vCloud Director Security

VMware Cloud Director 9.1

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

https://docs.vmware.com/

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

Contents

Introduction 1

VMware vCloud Director is a flexible system for providing cloud computing services. It leverages and extends VMware's core virtualization and management technologies for support of cloud environments.

Because the system was developed and tested with multitenancy, scalability and other security concerns in mind, the way in which it is deployed can have a significant impact on the security of the overall system. This document describes some possible threats the system faces, as well the security features provided by the overall VMware software stack and the related components it uses, such as databases.

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

In general, threats to vCloud 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. Additional security guidance and late-breaking advisories for vCloud Director will be posted there.

Scope of Recommendations

Recommendations provided in this guide are limited to the management of security issues specific to vCloud Director. As a Web application hosted on a Linux platform, vCloud Director is subject to the security vulnerabilities present in those two categories, all of which are documented elsewhere.

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 ancillary topics are not discussed in this guide.

Updated Information

This *vCloud Director Security* documentation is updated with each release of the product or when necessary.

This table provides the update history of the *vCloud Director Security*.

Revision	Description
10 JUL 2018	Updated Database Security to add information that vCloud Director does not support SSL connections to Oracle and Microsoft SQL Server databases.
08 MAR 2018	Initial release.

Threats

2

Security threats to vCloud 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 vCloud Director server group and threats to the installed vCloud Director software.

Multitenancy and Internal Threats

vCloud Director is designed to give tenants managed access to VMware vSphere ® network, computing and storage resources. Tenant users can log into vCloud Director and are generally given rights to deploy and/or use virtual machines, use storage, run applications, and (to a limited extent) share resources with other users.

One of the key features of vCloud 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 may still attempt to gain access to information about the system infrastructure on which their cloud-enabled applications run. If they were able to do so, they might be able to better launch 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, such as resources that belong to another organization. They might attempt privilege escalation, in particular, obtaining access to actions reserved for administrators. Users may 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, a variety of administrative users generally exist. These include the system administrator for a vCloud Director site, tenant organization administrators, administrators of databases and networks, and users with access rights to ESXi, vCenter, and guest operating systems that run management tools. These users have higher privileges compared to ordinary users, and usually have direct login to internal systems. Nevertheless their privileges are not unlimited. There is a potential threat that they too may attempt privilege escalation or take harmful actions.

As will be seen, the security of vCloud Director from these threats comes from the architecture, design, and implementation of vCloud Director, vSphere, and VMware NSX ™, along with 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, attacking vCloud Director through its APIs and Web interfaces (the vCloud Director Web Console and vCloud Director Tenant Portal), as well as the vApp transfer service and the virtual machine remote console. 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 considered to be the sources of external threats, as they may 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 in order to obtain information, acquire access to services, or simply to disrupt the operation of the cloud through 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 vCloud 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.

vCloud Director Architecture and Security Features

3

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

A vCloud Director server group consists of one or more Linux servers. Each server in the group runs a collection of services called a vCloud Director cell. All cells share a single vCloud Director database, and connect to multiple vCenter Server systems, the ESXi hosts that they manage, and the NSX Managers that provide networking services.

Figure 3-1. vCloud Director Architecture Diagram

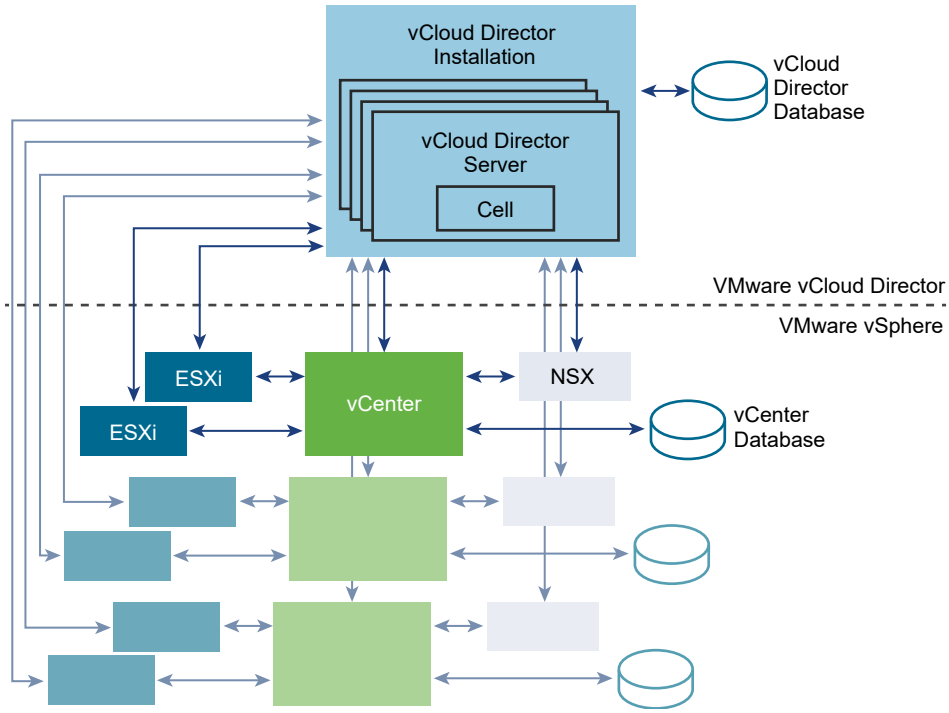


Figure Figure 3-1. vCloud Director Architecture Diagram shows a single vCloud Director server group (installation) Within the server group there might be many vCloud Director server hosts, each with a single cell running. Together, the server group shares the vCloud Director database and an NFS file share (not shown). The cloud abstraction is built using the vCloud Director software and leveraging capabilities in both vCenter and NSX, shown in the diagram as

connecting to the server group. vCloud Director organizations and their users do not interact directly with vCenter and NSX to create and manage their workloads. For anyone other than a system administrator, all interactions with vCenter and NSX are presented as vCloud Director operations on vCloud Director objects. Permission to access and operate on vCloud 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

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 vCloud 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 vCloud Director software-defined networks, the leveraging of NSX technology, and the security of the ESXi hosts themselves.

Security and the vCloud Director Abstraction

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

The vCloud Director abstraction enables a service provider to delegate vApp creation, management, and use to tenant organizations (or an IT department to delegate these capabilities to line of business teams). Tenant organization administrators and users do not operate on or manage vCenter features like vMotion, VSAN, and so on. Tenants deal only with deploying their workloads (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, there's no chance of a misconfigured vCenter 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, as they're sharing the same 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 vCloud Director is designed to hide system-level operations from tenants, certain features of the system can be configured to provide information that could be misused by a malicious tenant.

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 information about the physical host could be misused by a malicious tenant, you should 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

vCloud Director can collect metrics that provide current and historic information about virtual machine performance and resource consumption. Because some of these metrics include information about the physical host, which could be misused by a malicious tenant, you should consider configuring the metrics collection subsystem to collect only those metrics that are not subject to malicious use. See Configuring Metrics Collection in the *vCloud Director Administrator's Guide* for details.

Exercise Caution With Extensions

vCloud Director supports a number of extensibility methods. While these methods are all designed to prevent any extension from acquiring rights not granted to tenant users or escalating the privileges that they were assigned at installation, an extension can provide, intentionally or not, additional attack surfaces that someone who has knowledge of the extension

could exploit. Service providers and tenant administrators should 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

vCloud 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 they can be consumed by tenants.

This brief overview of vCloud Director is intended to establish 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 vCloud Director documentation at http://docs.vmware.com.

Provider-Level Network Resources

In the typical case, a service provider is responsible for creating one or more connections between vCloud 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 vCloud 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 portgroups 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 vCloud Director VXLAN network can also provide isolation by encapsulating Layer 2 packets in other Layer 2 packets (MAC-in-MAC) in the ESXi kernel, allowing the kernel when de-encapsulating packets to direct them to the correct guest virtual machines connected to the networks created out of this sort of pool.

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 portgroups provided by ESXi. From these resources, tenant organizations can create their own networks.

Organization VDC Networks

An organization VDC network allows virtual machines in the organization VDC to communicate with each other and to access other networks, including organization VDC networks and external networks, either directly or through an Edge Gateway that can provide firewall and NAT services.

- A direct organization VDC network connects directly to an external network. Only a system administrator can create a direct organization VDC network.
- A routed organization VDC network connects to an external network through an Edge Gateway. A routed organization VDC network also requires the containing VDC to include a network pool. After a system administrator has provisioned an organization VDC with an Edge Gateway and associated it with a network pool, organization administrator or system administrators can create routed organization VDC networks in that VDC.
- An isolated organization VDC network does not require an Edge Gateway or external network, but does require the containing VDC to be associated with a network pool. After a system administrator has created an organization VDC with a network pool, organization administrators or system administrators can create isolated organization VDC networks in that VDC.

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.	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 via an Edge Gateway. 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.

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. A shared organization VDC network can be used by all virtual machines in the organization.

vApp Networks

Every vApp contains a vApp network. 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 is concerned with protecting vCloud Director itself, but overall system security also requires securing the infrastructure on which vCloud Director depends, including vSphere, NSX, the cell Linux platform, and the vCloud Director database.

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 vCloud Director. Administrators should 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. https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.security.doc/GUID-52188148-C579-4F6A-8335-CFBCE0DD2167.html

NSX security

Securing VMware NSX for vSphere. https://communities.vmware.com/docs/DOC-27674 and https://communities.vmware.com/docs/DOC-28142.

Securing Your Cell Platforms

vCloud Director cells run on a Linux-based operating system as an unprivileged user (`vcloud.vcloud`) created during installation. The list of supported cell platform operating systems is included in the *vCloud Director Release Notes*. Securing the cell platform, whether it is physical or virtual, is a key part of securing vCloud Director.

Standard security hardening procedures should 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 may decrease security.

Protecting Sensitive Files After Installation

During installation, vCloud 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 vCloud Director database password and system keystore passwords. Unauthorized access to that file could give an attacker access to the vCloud Director database with the same permissions as the database user specified in the configuration script. The `global.properties` file also contains encrypted credentials that should 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 may either give too much access, reducing security, or restrict access too much, stopping the vCloud Director software from working. In order for the access controls to properly work, physical and logical access to the vCloud 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.

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

Administrative Credentials

Ensure that any credentials used for administrative access to the cell, vSphere, the vCloud Director database, to external firewalls and other devices, follow standards for adequate password complexity. Consider an expiration and rotation policy for passwords wherever possible. Please be aware, however, that an expired or changed database, vSphere, or NSX password will make part or all of the cloud infrastructure nonfunctional until vCloud 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 vCloud Director environment, including the vCloud Director cells, the vCloud Director DB, vSphere servers, and NSX manager. This is so that 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 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 properly secure the vCloud Director database per industry best practices.

The vCloud Director database user account should have only the system privileges listed in the appropriate database configuration guidance in the *vCloud Director Installation and Upgrade Guide*. The vCloud Director database user should not be given privileges over other databases on that server or other system administration privileges. This would violate the Principle of Least Privilege on the database server and give the user more rights than necessary.

We recommend consulting the following documents for database security information.

Microsoft SQL Server

SQL Server Security Best Practices at http://download.microsoft.com/download/8/f/a/8fabacd7-803e-40fc-adf8-355e7d218f4c/sql_server_2012_security_best_practice_whitepaper_apr2012.docx.

Note vCloud Director does not support SSL connections to a Microsoft SQL Server database.

Oracle

Oracle Database Security Guide at https://docs.oracle.com/cd/B28359_01/network.111/b28531.pdf.

Note vCloud Director 9.5 does not support Oracle databases.

vCloud Director 9.1 supports Oracle databases, but does not support HTTPS and SSL connections to an Oracle database.

PostgreSQL

In addition to enabling SSL for PostgreSQL connections, we recommend reviewing the PostgreSQL Server Administration documents.

System Security

5

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

Securing a vCloud Director server group from outside attackers, requires you to take the kinds of defensive measures common to all Web-based services, including securing HTTPS endpoints with signed certificates and placing a Web Application Firewall between the system and the Internet. In addiiotn, you must be sure to configure the services on which vCloud 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:

Network Security Requirements

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

Connect all vCloud Director servers to a network that is secured and monitored. vCloud Director network connections have several additional requirements:

- Do not connect vCloud Director directly to the public Internet. Always protect vCloud 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 vCloud 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 vCloud 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, 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 and ESXi connections.
903	TCP	vCenter and ESXi connections.
920	TCP, UDP	NFS rpc.statd used by transfer service.
1433	TCP	Default Microsoft SQL Server database port.
1521	TCP	Default Oracle database port.

Table 5-2. Ports That Must Allow Outgoing Packets From vCloud Director Hosts (continued)

Port	Protocol	Comments
5672	TCP, UDP	Optional. AMQP messages for task extensions.
61611	TCP	AMQP
61616	TCP	AMQP

- Route traffic between vCloud Director servers and the following servers over a dedicated private network.
  - vCloud Director database server
  - RabbitMQ
  - Cassandra
- If possible, route traffic between vCloud 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 vCloud Director transfer service is available lin VMware Knowledge Base article 2086127.

Certificates

vCloud 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 should 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 should include `subjectAltName` field that matches the host's IP address.

Additional information is available in (RFC 6125) and (RFC 5280). You should 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. Lower-level certificates (enterprise-CA or self-signed) cannot be checked in this way, have been created by your local security team, who can tell you where to import them from.

Certificates for Private (Internal) Endpoints

Endpoints on private networks, ones that are unreachable from public networks and have generally been created specifically for use by vCloud Director components such as the database and AMQP, 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 vCloud 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 vCloud Director component.

Supported Protocols and Cypher Suites

vCloud Director supports several HTTPS protocols, including TLS and SSL. TLS v1.0 is unsupported by default because it has known vulnerabilities. After installation, you can use the cell management tool configure the set of protocols and cypher suites that the system supports for HTTPS connections. See *vCloud Director Release Notes* for details.

Configuring vSphere Certificates

In vSphere 6.0 and later, the VMware Certificate Authority (VMCA) provisions each ESXi host and each vCenter Server service 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 the *vSphere Security* guide for more information about creating and replacing certificates used by vCenter and ESXi.

Configuring vCloud Director to Check vCenter Certificates

To configure vCloud Director to check vCenter certificates, create a Java keystore in JCEKS format that contains the trusted certificate(s) used to sign vCenter certificates. (Certificates for the individual vCenter servers are not in this store -- only the CA certificates that are used to sign them.)

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

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

Once you have created the keystore, log in to vCloud Director as a system administrator. In the **System Settings** section of the **Administration** tab, click **General** and navigate to the bottom of the page.

Select **Verify vCenter and vSphere SSO** certificates and **Verify NSX Manager certificates**. Click the **Browse** button to search for your Java keystore, then click **Open**. Enter the keystore password and click **Apply**.

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

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

Important If you have changed certificates after adding vCenters and NSX managers to vCloud Director, you must force reconnection to the servers.

Updating Certificates and Keys for vCloud Director Cells

Each vCloud 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 vCloud 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 and Import a Signed SSL Certificate in the *vCloud Director Installation 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, see Replacing Certificates for the HTTP and Console Proxy Endpoints in the *vCloud Director Administrator's Guide*.

Firewalls

vCloud Director cells must be accessible by tenants and system administrators, who typically connect to it from outside the service provider's network perimeter. The recommended approach to making vCloud Director services available to the outside is to place a Web Application Firewall between the Internet (or other enterprise network) and each vCloud Director public endpoint.

Network firewalls segment physical and/or virtual networks such that only a limited, well-defined set of traffic on specific ports and protocols pass between them. This document does not define the rationale for 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 it is suggested that network firewalls be placed in relation to the different components of a vCloud Director deployment.

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

As the vCloud Director cells are in the DMZ, their access to the services they need should also be mediated by a network firewall. Specifically, it is recommended that access to the vCloud Director DB, vCenter Server, ESXi hosts, AMQP and any backup or similar services be restricted 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

A number of firewall rules are recommended to protect the system against network threats:

- 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

These and other rules are typically applied by Web Application Firewalls and may be applied by default by the network firewall you choose to deploy. See your firewall's documentation for specific configuration instructions and default capabilities.

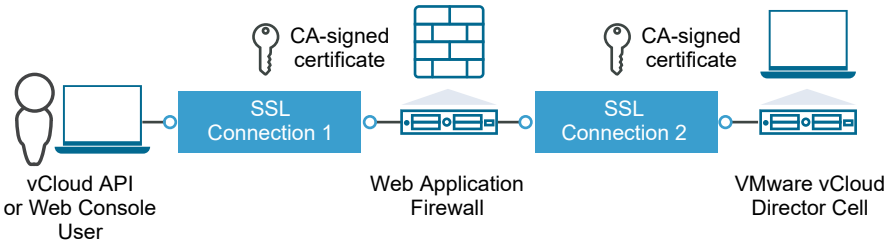
Load Balancers and SSL Termination

You should protect vCloud Director public endpoints with a Web Application Firewall (WAF). When used in conjunction with a load balancer, configure the WAF to allow inspection and blocking of malicious traffic by terminating the HTTPS connection at the WAF, allowing the WAF to complete the handshake using its own certificate and forward acceptable requests to the cell with an `X-Forwarded-For` header.

Client requests to vCloud 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, it is required that WAF-to-cell communication also be done 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 vCloud 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 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. 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 vCloud 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 *vCloud Director Administrator's Guide*.

X-Forwarded-For Header

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

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 will generally get 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.

Securing AMQP (RabbitMQ)

AMQP, the Advanced Message Queuing Protocol, is an open standard for message queuing that supports flexible messaging for enterprise systems. vCloud 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 vCloud 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 vCloud Director messages should be subject to audit by the service provider's security team.

For more information about RabbitMQ and how it works with vCloud Director, see the vCat-SP blog entry at https://blogs.vmware.com/vcat/2015/08/vcloud-director-for-service-providers-vcd-sp-and-rabbitmq-security.html

Protect the AMQP Service with SSL

To use SSL with the vCloud Director AMQP service, select **Use SSL** on the **AMQP Broker Settings** section of the **Extensibility** page of the vCloud 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 the *vCloud Director Administrator's Guide* for the complete procedure.

Important Although an **Accept all certificates** option is available, we do not recommend selecting 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 Cassandra (VM 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 like 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 Encryotion

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

We recommend using certificates that have been signed by a well-known CA. When you do this, no additional configuration is required in vCloud Director. If you are using self-signed certificates, you must import them manually into vCloud Director Director. Use the cell management tool's `import-trusted-certificates` command as shown in Importing SSL Certificates from External Services in the *vCloud Director Administrator's Guide*

Securing Access to JMX

As described in the *vCloud Director Administrator's Guide*, each vCloud Director cell exposes a number of 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 vCloud Director system administrators, who must authenticate to JMX using the same credentials they use to access vCloud 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 vCloud Director's management network. If the system has a third IP address assigned exclusively for management, bind JMX directly to this IP address. By default, the vCloud 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 organization users.

With this setting in `global.properties`, JMX can be reached only from the local vCloud Director system. No external connections to the JMX port will succeed 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 through the use of 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 vCloud 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 vCloud 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 will run `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 (not recommended for a production deployment) would make this process unwieldy, as you'd 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.

Management Network Configuration

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

Systems that connect to the management network include the vCloud Director database server, an NFS server for transfer storage, the vCenter servers, an optional LDAPv3 directory for authenticating provider administrators, any LDAPv3 directories maintained by the provider for authenticating organization users, and NSX managers. The vCenter servers 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 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 defense in depth.

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 vCloud Director cells exist physically on the DMZ. In the physical deployment diagram, the servers in the management pod that connect over to the cloud pods do so via a separate physical network, and specific firewall rules allow this traffic to pass.

The internal firewall that mediates vCenter and vCloud Director connections to vSphere (and other networks) is required from a network architecture perspective. This is not a question of 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. While the vCloud Director software was designed and implemented following VMware's Product Security Policy and with security requirements in mind, it is not a firewall itself and thus 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 depends 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 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

Being able to 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, whether 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 in mitigating the damage and preventing future attacks.

Whether or not it is required, it is part of good security practice to 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.

vCloud 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 vCloud Director cell creates several diagnostic log files described in Viewing the vCloud Director Logs in the *vCloud Director Administrator's Guide*.

Audit logs

Audit logs record significant actions, including login and logout. The system audit log is maintained in the vCloud 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.

We recommend using the `syslog` utility to preserve these and other vCloud 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`.

Using Syslog with vCloud Director

As detailed in the *vCloud Director Installation and Upgrade Guide*, a `syslog` server can be set up during installation. Exporting logs to a `syslog` server is recommended for multiple reasons:

- Database logs are not retained after 90 days, while logs transmitted via `syslog` can be retained as long as desired.
- 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 will integrate with vCloud Director. This allows:
  - Correlation of events and activities across vCloud 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 vCloud Director host to the `syslog` server. The `syslog` server configuration details are system specific and outside the scope of this document. It is recommended that the `syslog` server be configured with redundancy, to ensure essential events are always logged.

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 a variety of methods for collecting those logs including scheduling a job to periodically copy them to a centralized location, 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 is dependent on which system you prefer to use in your environment and is outside the scope of this document.

Important We recommend using a TLS-enabled `syslog` infrastructure. The default (UDP) `syslog` protocol offers neither in-transit encryption nor transmission control/acknowledgement. The lack of encryption exposes log data to sniffing (the information present in logs could be used to launch further attacks), and the lack of transmission control could 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 come with 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. For this reason, we recommend that you use `logrotate` or similar methods to control the size of logs and the number of old log files to keep.

The other diagnostic log files are limited to 400MB 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 will ensure you don't lose valuable diagnostic information as the 400MB log file total is reached and files are rotated and deleted.

NTP and Logs

The *vCloud Director Installation and Upgrade Guide* identifies NTP as a requirement for all vCloud 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 vCloud Director create audit logs that should be consolidated into your audit processes. These include logs from NSX Manager, the vCloud 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 vCloud Director tenant organization.

Securing a vCloud 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 often referred to as the "noisy neighbor" problem.

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

This chapter includes the following topics:

Network Security for Tenant Organizations

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

Within the vCloud Director system, VXLAN and VLAN networks enforce separation of packet traffic that is equivalent to what can be achieved 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 vCloud Director documentation at http://docs.vmware.com.

For the most part, a service provider who has designed effective protection for the system itself (including a Web Application Firewall, SSL-terminating load balancers, and well-signed digital certificates) need not 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 should keep in mind the firewall requirements of the vSphere infrastructure deployed and used by vCloud Director. Most likely, some vApps will either need access to the Internet or need to be accessed remotely, whether via RDP, SSH, and so on, for management, or via HTTP or other protocols for end users of those services. For that reason, two different virtual machine data networks are recommended (as seen in the architecture diagrams in Resource Allocation and Isolation) for different uses; each requires network firewall protection.

Virtual machines that need accessibility from outside the cloud (for example, from the Internet) would be either connected 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 would require a protecting firewall that allows in agreed-upon traffic to this DMZ network. That is, the service provider should ensure that not every port and protocol is allowed to initiate a connection to the external DMZ network. At the same time, it must ensure that enough traffic is allowed that organizations' vApps can provide the services for which they're intended. This typically includes port 80/TCP and 443/TCP, but could 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, it is recommended that vApps that need accessibility to and from the Internet 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 vCloud Director firewall protection. The separate firewall is needed to create a DMZ (this function could be performed by a separate NSX Edge instance, however).

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

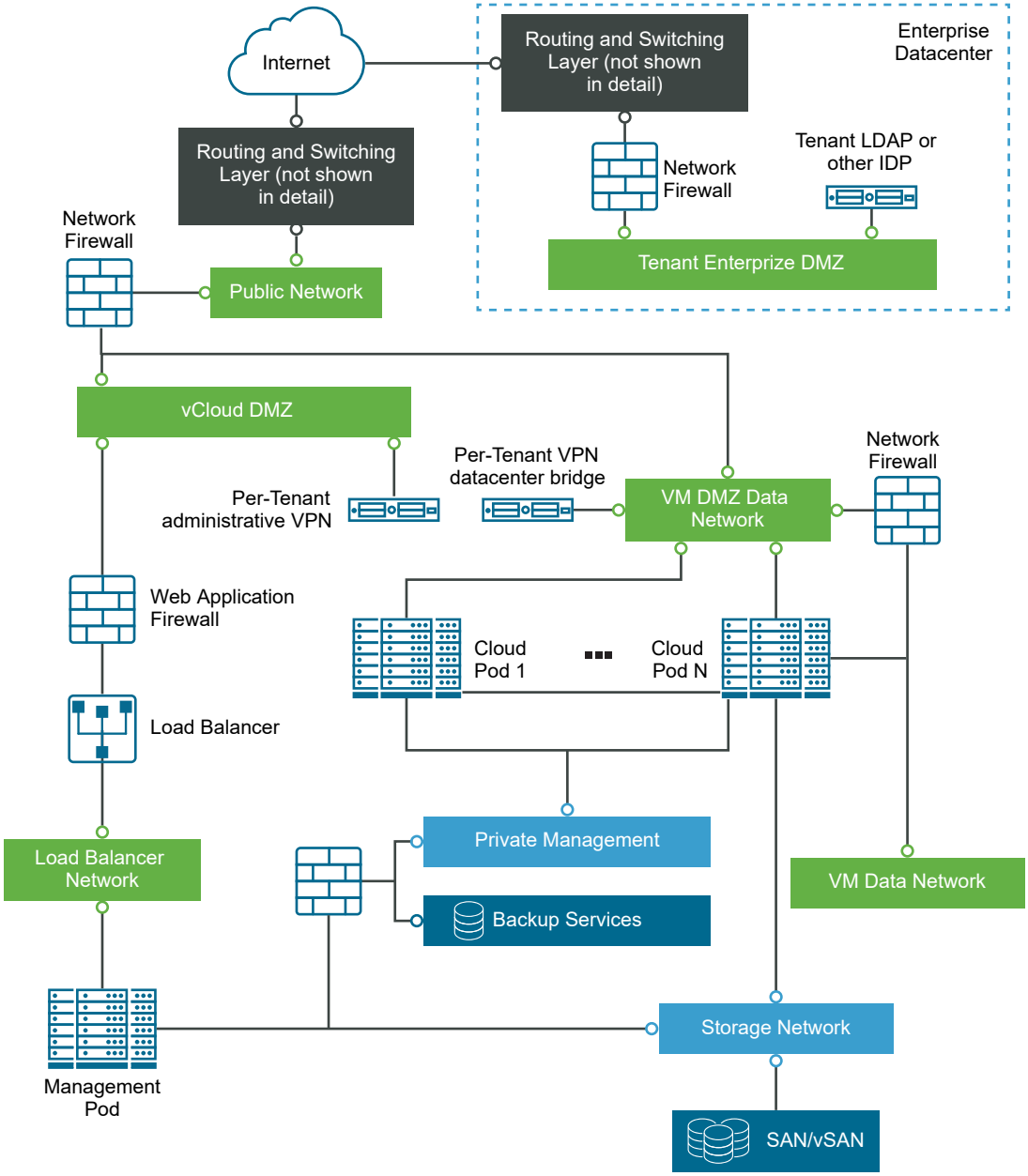
The standard service provider deployment of vCloud Director envisions the sharing of vSphere resources among multiple tenant organizations. This provides the organizations with maximum flexibility and the provider with maximum utilization of the provisioned compute, network, and storage resources. Sample logical and physical deployment diagrams are below.

The rest of this subsection describes the components at a high level, while subsequent subsections describe specific recommendations regarding the resource pools, datastores, networking and other components' configuration.

Shared Resource Deployment

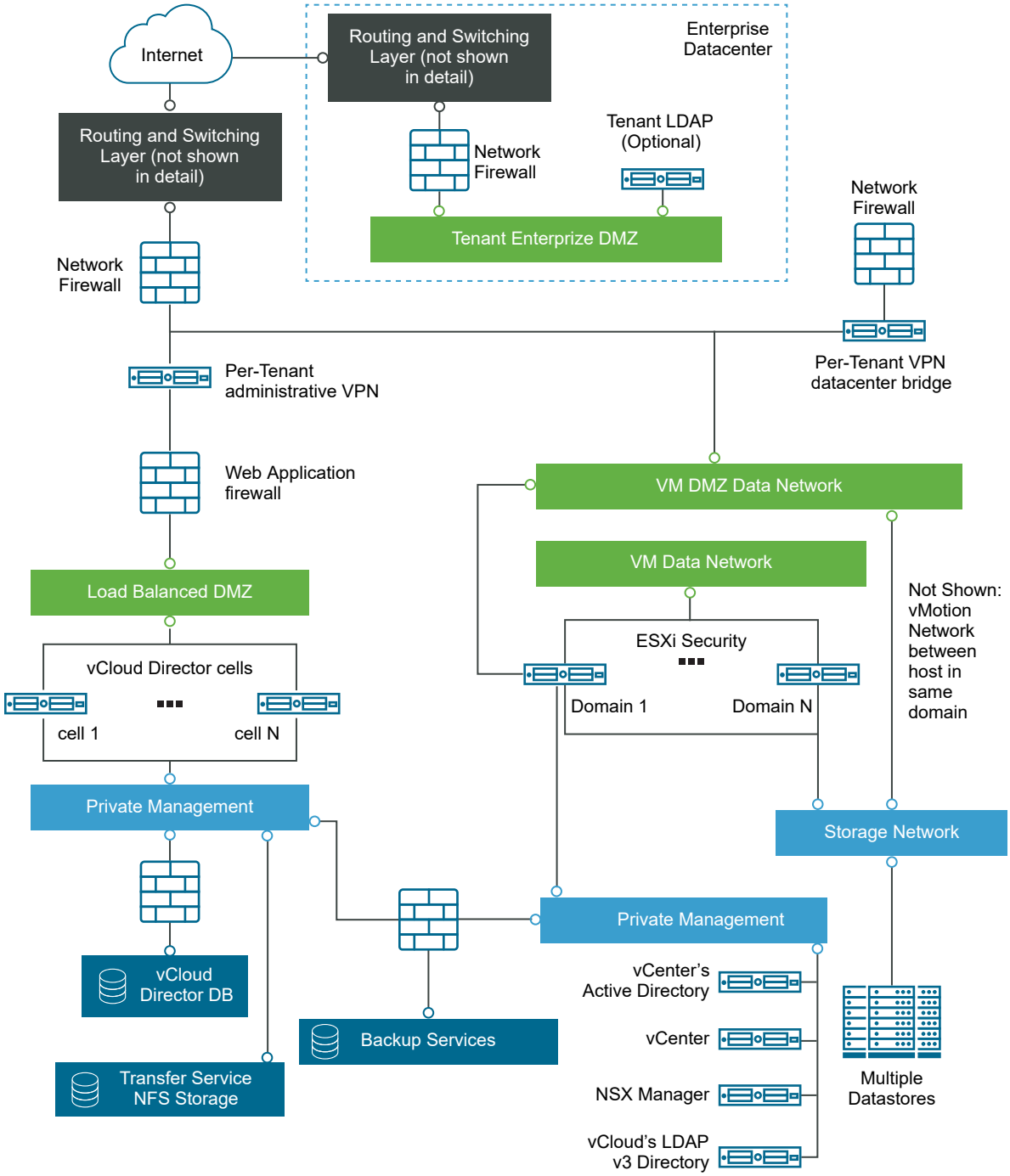
Figure 6-1. Physical Deployment Diagram and Figure 6-2. Logical Deployment Diagram are two views of the same vCloud Director installation. In these figures, we use the term "pod" to denote a group of resources (physical or virtual machines) dedicated to either system management ("management pod") or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

Figure 6-1. Physical Deployment Diagram



Looking at Figure 6-2. Logical Deployment Diagram, the left side shows the vCloud Director cells in a load-balanced DMZ. The DMZ also contains a WAF and optionally a per-tenant administrative VPN. This VPN can be configured by a service provider 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.

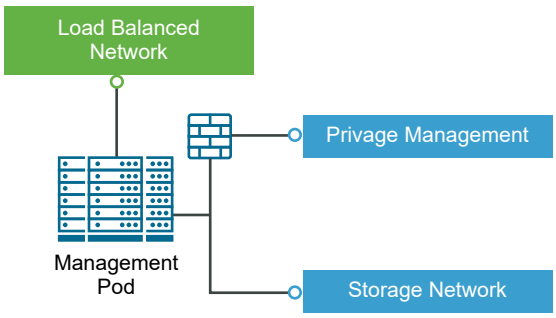
Figure 6-2. Logical Deployment Diagram



Behind the cells are the private management elements required by vCloud Director, including vCenter, NSX, the vCloud 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, if not three, 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.

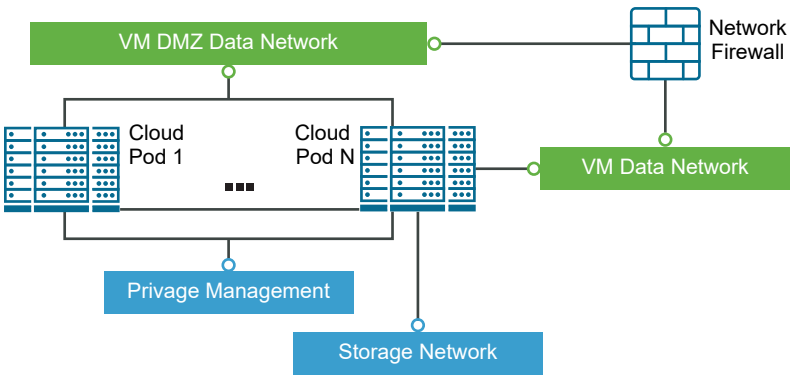
Figure 6-3. Management Pod Networks



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 may be routed to an External Network.

Figure Figure 6-4. Cloud Pod Networks focuses on the Cloud Pods. It shows four physical networks; however, the Storage Network is specific to the particular hardware and storage technologies chosen. If resource pools do not span clusters, you may not need to provide a physical VM data network. Otherwise (if resource pools span clusters), this document recommends a separate physical network for vMotion traffic.

Figure 6-4. Cloud Pod Networks



It is also assumed that typical datacenter security technologies, such as IDS/IPS, SIEM, configuration management, patch management, vulnerability management, anti-virus, and GRC management systems, will be applied to both the vCloud 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 vCloud Director software stack.

Tenant organizations share the underlying resource pools, datastores, and external networks exposed through a single Provider VDC without affecting (or even 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 teanant cannot deny service to another by accident or on purpose. For example, a very conservative configuration would set up all organization VDCs under the reservation pool allocation model and never overcommit resources. The full complement of options is not covered in this document; however, some points are made in the following subsections.

Security Domains and Provider VDCs

Despite the proper isolation in the software and proper organization configuration, there may be times when tenant organizations do not want different workloads to be run or stored on particular compute, network, or storage resources. This doesn't elevate the system overall to a "high-security environment" (discussion of which is beyond the scope of this document), but does necessitate the need for the cloud to be segmented into multiple security domains. Specific examples of workloads requiring such treatment include:

- Data subject to privacy laws that 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 defense in depth 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 may clearly 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 may 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 additional computing resources can be brought online by the provider. This guide does not define the different resource allocation models and how they impact each organization's usage 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 Denial of Service being caused by one organization, but security does not dictate a specific separation of organizations to meet this goal.

Limiting Shared Consumption of Shared Resources

In the default configuration, many vCloud Director compute and storage resources can be consumed in unlimited quantities by all tenants. 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 vCloud Director provides.

Limit resource-intensive operations

See Configure System Limits in the *vCloud 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 *vCloud 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 *vCloud Director Administrator's 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, since by definition those networks are public. 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 needed.

Private routed networks can share those External Networks in the same circumstances -- when they're 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 datacenter. In these cases, the External Network should not be shared between organizations.

Certainly, one cannot expect to have a separate physical network for each organization. Instead, it is recommended that a shared physical network be connected to a single External Network that is clearly identified as a DMZ network. Thus, organizations will 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 datacenter 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* (vCAT-SP)

Organization VDC networks owned by different tenants can share the same External Network (as an uplink from an Edge Gateway) as long as they don't allow access to the inside with NAT and IP masquerading.

Important vCloud Director Advanced Networking allows tenants and service providers to employ dynamic routing protocols such as OSPF. The OSPF autodiscovery mechanism, when used without authentication, could potentially 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

A single network pool can be used by multiple tenants as long as all networks in the pool are suitably isolated. VXLAN-backed Network Pools (the default) rely on the physical and virtual switches being configured to allow connectivity within a VXLAN and isolation between different VXLANs. Portgroup-backed Network Pools must be configured with portgroups that are isolated from each other. These portgroups could be isolated physically, through VXLANs.

Of the three types of Network Pools (portgroup, VLAN, and VXLAN), it is easiest to share a vCloud Director VXLAN Network Pool. VXLAN pools support many more networks than VLAN- or portgroup-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 (for example, at the physical layer).

Storage Profiles

vCloud Director storage profiles aggregate datastores in a way that enables the service provider to offer storage capabilities tiered by capacity, performance, and other attributes. Individual datastores are not accessible by tenant organizations. Instead, a tenant can choose from a set of storage profiles 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 may 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 noged in Limiting Shared Consumption of Shared Resources. Alternatively, if you do not share datastores, you must properly dedicate storage to the storage profiles 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, that requires rights not available to vCloud Director administrator or tenant. Tenant users who create and upload vApps simply store the vApps' VMDKs on one of the storage profiles 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. This guide recommends that they do not; a provider could 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 profiles available in their organization VDCs, and even that view is limited to the vCloud Director abstraction. They cannot browse the system's datastores. They see only what's 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. vCloud 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 *vCloud 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 vCloud Director system is by username 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 vCloud Director and provides recommendations on how to securely manage and use them given those constraints.

Limitations of Local User Accounts

While vCloud Director provides a self-contained identity provider for user accounts, which are created and maintained in the vCloud Director database. While not inherently vulnerable in a system configured with limited network access to the database (see Management Network Configuration), 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 re-try limits and account lockout rules.

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

A new installation of vCloud Director creates a local system administrator account. In the default configuration, vCloud 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 vCloud 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 (a SAML IDP) 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
```

Note that 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 *vCloud Director Administrator's 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 are outside the scope of this document. The vCloud 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 vCloud Director to handle this situation for other local users. It is recommended that all local account passwords be safely stored in a manner approved by your IT security department. Some organizations lock passwords in a vault. Others use commercially or freely available password storage programs. This document does not recommend a particular method.

Password Strength

The strength of IDP users' passwords is dependent on the controls provided by that IDP and/or the tools used to manage users within the directory. For example, if connecting vCloud Director to Active Directory, the typical Active Directory password length, complexity, and history controls associated with Microsoft Active Directory are enforced by the directory itself. Other IDPs tend to support similar capabilities. The details of password strength controls are directory specific and aren't covered here in more detail.

vCloud 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. It is recommended that any users, especially system and organization administrators, take great care in choosing their passwords to protect against brute force attacks (see account lockout issues below).

User Password Protection

The credentials of users managed by an IDP are never stored in the vCloud 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 vCloud 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 vCloud Director database stores passwords for connected vCenter servers and NSX managers. Changes to those passwords are not automatically updated in the system. You will need to manually change them using the vCloud Director configuration script (for the vCloud Director database password) or the Web UI for the vCenter and NSX.

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

Role-Based Access Control

vCloud Director implements a role-based authorization model. This section discusses the different identity sources, user types, authentication controls, roles, and rights present in vCloud Director. An understanding of this information is required to properly secure the system and provide the correct access to the right people.

A vCloud Director tenant organization can contain an arbitrary number of users and groups. Users can be created locally by the organization administrator or imported 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 vCloud Director functionality through the Web console, Tenant Portal, or vCloud API. Each user authenticates using a username and password. Password re-try and account lockout policies can be configured globally and per organization.

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

- System Administrator
- Organization Administrator
- Catalog Author
- vApp Author
- vApp User
- Console Access Only

The *vCloud Director Administrator's 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 may be appropriate for an administrator that needs to power on and off virtual machines, but if they also need to edit the amount of memory assigned to a virtual machine, then vApp Author would be a more appropriate role. These roles may 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 vCloud 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 vCloud Director, with a single set of credentials, an arrangement often referred to as single sign-on.

About Identity Providers

vCloud 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 (https://openid.net/specs/openid-connect-core-1_0.html).

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 vCloud Director service that authenticates users who are created locally or imported from LDAP.

LDAP

The vCloud Director integrated identity provider supports several popular LDAP services.

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

vCloud Director allows the system administrator to define a systemwide LDAP service that can be used by all tenants. Tenant user accounts are imported into the vCloud Director database where vCloud Director roles are assigned. LDAP users' 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 of the 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 OU specifically configured in that organization's vCloud Director System LDAP Service settings.

Cloud providers may 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 so that users can be managed by the organization administrator. The lack of such control would provide an extra burden on the system administrator and hinder the organization from easily and properly controlling access to their 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 vCloud Director cells to the system LDAP server and any organization LDAP servers must be enabled for the software to properly authenticate users. As recommended in this document, the system LDAP server must be located on the private management network, separated from the DMZ by a firewall. Some cloud providers and most IT organizations will run any organization LDAP servers required, and those too would be 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 vCloud Director cells, potentially through the enterprise datacenter's own DMZ.

In all of 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 needs to be accessible to the general public, so steps should be taken to limit access only to the vCloud Director cells. One simple way to do that is to configure the LDAP server and/or the external firewall to only allow access from IP addresses that belong to the vCloud 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 could 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 both limiting the source IP addresses of requests when possible to avoid inter-organization logon attempts as well as ensuring that organization names it assigns are never too similar to one another.

LDAP over TLS/SSL

It is highly recommended that you configure a LDAPv3 directory for user authentication. vCloud Director must be configured to connect to LDAP servers over SSL in order to properly protect the passwords being validated against those servers. See "Configure an LDAP Connection" in the *vCloud Director Administrator's Guide* for details. 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 a lot of 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. Please note that vCloud 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 vCloud 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 easily integrate cloud roles with internal organization groups/roles and the systems that provision and manage them.

As an example, an organization may 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 they need to perform could be added to other LDAP groups, also imported to vCloud Director and assigned to these more privileged roles. For instance, users with a need to create Catalogs could be added to the "Org A Catalog Author" group in the organization's LDAP server. Then the organization administrator for Org A would import the "Org A Catalog Author" group and map it to the predefined Catalog Author role in vCloud Director. This is accomplished by following the Import a Group instructions in the *vCloud Director User's Guide*.

Checklist

7

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

- In addition to the guidance in this document, you should 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 vCloud Director will be posted there.
- Administrators should apply the steps recommended in *vSphere Security* (https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.security.doc/GUID-52188148-C579-4F6A-8335-CFBCE0DD2167.html), *Securing VMware NSX for vSphere* (https://communities.vmware.com/docs/DOC-27674), and the *NSX-v 6.3.x Security Configuration Guide* (https://communities.vmware.com/docs/DOC-28142) to ensure that they have secure installations of those products.
- Apply current security patches to the cell Linux platform, vCloud Director database, and virtual infrastructure before installation; ongoing monitoring to keep these components at a current patch level is also crucial.
- Standard security hardening procedures should be applied to the cell Linux platform, including disabling unnecessary network services, removing unnecessary packages, restricting remote root access, and enforcing strong password policies. Use if possible 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 Linux platform, but it is recommended that you do not do this. Widening access to the cell OS may decrease security.
- Make the `responses.properties` file available only to those who have a need for it. When it is in use (while adding cells to a server group), place appropriate access controls on the location accessible to all target hosts. Any backups that are made should be carefully controlled and also encrypted if your backup software supports that. Once the software is installed on all server hosts, any copies of the `responses.properties` file in these accessible locations should be deleted.
- 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.

- Physical and logical access to the vCloud 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. Any backups of the servers must be strictly protected and encrypted, with the keys managed separately from the backups themselves.
- For database security requirements, please refer to the security guides for your chosen vCloud Director database software.
- The vCloud Director database user should not be given 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 Servers, the vCloud Director database, to firewalls and other devices follow standards for password complexity.
- It is important from a defense in depth perspective to vary the administrative passwords for the different servers in the vCloud Director environment, including the cells, the vCloud Director databse, vCenter Servers, and NSX.
- See https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.security.doc/GUID-779A011D-B2DD-49BE-B0B9-6D73ECF99864.html for information about creating and replacing certificates used by vCenter and ESXi. This is highly recommended.
- vCenter certificates should have a common name (CN) field that matches the FQDN (Fully Qualified Domain Name) of the server on which vCenter is installed.
- Configure vCloud Director to Check vCenter Certificates.
- vCenter Certificates should be signed by a CA and have a CN matching the FQDN of the host on which the cell is installed.
- The recommended approach to making vCloud Director services available to the outside is to place the cells in a DMZ, with a network firewall separating the Internet from vCloud Director cells on the DMZ. The only port that needs to be allowed through the Internet-facing firewall is 443/TCP.
- As the vCloud Director cells are in the DMZ, their access to the services they need should also be mediated by a network firewall. Specifically, it is recommended that access to the vCloud Director DB, vCenter Server, vSphere hosts, IDPs (including LDAP), and any backup or similar services be on the other side of a firewall that separates the DMZ from the internal network.
- Virtual machines that require access from outside the cloud (for example, from the Internet) would be either connected 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 would require a protecting firewall that allows in agreed-upon traffic to this DMZ network.

- In general, it is recommended that 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 may 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.
- To set the public Web URL, public console Proxy Address, and public REST API Base URL for a multicell cloud behind a WAF or load balancer.
- A Web Application Firewall (WAF) should be deployed in front of the vCloud Director cells.
- In such deployments, it is recommended that the WAF be configured so as 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.
- It is recommended that you enable generation of the `X–Forwarded–For` header at the firewall if possible.
- If the vCloud Director server has a third IP address assigned exclusively for management, bind JMX directly to this IP address. By default, the vCloud 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`*.
- The recommended and more secure configuration involves binding the JMX connector to the localhost address: `vcloud.cell.ip.management=127.0.0.1`. If JMX is only exposed to localhost, then securing JMX communications is accomplished through the use of SSH as a tunneling mechanism for any access to JMX. If your management requirements do not allow the use tis sort of localhost configuration and JMX must be exposed outside the vCloud Director server, then JMX should be secured with TLS or SSL.
- Behind the cells are the private management elements required by vCloud Director: its database, NSX, vCenter Server, the system LDAP server, if any, the Active Directory server used by vCenter, and the management interfaces of the vSphere hosts. Their connections are strictly controlled by firewalls, as those services should not be accessible from other machines on the DMZ or directly from the Internet.

- It is also assumed that typical datacenter security technologies, such as IDS/IPS, SIEM, configuration management, patch management, vulnerability management, anti-virus, and GRC management systems, will be applied to both the vCloud Director, its associated systems, vSphere and its associated systems, and the networks and storage infrastructure that support them.
- Proper management of leases, quotas, limits, and allocation models can ensure that one tenant organization cannot deny service to another by accident or on purpose.
- 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).
- 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 datacenter. 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 datacenter connection or a vApp-to-vApp bridge), it is recommended that an NSX Edge or other VPN virtual appliance be deployed in the organization VDC network.
- If Network Pools must be shared among tenants, 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 profiles, you should 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. This guide recommends that they do not; a provider could 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* (https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.security.doc/GUID-52188148-C579-4F6A-8335-CFBCE0DD2167.html), it is important for the management network to be separate 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 it 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.
- It is part of good security practice to 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.
- A syslog server can be set up during installation. We recommend using a TLS-enabled syslog infrastructure. Exporting logs to a syslog server is recommended for multiple reasons. It is recommended that the `syslog` server be configured with redundancy, to ensure essential events are always logged. Security Operations and IT Operations organizations may also benefit from the centralized aggregation and management of diagnostic logs. We recommend that you 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 will ensure you don't lose valuable diagnostic information as the 400MB log file total is reached and files are rotated and deleted.
- Other systems connected to and used by vCloud Director create audit logs that should be consolidated into your audit processes. These include logs from NSX, the vCloud Director database, vCenter Server, and vSphere hosts.
- After the initial local system administrator account is created, it is strongly recommended that all system administrator accounts be managed by an Identity Provider such as LDAP or the vSphere SSO service.
- Some cloud providers may 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, so steps should be taken to limit access only to the vCloud Director cells. One simple way to do that is to configure the LDAP server and/or the external firewall to only allow access from IP addresses that belong to the vCloud Director cells.
- The provider can take steps to protect against this and similar intertenant attacks by both limiting the source IP addresses of requests when possible as well as ensuring that organization names it assigns to tenants are never too similar to one another.

- vCloud Director must be configured to connect to LDAP servers over SSL in order to properly protect the passwords being validated against those servers. When configuring LDAP over SSL, do not accept all certificates.
- Best practices for managing users and their passwords are important to understand and apply.
- Log management, Security Information and Event Management (SIEM), or other monitoring systems, should be used to watch for attempts to crack passwords through brute force attacks.
- It is recommended that system administrators and organization administrators passwords be safely stored in a manner approved by your IT security department.