# Table of Contents

Introduction ................................................................. 5
Threats ........................................................................ 5
   Multitenancy and Internal Threats. ................................. 5
   Secure Hosting and External Threats ............................... 6
VMware® vCloud™ Director Architecture and Security Features .......................... 7
   Virtual Machine Security and Isolation ............................ 7
   Security and the Underlying Virtualization Layer ............... 8
   Security and the VMware vCloud Director Abstraction ........ 8
   Security and the Virtual Networking Layer ...................... 8
      Provider-Level Network Resources ............................ 8
      Organization Network Types ............................... 9
   vApp Networks ......................................................... 9
Infrastructure Hardening .................................................. 9
   Cell Guest OS ......................................................... 9
   Protecting Sensitive Files .......................................... 10
Oracle Database Security ................................................ 10
   Oracle Database User Configuration ............................. 10
   Administrative Database Credentials .............................. 11
Certificates ................................................................. 11
   Configuring vCenter Certificates ................................. 11
   Configuring VMware vCloud Director to Check vCenter Certificates............ 11
   Certificates and Keys for VMware vCloud Director Cells ..................... 12
      Replacing VMware vCloud Director Certificates .................. 12
Network Security — General Topics ................................ 12
   Firewalls (Packet Filtering) ........................................ 12
      Blocking Malicious Traffic .................................... 13
      Blocking JMX and JMS Traffic ................................ 13
Web Application Firewalls .............................................. 14
   Introduction .......................................................... 14
   Why Deploy a WAF? ............................................... 14
   Examples of WAF Rules .......................................... 15
   Remote API Access ............................................... 15
   Vendors and Products ............................................ 15
   Configuration of Public Web URLs and Addresses ............... 15
WAF, Load Balancers and TLSv1.0/SSL Termination .............................. 15
TLS/SSL Termination and Certificates .............................................. 16
X-Forwarded-For Header ............................................................... 16
Securing Access to JMX ................................................................. 16
JMX Authentication ................................................................. 16
Limiting Connections to JMX ......................................................... 16
Securing JMX Communications ..................................................... 17
JMS Message Queue Protection ..................................................... 17
JMS Authentication ................................................................. 17
Network Routing ........................................................................ 18

Network Security for Organizations ............................................. 18
Securing Organization Networks with VLANs and VLAN-backed Network Pools 18
A Brief VLAN Definition ................................................................. 18
VLAN-Backed Network Pools ......................................................... 18
When To Use VLAN-Backed Network Pools .................................. 18
VLAN-Backed Network Pool Setup ............................................... 18
Securing Organization Networks with VMware vCloud Director Network Isolation-Backed Network Pools ................................................................. 19
VMware vCloud Director Network Isolation Definition ......................... 19
VMware vCloud Director Network Isolation-Backed Network Pools ................................................................. 19
When To Use VMware vCloud Director Network Isolation-Backed Network Pools 19
VMware vCloud Director Network Isolation-Backed Network Pool Setup ................................................................. 20

Resource Allocation and Isolation .................................................. 20
Shared Resource Deployment .......................................................... 20
Resource Sharing and Isolation Recommendations .................................. 23
Security Domains and Provider VDCs .............................................. 23
Resource Pools ........................................................................ 23
External Networks ...................................................................... 23
Network Pools ........................................................................ 24
Datastores ............................................................................... 24
Isolating Storage ...................................................................... 24
Management Network Configuration .............................................. 25
Management Network Components .............................................. 25
Virtual Infrastructure Management Network Configuration Requirements ................................................................. 25
Other Related Networks ............................................................... 25
Auditing and Logging .......................................................... 26
  Introduction ...................................................................... 26
  Logging in VMware vCloud Director .............................. 26
  Diagnostic Logging and Log Rollover ......................... 27
  NTP .............................................................................. 27
  Additional Logs .............................................................. 27
User Management and Identities ........................................ 28
  About Users, Groups, Roles, and Rights ..................... 28
  Configuring Identity Sources ....................................... 28
  Naming Service (LDAPv3) Connectivity ....................... 29
  LDAP over TLS/SSL ....................................................... 30
  Importing Groups ......................................................... 30
  User and Credential Management. ......................... 31
    Password Strength .................................................... 31
    User Management ...................................................... 31
    Password Management ............................................ 31
    Other Passwords ....................................................... 31
    User Password Protection ......................................... 32
Checklist ........................................................................ 33
Introduction

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 will describe 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 VMware 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.

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.

In general, threats to VMware 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 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 VMware vCloud Director will be posted there.

Threats

Multitenancy and Internal Threats

VMware vCloud Director is designed to give limited and controlled access to network, computing and storage resources to users who are clients of the cloud. These users can log into the system 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 VMware 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, VMware ESX® access, physical storage locations, and so on—to non administrative users. However, users may 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—intended 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 VMware vCloud Director instance, Organization administrators, administrators of databases and networks,
and users with access rights to hypervisors, to VMware vCenter™, or to 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—and there is a potential threat that they too may attempt privilege escalation or do harmful actions.

As will be seen, the security of VMware vCloud Director from these threats comes from the architecture, design, and implementation of VMware vCloud Director, VMware vSphere™ 4.1 (“vSphere”), vShield, other security systems, and the infrastructure on which these systems are deployed. Due to the flexibility of these systems, like vSphere, following the specific guidance in this and other documents, such as the vSphere Hardening Guidelines, is critical to creating an environment that meets your organization’s specific security needs.

Secure Hosting and External Threats

The sources of external threats are systems and users outside the cloud, including attackers from the Internet against VMware vCloud Director through its APIs, the Web Console (written using Adobe Flex), 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 VMware vCloud Director attempts to enforce. While the deployment of the different layers of the system affect the mitigation of these threats, the externally facing interfaces, including firewalls, routers, VPNs, and so on, are of utmost concern.
VMware vCloud Director Architecture and Security Features

VMware vCloud Director was purpose built to provide Infrastructure as a Service on top of vSphere. Thus the system leverages the secure isolation of virtual machines and virtual networks provided by vSphere. In addition, VMware vCloud Director takes advantage of vShield to provide additional networking controls not found in vSphere. Finally, the VMware vCloud Director architecture enables the multitenant separation at the management and distribution layer required in a cloud environment.

![VMware vCloud Director Architecture](image)

Figure 1. VMware vCloud Director Architecture.

Figure 1 shows a single VMware vCloud Director cluster. Within the cluster there might be many vCloud Director server hosts, each with a single cell running. Together, the cluster shares the vCloud Director Oracle database and an NFS file share (not shown). The cloud abstraction is built using the VMware vCloud Director software and leveraging capabilities in both vCenter and vShield, shown in the diagram as connecting to the cluster. The effect is that Organizations and their users do not interact directly with vCenter and vShield to load and manage their vApps, but only through the vCloud Director. Even when connecting to virtual machines’ consoles (not shown), the VMware vCloud Director software proxies and mediates those connections.

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

Virtual Machine Security and Isolation

When we refer to security and network isolation, we are looking to assess the risk that network segregation 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:

- Demilitarized zones (DMZs)
- Payment-card industry (PCI) cardholder data environment
- Site-specific zones, such as segmentation according to department or function
- Application-defined zones, such as the three tiers of a Web application

Security and the Underlying Virtualization Layer

A significant portion of VMware vCloud Director security, especially in protecting multitenancy from internal threats, comes from the security design and the specific configuration of the underlying virtualization layer. This includes not only vSphere’s design but also the configuration of vSphere, additional security of VMware vCloud Director isolated networks, the leveraging of vShield technology, and the security of the ESX and VMware ESXi™ hosts themselves.

Security and the VMware vCloud Director Abstraction

The VMware vCloud Director abstraction allows 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). While providing these capabilities, the Organization administrators and users do not operate on or manage vCenter or vSphere’s capabilities, like VMware vMotion™. Tenants deal only with deploying vApps to resource pools, datastores, and networks created for and assigned to that 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 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 without explicitly sharing them. (The exception is vApps connected to the same External Network, as they’re sharing the same vSwitch.) Providing Organizations with unique datastores, networks, and resource pools enforces even greater separation between the Organizations through the quotas you can set in those abstractions.

The VMware vCloud Director layer also provides the ability to leverage vShield for network address translation (NAT) and firewalling of networks. This is discussed in more detail in the next section.

Security and the Virtual Networking Layer

How virtual networking in your virtual infrastructure is set up is critical to ensuring the security of VMware vCloud Director in general and isolation of individual tenants in particular. VMware vCloud Director leverages the virtual switches and portgroups set up in the virtual infrastructure when creating Organization Networks (via External Networks and Network Pools). The different types of networks and pools at the VMware vCloud Director layer provide different types of isolation:

Provider-Level Network Resources

These resources are used to create Organization and vApp networks:

- An External Network provides no isolation between virtual machines, vApps, or organizations by design. It is “external” in order to connect to systems outside the cloud. Connecting directly to that network doesn’t give the protection of the other types of networks.
- A VLAN-backed Network Pool provides isolation using VLANs across a vNetwork Distributed Switch.
• A VMware vCloud Director network isolation–backed Network Pool provides isolation by encapsulating Layer 2 packets in other Layer 2 packets (MAC-in-MAC) in the ESX or 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.

• A vSphere portgroup-backed Network Pool does not enforce isolation directly, but is dependent on the portgroups not being connected to the same vSwitches and physical networks. Isolation can be provided at the physical network with VLANs or other mechanisms. Further discussion of this network type is out of the scope for this document.

None of the provider-level network types provide confidentiality if packets are intercepted at the physical network.

Organization Network Types
The following Organization Networks exist and should be used for the following scenarios:

• A public Organization Network is based on an External Network. Machines on this type of network are directly reachable from any network that can route to the underlying vSwitch and portgroup. This type of network would be useful in an enterprise internal cloud when the vApps in the Organization need to be directly reachable and NAT is not necessary.

• A routed private Organization Network connects to an External Network, but sits behind a virtual NAT device. This type of network is useful for Organizations at a cloud service provider that need vApps to connect to the Internet but want to limit their visibility and accessibility from the outside. Firewall rules can also be applied to this type of Network Pool.

• An isolated private Organization Network is useful for vApps that don’t need access to any resources outside of the Organization. No other Organizations or systems outside of VMware vCloud Director can access an Organization’s internal Organization Network.

vApp Networks
A vApp can be connected to a vApp specific network or to an Organization Network.

• A vApp network isolates the virtual machines in that vApp from everything else; in that way, it is like an internal Organization Network, but is only used by that vApp.

• It is possible to “connect” the vApp network to an Organization Network and get access to it via NAT and Firewall protection.

• Connecting to an Organization Network gives the protections of that network.

• Fencing off a vApp allows its virtual machines to connect to Organization Networks without worrying about IP and MAC address conflicts. In addition, additional firewall rules can be added to protect virtual machines in the vApp.

Infrastructure Hardening
Much of this guide is concerned with protecting the VMware vCloud Director cell itself, but overall system security also depends on securing the infrastructure on which it depends.

Administrators should apply the steps recommended in the vSphere Security Hardening Guide to ensure that they have secure installations of vCenter Server and vSphere.

Applying current security patches to the OS, database, and virtual infrastructure before installation is a key step and ongoing monitoring to keep these components at a current patch level is also crucial.

Cell Guest OS
VMware vCloud Director cells run on a Linux-based guest operating system under a non-root user created by the installation script.
Standard security hardening procedures should be applied to the guest OS, 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 OS instance, but it is recommended that you do not do this—widening access to the cell OS may decrease security.

Securing network traffic to the cells will be discussed later.

Protecting Sensitive Files

The `global.properties` and `responses.properties` files, both found under `$VCLOUD_HOME/etc`, are critical files that contain sensitive information. The `responses.properties` file contains responses provided by the administrator when running the configuration script. That file contains an encrypted version of the Oracle database password and system KeyStore passwords. Unauthorized access to that file could give an attacker access to the VMware vCloud Director database with the same permissions as the Oracle user specified in the configuration script. The `global.properties` file also contains encrypted credentials that should not be made accessible to users besides the cell administrator.

The `Installation and Configuration Guide` recommends saving and using the `responses.properties` file when installing VMware vCloud Director on additional server hosts, placing it in a location accessible to all target hosts. That recommendation is enhanced here with the requirement that the file only be made available to authorized individuals. Appropriate access controls should be placed on the “location accessible to all target hosts.” Any backups that are made should be carefully controlled and 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. There will still be a copy on the original server host where it can be retrieved if another host needs to be installed at a later time.

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 VMware vCloud Director software from working. In order for the access controls to properly work, physical and logical access to the VMware 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.

Oracle Database Security

In general, Oracle database security is outside the scope of this document. Like all other systems used in creating your cloud deployment, you are expected to properly secure them per industry best practices. Please refer to guides such as the `Oracle Database Security Checklist`, the `Oracle Database Security Guide`, and similar resources and apply them as appropriate in your environment.

Oracle Database User Configuration

As specified in the “About the VMware vCloud Director Database” section of the `VMware vCloud Director Installation and Configuration Guide`, the Oracle database user account should not be a system administrator. Rather, it should only have the system privileges listed. Please see the above-referenced document for the complete list.

These privileges will allow the user to initialize the database as well as to read and write required data to that database. The 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.
Administrative Credentials

Ensure that any credentials used for administrative access—to the cell, the vCenters, the database, to 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, vCenter, or vShield password will make part or all of the cloud infrastructure nonfunctional until VMware 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 VMware vCloud Director environment, including the VMware vCloud Director cells, the Oracle DB, vCenter servers, and vSphere hosts. 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.

Certificates

vCloud Director uses digital certificates to enable secure communication based on SSL or TLS. Properly deployed, SSL/TLS provides privacy of communication (by using encryption) and also allows clients to verify the authenticity of the server with which they are communicating. Server authentication is necessary to prevent a man-in-the-middle attack, where the client is induced to connect to a server that is spoofing or proxying for the server it is supposed to be communicating with.

The Secure Sockets Layer (SSL) was originally designed by Netscape engineers for the World Wide Web (WWW) environment to provide a secure channel between two machines. More recently this protocol has been standardized by the Internet Engineering Task Force (IETF) and is now referred to as the Transport Layer Security (TLS) standard.

For processing Web requests from a browser or a REST API client, vCloud Director supports version 1.0 of the TLS standard (TLSv1.0) as well as version 3 of the older SSL protocol (SSLv3.0). When vCloud Director acts as a client, for example when it communicates to a vCenter server, it uses TLSv1.0 only. vCloud Director restricts the cipher suites used for encryption to those providing strong security (AES and DES3).

Verification of the server depends on having a certificate installed on the server that is signed by a recognized Certificate Authority (CA) and matches the host to which the client is connecting.

Configuring vCenter Certificates

There are instructions in the Replacing vCenter Server Certificates white paper for replacing vCenter self-signed certificates with certificates signed by a CA. This is highly recommended.

In addition to being signed by a CA, 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. (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 needs in addition a subjectAltName field that matches the host’s IP address. For further details consult the Certificate Authority you are using, or see RFC 5280.)

Once you have created any required certificates and installed them in vCenter, you should verify that vSphere Client is able to connect to the server.

Configuring VMware vCloud Director to Check vCenter Certificates

To configure VMware vCloud Director you need to create a Java KeyStore in JCEKS format that contains the trusted certificate(s) used to sign vCenter certificates. (The vCenter certificates for the individual vCenter servers are not in this store — only the CA certificates that are used to sign them.)
If “cacert.pem” is a CA certificate in PEM format, then you can create a KeyStore “myca.ks” with a command similar to the following:

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

To add another certificate, if desired:

• $ keytool -importcert -keystore myca.ks -storepass password -file cert2.pem -storetype JCEKS

(“keytool” is provided with Oracle’s Java Development Kit.)

Once you have created the KeyStore, log in to VMware vCloud Director as a system administrator. In the System Settings section of the user interface, open the General Settings page and navigate to the end of the page. There you will see a checkbox to “check vCenter Certificates.” Turn this option on. Click the “Browse” button to search for your Java KeyStore. Clicking “Open” in the browse dialog box or double-clicking the file will place the path to the file in the “Trust store” field. Also enter the password for this file (if there is one). Click on “Apply.”

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

Once this option is turned on, all certificates from all vCenters are checked, so every vCenter must have a correct certificate chain and a certificate that matches its FQDN. If it does not, connection to that vCenter will fail. If you have changed certificates after adding vCenters to VMware vCloud Director, then you should force reconnection to the servers by going to the “vCenters” part of the System Administration UI, right-clicking on each vCenter, and make them reconnect.

Certificates and Keys for VMware vCloud Director Cells

VMware vCloud Director cells also use certificates and an associated private key to identify the cell to TLS v1.0 or SSL clients. As for vCenter certificates, these should be signed by a CA and have a CN matching the FQDN of the host on which the cell is installed.

Replacing VMware vCloud Director Certificates

If you did not initially supply CA-signed certificates when you first installed vCloud Director, or if for any reason you later want to replace the VMware vCloud Director certificates, rerun the configure script (/opt/vmware/cloud-director/bin/configure) and when it prompts for the certificate store, provide the path to a new/updated one with the appropriate certificates.

Network Security — General Topics

Firewalls (Packet Filtering)

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 VMware vCloud Director deployment.

VMware vCloud Director cells must be accessible by Organizations’ users — the Organization administrators, Catalog owners, vApp owners, and so on. Those users, in a cloud service provider environment, will be initiating their connections to the Web Console and other interfaces from outside the service provider’s network perimeter. The recommended approach to making VMware vCloud Director services available to the outside is to place the cells in a DMZ, with a network firewall separating the Internet from VMware vCloud Director cells on the DMZ. The only port that needs to be allowed through the Internet facing firewall is 443/TCP.
NOTE: These management connections can be further limited via IP address restrictions in the network (or Web application firewall below) or with per-tenant VPNs. This level of protection may be appropriate in certain deployments, but is outside the scope of this document.

As the VMware 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 Oracle DB, vCenter Server, vSphere hosts, Directory (LDAPv3) directories, and any backup or similar services be on the other side of a firewall that separates the DMZ from the internal network. The ports that must be opened in that firewall are defined in Chapter 1 of the vCloud Director Installation and Configuration Guide, in the Network Security section.

It is also important to keep in mind the firewall requirements of the vSphere infrastructure deployed and used by VMware 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 below) for different uses; each requires network firewall protection.

Virtual machines that need accessibility from outside the cloud (for example, 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 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, but 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 sometimes 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 from the Internet be placed on a private, routed network. This provides the Organization control over firewall and port forwarding rules provided by vShield Edge. This configuration does not eliminate the need for a network firewall to separate the External Network used by these Organization Networks; this is because public Organization Networks do not have any vShield firewall protection. The separate firewall is needed to create a DMZ (this function could be performed by a separate vShield Edge instance, however).

Similarly, a private NAT-routed Organization Network is used for a virtual machine data network that allows virtual machines to access the Internet. As mentioned above, vShield 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.

### Blocking Malicious Traffic

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

1. Dropping packets that appear to originate from nonroutable addresses (IP spoofing)
2. Dropping malformed TCP packets
3. Limiting the rate of requests, especially of SYN requests — to protect against a SYN flood attack (an attempted denial of service)
4. Considering denying outbound traffic from the firewall that does not originate from an incoming request

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.

### Blocking JMX and JMS Traffic

Exposing JMX or JMS traffic outside the private networks meant for cloud management could expose the provider and the Organizations hosted at that provider to security threats. JMX can be used to manage the operation of the VMware vCloud Director cells themselves, exposing potentially sensitive information or impacting system operation. JMS is used by the cells in a cluster to coordinate activities, including vApp upload and download quarantine. Thus, the information in that message queue is sensitive.
No matter how the networks connected to the VMware vCloud Director cells are configured, 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. Attempts to connect to these services from outside that network might very well be malicious in nature.

As noted below in Management Network Configuration and Securing Communication Paths, the cells should be configured, if possible, to not expose these services to the DMZ network at all and to carefully restrict access to those services on the private management network.

**Web Application Firewalls**

**Introduction**

Before we can begin to understand the value of a Web Application Firewall (WAF) in the context of VMware vCloud Director, it is useful to have a general understanding of how malicious hackers can attack a Web site, the format of a typical Hypertext Transport Protocol (HTTP) request, where in the process an attacker can inject his own data, and what the top Web application threats are as defined by the Open Web Application Security Project (http://www.owasp.org/).

If we take a general approach here, a Web user makes a request, via a browser to a resource located on a Web server at a remote location. This request is either a simple uniform resource locator (URL) or a more complex POST or GET request that contains variables that the server can parse and use to create dynamic content to be delivered back to the browser. Because this process needs to work across a wide range of devices, operating systems, browsers, and programs, the request format is highly standardized into a collection of protocols (for example, HTTP, XML, HTTPS, and so on). The question then becomes, how can an attacker gain control over the data passing from a Web browser as it passes to and from the target Web application? The most popular method to do this is via a proxy program that runs on an attacker’s local system. A commonly used proxy program that is useful for this type of in-process data massaging is Burp. To review the complete list that summarizes the Top 10 threats, visit OWASP. Many other threats exist today, all of which are the focus of a WAF.

**What is a WAF?**

A WAF provides information-security technology that is designed to protect Web sites running Web applications from attacks. WAF solutions are capable of preventing attacks that network firewalls and intrusion detection systems cannot. They also do not require modification of the application source code. A WAF solution is like an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) that is designed to only detect and protect against a specific threat. By designating all the Web Application Firewall’s resources to two main protocols (HTTP/HTTPS), the solution can ignore everything but Web-related threats. This includes Operating System-level attacks and third-party application vulnerabilities. Secondly, because a WAF is more focused on a particular problem, it can be designed in several ways that give it more power and insight into what is actually happening on the Web server. As a result, with regard to Web traffic, the heuristics and intelligence of a typical WAF are very sophisticated.

**Why Deploy a WAF?**

A traditional IDS examines packets as they enter a network and uses various pieces of information from these packets to determine if a potential threat exists. Generally, this process involves monitoring for anomalies in the traffic flow and pattern-matching the packets against a known database of threat patterns. Although this functionality is great, it is usually not enough to properly protect a Web server running complex Web applications like VMware vCloud Director.

In summary, a WAF is an extremely valuable security solution because Web applications are too sophisticated for an IDS or IPS to protect. The simple fact that each Web application is unique makes it too complex for a static pattern-matching solution. A WAF is a unique security component because it has the capability to understand what characters are allowed within the context of the many pieces and parts of a Web page.
Examples of WAF Rules
1. Dropping requests that appear to be HTTP but do not conform to HTTP standards such as RFC 2616 and 1945
2. Limiting the size of the HTTP body and headers in requests (VMware vCloud Director also has some size limiting for request bodies)
3. Detecting common attacks such as attempted SQL injection

Remote API Access
VMware vCloud Director has an HTTP accessible REST API that can be used to control most of the functionality of the product from any client (not necessarily a browser) that can send HTTP requests. See the vCloud API Programming Guide for details.

There are three main parts of the API:
1. Features potentially accessible to all authenticated users (subject to permission checks) — these features are under the https://<hostname>/cloud/api/v1.0/URL
2. Features accessible to system and Organization administrators — these features are under the https://<hostname>/cloud/api/v1.0/admin URL
3. Features accessible only to system (provider) administrators — these features are under the https://<hostname>/cloud/api/v1.0/admin/extension URL

Remote access to the API does not presumably present significantly greater risk than remote access to the Flex-based VMware vCloud Director Web client. In fact, both the Web UI used by browser clients and the REST interface used by nonbrowser clients ultimately pass through a common layer in the VMware vCloud Director server and trigger the same access controls. Unauthenticated users cannot even load URLs under /cloud/api, except for login. And once logged in, users are able to see and manipulate only the resources to which they are entitled.

Nevertheless, it may be desired to block remote access to all of the API, or at least to that portion of it used only by system administrators, if you don’t have a legitimate use case for API clients outside of the firewall. This can be done by deploying a reverse proxy or WAF that redirects requests for the URLs under /api (the complete API) or /api/v1.0/admin/extension (the subset exclusive to system administrators) to an error page.

Vendors and Products
Many WAF products exist from many vendors — see http://www.owasp.org/index.php/Web_Application_Firewall for a list. Many of these products combine WAF functionality with other features such as packet filtering and NAT.

Configuration of Public Web URLs and Addresses
The Managing System Settings section of the VMware vCloud Director Administrator’s Guide discusses how and when 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. Beyond the reasons outlined in the guide, there is a security implication to these settings. Specifically, it ensures that IP addresses you did not intend to be exposed to customers stay hidden.

WAF, Load Balancers and TLSv1.0/SSL Termination
Web requests to the VMware vCloud Director UI or the REST API must be made over HTTPS. Requests that arrive as HTTP requests are redirected to an HTTPS URL and must then negotiate a secure connection. See the Certificates section for details of TLS/SSL configuration.

As recommended in the previous section, a WAF should be deployed in front of the VMware vCloud Director cells. In addition, many organizations will deploy a load balancer in front of the cells as well to distribute the load across the cluster. 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 TLSv1.0 or SSL termination: The WAF is configured to complete the TLSv1.0 or SSL handshake with the remote client, using a certificate that it controls.
Even though the interactions with the remote client to the WAF are secured with TLSv1.0 or SSL, it is required that WAF-to-cell communication also be done over HTTPS: An HTTP connection to the cell is not supported.

The following simple diagram, leaving out the load balancer, illustrates the two TLSv1.0 or SSL connections that exist when using TLSv1.0 or SSL termination, one between the user’s computer and the WAF, and one between the firewall and the VMware vCloud Director cell.

![Diagram](image)

**Figure 2.** TLSv1.0/SSL Configuration with WAF.

**TLS/SSL Termination and Certificates**

When configuring TLSv1.0 or SSL termination, it is important not only to install a CA-signed certificate at the 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. Self-signed certificates, even if the WAF accepts them, are only appropriate if each certificate is manually accepted at deployment time; however, this limits the flexibility of the VMware vCloud Director cluster, as each cell must be manually configured (and reconfigured when certificates are renewed).

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

**X-Forwarded-For Header**

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.

X-Forwarded-For is a widely used header — it was first used by Squid, a popular reverse proxy server, but is now supported by many proxies and firewalls. It is recommended that you enable generation of this header at the firewall if possible.

**Securing Access to JMX**

As described in the *vCloud Director Administrator’s Guide*, each vCloud Director service host 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 requires user authentication. The allowed users are VMware vCloud Director system administrator users. System administrators authenticate with the same usernames and passwords used to authenticate to the Web Console and the vCloud API. 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 VMware vCloud Director’s management network. If the VMware vCloud Director server has a third IP address assigned exclusively for management, bind JMX directly to this IP address. By default, the
VMware vCloud Director JMX connector binds to the primary IP addresses configured using the bin/configure script. This 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>
```

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.

The recommended and more secure configuration involves binding the JMX connector to the localhost address:

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

With this setting in `global.properties`, JMX can only be reached from the local VMware 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 only exposed to localhost (127.0.0.1) as recommended above, 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 of the above configuration and JMX must be exposed outside the VMware vCloud Director server, then JMX should be secured with TLS or SSL. TLS and SSL is configured by setting the following environment variable:

```
export VCLOUD_JAVA_OPTS="-Dcom.sun.management.jmxremote.ssl=true -Djavax.net. keyStore=<pathToKeyStore> -Djavax.net.ssl.keyStorePassword=<password> -Djavax.net.ssl.keyStoreType=<storeType>
```

You must then invoke

```
service vmware-vcd restart
```

JMX clients must now connect with SSL, 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 the 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 vCloud, 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.

### JMS Message Queue Protection

JMS is used in VMware vCloud Director to communicate between different cells as well as with any systems supporting the transfer service’s vApp quarantine. As described in the vCloud Director Installation and Configuration Guide, ActiveMQ is the technology used to support JMS. JMS security is provided through authentication and proper routing of messages.

#### JMS Authentication

Access to JMS message queues requires authentication. All vCloud Director users with the system administrator role have the right to these queues. Users or applications requiring access must authenticate with a system administrator username and password.
Network Routing
ActiveMQ uses TCP ports 61611 and 61616 for JMS communication. At this time, JMS is bound to the default IP address of the vCloud Director cell used by the HTTP service, and those messages are not protected by TLS, SSL or other confidentiality mechanisms. It is recommended that the VMware vCloud Director cell is assigned a default IP address that is configured via specific router and/or firewall rules to keep this traffic private to the VMware vCloud Director cluster on the DMZ network.

Network Security for Organizations

Securing Organization Networks with VLANs and VLAN-backed Network Pools

A Brief VLAN Definition
Conceptually, a VLAN, or Virtual Local Area Network, creates a logical group of switch ports through which virtual machines communicate exclusively as if they were physically separate from other machines on other switch ports. This provides a measure of privacy and isolation between machines that share the same switches and networks. In the physical world, VLANs are enforced by physical switches; similarly, in the virtual world, VLANs are enforced by virtual switches. The tricky part, described in more detail below, is that when virtual machines connected to virtual switches need to communicate to other virtual machines on other hosts or other physical machines, the vSphere hosts must be connected to a switch port that supports all VLANs used on that host, typically a VLAN trunk port.

VLANs do not provide cryptographically enforced confidentiality between endpoints, so they are not appropriate in an environment that might require a VPN or TLS (Transport Level Security). Packets tagged for particular VLANs can be intercepted due to misconfiguration, the use of a trunk port, or other physical infrastructure that ignores the VLANs. But VLANs are appropriate for isolation between different Organization Networks in a typical shared-resource cloud environment (see Shared Resource Cloud Service Provider Deployment below), and are a building block of VMware vCloud Director networks in general. The VMware vCloud Director assists in the configuration of consistent VLAN assignments, and vSphere enforces the separation of packets between different VLANs.

VLAN-Backed Network Pools
A VLAN-backed Network Pool is a pool of networks that are based on a range of VLANs and a vNetwork Distributed Switch. The distributed switch should be configured to span all the hosts in the resource pool assigned to the Organization VDC using its associated Network Pool. VMware vCloud Director enforces uniqueness of VLANs assigned to different Network Pools to help enforce isolation between vApps sharing a resource pool. Moreover, specific firewall rules can be assigned to Organization Networks created from Network Pools such as these.

When To Use VLAN-Backed Network Pools
Networks created from VLAN-backed Network Pools are slightly faster than those created from VMware vCloud Director Network Isolation-backed Network Pools, but they require one VLAN per Organization Network created from the pool. For that reason, there may be concerns regarding the use of VLAN-backed Network Pools in an environment where the provider is trying to maximize the number of hosts, organizations, and vApps in the vCenter cluster. In one where the number of Organization and vApp networks is not expected to be large, VLAN-backed Network Pools may be a perfectly appropriate choice. VLANs may also be consumed by the underlying computing and networking fabric, so it is important to pay attention to the total number of VLANs available per cluster.

VLAN-Backed Network Pool Setup
In order for VLAN-backed Network Pools to be set up, a vNetwork Distributed Switch and a range of VLAN IDs must be available. This is clear in the VMware vCloud Director Administration Guide and the Web Console user interface. However, you must also ensure that all VLANs in that range are uniformly available to all hosts in the resource pool to which the vNetwork Distributed Switch is connected. This may be done with trunk ports on the
physical switch to which the hosts are connected, essentially extending the VLAN enforcement from the physical switches to the virtual switches. Finally, the Web Console does not assist the administrator in choosing available VLANs. It only indicates when a range is chosen that is not available. It is recommended that for each resource pool/vNetwork Distributed Switch, the system administrator keeps a list of VLANs that are used by the underlying computing and network infrastructure, which ones are available to the hosts through the physical switching fabric, and which ones have been already assigned to Network Pools assigned to that vNetwork Distributed Switch.

Securing Organization Networks with VMware vCloud Director Network Isolation–Backed Network Pools

VMware vCloud Director Network Isolation Definition
VMware vCloud Director Network Isolation creates, like a VLAN, a logical group of switch ports through which virtual machines communicate exclusively as if they were physically separate from other machines on other switch ports. However, it is not implemented using VLANs. Instead, it is implemented with a kernel-level service in each vSphere host that controls this virtual network. The services make decisions regarding whether packets are destined for the same broadcast domain as their source. If so, they are encapsulated in this virtual network and then de-encapsulated by the destination virtual machine’s host and passed to the right vNIC. If not, the packet is subject to the routing and firewall rules of the Organization Network that uses this pool. It is similar to a switch-enforced VLAN, however, multiple VMware vCloud Director Isolated Networks can coexist using the same VLAN ID without communication leakage.

VMware vCloud Director Network Isolation–Backed Network Pools
A VMware vCloud Director Network Isolation–backed Network Pool is a pool of networks that are based on a vNetwork Distributed Switch and an optional VLAN ID with isolation enforced at the vSphere kernel. The distributed switch should be configured to span all the hosts in the resource pool assigned to the Organization VDC using its associated Network Pool. In addition, specific firewall rules can be assigned to Organization Networks created from Network Pools such as these.

When To Use VMware vCloud Director Network Isolation–Backed Network Pools
While networks created from VMware vCloud Director Network Isolation–backed Network Pools are slightly slower than those created from VLAN-backed Network Pools, they do not require the use of any VLANs. This is an advantage when there are many Organizations, hosts, and vApps assigned to a vCenter cluster and the available number of VLANs is of concern. These types of Network Pools are also useful when it is not feasible to assign large numbers of VLANs (or a trunk port) to the hosts in the cluster. This type of Network Pool is easier to manage, as you don’t need to keep track of large numbers of VLANs and their usage across computing and networking infrastructure. It is thus also easier to lock down the propagation of the optional VLAN to only the hosts that are part of the vNetwork Distributed Switch.

VMware vCloud Director Network Isolation–Backed Network Pool Setup
In order for VMware vCloud Director Network Isolation–backed Network Pools to be set up, a vNetwork Distributed Switch must be available. The use of a VLAN for this pool is optional. This is clear in the VMware vCloud Director Administration Guide and the Web Console user interface. If you use a VLAN, you must also ensure that it is uniformly available to all hosts in the resource pool to which the vNetwork Distributed Switch is connected. While the number of VLANs each host needs access to may be small when using pools such as these, it may still be appropriate, depending on your environment, to make the VLANs available to the hosts using trunk ports on the physical switch to which the hosts are connected, essentially extending the VLAN enforcement from the physical switches to the virtual switches. Other than VLAN and vNetwork Distributed Switch configuration, there is nothing else to be managed to set up pools of this sort.
Resource Allocation and Isolation

Shared Resource Deployment

The standard cloud service provider deployment of VMware vCloud Director envisions the sharing of resources in a Provider VDC among multiple 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.

Figure 3. Physical Deployment Diagram.
Looking at the logical diagram, the left side shows the VMware 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. Configuration of such a VPN is outside the scope of this document.

Behind the cells are the private management elements required by VMware vCloud Director: the Oracle DB, vShield Manager, vCenter Server, the vCloud Director directory server, if any, the Active Directory server used by vCenter, and the management interfaces of the vSphere hosts. 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.

The following figure 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. The specific storage network configuration will be cloud-provider specific.
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 Networks as well as virtual machine data networks for private Organization Networks that may be routed, via a (vShield) firewall to an External Network. The per-tenant VPN for bridging to the enterprise datacenter is meant to represent methods by which vApps can be connected to enterprise users and services not in the Organization VDC. There are many methods for enabling this capability, and a detailed description of the various methods and their configuration is outside the scope of this document.

Figure 6 focuses on the Cloud Pods. It shows four physical networks; however, the Storage Network is specific to the particular hardware and storage technologies chosen. Moreover, it is possible, depending on whether resource pools span pods to eliminate the need for a physical virtual machine data network. In addition, if resource pools span pods, this document recommends a separate physical network for vMotion for security and privacy of that data.
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 VMware 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**

As described above and seen in the diagrams, generally a cloud service provider under normal conditions can share resources among multiple Organizations, including compute, storage, and networking resources. vSphere and VMware vCloud Director enforce isolation through abstraction and secure engineering practices in the hypervisor and the vCloud Director software. Organizations can thus share the underlying resource pools, datastores, and networks exposed through a single Provider VDC without seeing and changing other Organizations’ networks, vApps, and so on. In addition, proper management of leases, quotas, limits, and allocation models can ensure that one Organization cannot deny service to another Organization by accident or on purpose. For example, a very conservative configuration would set up all Organizations 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 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,” not included in this version of the 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 must remain within specific 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 are used to help aggregate and manage CPU and memory resources from the underlying vSphere infrastructure. Segmenting different Organizations across different resource pools in a typical cloud service provider environment is not necessary from a confidentiality and integrity perspective. But from an availability perspective, there may be reasons to segment different Organizations across different resource pools. This resource-management problem depends on allocation models for each Organization, the expected workload, 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.

**External Networks**

Organization Networks, by definition, are unique to an Organization; however, the Network Pools from which they are created and the External Networks to which they connect may be shared.

External Networks are used to create public networks and to connect private, routed networks to other networks. An External Network can be safely shared between multiple public networks, since by definition those networks are public. Customers should be reminded that traffic on External Networks is subject to interception, and they should employ application-level or transport-level security 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 Network in order 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, it is recommended that a vShield Edge appliance (if the provider wants to manage it) or other VPN virtual appliance be deployed in the Organization network. 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.

Organization Networks that don’t allow access to the inside with NAT and IP masquerading can share the same External Network.

**Network Pools**

All (Organization) Networks can share Network Pools as long as the Network Pool is set up correctly such that all networks in the pool are isolated. VLAN-backed Network Pools rely on VLANs being configured properly on the physical and virtual switches to allow connectivity within a VLAN and isolation between different VLANs. VMware vCloud Director Network Isolation-backed Network Pools work similarly to VLANs, but also run under the assumption that no one unprivileged has access to the raw VLAN the Network Pool is running on top of. Portgroup-backed Network Pools must be configured with portgroups that are isolated from each other. These portgroups could be isolated physically, through VLANs or through technologies similar to VLANs.

Of the three types of Network Pools, it is easiest to share a VMware vCloud Director Network Isolation-backed Network Pool. It supports many more networks than a VLAN-backed Network Pool and isolation is enforced at the vSphere-kernel layer. While the physical switches don’t isolate the traffic without the use of the VLAN, it isn’t susceptible to misconfiguration at the hardware layer either. Recall from above that none of these Network Pools provide confidentiality protection for intercepted packets (for example, at the physical layer).

**Datastores**

If datastores are properly configured to be only accessible via vSphere’s management network, then the risk in sharing datastores comes, as for compute resources, with 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. Also carefully choose your storage leases. Alternatively, if you do not share datastores, you must properly allocate storage to each datastore for each Organization, potentially wasting storage by allocating it to Organizations that do not need it. As above, this is a resource-management challenge outside the scope of this document.

**Isolating Storage**

Datastores, whether NFS shares or iSCSI LUNs (logical units), are the logical storage volume presented to users of vSphere and VMware vCloud Director. These VMFS-formatted volumes are where VMDKs are stored. While vSphere administrators can see the physical storage systems from which these datastores are created, that requires specific rights not needed by a cloud administrator or vApp owner. Even if the vCloud Director cell is configured with a user with rights to create new datastores, that privilege is not exposed to the provider system administrator or Organization users. Instead, system administrators enable datastores, disable datastores and assign datastores to Organizations. Organization users that create and upload vApps simply store vApps’ VMDKs on the datastores assigned to the VDC they’re using for those vApps.
For this reason, 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.

Likewise, cloud users only see the datastores assigned to them, but even that view is limited to the vCloud Director abstraction. They cannot browse the datastore. They only see what's published in catalogs or that exist in vApps they manage. If Organizations do not share datastores, they 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.

Management Network Configuration

Management Network Components

The VMware vCloud Director management network, as mentioned above, is a private network that contains the systems for managing the underlying cloud infrastructure as well as access for client systems that perform system administration on VMware vCloud Director. These include the Oracle DB, an NFS server for temporary vApp storage, the vCenter servers, the VMware ESX® Service Consoles/ESXi™ vmkernel interface, an optional LDAPv3 directory for authenticating provider administrators, any LDAPv3 directories maintained by the provider for authenticating Organization users, and vShield managers (one per vCenter server). The vCenter servers on this network also need access to their configured Active Directory servers.

Virtual Infrastructure Management Network Configuration Requirements

As defined in the vSphere hardening guidelines, 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 VMware 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 VMware 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 VMware 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 Organizations’ 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

Introduction

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 is 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.

The system audit log is maintained in the Oracle 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. A more comprehensive view of the audit log (and long-term persistence) is achieved through the use of remote syslog, described in the Logging in VMware vCloud Director subsection below. A variety of log management and Security Information and Event Management (SIEM) systems are available from a variety of vendors and open-source projects.

Diagnostic logs, described below, contain information about system operation not defined as “audit events” and are stored as files in the local filesystem of each cell’s OS.

Logging in VMware vCloud Director

VMware vCloud Director includes two types of logs:

• Diagnostic logs that are maintained in each cell’s log directory
• Audit logs that are maintained in the database, and optionally, in a syslog server

Diagnostic logs can be useful for problem resolution but are not intended to preserve an audit trail of significant system interactions. Each VMware vCloud Director cell creates several diagnostic log files described in the Viewing the vCloud Director Logs section of the VMware vCloud Director Administrator’s Guide.

The audit logs, on the other hand, do record significant actions, including login and logout. As detailed in the vCloud Director Installation Guide, a syslog server can be set up during installation. Exporting logs to a syslog server is recommended for multiple reasons:

1. Database logs are not retained after 90 days, while logs transmitted via syslog can be retained as long as desired.
2. It allows audit logs from all cells to be viewed together in a central location at the same time.
3. It protects the audit logs from loss on the local system due to failure, a lack of disk space, compromise, and so on.
4. It supports forensics operations in the face of problems like those listed above.
5. It is the method by which many log management and Security Information and Event Management (SIEM) systems will integrate with VMware vCloud Director. This allows:
   a. Correlation of events and activities across VMware vCloud Director, vShield, vSphere, and even the physical hardware layers of the stack
b. 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

6. 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.

You must also ensure the proper ports (514/UDP) are open from the VMware vCloud Director host to the syslog server and properly configure the syslog server (which may be part of a larger log management or SIEM solution). 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 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.

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. Specific instructions may be provided in a future Knowledge Base article, similar to what has been written for ESX server in the past (see http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=3402740 for an example).

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

The Installation and Configuration Guide identifies NTP as a requirement for the system running the VMware vCloud Director cell for reasons of DB synchronization. A side benefit of using NTP is that log messages are more easily understood with the correct time, especially when comparing them with activity on other vCloud Director hosts and other systems in your infrastructure. 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 vShield Manager, the Oracle 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.
User Management and Identities

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

About Users, Groups, Roles, and Rights

All users are a member of a single Organization or a provider user. Users are assigned a role, and a role is assigned a set of rights. Users can be local users (only stored in the Oracle database) or LDAP users imported into the database. Users can also be members of one or more groups imported from an LDAP directory, potentially assigning an additional role for each group of which they are a member.

No unauthenticated user is allowed to access any VMware vCloud Director functionality, whether the access is via the vCloud API or the Web UI. Thus, all individuals whom you want to access VMware vCloud Director need to be created as local users in the system, imported from LDAP, or be members of LDAP groups you import into the system. Each user authenticates using a username and password. No other authentication methods are supported in this release of VMware vCloud Director. It may be possible to proxy or layer a stronger authentication method in front of the vCloud API and the Web UI, but such configurations have not been tested by VMware and are not supported.

Groups are not created in VMware vCloud Director; instead, they are imported from the LDAP directory associated with the system (provider) level or Organization. They allow users to authenticate to VMware vCloud Director without the need to create them in the database or manually import them from the Directory (LDAPv3) server. Instead, they can log in if they are a member of a group already imported from the Directory (LDAPv3) server. A user that is a member of multiple groups gets assigned all the roles assigned to those groups.

Roles are groupings of rights that provide capabilities for the user assigned that role. The predefined roles, as described in the Roles and Rights chapter of the VMware vCloud Director Administrator’s Guide, include:

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

The Administrator’s Guide also identifies which rights are assigned to each role. 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 customers’ organizations, so you also have the ability to 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 Sources

For system administrators and Organization users, you have the option of creating local users or importing users from a LDAPv3 directory. It is important to understand the differences between the different user types. Local users are stored in the VMware vCloud Director’s Oracle database with the hashes of their passwords. Those users are authenticated against their hashed entry in the database. Limited management functionality is available: Database users can only be enabled or disabled and assigned to roles. A six-character password minimum is enforced for local database user accounts.
System LDAP users are stored in the LDAP directory configured at the system level, and references to them are imported into the VMware vCloud Director database where 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 directory chosen. If an Organization is configured to use the system LDAP, its users come from the OU specifically configured in that Organization’s VMware vCloud Director System LDAP Service settings.

Organization, or custom, LDAP directories are unique to a specific Organization and can be hosted in the cloud provider’s infrastructure or at the Organization’s enterprise datacenter. A reference to these users too would be imported into the database just as in the above example.

It is strongly recommended that the system administrators and Organization users come from a directory server. At this time, users in the Oracle database are not managed with the password and authentication controls typically available in a directory, including authentication failure controls; password expiration, complexity and history; and integration with enterprise identity management systems. This last bit is worth emphasizing; creating local users adds additional management tasks when users change job functions or leave the company. Instead of managing those users using a single LDAP directory, you must remember to change roles and disable users immediately upon a change in their roles or their termination. As an alternative, an enterprise identity management system can be extended to manage local users via the vCloud Admin API, the details of which are outside the scope of this document. For more information on the vCloud API, see the vCloud API Programming Guide.

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. 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.

Finally, the main documentation set recommends having at least one local user for the system and each Organization so that if LDAP is not accessible, administrators can still access the system. Organizations should carefully weigh the benefits and risks of such an approach. As mentioned earlier, local users do not have password strength or authentication lockout controls. Those users are thus open, if accessible from the Internet, to brute force attacks. The cloud provider should carefully control which source IP addresses can authenticate to an Organization’s cloud URL if local users are configured. Another alternative is the use of the system LDAP or locally hosted LDAP system. If high availability is a concern, an alternative is the use of a replicated LDAP server, fronted by a load balancer, so as to reduce the possibility of the directory becoming unreachable.

**Naming Service (LDAPv3) Connectivity**

Connectivity from the VMware 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 VMware vCloud Director cells, potentially through the enterprise datacenter’s own DMZ (see Shared Resource Cloud Service Provider Deployment above).

In all of these circumstances, opening the appropriate ports through the various firewalls in the path between the cells and the LDAP server is required. By default, this port is 389/TCP for LDAP and 636/TCP for LDAPS; however, this port is customizable with most servers and in the LDAP settings in the Web UI. 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 VMware 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 VMware 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 beware 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. The VMware vCloud Director must be configured to connect to LDAP servers over SSL in order to properly protect the passwords being validated against those servers. In order to do that:

- Select “use SSL” on the LDAP settings screen for the system or on the Custom LDAP screen for the Organization.
- You are given the option to “accept all certificates”; select a certificate, or select a KeyStore.
  - It is recommended that you do NOT choose to accept all certificates. Accepting all certificates removes the system’s ability to authenticate the server and detect whether the LDAP server is being spoofed.
  - It is recommended that you provide the specific certificate of the LDAP server to which you’re connecting. This provides you with the greatest control over which servers the VMware vCloud Director will connect to and trust for authenticating users.
  - You may instead use a JCE KeyStore to specify which certificates you trust; however, a Key Store with lots of CA certificates (or even a lot of specific server certificates) does open you up to misconfiguration errors or simply accepting too many certificates as trusted.

In addition, 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 VMware 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. If the specific signed certificate of the LDAP server is not provided directly in the Web UI, then the certificate of the CA that signs the LDAP server certificate must be imported into the JCE KeyStore configured above. A JCE KeyStore is managed using the keytool command; specific command descriptions are provided with the JRE documentation and not in this document.

**Importing Groups**

The purpose of importing groups into VMware 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 only 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 VMware vCloud Director and assigned to these more privileged roles. For instance, users with a need to create Catalogs could be added to the “Cloud A Catalog Author” group in the Organization’s LDAP server. Then the Organization administrator would import the Cloud A Catalog Author group and map it to the predefined Catalog author role in VMware vCloud Director. This is accomplished by following the Import a Group instructions in the VMware vCloud Director User’s Guide.

User and Credential Management

The management of users and authentication credentials is important to the security of any system. All authentication to and within the VMware vCloud Director system is with usernames and passwords. Thus, best practices for managing users and their passwords are important to understand and apply. This section aims to define the capabilities and limitations of managing users and passwords in VMware vCloud Director and provides recommendations on how to securely manage and use them given those constraints.

Password Strength

The strength of LDAP users’ passwords is dependent on the controls provided by that directory 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 directories and management systems tend to support similar capabilities. The details of password strength controls are directory specific and aren’t covered here in more detail.

Local users in VMware vCloud Director are required to have passwords of at least six characters in length. However, that setting is not configurable, nor are there other complexity or history controls available. A tool built on top of the vCloud API could enforce stricter controls, but no details are provided here on constructing such a tool. 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 Management

Many LDAP-accessible directories support, in addition to user add and delete functionality, the ability to enable, disable, lock, and unlock users. Typically, user lockout occurs as the result of a user authentication failure threshold being reached, and users are unlocked either manually or automatically after a configurable time delay. This helps prevent brute force attacks against users’ passwords. The enable and disable functionality is typically used when a user temporarily leaves a project or after they leave the project/company but before the resources they own have been transferred to another user’s control.

Local users can be enabled and disabled. There is no lockout feature for these users, so that must be taken into consideration when exposing authentication interfaces to the Internet. In addition, 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.

Password Management

Some directory servers 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. There is no capability native to VMware vCloud Director to handle this situation. It is recommended that system administrators’ and Organization administrators’ 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.

Other Passwords

VMware vCloud Director maintains passwords for the users that the system logs in to the Oracle database and connected vCenter servers and vShield managers. If any of those users’ passwords change, they are not automatically updated in the system. You will need to manually change those passwords using the vCloud Director configuration script for the Oracle database password or the Web UI for the vCenter and vShield passwords.
User Password Protection

LDAP users’ passwords are stored in the LDAP directories. They are never stored in the vCloud Director database. They are transmitted using the method chosen in LDAP configuration. It is recommended that you use SSL and, if available on the target directory, Kerberos.

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

The vCloud Director also maintains passwords for accessing the private keys associated with its TLS/SSL certificates as well as the passwords to the Oracle database, vCenter servers, and vShield 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 earlier in this document, carefully protect any backups that contain that file.
Checklist

• 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 VMware vCloud Director will be posted there.

• Administrators should apply the steps recommended in the vSphere Security Hardening Guide to ensure that they have secure installations of vCenter Server and vSphere.

• Apply current security patches to the OS, 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 guest OS, 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 OS instance, but it is recommended that you do not do this—widening access to the cell OS may decrease security.

• Make the file available only to authorized individuals. Appropriate access controls should be placed on the “location accessible to all target hosts.” Any backups that are made should be carefully controlled and 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 VMware 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.

• Please refer to guides such as the Oracle Database Security Checklist, and the Oracle Database Security Guide.

• The 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 vCenters, the database, to firewalls and other devices—follow standards for adequate password complexity.

• It is important from a “defense in depth” perspective to vary the administrative passwords for the different servers in the VMware vCloud Director environment, including the VMware vCloud Director cells, the Oracle DB, vCenter servers, and vSphere hosts.

• There are instructions in the Replacing vCenter Server Certificates white paper for replacing vCenter self-signed certificates with certificates signed by a CA. 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 VMware 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 VMware vCloud Director services available to the outside is to place the cells in a DMZ, with a network firewall separating the Internet from VMware vCloud Director cells on the DMZ. The only port that needs to be allowed through the Internet-facing firewall is 443/TCP.
• As the VMware 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 Oracle DB, vCenter Server, vSphere hosts, Directory (LDAPv3) directories, 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 need accessibility from outside the cloud (for example, 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 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 Organization control over firewall and port forwarding rules provided by vShield Edge.

• 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.

• Nevertheless, it may be desired to block remote access to all of the API, or at least to that portion of it used only by system administrators, if you don’t have a legitimate use case for API clients outside of the firewall. This can be done by deploying a reverse proxy or WAF that redirects requests for the URLs under /api (the complete API) or /api/v1.0/admin/extension (the subset exclusive to system administrators) to an error page.

• 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.

• As recommended in the previous section, a WAF should be deployed in front of the VMware 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 v1.0 or SSL termination.

• When configuring TLS v1.0 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 this header at the firewall if possible.

• If the VMware vCloud Director server has a third IP address assigned exclusively for management, bind JMX directly to this IP address. By default, the VMware vCloud Director JMX connector binds to the primary IP addresses configured using the bin/configure script. This 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 (127.0.0.1) as recommended above, 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 of the above configuration and JMX must be exposed outside the VMware vCloud Director server, then JMX should be secured with TLS or SSL.

• Behind the cells are the private management elements required by VMware vCloud Director: the Oracle database, vShield Manager, 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 VMware 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 Organization cannot deny service to another Organization 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 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.

• Sometimes, an External Network may be used by an Organization Network in order 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.

• 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, it is recommended that a vShield Edge appliance (if the provider wants to manage it) or other VPN virtual appliance be deployed in the Organization network.

• If Network Pools must be shared, it is safest to share a VMware vCloud Director Network Isolation–backed Network Pool. It supports many more networks than a VLAN-backed Network Pool and isolation is enforced at the vSphere-kernel layer.

• If you share datastores, you should set a storage limit, enable thin provisioning if possible, and monitor storage usage carefully. Also carefully choose your 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 the vSphere hardening guidelines, 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 Organizations’ 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 Organizations’ 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. 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 the diagnostic logs mentioned above.

• 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. 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 vShield Manager, the Oracle database, vCenter Server, and vSphere hosts.

• It is strongly recommended that the system administrators and Organization users come from a directory server.

• 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, an Organization should only use a private LDAP directory that they themselves host and manage.

• The main documentation set recommends having at least one local user for the system and each Organization so that if LDAP is not accessible, administrators can still access the system. Organizations should carefully weigh the benefits and risks of such an approach. Local users do not have password strength or authentication lockout controls. Those users are thus open, if accessible from the Internet, to brute force attacks. The cloud provider should carefully control which source IP addresses can authenticate to an Organization’s cloud URL if local users are configured. Another alternative is the use of the system LDAP or locally hosted LDAP system. If high availability is a concern, an alternative is the use of a replicated LDAP server, fronted by a load balancer, so as to reduce the possibility of the directory becoming unreachable.

• 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 VMware 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 VMware vCloud Director cells as reported by the cloud provider.
• 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 are never too similar to one another.

• The VMware vCloud Director must be configured to connect to LDAP servers over SSL in order to properly protect the passwords being validated against those servers.

• It is recommended that you do NOT choose to accept all certificates.

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

• It is recommended that any users, especially system and Organization administrators, take great care in choosing their passwords to protect against brute force attacks.

• 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.