a central point of management (CPOM) for your vSphere environment.

Dedicated vCenter Server instances in VMware Cloud Director remove the requirement for vCenter Server to be publicly accessible.

VMware Cloud Director acts as a proxy by using the HTTP CONNECT method. VMware Cloud Director supports HTTPS by default.

The following diagram illustrates the sequence of events that leads to an SSL connection between a tenant and a vCenter Server, with VMware Cloud Director acting as a proxy server.

Figure 5-2. Client Connection to vCenter Server with VMWare Cloud Director Acting as a Proxy Server
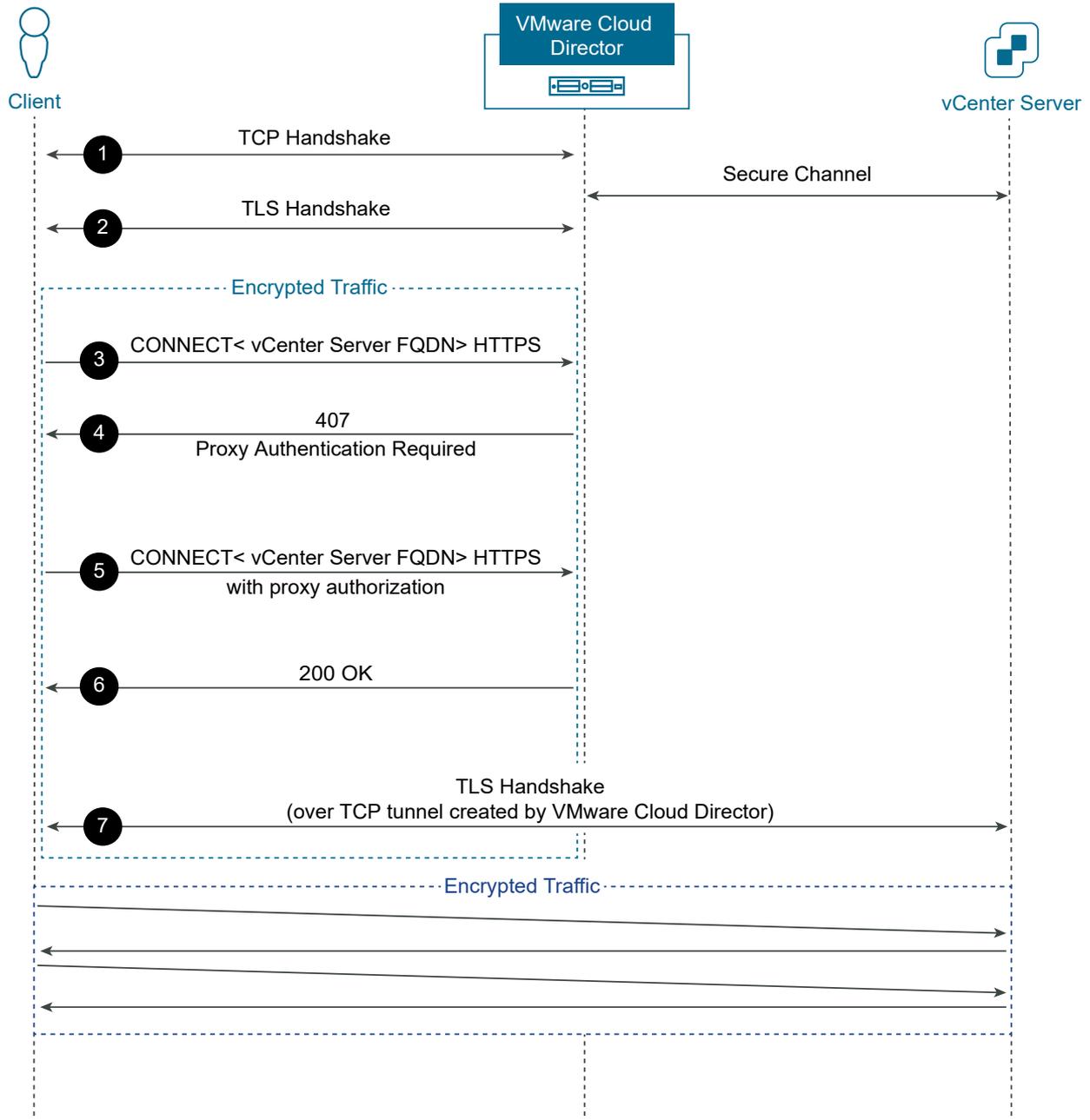
Tenants use proxy tokens to authenticate themselves when they access the underlying vSphere environment through a VMware Cloud Director instance that is acting as a proxy.

Proxy Token

A proxy token is a string generated by VMware Cloud Director that is associated with a specific user. A proxy token has a time-to-live (TTL) period. The default TTL value for a token is 30 days. When a token expires, the user with which the token is associated must delete the expired token before a new one can be generated.

HTTP Proxy

VMware Cloud Director supports proxy connections over HTTP. However, before using VMware Cloud Director for connections over HTTP, consider the security implications of such a configuration.

The following diagram illustrates the sequence of events that leads to a connection between a tenant and a vCenter Server, with VMware Cloud Director acting as an HTTP proxy server.

The credentials for vCenter Server are never exposed, because the connection between the client and vCenter Server communication is over TLS.

However, in case of a man-in-the-middle attack, a malicious actor can gain credentials for the VMware Cloud Director proxy, and the ability to sever the connection and introduce delays. Because the credentials for the proxy are a user name and a token, the attacker cannot use this connection for other goals. However, they can attempt a brute-force attack and connect to other proxied hosts that do not require TLS/SSL.

Figure 5-3. Client Connection to vCenter Server over HTTP, with VMWare Cloud Director Acting as a Proxy Server
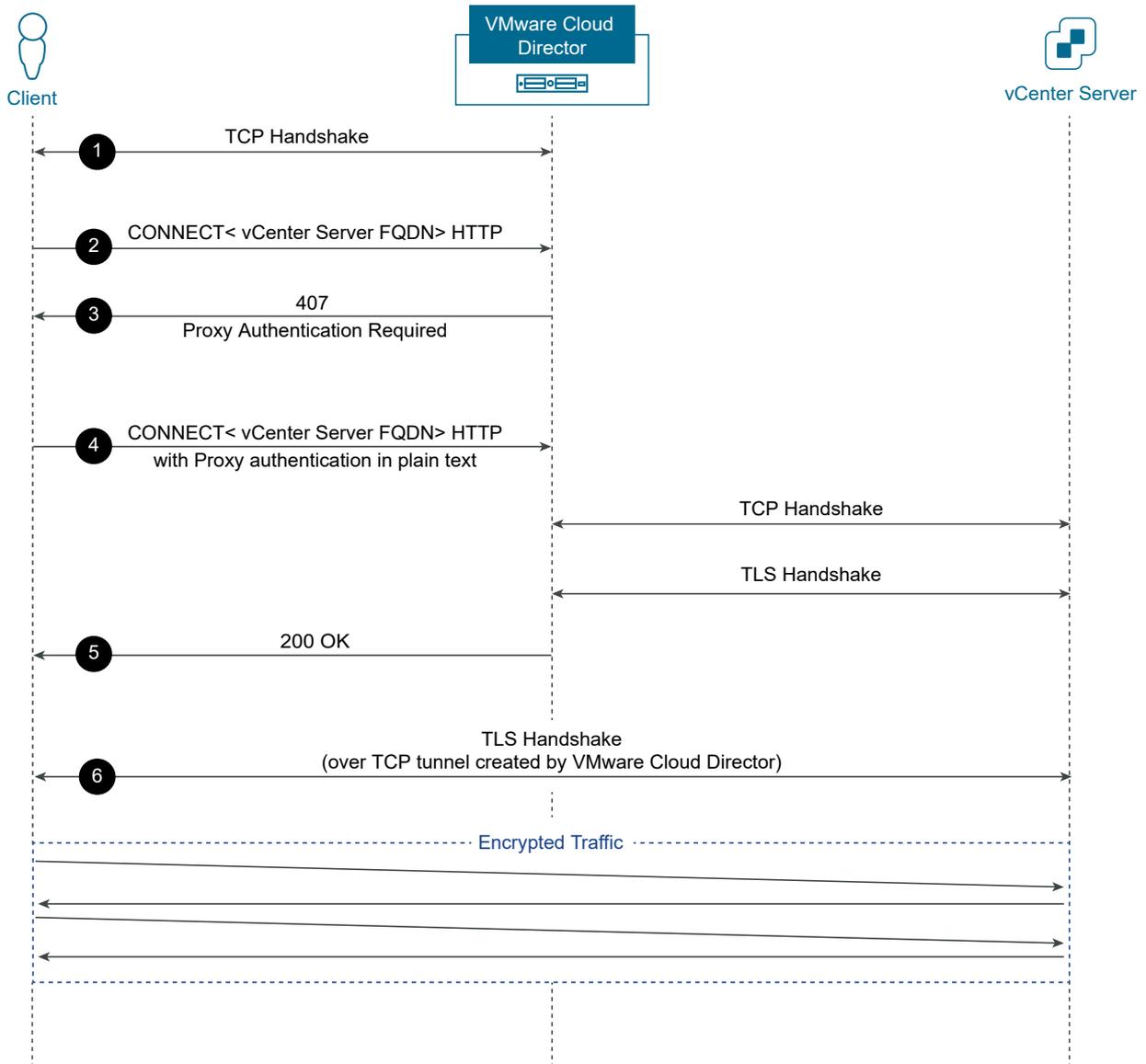
Figure 5-4. Man-in-the-middle Attack During a Client Connection to vCenter Server over HTTP, with VMWare Cloud Director Acting as a Proxy Server
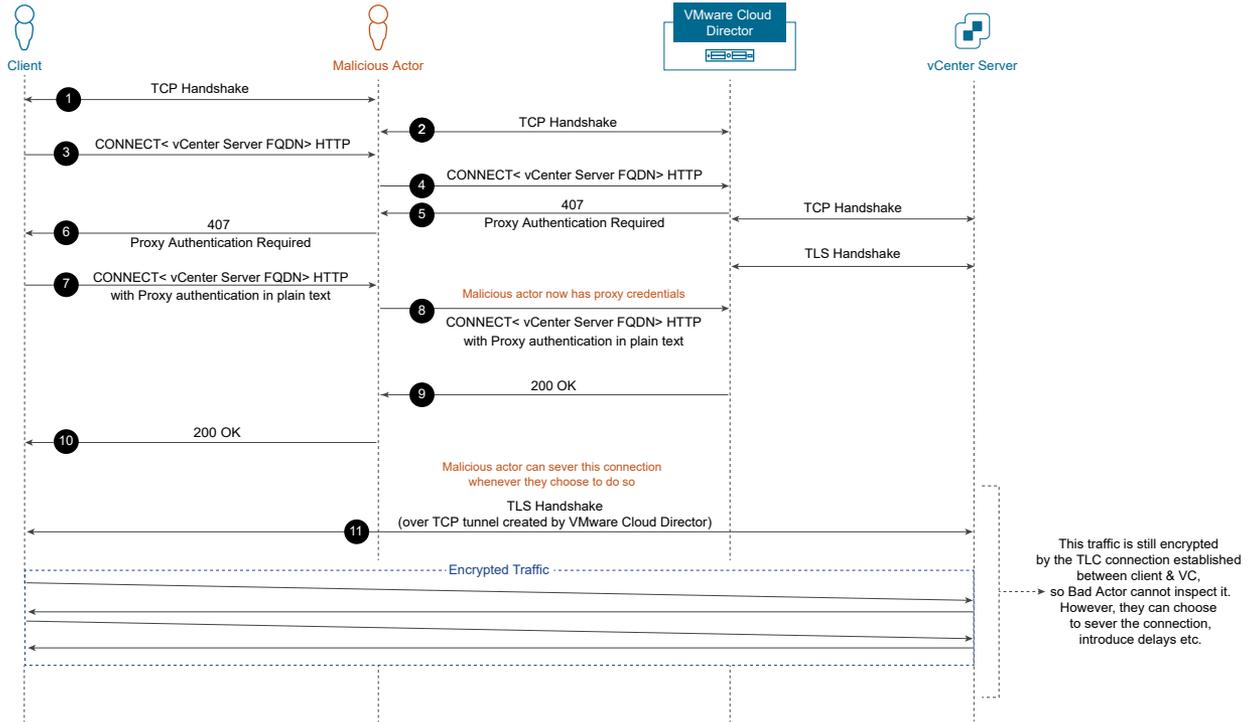
Securing MQTT

You can use an MQTT client to subscribe to messages about VMware Cloud Director events and tasks.

Starting with version 10.1, you can use the VMware Cloud Director API to subscribe to messages about VMware Cloud Director events and tasks in your organization through the MQTT protocol over HTTPS. This provides an alternative to the RabbitMQ AMQP Broker.

See Subscribe to Events and Tasks by Using an MQTT Client in *VMware Cloud Director Installation, Configuration, and Upgrade Guide* for details.

MQTT notifications are enabled by default.

You can enable or disable the MQTT notifications by setting the property `system.setting.allowMqtt` in the `/opt/vmware/vcloud-director/etc/global.properties` file to `true` or `false`.

Securing RabbitMQ AMQP

AMQP, the Advanced Message Queuing Protocol, is an open standard for message queuing that supports flexible messaging for enterprise systems. VMware Cloud Director uses the RabbitMQ AMQP broker to provide the message bus used by extension services, object extensions, and blocking task notifications.

Messages published to RabbitMQ include sensitive information. Exposing AMQP traffic between VMware Cloud Director cells can be a security threat to the system and its tenants. AMQP endpoints should be configured to use SSL.

AMQP ports should be blocked at the system firewall. Third-party clients that consume AMQP messages must be allowed to operate in the DMZ. Any code that consumes VMware Cloud Director messages should be subject to audit by the service provider's security team.

For more information about RabbitMQ and how it works with VMware Cloud Director, see vCloud Director for Service Providers (VCD-SP) and RabbitMQ Security.

Protect the AMQP Service with SSL

To use SSL with the VMware Cloud Director AMQP service, select **Use SSL** on the **AMQP Broker Settings** section of the **Extensibility** page of the VMware Cloud Director Web console, and provide either of the following:

- An SSL certificate pathname

- A JCEKS trust store pathname, user name, and password

See Configure an AMQP Broker in *VMware Cloud Director Service Provider Admin Portal Guide* for details.

Important Although an **Accept all certificates** option is available, do not select it when security is a concern. Accepting all certificates without checking them opens the way to man-in-the-middle attacks.

Block AMQP Ports at the System Firewall

As noted in Network Security Requirements, several AMQP ports must be accessible on the management network. No AMQP endpoints should be accessible from public or enterprise networks.

Securing a Cassandra Metrics Database

Cassandra is an open-source database that you can use to provide the backing store for a scalable, high-performance solution for collecting time series data, such as virtual machine metrics. Data sent to and stored in the Cassandra cluster can be sensitive and should be protected.

In addition to being placed on a dedicated management network, your Cassandra infrastructure should be secured with SSL.

Enable Cassandra Client-to-Node Encryption

See the Cassandra Client-to-node encryption page for information about installing SSL certificates and enabling encryption.

Use certificates signed by a well-known CA. When you do this, no additional configuration is required in VMware Cloud Director. If you are using self-signed certificates, you must import them manually into VMware Cloud Director. Use the `import-trusted-certificates` command of the cell management tool, as shown in Importing SSL Certificates from External Services in *VMware Cloud Director Installation, Configuration, and Upgrade Guide*.

Securing Access to JMX

Each VMware Cloud Director cell exposes MBeans through JMX to allow for operational management of the server and to provide access to internal statistics. Because this interface can expose sensitive information about the running system and impact its operation, it is imperative that access to JMX be strictly controlled.

JMX Authentication

The JMX interface is accessible only to VMware Cloud Director system administrators, who must authenticate to JMX using the same credentials they use to access VMware Cloud Director. This feature is not configurable.

Limiting Connections to JMX

Since JMX is a management interface meant only for **system administrators**, there is no reason for it to be exposed outside the management network of VMware Cloud Director. If the system has a third IP address assigned exclusively for management, bind JMX directly to this IP address. By default, the VMware Cloud Director JMX connector binds to the primary IP address specified during system configuration. You can override this default by inserting the following property in `/opt/vmware/vcloud-service-director/etc/global.properties`:

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

The most secure configuration binds the JMX connector to the localhost address:

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

Regardless of the routing and firewalling devices employed, the IP addresses assigned to this management network and the JMX port (default=8999) should not be allowed to traverse the network boundary to the Internet or to organization users.

With this setting in `global.properties`, JMX can be reached only from the local VMware Cloud Director system. External connections to the JMX port are blocked regardless of the routing configuration of the network.

Securing JMX Communications

If JMX is exposed only to the localhost address (`127.0.0.1`), then you can secure JMX communications by using SSH as a tunneling mechanism for any access to JMX.

If your management requirements do not allow the use of this configuration and JMX must be exposed outside the VMware Cloud Director cell, then JMX should be secured with HTTPS, which you can configure by setting the following environment variable:

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

You must then restart VMware Cloud Director.

JMX clients must now connect with HTTPS, but they must have access to the CA certificate. For example, for `jconsole` you should import the CA certificate to a keystore on the machine that runs `jconsole`. Then start `jconsole` with the following command-line arguments:

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

Self-signed certificates make this process unwieldy, as you need each self-signed certificate in a keystore on the machine running the JMX client. CA-signed certificates are easier to support here as only the CA certificate is required at the JMX client machine.

For information on using the JMX Service, see Access the JMX Service by Using JConsole.

Configuring the Management Network of VMware Cloud Director

The VMware Cloud Director management network is a private network that serves the cloud infrastructure and provides access for client systems used to perform administrative functions on VMware Cloud Director.

Systems that connect to the management network include the VMware Cloud Director database server, an NFS server for transfer storage, vCenter Server instances, an optional LDAPv3 directory for authenticating provider administrators, any LDAPv3 directories maintained by the provider for authenticating organization users, and NSX managers. The vCenter Server instances on this network also need access to their own Active Directory servers.

Virtual Infrastructure Management Network Configuration Requirements

It is important for the management network to be separate from the virtual machine data networks. This is even more important in a cloud environment where the provider and tenants are from separate organizations. You do not want to open the provider's management network to attack from the vApps of organizations' vApps. Similarly, the management network must be separate from the DMZ that provides access for organization administrators. Even though they may be accessing the same interfaces as provider system administrators, the DMZ concept is important in segmenting public from private traffic and providing in-depth defense.

From a physical connectivity perspective, the virtual machine data network must be separate from the management network. This is the only way to protect management systems from malicious virtual machines. Likewise, the VMware Cloud Director cells exist physically on the DMZ. In the physical deployment diagram, the servers in the management pod connect over to the cloud pods through a separate physical network, and specific firewall rules allow this traffic to pass.

The internal firewall that mediates vCenter Server and VMware Cloud Director connections to vSphere and other networks is required from a network architecture perspective. This is not a question whether different virtual machines on a single host can connect to both a DMZ and a private network. Rather, there are virtual machines in that management pod, the cloud cells, that are themselves connecting to both networks.

The design and implementation of VMware Cloud Director follows VMware's Product Security Policy and security requirements, but it is not a firewall itself and it should not mediate traffic on its own between DMZ and private management networks. This is the role of the firewall.

Other Related Networks

As shown on the physical and logical deployment diagrams, the storage networks are also physically separate. This follows vSphere best practices and protects tenant and provider storage from malicious virtual machines. The same is true of the backup network. It is technically a branch off the management network. Its specific requirements and configuration depend on the backup software and configuration in use.

vMotion is not always placed on a separate network from the management network. However, in the cloud it is important to do that from a Separation of Duties perspective. vMotion generally takes place in the clear, and if it is put on the management network, it allows a provider administrator or other user with access to that network to "sniff" on the vMotion traffic, violating organizations' privacy. For this reason, you should create a separate physical network for vMotion of cloud workloads.

Auditing and Logging

Record and monitor the activities of users is an important part of overall system security. Most organizations have rules governing who is allowed to access and make changes to software and related hardware resources. Maintaining an audit log of significant activities enables the organization to verify compliance with rules, detect any violations, and initiate remediation activities. Some businesses are

under external laws and regulations that require ongoing monitoring and verification of access and authorization rules.

An audit log can also be helpful in detecting attempts, successful or not, to gain illegitimate access to the system, probe its information, or disrupt its operation. Knowing an attack was attempted and the details of the attempt can help to mitigate the damage and to prevent future attacks.

It is part of good security practice to examine regularly logs for suspicious, unusual, or unauthorized activity. Routine log analysis also helps identify system misconfigurations and failures and ensure adherence to SLAs.

VMware Cloud Director includes two types of logs:

Diagnostic logs

> Diagnostic logs that are maintained in each cell's log directory. These logs can be useful for problem resolution but are not intended to preserve an audit trail of significant system interactions. Each VMware Cloud Director cell creates several diagnostic log files described in Viewing the VMware Cloud Director Logs in the *VMware Cloud Director Installation, Configuration, and Upgrade Guide*.

Audit logs

> Audit logs record significant actions, including login and logout. The system audit log is maintained in the VMware Cloud Director database and can be monitored through the Web UI. Each Organization administrator and the system administrator have a view into the log scoped to their specific area of control.

Use the `syslog` utility to preserve these and other VMware Cloud Director logs. In addition, you should consider use of vRealize Log Insight, which supports remote collection of other logs such as request logs, which are not based on `log4j`.

Starting with version 10.0, you can collect audit events from VMware Cloud Director by using the OpenAPI Event API at `/cloudapi/1.0.0/auditTrail`. The API only retrieves audit events that have occurred in the window defined by the configuration variable `com.vmware.vcloud.audittrail.history.days`, which is 45 days by default and has a maximum of 60 days.

Using Syslog with VMware Cloud Director

As detailed in the *VMware Cloud Director Installation, Configuration, and Upgrade Guide*, a `syslog` server can be set up during installation. Exporting logs to a `syslog` server has various advantages:

- Database logs are not retained after 90 days, while logs transmitted through `syslog` can be retained for unlimited time.

- It allows audit logs from all cells to be viewed together in a central location at the same time.

- It protects the audit logs from loss on the local system due to failure, a lack of disk space, compromise, and so on.

- It supports forensics operations in the face of problems like those listed above.

- It is the method by which many log management and Security Information and Event Management (SIEM) systems integrate with VMware Cloud Director. This allows:

    - Correlation of events and activities across VMware Cloud Director, vSphere, NSX, and even the physical hardware layers of the stack.

    - Integration of cloud security operations with the rest of the cloud provider's or enterprise's security operations, cutting across physical, virtual, and cloud infrastructures.

- Logging to a remote system other than the system the cell is deployed on inhibits tampering with the logs. A compromise of the cell does not necessarily enable access to or alteration of the audit log information.

If you did not set up a `syslog` destination for logging at initial install time, you can configure it later by going to each cell, editing the `$VCLOUD_HOME/etc/global.properties` file, and restarting the cell.

See Network Security Requirements for a list of ports that must remain open from the VMware Cloud Director host to the `syslog` server. The `syslog` server configuration details are system-specific and outside the scope of this document. To ensure that essential events are always logged, configure the `syslog` server with redundancy.

The above discussion covers only sending the audit log to a `syslog` server. Security Operations and IT Operations organizations may also benefit from the centralized aggregation and management of the diagnostic logs mentioned above. There are various methods for collecting those logs, including scheduling a job to copy them to a centralized location periodically, setting an additional logger in the `log4j.properties` file (`$VCLOUD_HOME/etc/log4j.properties`) to a central syslog server, or using a log-collection utility such as vRealize Log Insight to monitor and copy the log files to a centralized location. The configuration of these options depends on the system that you choose to use in your environment and is outside the scope of this document.

Important   Use a TLS-enabled `syslog` infrastructure. The default (UDP) `syslog` protocol does not offer in-transit encryption and transmission control/acknowledgement. The lack of encryption exposes log data to sniffing and the information present in logs might be used for further attacks. The lack of transmission control might enable an attacker to tamper with logging data. For more information, see Section 4 of RFC 5426.

Diagnostic Logging and Log Rollover

The Jetty request log file (`$VCLOUD_HOME/logs/yyyy_mm_dd.request.log`) is programmatically controlled by the Jetty (HTTP) server, but does not have a maximum size limit. For this reason, there is a risk of unbounded log file growth. A log entry is added to the current file for each HTTP request served by Jetty. To control the size of logs and the number of old log files to keep, use `logrotate` or similar methods.

The other diagnostic log files are limited to 400 MB total. Ensure that you have sufficient free disk space to accommodate those files plus the size that you allow the Jetty request logs to consume. As mentioned above, centralized logging ensures that you don't lose valuable diagnostic information as the 400 MB log file total is reached and files are rotated and deleted.

NTP and Logs

The *VMware Cloud Director Installation, Configuration, and Upgrade Guide* identifies NTP as a requirement for all VMware Cloud Director cells. A side benefit of using NTP is that log messages from all cells have synchronized timestamps. Certainly, log management tools and SIEM systems incorporate their own timestamps to help coordinate logs from multiple origins, but those timestamps are the time received by those systems, not the time the event was originally logged.

Additional Logs

Other systems connected to and used by VMware Cloud Director create audit logs that should be consolidated into your audit processes. These include logs from NSX Manager, the VMware Cloud Director database, vCenter Server, and vSphere hosts. The details of each system's log files and their purpose is beyond the scope of this document and can be found in documentation related to those products.

Tenant Security

6

The service provider, system administrators, and organization administrators are responsible for the security of each VMware Cloud Director tenant organization.

Securing a VMware Cloud Director tenant organization from external attacks is largely a matter of providing good system-level security, so that external attackers are not able to access tenant resources.

The service provider also has to be aware of the possibility that one tenant can attack, or simply interfere with, another. Potential intertenant attack vectors include snooping system-level details of compute, storage, and network resources. Interference, deliberate or not, arises when system resources are shared among tenants who may be mutually suspicious and one tenant manages to consume enough of those resources to deny other tenants their expected level of service. This situation is also known as the "noisy neighbor" problem.

As described in Chapter 3 VMware Cloud Director Architecture and Security Features , VMware Cloud Director provides transparent sharing of system resources among large numbers of tenants. In general, a service provider is free to deploy system resources in a way that maximizes system efficiency while minimizing the potential for downtime. Whenever resources are shared among tenant organizations, the service provider must consider how such sharing might affect various tenant operations, and whether it might enable intertenant attacks.

This chapter includes the following topics:

- Network Security for Tenant Organizations
- Resource Allocation and Isolation
- User Account Management

Network Security for Tenant Organizations

Although VMware Cloud Director organizations are responsible for their own network security, the service provider should protect external networks with a firewall.

Within the VMware Cloud Director system, VXLAN and VLAN networks enforce separation of packet traffic that is equivalent to using separate physical networks. They also offer a range of routing and firewalling options that give organizations fine-grained control over access to their workloads from external systems and those within the organization. These features are described in detail in the VMware Cloud Director documentation.

Usually, a service provider who has designed effective protection for the system itself, including a Web Application Firewall, SSL-terminating load balancers, and CA-signed digital certificates, does not need to take an active role in establishing or maintaining the security of organization VDC networks.

External Access to Tenant Workloads

When configuring access to organization workloads (vApps) from the Internet or an enterprise network, the service provider must consider the firewall requirements of the vSphere infrastructure deployed and used by VMware Cloud Director. Most likely, some vApps either need access to the Internet or must be accessed remotely, whether through RDP, SSH, and so on, for management, or through HTTP, or other protocols for end users of those services. For that reason, use two different virtual machine data networks, as described in the architecture diagrams in Resource Allocation and Isolation, for different uses. Each of the VM data networks requires network firewall protection.

Virtual machines that need accessibility from outside the cloud, that is, for example, from the public Internet, might be connected either to a public network or a private NAT-routed network with port forwarding configured for the exposed services. The external network to which these organization VDC networks are connected requires a protecting firewall that allows in agreed-upon traffic to this DMZ network. The service provider must ensure that not every port and protocol is allowed to initiate a connection to the external DMZ network. At the same time, enough traffic must be allowed for organizations' vApps to provide the services for which they are intended. This typically includes port 80/TCP and 443/TCP, but might include additional ports and protocols. The service provider must determine how best to strike this balance, understanding that from a security standpoint, unnecessary ports and protocols should be blocked.

In general, vApps that need accessibility to and from the Internet must be connected to a routed organization VDC network configured to allow only the required types of inbound and outbound connections. This gives the organization control over NSX firewall and port forwarding rules. Such a configuration does not eliminate the need for a network firewall to separate the external network used by these organization VDC networks. This is because public organization VDC networks do not have any VMware Cloud Director firewall protection. The separate firewall is necessary to create a DMZ. A separate NSX Edge instance can perform this function.

Similarly, a private NAT-routed organization VDC network is used for a virtual machine data network that allows virtual machines to access the Internet. As mentioned above, an NSX Edge provides the NAT and firewall capabilities for this internal virtual machine data network. Again, the external network portion of this routed network should be on the DMZ, so a separate network firewall separates the DMZ from the Internet connection itself.

Resource Allocation and Isolation

The standard service provider deployment of VMware Cloud Director envisions the sharing of vSphere resources among multiple tenant organizations.

This type of deployment provides the organizations with maximum flexibility and the provider with maximum use of the provisioned compute, network, and storage resources. Sample logical and physical deployment diagrams are below.

This subsection describes the components at a high level. Subsequent subsections describe specific recommendations regarding the resource pools, datastores, networking, and the configuration of other components.

Shared Resource Deployment

Figure 6-1. Physical Deployment Diagram and Figure 6-2. Logical Deployment Diagram are two views of the same VMware Cloud Director installation. In these figures, we use the term "pod" to denote a group of resources (physical or virtual machines) dedicated to either system management ("management pod") or tenant workloads ("cloud pod").

Figure 6-1. Physical Deployment Diagram
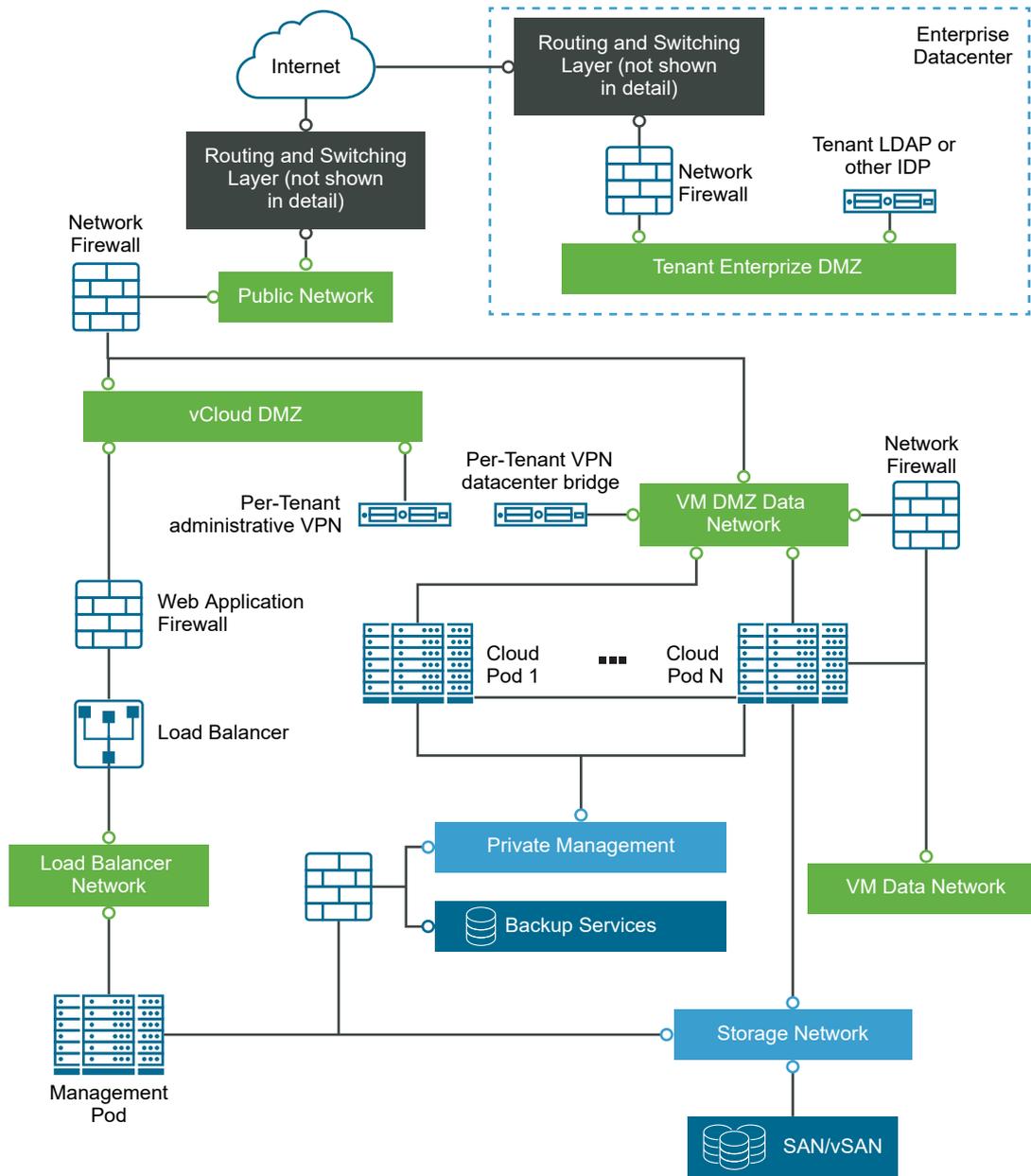
Looking at Figure 6-2. Logical Deployment Diagram, the left side shows the VMware Cloud Director cells in a load-balanced DMZ. The DMZ also contains a WAF and optionally a per-tenant administrative VPN. A service provider can configure this VPN for each organization to more strictly limit which users and IP addresses can access the services exposed through the WAF. In addition, a tenant can configure a VPN to connect their on-premises workloads and data with VMs in the cloud. Configuration of such VPNs is outside the scope of this document.

Figure 6-2. Logical Deployment Diagram
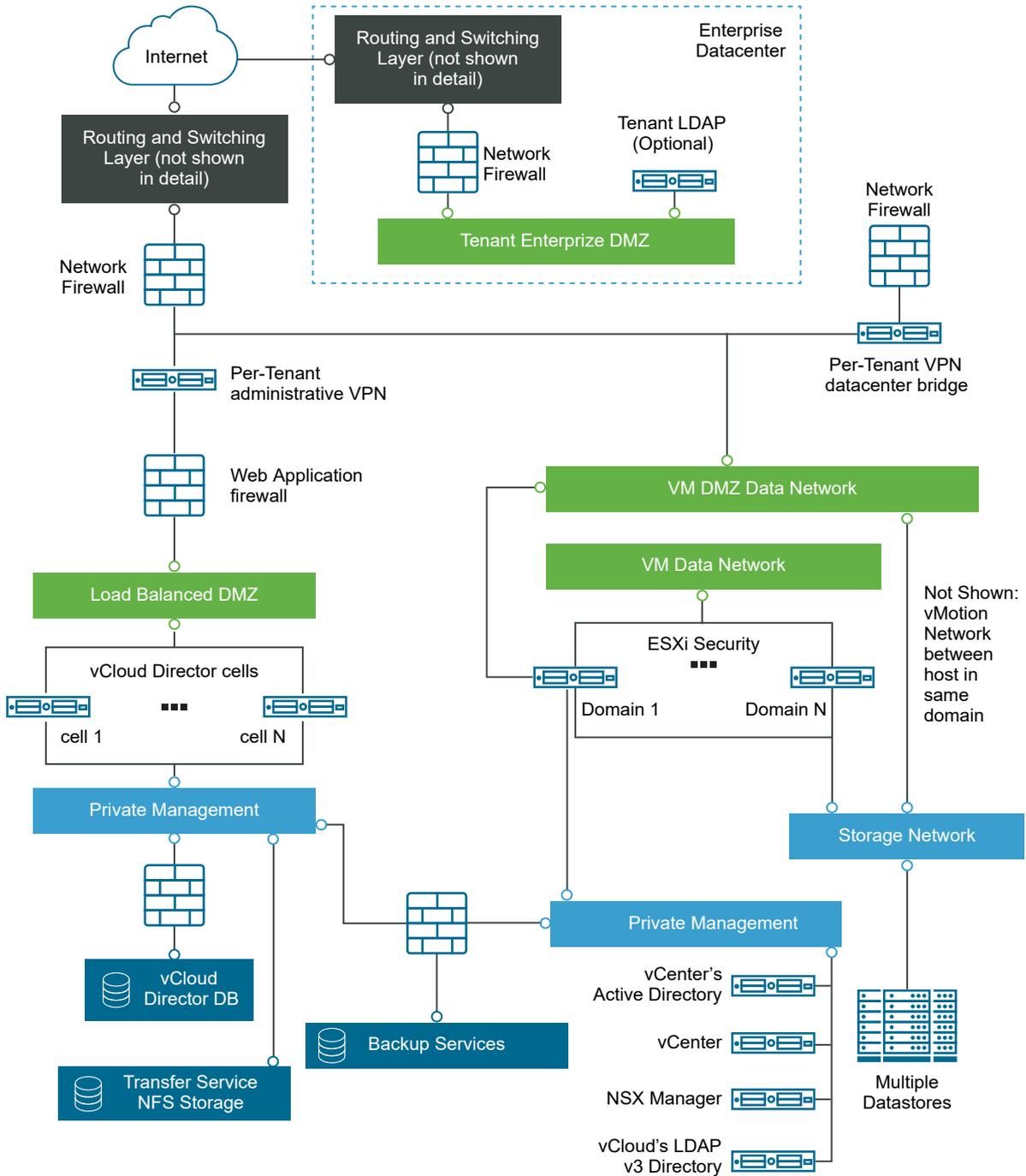
Behind the cells are the private management elements required by VMware Cloud Director, including vCenter, NSX, the VMware Cloud Director database, and so on. Their connections are strictly controlled by the firewalls in the diagram, as those services should not be accessible from other machines on the DMZ or directly from the Internet.

Figure Figure 6-3. Management Pod Networks focuses only on the management pod. It shows that there is a need for at least two separate physical networks connected to that pod. This includes the load-balanced DMZ network, the Private Management network, and an optional dedicated Storage Network, with a provider-specific configuration.

Figure 6-3. Management Pod Networks
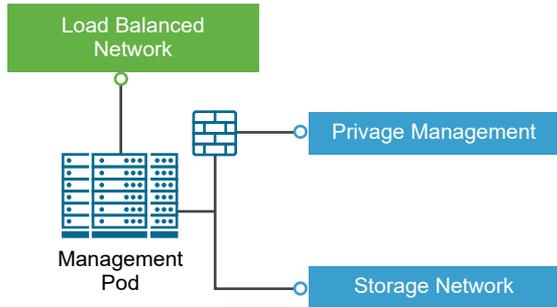
With respect to the vSphere hosts, grouped into different security domains, they each have external networks exposed as a virtual machine DMZ data network for use as public organization VDC networks, as well as virtual machine data networks for private organization VDC networks that might be routed to an external network.

Figure Figure 6-4. Cloud Pod Networks focuses on the Cloud Pods. It shows four physical networks. The Storage Network is specific to the particular hardware and storage technologies chosen. If resource pools do not span clusters, you might not need to provide a physical VM data network. If resource pools span clusters, use a separate physical network for vMotion traffic.

Figure 6-4. Cloud Pod Networks
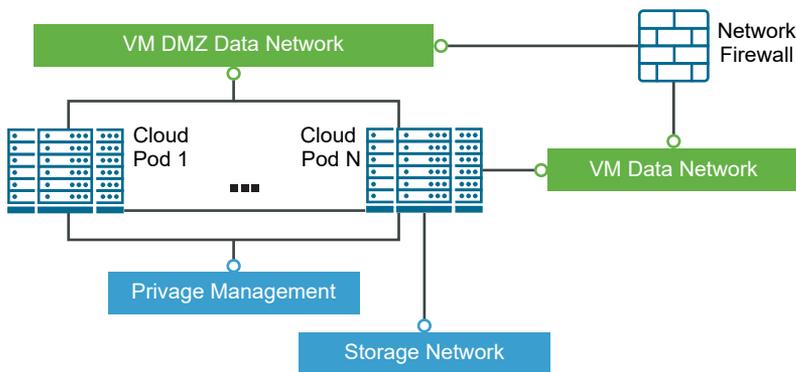
It is also assumed that typical data center security technologies, such as IDS/IPS, SIEM, configuration management, patch management, vulnerability management, anti-virus, and GRC management systems, is applied to both the VMware Cloud Director, its associated systems, vSphere and its associated systems, and the networks and storage infrastructure that support them. Details on these systems are also outside the scope of this document.

Resource Sharing and Isolation Recommendations

Under normal conditions, a service provider can share compute, storage, and networking resources among multiple tenant organizations. The system enforces isolation through abstraction, secure engineering practices in the hypervisor and the VMware Cloud Director software stack.

Tenant organizations share the underlying resource pools, datastores, and external networks exposed through a single provider virtual data center (VDC) without affecting and being aware of resources that they do not own. Proper management of vApp storage and runtime leases, vApp quotas, limits on resource-intensive operations, and organization VDC allocation models can ensure that one tenant cannot deny service to another by accident or on purpose.

For example, a conservative configuration might set up all organization VDCs under the reservation pool allocation model and never overcommit resources. The full range of options is not covered in this document.

Security Domains and Provider VDCs

Despite the proper isolation in the software and proper organization configuration, there might be times when tenant organizations do not want different workloads to be run or stored on particular compute, network, or storage resources. This does not elevate the system overall to a "high-security environment". However, it creates the need to segment the cloud into multiple security domains. Specific examples of workloads requiring such treatment include:

- Data that is subject to privacy laws which require it to be stored and processed within prescribed geographies.

- Data and resources owned by countries or organizations that, despite trusting the isolation of the cloud, require as a matter of prudence and in-depth defense that their VDCs cannot share resources with specific other tenants - for example, a competing company.

In these and other scenarios, resource pools, networks, and datastores should be segmented into different "security domains" by using different provider VDCs whereby vApps with similar concerns can be grouped (or isolated). For example, you might identify certain provider VDCs as storing and processing data in certain countries.

Resource Pools

Within a single provider VDC, you can have multiple resource pools that aggregate CPU and memory resources provided by the underlying vSphere infrastructure. Segmenting different organizations across different resource pools is not necessary from a confidentiality and integrity perspective. But from an availability perspective, there might be reasons to do that. This resource-management problem depends on organization VDC allocation models, the expected workloads, quotas and limits applied to these organizations, and the speed with which the provider can deploy additional computing resources. This guide does not define the different resource allocation models and how they impact each organization's use of a resource pool other than to say that whenever you allow the overcommitment of resources in a

pool used by more than one organization, you run the risk of causing service quality to degrade for one or more organizations. Proper monitoring of service levels is imperative to avoid an organization causing Denial of Service. However, security does not dictate a specific separation of organizations to achieve this goal.

Limiting Shared Consumption of Shared Resources

In the default configuration, all tenants can consume many VMware Cloud Director compute and storage resources in unlimited quantities. The system provides several ways for a system administrator to manage and monitor the consumption of these resources. Careful examination of the following areas is an important part of limiting the opportunity for a "noisy neighbor" to affect the level of service VMware Cloud Director provides.

Limit resource-intensive operations

See Configure System Limits in the *VMware Cloud Director Administrator's Guide*.

Impose sensible quotas

See Configure Organization Lease, Quota, and Limit Settings and (to limit the number of VDCs a tenant can create and limit the number of simultaneous connections per VM) Configure System Limits, both in the *VMware Cloud Director Administrator's Guide*.

Manage storage and runtime leases

Leases provide a level of control over tenant consumption of storage and compute resources. Limiting the length of time that a vApp can remain powered-on or that a powered-off vApp can consume storage is an essential step in managing shared resources. See Understanding Leases in the *VMware Cloud Director Tenant Portal Guide*.

External Networks

A service provider creates external networks and makes them accessible to tenants. An external network can be safely shared between multiple public networks. Tenants should be reminded that traffic on external networks is subject to interception, and they should employ application-level or transport-level security on these networks for confidentiality and integrity when necessary.

Private routed networks can share those external networks in the same circumstances - when they are used for connecting to a public network. Sometimes, an external network may be used by an organization VDC network to connect two different vApps and their networks or to connect a vApp network back to the enterprise data center. In these cases, the external network should not be shared between organizations.

Instead of using a separate physical network for each organization, the service provider can connect a shared physical network to a single external network that is clearly identified as a DMZ network. As a result, organizations know that it doesn't provide confidentiality protections.

For communications that traverse an external network but that require confidentiality protections, for instance, a vApp-to-enterprise data center connection or a vApp-to-vApp bridge over a public network, a VPN can be deployed. The reason for this is that in order for a vApp on a private routed network to be reachable, it must leverage IP address forwarding using an IP address routable on that external network.

Any other vApp that connects to that physical network can send packets to that vApp, even if it is another organization connected to another external network. To prevent this, a service provider can use NSX Distributed Firewall and Distributed Logical Routing to enforce separation of traffic form multiple tenants on a single External Network. See NSX Distributed Firewall and Logical Routing in the *VMware vCloud® Architecture Toolkit™ for Service Providers*

Note   Starting with version 10.1, VMware Cloud Director supports policy-based IPSec VPN for NSX-T Data Center edge gateways. To configure them, tenants provide a pre-shared key that is used on both ends of the VPN tunnel. This pre-shared key is visible to the service provider.

Organization VDC networks owned by different tenants can share an external network as an uplink from an edge gateway if they do not allow access to the inside with NAT and IP masquerading.

Important   VMware Cloud Director Advanced Networking allows tenants and service providers to employ dynamic routing protocols such as OSPF. The OSPF autodiscovery mechanism, when used without authentication, can establish peering relationships between edge gateways belonging to different tenants and start exchanging routes. To prevent this, do not enable OSPF on public shared interfaces unless you also enable OSPF authentication to prevent peering with unauthenticated edge gateways.

Network Pools

Each organization VDC in VMware Cloud Director can have one network pool. Multiple organization VDCs can share a network pool.

VXLAN-backed network pools rely on the physical and virtual switches being configured to allow connectivity within a VXLAN and isolation between different VXLANs. Network pools backed by vSphere port groups must be configured with port groups that are isolated from each other. These port groups can be isolated physically, through VXLANs.

VXLAN pools support many more networks than VLAN- or port group-backed network pools, and isolation is enforced at the vSphere-kernel layer.

While the physical switches don't isolate the traffic without the use of the VXLAN, VXLAN isn't susceptible to misconfiguration at the hardware layer either. Recall from above that none of the networks in any network pool provide confidentiality protection for intercepted packets.

With version 10.0, VMware Cloud Director introduces Geneve network pools. Every provider VDC that is backed by NSX-T Data Center includes a Geneve network pool. Geneve networks provide a number of benefits, including logical networks spanning layer 3 boundaries and logical networks spanning multiple racks on a single layer 2.

Storage Policies

VMware Cloud Director storage policies aggregate datastores in a way that enables the service provider to offer storage capabilities tiered by capacity, performance, and other attributes.

Starting with VMware Cloud Director 10.1, you can enablevSphere VM encryption on a storage policy. For more information, see Enabling VM Encryption on Storage Policies of a Provider Virtual Data Center.

Individual datastores are not accessible to tenant organizations. Instead, a tenant can choose from a set of storage policies offered by the service provider. If the underlying datastores are configured to be accessible only from the vSphere management network, then the risk in sharing datastores is limited, as with compute resources, to availability. One organization might end up using more storage than expected, limiting the amount of storage available to other organizations. This is especially true with organizations using the Pay-As-You-Go allocation model and the default "unlimited storage" setting. For this reason, if you share datastores, you should set a storage limit, enable thin provisioning if possible, and monitor storage usage carefully. You should also carefully manage your storage leases, as noted in Limiting Shared Consumption of Shared Resources. Alternatively, if you do not share datastores, you must properly dedicate storage to the storage policies you make available to each organization, potentially wasting storage by allocating it to organizations that do not need it.

vSphere datastore objects are the logical volumes where VMDKs are stored. While vSphere administrators can see the physical storage systems from which these datastores are created, this operation requires rights not available to VMware Cloud Director administrator or tenant. Tenant users who create and upload vApps simply store the vApps' VMDKs on one of the storage policies available in the organization VDC they're using.

For this reason, virtual machines never see any storage outside of that consumed by their VMDKs unless they have network connectivity to those storage systems. A provider can provide access to external storage for vApps as a network service, but it must be separate from the LUNs assigned to the vSphere hosts backing the cloud.

Likewise, tenant organizations see only the storage policies available in their organization VDCs, and even that view is limited to the VMware Cloud Director abstraction. They cannot browse the system's datastores. They see only what is published in catalogs or used by the vApps they manage. If organization VDC storage profiles do not share datastores, the organizations cannot impact each other's storage (except perhaps by using too much network bandwidth for storage I/O). Even if they do, the above restrictions and abstractions ensure proper isolation between the organizations. VMware Cloud Director administrators can enable vSphere storage I/O control on specific datastores to restrict the ability of a tenant to consume an inordinate amount of storage I/O bandwidth. See Configure Storage I/O Control Support in a Provider VDC in the *VMware Cloud Director Administrator's Guide*.

User Account Management

The management of users and their credentials is important to the security of any system. Because all authentication to and within the VMware Cloud Director system is by user name and password, it is critical to follow best practices for managing users and their passwords.

This topic aims to define the capabilities and limitations of managing users and passwords in VMware Cloud Director and provides recommendations on how to manage them securely and use them given those constraints.

Limitations of Local User Accounts

VMware Cloud Director provides a self-contained identity provider (IDP) for user accounts, which are created and maintained in the VMware Cloud Director database. While not inherently vulnerable in a system configured with limited network access to the database (see Configuring the Management Network of VMware Cloud Director), these accounts do not provide the kinds of password management features demanded by certain industries, such as the PCI Data Security Standard. To discourage brute-force attacks, local accounts should be subject to password retry limits and account lockout rules.

Service providers must carefully weigh the benefits and risks of continuing to use local accounts for system administrators, and carefully control which source IP addresses can authenticate to an organization's cloud URL if local system administrator accounts are configured. Consider eliminating or at least limiting the use of this identity provider for system administrator accounts.

A new installation of VMware Cloud Director creates a local system administrator account. In the default configuration, VMware Cloud Director requires at least one system administrator account to remain local. A service provider who has enabled the System organization to use the vSphere SSO service - a SAML IDP, or LDAP, can configure VMware Cloud Director to operate with no local system administrator accounts by taking the following steps:

1   Create one or more accounts for your system administrators in the vSphere SSO service or LDAP.

2   Import those accounts account into the System organization.

3   Run the cell management tool `manage-config` command to reconfigure the system so that no local system administrator accounts are required and no system administrator with a local account can authenticate to the system.

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

This does not disable local accounts for other organizations.

Note   In a system that has no local system administrator accounts, cell management tool commands that require you to specify system administrator credentials must use the $-i$ $--pid$ option instead, supplying the cell's process ID in *pid*. See the Cell Management Tool Reference in the *VMware Cloud Director Installation, Configuration, and Upgrade Guide*.

4   You can undo this change with a similar cell management tool command line, which re-enables access for system administrators who have local accounts.

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

Password Management

Most LDAP, OAuth, and SAML IDPs provide capabilities or integrate with systems to handle the situation where a user has forgotten their password. These capabilities are outside the scope of this document. The VMware Cloud Director cell management tool includes a `recover-password` command that can be used to recover a lost system administrator password. There is no capability native to VMware Cloud Director to handle this situation for other local users. Consider storing all local account passwords in a manner approved by your IT security department, such as, for example, locking passwords in a vault, or using password storage applications.

Password Strength

The strength of IDP users' passwords depends on the controls provided by that IDP and the tools that used to manage users within the directory. For example, if connecting VMware Cloud Director to Active Directory, the typical Active Directory password length, complexity, and history controls associated with Active Directory are enforced by the directory itself. Other IDPs tend to support similar capabilities. The details of password strength controls are directory-specific.

VMware Cloud Director requires local users to have passwords of at least six characters in length. That requirement is not configurable, and no other password complexity or history controls are available. Any users, especially system and organization administrators, must take great care in choosing their passwords to protect against brute force attacks.

User Password Protection

The credentials of users managed by an IDP are never stored in the VMware Cloud Director database. They are transmitted using the method chosen by the IDP. See Configuring Identity Providers for more information about securing this information channel.

Local users' passwords are salted and hashed before storage in the VMware Cloud Director database. The plain text password cannot be recovered from the database. Local users are authenticated by hashing the presented password and comparing it to the contents of their password field in the database.

Other Passwords

In addition to credentials for local users, the VMware Cloud Director database stores passwords for connected vCenter Server instances and NSX managers. Changes to those passwords are not automatically updated in the system. You must change them manually using the VMware Cloud Director configuration script for the VMware Cloud Director database password or the Web UI for the vCenter Server and NSX passwords.

VMware Cloud Director also maintains passwords for accessing the private keys associated with its TLS/SSL certificates and the passwords to the VMware Cloud Director database, vCenter Server instances, and NSX manager servers, as mentioned above. These passwords are encrypted using a unique key per VMware Cloud Director installation and stored in the `$VCLOUD_HOME/etc/global.properties` or the `responses.properties` file. As mentioned in Protecting Sensitive Files After Installation, you must carefully protect any backups that contain these files.

Role-Based Access Control

VMware Cloud Director implements a role-based authorization model. This section discusses the different identity sources, user types, authentication controls, roles, and rights present in VMware Cloud Director. Understanding this information helps to secure the system and to provide the correct access to the right people.

A VMware Cloud Director tenant organization can contain an arbitrary number of users and groups. An **Organization Administrator** can create users locally or import them from an external directory service (LDAP) or identity provider (OAuth, SAML). Imported users can be members of one or more groups. A user that is a member of multiple groups gets assigned all the roles assigned to those groups. Each organization is created with a default set of rights and a set of predefined roles that include combinations of those rights. A **System Administrator** can grant additional rights to an organization, and organization administrators can use those rights to create custom roles that are local to the organization. Permissions within an organization are controlled through the assignment of rights and roles to users and groups.

No unauthenticated user is allowed to access any VMware Cloud Director functionality through the Web console, Tenant Portal, or VMware Cloud Director API. Each user authenticates using a user name and password. You can configure password retry and account lockout policies globally and per organization.

Roles are groupings of rights that provide capabilities for the user that is assigned that role. Predefined roles include:

- **System Administrator**

- **Organization Administrator**

- **Catalog Author**

- **vApp Author**

- **vApp User**

- **Console Access Only**

The *VMware Cloud Director Service Provider Admin Portal Guide* also identifies which rights are assigned to each of these roles. The purpose of that section is to help you choose the appropriate role for each type of user. For example, the **vApp User** role might be appropriate for an administrator that must power on and off virtual machines, but if they also must edit the amount of memory assigned to a virtual machine, then **vApp Author** might be a more appropriate role. These roles might not have the exact sets of rights relevant to your tenants' organizations, so **Organization Administrators** can create custom roles. A description of what specific rights can be combined to create a useful custom role is outside the scope of this document.

Configuring Identity Providers

A VMware Cloud Director tenant organization can define an identity provider that it shares with other applications or enterprises. Users authenticate to the identity provider to obtain a token that they can then use to log in to the organization. Such a strategy can enable an enterprise to provide access to multiple, unrelated services, including VMware Cloud Director, with a single set of credentials, an arrangement often calles single sign-on (SSO).

About Identity Providers

VMware Cloud Director supports the following kinds of identity providers:

OAuth

An organization can define an external identity provider that supports OAuth authentication, as defined in RFC 6749 (http://tools.ietf.org/html/rfc6749).

SAML

An organization can define an external identity provider that supports the Security Assertion Markup Language (SAML) 2.0 standard.

Integrated

The integrated identity provider is a VMware Cloud Director service that authenticates users who are created locally or imported from LDAP.

OAuth

In any OAuth implementation, most of the security decisions happen at the OAuth authorization server layer. VMware Cloud Director is in the role of a resource server, which is a consumer of the token, and is responsible only for verifying the integrity of the token.

To protect your VMware Cloud Director sessions and the underlying sensitive assets, the OAuth authorization server must be set up securely and have its latest security patches installed.

If the OAuth authorization server can be set to redirect users to an arbitrary URL specified by a query parameter, the OAuth authorization server must be set up to validate URLs to prevent an attacker from controlling redirects to third-party applications. A white list of legitimate applications must be used for validation when available.

LDAP

The VMware Cloud Director integrated identity provider supports several popular LDAP services.

See the *VMware Cloud Director Release Notes* for a list of supported LDAP services.

The **system administrator** can define a systemwide LDAP service that all tenants use. Tenant user accounts are imported into the VMware Cloud Director database where VMware Cloud Director roles are assigned. LDAP user passwords are managed and maintained in the LDAP directory, and authentication occurs against that directory using the settings specified in the LDAP configuration screen. All LDAP directory's controls around authentication and passwords are preserved, including authentication failure lockouts, password expiration, history, complexity, and so on, and are specific to the LDAP service chosen. If an organization is configured to use the system LDAP, its users come from the organizational unit (OU) that is configured in that organization's VMware Cloud Director System LDAP Service settings.

Cloud providers might choose to allow tenant organizations to use an OU within the system LDAP or to host their own LDAP directory service. In either case, appropriate management access to that directory must be provided for the organization administrator to manage users. The lack of such control might provide an extra burden on the system administrator and hinder the organization from easily and properly controlling access to VDCs. In the absence of such management controls, an organization should only use a private LDAP directory that they themselves host and manage.

Connectivity from VMware Cloud Director cells to the system LDAP server and any organization LDAP servers must be enabled for the software to authenticate users. The system LDAP server must be on the private management network, separated from the DMZ by a firewall. Some cloud providers and most IT organizations run any organization LDAP servers required, and those too are on a private network, not the DMZ. Another option for an organization LDAP server is to have it hosted and managed outside of the cloud provider's environment and under the control of the organization. In that case, it must be exposed to the VMware Cloud Director cells, potentially through the enterprise data center's own DMZ.

In these circumstances, opening the appropriate ports through the various firewalls in the path between the cells and the LDAP server, as described in LDAP over TLS/SSL, is required. Also, a concern that arises when the organization is hosting their own LDAP server is exposing it through their DMZ. It is not a service that must be accessible to the general public, so steps should be taken to limit access only to the VMware Cloud Director cells. One simple way to do that is to configure the LDAP server and the external firewall to allow access only from IP addresses that belong to the VMware Cloud Director cells as reported by the cloud provider. Other options include systems such as per-organization site-to-site VPNs connecting those two sets of systems, hardened LDAP proxies or virtual directories, or other options, all outside the scope of this document.

Conversely, cloud providers should be aware that organization-hosted LDAP servers managed by unscrupulous customers might be used as part of an attack against other organizations. For example, one might conceive of an organization requesting an organization name that is a common misspelling of another organization's name and using the similar-looking login URL in a phishing attack. The provider can take steps to protect against this and similar intertenant attacks by limiting the source IP addresses of requests when possible to avoid inter-organization login attempts and by ensuring that organization names are never too similar to one another.

LDAP over TLS/SSL

Configure a LDAPv3 directory for user authentication. VMware Cloud Director must be configured to connect to LDAP servers over SSL to properly protect the passwords being validated against those servers. For details, see Manage LDAP Connections in the *VMware Cloud Director Service Provider Admin Portal Guide*. The most secure LDAP configuration specifies **Use SSL** and requires an SSL certificate provided by the LDAP service.

If the signed certificate of the LDAP server is not available, then the certificate of the CA that signs the LDAP server certificate must be imported into the system or organization JCE Key Store (JCEKS). LDAP configurations that specify a JCEKS Key Store are also secure, but can be subject to misconfiguration when lots of CA certificates, or even many specific server certificates, are trusted. In addition, it is preferable to choose an LDAP provider that supports Kerberos authentication.

Connectivity to the LDAP server is required. While plain (non-SSL) LDAP runs over port 389/TCP, servers that support LDAP over SSL use port 636/TCP by default. However, this port is also configurable.

Note   VMware Cloud Director supports the legacy LDAP over SSL (LDAPS) approach and does not support negotiating TLS within an LDAP connection using the StartTLS command.

Finally, the LDAP-enabled directory server must be properly configured with an SSL certificate. How that is done is beyond the scope of this document.

Importing Groups

The purpose of importing groups into VMware Cloud Director is to allow you to avoid manually importing individual users all with the same role. When LDAP users log in, their session gets assigned the roles that are mapped to the groups of which they are members. As users' group memberships change based on changes to their duties within their organizations, the roles assigned to those users change automatically based on the group to role mapping. This allows organizations to integrate cloud roles with internal organization groups/roles and the systems that provision and manage them.

As an example, an organization might decide to initially grant LDAP users the "Console Access Only" role to limit users' rights. To do so, all users that need this basic role are added to a single LDAP group, and when that group is imported, the **organization administrator** assigns it the **Console Access Only** role. Then, those users with additional job duties are added to other LDAP groups, also imported to VMware Cloud Director and assigned to these more privileged roles. For instance, users that need to create catalogs can be added to the "Org A Catalog Author" group in the organization's LDAP server. Then the **organization administrator** for Org A can import the "Org A Catalog Author" group and map it to the predefined Catalog Author role in VMware Cloud Director. See Import a Group in the *VMware Cloud Director Tenant Portal Guide*.

Checklist

<div style="text-align: right">7</div>

This checklist summarizes the key security configuration tasks described in this document.

- Log out of the VMware Cloud Director Service Provider Admin Portal or VMware Cloud Director Tenant Portal when you are not using the user interface. The inactivity timeout that ends your session automatically only functions when you have closed the browser window or tab with the VMware Cloud Director UI.

- In addition to the guidance in this document, you must monitor the security advisories at http://www.vmware.com/security/advisories/ and sign up for email alerts using the form on that page. Additional security guidance and late-breaking advisories for VMware Cloud Director are available there.

- Administrators should apply the steps described in *vSphere Security*, *Securing VMware NSX for vSphere* (https://communities.vmware.com/docs/DOC-27674), and *NSX Security Configuration Guide* (https://communities.vmware.com/docs/DOC-37726) to ensure that they have secure installations of those products.

- If you are using the VMware Cloud Director appliance, you must apply security patches by upgrading to the latest appliance builds.

- Apply current security patches to the cell Linux platform, VMware Cloud Director database, and virtual infrastructure before installation of VMware Cloud Director on Linux. Ongoing monitoring to keep these components at a current patch level is also crucial.

- If you are using VMware Cloud Director for Linux, apply standard security hardening procedures to the cell Linux platform, including disabling unnecessary network services, removing unnecessary packages, restricting remote root access, and enforcing strong password policies. If possible, use a centralized authentication service such as Kerberos. Consider installing monitoring and intrusion-detection tools.

  Note   The VMware Cloud Director appliance only supports the installation of VMware products.

- It is possible to install additional applications and provision additional users on the cell Linux platform. However, avoid doing this, because widening access to the cell OS might decrease security.

- Make the `responses.properties` file available only to those users that need it. When you use the file while adding cells to a server group, place appropriate access controls on the location accessible

to all target hosts. Carefully control and, if possible, encrypt any backups. For VMware Cloud Director on Linux, once the software is installed on all server hosts, delete any copies of the `responses.properties` file in these accessible locations. Do not delete the `responses.properties` file of the VMware Cloud Director appliance.

■ The `responses.properties` and `global.properties` files are protected by access controls on the `$VCLOUD_ HOME/etc folder` and the files themselves. Do not change the permissions on the files or folder.

■ Strictly limit physical and logical access to the VMware Cloud Director servers to those users that need to log in and only with the minimal levels of access required. This involves limiting the use of the root account through `sudo` and other best practices. Protect and encrypt any backups of the servers, with the keys managed separately from the backups themselves.

■ For database security requirements for VMware Cloud Director on Linux, refer to the PostgreSQL documentation.

■ Do not provide the VMware Cloud Director database with user privileges over other databases on that server or other system administration privileges.

■ Ensure that any credentials used for administrative access to the cell, the connected vCenter Server instances, the VMware Cloud Director database, to firewalls and other devices follow standards for password complexity.

■ It is important from a defense perspective to vary the administrative passwords for the different servers in the VMware Cloud Director environment, including the cells, the VMware Cloud Director database, vCenter Server instances, and NSX.

> **Note**   Upon deployment of a VMware Cloud Director appliance, the root password should be the same across all cells. You can change it after the initial deployment.

■ See vSphere Security Certificates for information about creating and replacing certificates used by vCenter Server and ESXi.

■ Ensure that vCenter Server certificates have a common name (CN) field that matches the FQDN of the server on which vCenter Server is installed.

■ Configure VMware Cloud Director to check vCenter Server certificates.

■ Ensure that vCenter Server certificates are signed by a CA and have a CN matching the FQDN of the host on which the cell is installed.

■ To make VMware Cloud Director services available to the outside, place the cells in a DMZ, with a network firewall separating the Internet from VMware Cloud Director cells on the DMZ. The only port that must be allowed through the Internet-facing firewall is 443/TCP.

■ As the VMware Cloud Director cells are in the DMZ, ensure their access to the services they need is mediated by a network firewall. Specifically, access to the VMware Cloud Director database, vCenter Server, vSphere hosts, IDPs, including LDAP, the shared transfer server storage, and any backup or similar services must be on the other side of a firewall that separates the DMZ from the internal network.

- Ensure that virtual machines that require access from outside the cloud, such as, for example, from the Internet, are connected either to a public network or to a private NAT-routed network with port forwarding configured for the exposed services. The external network to which these organization VDC networks are connected requires a firewall that allows in agreed-upon traffic to this DMZ network.

- In general, vApps that need accessibility from the Internet be placed on a private, routed network. This provides the tenant control over firewall and port forwarding rules provided by NSX. These and other rules might be applied by default by the network firewall you choose to deploy. See your firewall's documentation for specific configuration instructions and default capabilities.

- A defense-in-depth doctrine requires that JMX (port 8999/TCP) and JMS (ports 61611/TCP and 61616/TCP) be blocked at the network firewall that protects the DMZ to which the cells are connected.

- Set the public Web URL, public console Proxy Address, and public REST API base URL for a multicell cloud behind a Web Application Firewall (WAF) or load balancer.

- Deploy a Web Application Firewall (WAF) in front of the VMware Cloud Director cells.

- In such deployments, ensure that the WAF is configured to allow inspection and proper blocking of malicious traffic. This is typically done with TLS or SSL termination.

- When configuring TLS or SSL termination, it is important not only to install a CA-signed certificate at the Web Application Firewall (WAF) so that client applications of the vCloud API and the Web console can be assured of the identity of the server, but also to use a CA-signed certificate on the cells even though they are only seen by the WAF.

- Finally, if the load balancer is independent of the WAF, it too should use a CA-signed certificate.

- If possible, enable generation of the `X-Forwarded-For` header at the firewall.

- If the VMware Cloud Director server that is installed on Linux has a third IP address assigned exclusively for management, bind JMX directly to this IP address. By default, the VMware Cloud Director JMX connector binds to the primary IP addresses specified during configuration. This default can be overridden by inserting the following property in `/opt/vmware/vcloud-service-director/etc/global.properties`: `vcloud.cell.ip.management=`*IP or hostname for the management network to which the JMX connector should bind*.

- A more secure configuration involves binding the JMX connector to the local host address: `vcloud.cell.ip.management=127.0.0.1`. If JMX is only exposed to local host, secure JMX communications by using SSH as a tunneling mechanism for any access to JMX. If your management requirements do not allow the use this sort of local host configuration and JMX must be exposed outside the VMware Cloud Director server, secure JMX with TLS or SSL.

- Behind the cells are the private management elements required by VMware Cloud Director: its database, NSX, vCenter Server, the system LDAP server, if any, the Active Directory server used by vCenter Server, the shared transfer server storage, and the management interfaces of the vSphere hosts. Ensure that their connections are strictly controlled by firewalls and that these services are not accessible from other machines on the DMZ or directly from the Internet.

- It is also assumed that typical data center security technologies, such as IDS/IPS, SIEM, configuration management, patch management, vulnerability management, antivirus, and GRC management systems, are applied to VMware Cloud Director, its associated systems, vSphere and its associated systems, and the networks and storage infrastructure that support them. VMware Cloud Director does not support the installation of software on the VMware Cloud Director appliance. To get system updates and patches, update the appliance to the latest available version.

- To guarantee that one tenant organization cannot deny service to another by accident or on purpose, ensure proper management of leases, quotas, limits, and allocation models .

- In these and other scenarios, ensure that resource pools, networks, and datastores are segmented into different security domains by using different provider VDCs whereby vApps with similar concerns can be grouped or isolated.

- Whenever you allow the overcommitment of resources in a pool used by more than one tenant organization, you run the risk of causing service quality to degrade for other tenants. Proper monitoring of service levels is imperative to avoid Denial of Service being caused by a "noisy neighbor" tenant, but security does not require a separation of tenants into individual resource pools to meet this goal.

- Sometimes, an external network may be used by an organization VDC network to connect two different vApps and their networks or to connect a vApp network back to the enterprise data center. In these cases, the external network should not be shared between tenant organizations.

- For communications that traverse an external network and also require confidentiality protections (for instance, a vApp-to-enterprise data center connection or a vApp-to-vApp bridge), deploy an NSX Edge or other VPN virtual appliance in the organization VDC network.

- If tenants share network pools, it is safest to share a VXLAN-backed pool, which supports many more networks than a VLAN-backed pool, and enforces isolation at the ESXi-kernel layer.

- If you share datastores across storage policies, set a storage limit, enable thin provisioning if possible, and monitor storage usage carefully. Also carefully manage vApp storage leases.

- Virtual machines never see any storage outside of their VMDKs unless they have network connectivity to those storage systems. Ensure that they do not. A **system administrator** can provide access to external storage for vApps as a network service, but it must be separate from the LUNs assigned to the vSphere hosts backing the cloud.

- As defined in *vSphere Security*, it is important to separate the management network from the virtual machine data networks.

- Likewise, the management network must be separate from the DMZ that provides access for organization administrators.

- The storage networks are also physically separate. This follows vSphere best practices and protects tenant organization and provider storage from malicious virtual machines.

- vMotion is not always placed on a separate network from the management network. However, in the cloud, this is important from a Separation of Duties perspective. vMotion generally takes place in the clear, and if it is put on the management network, it allows a provider administrator or other user with access to that network to "sniff" on the vMotion traffic, violating tenant privacy. For this reason, you should create a separate physical network for vMotion of cloud workloads.

- Ensure that you regularly examine logs for suspicious, unusual, or unauthorized activity. Routine log analysis will also help identify system misconfigurations and failures and help ensure adherence to SLAs.

- You can set up a syslog server during installation. Use a TLS-enabled syslog infrastructure. Exporting logs to a syslog server is preferred for multiple reasons. To ensure that essential events are always logged, configure the `syslog` server with redundancy. Security Operations and IT Operations organizations might also benefit from the centralized aggregation and management of diagnostic logs. Use `logrotate` or similar methods to control the size of logs and the number of old log files to keep.

- Ensure that you have sufficient free disk space to accommodate diagnostic logs and Jetty request logs. Centralized logging ensures that you don't lose valuable diagnostic information as the 1.4 GB log file total is reached and files are rotated and deleted.

- Other systems connected to and used by VMware Cloud Director create audit logs that you must consolidate into your audit processes. These include logs from NSX, the VMware Cloud Director database, vCenter Server, and vSphere hosts.

- After the initial local system administrator account is created, ensure that all system administrator accounts be managed by an Identity Provider, such as LDAP or the vSphere SSO service.

- Some cloud providers might choose to allow organizations to use an OU within the system LDAP or to host the organization's LDAP directory. In either case, appropriate management access to that directory must be provided so that users can be managed by the organization administrator. In the absence of such management controls, a tenant organization should only use a private LDAP directory that they themselves host and manage.

- Another concern that arises when the organization is hosting their own LDAP server is exposure outside their DMZ. It is not a service that needs to be accessible to the general public. Take steps to limit access only to the VMware Cloud Director cells. One simple way to do that is to configure the LDAP server and the external firewall to only allow access from IP addresses that belong to the VMware Cloud Director cells.

- The provider can take steps to protect against this and similar intertenant attacks by limiting the source IP addresses of requests when possible and by ensuring that the organization names assigned to tenants are never too similar to one another.

- To properly protect the passwords being validated against LDAP servers, configure VMware Cloud Director to connect to these LDAP servers over SSL. When configuring LDAP over SSL, do not accept all certificates.

- Best practices for managing users and their passwords are important to understand and apply.

■ Use Log management, Security Information and Event Management (SIEM), or other monitoring systems, to watch for attempts to crack passwords through brute force attacks.

■ Store the **system administrator** and **organization administrator** passwords in a manner approved by your IT security department.