Security Guide

24 NOV 2022

VMware Cloud Director Availability 4.5

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

https://docs.vmware.com/

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

Contents

Security Guide

1

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

To aid with protecting the VMware Cloud Director Availability installation, the *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 required for the correct operation of the VMware Cloud Director Availability appliances.
- The network connectivity between the services and between paired sites.
- The locations on the appliance filesystem of the configuration files for the services.
- The configuration properties of the services with security compliance implications.
- The locations on the appliance filesystem and the purposes of the log files of the services.
- The **root** account privileges, the required system user accounts permissions, and the required rights in VMware Cloud Director™ for their roles.
- The files locations for the open-source license and for VMware General Terms.
- Obtaining the latest security updates by upgrading the cloud and the on-premises VMware Cloud Director Availability sites.

Intended Audience

The *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. The *Security Guide* introduces security and compliance as it relates to the VMware Cloud Director Availability solution.

Services and Network Ports

2

When deploying VMware Cloud Director Availability, by selecting the virtual appliance deployment type places the services of VMware Cloud Director Availability on dedicated cloud appliances, or on a combined appliance for testing purposes.

VMware Cloud Director Availability Appliance Services

VMware Cloud Director Availability services provide dedicated management interfaces for configuration and administration. The replication operations depend on the following services that run on each listed VMware Cloud Director Availability virtual appliances in the table.

Table 2-1. VMware Cloud Director Availability Services

Service Name	Service Description
Replicator Service instances	One or more service instances manage the vSphere Replication Server service and the LWD Proxy service and expose the low-level HBR primitives as a REST API. These instances operate with vCenter Server-level concepts, like virtual machines, folders, datastores. The following VMware Cloud Director Availability appliances each run a single Replicator Service instance, depending on the cloud site: ■ Replicating with a multi-tenant VMware Cloud Director site: ■ Providers deploy multiple Replicator Appliance instances or a single Cloud Director Combined Appliance instance. ■ Tenants deploy On-Premises to Cloud Director Replication Appliance ■ vSphere DR and migration between vCenter Server sites: ■ Providers deploy vCenter Replication Management Appliance ■ Tenants deploy On-Premises to Cloud vCenter Replication Appliance
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. The following VMware Cloud Director Availability appliances each run the Manager Service instance, depending on the cloud site: ■ Replicating with a multi-tenant VMware Cloud Director site: ■ Providers deploy Cloud Director Replication Management Appliance or Cloud Director Combined Appliance. ■ vSphere DR and migration between vCenter Server sites: ■ Providers deploy vCenter Replication Management Appliance ■ Tenants deploy On-Premises to Cloud vCenter Replication Appliance

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

Service Name	Service Description
Cloud Service	A service that operates with VMware Cloud Director-level concepts, like vApps and virtual machines. Manages the Manager Service by using REST API calls. The following VMware Cloud Director Availability appliances each run the Cloud Service instance: ■ Replicating with a multi-tenant VMware Cloud Director site: ■ Providers deploy Cloud Director Replication Management Appliance or Cloud Director Combined Appliance.

Tunnel Service	A service that orchestrates a secure tunnel creation and as a single endpoint channels both the incoming and outgoing site traffic, and both management data and replication data traffic using Lightweight Delta Protocol (LWD).
	The following VMware Cloud Director Availability appliances each run the Tunnel Service instance, depending on the cloud site:
	■ Replicating with a multi-tenant VMware Cloud Director site:
	  ■ Providers deploy Tunnel Appliance or Cloud Director Combined Appliance.
	  ■ Tenants deploy On-Premises to Cloud Director Replication Appliance
	■ vSphere DR and migration between vCenter Server sites:
	  ■ Providers deploy vCenter Replication Management Appliance
	  ■ Tenants deploy On-Premises to Cloud vCenter Replication Appliance

Table 2-2. Replication Services

Service Name	Service Description
vSphere® Replication™ Service with vSphere Replication filter	The vSphere Replication Service, also called the HBR Service manages low-level replication operations, creates replication instances, and others. Receives and records the delta information for each replicated workload. During replication, only the delta information is sent from the source site ESXi host to the destination site ESXi host. In a site, vSphere Replication Server operates in the following VMware Cloud Director Availability appliances: ■ Each Replicator Appliance instance or the single Cloud Director Combined Appliance instance ■ On-Premises to Cloud Director Replication Appliance ■ On-Premises to Cloud vCenter Replication Appliance ■ vCenter Replication Management Appliance
Lightweight Delta Protocol Service (LWD Proxy)	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. In a site, LWD Proxy operates in the following VMware Cloud Director Availability appliances: ■ Each Replicator Appliance instance or the single Cloud Director Combined Appliance instance ■ On-Premises to Cloud Director Replication Appliance ■ On-Premises to Cloud vCenter Replication Appliance ■ vCenter Replication Management Appliance
VMware Cloud on AWS Data Engine Service (Data Engine Service)	A new service, introduced with VMware Cloud Director Availability 4.2 for performing migrations to VMware Cloud on AWS by using the new **VMC** replication data engine, due to the design specifics of the Cloud Director service. By using the Data Engine Service and with the **VMC** data engine selected, VMware Cloud Director Availability migrates workloads to Cloud Director service. For information about migrating to VMware Cloud on AWS, see Migration to VMware Cloud Director service in the *Migration to VMware Cloud Director service Guide*. In a site, a Data Engine Service instance operates in the following VMware Cloud Director Availability appliances: ■ Each Replicator Appliance instance or the single Cloud Director Combined Appliance instance ■ On-Premises to Cloud Director Replication Appliance

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

Table 2-3. Other 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 inactive. After explicitly enabling SSH during deployment or in the management interface, this service activates and starts. Only the **root** user is allowed to authenticate. Three unsuccessful login attempts lock the **root** user account for 15 minutes.
systemd-timesyncd	A standard Linux service that provides NTP time management. To configure an NTP server, use the management interface. This service is constantly 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 during the appliance boot.
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 constantly running.

Network Ports

For information about the network ports required for the correct operation of VMware Cloud Director Availability, see VMware Cloud Director Availability - VMware Ports and Protocols.

For information about the services connectivity, see Chapter 3 Services Network Connectivity.

For information about the network requirements and the external interfaces between the paired sites of VMware Cloud Director Availability, select your version and see:

- Network Requirements in a Cloud backed by Cloud Director in the *Installation, Configuration, and Upgrade Guide in the Cloud Director Site*.
- Deployment Requirements for On-Premises to Cloud Director Appliance in the *Installation, Configuration, and Upgrade Guide in On-Premises and Provider Site*.
- Since version 4.4, see also Network Requirements for vSphere and DR in the *Installation, Configuration, and Upgrade Guide in On-Premises and Provider Site*.

Services Network Connectivity 3

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

For information about the network ports required for the correct operation of VMware Cloud Director Availability, see VMware Cloud Director Availability - VMware Ports and Protocols.

For information about the services of VMware Cloud Director Availability, see Chapter 2 Services and Network Ports.

For information about the network requirements and the external interfaces between the paired sites of VMware Cloud Director Availability, select your version and see:

- Network Requirements in the Cloud in the *Installation, Configuration, and Upgrade Guide in the Cloud Director Site*.
- Deployment Requirements On-Premises in the *Installation, Configuration, and Upgrade Guide in On-Premises and Provider Site*.
- Deployment Requirements for vSphre DR and Migration in the *Installation, Configuration, and Upgrade Guide in On-Premises and Provider Site*.

Services Network Connectivity

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

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

- All the Replicator Service instances must have a TCP access to the Manager Service, to the vCenter Server instance, 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 *Installation, Configuration, and Upgrade Guide in the Cloud Director Site* and in *Installation, Configuration, and Upgrade Guide in On-Premises and Provider Site*.

Services Configuration Files

4

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
VMware Cloud on AWS Data Engine Service	h4dm	`/usr/lib/systemd/system/h4dm.service`	`/opt/vmware/h4/h4dm/conf/conf.toml`
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`

Service	System Unit	System Unit Location	Configuration File Location
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

- VMware Cloud Director Availability does not support installing of any packages, 3rd party software or, and changes in yum configuration files.
- 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.

For information about configuring the security properties, see Chapter 5 Services Security Configuration Properties.

Services Security Configuration Properties

5

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. For information about the service configuration files, see Chapter 4 Services Configuration Files.

Property Name	Default Value	Description
`session.timeout`	1800000	The time in milliseconds to keep inactive sessions active. Each HTTP request resets the timer. The default value is 30 minutes. Applies to the following services: ■ Replicator Service ■ Manager Service ■ Cloud Service ■ Tunnel Service
`session.maxage`	86400000	The maximum session length in milliseconds. Even if the session is kept alive, after the time specified in this property, the session is terminated. This property prevents attacks based on stolen session cookies. The default value is 24 hours. Applies to the following services: ■ Replicator Service ■ Manager Service ■ Cloud Service ■ Tunnel Service

Property Name	Default Value	Description
`https.endpoint.protocols`	TLSv1.2	Corresponds to `sslEnabledProtocols` in Apache Tomcat. For more information, see Apache Tomcat Configuration Reference in the *Apache Tomcat documentation*. Applies to the following services: ■ Replicator Service ■ Manager Service ■ Cloud Service ■ Tunnel Service
`https.endpoint.ciphers`	An example that excludes DH: `HIGH:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!kRSA:!DH`	Corresponds to `ciphers` from `SSLHostConfig` in Apache Tomcat. For information about `SSLHostConfig`, see Apache Tomcat Configuration Reference in the *Apache Tomcat documentation*. Applies to the following services: ■ Replicator Service ■ Manager Service ■ Cloud Service ■ Tunnel Service
`vcd.hostnameverifier.noop`	false	When set to `true`, skips the verification of the host name of VMware Cloud Director when establishing a TLS session. 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. Applies only to the Cloud Service.

Property Name	Default Value	Description
`web.cors.allowedOrigins`	(empty string)	A list of origins (Cross-Origin Resource Sharing (CORS)) that are allowed to access the web resources. Applicable when operating a custom web server serving the plug-in with an iframe. The default value does not allow any origins, but due to the integrated user interface plug-in, the Cloud Service implicitly allows requests from VMware Cloud Director. Applies to the following services: ■ Replicator Service ■ Manager Service ■ Cloud Service ■ Tunnel Service
`admin.allow.from`	(empty string)	Controls the source IP addresses that are allowed to establish server sessions. In a production environment, deactivate the root access authentication from the Tunnel Service, as requests come from the Internet. The default value states: if the service has tunneling configuration set, reject tunnel requests, otherwise allow all. Applies to the following services: ■ Replicator Service ■ Manager Service ■ Cloud Service ■ Tunnel Service

Services Logs

6

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
VMware Cloud on AWS Data Engine Service	`/opt/vmware/h4/h4dm/log/h4dm*.log`	Contains the Data Engine Service specific logs and security-related messages.
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 Log	`/var/log/upgrade.log`	Contains the upgrade log entries.

Note

- VMware Cloud Director Availability does not support installing of any packages, 3rd party software or, and changes in yum configuration files.
- 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(Cre
dentialsAuthenticationProvider.java:84)
```

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

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

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

        at
org.springframework.security.web.authentication.AbstractAuthenticationProcessingFilter.doFi
lter(AbstractAuthenticationProcessingFilter.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(SsoCrede
ntialsAuthenticationProvider.java:101)

        at
com.vmware.h4.cloud.security.VcloudSsoCredentialsProvider.authenticate(VcloudSsoCredentials
Provider.java:44)

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

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

        at
org.springframework.security.web.authentication.AbstractAuthenticationProcessingFilter.doFi
lter(AbstractAuthenticationProcessingFilter.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(SsoCrede
ntialsAuthenticationProvider.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(ClientC
ertAuthenticationProvider.java:47)

        at
com.vmware.h4.cloud.peer.PeerClientCertAuthenticationProvider.authenticate(PeerClientCertAu
thenticationProvider.java:65)

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

        at
com.vmware.spring.security.clientcert.impersonate.ImpersonatingClientCertFilter.attemptAuth
entication(ImpersonatingClientCertFilter.java:45)

        at
org.springframework.security.web.authentication.AbstractAuthenticationProcessingFilter.doFi
lter(AbstractAuthenticationProcessingFilter.java:212)

        ...
```

Users Roles Rights and Sessions 7

VMware Cloud Director Availability requires privileges for the following users roles and rights and establishes the following sessions for performing disaster recovery (DR) operations.

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.

For vSphere DR and migration, VMware Cloud Director Availability supports users members of the following groups:

User member of:	In the On-Premises to Cloud vCenter Replication Appliance	In the provider vCenter Replication Management Appliance
ADMINISTRATORS group	On-premises **ADMINISTRATORS** users allow complete control.	Provider **ADMINISTRATORS** users allow complete control.
VRUSERS group	On-premises **VRUSERS** have permissions to only: ■ Monitor replications ■ Manage replications ■ Monitor replication tasks ■ Monitor peer sites. Users members of **VRUSERS** cannot modify the existing paired sites nor pair new sites. **Note** To pair with a provider site requires entering a provider user that belongs to **VRUSERS** or **ADMINISTRATORS** or **VRADMINISTRATORS** in that provider site. For most tenants, it is recommended to pair by using a user that belongs to the provider **VRUSERS** group. In summary, both users: an on-premises **ADMINISTRATORS** user plus a provider **VRUSERS** user are necessary for establishing a pairing from the on-premises site to the provider site.	Provider **VRUSERS** have permissions to only: ■ Monitor replications ■ Manage replications ■ Monitor replication tasks ■ Monitor peer sites. Users members of **VRUSERS** cannot pair new sites nor modify the existing paired sites, even for pairings from on-premise sites that use the same provider **VRUSERS** user for establishing the trust. **VRUSERS** users have no permission to modify any pairings, regardless of the peer site type.

- To establish a user session with **administrative** rights in VMware Cloud Director Availability, the credentials for both the source and the destination sites must belong either to the **ADMINISTRATORS** or **VRADMINISTRATORS** groups. This applies for both vSphere DR and migration and for replications with cloud sites backed by VMware Cloud Director.

  For example, the single sign-on user **Administrator@vsphere.local** is a member of the **ADMINISTRATORS** group.

- In VMware Cloud Director sites, 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.

- Tenants perform disaster recovery operations and manage the VMware Cloud Director Availability objects after authenticating as:
  - For vSphere DR and migration, as **VRUSERS** single-sign-on users the tenants 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.
  - In VMware Cloud Director sites, as **Organization Administrator** users, tenants 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.

For vSphere DR and migration, VMware Cloud Director Availability creates both the **VRADMINISTRATORS** and the **VRUSERS** groups in the local vCenter Server instance during the appliance configuration with the vCenter Server Lookup service. In VMware Cloud Director sites, the **VRUSERS** group is not available and the **VRADMINISTRATORS** group must be manually created only if custom permissions are needed for vCenter Server.

vSphere Privileges for VMware Cloud Director Availability Administrators

Restricted rights

For vSphere DR and migration, VMware Cloud Director Availability 4.5 and later allow login to the appliance management interface and to the vSphere plug-in by using a monitoring user granted with limited access to the system. The limited user can neither manage the replications nor the service.

After deployment or post-upgrade, registering the VMware Cloud Director Availability appliance with the vCenter Server Lookup service creates two additional new single-sign-on groups in vSphere: **VrMonitoringUsers** and **VrMonitoringAdministrators**.

To use the monitoring-only privileges of these groups, create a new single-sign-on user and make him a member of one of the two groups:

- **VrMonitoringUsers** membership allows the users to monitor replications.
- **VrMonitoringAdministrators** membership allows the administrators to monitor the replications and the system health.

The user privileges are as follows from highest to lowest: **Read-write administrator > Read-only administrator > Read-write user > Read-only user**.

As a **provider** or an on-premises **administrator**, allow the least privileges for the roles of the user accounts that register the vCenter Server Lookup service and operate VMware Cloud Director Availability. As a **provider** to prevent the tenants access to restricted infrastructure items, only allow the following minimum list of privileges as specified for audit certifications and security compliance of VMware Cloud Director Availability.

When using customized privileges for the **service user** account, the following privileges must apply to the user that operates with VMware Cloud Director Availability and registers it with the vCenter Server Lookup service:

Cryptographic Operations

- Cryptographic operations.Manage keys
- Cryptographic operations.Register host

Datastore Privileges

- Datastore.Browse
- Datastore.Configure datastore
- Datastore.Low level file operations

Extension Privileges

- Extension.Register extension
- Extension.Unregister extension
- Extension.Update extension

Global Privileges

- Global.Disable methods
- Global.Enable methods

Host Configuration Privileges

- Host.Configuration.Connection

Profile-driven Storage Privileges

- Profile-driven storage.Profile-driven storage view

Resource Privileges

- Resource.Assign virtual machine to resource pool

Storage Views Privileges

- StorageViews.View

Virtual Machine Configuration Privileges

- Virtual machine.Configuration.Add existing disk
- Virtual machine.Configuration.Change Settings

- Virtual machine.Configuration.Remove disk

Virtual Machine Inventory Privileges

- Virtual machine.Inventory.Register
- Virtual machine.Inventory.Unregister

Virtual Machine Interaction

- Virtual machine.Interaction.Power Off
- Virtual machine.Interaction.Power On

Virtual Machine State Privileges

- Virtual machine.Snapshot management.Create snapshot
- Virtual machine.Snapshot management.Remove snapshot

HBR Privileges

- Host.Hbr.HbrManagement
- VirtualMachine.Hbr.ConfigureReplication
- VirtualMachine.Hbr.ReplicaManagement
- VirtualMachine.Hbr.MonitorReplication

Note After adding a custom role in vSphere, the role is created as a Read Only role with three system-defined privileges:

- System.Anonymous
- System.Read
- System.View

  These privileges are not visible in the vSphere Client but are used to read specific properties of some managed objects. All the predefined roles in vSphere contain these three system-defined privileges.

For information about the roles privileges in vSphere, see Defined Privileges in the vSphere documentation.

VMware Cloud Director Roles Rights

VMware Cloud Director for users permissions 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 an individual organization. **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.

Restricted rights

VMware Cloud Director Availability 4.5 introduces two rights in VMware Cloud Director for the cloud site:

- VCDA_MODIFY_RIGHT for a full permission user in VMware Cloud Director Availability.
- VCDA_VIEW_RIGHT for a read-only user in VMware Cloud Director Availability.

To use these new rights in the cloud site, first the **System Administrator** user must publish the chosen right in a rights bundle in VMware Cloud Director. These rights cannot be used for on-premises users to log in to the On-Premises to Cloud Director Replication Appliance.

1. To create or modify an existing rights bundle, in VMware Cloud Director, in the left pane under the **Tenant Access Control** section click **Rights Bundles** then click **Add** or select an existing bundle and click **Edit**.
2. In the **Add Rights Bundle** window, under **Rights in Bundle**, under the **Other** category, select the right and click **Save**.
   - **VCDA_VIEW_RIGHT**
   - **VCDA_MODIFY_RIGHT**
3. To publish the rights bundle to all tenants or to specific tenants, select it and click **Publish**.
4. In the **Publish Rights Bundle** window, select the tenants to which to publish the new rights bundle and click **Save**.
   - **Publish to Tenants**
   - **Publish to All Tenants**

After the **System Administrator** publishes the rights bundle to one or more organizations, these organizations have access to use those rights when accessing VMware Cloud Director Availability in the cloud site.

Read-write rights

VMware Cloud Director Availability allows read-write access to **Organization Administrator** users or to users whose role is assigned with VCDA_MODIFY_RIGHT.

Read-only rights

In the user interface, all management-related actions remain hidden for read-only users. A tenant user whose role is assigned with VCDA_VIEW_RIGHT is restricted to only viewing his own replications and has no permissions to modify.

Conflicting rights

Determining the expected rights if a user role is assigned with conflicting rights, for example, both VCDA_READ_RIGHT and **Organization Administrator**, results in read-write access for

that user. Similarly, assigning both VCDA_READ_RIGHT and VCDA_MODIFY_RIGHT to the same user role again results in read-write access.

As a result:

- Read-write users can either have assigned VCDA_MODIFY_RIGHT to their custom role, or use the default **Organization Administrator** user.
- Read-only users have assigned VCDA_READ_RIGHT to their role.
- Assigning both VCDA_READ_RIGHT and either (VCDA_MODIFY_RIGHT or **Organization Administrator**) to the same role results in read-write rights.

List of the rights of all the users that allow log in to the Cloud Director Replication Management Appliance:

- Read-write **tenant** users have the same rights as the existing **Organization Administrator** user and allow both managing and monitoring only of their own replications.
- Read-only **tenant** users are introduced with version 4.5 and allow only monitoring of their own replications.
- Read-write **provider** users are the current provider login method and allow both managing and monitoring of all replications and of the system health.
- Read-only **provider** users are introduced with version 4.5 and allow only monitoring of all replications and of the system health.

As a prerequisite, for **tenant** roles that only grant the VCDA_MODIFY_RIGHT and are different than the default **Organization Administrator**, in VMware Cloud Director at minimum grant exactly the following rights:

- General: Administrator Control
- vApp: Edit VM Compute Policy *
- 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: Edit Association Settings
- 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
- Organization vDC Gateway: View L2 VPN **
- Organization vDC Gateway: Configure L2 VPN **

Note

- VMware Cloud Director Availability requires each and all of the above rights for the correct operation of the VMware Cloud Director tenant user.
- For the vRealize Operations Management Pack for Cloud Director Availability to be able to use auto-discovery of the VMware Cloud Director Availability address, when using a read-only user for the management pack, you must also add the right View Tenant Portal Plugin, shown in the user interface as UI Plugins: View right.
- * VMware Cloud Director Availability 4.3 and later require the **vApp: Edit VM Compute Policy** right that is not part of the Default Rights Bundle.
- ** In VMware Cloud Director service, to stretch an L2 network to an SDDC in the VMware Cloud™ on AWS, VMware Cloud Director Availability 4.4 and later require both the **Organization vDC Gateway: View L2 VPN** and the **Configure L2 VPN** rights that are not part of the Default Rights Bundle.

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 *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
`failover test`	No	Yes	Yes	Yes
`failover test cleanup`	No	Yes	Yes	Yes

VMware Cloud Director Availability License and General Terms Files

8

The files containing the VMware Cloud Director Availability open-source license and VMware General Terms can be located in the VMware Cloud Director Availability virtual appliances.

The VMware Cloud Director Availability 4.5 appliances store the open-source license and the general terms files in the following locations in their filesystems:

File	Location
VMware Cloud Director Availability™ Open Source License	`/opt/vmware/h4/doc/open_source_license_VMware_Cloud_Director_Availability_4.5_GA.txt`
VMware General Terms	`/opt/vmware/h4/doc/eula.txt`

Note

- VMware Cloud Director Availability does not support installing of any packages, 3rd party software or, and changes in yum configuration files.
- 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.

Upgrade for 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 to the latest version.

Cloud Site Upgrade

For information about upgrading VMware Cloud Director Availability in the cloud site, select your version and see Upgrading in the Cloud in the *Installation, Configuration, and Upgrade Guide in the Cloud Director Site*.

When upgrading, paired remote cloud sites might cause versions mismatch. For information about pairing with mismatching versions, select your version and see Managing Connections Between Cloud Sites in the *Administration Guide*.

On-Premises Upgrade

For information about upgrading VMware Cloud Director Availability on-premises, select your version and see Upgrading On-Premises in the *Installation, Configuration, and Upgrade Guide in On-Premises and Provider Site*.