

vCloud Availability Security

VMware vCloud Availability 3.5



vmware®

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

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

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

docfeedback@vmware.com

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

Copyright © 2019 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

- 1** What is vCloud Availability Security 4
- 2** vCloud Availability Services 5
- 3** vCloud Availability Configuration Files 8
- 4** vCloud Availability Security Configuration Properties 9
- 5** vCloud Availability Logs 12
- 6** vCloud Availability Users and Sessions 16
- 7** vCloud Availability Network Ports and Services Connectivity 18
- 8** vCloud Availability License and EULA Files 19
- 9** vCloud Availability Updates 20

What is vCloud Availability Security

1

vCloud Availability Security provides a reference to the security features in vCloud Availability.

To aid with protecting the vCloud Availability installation, *vCloud Availability Security* describes the security features in vCloud 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 vCloud Availability.
- Configuration settings with security implications.
- Location and purpose of log files.
- Required system accounts.
- How to obtain the latest security updates.

Intended Audience

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

vCloud Availability Services

2

The services of vCloud Availability can coexist on one virtual appliance or on dedicated appliances.

vCloud Availability services provide dedicated management interfaces for configuration and administration.

The operation of vCloud Availability depends on the following services that run on the listed vCloud Availability virtual appliances.

Table 2-1. vCloud Availability Services

Service Name	Service Description
vCloud Availability Replicator	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. vCloud Availability Replicator operates in the following vCloud Availability appliances: <ul style="list-style-type: none">■ vCloud Availability Cloud Replicator Appliance■ vCloud Availability Combined Appliance■ vCloud Availability On-Premises Appliance
vCloud Availability Replication Manager	A service that operates with vCenter Server-level concepts for managing the replication workflow and manages the vCloud Availability Replicator instances by using REST API calls. vCloud Availability Replication Manager operates in the following vCloud Availability appliances: <ul style="list-style-type: none">■ vCloud Availability Cloud Replication Management Appliance■ vCloud Availability Combined Appliance

Table 2-1. vCloud Availability Services (continued)

Service Name	Service Description
vCloud Availability vApp Replication Manager with an embedded vCloud Availability Portal	<p>Provides the main interface for replication operations. Operates with vCloud Director-level concepts, with vApps and virtual machines. Manages the vCloud Availability Replication Manager service by using REST API calls.</p> <p>The embedded vCloud Availability Portal provides the tenants and the service providers of the vCloud Availability Service Provider Portal with a graphic user interface to operate with vCloud Availability.</p> <p>vCloud Availability vApp Replication Manager operates in the following vCloud Availability appliances:</p> <ul style="list-style-type: none"> ■ vCloud Availability Cloud Replication Management Appliance ■ vCloud Availability Combined Appliance
vCloud Availability Tunnel	<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. vCloud Availability Tunnel operates in the following vCloud Availability appliances:</p> <ul style="list-style-type: none"> ■ vCloud Availability Cloud Tunnel Appliance ■ vCloud Availability Combined Appliance ■ vCloud Availability On-Premises Appliance

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 vCloud Availability appliances:</p> <ul style="list-style-type: none"> ■ vCloud Availability Cloud Tunnel Appliance ■ vCloud Availability Combined Appliance ■ vCloud Availability On-Premises Appliance
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 vCloud Availability appliances:</p> <ul style="list-style-type: none"> ■ vCloud Availability Cloud Tunnel Appliance ■ vCloud Availability Combined Appliance ■ vCloud Availability On-Premises Appliance

The following additional services run on all the vCloud 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 vCloud 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 root user is allowed to authenticate. After 3 unsuccessful login attempts, the root 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.

vCloud Availability Configuration Files

3

vCloud 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
vCloud Availability Replicator	replicator	/lib/systemd/system/ replicator.service	/opt/vmware/h4/replicator/config/ application.properties
vCloud Availability Replication Manager	manager	/lib/systemd/system/ manager.service	/opt/vmware/h4/manager/config/ application.properties
vCloud Availability vApp Replication Manager	cloud	/lib/systemd/system/ cloud.service	/opt/vmware/h4/cloud/config/ application.properties
vCloud Availability Tunnel	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.

vCloud Availability Security Configuration Properties

4

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

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

Property Name	Default Value	Description
session.timeout	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">■ vCloud Availability Replicator■ vCloud Availability Replication Manager■ vCloud Availability vApp Replication Manager■ vCloud Availability Tunnel
session.maxage	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">■ vCloud Availability Replicator■ vCloud Availability Replication Manager■ vCloud Availability vApp Replication Manager■ vCloud Availability Tunnel

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 Configuration Reference in the Apache Tomcat documentation.</p> <p>Applies to the following services:</p> <ul style="list-style-type: none"> ■ vCloud Availability Replicator ■ vCloud Availability Replication Manager ■ vCloud Availability vApp Replication Manager ■ vCloud Availability Tunnel
<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 Configuration Reference in the Apache Tomcat documentation.</p> <p>Applies to the following services:</p> <ul style="list-style-type: none"> ■ vCloud Availability Replicator ■ vCloud Availability Replication Manager ■ vCloud Availability vApp Replication Manager ■ vCloud Availability Tunnel
<code>vcd.hostnameverifier.noop</code>	false	<p>When set to <code>true</code>, skips the verification of the host name of vCloud Director when establishing a TLS session.</p> <p>Used to prevent an SSL error when the vCloud Director certificate subject or its list of SANs does not contain the provided vCloud Director address.</p> <p>Applies only to vCloud Availability vApp Replication Manager.</p>

Property Name	Default Value	Description
web.cors.allowedOrigins	(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, vCloud Availability vApp Replication Manager implicitly allows requests from vCloud Director.</p> <p>Applies to the following services:</p> <ul style="list-style-type: none"> ■ vCloud Availability Replicator ■ vCloud Availability Replication Manager ■ vCloud Availability vApp Replication Manager ■ vCloud Availability Tunnel
admin.allow.from	(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 vCloud Availability Tunnel, 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"> ■ vCloud Availability Replicator ■ vCloud Availability Replication Manager ■ vCloud Availability vApp Replication Manager ■ vCloud Availability Tunnel

vCloud Availability Logs

5

The log files that contain system messages are located in the vCloud Availability virtual appliances.

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

Service	Default Location	Description
vCloud Availability Replicator	/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.
vCloud Availability Replication Manager	/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.
vCloud Availability vApp Replication Manager	/opt/vmware/h4/cloud/log/cloud.log	Contains application-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.
vCloud Availability Tunnel	/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 vCloud Availability Tunnel.
	/opt/vmware/h4/tunnel/log/requests.log	When activated, contains HTTP request and response data like URL, response code, and timing entries.

Service	Default Location	Description
vSphere Replication Server	/var/log/vmware/hbrsrv.log	The log file of the HBR server. Useful for troubleshooting NFC errors other problems.
Upgrade Log	/opt/vmware/var/log/vami/vami.log	Contains upgrade log entries.

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(JsonCredentialsAuthenticationFilter.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 - [337a5316-56d7-4a28-8991-83911eadbdc9_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.SsoCredentialsAuthProvider.authenticate(SsoCredentialsA
uthenticationProvider.java:96)

```

- Certificate mismatch after replacing the certificate of a vCloud 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.ClientCertAuthProvider.authenticate(ClientCertAuth
enticationProvider.java:47)

```

```

        at
com.vmware.h4.cloud.peer.PeerClientCertAuthProvider.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)

```

```

...

```

vCloud Availability Users and Sessions

6

vCloud Availability uses the following users and establishes the followings sessions.

vCloud Availability Appliance root User Account

The **root** user account is used to access both the virtual appliance console and the management interface. This account is set up during the initial deployment of each vCloud Availability appliance. In the **OVF Deployment** wizard, an initial password for the **root** user account is established, with the requirement for the initial password to be more than 3 characters long. After the initial deployment, vCloud Availability forces the change of the initial password upon the first login by using the **root** user, with the following requirements for the **root** user account password.

- Length of more than 8 characters.
- Must contain digits, upper and lower case letters, and non-alphabetic characters.
- Must not reuse a previous password.
- Must contain more than 4 new characters compared to the previous password.

vCloud Availability Users

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

- Service providers manage vCloud Availability objects and the local vCloud Availability appliances after authenticating as vCloud Director **System administrator** users. These users can manage any local and monitor any remote vCloud Availability inventory object. To manage vCloud Availability objects in the remote site, authenticate as a **System administrator** to the remote site.
- Tenant users perform disaster recovery operations and manage local vCloud Availability objects after authenticating as vCloud Director **Organization administrator** users. These users can perform disaster recovery operations in the local site, can manage any local vCloud Availability object, and can monitor any remote vCloud Availability object that belongs to the vCloud Director organization. To manage remote vCloud Availability objects, authenticate as an **Organization administrator** user to the remote site.

For more information about authenticating to remote sites, see *Authenticating to Remote Sites* in *Using vCloud Availability*.

vCloud Availability User Sessions Requirements

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

The following table lists vCloud Availability vApp Replication Manager disaster recovery operations that require sessions on either of the sites, or on both.

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
failover test	No	Yes	Yes	Yes
failover test cleanup	No	Yes	Yes	Yes

vCloud Availability Network Ports and Services Connectivity

7

Allow the required TCP access in the site for the correct operation of vCloud Availability services.

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

Services Connectivity

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

- vCloud Availability vApp Replication Manager must have a TCP access to vCloud Director, vCloud Availability Replication Manager, vCenter Server, and, depending on where the vCenter Server Lookup service is hosted, to Platform Services Controller.
- vCloud Availability Replication Manager must have a TCP access to the vCenter Server Lookup service and to all the vCloud Availability Replicator instances in the site.
- vCloud Availability Replicator must have a TCP access to the vCloud Availability Replication Manager, vCenter Server, and the vCenter Server Lookup service.

For more information and a network diagram that shows the connectivity between all vCloud Availability components, see *Network Ports Requirements* in *Installing, Configuring, and Upgrading vCloud Availability in the Cloud* and in *Installing, Configuring, and Upgrading vCloud Availability On-Premises*.

vCloud Availability License and EULA Files

8

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

In the vCloud Availability appliance, you can find the license agreement files in the following locations.

File	Location
VMware vCloud Availability Open Source License	/opt/vmware/h4/doc/ open_source_license_VMware_vCloud_Availability_3.5. 0_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.

vCloud Availability Updates

9

To receive the latest security updates, upgrade the vCloud Availability appliances.

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

- For information about upgrading vCloud Availability in the cloud site, see *Upgrading vCloud Availability* in *Installing, Configuring, and Upgrading vCloud Availability in the Cloud*.
- For information about upgrading vCloud Availability on premises, see *Upgrading vCloud Availability On Premises* in *Installing, Configuring, and Upgrading vCloud Availability On-Premises*.