vCloud Availability for vCloud Director 2.0 Administration Guide

vCloud Availability for vCloud Director 2.0

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

Contents

vCloud Availability for vCloud Director 2.0 Administration Guide

1

The *vCloud Availability for vCloud Director* Administration Guide explains how to work, manage, and monitor the vCloud Availability for vCloud Director solution from both service provider and tenant sides.

Intended Audience

This information is intended for VMware Cloud Provider Program service providers and experienced system administrators who are familiar with virtual machine technology and data center operations including but not limited to the following areas:

- VMware vSphere®
- VMware vCloud Director®
- Virtual Infrastructure
- Secure Shell (SSH)
- Bash

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

This section includes the following topics:

- Managing the Solution from the Service Provider Side
- Working with the Solution from the Tenant Side

Managing the Solution from the Service Provider Side

The vCloud Availability for vCloud Director administration guide for service providers describes procedures for changing components passwords, updating components certificates, managing the environment, and backing up the solution. You can use
vCloud Availability for vCloud Director Service Manager Portal to monitor replications and IaaS consumption.

Working with the vCloud Availability for vCloud Director Service Manager Portal

With vCloud Availability for vCloud Director Service Manager Portal, you can monitor and manage the DR environment. You can generate and download reports, cleanup stale replications, and migrate failover replications. The service providers can impersonate as tenants and perform DR operations.

Log In to the vCloud Availability for vCloud Director Service Manager Portal

You log in to the vCloud Availability for vCloud Director Service Manager Portal only as a vCloud Director system administrator.

Procedure

1. Enter the URL of the vCloud Availability for vCloud Director Service Manager Portal into a Web browser.

   `https://UI02_ADDRESS:8443`

2. Log in to the vCloud Availability for vCloud Director Service Manager Portal with your vCloud Director system administrator credentials.

   Note You receive an error message if you try to log in to the vCloud Availability for vCloud Director Service Manager Portal with a role that is different from the vCloud Director system administrator role.

Monitoring IaaS Consumption

You can monitor the overall IaaS consumption by the tenants in the vCloud Availability for vCloud Director Service Manager Portal. You can track all the vCloud Director organizations enabled for replication and their system usage.

Getting Information from the Home Screen Dashboard

After you log in to the vCloud Availability for vCloud Director Service Manager Portal, you can review the **Summary Page** dashboard. You can find information about vCloud Director organizations enabled for replication. You can view the overall vCloud Director allocated and used storage used by those organizations and their replicated VMs. You can get the number of replications per organization, the storage use per organization VDC and the organization VDC with unlimited capacity.

You can obtain additional statistics about the distribution of the replications in **OK**, **Error**, and **Other** state.

Note Notice that the † symbol indicates a real-time value.

Generating Reports

The information on the **Summary Page** is generated from a report collection snapshot. You can see the date and time of the last generated report collection snapshot in the **Report page**.

You can view the number of vCloud Director organizations enabled for replication and total storage, total pre-allocated CPU, and total pre-allocated memory for those organizations. You can also see the number of to- and from cloud replications and their state.

To see the specific information about replications assigned to a particular organization VDC, click the link for that organization.

To generate a new report collection snapshot on-demand, you must click the **GENERATE** button on the **Report page**. You can generate and download reports on the overall allocated and used storage, memory, and CPU by organization VDC. You can get statistics on the corresponding to-cloud and from-cloud replications by their state.

Note It takes several minutes for the report collection snapshot generation. To confirm the completion of the report, you must leave and return to the report page, or refresh the browser.

Adjusting the Frequency of Report Generation

By default, the vCloud Availability for vCloud Director Service Manager Portal generates a report every 12 hours.

To adjust the frequency of report generation:

1 Use a text editor to open the `/opt/vmware/vcav-smp/conf/application.yml` file.

2 Set the *trigger* value to the desired value.

Manage the Cleanup of Stale Replications

You can delete the staled failover replications from the **Inventory** page of the vCloud Availability for vCloud Director Service Manager Portal.

A replication run is considered stale if either its state is null, or its vApp or VM does not exist.

Procedure

1. Log in to the vCloud Availability for vCloud Director Service Manager Portal with your vCloud Director system administrator credentials.
2. In the **Inventory** page, locate the organization whose replications you want to manage.
3. From the **Actions** menu for the selected organization, click **Scrub Stale Replications**.

   The list of all replications for the selected organization opens in a new window. The replications that are eligible for cleanup are displayed in yellow.
4. Select one or more replications to cleanup and click **NEXT**.
5. Review the configuration and click **RUN**.

   Important You cannot cancel the operation after you start it.

   You can track the Job ID.

Migrate Replications from One Datastore to Another

You can migrate failover replications from one datastore to another from the **Inventory** page in the vCloud Availability for vCloud Director Service Manager Portal.

Procedure

1. Log in to the vCloud Availability for vCloud Director Service Manager Portal with your vCloud Director system administrator credentials.
2. In the **Inventory** page, locate the organization whose replications you want to manage.
3. Under the **Actions** menu for the selected organization, click **Storage Migration**.
4. Follow the prompts to complete the Generic Storage Migration Wizard.
5. Review configuration and click **RUN MOVEAPI** to start the migration.

   Important You cannot cancel the operation after you start it.

   You can track the Job ID.

Impersonate a Tenant

As a service provider, you can impersonate a tenant to filter and drill down into particular tenant organizations and perform DR operations.

Prerequisites

Verify that you have the `--tenant-ui` argument configured during the vCloud Availability for vCloud Director Service Manager Portal host configuration. You can reconfigure it by running the `vcav vcd-ui configure-smp` command with `--reconfigure` argument.

Procedure

1. Log in to the vCloud Availability for vCloud Director Service Manager Portal by using your vCloud Director system administrator credentials.
2. In the **Inventory** page, locate the organization whose replications you want to manage.
3. Call out the **Actions** pane for the selected organization.
4. Click **Pose-as**.

   You are redirected to the corresponding vCloud Availability for vCloud Director Portal.

   For more information on how to work with the vCloud Availability for vCloud Director Portal, see Working with the Solution from the Tenant Side.

Using vCloud Availability Installer Appliance Scripts

The vCloud Availability Installer Appliance supports various operations that might be useful in certain situations.

Getting an IP Address of a vCloud Availability for vCloud Director Component

You can obtain the IP address of a single vCloud Availability for vCloud Director component at any time.

To get the IP address of a single vCloud Availability for vCloud Director component, run the following command.

Standard Command

```
# vcav vsphere get-ip \
--vsphere-address=$MGMT_VSPHERE_ADDRESS \
--vsphere-user=$MGMT_VSPHERE_USER \
--vsphere-password-file=~/.ssh/.vsphere.mgmt \
"--network=$MGMT_VSPHERE_NETWORK" \
--vm-name=host-vm-name
```

Command Using Registry

```
# vcav vsphere get-ip \
--vsphere=mgmt-vsphere-name \
"--network=VM Network" \
--vm-name=host-vm-name
```

The IP address is displayed.

Reconnecting to a vCloud Availability for vCloud Director Component

You reconnect to vCloud Availability for vCloud Director after you upgrade or redeploy your vCloud Availability Installer Appliance.

Reconnecting to a vSphere Replication Manager Appliance

To create a trust with the vSphere Replication Manager host, run the following command.

Standard Command

```
# vcav vsphere trust-ssh \
--vsphere-address=$MGMT_VSPHERE_ADDRESS \
--vsphere-user=$MGMT_VSPHERE_USER \
--vsphere-password-file=~/.ssh/.vsphere.mgmt \
--vm-name=hms-VM-name \
--root-password-file=~/.ssh/.root \
--vm-address=hms-address
```

Command Using Registry

```
# vcav vsphere trust-ssh \
--vsphere=mgmt-vsphere-name \
--vm-name=hms-VM-name \
--root-password-file=~/.ssh/.root \
--vm-address=hms-address
```

Connect to the vSphere Replication Manager by running the following command.

Standard Command

```
# vcav hms connect \
--root-password-file=~/.ssh/.root \
--vm-address=hms-address
```

Command Using Registry

```
# vcav hms connect \
--hms=hms.01
```

Reconnecting to a vSphere Replication Cloud Service Appliance

To create a trust with the vSphere Replication Cloud Service host, run the following command.

Standard Command	Command Using Registry

`# vcav vsphere trust-ssh \`
`--vsphere-address=$MGMT_VSPHERE_ADDRESS \`
`--vsphere-user=$MGMT_VSPHERE_USER \`
`--vsphere-password-file=~/.ssh/.vsphere.mgmt \`
`--vm-name=hcs-VM-name \`
`--root-password-file=~/.ssh/.root \`
`--vm-address=hcs-address`
	`# vcav vsphere trust-ssh \`
	`--vsphere=mgmt-vsphere-name \`
	`--vm-name=hcs-VM-name \`
	`--root-password-file=~/.ssh/.root \`
	`--vm-address=hcs-address`

Connect to the vSphere Replication Cloud Service by running the following command.

Standard Command	Command Using Registry

`# vcav hcs connect \`
`--root-password-file=~/.ssh/.root \`
`--vm-address=hcs-address`
	`# vcav hcs connect \`
	`--hcs=hcs.01`

Reconnecting to a vSphere Replication Server Appliance

To create a trust with the vSphere Replication Server host, run the following command.

Standard Command	Command Using Registry

`# vcav vsphere trust-ssh \`
`--vsphere-address=$MGMT_VSPHERE_ADDRESS \`
`--vsphere-user=$MGMT_VSPHERE_USER \`
`--vsphere-password-file=~/.ssh/.vsphere.mgmt \`
`--vm-name=hbr-VM-name \`
`--root-password-file=~/.ssh/.root \`
`--vm-address=hbr-address`
	`# vcav vsphere trust-ssh \`
	`--vsphere=mgmt-vsphere-name \`
	`--vm-name=hbr-VM-name \`
	`--root-password-file=~/.ssh/.root \`
	`--vm-address=hbr-address`

Connect to the vSphere Replication Server by running the following command.

Standard Command	Command Using Registry

`# vcav hbr connect \`
`--root-password-file=~/.ssh/.root \`
`--vm-address=hbr-address`
	`# vcav hbr connect \`
	`--hbr=hbr.01`

Connecting to a Docker Host

Connect to a Docker host by running the following command.

Standard Command	Command Using Registry

`# vcav docker connect \`
`--root-password-file=~/.ssh/.root \`
`--vm-address=docker-address`
	`# vcav docker connect \`
	`--docker=docker-name`

Reconfiguring a vCloud Availability for vCloud Director Component

You can change the configuration settings of any vCloud Availability for vCloud Director component.

During configuration of vCloud Availability for vCloud Director components, you run `configure` command for each appliance. If you want to change the configuration settings of a vCloud Availability for vCloud Director component host, you run the `configure` command again with an extra `--reconfigure` argument.

Add a New vCenter Server to the Service Provider Environment

You can add a new vCenter Server to the Service Provider environment.

A use case for the `--reconfigure` argument is adding vCenter Server to the vCloud Availability for vCloud Director solution.

Procedure

1 Add the new vCenter Server instance to your existing vCloud Director appliance, to make its resources available for use. For more information, see https://kb.vmware.com/kb/1026866.

2 Deploy vSphere Replication Manager and vSphere Replication servers to your new vCenter Server instance. For more information, see Installing vCloud Availability for vCloud Director.

3 Configure your new vSphere Replication Management server. For more information, see Configure vSphere Replication Manager.

4 Configure vSphere Replication Cloud service host, to add the new vCenter Server in your *vsphere-address-list*.

   a You must run `vcav hcs configure` command with an extra `--reconfigure` argument.

```
# vcav hcs configure \
--reconfigure \
--hcs-address=HCS-address \
--amqp-password-file=~/.ssh/.amqp \
--cassandra-replication-factor=number-of-Cassandra-nodes \
--vcd-address=VCD-address \
--vcd-user=VCD-User \
--vcd-password-file=~/.ssh/.vcd \
--sso-user=SSO-User \
--sso-password-file=~/.ssh/.sso \
```

   The system returns an `OK` message, after the process finishes.

   b Run the following command to verify that the `hcs` service starts successfully.

```
# vcav hcs wait-for-extension \
--hcs-address=$HCS01_ADDRESS \
--vcd-address=$VCD_ADDRESS \
--vcd-user=$VCD_USER \
--vcd-password-file=~/.ssh/.vcd \
--sso-user=$SSO_USER \
--sso-password-file=~/.ssh/.sso
```

If the `hcs` service starts successfully, the system displays an `OK` message.

If the system returns an error, or there is no output in 5 minutes, check the `/opt/VMware/logs/hms/hcs.log` file for errors.

c Assign vSphere Replication Cloud Service rights to the vCloud Director *Organization Administrator* role.

- For vCloud Director 8.10 and earlier, you assign vSphere Replication Cloud Service rights to the *Organization Administrator* role and it applies to all organizations.

Standard Command	Command Using Registry

`# vcav hcs add-rights-to-role \`
`--vcd-address=$VCD_ADDRESS \`
`--vcd-user=$VCD_USER \`
`--vcd-password-file=~/.ssh/.vcd \`
`"--role=Organization Administrator"`
	`# vcav hcs add-rights-to-role \`
	`--vcd=vcd-01-name \`
	`"--role=Organization Administrator"`

- For vCloud Director 8.20 and above, you assign vSphere Replication Cloud Service rights to the *Organization Administrator* role for each organization or for all organizations.

	Standard Command	Command Using Registry

for each organization	`# vcav hcs add-rights-to-role \`
	`--vcd-address=$VCD_ADDRESS \`
	`--vcd-user=$VCD_USER \`
	`--vcd-password-file=~/.ssh/.vcd \`
	`"--role=Organization Administrator" \`
	`--org=org-name`
		`# vcav hcs add-rights-to-role \`
		`--vcd=vcd-01-name \`
		`"--role=Organization Administrator" \`
		`--org=org-name`

for all organizations	`# vcav hcs add-rights-to-role \`
	`--vcd-address=$VCD_ADDRESS \`
	`--vcd-user=$VCD_USER \`
	`--vcd-password-file=~/.ssh/.vcd \`
	`"--role=Organization Administrator" \`
	`--org=*`
		`# vcav hcs add-rights-to-role \`
		`--vcd=vcd-01-name \`
		`"--role=Organization Administrator" \`
		`--org=*`

Note You do not need to restart any component for the changes to take effect.

Deploy Cassandra and RabbitMQ as Containers for Test and Development Environments

Containers store metadata and support storage of the metadata for replication services.

Important Containers created using this procedure are suitable for test and development environments. For production environments, you must create Cassandra and RabbitMQ hosts enabled for an SSL communication. For more information about Cassandra hosts for production, see Install and Configure a Cassandra Server. For more information about installing and configuring RabbitMQ hosts for production, see Installing and Configuring RabbitMQ Servers.

Prerequisites

Verify that you have deployed and configured a vCloud Availability Installer Appliance in your environment.

Procedure

1 If you are using a Docker RabbitMQ or Cassandra nodes, you must first create a Docker host.

a Start the Docker service.

Standard Command	Command Using Registry
`# systemctl start docker`	`# systemctl start docker`

b Deploy a Docker Host VM.

Standard Command	Command Using Registry

`# vcav docker create \`
`--vsphere-address=$MGMT_VSPHERE_ADDRESS \`
`--vsphere-user=$MGMT_VSPHERE_USER \`
`--vsphere-password-`
`file=~/.ssh/.vsphere.mgmt \`
`"--network=$MGMT_VSPHERE_NETWORK" \`
`--ntp=pool.ntp.org \`
`--root-password-file=~/.ssh/.root \`
`"--vsphere-locator=$MGMT_VSPHERE_LOCATOR" \`
`--datastore=$MGMT_VSPHERE_DATASTORE \`
`--vm-name=vcav-docker01`
	`# vcav docker create \`
	`--vsphere=mgmt-vsphere-address \`
	`--ntp=pool.ntp.org \`
	`--root-password-file=~/.ssh/.root \`
	`--vm-name=vcav-docker01`

The system displays the IP address of the Docker host VM. Write it down as you need it during configuration steps.

c Set a variable to the address of the created VM.

Standard Command	Command Using Registry
`# DOCKER01_ADDRESS=`vcav vsphere get-ip \` `--vsphere-address=$MGMT_VSPHERE_ADDRESS \` `--vsphere-user=$MGMT_VSPHERE_USER \` `--vsphere-password-` `file=~/.ssh/.vsphere.mgmt \` `"--network=$MGMT_VSPHERE_NETWORK" \` `--vm-name=vcav-docker01`  `# AMQP_ADDRESS=$DOCKER01_ADDRESS`  `# CASSANDRA_ADDRESS=$DOCKER01_ADDRESS`	`# DOCKER01_ADDRESS=`vcav vsphere get-ip \` `--vsphere=mgmt-vsphere-name \` `"--network=mgmt-vsphere-network" \` `--vm-name=vcav-docker01`  `# AMQP_ADDRESS=$DOCKER01_ADDRESS`  `# CASSANDRA_ADDRESS=$DOCKER01_ADDRESS`

2 Download RabbitMQ and Cassandra images.

You can skip this step if you already have RabbitMQ 3.4 and Cassandra 2.2 images.

Standard Command	Command Using Registry

`# docker pull rabbitmq:3.4`
 	
`# docker pull cassandra:2.2.9`
	`# docker pull rabbitmq:3.4`
	
	`# docker pull cassandra:2.2.9`

3 Create a RabbitMQ Container.

Standard Command	Command Using Registry

`# vcav amqp create \`
`--docker-address=$DOCKER01_ADDRESS \`
`--container-name=vcav-amqp01 \`
`--amqp-port=5671 \`
`--amqp-user=vcd \`
`--amqp-password-file=~/.ssh/.amqp`
	`# vcav amqp create \`
	`--docker-address=$DOCKER01_ADDRESS \`
	`--container-name=vcav-amqp01 \`
	`--amqp-port=5671 \`
	`--amqp-user=vcd \`
	`--amqp-password-file=~/.ssh/.amqp`

Note Passwords that containing a dollar sign ($) are not supported in RabbitMQ versions earlier than 3.5.1.

4 Create a trusted connection with the RabbitMQ host.

Standard Command	Command Using Registry

`# vcav trust add \`
`--address=$DOCKER01_ADDRESS \`
`--port=5671 \`
`--accept-all`
	`# vcav trust add \`
	`--address=$DOCKER01_ADDRESS \`
	`--port=5671 \`
	`--accept-all`

5 Create a Cassandra Container.

Standard Command	Command Using Registry

`# vcav cassandra create \`
`--docker-address=$DOCKER01_ADDRESS \`
`--docker-image=cassandra:2.2.9 \`
`--container-name=vcav-cass01 \`
`--cassandra-port=9042`
	`# vcav cassandra create \`
	`--docker-address=$DOCKER01_ADDRESS \`
	`--docker-image=cassandra:2.2.9 \`
	`--container-name=vcav-cass01 \`
	`--cassandra-port=9042`

6 Import the vSphere Replication Cloud Service host certificates to your Cassandra host.

```
# vcav cassandra import-hcs-certificate \
--docker-address=$DOCKER01_ADDRESS \
--container-name=vcav-cass01 \
--hcs-address=$HCS01_ADDRESS
```

7 Register the Cassandra hosts with the lookup service by running the following command.

Repeat this step for every Cassandra host in your environment.

Standard Command	Command Using Registry

`# vcav cassandra register \`
`--hcs-address=$HCS01_ADDRESS \`
`--cassandra-address=$DOCKER01_ADDRESS \`
`--cassandra-port=9042 \`
`--vcd-address=$VCD_ADDRESS \`
`--vcd-user=$VCD_USER \`
`--vcd-password-file=~/.ssh/.vcd \`
`--sso-user=$SSO_USER \`
`--sso-password-file=~/.ssh/.sso`
	`# vcav cassandra register \`
	`--hcs-address=$HCS01_ADDRESS \`
	`--cassandra-address=$DOCKER01_ADDRESS \`
	`--cassandra-port=9042 \`
	`--vcd=vcd-01-name`

The system displays an `OK` message upon a successful registration.

Managing Containers for Test and Development Environments

vCloud Availability Installer Appliance contains Docker administration scripts to ease RabbitMQ and Cassandra containers management.

Accessing the Docker Shell

You can access the container shell using your vCloud Availability Installer Appliance.

1 Connect to your vCloud Availability Installer Appliance over SSH using your **root** credentials.

2 Run the following command.

```
# docker exec -it <container-name> /bin/bash
```

Running Single Command on a Docker Container

1 Connect to your vCloud Availability Installer Appliance over SSH using your **root** credentials.

2 Use the following syntax to run command on the container.

```
# docker exec <container-name> <command>
```

Example commands

```
# docker exec vcav-amqp01 rabbitmqctl list_users

# docker exec vcav-cass01 cqlsh --ssl '-e show version'
```

Review Docker Container Logs

1 Connect to your vCloud Availability Installer Appliance over SSH using your **root** credentials.

2 Run the following command to view container logs.

```
# docker logs <container-name>
```

The configuration and log files for each container are stored in the `/srv/docker` directory of your Docker host.

Configuring vCloud Director Organizations

You can use the vCloud Availability Installer Appliance scripts to manage vCloud Director organizations for replication.

List the vCloud Director Organizations

You can view either all the organizations or all the organizations VDC for vCloud Director.

Procedure

1 Connect to the vCloud Availability Installer Appliance over SSH using **root** credentials.

2 To list all the organizations for vCloud Director, run the following command.

Standard Command	Command Using Registry

`# vcav org list \`
`--vcd-address=$VCD_ADDRESS \`
`--vcd-user=$VCD_USER \`
`--vcd-password-file=~/.ssh/.vcd`
	`# vcav org list \`
	`--vcd=vcd-01-name`

3 To list all the organizations VDC for vCloud Director, run the following command.

Standard Command	Command Using Registry

`# vcav org-vdc list \`
`--vcd-address=$VCD_ADDRESS \`
`--vcd-user=$VCD_USER \`
`--vcd-password-file=~/.ssh/.vcd \`
`--org=org1`
	`# vcav org-vdc list \`
	`--vcd=vcd-01-name \`
	`--org=org1`

Enable vCloud Director Organization VDC for Replication

You can enable a vCloud Director organization VDC for replication.

Prerequisites

Verify that you have assigned vSphere Replication Cloud Service rights to the vCloud Director *Organization Administrator* role for the organization. For more information, see the `vcav hcs add-rights-to-role` command in Assign vSphere Replication Cloud Service Rights to thevCloudDirector Organization Administrator Role.

Procedure

1 Create an SSH connection to the vCloud Availability Installer Appliance.

2 To enable an organization VDC for replication, run the following commands.

Standard Command	Command Using Registry

`# vcav org-vdc enable-replication \`
`--vcd-address=$VCD_ADDRESS \`
`--vcd-user=$VCD_USER \`
`--vcd-password-file=~/.ssh/.vcd \`
`--org=org1 \`
`--vdc=vdc_org1`
	`# vcav org-vdc enable-replication \`
	`--vcd=vcd-01-name \`
	`--org=org1 \`
	`--vdc=vdc_org1`

After the process finishes, you get an OK message.

Disable vCloud Director Organization VDC for Replication

You can disable a vCloud Director organization VDC for replication.

Prerequisites

Verify that you have assigned vSphere Replication Cloud Service rights to the vCloud Director *Organization Administrator* role for the organization. For more information, see the `vcav hcs add-rights-to-role` command Assign vSphere Replication Cloud Service Rights to thevCloudDirector Organization Administrator Role.

Procedure

1 Create an SSH connection to the vCloud Availability Installer Appliance.

2 To disable an organization VDC for replication, run the following commands.

Standard Command	Command Using Registry

`# vcav org-vdc disable-replication \`
`--vcd-address=$VCD_ADDRESS \`
`--vcd-user=$VCD_USER \`
`--vcd-password-file=~/.ssh/.vcd \`
`--org=org1 \`
`--vdc=vdc_org1`
	`# vcav org-vdc disable-replication \`
	`--vcd=vcd-01-name \`
	`--org=org1 \`
	`--vdc=vdc_org1`

After the process finishes, you get an OK message.

Password Management

For security reasons, you must change the passwords for the vCloud Availability for vCloud Director infrastructure and its components regularly.

Handling Password Changes of Infrastructure Components

You can change the passwords for the infrastructure components of the vCloud Availability for vCloud Director solution.

Change the Password for a vCloud Director System Administrator User

You can change the password for a vCloud Director System Administrator user.

Procedure

1 Update the Password for a vCloud Director System Administrator User

You can only edit account information for local users.

2 Configure vCloud Availability for vCloud Director with the New Password

After you change the password for the vCloud Director System Administrator account, you must configure vCloud Availability for vCloud Director to access vCloud Director.

3 Configure Service Manager Portal with the New Password

After you configure vCloud Availability for vCloud Director, you must also configure Service Manager.

Update the Password for a vCloud Director System Administrator User

You can only edit account information for local users.

Prerequisites

Verify that the new password meets the corporate requirements for password complexity of your organization.

Procedure

1 Log in to the vCloud Director Web console at **https://VCD IP** or at **hostname/cloud/login.jsp**.

You must use a System Administrator account.

2 Select the **Administration** tab.

3 Under **System Administrator & Roles**, select **Users**.

4 To open the **User Properties** dialog box, click the System Administrator account.

5 Type the new password in the **Password** and **Confirm** fields.

6 Click **OK**.

Configure vCloud Availability for vCloud Director with the New Password

After you change the password for the vCloud Director System Administrator account, you must configure vCloud Availability for vCloud Director to access vCloud Director.

Procedure

1 Create an SSH connection to the vCloud Availability Installer Appliance.

2 Use a text editor to open the **~/.vcav/registry** file.

3 Update the **api-password** value under the corresponding vCloud Director entry.

Configure Service Manager Portal with the New Password

After you configure vCloud Availability for vCloud Director, you must also configure Service Manager.

Procedure

- Run the reconfiguring command on the vCloud Availability Installer Appliance

```
# vcav vcd-ui configure-smp --reconfigure \
--ui-address=$SMPORTAL_01_ADDRESS \
--vcd=<vcd alias from registry file> \
--truststore-password-file=<path to truststore password file> \
--mongodb-password-file=<path to mongodb password file>
```

Change the Password of a vCloud Director Organization User

You can change the password for a vCloud Director organization user. You can only edit account information for local users within a given vCloud Director organization.

Procedure

1 Change the Password for a vCloud Director Organization User using a System Administrator account

   You can change the password for a vCloud Director organization user using a System Administrator account.

2 Change the Password for a vCloud Director Organization User Using a vCloud Director Organization Administrator Account

   You can change the password for a vCloud Director organization user using a vCloud Director Organization Administrator account.

3 Configure vCloud Availability for vCloud Director with the New Password

   After you change the password for a tenant vCloud Director organization being used to configure replications to cloud, you must update the tenant on-premise vSphere environment.

Change the Password for a vCloud Director Organization User using a System Administrator account

You can change the password for a vCloud Director organization user using a System Administrator account.

Prerequisites

Verify that the new password meets the corporate requirements for password complexity of your organization.

Procedure

1. Log in to vCloud Director web console at **https://VCD IP** or **hostname/cloud/login.jsp**.

   You must use a System Administrator account.
2. On the **Home** page, under **Organizations**, select **Manage organizations**.
3. In the **Organizations** list, double-click on the account's organization.
4. Click the **Administration** tab.
5. In the left pane, select **Users** under **Members**.
6. Find the User in the list and double-click on it.
7. Update the **Password** and **Confirm Password** fields with the new password and click **OK**.

Change the Password for a vCloud Director Organization User Using a vCloud Director Organization Administrator Account

You can change the password for a vCloud Director organization user using a vCloud Director Organization Administrator account.

Prerequisites

Verify that the new password meets the corporate requirements for password complexity of your organization.

Procedure

1. Log in to vCloud Director web console at **https://VCD IP** or **hostname/cloud/org/<*tenant_org_name*>.**

   Set <*tenant_org_name*> to the organization name for the tenant.

   You must use an Organization Administrator account.
2. Click the **Administration** tab.
3. In the left pane, select **Users** under **Members**.
4. Find the User in the list and double-click on it.
5. Update the **Password** and **Confirm Password** fields with the new password and click **OK**.

Configure vCloud Availability for vCloud Director with the New Password

After you change the password for a tenant vCloud Director organization being used to configure replications to cloud, you must update the tenant on-premise vSphere environment.

Procedure

1. Using vSphere Web Client, log in to the tenant vCenter environment.

   You must use an Administrator account.
2. On the vSphere Web Client **Home** page, select **vSphere Replication**.
3. In the vSphere Replication list, select the appropriate vCenter and in the toolbar select **Manage**.

4 In the vSphere Replication **Manage** page, select **Target Sites**.

5 In the **Target Sites** list, right click the corresponding vCloud Director target entry whose replication account password is changed and select **Reconnect Sites**.

6 On the **Reconnect Sites** confirmation dialog box, select **Yes**.

7 Fill in the vCloud Director organization user name and the updated password and click OK.

Change the Password for a vCloud Director or Cloud Proxy Root User

You can change the password for the root user on an vCloud Director or Cloud Proxy instance.

Prerequisites

Verify that the new password meets the corporate requirements for password complexity of your organization.

Procedure

1 Log in to vCloud Director or Cloud Proxy instance through SSH.

You must use **root** credentials.

2 Run the `passwd root` command.

3 Follow the on-screen prompts to enter a new or confirmation password for the **root** user.

4 Reconfigure the associated vSphere Replication Cloud Service host.

a Log in to the vCloud Availability Installer Appliance.

b Run the following command.

Standard Command

```
# vcav hcs configure \
--reconfigure \
--hcs-address=$HCS_ADDRESS \
--amqp-password-file=~/.ssh/.amqp \
--cassandra-replication-factor=number-of-
Cassandra-nodes \
--vcd-address=$VCD_ADDRESS \
--vcd-user=$VCD_USER \
--vcd-password-file=~/.ssh/.vcd \
--sso-user=$SSO_USER \
--sso-password-file=~/.ssh/.sso
```

Command Using Registry

```
# vcav hcs configure \
--reconfigure \
--hcs-address=$HCS_ADDRESS \
--amqp-password-file=~/.ssh/.amqp \
--cassandra-replication-factor=number-of-
Cassandra-nodes \
--vcd=vcd-01-name
```

Change the Password for a vCloud Director Database User

After your database administrator changes the password for the vCloud Director database, you must update all the vCloud Director and Cloud Proxy instances with the new password.

Note Plan downtime of the system until you update at least one vCloud Director instance with the new database password.

Prerequisites

Verify that the database administrator has changed the password for the vCloud Director database.

Procedure

1 Log in to vCloud Director or Cloud Proxy instance through SSH.

You must use **root** credentials.

2 To update the configuration of the vCloud Director or Cloud Proxy instance and leave all other connection properties unchanged, run the following command:

```
#cell-management-tool reconfigure-database \
-dbuser vcd-dba -dbpassword <new-password>
```

You can locate the cell management tool in the `/opt/vmware/vcloud-director/bin/cell-management-tool` directory.

3 Reboot the vCloud Director or Cloud Proxy instance.

What to do next

You must perform the procedure on all vCloud Director and Cloud Proxy instances within your environment.

For more information about vCloud Director database administration, see the *vCloud Director Administrator's Guide*.

Change the Password for an ESXi Host Root User

You can change the password for the root user on a tenant or service provider ESXi host.

Prerequisites

Verify that the new password meets the corporate requirements for password complexity of your organization.

Procedure

1 Log in to the ESXi host over SSH by using your **root** credentials.

2 Run the `passwd root` command.

3 Follow the on-screen prompts to enter a new password for the **root** user.

Change the Password for an NSX Manager Admin User

You can change the password for the admin user account for an NSX appliance.

Prerequisites

- Verify that the new password meets the corporate requirements for password complexity of your organization.

- Change the admin user account and Privileged mode passwords after initial log-in, to harden access to the CLI of an NSX virtual appliance.

Procedure

1. Log in to the vSphere Web Client and select an NSX virtual appliance from the inventory.
2. To open a CLI session, select the **Console** tab.
3. Log in to the CLI and switch to Privileged mode by running the command:

```
manager> enable
password:
manager#
```

4. Switch to Configuration mode by running the command:

```
manager# configure terminal
```

5. Change the admin account password by running the command:

```
manager(config)# cli password PASSWORD
```

6. Save the configuration:

```
manager(config)# write memory
Building Configuration...
Configuration saved.
[OK]
```

7. Add the new password to vCloud Director.
   a. Log in to vCloud Director.
   b. Navigate to **Manage and Monitor**.
   c. Select the vCenter Server that is associated with NSX Manager.
   d. Right click **vCenter Server > Properties > NSX Manager**.
   e. Verify the IP address of the NSX Manager and add the new password.

Change the Password for an NSX Controller

You can change the password for an NSX Controller.

Prerequisites

Verify that the new password meets the corporate requirements for password complexity of your organization.

Procedure

1. Log in to the vSphere Web Client.
2. Select **Networking & Security** and then select **Installation**.

3 Under **Management**, select the controller for which you want to change the password.

4 Click **Actions** and then click **Change Controller Cluster Password**.

5 Enter a new password and click **OK**.

Change the Password for a vCenter Server Root User

You can change the password for the root user on a tenant or service provider vCenter Server instance. The default root password for the vCenter Server instance is the password you enter during the deployment of the virtual appliance.

Prerequisites

Verify that the new password meets the corporate requirements for password complexity of your organization.

Procedure

1 Browse to the vCenter Server Appliance in the vSphere Web Client or the vSphere Client inventory.

2 On the **Summary** tab, click **Launch Console**.

3 Click inside the console window and press F2 to customize the system.

4 To log in to the Direct Console User Interface, type the current password of the root user and press Enter.

5 Select **Configure Root Password** and press Enter.

6 Type the old password of the root user, and press Enter.

7 Set up the new password and press Enter.

8 Press Esc until you return to the main menu of the Direct Console User Interface.

Change the Password for a vCenter Single Sign-On Administrator User

You can change the password for the Single Sign-On Administrator for a tenant or service provider vCenter Server instance.

Procedure

1 Update the Password for a vCenter Single Sign-On Administrator User

2 Update NSX Manager with the New Password

3 Update vCloud Director with the New Password

After you update NSX Manager, you must update vCloud Director.

4 Configure vCloud Availability for vCloud Director with the New Password

You must update vCloud Availability for vCloud Director with the new password for the Single Sign-On Administrator for the vCenter instance.

Update the Password for a vCenter Single Sign-On Administrator User

Prerequisites

Verify that the new password meets the corporate requirements for password complexity of your organization.

Procedure

1. From a Web browser, connect to the Platform Services Controller by specifying the following URL: *https://psc_hostname_or_IP/psc*

   In an embedded deployment, the Platform Services Controller host name, or IP address is the same as the vCenter Server host name or IP address.
2. Specify the user name and password for the *administrator@vsphere.local* user or another member of the vCenter Server Single Sign-On Administrators group.
3. In the upper navigation pane, to the left of the Help menu, click your user name to pull down the menu.
4. As an alternative, you can select **Single Sign-On** > **Users and Groups** and select **Edit User** from the right-button menu.
5. Select **Change Password** and type your current password.
6. Type a new password and confirm it.
7. Click **OK**.

Update NSX Manager with the New Password

After you change the password for the Single Sign-On Administrator for a vCenter Server instance, you must update NSX Manager.

If you use the *administrator@vsphere.local* user to connect NSX Manager to vCenter , you must perform the following procedure.

Procedure

1. In a Web browser, navigate to the NSX Manager appliance GUI at **https://<nsx-manager-ip>** or **https://<nsx-manager-hostname>**, and log in as admin.
2. From the home page, click **Manage vCenter Registration**.
3. Click Edit in the Lookup Service URL section.
4. Type the new password in the **Password** field.
5. Click OK.
6. Click Edit in the **vCenter Server** section.
7. Type the new password in the **Password** field.
8. Click OK.

9 Refresh the web page and verify the **Status** fields indicate **Connected**.

Update vCloud Director with the New Password

After you update NSX Manager, you must update vCloud Director.

If you use an *administrator@vsphere.local* user account to connect NSX Manager to vCenter, you must perform the following procedure.

Procedure

1 Log in to vCloud Director Web console at **https://VCD IP** or **hostname/cloud/login.jsp**.

You must use a System Administrator account.

2 Select **Manage & Monitor** tab.

3 Select **vCenters** under **vSphere Resources**.

4 Click the corresponding vCenter to open the **vCenter Properties** dialog box.

5 Under the **General** tab, update the **Password** text box with the new password.

6 If you use *administrator@vsphere.local* to attach to NSX Manager, update the **Password** text box on the **vShield Manager** tab.

7 Click OK.

Configure vCloud Availability for vCloud Director with the New Password

You must update vCloud Availability for vCloud Director with the new password for the Single Sign-On Administrator for the vCenter instance.

Procedure

1 Update a Local User Account

2 Update an Single Sign-On Account

3 Update Password Files

If you have protected password files on the vCloud Availability Installer Appliance for the *administrator@vsphere.local* user, you must perform the following procedure.

Update a Local User Account

If you use the *administrator@vsphere.local* user to connect to a vCenter Server instance, you must perform the following procedure.

Procedure

1 Create an SSH connection to vCloud Availability Installer Appliance.

2 Use a text editor to open the **~/.vcav/registry** file.

3 Update the **api-password** value under the corresponding vSphere entry.

Update an Single Sign-On Account

If you use the *administrator@vsphere.local* user as a Single Sign-On account, you must perform the following procedure.

Procedure

1 Create an SSH connection to vCloud Availability Installer Appliance.

2 Use a text editor to open the **~/.vcav/registry** file.

3 Update the **sso-password** value under the vCloud Director entry.

Update Password Files

If you have protected password files on the vCloud Availability Installer Appliance for the *administrator@vsphere.local* user, you must perform the following procedure.

Procedure

1 On the vCloud Availability Installer Appliance in the `.ssh` directory, update the protected password files with the new password.

2 Update the Service Manager by running the reconfiguring command on the vCloud Availability Installer Appliance

```
# vcav vcd-ui configure-smp --reconfigure \
--ui-address=$SMPORTAL_01_ADDRESS \
--vcd=<vcd alias from registry file> \
--truststore-password-file=<path to truststore password file> \
--mongodb-password-file=<path to mongodb password file>
```

Handling Password Changes of Solution Components

You can change the passwords for the vCloud Availability for vCloud Director components.

Change the Password for a RabbitMQ Server Admin User

You can change the password for the admin user of the RabbitMQ server.

Note Plan downtime of the system during the execution of the password change procedure.

Prerequisites

Verify that the new password meets the corporate requirements for password complexity of your organization.

Procedure

1 Connect to the RabbitMQ server over SSH.

2 Set the new password by running the `rabbitmqctl change_password admin vmware-new` command.

   For more information on changing the RabbitMQ password, see the Rabbitmqctl Manual Page.

3 Connect to your vCloud Availability Installer Appliance over SSH by using your **root** credentials.

4 Create or modify the new file by running the following vCloud Availability Installer Appliancecommands.

```
# vi ~/.ssh/.amqp_new
# chmod 0600 ~/.ssh/.amqp_new
```

5 Update the link from vCloud Director to RabbitMQ by running the command:

```
vcav vcd configure-amqp \
--vcd=vcd \
--amqp-address=$AMQP_ADDRESS \
--amqp-port=5671 \
--amqp-user=admin \
--amqp-password-file=~/.ssh/.amqp_new \
--amqp-vhost=/ \
--amqp-exchange=systemExchange
```

6 Reboot all the vCloud Director instances.

7 Reboot all the Cloud Proxy instances.

8 Run the following command:

```
vcav trust add-ssh \
--accept-all \
--address=$HCS_ADDRESS \
--root-password-file=~/.ssh/.root
```

9 Update vCloud Director configuration by reconfiguring all the vSphere Replication Cloud Service hosts:

```
vcav hcs configure --reconfigure \
--hcs-address=$HCS01_ADDRESS \
--amqp-password-file=~/.ssh/.amqp_new \
--cassandra-replication-factor=3 \
--vcd=vcd

vcav hcs wait-for-extension \
--hcs-address=$HCS01_ADDRESS \
--vcd=vcd
```

Change the Password for a Cassandra Host

You can change the password for a Cassandra host.

Prerequisites

Verify that the new password meets the corporate requirements for password complexity of your organization.

Procedure

1. Connect to the Cassandra host over SSH using **root** credentials.
2. Run the `# passwd root` command.
3. Follow the on-screen prompts to enter a new and confirmation password for the **root** user.

Change the Password for a vSphere Replication Server Appliance

You can change the password for a vSphere Replication Server appliance by using the Virtual Appliance Management Interface (VAMI).

Prerequisites

- Verify that the vSphere Replication Server is powered on.
- Verify that the new password meets the corporate requirements for password complexity of your organization.

Procedure

1. Use a supported browser to log in to the vSphere Replication Server VAMI.

   The URL for the VAMI is **https://vrs-appliance-address:5480**
2. Enter the **root** user name and the password for the appliance.

   You configured the root password during the OVF deployment of the vSphere Replication Server appliance.
3. Select the **VRS** tab and click **Security**.
4. Enter the current password in the **Current Password** field.
5. Enter the new password in the **New Password** and the **Confirm New Password** fields.
6. To change the password, click **Apply**.

Change the Password for a vSphere Replication Management Server Appliance

You can change the password for avSphere Replication Manager appliance by using the Virtual Appliance Management Interface (VAMI).

Prerequisites

- Verify that the vSphere Replication Manager is powered on.

- Verify that the new password meets the corporate requirements for password complexity of your organization.

Procedure

1. Use a supported browser to log in to the vSphere Replication Manager VAMI.

   The URL for the VAMI is **https://vrms-appliance-address:5480**
2. Enter the **root** user name and the password for the appliance.

   You configured the root password during the OVF deployment of the vSphere Replication Manager appliance.
3. Select the **VR** tab and click **Security**.
4. Enter the current password in the **Current Password** field.
5. Enter the new password in the **New Password** and the **Confirm New Password** fields.
6. To change the password, click **Apply**.

Change the Password for a vSphere Replication Cloud Service Appliance

You can change the password for a vSphere Replication Cloud Service appliance by using the Virtual Appliance Management Interface (VAMI).

Prerequisites

- Verify that the vSphere Replication Cloud Service is powered on.
- Verify that the new password meets the corporate requirements for password complexity of your organization.

Procedure

1. Use a supported browser to log in to the vSphere Replication Cloud Service VAMI.

   The URL for the VAMI is **https://vrcs-appliance-address:5480**
2. Enter the **root** user name and the password for the appliance.

   You configured the root password during the OVF deployment of the vSphere Replication Cloud Service appliance.
3. Select the **VRCS** tab and click **Security**.
4. Enter the current password in the **Current Password** field.
5. Enter the new password in the **New Password** and the **Confirm New Password** fields.
6. To change the password, click **Apply**.

Change the Password for a vCloud Availability for vCloud Director Portal Host Root User

You can change the password for the root user for the vCloud Availability for vCloud Director Portal host.

Prerequisites

Verify that the new root password meets your organization's corporate password complexity requirements.

Procedure

1. Connect to the vCloud Availability for vCloud Director Portal host over SSH using **root** credentials.
2. Run the `# passwd root` command.
3. Follow the on-screen prompts to enter a new/confirmation password for the **root** user.

What to do next

After you change the password for the root user for the vCloud Availability for vCloud Director Portal host, you must edit the corresponding truststore password file with the new root password.

Change the Password for a Service Manager Portal Host Root User

You can change the password for the root user for the
vCloud Availability for vCloud Director Service Manager Portal host at any time.

Prerequisites

Verify that the new root password meets your organization's corporate password complexity requirements.

Procedure

1. Connect to the vCloud Availability for vCloud Director Service Manager Portal host over SSH using **root** credentials.
2. Run the `# passwd root` command.
3. Follow the on-screen prompts to enter a new and confirmation password for the **root** user.

What to do next

After you change the password for the root user for the
vCloud Availability for vCloud Director Service Manager Portal host, you must edit the corresponding truststore password file with the new root password.

Certificate Management

You can use the vCloud Availability Installer Appliance to create trust connections and handle certificate updates.

Trust Types

The vCloud Availability Installer Appliance uses the following methods to trust certificates.

- Create a trust by using the SSL certificate for a specific IP address and port.
- Create a trust with a host VM by using SSH certificate.
- The vCloud Availability Installer Appliance can determine that a certificate is trusted from another endpoint, that is trusted using SSL or SSH certificate.

Endpoint Types

The vCloud Availability for vCloud Director solution interacts with the following certificate endpoints.

- vCloud Director
- vCenter Server
- vCenter Server Lookup Service
- ESXi
- RabbitMQ
- Cassandra
- vSphere Replication Manager
- vSphere Replication Cloud Service
- vSphere Replication Server
- vCloud Availability for vCloud Director Portal
- vCloud Availability for vCloud Director Service Manager Portal

Create a Certificate Trust

You can create a certificate trust by running `vcav trust add` command on the vCloud Availability Installer Appliance.

The trust relationship entry is stored in `~/.vcav` directory of the vCloud Availability Installer Appliance. Recreate trusts if you remove the `~/.vcav` directory, or you replace the vCloud Availability Installer Appliance.

Following are examples of using the `vcav trust add` command.

```
# vcav trust add --address=IP-address --port=443 --accept all
```

The system returns the following message.

```
WARNING  – Trusting 35:AA:07:A4:96:72:89:A6:9B:32:8B:38:83:9F:82:86:53:65:39:76 for IP–address:443
OK
```

You can use the thumbprint value as an argument in the `vcav trust add` command.

```
# vcav trust add ––address=IP–address \
––port=443 ––thumbprint=35:AA:07:A4:96:72:89:A6:9B:32:8B:38:83:9F:82:86:53:65:39:76
```

The vCloud Availability Installer Appliance displays an `OK` message.

Using the vCloud Availability Installer Appliance you can create a trust with a new vCenter Server instance by using the following command.

```
vcav trust add ––address=vsphere–IP–address ––port=port–number ––accept–all
```

The system returns the following message.

```
WARNING  – Trusting 35:AA:07:A4:96:72:89:A6:9B:32:8B:38:83:9F:82:86:53:65:39:76 for IP–address:443
OK
```

You can create a trust with a new vCloud Director instance.

Standard Command	Command Using Registry

`# vcav trust add \`
`––address=vcd–IP–address \`
`––port=port–number \`
`––accept–all`
	`# vcav trust add \`
	`––vcd=vcd–name \`
	`––port=port–number \`
	`––accept–all`

Create a Host Trust

You create a trust with a host virtual machine by using SSH connection with the vCloud Availability Installer Appliance.

The vCloud Availability Installer Appliance must trust the SSH certificate of the virtual machine. You connect the vCloud Availability Installer Appliance to the VM using a private SSH key.

You can use the SSH connection to the virtual machine to inspect the SSL certificate for a particular port.

Following are examples of creating a host trust.

The following command creates a host trust with a vSphere Replication Manager by running the `vcav vsphere trust–ssh` command on the vCloud Availability Installer Appliance.

Standard Command	Command Using Registry

`# vcav vsphere trust-ssh \`
`--vsphere-address=$VSPHERE_ADDRESS \`
`--vsphere-user=$SSO_USER \`
`--vsphere-password-file=~/.ssh/.sso \`
`--vm-name=hms \`
`--vm-address=hms-IP-address \`
`--root-password-file=~/.ssh/.root`
	`# vcav vsphere trust-ssh \`
	`--vsphere=vsphere-name \`
	`--vm-name=hms \`
	`--vm-address=hms-IP-address \`
	`--root-password-file=~/.ssh/.root`

The system returns an `OK` message, after the process finishes.

Alternatively, you can create a host trust by running the `vcav trust add-ssh` command on the vCloud Availability Installer Appliance.

```
# vcav trust add-ssh \
--address=VM-IP-address \
--root-password-file= /root/.ssh/.root \
--thumbprint=35:AA:07:A4:96:72:89:A6:9B:32:8B:38:83:9F:82:86:53:65:39:76
```

The system returns an `OK` message, after the process finishes.

Handling Certificate Updates

The vCloud Availability for vCloud Director solution is comprised of multiple components with individual certificate update procedure.

Handling vSphere Certificate Updates

Updating the vSphere SSL certificates might require a reconfiguration of vCloud Availability for vCloud Director components in both the service provider and the tenant environments.

Updating Service Provider vSphere Certificates

If you update the vSphere machine SSL certificate, you must reconfigure all vSphere Replication Manager hosts and vSphere Replication Cloud Service hosts.

Updating the solution user certificate of vSphere and the ESXi certificate does not require reconfiguring any of the vCloud Availability for vCloud Director components.

Add an Updated vSphere Machine SSL Certificate to vCloud Availability for vCloud Director

To add an updated vSphere machine SSL certificate to vCloud Availability for vCloud Director, you must reconfigure the vSphere Replication Manager and vSphere Replication Cloud Service hosts.

Prerequisites

Verify that you successfully replaced the vSphere machine SSL certificate. For more information about vSphere security certificates, see the following:

- For vSphere 6.5, see vSphere Security Certificates in the *Platform Services Controller Administration* documentation.

- For vSphere 6.0, see vSphere Security Certificates in the *Platform Services Controller Administration* documentation.

Procedure

1 From the vCloud Availability Installer Appliance, create a trust between the vSphere instance and the vCloud Availability Installer Appliance by running the following command:

```
# vcav trust add --address=$VSPHERE_ADDRESS --port=443 --accept-all
```

2 Reconfigure the associated vSphere Replication Manager.

Standard Command

```
# vcav hms configure \
--reconfigure \
--hms-address=$HMS_ADDRESS \
--vsphere-address=$VSPHERE_ADDRESS \
--vsphere-user=$SSO_USER \
--vsphere-password-file=~/.ssh/.sso \
--vcd-address=$VCD_ADDRESS \
--vcd-user=$VCD_USER \
--vcd-password-file=~/.ssh/.vcd \
--sso-user=$SSO_USER \
--sso-password-file=~/.ssh/.sso
```

Command Using Registry

```
# vcav hms configure \
--reconfigure \
--hms-address=$HMS_ADDRESS \
--vsphere=vsphere-name \
--vcd=vcd-name
```

The system returns an `OK` message, after the process finishes.

3 Verify that the `hms` service starts successfully.

Standard Command

```
# vcav hms wait-for-extension \
--hms-address=$HMS01_ADDRESS \
--vsphere-address=$VSPHERE01_ADDRESS \
--vsphere-user=$SSO_USER \
--vsphere-password-file=~/.ssh/.sso \
--vcd-address=$VCD_ADDRESS \
--vcd-user=$VCD_USER \
--vcd-password-file=~/.ssh/.vcd \
--sso-user=$SSO_USER \
--sso-password-file=~/.ssh/.sso
```

Command Using Registry

```
# vcav hms wait-for-extension \
--hms-address=$HMS01_ADDRESS \
--vsphere=vsphere-01-name \
--vcd=vcd-01-name
```

If the `hms` service starts successfully, the system displays an `OK` message.

If the system returns an error, or there is no output in 5 minutes, check the `/opt/vmware/logs/hms/hms.log` file.

4 Reconfigure the vSphere Replication Cloud Service Appliance.

The `cassandra-replication-factor` argument in the `vcav hcs configure` command defines the number of data replicas across the Cassandra cluster. Replication factor **4** means that there are four copies of each row, where each copy is on a different node.

Note The replication factor must not exceed the number of nodes in the Cassandra cluster.

By default, the `vcav hcs configure` command uses the AMQP settings from vCloud Director. If vCloud Director is configured to communicate with AMQP without SSL, the `vcav hcs configure` operation returns an error. To avoid this, you can specify the correct port to use with the `--amqp-port=`*port-number* argument.

Run the `vcav hcs configure` command for all vSphere Replication Cloud Service hosts.

Standard Command	Command Using Registry

`# vcav hcs configure \`
`--reconfigure \`
`--hcs-address=`*$HCS_ADDRESS* `\`
`--amqp-password-file=~/.ssh/.amqp \`
`--cassandra-replication-factor=`*number-of-Cassandra-nodes* `\`
`--vcd-address=`*$VCD_ADDRESS* `\`
`--vcd-user=`*$VCD_USER* `\`
`--vcd-password-file=~/.ssh/.vcd \`
`--sso-user=`*$SSO_USER* `\`
`--sso-password-file=~/.ssh/.sso`
	`# vcav hcs configure \`
	`--reconfigure \`
	`--hcs-address=`*$HCS_ADDRESS* `\`
	`--amqp-password-file=~/.ssh/.amqp \`
	`--cassandra-replication-factor=`*number-of-Cassandra-nodes* `\`
	`--vcd=`*vcd-01-name*

The system returns an `OK` message, after the process finishes.

5 Verify that the `hcs` service starts successfully.

Standard Command	Command Using Registry

`# vcav hcs wait-for-extension \`
`--hcs-address=`*$HCS01_ADDRESS* `\`
`--vcd-address=`*$VCD_ADDRESS* `\`
`--vcd-user=`*$VCD_USER* `\`
`--vcd-password-file=~/.ssh/.vcd \`
`--sso-user=`*$SSO_USER* `\`
`--sso-password-file=`*~/.ssh/.sso*
	`# vcav hcs wait-for-extension \`
	`--hcs-address=`*$HCS01_ADDRESS* `\`
	`--vcd=`*vcd-01-name*

If the `hcs` service starts successfully, the system displays an `OK` message.

If the system returns an error, or there is no output in 5 minutes, check the `/opt/VMware/logs/hms/hcs.log` file.

You have successfully added the updated vSphere machine SSL certificate to the vCloud Availability for vCloud Director instance.

Update the vCloud Director Certificate

After you update the vCloud Director certificate, you must configure all related components to work with the new certificate.

Procedure

1. Update the vCloud Director certificate. For more information on how to create and import a signed SSL certificate, see the *vCloud Director Installation and Upgrade Guide.*
2. Update the vCloud Director public endpoint configuration. For more information on how to customize public endpoints, see the *vCloud Director Administrator's Guide.*

   If you have not configured vCloud Director public endpoints, you can skip this step.
3. To use the new certificate, update all Cloud Proxy hosts. For more information, see (Optional) Create Cloud Proxy.

   If the Cloud Proxy hosts use their own certificates and these certificates are not expiring, you can skip this step.
4. Register the vCenter Server Lookup Service.
   a. Log in to the vCloud Director Web console.
   b. Unregister the vCenter Server Lookup Service.
   c. Disable SSO.
   d. Register the vCenter Server Lookup Service.
   e. Enable SSO.
5. Create a trust for the vCloud Director certificate. For more information, see Create a Certificate Trust.

6 Configure vSphere Replication Cloud Service host.

Repeat this step for every vSphere Replication Cloud Service host.

a Create an SSH connection to the vSphere Replication Cloud Service host.

b Restart the `hcs` service by running the `service hcs restart` command.

c Verify that the `hcs` service starts successfully.

Standard Command

```
# vcav hcs wait-for-extension \
--hcs-address=$HCS_ADDRESS \
--vcd-address=$VCD_ADDRESS \
--vcd-user=$VCD_USER \
--vcd-password-file=~/.ssh/.vcd \
--sso-user=$SSO_USER \
--sso-password-file=~/.ssh/.sso \
```

Command Using Registry

```
# vcav hcs wait-for-extension \
--hcs-address=$HCS_ADDRESS \
--vcd=vcd-name
```

If the `hcs` service starts successfully, the system displays an `OK` message.

If the system returns an error, or there is no output in 5 minutes, check the `/opt/VMware/logs/hms/hcs.log` file.

7 Configure the vCloud Availability for vCloud Director Portal hosts to use the new vCloud Director certificate by running the following command.

Standard Command

```
# vcav vcd-ui configure \
--reconfigure \
--ui-address=$UI01_ADDRESS \
--vcd-address=vcd-address \
--vcd-user=$VCD_USER \
--vcd-password-file=~/.ssh/.vcd
```

Command Using Registry

```
# vcav vcd-ui configure \
--reconfigure \
--ui-address=$UI_ADDRESS \
--vcd=vcd-name
```

The system returns an `OK` message, after the process finishes.

You have successfully updated the vCloud Director certificate.

What to do next

If you are using a self-signed certificate and you change the certificate for the to-the-cloud endpoint, you must update the tenant vSphere Replication Appliance certificate. For more information, see Update the vSphere Replication Appliances to Trust the vCloud Director Self-Signed Certificate in a Development Environment . You must also reconnect to the cloud provider and accept the new certificate. For more information, see Configure Cloud Provider.

Update the vSphere Replication Manager Certificate

You generate a new vSphere Replication Manager certificate and update all vSphere Replication Server instances to use the new certificate.

Note You cannot perform any replication management operations while you are performing the steps in the current procedure.

Procedure

1 To verify that you are replacing the correct vSphere Replication Manager certificate, run the following command on the vCloud Availability Installer Appliance.

```
# vcav hms print-certificate --hms-address=hms-IP-address
```

The following information is displayed.

```
Issued By: 10.192.43.10
Common Name: 10.192.43.10
Fingerprint: 2A:65:4A:EC:63:BA:2F:36:EA:DF:CA:5E:A3:6F:46:98:D8:73:F4:C2
Start Date: 2016-12-15 01:07:16
End Date: 2021-12-14 01:07:16
```

Write down the `Fingerprint` of the certificate. You need it to replace the certificate in the next step.

2 Replace the vSphere Replication Manager certificate by running the following command.

```
# vcav hms replace-certificate --hms-address=hms-IP-address \
--thumbprint=2A:65:4A:EC:63:BA:2F:36:EA:DF:CA:5E:A3:6F:46:98:D8:73:F4:C2
```

The system displays an `OK` message.

3 Verify that the replacement operation completed successfully by running the following command.

```
# vcav hms print-certificate --hms-address=hms-IP-address
```

The system displays the following information.

```
Issued By: 10.192.43.10
Common Name: 10.192.43.10
Fingerprint: E6:A8:5C:4E:B3:94:9E:D5:E8:30:25:A2:49:E6:21:8D:E7:22:6F:BA
Start Date: 2016-12-15 12:55:12
End Date: 2021-12-14 12:55:12
```

The new `Fingerprint` value indicates that the certificate is successfully replaced. You can note down the new `Fingerprint` for future operations.

4 Reconfigure the vSphere Replication Manager by running the following command.

Standard Command

```
# vcav hms configure \
--reconfigure \
--hms-address=$HMS_ADDRESS \
--vsphere-address=$VSPHERE_ADDRESS \
--vsphere-user=$SSO_USER \
--vsphere-password-file=~/.ssh/.sso \
--vcd-address=$VCD_ADDRESS \
--vcd-user=$VCD_USER \
--vcd-password-file=~/.ssh/.vcd \
--sso-user=$SSO_USER \
--sso-password-file=~/.ssh/.sso
```

Command Using Registry

```
# vcav hms configure \
--reconfigure \
--hms-address=hms-IP-address \
--vsphere=vsphere-name \
--vcd=vcd-name \
```

The system returns an `OK` message, after the process finishes.

5 Verify that the `hms` service starts successfully.

Standard Command

```
# vcav hms wait-for-extension \
--hms-address=$HMS_ADDRESS \
--vsphere-address=$VSPHERE_ADDRESS \
--vsphere-user=$SSO_USER \
--vsphere-password-file=~/.ssh/.sso \
--vcd-address=$VCD_ADDRESS \
--vcd-user=$VCD_USER \
--vcd-password-file=~/.ssh/.vcd \
--sso-user=$SSO_USER \
--sso-password-file=~/.ssh/.sso
```

Command Using Registry

```
# vcav hms wait-for-extension \
--hms-address=hms-IP-address \
--vsphere=vsphere-name \
--vcd=vcd-name
```

If the `hms` service starts successfully, the system displays an `OK` message.

If the system returns an error, or there is no output in 5 minutes, check the `/opt/vmware/logs/hms/hms.log` file for errors.

6 Load the new vSphere Replication Manager certificate to all connected vSphere Replication Server instances.

Standard Command

```
# vcav hbr configure \
--reconfigure \
--hbr-address=$HBR_ADDRESS \
--vsphere-address=$VSPHERE_ADDRESS \
--vsphere-user=$SSO_USER \
--vsphere-password-file=~/.ssh/.sso \
--vcd-address=$VCD_ADDRESS \
--vcd-user=$VCD_USER \
--vcd-password-file=~/.ssh/.vcd
```

Command Using Registry

```
# vcav hbr configure \
--reconfigure \
--hbr-address=$HBR_ADDRESS \
--vsphere=vsphere-name \
--vcd=vcd-name
```

The system returns an `OK` message, after the process finishes.

7 Verify that the hbr service starts successfully.

Standard Command	Command Using Registry

`# vcav hbr wait-for-extension \`
`--hbr-address=$HBR_ADDRESS \`
`--vsphere-address=$VSPHERE01_ADDRESS \`
`--vsphere-user=$SSO_USER \`
`--vsphere-password-file=~/.ssh/.sso \`
`--vcd-address=$VCD_ADDRESS \`
`--vcd-user=$VCD_USER \`
`--vcd-password-file=~/.ssh/.vcd`
	`# vcav hbr wait-for-extension \`
	`--hbr-address=$HBR_ADDRESS \`
	`--vsphere=vsphere-01-name \`
	`--vcd=vcd-01-name`

If the hbr service starts successfully, the system displays an OK message.

If the system returns an error, or there is no output in 5 minutes, check the /var/log/vmware/hbrsrv.log file for errors.

Update the vSphere Replication Cloud Service Host Certificate

To update the vSphere Replication Cloud Service host certificate, you generate a new one and import it to all connected Cassandra instances.

Note You cannot perform any replication management operations while you are performing the steps in the current procedure.

Procedure

1 Run the following command on the vCloud Availability Installer Appliance to verify that you are replacing the correct vSphere Replication Cloud Service host certificate.

```
# vcav hcs print-certificate --hcs-address=hcs-IP-address
```

The following information is displayed.

```
Issued By: 10.192.43.10
Common Name: 10.192.43.10
Fingerprint: 2A:65:4A:EC:63:BA:2F:36:EA:DF:CA:5E:A3:6F:46:98:D8:73:F4:C2
Start Date: 2016-12-15 01:07:16
End Date: 2021-12-14 01:07:16
```

Write down the Fingerprint of the certificate. You need it to replace the certificate in the next step.

2 Replace the vSphere Replication Cloud Service host certificate by running the following command.

```
# vcav hcs replace-certificate --hcs-address=hcs-IP-address \
--thumbprint=2A:65:4A:EC:63:BA:2F:36:EA:DF:CA:5E:A3:6F:46:98:D8:73:F4:C2
```

The system displays an OK message.

3 Verify that the replacement operation completed successfully by running the following command.

```
# vcav hcs print-certificate --hcs-address=hcs-IP-address
```

The system displays the following information.

```
Issued By: 10.192.43.10
Common Name: 10.192.43.10
Fingerprint: E6:A8:5C:4E:B3:94:9E:D5:E8:30:25:A2:49:E6:21:8D:E7:22:6F:BA
Start Date: 2016-12-15 12:55:12
End Date: 2021-12-14 12:55:12
```

The new `Fingerprint` value indicates that the certificate is successfully replaced. You can note down the new `Fingerprint` for future operations.

4 Import the new vSphere Replication Cloud Service host certificate into all Cassandra hosts.

Run the following command on every Cassandra host and for each vSphere Replication Cloud Service host.

```
# vcav cassandra import-hcs-certificate --cassandra-address=$CASSANDRA_ADDRESS --hcs-address=
$HCS01_ADDRESS
```

If the command cannot find the Cassandra configuration file, you can specify the path to the file by adding the `--cassandra-config-file=path-to-Cassandra-config-file`.

5 Reconfigure the vSphere Replication Cloud Service host by running the following command.

Standard Command	Command Using Registry

`# vcav hcs configure \`
`--reconfigure \`
`--hcs-address=$HCS_ADDRESS \`
`--amqp-password-file=~/.ssh/.amqp \`
`--vcd-address=$VCD_ADDRESS \`
`--vcd-user=$VCD_USER \`
`--vcd-password-file=~/.ssh/.vcd \`
`--sso-user=$SSO_USER \`
`--sso-password-file=~/.ssh/.sso \`
	`# vcav hcs configure \`
	`--reconfigure \`
	`--hcs-address=hcs-IP-address \`
	`--amqp-password-file=~/.ssh/.amqp \`
	`--vcd=vcd-01-name`

The system displays an `OK` message.

6 Run the following command to verify that the `hcs` service starts successfully.

Standard Command	Command Using Registry

`# vcav hcs wait-for-extension \`
`--hcs-address=$HCS01_ADDRESS \`
`--vcd-address=$VCD_ADDRESS \`
`--vcd-user=$VCD_USER \`
`--vcd-password-file=~/.ssh/.vcd \`
`--sso-user=$SSO_USER \`
`--sso-password-file=~/.ssh/.sso \`
	`# vcav hcs wait-for-extension \`
	`--hcs-address=hcs-IP-address \`
	`--vcd=vcd-01-name`

If the `hcs` service starts successfully, the system displays an `OK` message.

If the system returns an error, or there is no output in 5 minutes, check the `/opt/VMware/logs/hms/hcs.log` file for errors.

Update the vSphere Replication Server Certificate

To update the vSphere Replication Server certificate, you must replace the old certificate with a newly generated one, and reconfigure the vSphere Replication Server.

Procedure

1. Run the following command on the vCloud Availability Installer Appliance to verify that you are replacing the correct vSphere Replication Server certificate.

   ```
   # vcav hbr print-certificate --hbr-address=hbr-IP-address
   ```

   The following information is displayed.

   ```
   Issued By: 10.192.43.10
   Common Name: 10.192.43.10
   Fingerprint: 2A:65:4A:EC:63:BA:2F:36:EA:DF:CA:5E:A3:6F:46:98:D8:73:F4:C2
   Start Date: 2016-12-15 01:07:16
   End Date: 2021-12-14 01:07:16
   ```

   Write down the `Fingerprint` of the certificate. You need it to replace the certificate in the next step.

2. Replace the vSphere Replication Server certificate by running the following command.

   ```
   # vcav hbr replace-certificate --hbr-address=10.192.43.10 \
   --thumbprint=2A:65:4A:EC:63:BA:2F:36:EA:DF:CA:5E:A3:6F:46:98:D8:73:F4:C2
   ```

   The system displays an `OK` message.

3. Verify that the replacement operation completed successfully by running the following command.

   ```
   # vcav hbr print-certificate --hbr-address=hbr-IP-address
   ```

   The system displays the following information.

   ```
   Issued By: 10.192.43.10
   Common Name: 10.192.43.10
   Fingerprint: E6:A8:5C:4E:B3:94:9E:D5:E8:30:25:A2:49:E6:21:8D:E7:22:6F:BA
   Start Date: 2016-12-15 12:55:12
   End Date: 2021-12-14 12:55:12
   ```

   The new `Fingerprint` value indicates that the certificate is successfully replaced. You can note down the new `Fingerprint` for future operations.

4 Reconfigure the vSphere Replication Server.

Standard Command

```
# vcav hbr configure \
--reconfigure \
--hbr-address=$HBR_ADDRESS \
--vsphere-address=$VSPHERE_ADDRESS \
--vsphere-user=$SSO_USER \
--vsphere-password-file=~/.ssh/.sso \
--vcd-address=$VCD_ADDRESS \
--vcd-user=$VCD_USER \
--vcd-password-file=~/.ssh/.vcd
```

Command Using Registry

```
# vcav hbr configure \
--reconfigure \
--hbr-address=hbr-IP-address \
--vsphere=vsphere-name \
--vcd=vcd-name
```

The system returns an `OK` message, after the process finishes.

5 Verify that the `hbr` service starts successfully.

Standard Command

```
# vcav hbr wait-for-extension \
--hbr-address=$HBR_ADDRESS \
--vsphere-address=$VSPHERE01_ADDRESS \
--vsphere-user=$SSO_USER \
--vsphere-password-file=~/.ssh/.sso \
--vcd-address=$VCD_ADDRESS \
--vcd-user=$VCD_USER \
--vcd-password-file=~/.ssh/.vcd
```

Command Using Registry

```
# vcav hbr wait-for-extension \
--hbr-address=$HBR_ADDRESS \
--vsphere=vsphere-01-name \
--vcd=vcd-01-name
```

If the `hbr` service starts successfully, the system displays an `OK` message.

If the system returns an error, or there is no output in 5 minutes, check the `/var/log/vmware/hbrsrv.log` file for errors.

Update the Cassandra Server Certificate

To update the Cassandra server certificate, you must generate a new certificate, register every Cassandra instance, and restart the `hcs` service on every vSphere Replication Cloud Service Host.

Procedure

1 Recreate the Cassandra server certificate. For more information, see Install and Configure a Cassandra Server.

2 Restart the Cassandra service by running the following command.

```
# service cassandra restart
```

3 Register the new certificate for each Cassandra host by running the following command on the vCloud Availability Installer Appliance.

Standard Command

```
# vcav cassandra register \
--hcs-address=$HCS01_ADDRESS \
--cassandra-address=$CASSANDRA_ADDRESS \
--cassandra-port=9042 \
--vcd-address=$VCD_ADDRESS \
--vcd-user=$VCD_USER \
--vcd-password-file=~/.ssh/.vcd \
--sso-user=$SSO_USER \
--sso-password-file=~/.ssh/.sso
```

Command Using Registry

```
# vcav cassandra register \
--hcs-address=hcs-IP-address \
--cassandra-address=$CASSANDRA_ADDRESS \
--cassandra-port=9042 \
--vcd=vcd-01-name
```

4 Run the following command to verify that the `hcs` service starts successfully.

Standard Command

```
# vcav hcs wait-for-extension \
--hcs-address=$HCS01_ADDRESS \
--vcd-address=$VCD_ADDRESS \
--vcd-user=$VCD_USER \
--vcd-password-file=~/.ssh/.vcd \
--sso-user=$SSO_USER \
--sso-password-file=~/.ssh/.sso \
```

Command Using Registry

```
# vcav hcs wait-for-extension \
--hcs-address=hcs-IP-address \
--vcd=vcd-01-name
```

If the `hcs` service starts successfully, the system displays an OK message.

If the system returns an error, or there is no output in 5 minutes, check the `/opt/VMware/logs/hms/hcs.log` file for errors.

Update the RabbitMQ Server Certificate

To update the RabbitMQ server certificate, you must recreate the certificate, register the new AMQP certificate in vCloud Director, and import the new certificate to every vSphere Replication Cloud Service host.

Procedure

1 Recreate the RabbitMQ server certificate. For more information, see Create Self-Signed Certificates for the Primary RabbitMQ Server.

2 Restart the `amqp` service by running the following command.

```
# service rabbitmq-server restart
```

3 Register the new AMQP certificate in vCloud Director. If vCloud Director is not using SSL to connect with RabbitMQ, you can skip this step.

a Create a trusted connection between the RabbitMQ host and the vCloud Availability Installer Appliance.

```
# vcav trust add --address=$AMQP_ADDRESS --port=5671 --accept-all
```

b Register the RabbitMQ host with vCloud Director.

This registration can also be done by using the vCloud Director user interface.

Standard Command

```
# vcav vcd configure-amqp \
--vcd-address=$VCD_ADDRESS \
--vcd-user=$VCD_USER \
--vcd-password-file=~/.ssh/.vcd \
--amqp-address=$AMQP_ADDRESS \
--amqp-port=5671 \
--amqp-user=vcd \
--amqp-password-file=~/.ssh/.amqp \
--amqp-vhost=/ \
--amqp-exchange=systemExchange
```

Command Using Registry

```
# vcav vcd configure-amqp \
--vcd=vcd-01-name \
--amqp-address=$AMQP_ADDRESS \
--amqp-port=5671 \
--amqp-user=vcd \
--amqp-password-file=~/.ssh/.amqp \
--amqp-vhost=/ \
--amqp-exchange=systemExchange
```

The system returns an `OK` message, after the process finishes.

c Restart vCloud Director and Cloud Proxy hosts after configuring AMQP settings, by creating an SSH connection to the hosts and restarting the `vmware-vcd` service.

4 Import the new AMQP certificate to all vSphere Replication Cloud Service hosts by running the following command on the vCloud Availability Installer Appliance.

Standard Command

```
# vcav hcs configure \
--reconfigure \
--hcs-address=$HCS_ADDRESS \
--amqp-password-file=~/.ssh/.amqp \
--vcd-address=$VCD_ADDRESS \
--vcd-user=$VCD_USER \
--vcd-password-file=~/.ssh/.vcd \
--sso-user=$SSO_USER \
--sso-password-file=~/.ssh/.sso \
```

Command Using Registry

```
# vcav hcs configure \
--reconfigure \
--hcs-address=hcs-IP-address \
--amqp-password-file=~/.ssh/.amqp \
--vcd=vcd-01-name
```

The system returns an `OK` message, after the process finishes.

5 To verify that the `hcs` service starts successfully, run the following command.

Standard Command	Command Using Registry

`# vcav hcs wait-for-extension \`
`--hcs-address=$HCS01_ADDRESS \`
`--vcd-address=$VCD_ADDRESS \`
`--vcd-user=$VCD_USER \`
`--vcd-password-file=~/.ssh/.vcd \`
`--sso-user=$SSO_USER \`
`--sso-password-file=~/.ssh/.sso \`
	`# vcav hcs wait-for-extension \`
	`--hcs-address=hcs-IP-address \`
	`--vcd=vcd-01-name`

If the `hcs` service starts successfully, the system displays an `OK` message.

If the system returns an error, or there is no output in 5 minutes, check the `/opt/VMware/logs/hms/hcs.log` file for errors.

Update the vCloud Availability for vCloud Director Portal Host Certificate

To update the vCloud Availability for vCloud Director Portal certificate, you can generate a new self-signed certificate with the vCloud Availability Installer Appliance, or import an externally signed certificate.

Generate a New Self-Signed Certificate

To generate a new self-signed certificate and replace the old vCloud Availability for vCloud Director Portal certificate, complete the following steps.

1 To verify that you are replacing the correct vCloud Availability for vCloud Director Portal certificate, run the following command on the vCloud Availability Installer Appliance.

```
# vcav vcd-ui print-certificate --ui-address=portal-host-IP-address
```

The following information is displayed.

```
Issued By: 10.192.43.10
Common Name: 10.192.43.10
Fingerprint: 2A:65:4A:EC:63:BA:2F:36:EA:DF:CA:5E:A3:6F:46:98:D8:73:F4:C2
Start Date: 2016-12-15 01:07:16
End Date: 2021-12-14 01:07:16
```

Write down the `Fingerprint` of the certificate. You need it to replace the certificate in the next step.

2 Replace the vCloud Availability for vCloud Director Portal certificate by running the following command.

```
# vcav vcd-ui replace-certificate --ui-address=portal-host-IP-address \
--thumbprint=2A:65:4A:EC:63:BA:2F:36:EA:DF:CA:5E:A3:6F:46:98:D8:73:F4:C2
```

The system displays an `OK` message.

3 Verify that the replacement operation completed successfully by running the following command.

```
# vcav vcd-ui print-certificate --ui-address=portal-host-IP-address
```

The system displays the following information.

```
Issued By: 10.192.43.10
Common Name: 10.192.43.10
Fingerprint: E6:A8:5C:4E:B3:94:9E:D5:E8:30:25:A2:49:E6:21:8D:E7:22:6F:BA
Start Date: 2016-12-15 12:55:12
End Date: 2021-12-14 12:55:12
```

The new `Fingerprint` value indicates that the certificate is successfully replaced. You can note down the new `Fingerprint` for future operations.

Import an Externally Signed Certificate

To import an externally signed certificate, run the following command on the vCloud Availability Installer Appliance.

Standard Command

```
# vcav vcd-ui configure \
--reconfigure \
--ui-address=$UI01_ADDRESS \
--https-certificate=/file-path-to-certificate-file \
--https-key=/file-path-to-certificate-public-key \
--truststore-password-file=~/.ssh/.truststore \
--vcd-address=$VCD_ADDRESS \
--vcd-user=$VCD_USER \
--vcd-password-file=~/.ssh/.vcd \
--sso-user=administrator@vsphere.local \
--sso-password-file=~/.ssh/.sso
```

Command Using Registry

```
# vcav vcd-ui configure \
--reconfigure \
--ui-address=$UI01_ADDRESS \
--https-certificate=/file-path-to-certificate-file \
--https-key=/file-path-to-certificate-public-key \
--truststore-password-file=~/.ssh/.truststore \
--vcd=vcd-01-name
```

The system displays and `OK` message, after the process completes.

Update the vCloud Availability for vCloud Director Service Manager Portal Host Certificate

To update the vCloud Availability for vCloud Director Service Manager Portal certificate, you can generate a new self-signed certificate with the vCloud Availability Installer Appliance, or import an externally signed certificate.

Generate a New Self-Signed Certificate

To generate a new self-signed certificate and replace the old vCloud Availability for vCloud Director Service Manager Portal certificate, complete the following steps.

1 To verify that you are replacing the correct vCloud Availability for vCloud Director Service Manager Portal certificate, run the following command on the vCloud Availability Installer Appliance.

```
# vcav vcd-ui print-certificate --ui-address=SMP-host-IP-address
```

The following information is displayed.

```
Issued By: 10.192.43.10
Common Name: 10.192.43.10
Fingerprint: 2A:65:4A:EC:63:BA:2F:36:EA:DF:CA:5E:A3:6F:46:98:D8:73:F4:C2
Start Date: 2016-12-15 01:07:16
End Date: 2021-12-14 01:07:16
```

Write down the `Fingerprint` of the certificate. You need it to replace the certificate in the next step.

2 Replace the vCloud Availability for vCloud Director Service Manager Portal certificate by running the following command.

```
# vcav vcd-ui replace-certificate --ui-address=SMP-host-IP-address \
--thumbprint=2A:65:4A:EC:63:BA:2F:36:EA:DF:CA:5E:A3:6F:46:98:D8:73:F4:C2
```

The system displays an `OK` message.

3 Verify that the replacement operation completed successfully by running the following command.

```
# vcav vcd-ui print-certificate --ui-address=SMP-host-IP-address
```

The system displays the following information.

```
Issued By: 10.192.43.10
Common Name: 10.192.43.10
Fingerprint: E6:A8:5C:4E:B3:94:9E:D5:E8:30:25:A2:49:E6:21:8D:E7:22:6F:BA
Start Date: 2016-12-15 12:55:12
End Date: 2021-12-14 12:55:12
```

The new `Fingerprint` value indicates that the certificate is successfully replaced. You can note down the new `Fingerprint` for future operations.

Import an Externally Signed Certificate

To import an externally signed certificate, run the following command on the vCloud Availability Installer Appliance.

Standard Command

```
# vcav vcd-ui configure-smp \
--reconfigure \
--ui-address=$SMP-host-IP-address \
--https-certificate=/file-path-to-certificate-file \
--https-key=/file-path-to-certificate-public-key \
--truststore-password-file=~/.ssh/.truststore \
--vcd-address=$VCD_ADDRESS \
--vcd-user=$VCD_USER \
--vcd-password-file=~/.ssh/.vcd \
--sso-user=administrator@vsphere.local \
--sso-password-file=~/.ssh/.sso
```

Command Using Registry

```
# vcav vcd-ui configure-smp \
--reconfigure \
--ui-address=$SMP-host-IP-address \
--https-certificate=/file-path-to-certificate-file \
--https-key=/file-path-to-certificate-public-key \
--truststore-password-file=~/.ssh/.truststore \
--vcd=vcd-01-name
```

The system displays and `OK` message, after the process completes.

Using Day 2 Operations Scripts

Day 2 operations happen post provisioning and include routine maintenance tasks and changes to the virtual environment. For vCloud Availability for vCloud Director, the operations include scripts for replication management and VM snapshot consolidation, password and certificate management, and diagnostic information for service provider and tenant users. There are several scripts embedded in the vCloud Availability Installer Appliance to support these operations.

To use the scripts, you must create an SSH connection to the vCloud Availability Installer Appliance, and run the commands from the root user's home directory.

You must log in to vCloud Director. You can provide credentials in two ways:

- Pass your credentials to the `vcav login vcd` command.

  Note If your session expires, you must repeat the login process and pass your credentials to the `vcav login vcd` command.

- Pass the following arguments to the `vcd` command.

  ```
  --vcd-address <vcd_address> --vcd-user <vcd_user> --vcd-password-file <vcd_password_file_txt>
  ```

Replications Management Scripts

vCloud Availability for vCloud Director Portal contains replication management scripts. You can use these scripts to delete replications, to move replications between datastores, or to switch replications between vSphere Replication Server instances. You perform these operations without impacting tenant replication.

Moving Replications Between Datastores

If you need to free space on existing datastore, to rebalance I/O for specific datastores, or to move replications to different datastore, use the `move-replications` command of the vCloud Availability Installer Appliance.

Use a command line in the following format: `vcav move-replications SUBCOMMAND [ARGUMENT]`.

You can pass the following subcommand values and arguments:

SUBCOMMAND	ARGUMENT	Description
`start`	`<vc_host_ip> <source_ds_name> <target_ds_name>`	Moves replications of the `<vc_host_ip>` from `<source_ds_name>` to `<target_ds_name>`. For example: `vcav move-replications start 10.26.235.63 ds_local3_10_26_236_148 ds_local3_10_26_236_148`.
`continue`	None	Continues the operation if the `start` command fails at some point.
`abort`	None	Aborts the operation if the `start` command fails at some point.

Switching Replications Between vSphere Replication Server Instances

If you need to move replications from one vSphere Replication Server to another, for example if the first instance has to enter maintenance mode or to be evacuated, use the `switch-vr` command of the vCloud Availability Installer Appliance.

Use a command line in the following format: `vcav switch-vr SUBCOMMAND [ARGUMENT]`.

You can pass the following subcommand values and arguments:

SUBCOMMAND	ARGUMENT	Description
`start`	`<vc_host_ip> <source_vr_server_host_ip> <target_vr_server_host_ip>`	Switches the replications of the `<vc_host_ip>` from `<source_vr_server_host_ip>` to `<target_vr_server_host_ip>`. For example, `vcav switch-vr start 10.26.235.63 10.26.235.27 10.26.235.28`.
`continue`	None	Continues the operation if the `start` command fails at some point.
`abort`	None	Aborts the operation if the `start` command fails at some point.

Deleting Replications

Use the `delete-vdc` command of the vCloud Availability Installer Appliance to delete replications.

Use a command line in the following format: `vcav delete-vdc SUBCOMMAND [ARGUMENT]`.

You can pass the following subcommand values and arguments:

SUBCOMMAND	ARGUMENT	Description
`start`	`--orgs <org_name1>[<org_name2>...<org_nameN>]`	Deletes replications of `<org_name1>[<org_name2>...<org_nameN>]`. It breaks all tenant peers.
`start`	`--vdcs <vdc_name1>[<vdc_name2>...<vdc_nameN>]`	Deletes replications of `<vdc_name1>[<vdc_name2>...<vdc_nameN>]`. It breaks all tenant peers.
`start`	`--replications <replication_id1> [<replication_id2>...<replication_idN>]`	Deletes replications specified by `<replication_id1> [<replication_id2>...<replication_idN>]`. For example, `vcav delete-vdc start --replications d090f67c-24e3-4648-a2c3-9a3926d0782d--CGID-29d48892-c754-4f9d-8839-225547a851be`.
`continue`	None	Continues the operation if the `start` command fails at some point.
`abort`	None	Abort the operation if the `start` command fails at some point.

Note You can combine subcommands into a single line. For example, `vcav delete-vdc start --orgs <org_name1> <org_name2> --vdcs <vdc_name1> <vdc_name2>`.

Script Error Logging

You can view the errors during the script execution in the `errorReport.txt` file in the current working directory.

In case of an error in the script, you can read the error message in the file.

In case an error occurs during the task execution, you can check the task ID in the file. You can use the task ID with the vCloud Director API to find out more about the error.

VM Snapshot Consolidation Scripts

vCloud Availability for vCloud Director Portal contains scripts to support consolidation of failed over, powered on VMs with MPIT (Multiple Point in Time) snapshots. You can consolidate the stale snapshots of the VMs for the entire vCloud Director, an organization, an organization VDC, a vApp, or a single VM.

If a protected VM uses snapshots, all of them are retained after a failover. Such redundant snapshots have a negative impact on the failed over VM because of the following:

- Storage performance is non-optimal due to complex disk write I/O.
- Storage allocation is not properly reported on vCloud Director since it does not include snapshots.
- Storage billing and provisioning can be mislead.

To free a VM of its stale snapshots, use the `vcd` command of the vCloud Availability Installer Appliance.

Use a command line in the following format: `vcav vcd SUBCOMMAND [ARGUMENT]`.

You can pass the following subcommand values and arguments:

SUBCOMMAND	ARGUMENT	Description
`consolidate`	None	Consolidates the snapshots of all VMs in vCloud Director. **Note** It can be potentially long operation.
`consolidate`	`--orgs <org_name1>[<org_name2>...<org_nameN>]`	Consolidates the snapshots of the VMs in the organizations `<org_name1>[<org_name2>...<org_nameN>]`.
`consolidate`	`--vdcs <org_vdc_name1>[<org_vdc_name2>...<org_vdc_nameN>]`	Consolidates the snapshots of the VMs in the organization VDCs `<org_vdc_name1>[<org_vdc_name2>...<org_vdc_nameN>]`.

SUBCOMMAND	ARGUMENT	Description
`consolidate`	`--vapps <vapp_name1>[<vapp_name2>...<vapp_nameN>]`	Consolidates the snapshots of the VMs in the vApps `<vapp_name1>[<vapp_name2>...<vapp_nameN>]`.
`consolidate`	`--vms <vm_name1>[<vm_name2>...<vm_nameN>]`	Consolidates the snapshots of the VMs `<vm_name1>[<vm_name2>...<vm_nameN>]`.

You can combine subcommands into a single line. For example, `vcav vcd consolidate --orgs <org_name1> <org_name2> --vapps <vapp_name1> <vapp_name2>.`

Scripts Options for Help and Error Handling

Day 2 operations scripts include error-handling options and in-product help. You can specify which action to take if a command fails.

You can use the following options and arguments for the scripts:

Option	Value	Description
`--help (-h)`	None	Get more details for the script.
`--tasks_no`	`integer`	Set the number of parallel tasks to run against vCloud Director. The default is 10.
`--error_action`	`ask|continue|abort`	Set an action in case of an error: ■ `ask` - Prompts you to select how to proceed. This is the default. ■ `continue` - Ignores the error and continues. ■ `abort` - Aborts the script execution.

Also, if HTTP call fails, you can select to continue with the next entity or to abort.

Disaster Recovery Orchestration

VMware vRealize® Orchestrator™ is a development- and process-automation platform that provides a library of extensible workflows to allow you to create and run automated, configurable processes to manage the vSphere infrastructure, and other VMware and third-party technologies.

vRealize Orchestrator exposes every operation in the vCenter Server API, allowing you to integrate all these operations into your automated processes. Orchestrator also allows you to integrate with other management and administration solutions through its open plug-in architecture.

Key Features

The following list presents the key vRealize Orchestrator features.

Persistence Production grade external databases are used to store relevant information, such as processes, workflow states, and configuration information.

Central Management vRealize Orchestrator provides a central way to manage your processes. The application server-based platform, with full version history, allows you to have scripts and process-related primitives in one place. This way, you can avoid scripts without versioning and proper change control spread on your servers.

Check-pointing Every step of a workflow is saved in the database, which allows you to restart the server without losing state and context. This feature is especially useful for long-running processes.

Versioning All vRealize Orchestrator objects have an associated version history. This feature enables basic change management when distributing processes to different project stages or locations.

Scripting engine The Mozilla Rhino JavaScript engine provides a way to create building blocks for vRealize Orchestrator. The scripting engine is enhanced with basic version control, variable type checking, name space management, and exception handling. It can be used in the following building blocks:

- Actions
- Workflows
- Policies

Workflow engine The workflow engine allows you to capture business processes. It uses the following objects to create a step-by-step process automation in workflows:

- Workflows and actions that vRealize Orchestrator provides
- Custom building blocks created by the customer
- Objects that plug-ins add to vRealize Orchestrator

Users, other workflows, a schedule, or a policy can start workflows.

Policy engine	The policy engine allows monitoring and event generation to react to changing conditions in the vRealize Orchestrator or the plugged-in technology. Policies can aggregate events from the platform or the plug-ins, which allows you to handle changing conditions on any of the integrated technologies.
Security	vRealize Orchestrator provides the following advanced security functions: ■ Public Key Infrastructure (PKI) to sign and encrypt content imported and exported between servers ■ Digital Rights Management (DRM) to control how exported content might be viewed, edited, and redistributed ■ Secure Sockets Layer (SSL) encrypted communications between the desktop client and the server and HTTPS access to the Web front-end ■ Advanced access rights management to provide control over access to processes and the objects manipulated by these processes

For more information about installation, configuration, use, and developing with vRealize Orchestrator visit vRealize Orchestrator 6.0 Documentation Center.

You can download vRealize Orchestrator 6.0 from the product download page.

vRealize Orchestrator Plug-Ins

Using vRealize Orchestrator plug-ins, you can access and control external technologies and applications. Exposing an external technology in an vRealize Orchestrator plug-in enables you to incorporate objects and functions in workflows and run workflows on the objects of that external technology. The external technologies that you can access using plug-ins include virtualization management tools, email systems, databases, directory services, and remote control interfaces.

vRealize Orchestrator provides a standard set of preinstalled plug-ins, which expose the vCenter Server API, email and authentication capabilities, and other technologies. In addition, the Orchestrator open plug-in architecture lets you develop plug-ins to access other applications. vRealize Orchestrator implements open standards to simplify integration with external systems. For information about developing custom content, see Developing with vRealize Orchestrator.

The standard set of plug-ins is automatically installed with the Orchestrator server. You might need to configure some of the plug-ins, for example the vCenter Server plug-in, before using them.

Plug-ins extend the vRealize Orchestrator scripting engine with new object types and methods, and plug-ins publish notification events from the external system that triggers events in vRealize Orchestrator and in the plugged-in technology. Plug-ins provide an inventory of JavaScript objects that you can access on the **Inventory** tab of the Orchestrator client. Each plug-in contains packages of workflows and actions that you can run on the objects in the inventory to automate the typical use cases of the integrated product.

vRealize Orchestrator plug-in for vSphere Replication is used to orchestrate vCloud Availability for vCloud Director.

vRealize Orchestrator Plug-In for vSphere Replication and vCloud Availability for vCloud Director

Users and tenants of vCloud Availability for vCloud Director can use vRealize Orchestrator and vRealize Orchestrator Plug-in for vSphere Replication to extend automation capabilities for various operations by including actions in vRealize Orchestrator workflows and combine on-premises vCenter Server operations with its corresponding vCloud Availability for vCloud Director disaster recovery account. The plug-in also delivers pre-built out-of-the-box workflows that cover some existing disaster recovery actions.

Build-In Workflows

- Configure a Replication workflow:
  a. Between on-premise vCenter Server data centers
  b. From on-premise vCenter Server to vCloud Availability for vCloud Director
  c. From vCloud Availability for vCloud Director to an on-premise vCenter Server data center
- Reverse replication workflow:
  a. From vCloud Availability for vCloud Director to an on-premise vCenter Server data center
- Planned migration workflow:
  a. From an on-premise vCenter Server data center to vCloud Availability for vCloud Director
  b. From vCloud Availability for vCloud Director to an on-premise vCenter Server data center
- Test Recovery workflow:
  a. From an on-premise vCenter Server data center to vCloud Availability for vCloud Director
  b. From vCloud Availability for vCloud Director to an on-premise vCenter Server data center
- Cleanup of test instances:
  a. From an on-premise vCenter Server data center to vCloud Availability for vCloud Director
  b. From vCloud Availability for vCloud Director to an on-premise vCenter Server data center
- Real Recovery Workflow:
  a. From vCloud Availability for vCloud Director to an on-premise vCenter Server data center
  b. From an on-premise vCenter Server data center to vCloud Availability for vCloud Director
- Unconfigure a Replication workflow:
  a. Between on-premise vCenter Server data centers
  b. From an on-premise vCenter Server data center to vCloud Availability for vCloud Director
  c. From vCloud Availability for vCloud Director to an on-premise vCenter Server data center

- Workflows that do not require an on-premise site:
  a Test recovery for a virtual machine replicated to vCloud Availability for vCloud Director
  b Clean up test recovery for a virtual machine replicated to vCloud Availability for vCloud Director
  c Real Recovery for a virtual machine replicated to vCloud Availability for vCloud Director

For more information about downloads, installation, and known issues for vRealize Orchestrator plug-in for vSphere Replication visit the links bellow:

- Using the vRealize Orchestrator Plug-In for vSphere Replication 6.5 in the *vSphere Replication 6.5* documentation
- vRealize Orchestrator plug-in for vSphere Replication 6.5 Release Notes
- vRealize Orchestrator plug-in for vSphere Replication 6.1 Release Notes
- vRealize Orchestrator plug-in for vSphere Replication 6.0 Release Notes

Service Provider Diagnostics

Due to the large number of different components used to support the vCloud Availability for vCloud Director deployment, logs must be collected from all the systems. If the problem is affecting only one instance or component, the number of logs collected can be reduced.

Getting a vCloud Availability for vCloud Director Component Version

You can review the version and build number of a single vCloud Availability for vCloud Director component.

To get the version of a vCloud Availability for vCloud Director component, you must create an SSH connection to its host and run the following command:

```
grep fullVersion /opt/vmware/etc/appliance-manifest.xml
```

The system provides you the full version and build number of the appliance you are connected to.

Collecting Logs Using the vCloud Availability Installer Appliance

You can set automatic generation of logs by running a script on the vCloud Availability Installer Appliance.

The script `/opt/vmware/vcav-installer/support-scripts/vcav_support_logs` on the vCloud Availability Installer Appliance provides an easy way to collect logs from all vCloud Availability for vCloud Director components.

To use the automatic generation of logs, verify that you have the following information:

- vSphere Replication Manager IP address
- vCenter Server IP address
- vCenter Server single sign-on user name and password
- vSphere Replication Cloud Service host IP address

- vCloud Director host IP address
- vCloud Availability for vCloud Director Portal host IP address
- vCloud Availability for vCloud Director Service Manager Portal host IP address

Collecting Logs Only from a vSphere Replication Cloud Service Appliance

To generate logs from a vSphere Replication Cloud Service Appliance, run the following command.

```
# vcav_support_logs \
hcs_host=HCS–Host–VM–IP–Address
```

To download support log bundle to the `/tmp` directory on the vCloud Availability Installer Appliance, you must enter the password for the vSphere Replication Cloud Service host.

Collecting Logs Only from a vSphere Replication Manager Appliance

To generate logs from a vSphere Replication Manager Appliance, run the following command.

```
# vcav_support_logs \
hms_host=HMS–Host–VM–IP–Address \
vc_host=vCenter–Host–VM–IP–Address \
sso_user=SSO–Username \
sso_pass=SSO–Password
```

To download support log bundle to the `/tmp` directory on the vCloud Availability Installer Appliance, you must enter the password for the vSphere Replication Manager host.

Collecting Logs Only from a vCloud Availability for vCloud Director Portal Host

To generate logs from a vCloud Availability for vCloud Director Portal Appliance, run the following command.

```
# vcav_support_logs \
ui_host=Portal–Host–VM–IP–Address
```

To download support log bundle to the `/tmp` directory on the vCloud Availability Installer Appliance, you must enter the password for the vCloud Availability for vCloud Director Portal host.

Collecting Logs Only from a vCloud Availability for vCloud Director Service Manager Portal Host

To generate logs from a vCloud Availability for vCloud Director Service Manager Portal Appliance, run the following command.

```
# vcav_support_logs \
smp_host=SMP–Portal–Host–VM–IP–Address
```

To download support log bundle to the `/tmp` directory on the vCloud Availability Installer Appliance, you must enter the password for the vCloud Availability for vCloud Director Service Manager Portal host.

Collecting Logs Only from All the vCloud Availability for vCloud Director Components

To generate logs from all the vCloud Availability for vCloud Director components, run the following command.

```
# vcav_support_logs \
hms_host=HMS-Host-VM-IP-Address \
vc_host=vCenter-Host-VM-IP-Address \
sso_user=SSO-Username \
sso_pass=SSO-Password \
hcs_host=HCS-Host-VM-IP-Address \
vcd_host=vCD-Host-VM-IP-Address \
smp_host=SMP-Portal-Host-VM-IP-Address
ui_host=Portal-Host-VM-IP-Address
```

You can find the logs in the `/tmp` directory on the vCloud Availability Installer Appliance.

Locating the vCloud Availability for vCloud Director Service Manager Portal Logs

You can obtain the vCloud Availability for vCloud Director Service Manager Portal logs for troubleshooting purposes.

You can find the vCloud Availability for vCloud Director Service Manager Portal log files at the `/opt/vmware/vcav-smp/logs` directory.

Filename	Description
`service.log`	This file contains HTTP client error exceptions and Java exceptions.
`dr-service-manager.log`	vCloud Availability for vCloud Director Portal generates this file. It contains the following: ■ Routing information. ■ Details for requests to vCloud Director. ■ Details for responses from vCloud Director. ■ Other runtime information.

Collecting Support Bundles for the vCloud Availability for vCloud Director Components

VMware Technical Support routinely requests diagnostic information from you when a support request is handled. The information is gathered using a specific script or tool for each product. Support bundles contain product-specific logs, configuration files, and data appropriate to the situation.

Collecting a Support Bundle from vCenter Server

You can generate the vCenter Server support bundle by performing the following steps:

1 In a Web browser, navigate to **`https://(vCenter_Server_FQDN):443/appliance/support-bundle`**.

2 Enter root credentials and click **Enter**.

3 The download starts.

For more information about vCenter Server Diagnostic, see Collecting diagnostic information for VMware vCenter Server KB Article.

Collecting a Support Bundle from vCloud Director

To collect the vCloud Director support bundle, establish an SSH connection to **one** of the vCloud Director VMs and run the following command:

```
/opt/vmware/vcloud-director/bin/vmware-vcd-support --all --multicell
```

The command produces a file in the following format: `vmware-cvd-support-YYYY-MM-DD.NNNN.tgz`. The support bundle file is at: `/opt/vmware/vcloud-director/data/transfer/vmware-vcd-support`

Collecting a Support Bundle from vSphere Replication Manager

To collect the support bundle for vSphere Replication Manager, perform the following steps:

1 In a Web browser, navigate to **`https://(vRMS hostname or IP address):5480`**

2 Log in and select the **VR** tab

3 To create a support bundle file, click **Generate**.

4 After the support bundle file is generated, click the file to download the support bundle

The vSphere Replication Manager support bundle includes support bundles from all connected vSphere Replication Server instances.

Collecting a Support Bundle from vSphere Replication Server

The vSphere Replication Server can generate a diagnostic bundle used to diagnose replication problems. You can generate the diagnostic bundle by opening the vSphere Replication **VAMI**, selecting the **VRM** tab, and clicking **Support**.

Click the **Generate** button and a `.zip` package is created containing the logs.

Collecting a Support Bundle from vSphere Replication Cloud Service

You can generate the vSphere Replication Cloud Service support bundle by running the following command on the host VM:

```
# /opt/vmware/hms/bin/generatesupportbundle.sh
```

The output is located in a subfolder at `/opt/vmware/hms`.

Find Job ID in vCloud Director Org log for Configure Replication task. This task can then be traced into the vSphere Replication Cloud Service logs.

vCloud Availability for vCloud Director Log File Locations

You can collect diagnostic information manually if you do not use the support bundle capability.

The following table lists the log locations for all the vCloud Availability for vCloud Director components.

Component	Log Location
vCenter Server 6.x	%ALLUSERSPROFILE%\VMWare\vCenterServer\logs\
vSphere Replication Appliance	/var/log/vmware/vpxd/
vCloud Director/Cloud Proxy	/opt/vmware/vcloud-director/logs
vSphere Replication Manager 6.x	/opt/vmware/hms/logs, /opt/vmware/var/log/lighttpd/error.log, /opt/vmware/etc/vami/ovfEnv.xml, /var/log/boot.omsg, /var/log/boot.msg
vSphere Replication Cloud Service 6.x	/opt/vmware/hms/logs
vSphere Replication Server 6.x	/var/log/vmware/
vCloud Availability for vCloud Director Portal	/opt/vmware/logs/vcav-ui
vCloud Availability for vCloud Director Service Manager Portal	/opt/vmware/vcav-smp/logs
hostd	/var/run/log/hostd.log
vmkernel	/var/run/log/vmkernel.log
Cassandra Database	/opt/apache-cassandra/logs/system.log
RabbitMQ Server	/var/log/rabbitmq/rabbit@vcd.log

(Optional) Securing vSphere Replication Server Traffic

vSphere Replication Server provides replication of data that must be secured using SSL and a certificate through `stunnel`.

Securing vSphere Replication Server Traffic with `stunnel`

Download the `stunnel` RPM:

```
# rpm –ivh
http://pkgs.clodo.ru/suse/test/213.141.145.240/SLES11SP2_UPD64/stunnel-4.36-0.10.1.x86_64.rpm
```

Generate `stunnel` certificate using the command shown. Use a CA signed certificate or self signed wildcard certificate:

```
# cd /etc/stunnel
# openssl req –new –x509 –keyout stunnel.pem –out stunnel.pem –days 3650 –nodes –subj
"/C=US/ST=California/L=SanFrancisco/O=Palo Alto/CN=*.se.vpc.vmw"
```

Note The `stunnel` certificate can be used for all vSphere Replication servers as it is a wildcard certificate and simplifies the importing of `stunnel` certificates into the Cloud Proxy truststore as mentioned in next section.

Create directories and change ownership and permissions:

```
# mkdir /var/run/stunnel/
# mkdir /var/log/stunnel
# chown –R stunnel:nogroup /var/run/stunnel/ /var/log/stunnel
# chown stunnel:nogroup /etc/stunnel/stunnel.pem
# chmod 600 /etc/stunnel/stunnel.pem
```

Modify the `stunnel.conf` file to reflect the following configuration entries only:

```
client = no
foreground=no   this needs to be added
pid = /var/run/stunnel/stunnel.pid
debug = 1
output = /var/log/stunnel/stunnel.log
cert = /etc/stunnel/stunnel.pem

[$VRS_HOSTNAME]
accept = 9998
connect = 31031
```

Start and enable the `stunnel` service:

```
service stunnel start
chkconfig stunnel on
```

Firewall Configuration

After starting `stunnel` on vSphere Replication Server appliance, you must drop packages from outside of the network to ports *31031*, *44046*, and *9998* must be allowed in firewall configuration.

Steps for `SuSE firewall` configuration:

```
# vi  /etc/sysconfig/SuSEfirewall2
```

Change from

```
FW_SERVICES_EXT_TCP="22 80 5480 8043 8123 10000:10020 31031 40404 41111 44046"
```

To

```
FW_SERVICES_EXT_TCP="22 80 5480 8043 8123 9998 10000:10020 40404 41111"
```

Restart the `SuSE firewall`:

```
# /etc/init.d/SuSEfirewall2_setup reload
```

Enable `stunnel` service in `TCP_WRAPPERS` in /etc/hosts.allow

```
# vi /etc/hosts.allow
```

Add the following line

```
$VRS_HOSTNAME : ALL : ALLOW
```

Import `Stunnel` Certificates to Cloud Proxy TrustStore

Note This action is required to use Self-signed certificates in `stunnel`

Copy `stunnel` certificate from one vSphere Replication Server to one of the cloud Proxy cells to use wildcard certification for `stunnel` for all vSphere Replication Server:

```
# scp ${VRS_HOSTNAME}:/etc/stunnel/stunnel.pem ${CLOUDPROXY_HOSTNAME}:/tmp/
```

Convert `.pem` file to `.der`

```
# openssl x509 –outform der –in stunnel.pem –out stunnel.der
```

Import the certificate into `/opt/vmware/vcloud–director/jre/lib/security/cacerts` of the Cloud proxy:

```
# keytool –import –alias stunnel_{VRS_HOSTNAME} –keystore /opt/vmware/vcloud–
director/jre/lib/security/cacerts –file stunnel.der
```

Restart the cloud proxy service:

```
# service vmware–vcd restart
```

Copy `/opt/vmware/vcloud–director/jre/lib/security/cacerts` from the first cloud proxy cell to the remaining cells and restart the `vmware–vcd` service.

Backing up the vCloud Availability for vCloud Director Solution

You can back up and recover the vCloud Availability for vCloud Director solution by using a combination of the vSphere API for Data Protection (VADP) compatible backup solution at VM level and database level backups.

The following table provides information about the backup strategy for each component of the vCloud Availability for vCloud Director solution.

Table 1-1. Backup Strategy for vCloud Availability for vCloud Director Components.

Component name	Back up Strategy
vSphere Replication Management Server	Combine VM level backups with external database backups.
vSphere Replication Cloud Service	Run stateless backups on the VM level.
vSphere Replication Server	Run VM level backups.
Cloud Proxy	Run stateless VM level backups.
Platform Services Controller (PSC)	Run VM level backups. For more information on how to back up and restore the Platform Services Controller, see the *vSphere Installation and Setup* guide.
vRealize Orchestrator Appliance	Combine VM level backups with external database backups.
RabbitMQ Server	Run stateless VM level backups.
Cassandra Server	Run VM level backups.

Working with the Solution from the Tenant Side

The vCloud Availability for vCloud Director administration guide for tenants describes how to replicate virtual machines to cloud, configure replications from cloud, work with vCloud Availability for vCloud Director Service Manager Portal and collect logs.

Replicating Virtual Machines to Cloud

You can configure replications from vSphere environments to cloud for a single virtual machine or for multiple virtual machines.

To replicate virtual machines to cloud, you must deploy a vSphere Replication appliance at the source site, and your cloud provider must enable replications to the cloud in your cloud organization.

The source and target sites must be connected so that you can configure replications. Though you can create connections to the cloud while you configure replications, the good practice is to create cloud connections before you start the **Configure Replication** wizard. See Connect to a Cloud Provider Site in the *vSphere Replication for Disaster Recovery to Cloud*.

To avoid copying big volumes of data between the source site and the cloud over a network connection, you can create replication seeds on the target site and configure replication tasks to use them. See Using Replication Seeds.

For each replication task, you can set a recovery point objective (RPO) to a certain time interval depending on your data protection needs. vSphere Replication applies all changes made to replication source virtual machines to their replicas on the target site. This process reoccurs at the RPO interval that you set.

You can configure replications for powered-off virtual machines, but the data synchronization begins when the virtual machine is powered on. While the source virtual machine is powered off, the replication appears in `Not active` status.

You cannot use vSphere Replication to replicate virtual machine templates.

Configure a Replication to Cloud for a Single Virtual Machine

To start replicating virtual machines to your cloud organization, you configure replication from the source site by using the vSphere Web Client.

When you configure replication, you set a recovery point objective (RPO) to determine the maximum data loss that you can tolerate. For example, an RPO of 1 hour seeks to ensure that a virtual machine loses the data for no more than 1 hour during the recovery. For smaller RPO values, less data is lost in a recovery, but more network bandwidth is consumed keeping the replica up to date. The RPO value affects replication scheduling, but vSphere Replication does not adhere to a strict replication schedule. See How the Recovery Point Objective Affects Replication Scheduling in *vSphere Replication Administration*.

Every time that a virtual machine reaches its RPO target, vSphere Replication records approximately 3800 bytes of data in the vCenter Server events database. If you set a low RPO period, this can quickly create a large volume of data in the database. To reduce the volume of data that is kept in the vCenter Server events database, limit the number of days that vCenter Server retains event data. Alternatively, set a higher RPO value.

vSphere Replication guarantees crash consistency amongst all the disks that belong to a virtual machine. If you use quiescing, you might obtain a higher level of crash consistency amongst the disks that belong to a virtual machine. The available quiescing types are determined by the virtual machine's operating system. See *Compatibility Matrixes for vSphere Replication* for quiescing support for Windows and Linux virtual machines.

If you plan to use replication seeds, read and understand the information in topic Using Replication Seeds.

Note By default, when you configure a virtual machine for replication to cloud, its NICs and MAC addresses are copied automatically to the target site as part of the provisioning of the placeholder virtual machine. If the test network is not isolated from the production network and these networks have common routing, a test recovery of a replicated virtual machine might result in duplicate MAC addresses in your virtual data center. See Disable the Automatic Export of MAC Addresses During Replication in *vSphere Replication for Disaster Recovery to Cloud*.

Prerequisites

- Verify that the vSphere Replication appliance is deployed in your environment.
- Verify that the Disaster Recovery to Cloud service is enabled in the target cloud organization.
- Configure a connection to the cloud organization to which you want to replicate data. See Connect to a Cloud Provider Site in *Installing and Configuring vSphere Replication to Cloud*.

Procedure

1 On the vSphere Web Client Home page, click **VMs and Templates**.

2 In the inventory tree, right-click the virtual machine that you want to replicate and select **All vSphere Replication Actions > Configure Replication**.

The **Configure Replication** wizard opens.

3 Select **Replicate to a cloud provider** and click **Next**.

4 Select the target site to which you want to replicate the VM.

- If you have created a connection to the cloud provider, select the target virtual data center from the list and click **Next**.

  If the status of the connection is `Not authenticated`, you must provide credentials to authenticate with the cloud organization. If you have not selected the networks on the target site to use for recovery operations, you are prompted to do so.

- If you have not created a connection to the cloud provider, click **New Provider VDC**, click **Next**, and follow the on-screen prompts to connect to the target cloud organization.

5 On the Target location page, select where to store replication data.

Option	Procedure
Use storage policy	From the drop-down menu, select the storage policy for replication placement and click **Next**.
Use replication seeds	a Click **Next** to navigate to the list of available seed vApps on the target site. b Select a seed vApp from the list and click **Next**. **Note** If you remove a disk from a replication source virtual machine, the seed disk is not deleted from the datastore on the target site.

6 (Optional) On the Replication options page, select the quiescing method for the guest OS of the source VM.

Note Quiescing options are available only for VMs that support quiescing.

7 (Optional) Select **Enable network compression for VR data**.

Compressing the replication data that is transferred through the network saves network bandwidth and might help reduce the amount of buffer memory used on the vSphere Replication Server. However, compressing and decompressing data requires more CPU resources on both the source site and the server that manages the target datastore.

8 On the Recovery settings page, use the RPO slider or the time spinners to set the acceptable period for which data can be lost in the case of a site failure.

The available RPO range is from 15 minutes to 24 hours.

9 (Optional) To save multiple replication instances that can be converted to snapshots of the source VM during recovery, select **Enable** in the Point in time instances pane, and adjust the number of instances to keep.

Note You can keep up to 24 instances for a VM. This means that if you configure vSphere Replication to keep 6 replication instances per day, the maximum number of days you can set is 4 days.

The number of replication instances that vSphere Replication keeps depends on the configured retention policy, and requires that the RPO period is short enough for these instances to be created. Because vSphere Replication does not check whether the RPO settings will create enough instances to keep, and does not display a warning message if the number of instances is not sufficient, you must ensure that you set vSphere Replication to create the instances that you want to keep. For example, if you set vSphere Replication to keep 6 replication instances per day, the RPO period should not exceed 4 hours, so that vSphere Replication can create 6 instances in 24 hours.

10 Click **Next**.

11 On the Ready to complete page, review the replication settings, and click **Finish**.

A virtual machine configuration task appears in the Recent Tasks list at the bottom of the vSphere Web Client. A progress bar indicates that the source VM is being configured for replication.

If the configuration operation finishes successfully, the replication task that you created appears in the list of outgoing replications on the **vSphere Replication** tab under **Monitor**.

Note If the replication source VM is powered off, the replication remains in a `Not Active` state until you power on the VM.

Configure a Cloud Replication Task for Multiple Virtual Machines

To configure batches of virtual machines for replication to the cloud, you can select multiple virtual machines and start the **Configure Replication** wizard.

When you configure replication, you set a recovery point objective (RPO) to determine the maximum data loss that you can tolerate. For example, an RPO of 1 hour seeks to ensure that a virtual machine loses the data for no more than 1 hour during the recovery. For smaller RPO values, less data is lost in a recovery, but more network bandwidth is consumed keeping the replica up to date. The RPO value affects replication scheduling, but vSphere Replication does not adhere to a strict replication schedule. See How the Recovery Point Objective Affects Replication Scheduling in *vSphere Replication Administration*.

Every time that a virtual machine reaches its RPO target, vSphere Replication records approximately 3800 bytes of data in the vCenter Server events database. If you set a low RPO period, this can quickly create a large volume of data in the database. To reduce the volume of data that is kept in the vCenter Server events database, limit the number of days that vCenter Server retains event data. Alternatively, set a higher RPO value.

vSphere Replication guarantees crash consistency amongst all the disks that belong to a virtual machine. If you use quiescing, you might obtain a higher level of crash consistency amongst the disks that belong to a virtual machine. The available quiescing types are determined by the virtual machine's operating system. See the *Compatibility Matrixes for vSphere Replication* for quiescing support for Windows and Linux virtual machines.

If you plan to use replication seeds, read and understand the information in topic Using Replication Seeds.

Note By default, when you configure a virtual machine for replication to cloud, its NICs and MAC addresses are copied automatically to the target site as part of the provisioning of the placeholder virtual machine. If the test network is not isolated from the production network and these networks have common routing, a test recovery of a replicated virtual machine might result in duplicate MAC addresses in your virtual data center. See Disable the Automatic Export of MAC Addresses During Replication in *vSphere Replication for Disaster Recovery to Cloud*.

Prerequisites

- Verify that the vSphere Replication appliance is deployed in your environment.
- Verify that the Disaster Recovery to Cloud service is enabled in the target cloud organization.
- Configure a connection to the cloud organization to which you want to replicate data. See Connect to a Cloud Provider Site in *Installing and Configuring vSphere Replication to Cloud*.

Procedure

1. On the vSphere Web Client Home page, click **VMs and Templates**.
2. Select a data center, navigate to the **Related Objects** tab, and click the **Virtual Machines** tab.
3. Select the virtual machines for which you want to configure replications.
4. Right-click the virtual machines and select **All vSphere Replication Actions > Configure Replication**.

   The **Configure Replication** wizard opens and vSphere Replication validates the virtual machines that can be configured for replication.
5. Verify the validation results and click **Next**.
6. Select **Replicate to a cloud provider** and click **Next**.
7. Select the target site to which you want to replicate the virtual machine.
   - If you have created a connection to the cloud provider, select the target virtual data center from the list and click **Next**.

     If the status of the connection is `Not authenticated`, you must provide credentials to authenticate with the cloud organization. If you have not selected the networks on the target site to use for recovery operations, you are prompted to do so.
   - If you have not created a connection to the cloud provider, click **New Provider VDC**, click **Next**, and follow the on-screen prompts to connect to the target cloud organization.

8 On the Target location page, select where to store replication data.

Option	Procedure
Use storage policy	From the drop-down menu, select the storage policy for replication placement and click **Next**.
Use replication seeds	a Select the storage policy to use for virtual machines without seeds. b Select the **Use replication seeds** check box and click **Next**. c On the Replication seed page, assign seed vApps to source virtual machines, and click **Next**. For all source virtual machines that do not have a seed vApp assigned, vSphere Replication applies the storage policy that you selected from the drop-down menu on the Target location page. **Note** If you remove a disk from a replication source virtual machine, the seed disk is not deleted from the datastore on the target site.

9 (Optional) On the Replication options page, select the quiescing method for the guest operating system of the source virtual machine.

Note Quiescing options are available only for virtual machines that support quiescing.

10 (Optional) Select **Enable network compression for VR data**.

Compressing the replication data that is transferred through the network saves network bandwidth and might help reduce the amount of buffer memory used on the vSphere Replication server. However, compressing and decompressing data requires more CPU resources on both the source site and the server that manages the target datastore.

11 On the Recovery settings page, use the RPO slider or the time spinners to set the acceptable period for which data can be lost in the case of a site failure.

The available RPO range is from 15 minutes to 24 hours.

12 (Optional) To save multiple replication instances that can be converted to snapshots of the source virtual machine during recovery, select **Enable** in the Point in time instances pane, and adjust the number of instances to keep.

Note You can keep up to 24 instances for a virtual machine. This means that if you configure vSphere Replication to keep 6 replication instances per day, the maximum number of days you can set is 4 days.

The number of replication instances that vSphere Replication keeps depends on the configured retention policy, and requires that the RPO period is short enough for these instances to be created. Because vSphere Replication does not check whether the RPO settings will create enough instances to keep, and does not display a warning message if the number of instances is not sufficient, you must ensure that you set vSphere Replication to create the instances that you want to keep. For example, if you set vSphere Replication to keep 6 replication instances per day, the RPO period should not exceed 4 hours, so that vSphere Replication can create 6 instances in 24 hours.

13 Click **Next**.

14 On the Ready to complete page, review the replication settings, and click **Finish**.

For each source virtual machine, a configuration task appears in the Recent Tasks list in the bottom of the vSphere Web Client. A progress bar indicates that the source virtual machine is being configured for replication.

For each source virtual machine that is configured successfully, a replication task appears on the **vSphere Replication** tab under **Monitor**.

For source virtual machines that are powered on, the initial synchronization starts after the configuration. For source virtual machine that are powered off, the initial synchronization starts when you power on the virtual machines.

Note If a replication source virtual machine is powered off, the replication remains in `Not Active` state until you power on the virtual machine.

What to do next

On the **vSphere Replication** tab under **Monitor**, you can check the state of each replication. See Monitoring the Status of Replication Tasks in *vSphere Replication for Disaster Recovery to Cloud*.

You can click a replication task in the list and use the tabs at the bottom of the vSphere Web Client to view details about the replication, the recovery status, and the latest performed test, if test results are not cleared yet.

Configuring Replications from Cloud

You can replicate a virtual machine from your cloud environment to a vCenter Server if the virtual machine was recovered in the cloud.

You select whether to configure a new replication from cloud or a reverse replication from cloud depending on the condition of your local environment.

Configuring Replications from Cloud

When the local site does not contain data about an outgoing or incoming cloud replication for the virtual machine that you want to replicate, you can configure a replication from cloud for that machine.

In addition to simply replicating virtual machines from cloud to your local site, you can use replications from cloud to restore your site by using the data that was previously replicated in the cloud. For example, a partial or complete breakdown has occurred at your local site, and the source virtual machines that were used for replications to cloud are missing. Additionally, the data for outgoing cloud replications is missing, too. In your cloud organization, you have recovered some of the replicated virtual machines. To restore them back on your local site, you can configure replications from cloud for the recovered virtual machines.

Configuring Reverse Replications

On the local site, for an outgoing cloud replication that is in the Recovered state, you can reverse that replication to start transferring data from the recovered virtual machine in the cloud to the local virtual machine that served as the replication source before the recovery operation.

You can configure a reverse replication to update a replicated virtual machine on your local site with the changes that occurred on its restored copy in the cloud. For example, you replicated a virtual machine from the local site to the cloud and recovered the virtual machine to the cloud to use it while your local site is being maintained. While the local site was offline, changes occurred in the recovered virtual machine in the cloud. When your local site is back online, you can copy the changes from the cloud to your local environment, or even migrate the virtual machine from the cloud back to the local environment.

When you reverse a replication, you can only use the original replication settings. You cannot change the datastore location, RPO, PIT policy, and so on.

Configure a Replication From Cloud

You can use vSphere Replication to configure a replication from cloud to your local site.

If your local site was recovered from a major breakdown and you need to restore it, or you cannot configure a reverse replication, you can configure a new replication from cloud to synchronize data from cloud to your local site.

Note You can configure a replication from cloud for only one virtual machine in a vApp.

Prerequisites

- Verify that the cloud site is available and connected to the local site. See Connect to a Cloud Provider Site in *vSphere Replication for Disaster Recovery to Cloud*.
- Verify that the list of incoming replications does not contain a replication for the virtual machine that you want to configure for replication from cloud. See Stop a Replication From Cloud in *vSphere Replication for Disaster Recovery to Cloud*.

Procedure

1. Use the vSphere Web Client to connect to your local site.
2. Navigate to the **vSphere Replication** tab under **Monitor**, and click **Incoming Replications**.
3. Above the list of incoming replications, click the **Configure replication from cloud provider** icon ().

   The **Configure Replication From Cloud Provider** wizard opens.

4 On the Source site page, select the cloud provider site where the virtual machine is located.

- If you have created a connection to the cloud provider, select the source virtual data center from the list and click **Next**.

  If the status of the connection is `Not authenticated`, you must provide credentials to authenticate with the cloud organization.

- If you have not created a connection to the cloud provider, click **New Provider VDC**, click **Next**, and follow the on-screen prompts to connect to the target cloud organization.

5 On the Available VMs page, select the virtual machine that you want to replicate.

You can select only one virtual machine from a vApp.

6 Accept the automatic assignment of a vSphere Replication server or select a particular server on the local site and click **Next**.

7 On the Target location page, click **Edit** to select the datastore where replication data will be saved.

If you want to use existing disks as seeds for the replication, browse the datastore to locate the folder where the seed disks are located.

8 (Optional) To configure the replication of individual disks, click the name of the source virtual machine.

The list of disks on the source virtual machine expands.

For each disk, you can select the virtual format, storage policy, and a datastore where it is replicated. If the source virtual machine contains more than one disk, you can disable the replication of a disk by clicking **Disable** in its Replication Enabled row.

9 (Optional) On the Replication options page, select the quiescing method for the guest operating system of the source virtual machine.

Note Quiescing options are available only for virtual machines that support quiescing. vSphere Replication does not support VSS quiescing on Virtual Volumes.

10 (Optional) Select **Network Compression**.

Compressing the replication data that is transferred through the network saves network bandwidth and might help reduce the amount of buffer memory used on the vSphere Replication server. However, compressing and decompressing data requires more CPU resources on both the source site and the server that manages the target datastore.

11 On the Recovery settings page, use the RPO slider or the time spinners to set the acceptable period for which data loss is acceptable in the case of a site failure.

The available RPO range is from 15 minutes to 24 hours.

12 (Optional) To save multiple replication instances that can be converted to snapshots of the source virtual machine during recovery, select **Enable** in the Point in time instances pane, and adjust the number of instances to keep.

Note You can keep up to 24 instances for a virtual machine. This means that if you configure vSphere Replication to keep 6 replication instances per day, the maximum number of days you can set is 4 days.

The number of replication instances that vSphere Replication keeps depends on the configured retention policy, and requires that the RPO period is short enough for these instances to be created. Because vSphere Replication does not check whether the RPO settings will create enough instances to keep, and does not display a warning message if the instances are not enough, you must ensure that you set vSphere Replication to create the instances that you want to keep. For example, if you set vSphere Replication to keep 6 replication instances per day, the RPO period should not exceed 4 hours, so that vSphere Replication can create 6 instances in 24 hours.

13 On the Ready to complete page, review the replication settings, and click **Finish**.

A virtual machine configuration task appears in the Recent Tasks list at the bottom of the vSphere Web Client. A progress bar indicates that the source virtual machine is being configured for replication.

If the configuration operation completes successfully, the replication task that you created appears in the list of incoming replications on the **vSphere Replication** tab under **Monitor**.

Note If the replication source virtual machine is powered off, the replication remains in `Not Active` state until you power on the virtual machine.

What to do next

On the **vSphere Replication** tab under **Monitor**, you can check the state of each replication. See Monitoring the Status of Replication Tasks in *vSphere Replication for Disaster Recovery to Cloud*.

Note You can pause, resume, sync, test, recover, and stop replications from cloud, but you cannot reconfigure or move these replications between vSphere Replication servers.

Configure a Reverse Replication from Cloud

You can use vSphere Replication to reverse a recovered outgoing replication and start copying data from the cloud to your local site.

If you replicated a virtual machine from the local site to the cloud and recovered the virtual machine at the cloud site to use it while your local site is being maintained, when your local site is back online, you can synchronize the changes from the cloud to your local environment, or migrate the virtual machine from the cloud back to the local environment.

When you reverse a replication, you can only use the original replication settings. You cannot change the datastore location, RPO, PIT policy, and so on.

Note When you reverse a replication, the source virtual machine on the local site is unregistered from the inventory and its disks are overridden by the disks that are replicated from the cloud. When the source virtual machine is unregistered, you can no longer use it unless you recover the replication.

Prerequisites

- Verify that the cloud site is available and connected to the local site. See Connect to a Cloud Provider Site in *vSphere Replication for Disaster Recovery to Cloud*.
- Verify that the list of incoming replications does not contain a replication for the virtual machine that you want to configure for replication from cloud. See Stop a Replication From Cloud in *vSphere Replication for Disaster Recovery to Cloud*.

Procedure

1. Use the vSphere Web Client to connect to your local site.
2. Navigate to the **vSphere Replication** tab under **Monitor**, and click **Outgoing Replications**.
3. In the list of outgoing replications, select the replication that you want to reverse, and click the **Reverse replication** icon ().

   Note The replication status must be `Recovered`.

   vSphere Replication validates the source and target virtual machine, and the Reverse Replication dialog box opens.
4. Review the settings for the reverse replication and click **OK**.

   Caution The source virtual machine on the local site is unregistered from the inventory and becomes inaccessible until you recover the replication.

vSphere Replication starts synchronizing data from the cloud to your local environment.

The reversed replication is removed from the list of outgoing replications and appears in the list of incoming replications.

What to do next

You can recover the replication to migrate your virtual machine from cloud to your local environment.

Note You can pause, resume, sync, test, recover, and stop replications from cloud, but you cannot reconfigure or move these replications between vSphere Replication servers.

If the reverse replication cannot be configured, try configuring a new replication from cloud. See Configure a Replication From Cloud.

Using Replication Seeds

For each new replication that you configure, an initial full synchronization operation is performed. During this operation, vSphere Replication copies the whole data from the source virtual machine to a placeholder vApp on the target site.

Due to VM size or network bandwidth, the initial full sync might take a long time. Therefore, you might choose to copy the source VM to the target site by using removable media, or other means of data transfer. Then you can configure a replication and use the VM copy on the target site as a replication seed. When a replication is configured to use a seed vApp, vSphere Replication does not copy the whole source VM to the target site. Instead, it copies to the seed vApp only the different blocks between the source VM and the seed.

Note vSphere Replication stores the replication data in the seed vApp. No copies of the seed vApp are created. Therefore, a seed vApp can be used for only one replication.

Creating Seed vApps in the Cloud

Seed vApps on the target site can be created in the following ways.

- Offline data transfer: You can export a VM as an OVF package and let a Cloud service administrator import the package in your cloud organization.
- Clone a VM: A VM in the org virtual data center can be cloned to create a seed vApp. vSphere Replication calculates checksum and exchanges the different blocks from the replication source to the seed vApp.
- Copy over the network: A source VM can be copied to the cloud organization by using means other than vSphere Replication to transfer source data to the target site.

Note The size and number of disks, and their assignment to disk controllers and bus nodes must match between the replication source and the seed VM. For example, if the replication source VM has two disks of 2 GB each, one of them assigned to SCSI controller 0 at bus number 0, and the second one assigned to SCSI controller 1 at bus number 2, the seed vApp that you use must have the same hardware configuration - 2 disks of 2 GB each, at SCSI 0:0 and at SCSI 1:2.

Export a Virtual Machine to Removable Media

To use a replication seed for configuring a replication, you must export a virtual machine to removable media and provide it to your service provider.

Prerequisites

- Verify that you have sufficient user privileges in the vSphere Web Client to power off a virtual machine.
- Verify that you have the VMware OVF Tool installed and configured.

Procedure

1 Power off the virtual machine on the protected side by using the vSphere Web Client.

2 Run the following command to export the virtual machine from a vCenter Server to a removable media.

```
ovftool 'vi://root@VC_IP/Datacenter_Name/vm/VM_FQDN' VM_FQDN.ova
```

You can power on the virtual machine, after the process finishes.

3 Provide the removable media containing the exported virtual machine files to your service provider.

Importing Virtual Machine from Removable Media

You can import a virtual machine from removable media directly into vCloud Director. Alternatively, you can import a virtual machine into a vCenter Server and then import the virtual machine into vCloud Director by using the vSphere Web Client.

Import Virtual Machine Directly into vCloud Director

Import the virtual machine directly into vCloud Director to configure replication.

Prerequisites

Verify that you have a removable media containing exported virtual machine files.

Procedure

- Run the following command to import the virtual machine from the removable media into vCloud Director.

```
ovftool PATH_TO_DISK/VM_FQDN/VM_FQDN.ovf 'vcloud://VCD_USER@VCD_IP:443?
org=org1&vapp=VM_FQDNvApp&vdc=vdc_org_name'
```

Note Do not power on the imported virtual machine.

What to do next

You can now configure a replication by using the created seed vApp in vCloud Director.

Import Virtual Machine into vCloud Director Through a vCenter Server

Import a virtual machine into vCloud Director to configure replication by using vCenter Server.

Prerequisites

Verify that you have a removable media containing exported virtual machine files.

Procedure

1 Run the following command to deploy the VM from the removable media to a vCenter Server.

```
ovftool –ds=DATASTORE_NAME VM_FQDN.ova "vi://root@VC_IP/?ip=HOST_IP"
```

Note Do not power on the imported VM.

2 In the vSphere Web Client, drag the VM to the tenant resource pool.

3 Import vApp from vCenter Server into vCloud Director. For more information, see the Import a Virtual Machine from vCenter topic in the *vCloud API Programming Guide for Service Providers*.

What to do next

You can now configure a replication by using the created seed vApp in vCloud Director.

Configure Replication Using Replication Seeds

After a virtual machine is imported in vCloud Director, you can use replication seeds to configure a replication to cloud.

Prerequisites

Verify that the virtual machine is successfully imported into vCloud Director.

Procedure

1 In the vSphere Web Client Home page, click **VMs and Templates**.

2 In the inventory tree, right-click the virtual machine and select **All vSphere Replication Actions > Configure Replication**.

The **Configure Replication** wizard opens.

3 Select **Replicate to a cloud provider** and click **Next**.

4 Select the target site to which you want to replicate the virtual machine.

5 On the Target location page, select where to store replication data.

6 Select **Use replication seeds**

7 Click **Next** to navigate to the list of available seed vApps on the target site.

8 Select the seed vApp from the list and click **Next**.

Note If you remove a disk from a replication source virtual machine, the seed disk is not deleted from the datastore on the target site.

9 On the Replication options page, select the quiescing method for the guest OS of the source virtual machine.

Note Quiescing options are available only for VMs that support quiescing.

10 Select **Enable network compression for VR data**.

Compressing the replication data that is transferred through the network saves network bandwidth and might help reduce the amount of buffer memory used on the vSphere Replication Server. However, compressing and decompressing data requires more CPU resources on both the source site and the server that manages the target datastore.

11 On the Recovery settings page, use the RPO slider or the time spinners to set the acceptable period for which data can be lost when a site failure.

   The available RPO range is from 15 minutes to 24 hours.

12 To save multiple replication instances that can be converted to snapshots of the source virtual machine during recovery, select **Enable** in the Point in time instances pane, and adjust the number of instances to keep.

   Note You can keep up to 24 instances for a virtual machine. This means that if you configure vSphere Replication to keep 6 replication instances per day, the maximum number of days you can set is 4 days.

   The number of replication instances that vSphere Replication keeps depends on the configured retention policy, and requires that the RPO period is short enough for these instances to be created. Because vSphere Replication does not check whether the RPO settings will create enough instances to keep, and does not display a warning message if the number of instances is not sufficient, you must ensure that you set vSphere Replication to create the instances that you want to keep. For example, if you set vSphere Replication to keep 6 replication instances per day, the RPO period must not exceed 4 hours, so that vSphere Replication can create 6 instances in 24 hours.

13 Click **Next**.

14 On the Ready to complete page, review the replication settings, and click **Finish**.

A virtual machine configuration task appears in the Recent Tasks list at the bottom of the vSphere Web Client. A progress bar indicates that the source virtual machine is being configured for replication.

If the configuration operation finishes successfully, the replication task that you created appears in the list of outgoing replications on the **vSphere Replication** tab under **Monitor**.

Note If the replication source virtual machine is powered off, the replication remains in a `Not Active` state until you power on the virtual machine.

Working with the vCloud Availability for vCloud Director Portal

With the vCloud Availability for vCloud Director Portal, you can perform vCloud Availability for vCloud Director tasks or monitor the progress of running tasks.

Monitoring vCloud Availability for vCloud Director Processes

You can monitor the overall vCloud Availability for vCloud Director status by using the vCloud Availability for vCloud Director Portal **Home page**. The Home page contains read-only information that presents a workload health summary and a list of your DR-Enabled Virtual Data Centers.

You monitor the progress and status of complete and ongoing tasks by using the **Tasks page**.

Performing vCloud Availability for vCloud Director Tasks

By using the **Workspaces page**, you can perform the following vCloud Availability for vCloud Director tasks.

- Failover workloads from on-premise to cloud sites.
- Failback workloads from cloud to on-premise sites.
- Failover Reverse workloads to synchronize data from a cloud to on-premise sites.
- Failback Reverse workloads to synchronize data from on-premise to cloud sites.
- Test replication tasks and Cleanup test data.
- Power VMs on and off.
- Detach or Unprotect workloads to remove a virtual machine from the vCloud Availability for vCloud Director managed virtual machine set.

The **Workloads** tab on the **Workspaces page** contains a detailed list of all protected virtual machines that are running in your vSphere site. All these virtual machines are ready for migration to your vCloud Director site.

The **Reversed** tab on the **Workspaces page** lists all reverse protected virtual machines that are running in your vCloud Director environment. These virtual machines are ready for migration to your vSphere environment.

To initiate a task on a virtual machine in the **Workloads** tab or the **Reversed** tab, you must call out the **Actions** pane by clicking the virtual machine. The **Actions** pane lists all available actions and details about the current state of the in-cloud virtual machine.

- Log in to vCloud Availability for vCloud Director Portal

  Tenant Organization administrator users can log in to the vCloud Availability for vCloud Director Portal to operate workloads enabled for replication from their vCenter Server instances.

- vCloud Availability for vCloud Director Portal Test Tasks

  Test tasks allow you to verify that source data is replicated correctly on the target side.

- Perform a Failover Task Using the vCloud Availability for vCloud Director Portal

  You can start a Failover task to migrate a VM from your vSphere (on-prem) environment to vCloud Director (cloud) environment.

- Perform a Failback Task Using the vCloud Availability for vCloud Director Portal

  You start a Failback task to migrate a VM from vCloud Director (cloud) environment back to a vSphere (on-prem) environment.

- vCloud Availability for vCloud Director Portal Reverse Tasks

  You perform a Reverse task to synchronize data between source and target sites. These tasks protects the VM in the target site, while the VM continues to run on the source site.

- Virtual Machine Power Management

  You can turn VMs on and off using the vCloud Availability for vCloud Director Portal.

- Unprotect a Virtual Machine Using the vCloud Availability for vCloud Director Portal

  You can remove a VM from the vCloud Availability for vCloud Director solution by running an Unprotect task.

- Detach a Virtual Machine Using the vCloud Availability for vCloud Director Portal

  You can remove a VM from the vCloud Availability for vCloud Director solution by running a Detach task.

- Configure Replication from Cloud to a Second vCenter Server

  You can use the vCloud Availability for vCloud Director solution to support a replication from a vCloud Director site to a second vCenter Server.

Log in to vCloud Availability for vCloud Director Portal

Tenant Organization administrator users can log in to the vCloud Availability for vCloud Director Portal to operate workloads enabled for replication from their vCenter Server instances.

Prerequisites

Verify that your user profile is assigned **Organization Administrator** privileges.

Procedure

1. Enter the URL of the vCloud Availability for vCloud Director Portal into a Web browser, for example `https://$UI01_ADDRESS:8443`.
2. Use *username@Org-Name* to log in to the vCloud Availability for vCloud Director Portal.

vCloud Availability for vCloud Director Portal Test Tasks

Test tasks allow you to verify that source data is replicated correctly on the target side.

- Test Failover Using the vCloud Availability for vCloud Director Portal

  With test failover tasks, you can verify whether the source data from the vSphere site is replicated correctly on the target vCloud Director site.

- Test Failback Using the vCloud Availability for vCloud Director Portal

  With test failback tasks, you can verify whether the source data from the vCloud Director site is replicated correctly on the target vSphere site.

- Cleanup a Test Task Using the vCloud Availability for vCloud Director Portal

  You can run vCloud Availability for vCloud Director Portal operations to a protected workload only after the results of its previous test are cleaned up.

Test Failover Using the vCloud Availability for vCloud Director Portal

With test failover tasks, you can verify whether the source data from the vSphere site is replicated correctly on the target vCloud Director site.

Prerequisites

Verify that the VM is protected in your vCloud Director (cloud) site.

Procedure

1. Log in to the vCloud Availability for vCloud Director Portal using Organization administrator credentials.
2. Navigate to the **Workloads** tab under **Workspaces** and locate the VM that you want to test.
3. Call out the **Actions** pane by clicking the VM.
4. Click **Test** to select the task.

   You can optionally select to turn on the test VM, after the test is finished.
5. Click **Start** in the **Actions** pane to initiate the Test Failover task.

   You can monitor the progress of the task in the **Actions** pane.

Test Failback Using the vCloud Availability for vCloud Director Portal

With test failback tasks, you can verify whether the source data from the vCloud Director site is replicated correctly on the target vSphere site.

Prerequisites

Verify that the virtual machine is running in your vCloud Director (cloud) site and is protected in your vSphere (on-premise) site.

Procedure

1. Log in to the vCloud Availability for vCloud Director Portal using Organization administrator credentials.
2. Navigate to the **Reversed** tab under **Workspaces** and locate the virtual machine that you want to test.
3. Call out the **Actions** pane by clicking the virtual machine.
4. Click **Test** to select the task.

   Optionally, you can select to turn on the test virtual machine after the test is finished.
5. Click **Start** in the **Actions** pane to initiate the Test Failback task.

   You can monitor the progress of the task in the **Actions** pane.

Cleanup a Test Task Using the vCloud Availability for vCloud Director Portal

You can run vCloud Availability for vCloud Director Portal operations to a protected workload only after the results of its previous test are cleaned up.

Prerequisites

Verify that the Test task finished on the VM that you want to Cleanup.

Procedure

1. Log in to the vCloud Availability for vCloud Director Portal using Organization administrator credentials.
2. Locate the VM that you want to Clean up under the **Workloads** or **Reversed** tab.
3. Call out the **Actions** pane by clicking the VM.
4. Click **Cleanup** to select the task.
5. Click **Confirm** in the **Actions** pane to initiate the Cleanup task.

   You can monitor the progress of the task in the **Actions** pane.

Perform a Failover Task Using the vCloud Availability for vCloud Director Portal

You can start a Failover task to migrate a VM from your vSphere (on-prem) environment to vCloud Director (cloud) environment.

Prerequisites

Verify that the VM that you want to migrate to vCloud Director is protected through your vSphere environment.

Procedure

1. Log in to the vCloud Availability for vCloud Director Portal using Organization administrator credentials.
2. Navigate to the **Workloads** tab under **Workspaces** and locate the VM that you want to migrate.
3. Call out the **Actions** pane by clicking the VM.
4. Click **Failover** to select the task.

   Optionally, you can select to turn on the VM after the migration is finished.
5. Click **Start** in the **Actions** pane to initiate the **Failover** task.

   You can monitor the progress of the task in the **Actions** pane.

When the Failover task is finished, an **F** letter appears in the status icon on the **Workloads** tab. The **Actions** pane displays an **OK** message. The migrated VM is running in the vCloud Director (cloud) environment and is recovered from the vSphere (on-prem) site.

What to do next

You can perform a Reverse task to protect the VM in your vSphere (on-prem) environment. Ensure the target VM at the vSphere (on-prem) site is powered off. If the target VM is powered on, the Reverse task fails and the workload state returns back to **Normal**. You can use the **Actions** pane to power off the target VM.

Perform a Failback Task Using the vCloud Availability for vCloud Director Portal

You start a Failback task to migrate a VM from vCloud Director (cloud) environment back to a vSphere (on-prem) environment.

Prerequisites

Verify that you have reversed a failover VM.

Procedure

1. Log in to the vCloud Availability for vCloud Director Portal using Organization administrator credentials.
2. Navigate to the **Reversed** tab under **Workspaces** and locate the VM you want to migrate.
3. Call out the **Actions** pane by clicking the VM.
4. Click **Failback** to select the task.

   You can optionally select to turn on the VM, after the migration is finished.
5. Click **Start** in the **Actions** pane to initiate the Failover task.

   You can monitor the progress of the task in the **Actions** pane.

After the Failback task is finished, a **B** letter appears in the status icon on the **Workloads** tab. The **Actions** pane displays an **OK** message. The migrated VM is running on your vSphere (on-prem) environment and is recovered from your vCloud Director (cloud) site.

What to do next

You can perform a Reverse replication task to protect the VM in your vCloud Director (cloud) environment. You must turn off the target VM. If the target VM is powered on, the Reverse replication task will not be available in the **Actions** pane. You can power off the target VM by using the power switch in **VM INFO** in the **Actions** pane.

vCloud Availability for vCloud Director Portal Reverse Tasks

You perform a Reverse task to synchronize data between source and target sites. These tasks protects the VM in the target site, while the VM continues to run on the source site.

- Perform a Failover Reverse Task Using the vCloud Availability for vCloud Director Portal

  Synchronize workload data from vCloud Director (cloud) to vSphere (on-premise) site.

- Perform a Failback Reverse Task Using the vCloud Availability for vCloud Director Portal

  Synchronize VM data from vSphere (on-prem) to vCloud Director (cloud) site.

Perform a Failover Reverse Task Using the vCloud Availability for vCloud Director Portal

Synchronize workload data from vCloud Director (cloud) to vSphere (on-premise) site.

After you delete a tenant VM, you lose the placeholder VM in the vCloud Availability for vCloud Director Portal. In this case, you cannot trigger a **Failover reverse** by task using the vCloud Availability for vCloud Director Portal. You must perform a **Failover reverse** task by using the vSphere Web Client.

After you perform a failover migration from the vSphere (on-premise) environment to a vCloud Director (cloud) environment, the migrated virtual machine is running on the vCloud Director (source) site. A subsequent Reverse task synchronizes and protects data from vCloud Director (cloud) back to the vSphere (on-premise) site.

Prerequisites

- Verify that you have performed a Failover task to the virtual machine before starting the Reverse task.
- Verify that the virtual machine that you want to reverse is turned off at the target side.

Procedure

1. Log in to the vCloud Availability for vCloud Director Portal using Organization administrator credentials.
2. Locate the virtual machine that you want to reverse in the **Workloads** tab and verify that it is turned off at the source side.

   The virtual machine must be turned off in the vSphere (on-premise) site.
3. Call out the **Actions** pane by clicking the virtual machine.
4. Click **Reverse** to select the task.
5. Click **Confirm** in the **Actions** pane to initiate the Reverse task.

   You can monitor the progress of the task in the **Actions** pane.

After the Failover Reverse task is finished, the workload appears in the **Reversed** tab. The virtual machine is running in the vCloud Director (cloud) site and is protected in the vSphere (on-premise) site.

Perform a Failback Reverse Task Using the vCloud Availability for vCloud Director Portal

Synchronize VM data from vSphere (on-prem) to vCloud Director (cloud) site.

After you perform a failback migration from the vCloud Director (cloud) site to a vSphere (on-prem) environment, the migrated VM is running on the vSphere (source) site. A subsequent Reverse task synchronizes and protects data from vSphere (on-prem) back to the vCloud Director (cloud) site.

Prerequisites

- Verify that you have performed a Failback task to the VM before starting a reverse task.

- Verify that the VM that you want to reverse is turned off at the target side.

Procedure

1. Log in to the vCloud Availability for vCloud Director Portal using Organization administrator credentials.
2. Locate the VM that you want to reverse in the **Reversed** tab and verify that it is turned off at the source side.

   The VM must be turned off in the vCloud Director (cloud, source) site.
3. Call out the **Actions** pane by clicking the VM.
4. Click **Reverse** to select the task.
5. Click **Confirm** in the **Actions** pane to initiate the Reverse task.

   You can monitor the progress of the task in the **Actions** pane.

After the Failback Reverse task is performed on a VM, the VM appears in the **Workloads** tab. The VM runs in the vSphere (on-prem) environment and is protected in the vCloud Director (cloud) site.

Virtual Machine Power Management

You can turn VMs on and off using the vCloud Availability for vCloud Director Portal.

You can power VMs on and off on the vSphere (on-prem) site, by using the **Actions** pane.

Unprotect a Virtual Machine Using the vCloud Availability for vCloud Director Portal

You can remove a VM from the vCloud Availability for vCloud Director solution by running an Unprotect task.

The Unprotect task stops the replication of data from the source to the target site.

You cannot run an Unprotect task after Failover and Failback tasks. In such cases, you can only run a Detach task to the VM.

Prerequisites

- Verify that the VM that you want to remove from the vCloud Availability for vCloud Director solution is protected.
- Force Stop the replication of the VM in your vSphere (on-prem) environment. For more information, see topic *Stop Replicating a Virtual Machine* in the *VMware vSphere Replication Administration Guide*.

Procedure

1. Log in to the vCloud Availability for vCloud Director Portal using Organization administrator credentials.
2. Locate the VM that you want to Unprotect under **Workloads** or **Reversed** tab .

3 Call out the **Actions** pane by clicking the VM.

4 Click **Unprotect** to select the task.

5 Click **Confirm** in the **Actions** pane to initiate the Unprotect task.

You can monitor the progress of the task in the **Actions** pane.

The VM is no longer protected by the vCloud Availability for vCloud Director solution and disappears from the VM lists in the vCloud Availability for vCloud Director Portal upon task completion.

Detach a Virtual Machine Using the vCloud Availability for vCloud Director Portal

You can remove a VM from the vCloud Availability for vCloud Director solution by running a Detach task.

Detach tasks can only be run on a VM after Failover or Failback tasks.

Detach tasks keep the VMs running on the replication target site.

Prerequisites

Verify that the VM that you want to remove from the vCloud Availability for vCloud Director solution is protected.

Procedure

1 Log in to the vCloud Availability for vCloud Director Portal using Organization administrator credentials.

2 Locate the workload that you want to Detach under the **Workloads** or **Reversed** tab.

3 Call out the **Actions** pane by clicking the VM.

4 Click **Detach** to select the task.

5 Click **Confirm** in the **Actions** pane to initiate the Detach task.

You can monitor the progress of the task in the **Actions** pane.

The VM is no longer protected by the vCloud Availability for vCloud Director solution and disappears from the VM lists in the vCloud Availability for vCloud Director Portal upon task completion.

Configure Replication from Cloud to a Second vCenter Server

You can use the vCloud Availability for vCloud Director solution to support a replication from a vCloud Director site to a second vCenter Server.

You can make use of this capability when your original vCenter Server is offline and you must migrate the VM from the vCloud Director site to another vCenter Server. This use case is often called *Unplanned Failover*. For more information about the replication topology, see vCloud Availability for vCloud Director Portal Overview in the *vCloud Availability for vCloud Director Installation and Configuration Guide*.

Prerequisites

- Verify that the virtual machine is successfully recovered in the vCloud Director site through a Failover task. You can perform a Failover task using the vCloud Availability for vCloud Director Portal. For more information, see Perform a Failover Task Using the vCloud Availability for vCloud Director Portal .
- Verify that the virtual machine is detached and does not appear in the **Workloads** tab of the vCloud Availability for vCloud Director Portal. You can detach a workload by running a **Detach** task in the vCloud Availability for vCloud Director Portal. For more information about detaching workloads through the vCloud Availability for vCloud Director Portal, see Detach a Virtual Machine Using the vCloud Availability for vCloud Director Portal. .
- If you are recreating the second vCenter Server on top of the original on-premise environment, for example, reconnecting the same ESXi hosts, verify that you do not need the original on-premise VM and delete it from the inventory to avoid a UUID conflict.

Procedure

1. Use the vSphere Web Client to connect to your second vCenter Server.
2. Navigate to **vSphere Replication** tab under **Monitor**, and click **Incoming Replications**.
3. Above the list of incoming replications, click the **Configure replication from cloud provider** icon ().

   The **Configure Replication From Cloud Provider** wizard opens.
4. On the Source site page, select the cloud provider site where the virtual machine is located.
   - If you have created a connection to the cloud provider, select the source virtual data center from the list and click **Next**.

     If the status of the connection is `Not authenticated`, you must provide credentials to authenticate with the cloud organization.
   - If you have not created a connection to the cloud provider, click **New Provider VDC**, click **Next**, and follow the on-screen prompts to connect to the target cloud organization.
5. On the Available virtual machines page, select the virtual machine that you want to replicate.

   You can select only one virtual machine from a vApp.
6. Accept the automatic assignment of a vSphere Replication server or select a particular server on the local site and click **Next**.
7. On the Target location page, click **Edit** to select the datastore where replication data is saved.

   If you want to use existing disks as seeds for the replication, browse the datastore to locate the folder where the seed disks are located.
8. (Optional) To configure a replication of individual disks, click the name of the source virtual machine.

   The list of disks on the source virtual machine expands.

For each disk, you can select the virtual format, storage policy, and a datastore where it is replicated. If the source virtual machine contains more than one disk, you can disable the replication of a disk by clicking **Disable** in its Replication Enabled row.

9 (Optional) On the Replication options page, select the quiescing method for the guest OS of the source virtual machine.

Note Quiescing options are available only for VMs that support quiescing. vSphere Replication does not support VSS quiescing on Virtual Volumes.

10 (Optional) Select **Network Compression**.

Compressing the replication data that is transferred through the network saves network bandwidth. Compressing the replication data might also help reduce the amount of buffer memory used on the vSphere Replication server. However, compressing and decompressing data requires more CPU resources on both the source site and the server that manages the target datastore.

11 (Optional) On the Failback recovery settings page, select the Configure recovery settings check box, and then select a virtual machine folder and host or resource pool.

12 On the Recovery settings page, use the RPO slider or the time spinners to set the acceptable period for which data loss is acceptable in the case of a site failure.

The available RPO range is from 15 minutes to 24 hours.

13 (Optional) To save multiple replication instances that can be converted to snapshots of the source virtual machine during recovery, select **Enable** in the **Point in time instances** pane, and adjust the number of instances to keep.

14 On the **Ready to complete** page, review the replication settings, and click **Finish**.

A virtual machine configuration task appears in the Recent Tasks list at the bottom of the vSphere Web Client. A progress bar indicates that the source virtual machine is being configured for replication.

If the configuration operation completes successfully, the replication task that you created appears in the list of incoming replications on the **vSphere Replication** tab under **Monitor** in the vSphere Web Client.

The virtual machine appears in the **Reversed** tab of the vCloud Availability for vCloud Director Portal.

The virtual machine is running in the vCloud Director (cloud) site and is protected on the second vCenter Server (on-premise) site.

Tenant Diagnostics

Within a tenant environment, it is important to collect the information from the vSphere Replication components. If the problem exists within other systems, collect the logs from all the relevant components at the same time to ensure that the errors can be correlated correctly.

VMware Technical Support routinely requests diagnostic information from you when a support request is handled. The information is gathered using a specific script or tool for each product.

Collect the Support Bundle for a vSphere Replication Appliance

Support bundles are generated automatically and contain product-specific logs, configuration files, and data appropriate to the situation.

Perform the following steps to collect the support bundle for vSphere Replication Appliance:

1 In a Web browser, navigate to the vSphere Replication virtual appliance management interface (VAMI) at

`https://(hostname or IP address):5480`.

2 Log in and select the **VR** tab.

3 Click **Generate** to create a support bundle file.

4 After the support bundle file is generated, click the file to download the support bundle.

Tenant Log File Locations

You can collect diagnostic information manually if you do not use the support bundle capability.

Log File Locations

If you do not use the support bundle capability, you can collect diagnostic information manually. The following table lists the log locations for all the tenant components.

Component	Log Location
vCenter Server 6.x	`%ALLUSERSPROFILE%\VMWare\vCenterServer\logs\`
vCenter Server 5.x and earlier versions on Windows XP, 2000, 2003	`%ALLUSERSPROFILE%\Application Data\VMware\VMware VirtualCenter\Logs\`
vCenter Server 5.x and earlier versions on Windows Vista, 7, 2008	`C:\ProgramData\VMware\VMware VirtualCenter\Logs\`
vSphere Replication Appliance	`/opt/vmware/hms/logs`
vCTA	`/opt/vmware/vcta/logs` on the vSphere Replication Appliance.
hostd	`/var/run/log/hostd.log` on the ESXi host.
vmkernel	`/var/run/log/vmkernel.log` on the ESXi host.

Locating the vCloud Availability for vCloud Director Portal Logs

You can obtain the vCloud Availability for vCloud Director Portal logs for troubleshooting purposes.

You can find the vCloud Availability for vCloud Director Portal log files at the `/opt/vmware/logs/vcav-ui` directory.

Filename	Description
`access.log`	The `nginx` process generates the log file. It contains external request and response statuses.
`dr2c.log`	vCloud Availability for vCloud Director Portal generates this log file. It contains the following: ■ Routing information. ■ Details for requests to vCloud Director. ■ Details for responses from vCloud Director. ■ Other runtime information.
`error.log`	The `nginx` process generates the log file. It contains unhandled runtime errors.