

# VMware Cloud Director Availability Security Guide

26 NOV 2020

VMware Cloud Director Availability 4.1

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

<https://docs.vmware.com/>

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

Copyright © 2018-2020 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

# Contents

- 1** What is VMware Cloud Director Availability Security Guide 4
- 2** VMware Cloud Director Availability Services 5
- 3** VMware Cloud Director Availability Configuration Files 8
- 4** VMware Cloud Director Availability Security Configuration Properties 9
- 5** VMware Cloud Director Availability Logs 12
- 6** VMware Cloud Director Availability Users and Sessions 16
- 7** VMware Cloud Director Availability Network Connectivity 20
- 8** VMware Cloud Director Availability License and EULA Files 21
- 9** VMware Cloud Director Availability Updates 22

# What is VMware Cloud Director Availability Security Guide

# 1

*VMware Cloud Director Availability Security Guide* provides a reference to the security features in VMware Cloud Director Availability.

To aid with protecting the VMware Cloud Director Availability installation, *VMware Cloud Director Availability Security Guide* describes the security features in VMware Cloud Director Availability and the measures to take to protect the disaster recovery infrastructure from threats.

- External interfaces, ports, and services that are required for the correct operation of VMware Cloud Director Availability.
- Configuration settings with security implications.
- Location and purpose of log files.
- Required system accounts.
- How to obtain the latest security updates.

## Intended Audience

*VMware Cloud Director Availability Security Guide* is intended for cloud architects, infrastructure administrators, cloud administrators, and cloud operators using VMware Cloud Director Availability in a disaster recovery environment that complies with the requirements for capacity, scalability, business continuity, and disaster recovery. VMware software familiarity is required. *VMware Cloud Director Availability Security Guide* introduces security and compliance as it relates to the VMware Cloud Director Availability solution.

# VMware Cloud Director Availability Services

## 2

The services of VMware Cloud Director Availability can coexist on one virtual appliance or on dedicated appliances.

VMware Cloud Director Availability services provide dedicated management interfaces for configuration and administration.

The operation of VMware Cloud Director Availability depends on the following services that run on the listed VMware Cloud Director Availability virtual appliances.

**Table 2-1. VMware Cloud Director Availability Services**

Service Name	Service Description
Replicator Service	One or more service instances manage the vSphere Replication Server and LWD Proxy services and expose the low-level HBR primitives as a REST API. Operate with vCenter Server-level concepts like VMs, folders, datastores. Replicator Service operates in the following VMware Cloud Director Availability appliances: <ul style="list-style-type: none"><li>■ Cloud Replicator Appliance</li><li>■ Combined Appliance</li><li>■ VMware Cloud Director Availability On-Premises Appliance</li></ul>
Manager Service	A service that operates with vCenter Server-level concepts for managing the replication workflow and manages the Replicator Service instances by using REST API calls. Manager Service operates in the following VMware Cloud Director Availability appliances: <ul style="list-style-type: none"><li>■ Cloud Replication Management Appliance</li><li>■ Combined Appliance</li></ul>

**Table 2-1. VMware Cloud Director Availability Services (continued)**

Service Name	Service Description
Cloud Service with an embedded VMware Cloud Director Availability Tenant Portal	<p>Provides the main interface for replication operations. Operates with VMware Cloud Director-level concepts, with vApps and virtual machines. Manages the Manager Service by using REST API calls.</p> <p>The embedded VMware Cloud Director Availability Tenant Portal provides the tenants and the service providers of the VMware Cloud Director Availability Provider Portal with a graphic user interface to operate with VMware Cloud Director Availability.</p> <p>Cloud Service operates in the following VMware Cloud Director Availability appliances:</p> <ul style="list-style-type: none"> <li>■ Cloud Replication Management Appliance</li> <li>■ Combined Appliance</li> </ul>
Tunnel Service	<p>Orchestrates a secure tunnel creation and as a single point channels the incoming and outgoing site traffic, both management and replication data (LWD) traffic. Tunnel Service operates in the following VMware Cloud Director Availability appliances:</p> <ul style="list-style-type: none"> <li>■ Cloud Tunnel Appliance</li> <li>■ Combined Appliance</li> <li>■ VMware Cloud Director Availability On-Premises Appliance</li> </ul>

**Table 2-2. Replication Services**

Service Name	Service Description
vSphere Replication Server with vSphere Replication Filter	<p>Manages low-level replication operations, creates replication instances, and others. Receives and records the delta information for each replicated workload. During a replication, only the delta information is sent from the source site ESXi host to the destination site ESXi host. vSphere Replication Server operates in the following VMware Cloud Director Availability appliances:</p> <ul style="list-style-type: none"> <li>■ Cloud Tunnel Appliance</li> <li>■ Combined Appliance</li> <li>■ VMware Cloud Director Availability On-Premises Appliance</li> </ul>
Lightweight Delta Protocol Service (LWD Proxy)	<p>A proprietary replication protocol service that manages the encryption, compression, and traffic monitoring of the replication traffic. Verifies that each incoming replication data stream comes only from the authorized source LWD Proxy instance. Also verifies that each outgoing replication data stream goes only to an authorized destination LWD Proxy instance. LWD Proxy operates in the following VMware Cloud Director Availability appliances:</p> <ul style="list-style-type: none"> <li>■ Cloud Tunnel Appliance</li> <li>■ Combined Appliance</li> <li>■ VMware Cloud Director Availability On-Premises Appliance</li> </ul>

The following additional services run on all the VMware Cloud Director Availability virtual appliances.

Table 2-3. Additional Services

Service Name	Service Description
sshd	A standard Linux service that provides Secure Shell (SSH) access on port 22 to the VMware Cloud Director Availability appliances. By default, this service is disabled. After explicitly enabling SSH during deployment or in the vCAv portal, this service is enabled and started. Only the <b>root</b> user is allowed to authenticate. After 3 unsuccessful login attempts, the <b>root</b> user account is locked for 15 minutes.
systemd-timesyncd	A standard Linux service that provides the NTP time management. Use the vCAv Portal to configure the NTP server. This service is always running.
vaos	A VMware service for guest OS initialization, operating VMware infrastructure settings. For example, network settings, hostname settings, creating ssh keys, running boot scripts, accepting EULA, and others. This service runs when the appliance boots.
h4postgresql	An embedded PostgreSQL server, that only listens on the local loopback device. You cannot use an external database and you cannot expose the embedded database externally. This service is always running.

# VMware Cloud Director Availability Configuration Files

## 3

VMware Cloud Director Availability services use the following configuration files.

To apply changes in the configuration files, restart the affected service by using the service management interface, or in an SSH session, run the following command.

```
systemctl restart <SERVICE>
```

Service	System Unit	System Unit Location	Configuration File Location
Replicator Service	replicator	/lib/systemd/system/ replicator.service	/opt/vmware/h4/replicator/config/ application.properties
Manager Service	manager	/lib/systemd/system/ manager.service	/opt/vmware/h4/manager/config/ application.properties
Cloud Service	cloud	/lib/systemd/system/ cloud.service	/opt/vmware/h4/cloud/config/ application.properties
Tunnel Service	tunnel	/lib/systemd/system/ tunnel.service	/opt/vmware/h4/tunnel/config/ application.properties
vSphere Replication Server	hbrsrv	/usr/lib/systemd/ system/ hbrsrv.service	/etc/vmware/hbrsrv.xml
Lightweight Delta Protocol Service	lwdproxy	/lib/systemd/system/ lwdproxy.service	/opt/vmware/h4/lwdproxy/conf/ lwdproxy.properties
PostgreSQL database server	h4postgresql	/lib/systemd/system/ h4postgresql.service	/opt/vmware/h4/db/postgresql.conf

**Note** The resources that relate to security operate with the required OS permissions and ownership. Do not attempt to change the ownership or permissions of these files.



# VMware Cloud Director Availability Security Configuration Properties

## 4

Configuration properties that relate to security can be modified in the service configuration files.

In the VMware Cloud Director Availability service configuration files, you can modify the following security-related properties.

Property Name	Default Value	Description
<code>session.timeout</code>	1800000	<p>The time in milliseconds to keep inactive sessions active.</p> <p>Each HTTP request resets the timer.</p> <p>The default value is 30 minutes.</p> <p>Applies to the following services:</p> <ul style="list-style-type: none"><li>■ Replicator Service</li><li>■ Manager Service</li><li>■ Cloud Service</li><li>■ Tunnel Service</li></ul>
<code>session.maxage</code>	86400000	<p>The maximum session length in milliseconds.</p> <p>Even if the session is kept alive, after the time specified in this property, the session is terminated.</p> <p>This property prevents attacks based on stolen session cookies.</p> <p>The default value is 24 hours.</p> <p>Applies to the following services:</p> <ul style="list-style-type: none"><li>■ Replicator Service</li><li>■ Manager Service</li><li>■ Cloud Service</li><li>■ Tunnel Service</li></ul>

Property Name	Default Value	Description
<code>https.endpoint.protocols</code>	TLSv1.2	<p>Corresponds to <code>sslEnabledProtocols</code> in Apache Tomcat.</p> <p>For more information, see <a href="#">Configuration Reference</a> in the Apache Tomcat documentation.</p> <p>Applies to the following services:</p> <ul style="list-style-type: none"> <li>■ Replicator Service</li> <li>■ Manager Service</li> <li>■ Cloud Service</li> <li>■ Tunnel Service</li> </ul>
<code>https.endpoint.ciphers</code>	<p>An example that excludes DH:</p> <p>HIGH:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!kRSA:!DH</p>	<p>Corresponds to <code>ciphers</code> from <code>SSLHostConfig</code> in Apache Tomcat.</p> <p>For more information, see <a href="#">Configuration Reference</a> in the Apache Tomcat documentation.</p> <p>Applies to the following services:</p> <ul style="list-style-type: none"> <li>■ Replicator Service</li> <li>■ Manager Service</li> <li>■ Cloud Service</li> <li>■ Tunnel Service</li> </ul>
<code>vcd.hostnameverifier.noop</code>	false	<p>When set to true, skips the verification of the host name of VMware Cloud Director when establishing a TLS session.</p> <p>Used to prevent an SSL error when the VMware Cloud Director certificate subject or its list of SANs does not contain the provided VMware Cloud Director address.</p> <p>Applies only to Cloud Service.</p>

Property Name	Default Value	Description
<code>web.cors.allowedOrigins</code>	(empty string)	<p>A list of origins (Cross-Origin Resource Sharing (CORS)) that are allowed to access the web resources.</p> <p>Applicable when operating a custom web server serving the plug-in with an iframe.</p> <p>The default value does not allow any origins, but due to the integrated user interface plug-in, Cloud Service implicitly allows requests from VMware Cloud Director.</p> <p>Applies to the following services:</p> <ul style="list-style-type: none"> <li>■ Replicator Service</li> <li>■ Manager Service</li> <li>■ Cloud Service</li> <li>■ Tunnel Service</li> </ul>
<code>admin.allow.from</code>	(empty string)	<p>Controls the source IP addresses that are allowed to establish server sessions. In a production environment, disable the root access authentication from Tunnel Service, as requests come from the Internet.</p> <p>The default value states: if the service has tunneling configuration set, reject tunnel requests, otherwise allow all.</p> <p>Applies to the following services:</p> <ul style="list-style-type: none"> <li>■ Replicator Service</li> <li>■ Manager Service</li> <li>■ Cloud Service</li> <li>■ Tunnel Service</li> </ul>

# VMware Cloud Director Availability Logs

# 5

The log files that contain system messages are located in the VMware Cloud Director Availability virtual appliances.

Each VMware Cloud Director Availability service uses a separate log file, located in the following folders in the VMware Cloud Director Availability appliances.

Service	Default Location	Description
Replicator Service	/opt/vmware/h4/replicator/log/replicator.log	Contains application-specific logs and security-related messages.
	/opt/vmware/h4/replicator/log/requests.log	When activated, contains HTTP request and response data like URL, response code, and timing entries.
Manager Service	/opt/vmware/h4/manager/log/manager.log	Contains application-specific logs and security-related messages.
	/opt/vmware/h4/manager/log/requests.log	When activated, contains HTTP request and response data like URL, response code, and timing entries.
Cloud Service	/opt/vmware/h4/cloud/log/cloud.log	Contains applicationvmware/var/log/-specific logs security-related messages.
	/opt/vmware/h4/cloud/log/requests.log	When activated, contains HTTP request and response data like URL, response code, and timing entries.

Service	Default Location	Description
Tunnel Service	/opt/vmware/h4/tunnel/log/tunnel.log	Contains entries with the source or destination IP and the source or destination port for newly established TCP connections to and from the Tunnel Service.
	/opt/vmware/h4/tunnel/log/requests.log	When activated, contains HTTP request and response data like URL, response code, and timing entries.
vSphere Replication Server	/var/log/vmware/hbrsrv.log	The log file of the HBR server. Useful for troubleshooting NFC errors other problems.
Upgrade Logs	■ /opt/vmware/var/log/vami/vami.log	Contain upgrade log entries.
	■ /opt/vmware/var/log/vami/updatecli.log	

**Note** The resources that relate to security operate with the required OS permissions and ownership. Do not attempt to change the ownership or permissions of these files.

## Log Messages Related to Security

- Attempting to log in by using an incorrect password for the **root** user account of the appliance shows the following log output.

```
2019-10-22 08:48:29.949 WARN - [3c08455a-343d-46d8-a21b-beefcc0a93fa_9V] [https-jsse-nio-8046-exec-10] c.v.h.c.system.AppliancePasswordHelper : stderr: Unable to authenticate root.

2019-10-22 08:48:29.950 WARN - [3c08455a-343d-46d8-a21b-beefcc0a93fa_9V] [https-jsse-nio-8046-exec-10] c.v.h.c.system.AppliancePasswordHelper : Incorrect appliance password received!

2019-10-22 08:48:29.953 ERROR - [3c08455a-343d-46d8-a21b-beefcc0a93fa_9V] [https-jsse-nio-8046-exec-10] c.v.h4.common.config.SecurityConfig : An unauthorized POST request from 127.0.0.1 port 46406 to /sessions failed.

org.springframework.security.authentication.BadCredentialsException: Login failed

    at
com.vmware.spring.security.creds.generic.CredentialsAuthenticationProvider.authenticate(CredentialsAuthenticationProvider.java:84)

    at
com.vmware.h4.cloud.security.VcloudCredentialsProvider.authenticate(VcloudCredentialsProvider.java:40)

    at
org.springframework.security.authentication.ProviderManager.authenticate(ProviderManager.java:175)
```

```

        at
com.vmware.spring.security.creds.JsonCredentialsAuthenticationFilter.attemptAuthentication(JsonCre
dentialsAuthenticationFilter.java:140)

        at
org.springframework.security.web.authentication.AbstractAuthenticationProcessingFilter.doFilter(Ab
stractAuthenticationProcessingFilter.java:212)

```

- Attempting to log in from the Internet by using the **root** user account of the appliance shows the following log output.

```

2019-10-22 08:51:19.245 ERROR - [6d57eddb-a9d7-4f85-8fec-98503d912c7e_JK] [https-jsse-nio-8043-
exec-10] c.v.spring.security.SourceIpAuthorizer : Authorization by source IP failure: the
client IP 127.0.0.1 did not match the rule Rule{ != 127.0.0.1 }

```

- Attempting to log in by using incorrect single sign-on user credentials shows the following log output.

```

2019-10-22 08:51:59.292 ERROR - [337a5316-56d7-4a28-8991-8391leadbdc9_9W] [https-jsse-nio-8046-
exec-3] c.v.h4.common.config.SecurityConfig : An unauthorized POST request from 127.0.0.1
port 46430 to /sessions failed.

org.springframework.security.authentication.BadCredentialsException: Login failed

        at
com.vmware.spring.security.creds.SsoCredentialsAuthenticationProvider.authenticate(SsoCredentialsA
uthenticationProvider.java:101)

        at
com.vmware.h4.cloud.security.VcloudSsoCredentialsProvider.authenticate(VcloudSsoCredentialsProvide
r.java:44)

        at
org.springframework.security.authentication.ProviderManager.authenticate(ProviderManager.java:175)

        at
com.vmware.spring.security.creds.JsonCredentialsAuthenticationFilter.attemptAuthentication(JsonCre
dentialsAuthenticationFilter.java:140)

        at
org.springframework.security.web.authentication.AbstractAuthenticationProcessingFilter.doFilter(Ab
stractAuthenticationProcessingFilter.java:212)

        ...

Caused by: com.vmware.vlsi.client.sso.SsoException:
com.vmware.vim.sso.client.exception.AuthenticationFailedException: Provided credentials are not
valid.

        at com.vmware.vlsi.client.sso.SsoException.toSsoEx(SsoException.java:34)

        at com.vmware.vlsi.client.sso.StsService.acquireBearerToken(StsService.java:90)

```

```

        at com.vmware.vlsi.client.sso.StsService.acquireBearer(StsService.java:82)

        at
com.vmware.spring.security.creds.SsoCredentialsAuthenticationProvider.authenticate(SsoCredentialsA
uthenticationProvider.java:96)

```

- Certificate mismatch after replacing the certificate of a VMware Cloud Director Availability service. The following log output shows a remote cloud site attempting to connect to the local cloud site, when trust is established with the old certificate.

```

2019-10-22 09:00:29.748 WARN - [cd88c84a-be07-4ae2-8150-1ba9a3806ad8_Ah] [https-jsse-nio-8046-
exec-1] com.vmware.h4.cloud.peer.PeerRepo : Unrecognized peer certificate:
SHA-256:DC:8F:7E:F9:64:EF:45:A8:2A:EF:C1:71:E8:03:83:6C:B7:9F:F8:80:86:03:D9:2C:4E:51:E6:1F:B6:9F:
BB:10

2019-10-22 09:00:29.749 ERROR - [cd88c84a-be07-4ae2-8150-1ba9a3806ad8_Ah] [https-jsse-nio-8046-
exec-1] c.v.h4.common.config.SecurityConfig : An unauthorized GET request from 172.16.198.49
port 46872 to /diagnostics/peer-health failed.

org.springframework.security.authentication.BadCredentialsException: Unrecognized client
certificate

        at
com.vmware.spring.security.clientcert.ClientCertAuthenticationProvider.authenticate(ClientCertAuth
enticationProvider.java:47)

        at
com.vmware.h4.cloud.peer.PeerClientCertAuthenticationProvider.authenticate(PeerClientCertAuthentic
ationProvider.java:65)

        at
org.springframework.security.authentication.ProviderManager.authenticate(ProviderManager.java:175)

        at
com.vmware.spring.security.clientcert.impersonate.ImpersonatingClientCertFilter.attemptAuthenticat
ion(ImpersonatingClientCertFilter.java:45)

        at
org.springframework.security.web.authentication.AbstractAuthenticationProcessingFilter.doFilter(Ab
stractAuthenticationProcessingFilter.java:212)

        ...

```

# VMware Cloud Director Availability Users and Sessions

## 6

VMware Cloud Director Availability uses the following users and establishes the followings sessions.

### VMware Cloud Director Availability Appliance **root** User Account

VMware Cloud Director Availability uses the **root** user account for access to both the virtual appliance console and the management interface. The initial deployment of each VMware Cloud Director Availability appliance sets up this account. The **OVF Deployment** wizard requires an initial password for the **root** user account, with an initial requirement being over three characters long. After the initial deployment, VMware Cloud Director Availability forces changing this initial password on the first login by using the **root** user, with the following requirements for the persistent **root** user account password.

- The password must be over eight characters.
- The password must contain digits, upper and lower case letters, and non-alphabetic characters.
- The password cannot match any previous password.
- The password must contain more than four new characters compared to the previous password.



## VMware Cloud Director Availability Users

VMware Cloud Director Availability distinguishes administrator users from regular users. To establish a user session with administrator rights, the credentials for both the source and the destination sites must belong to the **ADMINISTRATORS** or **VRADMINISTRATORS** group. For example, the single sign-on user **Administrator@vsphere.local** is a member of the **ADMINISTRATORS** group.

- Service providers manage VMware Cloud Director Availability objects and the local VMware Cloud Director Availability appliances after authenticating as VMware Cloud Director **System Administrator** users. By default, the **System Administrator** role has all VMware Cloud Director rights. Users belonging to that role can manage any local and monitor any remote VMware Cloud Director Availability inventory object. To manage VMware Cloud Director Availability objects in the remote site, authenticate as a **System Administrator** to the remote site.
- Tenant users perform disaster recovery operations and manage local VMware Cloud Director Availability objects after authenticating as VMware Cloud Director **Organization Administrator** users. These users can perform disaster recovery operations in the local site, can manage any local VMware Cloud Director Availability object, and can monitor any remote VMware Cloud Director Availability object that belongs to the VMware Cloud Director organization. To manage remote VMware Cloud Director Availability objects, authenticate as an **Organization Administrator** user to the remote site.

VMware Cloud Director publishes the predefined global tenant roles and the rights they contain to all organizations. **System Administrator** users can modify the rights and the global tenant roles from individual organizations. **System Administrator** users can modify, create, or remove predefined global tenant roles.

For more information, see [System Administrator Rights](#) and [Rights in Predefined Global Tenant Roles](#) in the VMware Cloud Director documentation.

For tenant roles, different than the default **Organization Administrator**, at minimum grant exactly the following rights in VMware Cloud Director:

- General: Administrator Control
- vApp: Edit VM Properties
- vApp: Delete
- vApp: Edit VM Network
- vApp: Edit Properties
- vApp: Power Operations
- vApp: View VM metrics
- vApp: View ACL
- Organization: View

- Organization Network: View
- Organization vDC Network: View
- Organization vDC Compute Policy: View
- Organization vDC: View ACL
- Access All Organization VDCs
- Catalog: View Private and Shared Catalogs
- Catalog: View ACL
- Organization vDC Named Disk: Delete
- Organization vDC Named Disk: Create
- Organization vDC Named Disk: View Properties
- Organization vDC Named Disk: Edit Properties

**Note** VMware Cloud Director Availability requires each and all of the above rights for the correct operation of the tenant user.

## VMware Cloud Director Availability Users Sessions Extension

Each VMware Cloud Director Availability user session must have a VMware Cloud Director user and a VMware Cloud Director organization associated with the session.

For more information about the sessions and authenticating to remote sites, see [Extended Session Authentication](#) in the *VMware Cloud Director Availability User Guide*.

See the Cloud Service disaster recovery operations that require an extension of the user session in the following table:

Operation	Incoming Replication		Outgoing Replication	
	Required Session on Source Site	Required Session on Destination Site	Required Session on Source Site	Required Session on Destination Site
start	Yes	Yes	Yes	Yes
stop	No	Yes	Yes	Yes
reconfigure	No	Yes	Yes	Yes
failover	No	Yes	Yes	Yes
migrate	Yes	Yes	Yes	Yes
sync	No	Yes	Yes	Yes
pause	No	Yes	Yes	Yes
resume	No	Yes	Yes	Yes
reverse	Yes	Yes	Yes	Yes

<b>Operation</b>	<b>Incoming Replication</b>		<b>Outgoing Replication</b>	
	<b>Required Session on Source Site</b>	<b>Required Session on Destination Site</b>	<b>Required Session on Source Site</b>	<b>Required Session on Destination Site</b>
failover test	No	Yes	Yes	Yes
failover test cleanup	No	Yes	Yes	Yes

# VMware Cloud Director Availability Network Connectivity

# 7

Allow the required TCP access in the site for the correct operation of VMware Cloud Director Availability services.

For a list of the required open firewall ports, see [Cloud-Director Availability Network Ports](#).

## Services Connectivity

VMware Cloud Director Availability services must be able to communicate with each other and with the disaster recovery infrastructure.

- The Cloud Service must have a TCP access to the Manager Service, to VMware Cloud Director, to vCenter Server, and to Platform Services Controller, depending on where the vCenter Server Lookup service is hosted.
- The Manager Service must have a TCP access to all the Replicator Services in both local, and in remote sites and to the vCenter Server Lookup service.
- All the Replicator Services must have a TCP access to the Manager Service, to vCenter Server, and to the vCenter Server Lookup service.

---

**Note** The VMware Cloud Director Availability services use end-to-end encryption for the communication across sites. For example, when a Replicator Service on site 1 is communicating to a Replicator Service on site 2, VMware Cloud Director Availability expects that the TLS session is terminated at each Replicator Service.

VMware Cloud Director Availability does not support any TLS terminating products or solutions placed between the appliances, for example, HAProxy, Nginx, Fortinet, and others. If such tools are in place, they must be configured in pass-thru mode, also known as TCP mode, to prevent from interfering with the TLS traffic of VMware Cloud Director Availability.

---

For more information and a network diagram that shows the connectivity between all VMware Cloud Director Availability components, see *Network Requirements* in *VMware Cloud Director Availability Installation, Configuration, and Upgrade Guide in the Cloud* and in *VMware Cloud Director Availability Installation, Configuration, and Upgrade Guide On-Premises*.

# VMware Cloud Director Availability License and EULA Files



The VMware Cloud Director Availability open-source license and the end-user license agreement (EULA) files are located in the VMware Cloud Director Availability virtual appliances.

In the VMware Cloud Director Availability appliance, you can find the license agreement files in the following locations.

File	Location
VMware Cloud Director Availability™ Open Source License	/opt/vmware/h4/doc/ open_source_license_VMware_Cloud_Director_Availabil ity_4.1_GA.txt
End-user license agreement	/opt/vmware/etc/isv/EULA/en/0

**Note** The resources that relate to security operate with the required OS permissions and ownership. Do not attempt to change the ownership or permissions of these files.

# VMware Cloud Director Availability Updates

# 9

To receive the latest security updates, upgrade the VMware Cloud Director Availability appliances.

VMware Cloud Director Availability virtual appliances use the VMware Photon OS as the guest operating system. To receive the latest updates, upgrade the VMware Cloud Director Availability appliances.

- For information about upgrading VMware Cloud Director Availability in the cloud site, see *Upgrading VMware Cloud Director Availability in VMware Cloud Director Availability Installation, Configuration, and Upgrade Guide in the Cloud*.
- For information about upgrading VMware Cloud Director Availability on premises, see *Upgrading VMware Cloud Director Availability On Premises in VMware Cloud Director Availability Installation, Configuration, and Upgrade Guide On-Premises*.