vCloud Availability for vCloud Director 1.0.1

vCloud Availability for vCloud Director 1.0.1

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Copyright © 2017 VMware, Inc. All rights reserved. Copyright and trademark information.

Contents

VMware vCloud Availability for vCloud Director 1.0.1 Documentation 5

1 Updated Information 6

2 Introduction 10

3 Deployment of Components 15
- Production Deployment 16
- Development and Testing Deployments 18
- Firewall and Port Configuration 18
- Load Balancing 21
- Domain Name System Support 24

4 Service Provider Installation and Configuration 25
- Preparing Your Environment to Install vCloud Availability 25
- Installing vCloud Availability 47
- Configuring vCloud Availability for vCloud Director 56

5 Tenant Installation and Configuration 67
- Prepare Your Environment to Install vSphere Replication 67
- Deploy the vSphere Replication Virtual Appliance 68
- Register the vSphere Replication Appliance with vCenter Single Sign-On 70
- Using a Self-Signed Certificate in a Development Environment 72
- Configure Cloud Provider 73
- Replicating Virtual Machines to Cloud 74
- Configuring Replications from Cloud 80
- Using Replication Seeds 84

6 vCloud Availability Administration Portal Overview 89
- Working with the vCloud Availability Administration Portal 89

7 vCloud Availability Portal Overview 93
- Working with the vCloud Availability Portal 94

8 Upgrading vCloud Availability 104
- Deploy vCloud Availability Installer Appliance 104
- Prepare the vCloud Availability Installer Appliance for Upgrading to vCloud Availability 1.0.1 108
- Add Trusted Thumbprints to the vCloud Availability Installer Appliance 110

Connect to vCloud Availability Appliances 111
Create vCloud Availability Portal Host 114
Configure vCloud Availability Portal Host 116

9 Backing up the vCloud Availability Solution 119

10 Disaster Recovery Orchestration 120
Key Features 120
vRealize Orchestrator Plug-Ins 122
vRealize Orchestrator Plug-In for vSphere Replication and vCloud Availability 122

11 Day 2 Operations 124
Day 2 Operations Scripts 124
Password Management 128
Certificate Management 142
Diagnostic Information 161

12 Useful Operations 166
vCloud Availability Installer Appliance Useful Operations 166
Register vCloud Director with Shared SSO 174
Securing vSphere Replication Server Traffic 175

13 Using the vCloud API Schema Reference 178
API Workflow 178
vCloud Director for Connection and Authentication 178
vSphere Replication Server Registration Example 179
Enabling Replication Example 182

VMware vCloud Availability for vCloud Director 1.0.1 Documentation

The *vCloud Availability for vCloud Director Documentation* provides information on how to install, configure, and manage the vCloud Availability for vCloud Director 1.0.1 DRaaS solution.

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.

Updated Information

1

This *vCloud Availability for vCloud Director* document is updated with each release of the product or when necessary.

This table provides the update history of the *vCloud Availability for vCloud Director 1.0.1 Documentation*.

Revision	Description
22 FEB 2018	■ Introduced *vCloud Availability* as the new short name for the *vCloud Availability for vCloud Director* solution. ■ The name of the *vCloud Availability for vCloud Director Portal* changes to *vCloud Availability Portal*. ■ The name of the *vCloud Availability for vCloud Director Service Manager Portal* changes to *vCloud Availability Administration Portal*.
18 JAN 2018	Updated the information in Replications Management Scripts topic. Added the following topics: ■ Create vCloud Availability Administration Portal Host ■ Configure vCloud Availability Administration Portal Host ■ Chapter 6 vCloud Availability Administration Portal Overview ■ Working with the vCloud Availability Administration Portal ■ Log In to the vCloud Availability Administration Portal ■ Monitoring IaaS Consumption ■ Manage the Cleanup of Stale Replications ■ Migrate Replications from One Datastore to Another ■ Impersonate a Tenant
11 NOV 2017	Updated the disk space volumes for small, medium and large vCloud Availability Portal hosts in topic Create vCloud Availability Portal Host.
17 AUG 2017	Updated the information in the following topics: ■ Configure vSphere Replication Server ■ Update the vSphere Replication Manager Certificate ■ Update the vSphere Replication Server Certificate

Revision	Description
10 AUG 2017	■ Added the chapter: Password Management. ■ Updated the information in the following chapters: ■ Diagnostic Information ■ Certificate Management ■ Updated the information in the following topics: ■ Create vCloud Availability Installer Appliance ■ Download vCloud Availability Appliances ■ Cassandra Installation and Configuration ■ Configuring vCloud Director for Installation ■ Create Cloud Proxy ■ Create vSphere Replication Manager ■ Create vCloud Availability Portal Host ■ Configure Cassandra Servers ■ Configure vSphere Replication Cloud Service ■ Configure vCloud Availability Portal Host ■ Configure Service Provider vCloud Director Organizations ■ Using a Self-Signed Certificate in a Development Environment ■ vRealize Orchestrator Plug-In for vSphere Replication and vCloud Availability ■ Create Containers for Test and Development Environments ■ Useful Commands
EN-002365-04	■ Added the chapter: Day 2 Operations Scripts. ■ Added the following topics to the Day 2 Operations Scripts chapter: ■ Replications Management Scripts ■ VM Snapshot Consolidation Scripts ■ Scripts Options for Help and Error Handling ■ Updated the information in the following topics: ■ Using a Self-Signed Certificate in a Development Environment ■ Configure vSphere Replication Cloud Service ■ Configure Service Provider vCloud Director Organizations ■ Useful Commands ■ Create Containers for Test and Development Environments ■ Create vSphere Replication Manager ■ Configure vCloud Availability Portal Host ■ Configure vSphere Replication Cloud Service ■ Configuring vCloud Director for Installation

Revision	Description
EN-002365-03	■ Added the following topics to the Chapter 5 Tenant Installation and Configuration chapter: ■ Replicating Virtual Machines to Cloud ■ Configure a Replication to Cloud for a Single Virtual Machine ■ Configure a Cloud Replication Task for Multiple Virtual Machines ■ Configuring Replications from Cloud ■ Configure a Replication From Cloud ■ Configure a Reverse Replication from Cloud ■ Using Replication Seeds ■ Export a Virtual Machine to Removable Media ■ Importing Virtual Machine from Removable Media ■ Import Virtual Machine Directly into vCloud Director ■ Import Virtual Machine into vCloud Director Through a vCenter Server ■ Configure Replication Using Replication Seeds ■ Updated the information in the following topics: ■ Prepare the vCloud Availability Installer Appliance for vCloud Availability Installation ■ Add Trusted Thumbprints to the vCloud Availability Installer Appliance ■ Configuring vCloud Director for Installation ■ Configure vSphere Replication Cloud Service ■ Removed *Changing or Renewing SSL Certificates in vCloud Director* topic. ■ Removed *Configure Replication* topic from chapter Chapter 5 Tenant Installation and Configuration. ■ Reorganized the content in chapter Chapter 12 Useful Operations. ■ Changed name of chapter *API Reference* to Chapter 13 Using the vCloud API Schema Reference.
EN-002365-02	■ Updated the diagram in topic Chapter 2 Introduction. ■ Updated order of topics in chapter Preparing Your Environment to Install vCloud Availability. ■ Updated the information in topic Download vCloud Availability Appliances. ■ Updated the information in topic Cassandra Installation and Configuration. ■ Updated the information in topic RabbitMQ Installation and Configuration. ■ Updated the information in topic Configuring vCloud Director for Installation. ■ Updated the information in topic Create Cloud Proxy. ■ Updated the information in topic Configure Cassandra Servers. ■ Updated the information in topic Create Containers for Test and Development Environments. ■ Updated the `vcav [appliance-alias] create` commands in topics Create vSphere Replication Manager, Create vSphere Replication Cloud Service Host, Create vSphere Replication Server, and Create vCloud Availability Portal Host.

Revision	Description
EN-002365-01	■ Added topic Update the vCloud Availability Portal Host Certificate. ■ Added topic Configure Replication from Cloud to a Second vCenter Server. ■ Updated the diagram in topic Chapter 2 Introduction. ■ Updated the information in topic Create vCloud Availability Installer Appliance. ■ Updated the information in topic Prepare the vCloud Availability Installer Appliance for vCloud Availability Installation. ■ Updated the information in topic Create vCloud Availability Portal Host. ■ Updated the information in topic Configuring vCloud Director for Installation. ■ Updated the information in topic Configure vSphere Replication Cloud Service. ■ Updated the information in topic Configure vCloud Availability Portal Host. ■ Updated the information in topic Tenant Diagnostics. ■ Updated the information in topic *Changing or Renewing SSL Certificates in vCloud Director*. ■ Updated the information about the `wait-for-extension` operation in topics Configure vSphere Replication Manager, Configure vSphere Replication Cloud Service, Update the RabbitMQ Server Certificate, Update the vCloud Director Certificate, Update the Cassandra Server Certificate, Update the vSphere Replication Manager Certificate, Update the vSphere Replication Cloud Service Host Certificate, and Useful Commands.
EN-002365-00	Initial release.

Introduction 2

This section describes the core architecture of the vCloud Availability service.

vCloud Availability is a Disaster Recovery-as-a-Service (DRaaS) solution that provides simple and secure asynchronous replication and failover for vSphere managed workloads. The service operates through a VMware vCloud® Air™ Network Service Provider, and each installation provides recovery for multiple tenants. The service provides the following features:

- Self-service protection, failover, and failback workflows per virtual machine
- Recovery point objective (RPO) from 15 minutes to 24 hours
- Initial data seeding by shipping a disk

For the service provider,vCloud Availability:

- Integrates with existing vSphere environments
- Multi-tenant support
- Built-in encryption of replication traffic
- Supports multiple vSphere versions
- Supports multiple ESXi versions
- Individual systems are isolated as virtual machine files
- Full integration with the vCenter Server Web client
- Automation provided through standard Web service APIs

Failover from on-premises to Cloud	Replicates data from on-premises vSphere workloads to service provider cloud environments. After the virtual machines are replicated, failover support for running the workloads in the cloud. Recovery Point Objective (RPO) can be configured from 15 minutes to 24 hours.
Fail back to on-premises	For failover loads that have been migrated to the cloud, changes can be replicated back to the on-premise environment. You can then failback workloads in the on-premise environment.

Multiple Points In Time (MPIT) Recovery	Up to 24 restore points can be created. Depending on the RPO configuration, restoration is available from any recovery point.
Orchestration	Using VMware vRealize® Orchestrator™ Appliance and plug-in for vSphere Replication you can easily design and deploy scalable workflows that automate complex IT processes.

Architecture

The architecture of the solution relies on the service provider environment that provides the replication target and the customer, or tenant, environment that employs vSphere Replication to move the data to the service provider. In the service provider environment, multiple components operate together to support replication, secure communication, and storage of the replicated data. Each service provider can support recovery for multiple customer environments that can scale to handle increasing loads for each tenant, and for multiple tenants.

On the tenant side, a single VM instance is deployed in the tenant vSphere environment. This deployment provides management service that is used to oversee the replication operation for each replicated VM. Standard vSphere Replication is used to exchange this information with the service provider infrastructure.

The gray cells in the following diagram represent existing components in the service provider and tenant environments. The remaining colored cells represent vCloud Availability components that you deploy during vCloud Availability Installation and Configuration procedures.

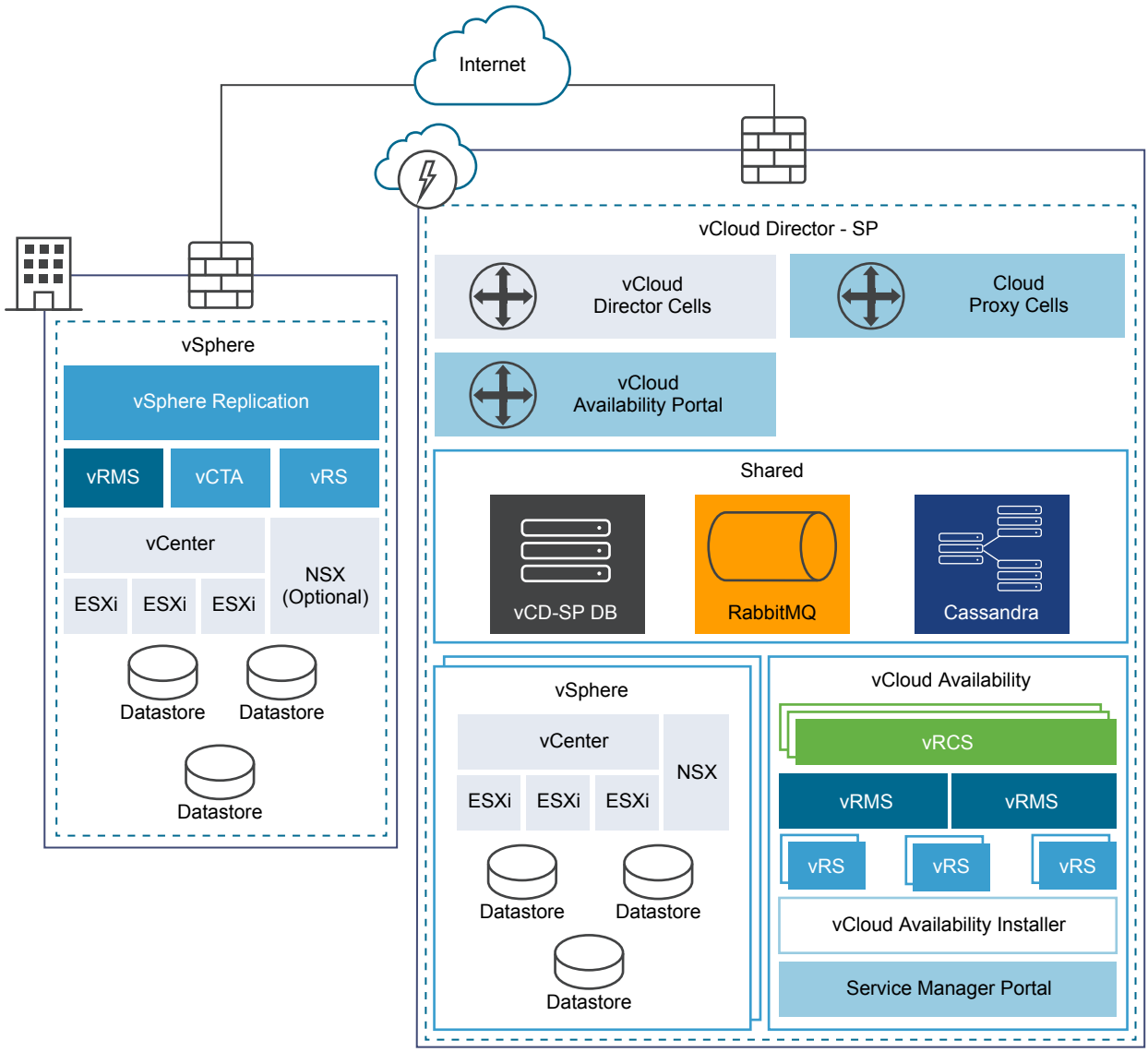


Table 2-1. vCloud Availability Component Definitions.

Name	Abbreviation/Internal Name	Description
vSphere Replication Cloud Service	vRCS/HCS	A tenant-aware replication manager that provides the required API for managing the service and all the components. vSphere Replication Cloud Service registers as a VMware vCloud Director® extension enabling the functionality through the existing vCloud Director API.
vSphere Replication Manager	vRMS/HMS	The management server manages and monitors the replication process from tenant VMs to the service provider environment. A vSphere Replication Management Server runs for each vCenter Server and tracks changes to VMs and infrastructure related to replication.

Table 2-1. vCloud Availability Component Definitions. (Continued)

Name	Abbreviation/Internal Name	Description
vSphere Replication Server	vRS/HBR	The replication server receives and records delta information for each replicated VM. During to-cloud replication, delta information is sent by the tenant ESXi host and recorded by the provider vRS. During from-cloud replication, delta information is sent by the provider ESXi host and recorded by the tenant vSphere Replication Server.
vCloud Tunneling Agent	vCTA	vCTA is a software component which supports tunneling functionality at the on-premise data center. vCTA is responsible for orchestrating a secure tunnel creation for both to-the-cloud and from-the-cloud tunnels.
vCloud Director	vCD	With the vCloud Director solution service providers can build secure, multi-tenant private clouds by pooling infrastructure resources into virtual data centers and exposing them to users through Web-based portals and programmatic interfaces as fully automated, catalog-based services.
Cloud Proxy	n/a	Provides the vCloud Director endpoint for tunnels use to replicated data from on-premises vCTA to and from vCloud Director.
Management vCenter Server	n/a	The Management vCenter Server environment is managed by the service provider and not accessible for tenants.
Resource vCenter Server	n/a	The Resource vCenter Server is a vCenter Server registered to vCloud Director and made available to tenants. Tenants do not have direct access to the Resource vCenter Server environment. Tenants can only locate workloads on the Resource vCenter Server instances using vCloud Director.
Tenant vCenter Server	n/a	The Tenant vCenter Server environment is used solely by the tenant users and is not connected to vCloud Director.
VMware Platform Services Controller™	PSC	The Platform Services Controller provides common infrastructure services to the vSphere environment. Services include licensing, certificate management, and authentication with VMware vCenter ®Single Sign-On.
Cassandra	C	Cassandra is used to store metadata about the replication, replicated VM instances, and infrastructure elements required to support the service. Cassandra is used as a fault-tolerant datastore.
RabbitMQ	n/a	An open source message broker that implements the Advanced Message Queuing Protocol (AMQP). When vSphere Replication Cloud Service registers as a vCloud Director extension, RabbitMQ is used to exchange information with vCloud Director.

Table 2-1. vCloud Availability Component Definitions. (Continued)

Name	Abbreviation/Internal Name	Description
Locator	n/a	The locator must be a valid path to be used with the VMware OVF Tool, as shown in the following examples. ■ */datacenter-name/host/esx-name* ■ */datacenter-name/host/cluster-name*
Datastore	n/a	The name of a vSphere datastore, accessible by the locator.

Deployment of Components

3

Deployment involves installing components within the service provider environment, and just one component within each tenant vCenter Server.

Deployment of vCloud Availability is based on configuring several different components. Some components, such as Cassandra, or NSX may already be deployed within your environment. All the components work together to provide the overall service. Some components are required only once, others are required two or three times to provide redundancy, some are required multiple times to support an increasing number of protected virtual machines.

A typical deployment includes the following components:

- Tenant Service
  - The tenant service, which consists of the vSphere Replication Appliance, is installed on-site in an existing vSphere environment and provides the necessary tools to replicate information to the service provider site.
- Service Provider Service
  - The service provider side of the system supports one or more tenants. A Cloud Proxy provides network connectivity, a vSphere Replication Manager handles the replication of data and controls the replication, and a cluster of appliances receives the disk updates and stores the information ready for the failover of operation from the tenant site to the service provider environment. The number of instances of each component required varies depending on the number of VMs on the tenant side that need to be protected.
- Production Deployment

  Production deployments of vCloud Availability have specific sizing and component configurations.
- Development and Testing Deployments

  Development and test environments can use a minimum configuration to confirm and test the service.
- Firewall and Port Configuration

  Network Firewall ports that are required to be used between different components and systems.
- Load Balancing

  vCloud Availability does not support load balancing. However, a best practice is to apply Layer 4 or Layer 7 load balancing models .

- Domain Name System Support

  You can configure and work with the vCloud Availability solution using IP addresses or domain names.

Production Deployment

Production deployments of vCloud Availability have specific sizing and component configurations.

A production deployment uses multiple components to support many protected virtual machines, and to provide a fault-tolerance within the DRaaS environments.

Production Architecture

Production deployments must meet certain requirements.

- At each tenant site, there is one or more single-tenant environments to be protected.
- In the service provider disaster recovery site, one or more vCloud Director is configured with a specific number of components designed to handle the required number of VMs from each tenant.
- A single vCloud Director environment in a data center hosts up to 500 individual tenants.

Using this information as a base, you must install and configure a new vCloud Availability service pod for every 100 tenants that use the service.

In a single vCloud Director deployment, there is a limit to the number of VMs that can be replicated as part of the DR solution. The exact combination depends on the number of VMs that must be supported combined with the system limits for each component.

Component Sizing

Individual components have a minimum installation count required for a base installation.

Table 3-1. Relative Component Sizing

Component	Related Component
vCloud Director	2 vCenter Server Appliances
vSphere Replication Manager	4 vSphere Replication Server

Component Limits

Individual components have limits for the maximum number of supported services, instances, or connections required.

Table 3-2. Component Counts and Limits per Pod

Component	Limit
Cloud Proxy	2000 Connections
vSphere Replication Server	500 active replications
Tenants	500 per vCloud Director

Table 3-2. Component Counts and Limits per Pod (Continued)

Component	Limit
vCloud Director	10 vCenter Server Instances
vCloud Availability Portal	800 concurrent sessions

Sample Deployment Scaling

Using the information on sizing and configurations, for a single pod, supporting up to the maximum of 100 tenants.

Table 3-3. Component Counts for Production Deployments

Protected VMs	500	1000	2000	3000	5000	10000
vSphere Replication Server	12	24	48	60	120	240
vSphere Replication Cloud Service	2	2	3	3	3	3
Cloud Proxy	2	2	2	2	3	5

Sample Deployment Configuration

Production deployment depends on the number of supported VMs and Tenants. An example configuration of a production deployment is provided in the table.

Table 3-4. Component Deployment for Production Deployments

Component	Host 1	Host 2	Host 3	Host 4	Quantity
Cassandra	Yes	Yes	Yes	Yes	4
Cloud Proxy			Yes	Yes	2
Microsoft SQL Server	Yes	Yes		Yes	3
NFS				Yes	1
NSX Manager				Yes	1
RabbitMQ		Yes	Yes	Yes	3
vCenter Server Appliance	Yes				1
vCloud Director	Yes	Yes			2
vSphere Replication Cloud Service		Yes			1
vSphere Replication Manager		Yes			1
vSphere Replication Server	Yes	Yes	Yes	Yes	4
vCloud Availability Portal	Yes				1

Within a production deployment, the underlying network architecture is important. The following describes a best practice network configuration.

- Each underlying physical ESXi installation is configured with a VMXNET3 high-speed network adapter, connected to two separate 10Gbe switches using NIC teaming.
- The two switches are connected to each other using two 40gbe QSFP cables.
- The switches are configured to present a VLAN that is configured as a port group on the ESXi hosts.
- The virtual machines that make up the environment are all configured in this flat broadcast domain.

Development and Testing Deployments

Development and test environments can use a minimum configuration to confirm and test the service.

For development and testing deployments, the architecture and system count for each component should use the following configuration for a base installation. In these types of deployment, the configuration provides the bare minimum required to support the service.

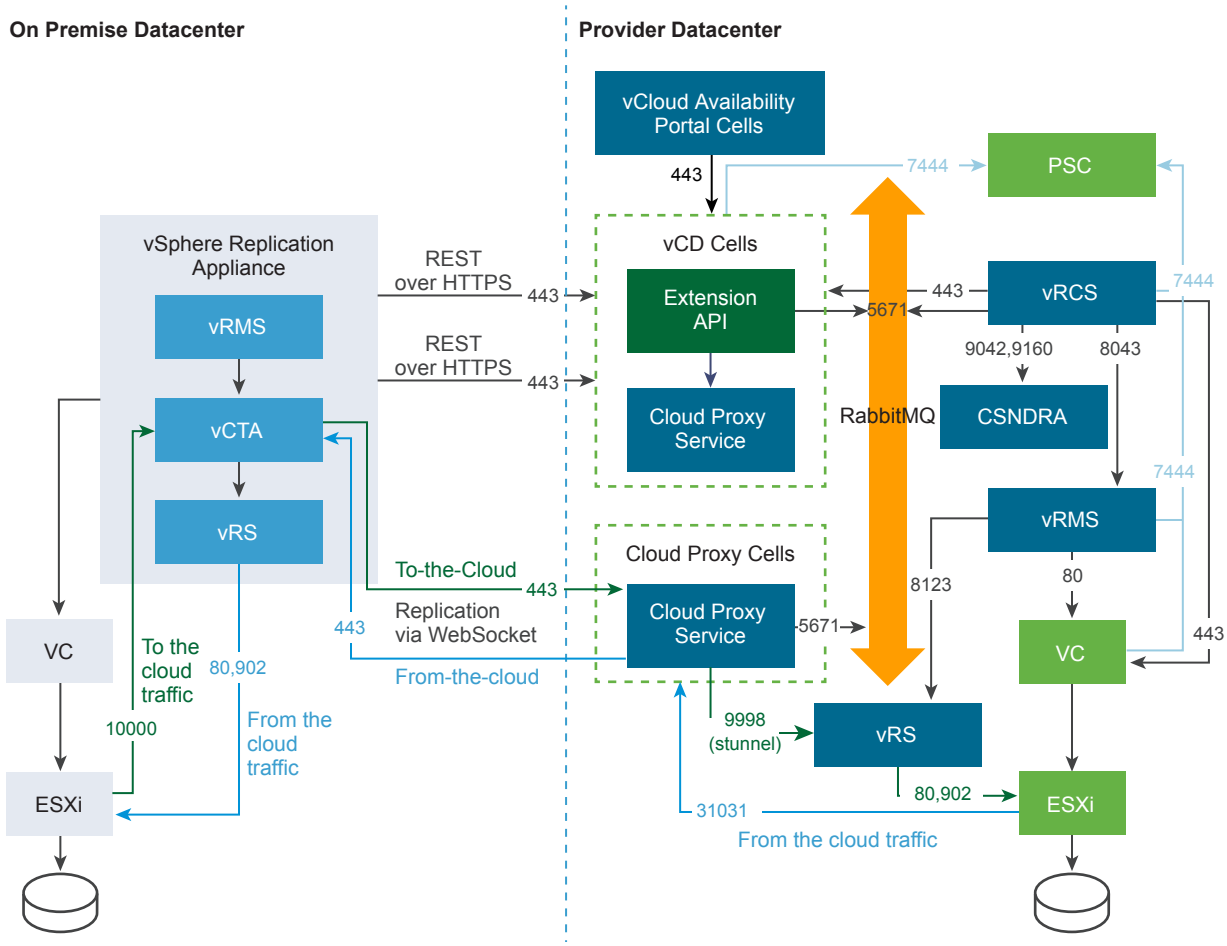
In a development or test environment, to verify functionality and develop the final solution, deployment can consist of one of each of the following components.

- vCloud Availability Installer Appliance
- Cloud Proxy
- vCloud Director
- vSphere Replication Cloud Service
- vSphere Replication Manager
- vSphere Replication Server
- vCloud Availability Portal
- Cassandra
- RabbitMQ

Firewall and Port Configuration

Network Firewall ports that are required to be used between different components and systems.

The following diagram shows the flow of network ports and data through a typical deployment on both the service provider and tenant side.



The following table provides a list of ports to be used between the different systems and components.

Table 3-5. Firewall Port Component Configurations within a Service Provider Deployment

Source	Destination	Port Number	Protocol or Description
Cloud Proxy	vCloud Director DB	1433 or 1521	TCP Port 1433 is the default Microsoft SQL Server database port. Port 1521 is the default Oracle database port.
Cloud Proxy	RabbitMQ	5671	AMQP
Cloud Proxy	vSphere Replication Server	31031	Initial and ongoing replication traffic
ESXi	Cloud Proxy	31031	Initial and ongoing replication traffic
External	Cloud Proxy	443	Initial and ongoing replication traffic
Web Browser	vSphere Replication Manager	5480	Virtual Appliance Management Interface (VAMI) Web UI. Administrator's Web browser.

Table 3-5. Firewall Port Component Configurations within a Service Provider Deployment (Continued)

Source	Destination	Port Number	Protocol or Description
Web Browser	vSphere Replication Server	5480	Virtual Appliance Management Interface (VAMI) Web UI. Administrator's Web browser.
vCloud Director	RabbitMQ	5671	Default RabbitMQ port. AMQP, API Extensibility, Notifications.
Cloud Proxy	vCloud Director	61616	JMS
vCloud Director	Cloud Proxy	61616	JMS
vCloud Director	PSC	7444,443	SOAP
vSphere Replication Manager	PSC	7444, 443	SOAP
vSphere Replication Cloud Service	PSC	7444, 443	SOAP
vSphere Replication Cloud Service	vCenter Server	80	HTTP
vSphere Replication Cloud Service	vCloud Director	443	HTTP
vSphere Replication Cloud Service	vCenter Server	443	SOAP
vSphere Replication Cloud Service	RabbitMQ	5671	Default Rabbit MQ port. AMQP
vSphere Replication Cloud Service	vSphere Replication Manager	8043	SOAP
vSphere Replication Cloud Service	Cassandra	9042	Default Cassandra port. CQL Native Transport Port
vSphere Replication Cloud Service	Cassandra	9160	Default Cassandra port. Thrift.
vSphere Replication Manager	vCenter Server	80	SOAP
vSphere Replication Manager	vCenter Server	443	SOAP
vSphere Replication Manager	vSphere Replication Server	8123	SOAP
vSphere Replication Server	ESXi	80	SOAP
vSphere Replication Server	ESXi	902	NFC
vCloud Availability Portal	vCloud Director	443	HTTPS

For the deployment within a tenant, configure the following ports.

Table 3-6. Firewall Port Configurations within a Tenant Environment

Source	Destination	Port Number	Protocol or Description
vSphere Replication Appliance	vCenter Server	80	SOAP
vSphere Replication Server	ESXi	80	SOAP
vSphere Replication Server	ESXi	902 (TCP and UDP)	NFC
Web Browser	vSphere Replication Appliance	5480	Administrator's Web browser. VAMI.
vSphere Replication Server	vSphere Replication Appliance	8043	SOAP
Web Browser	vSphere Replication Server	5480	Administrator's Web browser. VAMI.
vSphere Replication Manager	vSphere Replication Server	8123	SOAP
vSphere Replication Appliance	vCloud Director at Service Provider	443	HTTP
ESXi	vSphere Replication Appliance at Service Provider	10000-10010	Replication traffic, local vSphere Replication Appliance
Web Browser	vCloud Availability Portal	8443	Default vCloud Availability Portal port. HTTPS

Load Balancing

vCloud Availability does not support load balancing. However, a best practice is to apply Layer 4 or Layer 7 load balancing models .

- To-the-Cloud Traffic

  To support a large number of clients connecting to a public listening port, Service Providers running vCloud Availability can deploy multiple instances of Cloud Proxy and a load balancer to distribute requests to a public port across Cloud Proxy instances.

- From-the-Cloud Traffic

  To establish a from-the-cloud connection, Cloud Proxy sends a request to the vSphere Replication Appliance on premises, using the vCloud Tunneling Agent control connection.

- Using Layer 4 Load Balancing

  Layer 4 load balancers operate on the transport layer, using information defined at the networking transport layer as the basis for client request distribution decisions.

- Using Layer 7 Load Balancing

  Layer 7 load balancers operate on the application layer.

To-the-Cloud Traffic

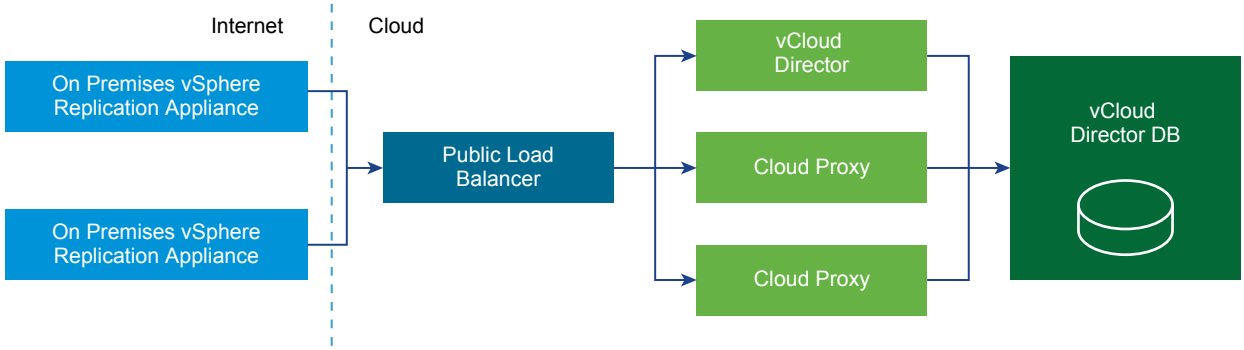
To support a large number of clients connecting to a public listening port, Service Providers running vCloud Availability can deploy multiple instances of Cloud Proxy and a load balancer to distribute requests to a public port across Cloud Proxy instances.

To-the-Cloud traffic setup has the following specifications .

- All Cloud Proxy instances must use the same persistence database as the rest of the vCloud Director instances
- All Cloud Proxy instances must use the same transfer share as the rest of the vCloud Director instances
- All Cloud Proxy instances must use the same NTP time source as the rest of the components (recommended to use an internal NTP source)
- The load balancer exposes a single public port
- Public ports on the Cloud Proxy instances are not exposed to internet
- Cloud Proxy instances do not require to be aware of the load balancer

The Cloud Proxy load balancer can be the same load balancer that is used to distribute REST API requests among vCloud Director instances. In case of high load, a best practice is to have dedicated load balancers for each replication direction, as the traffic can come from Internet and from the cloud .

Figure 3-1. Cloud Proxy Load Balancing Deployment Model



Public Cloud Proxy endpoint (URI) for to-the-cloud tunnel termination and internal IP address for from-the-cloud traffic (used by ESXi host-based replication) must be specifically configured in vCloud Director using the vCloud Director API call . For more information about Cloud Proxy configuration, see Create Cloud Proxy.

From-the-Cloud Traffic

To establish a from-the-cloud connection, Cloud Proxy sends a request to the vSphere Replication Appliance on premises, using the vCloud Tunneling Agent control connection.

In response the vCloud Tunneling Agent initiates a from-the-cloud connection back to the Cloud Proxy. There is only one control connection per tenant (source site), so only one instance of Cloud Proxy can send requests to a particular vCloud Tunneling Agent. Since the load balancer can forward connections to any instance of the Cloud Proxy, the particular instance serving the client request may not have access to the control connection corresponding to the (source site). Furthermore, once from-the-cloud connection is established, there is no guarantee that this connection will be forwarded to the same instance of Cloud Proxy serving the tenant (source site).

The recommended solution consists of the following two elements.

- Using an internal message bus to request from-the-cloud connection
- Configure L4 or L7 load balancing mechanism (Service Providers are expected to configure the load balancer mechanism accordingly)

Using Layer 4 Load Balancing

Layer 4 load balancers operate on the transport layer, using information defined at the networking transport layer as the basis for client request distribution decisions.

A Layer 4 load balancer delivers messages with no regard to the content of the message. Such load balancers only forward network packets to and from an upstream host without inspecting the content of the packets.

If you use a Layer 4 load balancer, the solution requires a load balanced Virtual IP address for each Cloud Proxy instance, with a specific override of its public fully qualified domain name (FQDN) to a specific one .

To override, you must add the following property to the `/opt/vmware/vcloud-director.etc/global.properties` file. `cloudproxy.reverseconnection.fqdn = name.com:443`

Layer 4 load balancing advantages

- Better **performance** compared to Layer 7 load balancing. Layer 4 load balancers only use the network transport layer information, disregarding the content of the packages .
- Better **throughput**.

Layer 4 load balancing disadvantages

- You need multiple Virtual IP addresses.
- You need multiple IP addresses.
- You need multiple certificates.
- You need multiple one member IP pools.

Using Layer 7 Load Balancing

Layer 7 load balancers operate on the application layer.

A layer 7 load balancer stops the network traffic and reads the message to make a distribution decision based on the content of the message.

If you use a layer 7 load balancer, the solution requires application rules, which terminates the SSL connections, inspects the Uniform Resource Identifier (URI), and redirects the connection to the correct Cloud Proxy instance .

Layer 7 load balancing advantages

- You need one public Virtual IP address endpoint.
- You need one IP address.
- You need one certificate.
- You need one IP pool.

Layer 7 load balancing disadvantages

- Layer 7 load balancers read each message to determine the destination, which affects the **performance** compared to the Layer 4 load balancing model .
- Lower **throughput** compared to Layer 4 load balancers .

Domain Name System Support

You can configure and work with the vCloud Availability solution using IP addresses or domain names.

To use Domain Name System (DNS), you must register the domain names with a DNS server. This DNS server must be accessible to the vCloud Availability appliances that are deployed in the service provider data center.

If you use static IP addresses, the vCenter Server IP pool must have a valid DNS server.

If you use Dynamic Host Configuration Protocol (DHCP) for IP address management, the DHCP server must provide a valid DNS server for each deployed appliance.

Service Provider Installation and Configuration

4

vCloud Availability is comprised of multiple components that must be installed and configured in a specific order.

In environments where the service provider and tenant workloads run on the same network, vCloud Availability 1.01 components are installed, configured, and operate on a single vCloud Director instance.

Environments where the service provider and the tenant networks are separated are also supported. In such environments, the vSphere Replication appliances are deployed on the tenant, resource side. The remaining components are deployed in the service provider management environment.

1 Preparing Your Environment to Install vCloud Availability

   Before installing vCloud Availability, you must prepare your environment.

2 Installing vCloud Availability

   Before configuring, you must deploy virtual appliances to support vCloud Availability services.

3 Configuring vCloud Availability for vCloud Director

   After you deploy all individual components of vCloud Availability, you must configure them to support DRaaS.

Preparing Your Environment to Install vCloud Availability

Before installing vCloud Availability, you must prepare your environment.

Procedure

1 Create vCloud Availability Installer Appliance

   To begin installing the components of vCloud Availability, you must first install and configure the vCloud Availability Installer Appliance.

2 Download vCloud Availability Appliances

   The vCloud Availability appliances are available for download at the My VMware® website.

3 Prepare the vCloud Availability Installer Appliance for vCloud Availability Installation

   You can simplify the deployment of individual components by defining installation variables or by creating a registry file on your vCloud Availability Installer Appliance.

4 Add Trusted Thumbprints to the vCloud Availability Installer Appliance

The vCloud Availability Installer Appliance must be able to verify the thumbprint of the vCenter Server and vCloud Director hosts that it works with.

5 Enable Static IP Addresses Deployment

By default, the vCloud Availability Installer Appliance creates VMs with DHCP. You can apply static IP addresses by adding the **`--vm-address`** option to any command that deploys an OVF.

6 Cassandra Installation and Configuration

Cassandra stores metadata and supports storage of the metadata for replication services.

7 RabbitMQ Installation and Configuration

RabbitMQ is used to exchange messages within a vCloud Director environment.

8 Configuring vCloud Director for Installation

vCloud Director must be configured to support environments that can securely support multiple tenants.

9 Create Cloud Proxy

The Cloud Proxy is a standalone, optional component of vCloud Director that can act as a generic Transmission Control Protocol (TCP) connection proxy. It supports forwarding incoming TCP connections and listening incoming connections.

10 Check vCloud Director Endpoints

Verify that your environment is properly configured for vCloud Availability installation, by checking the vCloud Director endpoints for known problems.

Create vCloud Availability Installer Appliance

To begin installing the components of vCloud Availability, you must first install and configure the vCloud Availability Installer Appliance.

You run all installation and configuration commands from the vCloud Availability Installer Appliance, unless documentation instructs otherwise.

This procedure demonstrates how to deploy and configure a vCloud Availability Installer Appliance by using the VMware OVF Tool. Alternatively, you can use the vSphere Web Client to install the vCloud Availability Installer Appliance.

The vCloud Availability Installer Appliance is deployed as an OVA file and includes the following components:

- vCloud Availability scripts for installation and maintenance operations
- SLES 12 SP1 image to provide a Docker container hosting

Installation and configuration procedures contain long commands with multiple arguments which you must run as single commands. For better visibility line breaks are marked with backslash (\) within a command. The beginning of a new command is marked with the number sign (#).

Procedure

1 Download the vCloud Availability Installer Appliance.

   a In a Web browser, navigate to the download page.

   b Download the `vcloud-availability-installer-appliance-release_number-xxx-build_number.ova` file.

2 Define deployment variables.

   The *VSPHERE_LOCATOR* value contains the target data center name, the tag *host*, the name of the target cluster, and the IP address or the fully qualified domain name (FQDN) of the target ESXi host. The *VSPHERE_LOCATOR* value depends on the topology of your vSphere environment. Following are examples for valid *VSPHERE_LOCATOR* values.

   - /*data-center-name*/host/*cluster-1-name*/*fully-qualified-domain-name*
   - /*data-center-name*/host/*cluster-2-name*/*host-IP-address*

   If the target ESXi host is not part of a cluster, skip the *cluster-name* element, as shown in the following examples.

   - /*data-center-name*/host/*fully-qualified-domain-name*
   - /*data-center-name*/host/*host-IP-address*

   The *VSPHERE_DATASTORE* value is the datastore name as it is displayed in the vSphere Web Client.

   For more information about the *VSPHERE_LOCATOR* and *VSPHERE_DATASTORE* values, see *Specifying the Inventory Path for a Cluster, Host, or Resource Pool* in the OVF Tool User's Guide.

```
# OVA_VM_NAME=vcav-installer-name

# VSPHERE_LOCATOR="vsphere-locator"

# VSPHERE_DATASTORE="vsphere-datastore"

# VSPHERE_ADDRESS=vsphere-ip-address

# VSPHERE_USER=vsphere-admin-user

# VSPHERE_NETWORK="VM-Network"

# OVA=local_client_path/vcloud-availability-installer-appliance-release_number-xxx-build_number.ova

# ROOT_PASSWORD=vcloud-availability-installer-appliance-root-password
```

3 Deploy vCloud Availability Installer Appliance OVA.

Note Password authentication is the default method for deploying the vCloud Availability Installer Appliance. You can deploy the appliance using SSH key authentication by adding the "--prop:guestinfo.cis.appliance.root.sshkey=${SSH_KEY}" argument in the installation command. You also must have a valid SSH public key to deploy vCloud Availability Installer Appliance using SSH key authentication method.

The following is a long, single command that should be run as one. There are breaks for better visibility marked with backslash (\).

```
# ovftool \
--acceptAllEulas \
--skipManifestCheck \
--X:injectOvfEnv \
--allowExtraConfig \
--X:enableHiddenProperties \
--sourceType=OVA \
--allowAllExtraConfig \
--powerOn \
--X:waitForIp \
"--net:VM Network=${VSPHERE_NETWORK}" \
--diskMode=thin \
--datastore=${VSPHERE_DATASTORE} \
--name=${OVA_VM_NAME} \
--prop:guestinfo.cis.appliance.net.pnid=${OVA_VM_NAME} \
--prop:guestinfo.cis.appliance.ssh.enabled=True \
"--prop:guestinfo.cis.appliance.root.password=${ROOT_PASSWORD}" \
${OVA} \
"vi://${VSPHERE_USER}@${VSPHERE_ADDRESS}${VSPHERE_LOCATOR}"
```

The system prints the IP address of the vCloud Availability Installer Appliance. Write down the IP address, because you are going to use it during the installation.

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

```
# ssh root@vCloud-Availability-Installer-Appliance-IP-Address
```

Working with the vCloud Availability Installer Appliance

You can use vCloud Availability Installer Appliance scripts to install, configure, and manage the vCloud Availability.

vCloud Availability Installer Appliance Basic Operations

You must create an SSH connection to the vCloud Availability Installer Appliance, to use the available scripts.

You must run vCloud Availability Installer Appliance commands from the **root** user's home directory of your vCloud Availability Installer Appliance.

The vCloud Availability Installer Appliance uses the following command-line syntax logic.`vcav [OPTIONS] COMMAND SUBCOMMAND [ARGUMENT]`

All arguments that end with an equals sign (=) require a value.

Asterisk (*) marks required arguments for a command.

If you are using a registry file to work with the vCloud Availability Installer Appliance, you can replace the `--vsphere-address`, `--vsphere-user`, and `--vsphere-password-file` options with the `--vsphere=`*`vsphere-name`* argument.

If you are using a registry file to work with the vCloud Availability Installer Appliance, you can replace the `--vcd-address`, `--vcd-user`, and `--vcd-password-file` options with `--vcd=`*`vcd-name`* . For more information about the registry file that the vCloud Availability Installer Appliance uses, see Prepare the vCloud Availability Installer Appliance for vCloud Availability Installation.

You can see the basic vCloud Availability Installer Appliance options and arguments in the following table.

Table 4-1. Basic vCloud Availability Installer Appliance Options and Arguments

Option	Argument	Description
`--help (-h)`	None	Displays a summary of options and arguments.
`--session-dir=`	File path	Define the location to store files and create a registry file.
`--log-level=`	`Error`, `Warning` , `Info`, and `Debug`	Define the level for logging in to the session directory.
`--debug (-d)`	None	Displays a `DEBUG` message in the vCloud Availability Installer Appliance console and creates an entry with the same information in the log file. By default, the value is set to `False`. You can append the option to every command that you run on the vCloud Availability Installer Appliance.
`--info (-i)`	None	Displays an `INFO` message to the vCloud Availability Installer Appliance console and creates an entry with the same information in the log file. By default, the value is set to `False`. You can append the option to every command that you run on the vCloud Availability Installer Appliance.
`--ssh-cert=`	`File path`	Use the option to provide the path to a private SSH certificate.
`--registry=`	`File path`	Use the option to provide the path to a registry file.

Table 4-1. Basic vCloud Availability Installer Appliance Options and Arguments (Continued)

Option	Argument	Description
`--dry-run`	None	Use this command to validate a process without running the command. By default, the value is set to `False`. You can append the option to every command that you run on the vCloud Availability Installer Appliance.
`-k`	None	**Caution** With this option, you can use SSL and SSH connections without a certificate validation. By default, the value is set to `False`. You can append the option to every command that you run on the vCloud Availability Installer Appliance.

Download vCloud Availability Appliances

The vCloud Availability appliances are available for download at the My VMware® website.

Download the vCloud Availability Portal Appliance

1 In a web browser, go to the download page.

2 Download the `vcloud-availability-for-vcd-ui-ova-`*`release_number`*`-xxxx-build_number.ova` file.

3 Upload the file to the **root** user's home directory of your vCloud Availability Installer Appliance.

Download the vCloud Availability 1.0.0 Appliances

1 In a web browser, go to the download page.

2 Download the `vCloud Availability for vCloud Director 1.0.0 (zip)` file.

3 Upload the file in the **root** directory of your vCloud Availability Installer Appliance.

4 Connect to the vCloud Availability Installer Appliance over SSH.

5 Unzip the file.

The `ZIP` contains the following files.

```
vCloud_Availability_4vCD-support.vmdk
vCloud_Availability_4vCD-system.vmdk
vCloud_Availability_4vCD_AddOn_OVF10.cert
vCloud_Availability_4vCD_AddOn_OVF10.mf
vCloud_Availability_4vCD_AddOn_OVF10.ovf
vCloud_Availability_4vCD_Cloud_Service_OVF10.cert
vCloud_Availability_4vCD_Cloud_Service_OVF10.mf
vCloud_Availability_4vCD_Cloud_Service_OVF10.ovf
vCloud_Availability_4vCD_OVF10.cert
```

```
vCloud_Availability_4vCD_OVF10.mf
vCloud_Availability_4vCD_OVF10.ovf
copyright.txt
readme
```

Prepare the vCloud Availability Installer Appliance for vCloud Availability Installation

You can simplify the deployment of individual components by defining installation variables or by creating a registry file on your vCloud Availability Installer Appliance.

Both ways to deploy and configure vCloud Availability are displayed for your reference. The installation using variables is presented in the left column of the table in each step, containing standard installation and configuration commands. The installation with simple commands, using a vCloud Availability Installer Appliance registry file, is presented in the right column of the table in each step.

Procedure

1 Create protected password files on your vCloud Availability Installer Appliance.

OS credentials are stored in text files in `~/.ssh` directory for all appliances. The files are only accessible to the system **root** user for security purposes. You provide the path to the respective password file during installation and configuration steps.

Note The *appliances-root-password* is the **root** password that is set for the vCloud Availability appliances that you create during installation procedures. The following example uses the same **root** password for all vCloud Availability appliances. You can set different passwords for all appliances, by creating a dedicated password file in the `~/.ssh` directory. Provide the path to the correct password file in the respective installation and configuration step.

Standard Command	Command Using Registry

`# mkdir ~/.ssh`
`# chmod 0700 ~/.ssh`
`# echo 'appliances-root-password' > ~/.ssh/.root`
`# echo 'vcd-password' > ~/.ssh/.vcd`
`# echo 'sso-password' > ~/.ssh/.sso`
`# echo 'management-vsphere-password' > ~/.ssh/.vsphere.mgmt`
`# find ~/.ssh -type f -name '.*' -print0 | xargs -0 chmod 0600`
	`# mkdir ~/.ssh`
	`# chmod 0700 ~/.ssh`
	`# echo 'appliances-root-password' > ~/.ssh/.root`
	`# find ~/.ssh -type f -name '.*' -print0 | xargs -0 chmod 0600`

2 Define installation variables.

In the current example, the deployment environment consists of one management vSphere and two resource vSphere sites.

The management vSphere details refer to the path of the environment managed by the service providers that is not available to tenant users. The resource vSphere details relate to the path of the environment that tenants use.

The resource vSphere sites are part of the same SSO domain to which the vCloud Director host is federated.

The management vSphere hosts the vSphere Replication Cloud Service and the vCloud Availability Portal.

A resource vSphere hosts the vSphere Replication Manager and the vSphere Replication Server.

For test and development environments, if you use docker to manage your Cassandra and RabbitMQ hosts, the commands in the current example place the docker host in the management vSphere environment.

If necessary, you can host all the components in the management vSphere.

The *VSPHERE_PLACEMENT_LOCATOR* value contains the target data center name, the tag *host*, the name of the target cluster, and the IP address or the fully qualified domain name (FQDN) of the target ESXi host. The *VSPHERE_PLACEMENT_LOCATOR* value depends on the topology of your vSphere environment. Following are examples for valid *VSPHERE_PLACEMENT_LOCATOR* values.

- /*data-center-name*/host/*cluster-1-name*/*fully-qualified-domain-name*
- /*data-center-name*/host/*cluster-2-name*/*host-IP-address*

If the target ESXi host is not part of a cluster, skip the *cluster-name* element, as shown in the following examples.

- /*data-center-name*/host/*fully-qualified-domain-name*
- /*data-center-name*/host/*host-IP-address*

The *VSPHERE_PLACEMENT_DATASTORE* value is the datastore name as it is displayed in the vSphere Web Client.

For more information about the *VSPHERE_PLACEMENT_LOCATOR* and *VSPHERE_PLACEMENT_DATASTORE* values, see *Specifying the Inventory Path for a Cluster, Host, or Resource Pool* in the OVF Tool User's Guide.

Important The *Variables* listed in the table are used as an example. Update values to match your environment.

Define Installation Variables

```
# export MGMT_VSPHERE_ADDRESS=mgmt-vsphere-address
# export MGMT_VSPHERE_USER=mgmt-vsphere-admin-user
# export MGMT_VSPHERE_LOCATOR='mgmt-locator'
# export MGMT_VSPHERE_DATASTORE='mgmt-datastore'
# export MGMT_VSPHERE_NETWORK='mgmt-network'

# export VSPHERE01_ADDRESS=vsphere-01-address
# export VSPHERE01_PLACEMENT_LOCATOR=vsphere-01-locator
# export VSPHERE01_PLACEMENT_DATASTORE=vsphere-01-datastore
# export VSPHERE01_PLACEMENT_NETWORK=vsphere-01-network


# export VSPHERE02_ADDRESS=vsphere-02-address
# export VSPHERE02_PLACEMENT_LOCATOR=vsphere-02-locator
# export VSPHERE02_PLACEMENT_DATASTORE=vsphere-02-datastore
# export VSPHERE02_PLACEMENT_NETWORK=vsphere-02-network


# export VCD_ADDRESS=vcd-01-address
# export VCD_USER=root@system
# export SSO_USER=administrator@vsphere.local
```

Create Registry File

1 Create a **~/.vcav/registry** file to hold installation variables. Update the values to match your environment.

```
vsphere mgmt-vsphere-name
    address mgmt-vsphere-address
    api-port 443
    api-user admin-user
    api-password admin-user-password
    placement-locator mgmt-locator
    placement-datastore mgmt-datastore
    placement-network mgmt-network

vsphere vsphere-01-name
    address vsphere-01-address
    api-port 443
    api-user vsphere-01-admin-user
    api-password vsphere-01-admin-password
    placement-locator vsphere-01-locator
    placement-datastore vsphere-01-datastore
    placement-network vsphere-01-network

vsphere vsphere-02-name
    address vsphere-02-address
    api-port 443
    api-user vsphere-02-admin-user
    api-password admin-user-password
    placement-locator vsphere-02-locator
    placement-datastore vsphere-02-datastore
    placement-network vsphere-02-network

VCD vcd-01-name
    address vcd-01-address
    api-port 443
    api-user root@System
    api-password vcd-root-password
    sso-user administrator@vsphere.local
    sso-password sso-password
```

2 Update the file permissions

```
# chmod 0600 ~/.vcav/registry
```

Add Trusted Thumbprints to the vCloud Availability Installer Appliance

The vCloud Availability Installer Appliance must be able to verify the thumbprint of the vCenter Server and vCloud Director hosts that it works with.

To achieve this, you first import the SSL certificate thumbprint of these hosts into the vCloud Availability Installer Appliance, by running the `vcav trust add` command. The command displays the thumbprint that you are importing. For security purposes, you must verify that the displayed thumbprint matches the actual server certificate.

If the SSL certificate of one of the servers changes, rerun the `vcav trust add` command for that host.

Procedure

1 Create a trust between your vSphere instances and the vCloud Availability Installer Appliance.

Repeat this step for every vCenter Server.

a

Standard Command	Command Using Registry
`# vcav trust add --address= $VSPHERE01_ADDRESS --port=443 --accept-all`	`# vcav trust add --vsphere=vsphere-01-name --accept-all`

b

Standard Command	Command Using Registry
`# vcav trust add --address= $VSPHERE02_ADDRESS --port=443 --accept-all`	`# vcav trust add --vsphere=vsphere-02-name --accept-all`

c

Standard Command	Command Using Registry
`# vcav trust add --address= $MGMT_VSPHERE_ADDRESS --port=443 --accept-all`	`# vcav trust add --vsphere=mgmt-vsphere-name --accept-all`

2 Create a trust with vCloud Director.

Standard Command	Command Using Registry
`# vcav trust add --address=$VCD_ADDRESS --port=443 --accept-all`	`# vcav trust add --vcd=vcd-01-name --accept-all`

Enable Static IP Addresses Deployment

By default, the vCloud Availability Installer Appliance creates VMs with DHCP. You can apply static IP addresses by adding the **`--vm-address`** option to any command that deploys an OVF.

You must add an IP Pool and IP Range in the Management vCenter Server for the network that you want to manage. The IP Pool objects assign all network parameters to VMs, except the IP address. The IP Pool object also ensures that the desired IP is supported on the requested network.

Procedure

1 List existing IP Pools, defined in your environment.

Standard Command	Command Using Registry

`# vcav ip-pool list \`
`--vsphere-address=$VSPHERE01_ADDRESS \`
`--vsphere-user=$SSO_USER \`
`--vsphere-password-file=~/.ssh/.sso`
	`# vcav ip-pool list --vsphere=vsphere-01-name`

The system displays the following result if you have no IP pools.

```
BackingDC
    No IP Pools
VC4
    No IP Pools
```

2 Create an IP pool.

The values used in the following command are used as examples. Update the values in the command to match your environment.

Standard Command	Command Using Registry

`# vcav ip-pool create \`
`--vsphere-address=$VSPHERE01_ADDRESS \`
`--vsphere-user=$SSO_USER \`
`--vsphere-password-file=~/.ssh/.sso \`
`--datacenter=VC4 \`
`--name=WDC3-Routed \`
`--subnet=10.158.12.0 \`
`--gateway=10.158.15.253 \`
`--netmask=255.255.252.0 \`
`"--dns=10.158.12.104,10.158.12.105" \`
`"--networks=VM Network"`
	`# vcav ip-pool create \`
	`--vsphere=vsphere-01-name \`
	`--datacenter=VC4 \`
	`--name=WDC3-Routed \`
	`--subnet=10.158.12.0 \`
	`--gateway=10.158.15.253 \`
	`--netmask=255.255.252.0 \`
	`"--dns=10.158.12.104,10.158.12.105" \`
	`"--networks=VM Network" \`

You created an IP pool. Running the **`vcav ip-pool list`** command now brings the following output.

```
BackingDC
    No IP Pools
VC4
    WDC3-Routed
        Networks:     VM Network
        IPv4 Subnet:  10.158.12.0
        IPv4 Gateway: 10.158.15.253
        IPv4 Netmask: 255.255.252.0
        IPv4 DNS:     10.158.12.104, 10.158.12.105
        IPv4 DHCP:    False
```

3 Associate the IP pool object with more networks.

Standard Command	Command Using Registry

`# vcav ip-pool update \`
`--vsphere-address=$VSPHERE01_ADDRESS \`
`--vsphere-user=$SSO_USER \`
`--vsphere-password-file=~/.ssh/.sso \`
`--datacenter=VC4 \`
`--name=WDC3-Routed \`
`"--networks=VM Network, Private Network"`
	`# vcav ip-pool update \`
	`--vsphere=vsphere-01-name \`
	`--datacenter=VC4 \`
	`--name=WDC3-Routed \`
	`"--networks=VM Network, Private Network"`

The associated networks are updated. Running the **`vcav ip-pool list`** command now results in the following output:

```
BackingDC
    No IP Pools
VC4
    WDC3-Routed
        Networks:     VM Network, Private Network
        IPv4 Subnet:  10.158.12.0
        IPv4 Gateway: 10.158.15.253
        IPv4 Netmask: 255.255.252.0
        IPv4 DNS:     10.158.12.104, 10.158.12.105
        IPv4 DHCP:    False
```

You created an IP pool in your environment and can create VMs with static IP addresses by adding **`--vm-address`** in any command that deploys an OVF.

Cassandra Installation and Configuration

Cassandra stores metadata and supports storage of the metadata for replication services.

For test and development environments, you can optionally skip this topic, and follow the instructions at Create Containers for Test and Development Environments to have Cassandra run in a Docker container instead.

The following is an example of the installation and configuration of a Cassandra server on a CentOS 6.5 host.

Prerequisites

- Verify that you have Python 2.7 or later.

- Verify that Java 1.7.X is installed and configured.

```
# cd /opt

# wget --no-cookies --no-check-certificate --header \
"Cookie: gpw_e24=http%3A%2F%2Fwww.oracle.com%2F; oraclelicense=accept-securebackup-cookie" \
"http://download.oracle.com/otn-pub/java/jdk/7u79-b15/jdk-7u79-linux-x64.tar.gz"

# tar xzf jdk-7u79-linux-x64.tar.gz
```

Update Security

```
# wget --no-cookies --no-check-certificate --header \
"Cookie: gpw_e24=http%3A%2F%2Fwww.oracle.com%2F; oraclelicense=accept-securebackup-cookie" \
http://download.oracle.com/otn-pub/java/jce/7/UnlimitedJCEPolicyJDK7.zip

# unzip UnlimitedJCEPolicyJDK7.zip

# cp UnlimitedJCEPolicy/*.jar /opt/jdk1.7.0_79/jre/lib/security/
```

Install and Configure Java

```
# cd /opt/jdk1.7.0_79/

# alternatives --install /usr/bin/java java /opt/jdk1.7.0_79/bin/java 2

# alternatives --config java
```

Verify that the latest version of Java is installed and active

```
# java –version
```

Procedure

1 Run the following commands to add the DataStax Community repository and install Cassandra.

a Create the file `/etc/yum.repos.d/datastax.repo`. The contents are:

```
[datastax]
name = DataStax Repo for Apache Cassandra
baseurl = https://rpm.datastax.com/community
enabled = 1
gpgcheck = 0
```

b Install Cassandra

```
# yum install dsc22 cassandra22 –y
```

c Start and verify the newly installed Cassandra.

```
# service cassandra start
```

d Check Cassandra service status:

```
# service cassandra status
```

e Enter Cassandra command line to verify setup:

```
# cqlsh
```

If an error regarding python occurs when running cqlsh, update Python to Python 2.7:

```
# yum install –y centos–release–SCL

# yum install –y python27

# scl enable python27 bash

# echo "/usr/lib/python2.7/site–packages/" > \
/opt/rh/python27/root/usr/lib/python2.7/site–packages/usrlocal.pth
```

2 Modify Cassandra to enable SSL

Cassandra requires SSL communication between client and node to enable vSphere Replication Cloud Service to communicate with Cassandra.

a On each node, create a certificate:

Generate SSL certificate

```
# /opt/jdk1.7.0_79/bin/keytool –keystore /etc/cassandra/conf/.keystore \
–storepass vmware –validity 365 –storetype JKS –genkey –keyalg RSA \
–alias ${CASS_NODE} –dname 'cn=${CASS_NODE}, ou=DR2C, o=VMware, c=US' \
–keypass vmware
```

b Export Cassandra certificate. In `cloud–cassandra–X.pem`, the X represents the node number.

```
# /opt/jdk1.7.0_79/bin/keytool –export –rfc \
–keystore /etc/cassandra/conf/.keystore –storepass vmware \
–file /root/cloud–${CASS_NODE}.pem –alias ${CASS_NODE}
```

c Copy `.pem` files to all other servers

d Import each certificate into `truststore`:

```
# /opt/jdk1.7.0_79/bin/keytool –noprompt –import –trustcacerts \
–alias ${CASS_NODE} –file /root/cloud–${CASS_NODE}.pem \
–keystore /etc/cassandra/conf/.truststore –storepass vmware
```

The truststore contains a copy of the pem certificate of all the nodes.

3 Modify Cassandra to enable SSL

a Enable client communication with Cassandra over SSL by editing: `/etc/cassandra/conf/cassandra.yaml`

```
# Comment out listen_address and bind to listen_interface instead

#listen_address: localhost
listen_interface: eth1

# Comment out rpc_address and bind to rpc_interface instead

#rpc_address: localhost
rpc_interface: eth1

# ----------------- Further down in file
server_encryption_options:
   internode_encryption: all
   keystore: /etc/cassandra/conf/.keystore
   keystore_password: vmware
   truststore: /etc/cassandra/conf/.truststore
   truststore_password: vmware
   require_client_auth: true
   store_type: JKS
#------------------------

# ----------------- Further down in file
Client_encryption_options:
enabled: true
keystore: /etc/cassandra/conf/.keystore
keystore_password: vmware
require_client_auth: true

# Set trustore and truststore_password if require_client_auth is true
truststore: /etc/cassandra/conf/.truststore
truststore_password: vmware

# More advanced defaults below:

# protocol: TLS

# algorithm: SunX509
store_type: JKS
```

b Restart Cassandra

```
# service cassandra restart
```

RabbitMQ Installation and Configuration

RabbitMQ is used to exchange messages within a vCloud Director environment.

If you have already installed RabbitMQ, make sure that the host is configured to support SSL connections.

For test and development environments, you can optionally skip this procedure and follow the instructions at Create Containers for Test and Development Environments to have RabbitMQ run in a Docker container instead.

The following is an example of the process of installing and configuring a RabbitMQ host.

Download an Install RabbitMQ

```
# wget https://www.rabbitmq.com/releases/erlang/erlang-18.3-1.el6.x86_64.rpm
# rpm -i erlang-18.3-1.el6.x86_64.rpm
# wget http://www.rabbitmq.com/releases/rabbitmq-server/v3.6.1/rabbitmq-server-3.6.1-1.noarch.rpm
# rpm --import https://www.rabbitmq.com/rabbitmq-signing-key-public.asc
# rpm -i rabbitmq-server-3.6.1-1.noarch.rpm
```

Create Self-Signed Certificates

```
# wget https://github.com/michaelklishin/tls-gen/archive/master.zip
# unzip master.zip
# cd tls-get-master/basic
```

Replace `vcd-db.gcp.local` with your domain:

```
# CN=vcd-db.gcp.local PASSWORD=vmware make
# mv testca/ /etc/rabbitmq/
# mv server/ /etc/rabbitmq/
# mv client/ /etc/rabbitmq/
```

Set Owner:

```
# chown -R rabbitmq: /etc/rabbitmq/testca
# chown -R rabbitmq: /etc/rabbitmq/server
# chown -R rabbitmq: /etc/rabbitmq/client
```

Create the file `/etc/rabbitmq/rabbitmq.config` with the following content.

```
[
  {ssl, [{versions, ['tlsv1.2', 'tlsv1.1', tlsv1]}]},
  {rabbit, [
     {ssl_listeners, [5671]},
     {ssl_options, [{cacertfile,"/etc/rabbitmq/testca/cacert.pem"},
                    {certfile,"/etc/rabbitmq/server/cert.pem"},
                    {keyfile,"/etc/rabbitmq/server/key.pem"},
            {versions, ['tlsv1.2', 'tlsv1.1', tlsv1]},
            {ciphers,  ["ECDHE-ECDSA-AES256-GCM-SHA384","ECDHE-RSA-AES256-GCM-SHA384",
             "ECDHE-ECDSA-AES256-SHA384","ECDHE-RSA-AES256-SHA384",
             "ECDH-ECDSA-AES256-GCM-SHA384","ECDH-RSA-AES256-GCM-SHA384",
             "ECDH-ECDSA-AES256-SHA384","ECDH-RSA-AES256-SHA384",
             "DHE-RSA-AES256-GCM-SHA384","DHE-DSS-AES256-GCM-SHA384",
```

```
              "DHE-RSA-AES256-SHA256","DHE-DSS-AES256-SHA256","AES256-GCM-SHA384",
              "AES256-SHA256","ECDHE-ECDSA-AES128-GCM-SHA256",
              "ECDHE-RSA-AES128-GCM-SHA256","ECDHE-ECDSA-AES128-SHA256",
              "ECDHE-RSA-AES128-SHA256","ECDH-ECDSA-AES128-GCM-SHA256",
              "ECDH-RSA-AES128-GCM-SHA256","ECDH-ECDSA-AES128-SHA256",
              "ECDH-RSA-AES128-SHA256","DHE-RSA-AES128-GCM-SHA256",
              "DHE-DSS-AES128-GCM-SHA256","DHE-RSA-AES128-SHA256","DHE-DSS-AES128-SHA256",
              "AES128-GCM-SHA256","AES128-SHA256","ECDHE-ECDSA-AES256-SHA",
              "ECDHE-RSA-AES256-SHA","DHE-RSA-AES256-SHA","DHE-DSS-AES256-SHA",
              "ECDH-ECDSA-AES256-SHA","ECDH-RSA-AES256-SHA","AES256-SHA",
              "ECDHE-ECDSA-DES-CBC3-SHA","ECDHE-RSA-DES-CBC3-SHA","EDH-RSA-DES-CBC3-SHA",
               "EDH-DSS-DES-CBC3-SHA","ECDH-ECDSA-DES-CBC3-SHA","ECDH-RSA-DES-CBC3-SHA",
              "DES-CBC3-SHA","ECDHE-ECDSA-AES128-SHA","ECDHE-RSA-AES128-SHA",
               "DHE-RSA-AES128-SHA","DHE-DSS-AES128-SHA","ECDH-ECDSA-AES128-SHA",
               "ECDH-RSA-AES128-SHA","AES128-SHA","EDH-RSA-DES-CBC-SHA","DES-CBC-SHA"]},
              {verify,verify_none},
                      {fail_if_no_peer_cert,false}]}]}
].
```

Start RabbitMQ

```
# service rabbitmq-server start
```

Enable RabbitMQ UI

To enable the UI on `http://server-name:15672/`

```
# rabbitmq-plugins enable rabbitmq_management
```

Create admin user to log in:

```
# rabbitmqctl add_user admin vmware
# rabbitmqctl set_permissions -p / admin ".*" ".*" ".*"
# rabbitmqctl set_user_tags admin administrator
```

Configuring vCloud Director for Installation

vCloud Director must be configured to support environments that can securely support multiple tenants.

The vCloud Director environment must be fully configured to support workloads before you can continue with the vCloud Availability installation. You must create the Resource vSphere, Provider VDCs, Organizations, and Organization VDCs before installing the vCloud Availability solution. For more information, see the vCloud Director 8.10 Administrator's Guide.

vCloud Director is configured to use the following settings:

- Port 5671 is used for AMQP messaging over SSL. SSL connections are recommended, but if there is a requirement to use non-SSL connections for vCloud Director, you can add the `--amqp-port=`*`port-number`* argument to the `vcav hcs configure` command. For more information, see Configure vSphere Replication Cloud Service. You can configure RabbitMQ to listen on both SSL and non-SSL ports. For more information, see RabbitMQ Installation and Configuration. For more information about configuring an AMQP broker, see Configure an AMQP Broker in *vCloud Director Administrator's Guide*.

  To configure vCloud Director to use the RabbitMQ Servers, do the following:

  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 by running the follwoing command on the vCloud Availability Installer Appliance:

  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
  ```

  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.

- Enabled Public URL and certificates. For more information, see Configuring Public Addresses in *vCloud Director Administrator's Guide.*
- Shared single sign-on. For more information, see Configure vCloud Director to use vCenter Single Sign On in *vCloud Director Administrator's Guide.*

By default, vCloud Availability 1.0.1 supports the use of TLS 1.2 during the SLL handshake process. To build a pure TLS 1.2 environment for vCloud Availability operations, the vSphere Replication and vCenter Server instances that are deployed on-premise must also support TLS 1.2. For more information, select the *Transport Layer Security* category from the drop-down in the Interoperability Pages for vCloud Availability 1.0.1.

Configure the timeout settings for the vCloud Director extensions.

Use a text editor to open */opt/vmware/vcloud-director/etc/global.properties* file. Set the *extensibility.timeout* value to 60.

Use a wildcard certificate for all public interfaces of vCloud Director to enable certificate sharing between multiple hosts and subdomains. For example:

```
*.provider.com
```

Copies of the following files are required to create and configure a Cloud Proxy:

- `/opt/vmware/vcloud-director/etc/responses.properties`
- `certificates.ks`

Create Cloud Proxy

The Cloud Proxy is a standalone, optional component of vCloud Director that can act as a generic Transmission Control Protocol (TCP) connection proxy. It supports forwarding incoming TCP connections and listening incoming connections.

By default, the Cloud Proxy can create virtual connections for data to travel from the tenant (on-premise) site to the service provider (cloud) site and reverse. A vCloud Director instance runs Cloud Proxy services on the same Java Virtual Machine (JVM). For scalability purposes, vCloud Director appliances can be configured to act as a different type of cell, each one with its own JVM. For example, you can configure a vCloud Director appliance to act as an Application cell, as a Cloud Proxy cell, or as a combination of both types on the same cell. Cloud Proxy scales out horizontally, depending on the number of concurrent connections.

If you are installing vCloud Availability on top of an existing vCloud Director infrastructure, you can configure existing vCloud Director appliances to serve as Cloud Proxy instances, by disabling most of the vCloud Director services. Cloud Proxy hosts must have access to the vCloud Director data base and the transfer share.

You can load balance Cloud Proxy instances with different public Virtual IP addresses (VIPs). You can also use SSL certificates different from the other vCloud Director instances.

Cloud Proxy scales out horizontally, depending on the number of concurrent connections.

Cloud Proxy provides the endpoints used for replicating data for the vCloud Availability solution. Cloud Proxy installation and configuration for vCloud Availability requires configuration of a vCloud Director instance and network interface.

For testing and developing deployments, you can use the primary vCloud Director host as a Cloud Proxy. Deploy additional Cloud Proxy hosts and register them with vCloud Director to expand capacity.

Prerequisites

- Create a virtual machine to run the Cloud Proxy. The Cloud Proxy uses the same OS and configuration as the vCloud Director hosts. For more information about supported operating systems, see the *vCloud Director for Service Providers Release Notes*.
- Verify that all vCloud Director and Cloud Proxy instances have FQDN configured.
- Verify that NTP is configured.

- Verify that the OpenSSL version used in the Guest OS of vCloud Director instance is 1.0.1e-30 or later.
- Verify that the Cloud Proxy hosts use a wildcard certificate and cover all Cloud Proxy host names. If the Cloud Proxy certificate differs from the one used on your vCloud Director instances, you must update the SSL certificates on the Cloud Proxy hosts. For more information about creating and importing SSL certificates, see the *vCloud Director Installation and Upgrade Guide*.

Procedure

1 Pre-installation

a Copy the `vmware-vcloud-director-X.X.X-YYYY.bin` file to the `/tmp` folder of the new Cloud Proxy virtual machine by running the following command.

```
# scp root@vcd-address:/file-path/vmware-vcloud-director-X.X.X-YYYY.bin /tmp
# chmod 755 /tmp/vmware-vcloud-director-X.X.X-YYYY.bin
```

The `certificates.ks` file is located in the same location as on the primary vCloud Director host. You can find the exact path at `user.keystore.path` in the `responses.properties` file. Update the `user.keystore.path` value to reflect the new path to the certificates file.

b Copy the configuration file to the `/tmp` folder of the new Cloud Proxy virtual machine by running the following command.

```
# scp root@vcd-address:/opt/vmware/vcloud-director/etc/responses.properties /tmp
# chmod 644 /tmp/responses.properties
```

c Copy the certificates file to the `/tmp` folder of the new Cloud Proxy virtual machine by running the following command.

```
# scp root@vcd-address:/root/certificates.ks /tmp
# chmod 644 /tmp/certificates.ks
```

d Update the `database.jdbcUrl` value in the `responses.properties` file to use FQDN for a database host.

e Mount shared NFS storage.

Verify that you have mounted the shared NFS storage to your Cloud Proxy `/opt/vmware/vcloud-director/data/transfer`.

f Cloud Proxy Second Network Interface

The vCloud Director installation requires a second NIC to be present, but the Cloud Proxy does not use the second NIC. If you have already provisioned your virtual machine with a second NIC you can set the IP address to a single CIDR address, for example *192.168.254.254/32*. In this case, you do not need to configure the alias NIC.

g If necessary, set up an alias NIC:

```
# ifconfig eth0:5 192.168.254.254 up
```

2 Install

Run the vCloud Director install script: `vmware-vcloud-director-X.X.X-YYYY.bin`

- Do not run the configuration
- Do not start the `vmware-vcd` service

3 Configure

Use the `responses.properties` file to configure the vCloud Director host. Make sure that you do not start the `vmware-vcd` service.

```
# /opt/vmware/vcloud-director/bin/configure -r /tmp/responses.properties
```

This operation takes a few minutes to finish. The system does not display any output during this time.

4 Specialize a vCloud Director cell to become a dedicated Cloud Proxy cell

Edit `/opt/vmware/vcloud-director/etc/global.properties`:

Add the following property:

```
com.vmware.cell.runtime.application=com.vmware.vcloud.cloud-proxy-server.cloudProxyApplication
```

5 Second NIC

The second NIC or alias that you used for the install is no longer required. You can safely turn off the interface.

```
# ifconfig eth0:5 192.168.254.254 down
```

6 Start the vCloud Director service.

```
service vmware-vcd start
```

7 Modify Cloud Proxy address.

If you are running separate Cloud Proxy instances, you must change the address for the Cloud Proxy server.

a Create a protected password files on your vCloud Availability Installer Appliance in the `~/.ssh` directory.

```
# mkdir ~/.ssh
# chmod 0700 ~/.ssh
# echo 'vcd-password' > ~/.ssh/.vcd
# find ~/.ssh -type f -name '.*' -print0 | xargs -0 chmod 0600
```

b To see the currently configured Cloud Proxy address, run the following command on the vCloud Availability Installer Appliance.

```
# vcav vcd get-cloud-proxy \
--type=to-the-cloud \
--vcd-address=vcd-address \
--vcd-user=vcd-user \
--vcd-password-file=~/.ssh/.vcd
```

The vCloud Availability Installer Appliance returns the following message.

```
wss://cloud-proxy-IP-address:to-the-cloud-port/socket/cloudProxy
```

c Modify the Cloud Proxy by using the following command.

You can modify `--to-the-cloud-address`, `--to-the-cloud-port`, and `--from-the-cloud-address`. For this example, `--to-the-cloud-address` is modified.

```
# vcav vcd set-cloud-proxy \
--to-the-cloud-address=cloud-proxy-FQDN \
--vcd-address=vcd-address \
--vcd-user=vcd-user \
--vcd-password-file=~/.ssh/.vcd
```

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

Check vCloud Director Endpoints

Verify that your environment is properly configured for vCloud Availability installation, by checking the vCloud Director endpoints for known problems.

This check verifies the connectivity between vCloud Director and all related vCenter Server instances.

Procedure

- To verify that your environment is properly configured, run the following command.

Standard Command	Command Using Registry

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

The system returns an **OK** message upon successful validation.

Installing vCloud Availability

Before configuring, you must deploy virtual appliances to support vCloud Availability services.

You install all individual components of vCloud Availability by using the vCloud Availability Installer Appliance. The vCloud Availability Installer Appliance simplifies the installation by supporting a text registry file where all vSphere and vCloud Director details are stored.

There are two ways to deploy and configure vCloud Availability

- You can use **Full Commands Installation**. The commands include addresses, user names, and the location of password files for all vCenter Server instances and vCloud Director hosts.
- With **Simple Command Installation** you are using a vCloud Availability Installer Appliance registry. This way all vCenter Server and vCloud Director details are contained in a registry file.

Both ways to deploy and configure vCloud Availability are demonstrated for your reference.

You run all installation commands from the vCloud Availability Installer Appliance, unless documentation instructs otherwise.

Create vSphere Replication Manager

The vSphere Replication Manager manages and monitors the replication process from tenant VMs to the service provider environment. A vSphere Replication management service runs for each vCenter Server and tracks changes to VMs and infrastructure related to replication.

The Resource vCenter Server is a vCenter Server registered to vCloud Director and made available to tenants.

Important Deploy one vSphere Replication Manager for each Resource vCenter Server. The total number of vSphere Replication Management servers depends on your environment and deployment requirements.

Procedure

1 Create an SSH connection to the vCloud Availability Installer Appliance using your **root** credentials. You run all installation and configuration commands from the vCloud Availability Installer Appliance.

2 Create a vSphere Replication Manager.

Standard Command	Command Using Registry

`# vcav hms create \`
`--ovf-url=vCloud_Availability_4vCD_OVF10.ovf \`
`--vsphere-address=$VSPHERE01_ADDRESS \`
`--vsphere-user=$SSO_USER \`
`--vsphere-password-file=~/.ssh/.sso \`
`"--network=$VSPHERE01_PLACEMENT_NETWORK" \`
`"--vsphere-locator=`
`$VSPHERE01_PLACEMENT_LOCATOR" \`
`--datastore=$VSPHERE01_PLACEMENT_DATASTORE \`
`--ntp=pool.ntp.org \`
`--root-password-file=~/.ssh/.root \`
`--vm-name=hms01-name`
	`# vcav hms create \`
	`--ovf-url=vCloud_Availability_4vCD_OVF10.ovf \`
	`--vsphere=vsphere-01-name \`
	`--ntp=pool.ntp.org \`
	`--root-password-file=~/.ssh/.root \`
	`--vm-name=hms01-name`

The IP address of the new vSphere Replication Manager is displayed. Write it down because you need it during the configuration.

Repeat this step for every resource vCenter Server in your environment.

3 If necessary, unregister the vSphere Replication extension from the vSphere Web Client.

By default, the vSphere Replication Manager registers as an extension to the instance of vSphere it is deployed to. This model is called in inventory deployment. For in inventory deployments, the vSphere Replication Manager manages the replications to the vSphere instance it is deployed to. In such cases, you must skip this step.

You can deploy a vSphere Replication Manager to an infrastructure pool that tenants are not using and register the vSphere Replication Manager to a resource pool instance of vSphere. This model is called out of inventory deployment. For out of inventory deployments, the vSphere Replication Manager does not manage the replications to the vSphere instance it is deployed to. In such cases, you must unregister the vSphere Replication extension by running the following command.

Standard Command	Command Using Registry

`# vcav hms unregister-extension \`
`--vsphere-address=$VSPHERE01_ADDRESS \`
`--vsphere-user=$SSO_USER \`
`--vsphere-password-file=~/.ssh/.sso`
	`# vcav hms unregister-extension \`
	`--vsphere=vsphere-01-name`

4 Set a variable to the address of the created virtual machine.

Standard Command

```
# HMS01_ADDRESS=`vcav vsphere get-ip \
--vsphere-address=$VSPHERE01_ADDRESS \
--vsphere-user=$SSO_USER \
--vsphere-password-file=~/.ssh/.sso \
"--network=$VSPHERE01_PLACEMENT_NETWORK" \
--vm-name=hms01-name`
```

Command Using Registry

```
# HMS01_ADDRESS=`vcav vsphere get-ip \
--vsphere=vsphere-01-name \
"--network=vsphere-01-network" \
--vm-name=hms01-name`
```

5 If you use Fully Qualified Domain Names (FQDN) to access and manage appliances, you must verify that the DNS record matches the vSphere Replication Manager IP address and trusts the SSH certificate for this FQDN.

a Check the DNS server to ensure that the entry matches the IP address of the vSphere Replication Manager.

b Run the following command to trust the certificate for the vSphere Replication Manager FQDN.

Standard Command

```
# vcav vsphere trust-ssh \
--vsphere-address=$VSPHERE01_ADDRESS \
--vsphere-user=$SSO_USER \
--vsphere-password-file=~/.ssh/.sso \
--root-password-file=~/.ssh/.root \
--vm-name=hms01-name \
--vm-address=hms01-FQDN
```

Command Using Registry

```
# vcav vsphere trust-ssh \
--vsphere=vsphere-01-name \
--root-password-file=~/.ssh/.root \
--vm-name=hms01-name \
--vm-address=hms01-FQDN
```

Create vSphere Replication Cloud Service Host

The vSphere Replication Cloud Service is a tenant-aware replication manager that provides the required API for managing the service and all the components. vSphere Replication Cloud Service registers as a vCloud Director extension and is accessible through the vCloud Director interface.

Procedure

1 Create a vSphere Replication Cloud Service host.

Standard Command

```
# vcav hcs create \
--ovf-
url=vCloud_Availability_4vCD_Cloud_Service_OVF10.ovf \
--vsphere-address=$MGMT_VSPHERE_ADDRESS \
--vsphere-user=$MGMT_VSPHERE_USER \
--vsphere-password-file=~/.ssh/.vsphere.mgmt \
"--network=$MGMT_VSPHERE_NETWORK" \
"--vsphere-locator=$MGMT_VSPHERE_LOCATOR" \
--datastore=$MGMT_VSPHERE_DATASTORE \
--ntp=pool.ntp.org \
--root-password-file=~/.ssh/.root \
--vm-name=hcs01-name
```

Command Using Registry

```
# vcav hcs create \
--ovf-
url=vCloud_Availability_4vCD_Cloud_Service_OVF10.ovf \
--vsphere=mgmt-vsphere-name \
--ntp=pool.ntp.org \
--root-password-file=~/.ssh/.root \
--vm-name=hcs01-name
```

The IP address of the new vSphere Replication Cloud Service host is displayed. Write it down because you need it during the configuration.

2 Set a variable to the address of the created virtual machine.

Standard Command

```
# HCS01_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=hcs01-name`
```

Command Using Registry

```
# HCS01_ADDRESS=`vcav vsphere get-ip \
--vsphere=mgmt-vsphere-name \
"--network=mgmt-network" \
--vm-name=hcs01-name`
```

3 If you use Fully Qualified Domain Names (FQDN) to access and manage appliances, you must verify that the DNS record matches the vSphere Replication Cloud Service host IP address, and trusts the SSH certificate for this FQDN.

a Check the DNS server to ensure that the record matches the IP address of the vSphere Replication Cloud Service host.

b Run the following command to trust the certificate for the vSphere Replication Cloud Service host FQDN.

Standard Command

```
# vcav vsphere trust-ssh \
--vsphere-address=$MGMT_VSPHERE_ADDRESS \
--vsphere-user=$MGMT_VSPHERE_USER \
--vsphere-password-
file=~/.ssh/.vsphere.mgmt \
--root-password-file=~/.ssh/.root \
--vm-name=hcs01-name \
--vm-address=hcs01-FQDN
```

Command Using Registry

```
# vcav vsphere trust-ssh \
--vsphere=mgmt-vsphere-name \
--root-password-file=~/.ssh/.root \
--vm-name=hcs01-name \
--vm-address=hcs01-FQDN
```

Create vSphere Replication Server

The vSphere Replication Server handles the replication process for each protected virtual machine.

Important Deploy at least one vSphere Replication Server for each vSphere Replication Manager.

Procedure

1 Create vSphere Replication Server.

Standard Command

```
# vcav hbr create \
--ovf-
url=vCloud_Availability_4vCD_AddOn_OVF10.ovf \
--vsphere-address=$VSPHERE01_ADDRESS \
--vsphere-user=$SSO_USER \
--vsphere-password-file=~/.ssh/.sso \
"--network=$VSPHERE01_PLACEMENT_NETWORK" \
"--vsphere-locator=
$VSPHERE01_PLACEMENT_LOCATOR" \
--datastore=$VSPHERE01_PLACEMENT_DATASTORE \
--ntp=pool.ntp.org \
--root-password-file=~/.ssh/.root \
--vm-name=hbr01-name
```

Command Using Registry

```
# vcav hbr create \
--ovf-
url=vCloud_Availability_4vCD_AddOn_OVF10.ovf \
--vsphere=vsphere-01-name \
--ntp=pool.ntp.org \
--root-password-file=~/.ssh/.root \
--vm-name=hbr01-name
```

The IP address of the new vSphere Replication Server is displayed. Write it down because you need it during the configuration.

Important Repeat this step for every vSphere Replication Manager in your environment.

2 Set a variable to the address of the created virtual machine.

Standard Command

```
# HBR01_ADDRESS=`vcav vsphere get-ip \
--vsphere-address=$VSPHERE01_ADDRESS \
--vsphere-user=$SSO_USER \
--vsphere-password-file=~/.ssh/.sso \
"--network=$VSPHERE01_PLACEMENT_NETWORK" \
--vm-name=hbr01-name`
```

Command Using Registry

```
# HBR01_ADDRESS=`vcav vsphere get-ip \
--vsphere=vsphere-01-name \
"--network=vsphere-01-network" \
--vm-name=hbr01-name`
```

3 If you use Fully Qualified Domain Names (FQDN) to access and manage appliances, you must verify that the DNS record matches the vSphere Replication Server IP address, and trust the SSH certificate for this FQDN.

   a Check the DNS server to ensure that the entry matches the IP address of the vSphere Replication Server.

   b Run the following command to trust the certificate for the vSphere Replication Server FQDN.

Standard Command	Command Using Registry

`# vcav vsphere trust-ssh \`
`--vsphere-address=$VSPHERE01_ADDRESS \`
`--vsphere-user=$SSO_USER \`
`--vsphere-password-file=~/.ssh/.sso \`
`--root-password-file=~/.ssh/.root \`
`--vm-name=hbr01-name \`
`--vm-address=hbr01-FQDN`
	`# vcav vsphere trust-ssh \`
	`--vsphere=vsphere-01-name \`
	`--root-password-file=~/.ssh/.root \`
	`--vm-name=hbr01-name \`
	`--vm-address=hbr01-FQDN`

Create vCloud Availability Portal Host

The vCloud Availability Portal provides a graphic user interface to facilitate the management of vCloud Availability operations.

The vCloud Availability Portal back end (PBE) scales horizontally. You can deploy a new vCloud Availability Portal instance on demand connected to the same load balancer that all the vCloud Availability Portal instances are under. The load balancer must support sticky sessions, so that the same PBE instance processes user requests within a session. This setting ensures that all the information displayed in the vCloud Availability Portal is consistent.

Depending on the number of concurrent sessions that the vCloud Availability Portal is expected to host, you can deploy `small`, `medium`, or `large` vCloud Availability Portal host. The vCloud Availability Portal sends requests to a vCloud Director instance and receives data from the same vCloud Director instance. To host the maximum number of concurrent sessions, ensure that the vCloud Director database can use similar compute resources that you allocate to the vCloud Availability Portal host. You can find details about the vCloud Availability Portal deployment types in the following table.

Table 4-2. vCloud Availability Portal Host Deployment Types

Deployment Type	Description
`Small`	Deploys an appliance with 2 CPUs, 2 GB of memory, 10 GB of disk space, and 512 MB of Java Virtual Memory. Suitable for hosting up to 150 concurrent sessions.
`Medium`	Deploys an appliance with 2 CPUs, 4 GB of memory, 10 GB of disk space, and 1.5 GB of Java Virtual Memory. Suitable for hosting up to 400 concurrent sessions.
`Large`	Deploys an appliance with 4 CPUs, 6 GB of memory, 10 GB of disk space, and 3 GB of Java Virtual Memory. Suitable for hosting up to 800 concurrent sessions.

Procedure

1 Create a vCloud Availability Portal host by running the following command.

Important The `--deployment-type` argument in the following command defines the compute resources that you allocate to the vCloud Availability Portal host. By default, the value is `small`. You can change the value depending on your requirements.

Standard Command

```
# vcav vcd-ui create \
--ovf-url=vcloud-availability-for-vcd-ui-
ova-1.0.1.2-xxx-build_number.ova \
--deployment-type=small \
--vsphere-address=$MGMT_VSPHERE_ADDRESS \
--vsphere-user=$MGMT_VSPHERE_USER \
--vsphere-password-file=~/.ssh/.vsphere.mgmt \
"--network=$MGMT_VSPHERE_NETWORK" \
"--vsphere-locator=$MGMT_VSPHERE_LOCATOR" \
--datastore=$MGMT_VSPHERE_DATASTORE \
--ntp=pool.ntp.org \
--root-password-file=~/.ssh/.root \
--vm-name=ui01-name
```

Command Using Registry

```
# vcav vcd-ui create \
--ovf-url=vcloud-availability-for-vcd-ui-
ova-1.0.1.2-xxx-build_number.ova \
--deployment-type=small \
--vsphere=mgmt-vsphere-name \
--ntp=pool.ntp.org \
--root-password-file=~/.ssh/.root \
--vm-name=ui01-name
```

The IP address of the new vCloud Availability Portal virtual machine is displayed. Write it down because you need it during the configuration.

2 Set a variable to the address of the created virtual machine.

Standard Command

```
# UI01_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=ui01-name`
```

Command Using Registry

```
# UI01_ADDRESS=`vcav vsphere get-ip \
--vsphere=mgmt-vsphere-name \
"--network=mgmt-network" \
--vm-name=ui01-name`
```

3 Update the `truststore` file with the vCloud Availability Portal virtual machine credentials.

```
# echo 'Portal-VM-Password' > ~/.ssh/.truststore

# chmod 0600 ~/.ssh/.truststore
```

4 If you use Fully Qualified Domain Names (FQDN) to access and manage appliances, you must verify that the DNS record matches the vCloud Availability Portal IP address, and trusts the SSH certificate for this FQDN.

   a Check the DNS server to ensure that the entry matches the IP address of the vCloud Availability Portal host.

   b Run the `trust-ssh` command to trust the certificate for the vCloud Availability Portal FQDN.

Standard Command

```
# vcav vsphere trust-ssh \
--vsphere-address=$MGMT_VSPHERE_ADDRESS \
--vsphere-user=$MGMT_VSPHERE_USER \
--vsphere-password-
file=~/.ssh/.vsphere.mgmt \
--root-password-file=~/.ssh/.root \
--vm-name=ui01-name \
--vm-address=ui01-FQDN
```

Command Using Registry

```
# vcav vsphere trust-ssh \
--vsphere=mgmt-vsphere-name \
--root-password-file=~/.ssh/.root \
--vm-name=ui01-name \
--vm-address=ui01-FQDN
```

Create vCloud Availability Administration Portal Host

The vCloud Availability Administration Portal provides a graphic user interface to facilitate the service providers to monitor and manage their DR environments.

Important You must deploy vCloud Availability Administration Portal separately from vCloud Availability Portal. The best practice is to deploy it behind a VPN to limit access.

Depending on the number of concurrent sessions that the vCloud Availability Administration Portal is expected to host, you can deploy `small`, `medium`, or `large` vCloud Availability Administration Portal host. The vCloud Availability Administration Portal sends requests to a vCloud Director instance and receives data from the same vCloud Director instance. To host the maximum number of concurrent sessions, ensure that the vCloud Director database can use similar compute resources that you allocate to the vCloud Availability Administration Portal host. You can find details about the vCloud Availability Administration Portal deployment types in the following table.

Table 4-3. vCloud Availability Administration Portal Host Deployment Types

Deployment Type	Description
`Small`	Deploys an appliance with 2 CPUs, 2 GB of memory, 10 GB of disk space, and 512 MB of Java Virtual Memory. Suitable for hosting up to 150 concurrent sessions.
`Medium`	Deploys an appliance with 2 CPUs, 4 GB of memory, 10 GB of disk space, and 1.5 GB of Java Virtual Memory. Suitable for hosting up to 400 concurrent sessions.
`Large`	Deploys an appliance with 4 CPUs, 6 GB of memory, 10 GB of disk space, and 3 GB of Java Virtual Memory. Suitable for hosting up to 800 concurrent sessions.

Procedure

1 Create a vCloud Availability Administration Portal host by running the following command.

Important The `--deployment-type` argument in the following command defines the compute resources that you allocate to the vCloud Availability Administration Portal host. By default, the value is `small`. You can change the value depending on your requirements.

Standard Command

```
# vcav vcd-ui create \
--ovf-url=vcloud-availability-release_number-
xxx-build_number_OVF10.ova \
--deployment-type=small \
--vsphere-address=$MGMT_VSPHERE_ADDRESS \
--vsphere-user=$MGMT_VSPHERE_USER \
--vsphere-password-file=~/.ssh/.vsphere.mgmt \
"--network=$MGMT_VSPHERE_NETWORK" \
"--vsphere-locator=$MGMT_VSPHERE_LOCATOR" \
--datastore=$MGMT_VSPHERE_DATASTORE \
--ntp=pool.ntp.org \
--root-password-file=~/.ssh/.root \
--vm-name=ui02-name
```

Command Using Registry

```
# vcav vcd-ui create \
--ovf-url=vcloud-availability-release_number-
xxx-build_number_OVF10.ova \
--deployment-type=small \
--vsphere=mgmt-vsphere-name \
--ntp=pool.ntp.org \
--root-password-file=~/.ssh/.root \
--vm-name=ui02-name
```

The IP address of the new vCloud Availability Administration Portal virtual machine is displayed. Write it down because you need it during the configuration.

2 Set a variable to the address of the created virtual machine.

Standard Command

```
# UI02_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=ui02-name`
```

Command Using Registry

```
# UI02_ADDRESS=`vcav vsphere get-ip \
--vsphere=mgmt-vsphere-name \
"--network=mgmt-network" \
--vm-name=ui02-name`
```

3 Update the `truststore` file with the vCloud Availability Administration Portal virtual machine credentials.

```
# echo 'SMP-Portal-VM-Password' > ~/.ssh/.truststore

# chmod 0600 ~/.ssh/.truststore
```

4 If you use Fully Qualified Domain Names (FQDN) to access and manage appliances, you must verify that the DNS record matches the vCloud Availability Administration Portal IP address, and trusts the SSH certificate for this FQDN.

   a Check the DNS server to ensure that the entry matches the IP address of the vCloud Availability Administration Portal host.

   b Run the `trust-ssh` command to trust the certificate for the vCloud Availability Administration Portal FQDN.

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 \`
`--root-password-file=~/.ssh/.root \`
`--vm-name=ui02-name \`
`--vm-address=ui02-FQDN`
	`# vcav vsphere trust-ssh \`
	`--vsphere=mgmt-vsphere-name \`
	`--root-password-file=~/.ssh/.root \`
	`--vm-name=ui02-name \`
	`--vm-address=ui02-FQDN`

Validate Deployment

Before you configure vCloud Availability, you must confirm that all appliances are ready to be configured.

Procedure

- Verify that all components are ready for configuration.

Standard Command	Command Using Registry

`# vcav vcd wait-for-api \`
`--vcd-address=$VCD_ADDRESS \`
`--vcd-user=$VCD_USER \`
`--vcd-password-file=~/.ssh/.vcd \`
`--timeout=300`
 	
`# vcav vcd is-federation-enabled \`
`--vcd-address=$VCD_ADDRESS \`
`--vcd-user=$VCD_USER \`
`--vcd-password-file=~/.ssh/.vcd`
	`# vcav vcd wait-for-api \`
	`--vcd=vcd-01-name \`
	`--timeout=300`
	
	`# vcav vcd is-federation-enabled \`
	`--vcd=vcd-01-name`

Configuring vCloud Availability for vCloud Director

After you deploy all individual components of vCloud Availability, you must configure them to support DRaaS.

Procedure

1 Configure vSphere Replication Manager

   Each vSphere Replication Manager must be registered to a single vCenter Server.

2 Configure Cassandra Servers

Update each Cassandra server to trust every vSphere Replication Cloud Service appliance and register each Cassandra server with the lookup service used by vCloud Director.

3 Configure vSphere Replication Cloud Service

To configure the vSphere Replication Cloud Service host, you must register each vSphere Replication Cloud Service appliance to your vCloud Director appliance, resource vCenter Server, and RabbitMQ.

4 Configure vSphere Replication Server

Attach each vSphere Replication Server to your vSphere Replication Manager and vCenter Server.

5 Configure vCloud Availability Portal Host

6 Configure vCloud Availability Administration Portal Host

You must configure the vCloud Availability Administration Portal host with both the vCloud Director server and the embedded MongoDB server, and start the system services.

7 Configure Service Provider vCloud Director Organizations

Each Organization VDC must be enabled for replication, before configuring tenant environment.

Configure vSphere Replication Manager

Each vSphere Replication Manager must be registered to a single vCenter Server.

Procedure

1 Configure the vSphere Replication Manager.

Standard Command	Command Using Registry

`# vcav hms configure \`
`--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`
	`# vcav hms configure \`
	`--hms-address=$HMS01_ADDRESS \`
	`--vsphere=vsphere-01-name \`
	`--vcd=vcd-01-name`

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

2 Run the following command to verify that the `hms` service starts successfully.

Standard Command	Command Using Registry

`# 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`
	`# 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 for errors.

Important Repeat these steps for every vSphere Replication Manager that you deployed.

Configure Cassandra Servers

Update each Cassandra server to trust every vSphere Replication Cloud Service appliance and register each Cassandra server with the lookup service used by vCloud Director.

Note The current procedure pertains to configuring Cassandra servers for production deployments. If you use a Docker container to manage your Cassandra servers in test and development environments, perform the steps documented in Create Containers for Test and Development Environments.

Procedure

1 Create a password file for the Cassandra host *root* user in `/.ssh/cassandra.root.password`.

2 Create a trusted connection between the vCloud Availability Installer Appliance and your Cassandra hosts. This connection allows the vCloud Availability Installer Appliance to trust the Cassandra certificate and is required before you can add the Cassandra hosts to the lookup service used by vCloud Director.

Repeat this step for every Cassandra host in your environment.

```
# vcav trust add-ssh --address=$CASSANDRA_ADDRESS --root-password-
file=/.ssh/cassandra.root.password --accept-all
```

3 Add the vSphere Replication Cloud Service certificate to the Cassandra truststore, so that the Cassandra host accepts SSL connections from the vSphere Replication Cloud Service.

The Cassandra truststore stores the certificates that are accepted for connection. The Cassandra keystore only stores the certificate that the Cassandra server publishes.

Run the following command on every Cassandra server before you finish the vCloud Availability configuration. Run the commands 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`*.

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

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

Configure vSphere Replication Cloud Service

To configure the vSphere Replication Cloud Service host, you must register each vSphere Replication Cloud Service appliance to your vCloud Director appliance, resource vCenter Server, and RabbitMQ.

Important If you have more than one vCloud Director instance configured in your vCenter Server lookup service, the vSphere Replication Cloud Service VM registers to the first vCloud Director instance in the lookup service.

Procedure

1 Configure the vSphere Replication Cloud Service Appliance.

The `cassandra-replication-factor` argument in the following command defines the number of data replicas across the Cassandra cluster. A replication factor 4 means that there are four copies of each row, where each copy is on a different node. The replication factor must not exceed the number of nodes in the Cassandra cluster.

By default, the following command uses the AMQP settings from vCloud Director. If vCloud Director is not using an SSL port for AMQP, the `vcav hcs configure` operation returns an error. You can add the `--amqp-port=`*`port-number`* argument to override the vCloud Director port and point the AMQP service to an SSL port.

Standard Command	Command Using Registry

`# vcav hcs configure \`
`--hcs-address=$HCS01_ADDRESS \`
`--amqp-password-file=~/.ssh/.amqp \`
`--cassandra-replication-factor=number-of-Cassandra-nodes \`
`--vcd-address=$VCD_ADDRESS \`
`--vcd-user=$VCD_USER \`
`--vcd-password-file=~/.ssh/.vcd \`
`--sso-user=$SSO_USER \`
`--sso-password-file=~/.ssh/.sso`
	`# vcav hcs configure \`
	`--hcs-address=$HCS01_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.

2 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=$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 for errors.

3 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.

Configure vSphere Replication Server

Attach each vSphere Replication Server to your vSphere Replication Manager and vCenter Server.

Procedure

1 Configure your vSphere Replication Server.

Standard Command	Command Using Registry

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

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

Important Repeat this step for every vSphere Replication Server in your environment.

2 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.

Configure vCloud Availability Portal Host

Procedure

1 Configure the vCloud Availability Portal host by running the following command.

In the following example, the vCloud Availability Portal is configured to operate with a new generated self-signed SSL certificate. You can set up the vCloud Availability Portal to use an externally signed SSL certificate, by replacing the `--keep-self-signed-certificate` argument with `--https-certificate=/file-path-to-certificate-file` and `--https-key=/file-path-to-certificate-public-key`. The vCloud Availability Portal appliance provides the certificate and key files to an `nginx` process.

Standard Command	Command Using Registry

`# vcav vcd-ui configure \`
`--ui-address=$UI01_ADDRESS \`
`--keep-self-signed-certificate \`
`--truststore-password-file=~/.ssh/.truststore \`
`--vcd-address=$VCD_ADDRESS \`
`--vcd-user=$VCD_USER \`
`--vcd-password-file=~/.ssh/.vcd \`
`--sso-user=administrator@vsphere.local \`
`--sso-password-file=~/.ssh/.sso`
	`# vcav vcd-ui configure \`
	`--ui-address=$UI01_ADDRESS \`
	`--keep-self-signed-certificate \`
	`--truststore-password-file=~/.ssh/.truststore \`
	`--vcd=vcd-01-name`

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

2 You allocate small, medium, and large sizes of Java Virtual Memory (JVM) to the vCloud Availability Portal service process during the host deployment. Only for medium and large deployments with vCloud Availability versions earlier than 1.0.1.2, you must complete steps Step 2d and Step 2g, so that the service process can start successfully after configuration. In other cases, you can optionally update the allocated JVM by completing the following steps. For more information about the vCloud Availability Portal deployment types and related JVM configuration, see Create vCloud Availability Portal Host.

a Use SSH to connect to the vCloud Availability Portal host.

b Use a text editor to open the `/opt/vmware/conf/vcav-ui/nginx/nginx.conf` file.

c The initial size of the memory allocation pool is defined in the following line. Change the numeric value to designate more JVM to the vCloud Availability Portal host.

```
jvm_options "-Xms1024m";
```

d The following line defines the maximum size of memory allocation pool for the `nginx` process. The numeric value must be equal to or greater than the numeric value you defined in the previous step.

Important This step required for medium and large vCloud Availability Portal deployments.

```
jvm_options "-Xmx1024m";
```

e You can optionally uncomment the following lines to enable JVM heap dump and define the heap dump file path.

```
jvm_options "-XX:+HeapDumpOnOutOfMemoryError";
jvm_options "-XX:HeapDumpPath=/opt/vmware/logs/vcav-ui/jvm.hprof";
```

f By default, the maximum number of concurrent client sessions is set to 1024. To increase this number, use a text editor to open the `/usr/lib/systemd/system/vcav-ui.service` and add the following line after the `[Service]` line.

```
LimitNOFILE=8192
```

g Restart the vCloud Availability Portal service to complete this configuration, by running the following command.

Important This step required for medium and large vCloud Availability Portal deployments.

```
systemctl restart vcav-ui
```

3 Configure the timeout settings for the vCloud Availability Portal host.

a Use a text editor to open the `opt/vmware/conf/vcav-ui/config.yml` file.

b Set the *connectTimeout* value to 60000 and the *socketTimeout* value to 60000.

4 Configure the `nginx` process to run for a `non-root` user.

The vCloud Availability Portal host `nginx` process runs under the system `root` user by default. You can change the user that the `nginx` process uses by modifying the vCloud Availability Portal service script. If you do not want to edit the `nginx` process user, you can skip this step.

a Use SSH to connect to the vCloud Availability Portal host as `root`.

b Stop the vCloud Availability Portal service by running the following command.

```
# systemctl stop vcav-ui
```

c Use a text editor to modify the `/usr/lib/systemd/system/vcav-ui.service` file, by adding `User=new-user-name` line after the `[Service]` line.

d Change the line that provides the `PID` file location to read `PIDFile=/opt/vmware/logs/vcav-ui/vcav-ui.pid`.

e Using a text editor open the `/opt/vmware/conf/vcav-ui/nginx/nginx.conf` and change the line that provides the `PID` file location to read `pid /opt/vmware/logs/vcav-ui/vcav-ui.pid`.

f Change the ownership of the log files that the service uses by running the following commands.

```
# chown -R new-user-name /opt/vmware/logs/vcav-ui

# chown -R new-user-name /opt/vmware/vcav-ui/logs
```

g Start the vCloud Availability Portal service by running the following command.

```
# systemctl start vcav-ui
```

5 Assign a domain name to your vCloud Availability Portal host.

It is a best practice to assign a domain name to your vCloud Availability Portal VM for production deployments.

6 Verify that the vCloud Availability Portal is configured correctly, by running the following command.

```
'curl –k https://$UI01_ADDREESS:8443/
```

Configure vCloud Availability Administration Portal Host

You must configure the vCloud Availability Administration Portal host with both the vCloud Director server and the embedded MongoDB server, and start the system services.

Procedure

1 To configure vCloud Availability Administration Portal, run the following command.

Standard Command

```
# vcav vcd-ui configure-smp \
--ui-address=$UI02_ADDRESS \
--keep-self-signed-certificate \
--truststore-password-file=~/.ssh/.truststore \
--vcd-address=$VCD_ADDRESS \
--vcd-user=$VCD_USER \
--vcd-password-file=~/.ssh/.vcd \
--sso-user=administrator@vsphere.local \
--sso-password-file=~/.ssh/.sso \
--mongodb-password-file=~/.ssh/.root \
--amqp-user= $AMQP_USER \
--amqp-password-file= ~/.ssh/.amqp \
--tenant-ui-url= tenant-ui-url \
--max-jvm-memory=1024
```

Command Using Registry

```
# vcav vcd-ui configure-smp \
--ui-address=$UI02_ADDRESS \
--keep-self-signed-certificate \
--truststore-password-file=~/.ssh/.truststore \
--vcd=vcd-01-name \
--mongodb-password-file=~/.ssh/.root \
--amqp-user= $AMQP_USER \
--amqp-password-file= ~/.ssh/.amqp \
--tenant-ui-url=tenant-ui-url \
--max-jvm-memory=1024
```

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

Important To enable tenant impersonation, you must set `--tenant-ui-url` argument value to the base URL of the tenant vCloud Availability Portal.

The `--amqp-user` and `--amqp-password-file` argument values are mandatory.

In the example, the vCloud Availability Administration Portal is configured to operate with a new generated self-signed SSL certificate. You can set up the vCloud Availability Administration Portal to use an externally signed SSL certificate, by replacing the `--keep-self-signed-certificate` argument with `--https-certificate=/file-path-to-certificate-file` and `--https-key=/file-path-to-certificate-public-key`. The vCloud Availability Administration Portal appliance provides the certificate and key files to a *java* process.

2 Assign a domain name to your vCloud Availability Administration Portal host. It is a best practice to assign a domain name to your vCloud Availability Administration Portal host for production deployments.

3 Verify that the vCloud Availability Administration Portal is configured correctly, by running the following command.

```
curl –k https://$UI02_ADDRESS:8443/
```

Configure Service Provider vCloud Director Organizations

Each Organization VDC must be enabled for replication, before configuring tenant environment.

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 Configure vSphere Replication Cloud Service.

Procedure

- Enable Organization VDC for replication using the vCloud Availability Installer Appliance.

Standard Command

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

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

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

Command Using Registry

```
# vcav org list \
--vcd=vcd-01-name

# vcav org-vdc list \
--vcd=vcd-01-name \
--org=org1

# vcav org-vdc enable-replication \
--vcd=vcd-01-name \
--org=org1 \
--vdc=vdc_org1
```

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

Tenant Installation and Configuration

5

Client configuration relies on the configuration of vSphere Replication within the tenant environment

1 Prepare Your Environment to Install vSphere Replication

   Before you deploy the vSphere Replication appliance, you must prepare the environment.

2 Deploy the vSphere Replication Virtual Appliance

   vSphere Replication is distributed as an OVF virtual appliance.

3 Register the vSphere Replication Appliance with vCenter Single Sign-On

   You must register the vSphere Replication Management Server with vCenter Single Sign-On on both the source and the target sites.

4 Using a Self-Signed Certificate in a Development Environment

   By using a self-signed certificate in the tenant configuration, you ensure security and encryption for tenant deployments.

5 Configure Cloud Provider

   You configure the Cloud Provider to assign the correct service provider destination for replication.

6 Replicating Virtual Machines to Cloud

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

7 Configuring Replications from Cloud

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

8 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.

Prepare Your Environment to Install vSphere Replication

Before you deploy the vSphere Replication appliance, you must prepare the environment.

Procedure

1 Verify that you have vSphere and vSphere Web Client installations for the source and target sites.

2 In the vSphere Web Client, select the vCenter Server instance on which you are deploying vSphere Replication, click **Configure > Settings > Advanced Settings**, and verify that the `VirtualCenter.FQDN` value is set to a fully-qualified domain name or a literal address.

Note vSphere Replication can be deployed with either IPv4 or IPv6 address. Mixing IP addresses, for example having a single appliance with an IPv4 and an IPv6 address, is not supported. To register as an extension, vSphere Replication relies on the `VirtualCenter.FQDN` property of the vCenter Server. When an IPv6 address is used for vSphere Replication, the `VirtualCenter.FQDN` property must be set to a fully qualified domain name that can be resolved to an IPv6 address or to a literal address. When operating with an IPv6 address, vSphere Replication requires that all components in the environment, such as vCenter Server and ESXi hosts are accessible using the IPv6 address.

What to do next

You can deploy the vSphere Replication appliance.

Deploy the vSphere Replication Virtual Appliance

vSphere Replication is distributed as an OVF virtual appliance.

You deploy the vSphere Replication appliance by using the standard vSphere OVF deployment wizard.

Note vSphere Replication can be deployed with either IPv4 or IPv6 address. Mixing IP addresses, for example having a single appliance with an IPv4 and an IPv6 address, is not supported. To register as an extension, vSphere Replication relies on the `VirtualCenter.FQDN` property of the vCenter Server. When an IPv6 address is used for vSphere Replication, the `VirtualCenter.FQDN` property must be set to a fully qualified domain name that can be resolved to an IPv6 address or to a literal address. When operating with an IPv6 address, vSphere Replication requires that all components in the environment, such as vCenter Server and ESXi hosts are accessible using the IPv6 address.

Prerequisites

Download the vSphere Replication ISO image and mount it on a system in your environment.

Procedure

1 Log in to the vSphere Web Client on the source site.

2 Select **vCenter > Hosts and Clusters**.

3 Right-click a host and select **Deploy OVF template**.

4 Provide the location of the OVF file from which to deploy the vSphere Replication appliance, and click **Next**.

   - Select **URL** and provide the URL to deploy the appliance from an online URL.
   - If you downloaded and mounted the vSphere Replication ISO image on a system in your environment, select **Local file > Browse** and navigate to the `\bin` directory in the ISO image, and select the `vSphere_Replication_OVF10.ovf`, `vSphere_Replication-system.vmdk`, and `vSphere_Replication-support.vmdk` files.

5 Review the virtual appliance details and click **Next**.

6 Accept the end user license agreements (EULA) and click **Next**.

7 Accept the name, select or search for a destination folder or datacenter for the virtual appliance, and click **Next**.

   You can enter a new name for the virtual appliance. The name must be unique within each vCenter Server virtual machine folder.

8 Select the number of vCPUs for the virtual appliance and click **Next**.

   Note Selecting higher number of vCPUs ensures better performance of the vSphere Replication Management Server, but might slow down the replications that run on ESXi host systems that have 4 or less cores per NUMA node. If you are unsure what the hosts in your environment are, select 2 vCPUs.

9 Select a cluster, host, or resource pool where you want to run the deployed template, and click **Next**.

10 Select a destination datastore and disk format for the virtual appliance and click **Next**.

11 Select a network from the list of available networks, set the IP protocol and IP allocation, and click **Next**.

   vSphere Replication supports both DHCP and static IP addresses. You can also change network settings by using the virtual appliance management interface (VAMI) after installation.

12 Set the password for the root account for the customized template, and click **Next**.

   The password must be at least eight characters long.

13 Review the binding to the vCenter Extension vService and click **Next**.

14 Review the settings and click **Finish**.

   The vSphere Replication appliance is deployed.

15 Power on the vSphere Replication appliance. Take a note of the IP address of the appliance and log out of the vSphere Web Client.

16 Repeat the procedure to deploy vSphere Replication on the target site.

What to do next

Register the vSphere Replication appliance with the SSO service.

Register the vSphere Replication Appliance with vCenter Single Sign-On

You must register the vSphere Replication Management Server with vCenter Single Sign-On on both the source and the target sites.

After you deploy the vSphere Replication appliance, you use the Virtual Appliance Management Interface (VAMI) to register the endpoint and the certificate of the vSphere Replication Management Server with the vCenter Lookup Service, and to register the vSphere Replication solution user with the vCenter Single Sign-On administration server.

If you do not register vSphere Replication with vCenter Single Sign-On on the target site, vSphere Replication cannot operate as expected. In addition, storage DRS does not detect the replicated data that vSphere Replication stores on the target site and might destroy it.

Prerequisites

- Verify that the vSphere Replication appliance is powered on.
- Verify that you have administrator privileges to configure the vSphere Replication appliance.
- Verify that the vSphere Replication management server is synchronized with the time of the Single Sign-On server.

Procedure

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

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

   You configured the root password during the OVF deployment of the vSphere Replication appliance.
3. Click the **Configuration** tab.
4. In the **LookupService Address** text box, enter the IP address or domain name of the server where the lookup service runs.
5. Enter the credentials of a user with administrator privileges to vCenter Single Sign-On.
6. Click **Save and Restart Service**.
7. Repeat the procedure to register vSphere Replication on the target site.

vSphere Replication appears on the **Home** tab in the vSphere Web Client.

What to do next

Note If you registered the vSphere Replication appliance with SSO as part of the upgrade procedure, all existing connections will turn into `Connection issue` status. See Reconnect to a Remote Site.

If you competed this procedure as part of the installation process, you can configure connections between the source and target sites.

Perform optional reconfiguration of the vSphere Replication appliance by using the VAMI. You can install a certificate, change the appliance root password, change the trust policy, or configure vSphere Replication to use an external database.

States of vSphere Replication Displayed in the vSphere Web Client

Before you can start using vSphere Replication, you must register the vSphere Replication appliance with the vCenter Lookup Service and the Single Sign-On administration server in the environment.

In the vSphere Web Client, on the vSphere Replication **Home** tab, you can check the list of vCenter Server instances in the Single-Sing On domain, and the status of vSphere Replication on each vCenter Server instance.

The following table lists the vSphere Replication states that you can observe, their meanings, and what you can do to change a state back to normal.

Table 5-1. vSphere Replication States on vCenter Server Instances

Status	Description	Remediation
Not installed	The vSphere Replication extension is not registered in the vCenter Server Extension Manager. The vSphere Replication appliance is either not deployed or the vSphere Replication extension has been deleted from the vCenter Server Extension Manager.	If a vSphere Replication appliance is deployed on this vCenter Server, restart the appliance or the vSphere Replication Management service on the appliance. 1 Use a supported browser to log in to the vSphere Replication VAMI as the root user. The URL for the VAMI is https://*vr-appliance-address*:5480. 2 On the **Configuration** tab, click **Save and Restart Service**.
Enabled (Configuration issue)	A configuration error occurred. The vSphere Replication Management Server is either not registered with the vCenter SSO components, or the configuration is incorrect and must be updated. You cannot manage existing replications, or configure new replications to this server .	Configure the vSphere Replication appliance. 1 Select the row that indicates the `Enabled (Configuration issue)` status. 2 Point to the `Enabled (Configuration issue)` status. The detailed error message appears in a tooltip. 3 Click the **Configure** icon ( ) above the list of vCenter Server instances. The vSphere Replication VAMI opens. 4 On the **Configuration** tab, enter the parameters that were indicated in the error message and click **Save and Restart Service** .

Table 5-1. vSphere Replication States on vCenter Server Instances (Continued)

Status	Description	Remediation
Enabled (Not accessible)	The vSphere Replication Management Server is not accessible. The vSphere Replication extension is registered in the vCenter Server Extension Manager, but the vSphere Replication appliance is missing or powered off, or the vSphere Replication Management service is not running. You cannot manage existing replications, or configure new replications to this server .	■ Verify that the vSphere Replication appliance exists on the vCenter Server. ■ Verify that the vSphere Replication appliance is powered on. ■ Restart the VRM service. a On the vSphere Replication **Home** tab, select the row that indicates the `Enabled (Not accessible)` status and click the **Configure** icon ( ) above the list of replication servers. b On the **Configuration** tab, restart the VRM service.
Enabled (OK)	The vSphere Replication appliance is installed, configured, and functioning properly.	Not needed.

Using a Self-Signed Certificate in a Development Environment

By using a self-signed certificate in the tenant configuration, you ensure security and encryption for tenant deployments.

If the service provider vCloud Director instances use a self-signed certificate, you must update the tenant vSphere Replication appliances to trust the self-signed certificate, by completing the following steps.

Note The following procedure contains long, single commands that should be run as one. There are breaks in the command for better visibility marked with "\". "#" marks the beginning of a new command.

Procedure

1 Copy the self-signed certificate to the client vSphere Replication Appliance and load it into the `keystore`.

   a Log in to vSphere Replication Appliance using the remote console

   b Export the vCloud Director certificate and import it into the Java `keystore`:

```
# openssl s_client –connect $VCD_IP:443 –tls1 </dev/null 2>/dev/null \
| openssl x509 > /tmp/vcloud.pem

# /usr/java/default/bin/keytool –noprompt \
–import –trustcacerts –alias vcloud –file /tmp/vcloud.pem \
–keystore /usr/java/default/lib/security/cacerts –storepass changeit
```

   Note Keytools may be located on a different folder depending on the vSphere Replication release.

2 Restart the services that use the keystore file by running the following commands.

```
# service hms restart

# service vmware–vcd restart
```

Configure Cloud Provider

You configure the Cloud Provider to assign the correct service provider destination for replication.

Prerequisites

Open the vCenter Server administration interface.

Procedure

1 Open the vCenter Server by using the Web Client.

2 Navigate to the **Connect to a Cloud Provider** tab.

3 In the **Manage** tab, click **`vSphere Replication`**.

4 Click **Target Sites** and click the **Connect to Cloud Provider** icon.

5 **Connect to Cloud Provider**.

   a Enter the Cloud Provider Address: `vcd.provider.com` without the `/cloud` suffix

   b Enter the Organization Name.

   c Enter user name and password. The user profile must be assigned with Replication Rights.

6 After you configure the Cloud Provider, right-click and select **Configure Target Networks**.

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 the vSphere Replication 5.8 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 Compatibility Matrixes for vSphere Replication 6.5 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 vCloud Air 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.

vCloud Availability Administration Portal Overview

6

The vCloud Availability Administration Portal provides a graphic user interface to facilitate the service providers to monitor and manage the vCloud Availability solution.

The service providers can use the vCloud Availability Administration Portal as a dashboard providing information about replications, and as a tool to clean up stale replications and migrate replications from one datastore to another.

By using the impersonation feature, the service providers can pose as tenants and perform all DR tasks in the tenant vCloud Availability Portal.

Working with the vCloud Availability Administration Portal

With vCloud Availability Administration 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 Administration Portal

You log in to the vCloud Availability Administration Portal only as a vCloud Director system administrator.

Procedure

1. Enter the URL of the vCloud Availability Administration Portal into a Web browser.

   `https://UI02_ADDRESS:8443`

2. Log in to the vCloud Availability Administration Portal with your vCloud Director system administrator credentials.

   Note You receive an error message if you try to log in to the vCloud Availability Administration 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 Administration 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 Administration 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 Administration 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 Administration 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 Administration 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 Administration Portal.

Procedure

1. Log in to the vCloud Availability Administration 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 Administration 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 Administration 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 Portal.

   For more information about working with the vCloud Availability Portal, see Working with the vCloud Availability Portal.

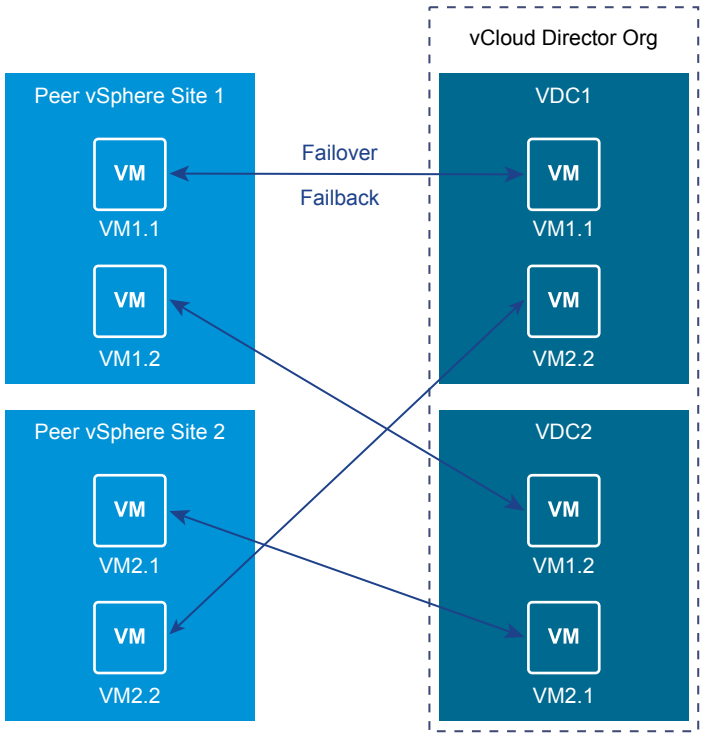
vCloud Availability Portal Overview

7

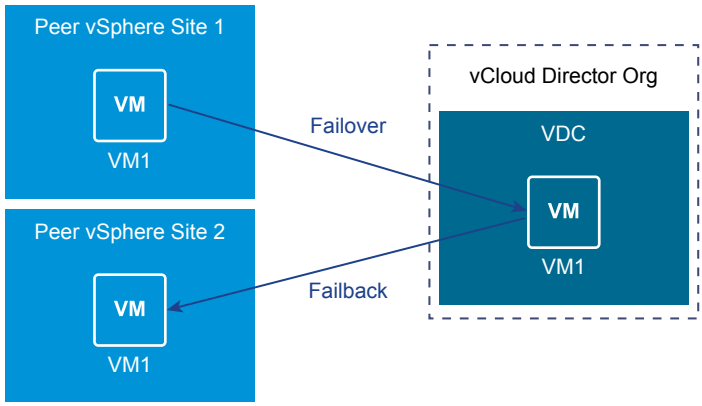
The vCloud Availability Portal provides tenants with a graphic user interface to facilitate the management of the vCloud Availability solution.

The vCloud Availability Portal uses vCloud Availability Installer Appliance and vCloud Director APIs to perform common vCloud Availability tasks. The vCloud Availability Portal also provides overall system and workload information.

The first step in the disaster recovery workflow is protecting the VMs from your vSphere (on-premise) environment into your vCloud Director (cloud) environment. You can replicate the protected VMs from multiple vSphere (on-premise) environments to multiple vCloud Director VDC instances, and the reverse. The following diagram illustrates the replication topology for the use case.



You can fail over a virtual machine from one vSphere (on-premise) environment to a vCloud Director (cloud) site and failback the same virtual machine to a different peer vSphere (on-premise) environment. After a successful failover, you detach the workload by using the vCloud Availability Portal, and attach the virtual machine to the second peer vSphere (on-premise) environment. The following diagram illustrates the replication topology for the use case.



Working with the vCloud Availability Portal

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

Monitoring vCloud Availability Processes

You can monitor the overall vCloud Availability status by using the vCloud Availability 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 Tasks

By using the **Workspaces page**, you can perform the following vCloud Availability 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 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 Portal

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

- vCloud Availability 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 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 Portal

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

- vCloud Availability 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 Portal.

- Unprotect a Virtual Machine Using the vCloud Availability Portal

  You can remove a VM from the vCloud Availability solution by running an Unprotect task.

- Detach a Virtual Machine Using the vCloud Availability Portal

  You can remove a VM from the vCloud Availability solution by running a Detach task.

- Configure Replication from Cloud to a Second vCenter Server

  You can use the vCloud Availability solution to support a replication from a vCloud Director site to a second vCenter Server.

Log in to vCloud Availability Portal

Tenant Organization administrator users can log in to the vCloud Availability 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 Portal into a Web browser, for example `https://$UI01_ADDRESS:8443`.
2. Use *username@Org-Name* to log in to the vCloud Availability Portal.

vCloud Availability 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 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 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 Portal

  You can run vCloud Availability Portal operations to a protected workload only after the results of its previous test are cleaned up.

Test Failover Using the vCloud Availability 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 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 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 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 Portal

You can run vCloud Availability 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 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 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 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 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 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 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 Portal

  Synchronize workload data from vCloud Director (cloud) to vSphere (on-premise) site.
- Perform a Failback Reverse Task Using the vCloud Availability Portal

  Synchronize VM data from vSphere (on-prem) to vCloud Director (cloud) site.

Perform a Failover Reverse Task Using the vCloud Availability Portal

Synchronize workload data from vCloud Director (cloud) to vSphere (on-premise) site.

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 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 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 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 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 Portal

You can remove a VM from the vCloud Availability 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 solution is protected.

- Force Stop the replication of the VM in your vSphere (on-prem) environment. For more information, see Stop Replicating a Virtual Machine in the *VMware vSphere Replication Administration Guide*.

Procedure

1. Log in to the vCloud Availability 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 solution and disappears from the VM lists in the vCloud Availability Portal upon task completion.

Detach a Virtual Machine Using the vCloud Availability Portal

You can remove a VM from the vCloud Availability 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 solution is protected.

Procedure

1. Log in to the vCloud Availability 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 solution and disappears from the VM lists in the vCloud Availability Portal upon task completion.

Configure Replication from Cloud to a Second vCenter Server

You can use the vCloud Availability 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 Chapter 7 vCloud Availability Portal Overview.

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 Portal. For more information, seePerform a Failover Task Using the vCloud Availability Portal .
- Verify that the virtual machine is detached and does not appear in the **Workloads** tab of the vCloud Availability Portal. You can detach a workload by running a **Detach** task in the vCloud Availability Portal. For more information about detaching workloads through the vCloud Availability Portal, see Detach a Virtual Machine Using the vCloud Availability 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 Portal.

The virtual machine is running in the vCloud Director (cloud) site and is protected on the second vCenter Server (on-premise) site.

Upgrading vCloud Availability

8

You upgrade vCloud Availability by installing and configuring a vCloud Availability Installer Appliance and vCloud Availability Portal host, and connecting the remaining vCloud Availability appliances that are already installed and configured in your environment.

1 Deploy vCloud Availability Installer Appliance

   To upgrade to vCloud Availability 1.0.1, you must first install and configure the vCloud Availability Installer Appliance.

2 Prepare the vCloud Availability Installer Appliance for Upgrading to vCloud Availability 1.0.1

   You can simplify the deployment of individual components by defining installation variables or by creating a registry file on your vCloud Availability Installer Appliance.

3 Add Trusted Thumbprints to the vCloud Availability Installer Appliance

   The vCloud Availability Installer Appliance must be able to verify the thumbprint of the vCenter Server and vCloud Director hosts that it works with.

4 Connect to vCloud Availability Appliances

   Establish a trusted connection between the vCloud Availability Installer Appliance and the remaining vCloud Availability components.

5 Create vCloud Availability Portal Host

   The vCloud Availability Portal provides a graphic user interface to facilitate the management of vCloud Availability operations.

6 Configure vCloud Availability Portal Host

Deploy vCloud Availability Installer Appliance

To upgrade to vCloud Availability 1.0.1, you must first install and configure the vCloud Availability Installer Appliance.

This procedure demonstrates how to deploy and configure a vCloud Availability Installer Appliance by using the VMware OVF Tool. Alternatively, you can use the vSphere Web Client to install the vCloud Availability Installer Appliance.

The vCloud Availability Installer Appliance is deployed as an OVA file and includes the following components:

- vCloud Availability scripts for installation and maintenance operations
- SLES 12 SP1 image to provide Docker container hosting

You run all installation and configuration commands from the vCloud Availability Installer Appliance, unless documentation instructs otherwise.

Installation and configuration procedures contain long, single commands that should be run as one. There are breaks for better visibility marked with backslash (\). The beginning of a new command is marked with the number sign (#).

Procedure

1 Download the vCloud Availability Installer Appliance.

   a In a Web browser, navigate to the download page.

   b Download the `vcloud-availability-release_number-xxx-build_number_OVF10.ova` file.

2 Define deployment variables.

   The *VSPHERE_LOCATOR* value contains the target data center name, the tag *host*, the name of the target cluster, and the IP address or the fully qualified domain name (FQDN) of the target ESXi host. The *VSPHERE_LOCATOR* value depends on the topology of your vSphere environment. Following are examples for valid *VSPHERE_LOCATOR* values.

   - /*data-center-name*/host/*cluster-1-name*/*fully-qualified-domain-name*
   - /*data-center-name*/host/*cluster-2-name*/*host-IP-address*

   If the target ESXi host is not part of a cluster, skip the *cluster-name* element, as shown in the following examples.

   - /*data-center-name*/host/*fully-qualified-domain-name*
   - /*data-center-name*/host/*host-IP-address*

   The *VSPHERE_DATASTORE* value is the datastore name as it is displayed in the vSphere Web Client.

   For more information about the *VSPHERE_LOCATOR* and *VSPHERE_DATASTORE* values, see *Specifying the Inventory Path for a Cluster, Host, or Resource Pool* in the OVF Tool User's Guide.

```
# OVA_VM_NAME=vcav-installer-name

# VSPHERE_LOCATOR="vsphere-locator"

# VSPHERE_DATASTORE="vsphere-datastore"

# VSPHERE_ADDRESS=vsphere-ip-address

# VSPHERE_USER=vsphere-admin-user
```

```
# VSPHERE_NETWORK="VM-Network"

# OVA=local_client_path/vcloud-availability-installer-appliance-1.0.1.1-xxx-build_number.ova

# ROOT_PASSWORD=vcloud-availability-installer-appliance-root-password
```

3 Deploy vCloud Availability Installer Appliance OVA.

Note Password authentication is the default method for deploying the vCloud Availability Installer Appliance. You can deploy the appliance using SSH key authentication by adding the "--prop:guestinfo.cis.appliance.root.sshkey=${SSH_KEY}" argument in the installation command. You also must have a valid SSH public key to deploy vCloud Availability Installer Appliance using SSH key authentication method.

The following is a long, single command that should be run as one. There are breaks for better visibility marked with backslash (\).

```
# ovftool \
--acceptAllEulas \
--skipManifestCheck \
--X:injectOvfEnv \
--allowExtraConfig \
--X:enableHiddenProperties \
--sourceType=OVA \
--allowAllExtraConfig \
--powerOn \
--X:waitForIp \
"--net:VM Network=${VSPHERE_NETWORK}" \
--diskMode=thin \
--datastore=${VSPHERE_DATASTORE} \
--name=${OVA_VM_NAME} \
--prop:guestinfo.cis.appliance.net.pnid=${OVA_VM_NAME} \
--prop:guestinfo.cis.appliance.ssh.enabled=True \
"--prop:guestinfo.cis.appliance.root.password=${ROOT_PASSWORD}" \
${OVA} \
"vi://${VSPHERE_USER}@${VSPHERE_ADDRESS}${VSPHERE_LOCATOR}"
```

The system prints the IP address of the vCloud Availability Installer Appliance. Write down the IP address, because you are going to use it during the installation.

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

```
# ssh root@vCloud-Availability-Installer-Appliance-IP-Address
```

Working with the vCloud Availability Installer Appliance

You can use vCloud Availability Installer Appliance scripts to install, configure, and manage the vCloud Availability.

vCloud Availability Installer Appliance Basic Operations

You must create an SSH connection to the vCloud Availability Installer Appliance, to use the available scripts.

You must run vCloud Availability Installer Appliance commands from the **root** user's home directory of your vCloud Availability Installer Appliance.

The vCloud Availability Installer Appliance uses the following command-line syntax logic.`vcav [OPTIONS] COMMAND SUBCOMMAND [ARGUMENT]`

All arguments that end with an equals sign (=) require a value.

Asterisk (*) marks required arguments for a command.

If you are using a registry file to work with the vCloud Availability Installer Appliance, you can replace the `--vsphere-address`, `--vsphere-user`, and `--vsphere-password-file` options with the `--vsphere=`*`vsphere-name`* argument.

If you are using a registry file to work with the vCloud Availability Installer Appliance, you can replace the `--vcd-address`, `--vcd-user`, and `--vcd-password-file` options with `--vcd=`*`vcd-name`* . For more information about the registry file that the vCloud Availability Installer Appliance uses, see Prepare the vCloud Availability Installer Appliance for vCloud Availability Installation.

You can see the basic vCloud Availability Installer Appliance options and arguments in the following table.

Table 8-1. Basic vCloud Availability Installer Appliance Options and Arguments

Option	Argument	Description
`--help (-h)`	None	Displays a summary of options and arguments.
`--session-dir=`	File path	Define the location to store files and create a registry file.
`--log-level=`	`Error`, `Warning` , `Info`, and `Debug`	Define the level for logging in to the session directory.
`--debug (-d)`	None	Displays a `DEBUG` message in the vCloud Availability Installer Appliance console and creates an entry with the same information in the log file. By default, the value is set to `False`. You can append the option to every command that you run on the vCloud Availability Installer Appliance.
`--info (-i)`	None	Displays an `INFO` message to the vCloud Availability Installer Appliance console and creates an entry with the same information in the log file. By default, the value is set to `False`. You can append the option to every command that you run on the vCloud Availability Installer Appliance.

Table 8-1. Basic vCloud Availability Installer Appliance Options and Arguments (Continued)

Option	Argument	Description
`--ssh-cert=`	`File path`	Use the option to provide the path to a private SSH certificate.
`--registry=`	`File path`	Use the option to provide the path to a registry file.
`--dry-run`	None	Use this command to validate a process without running the command. By default, the value is set to `False`. You can append the option to every command that you run on the vCloud Availability Installer Appliance.
`-k`	None	**Caution** With this option, you can use SSL and SSH connections without a certificate validation. By default, the value is set to `False`. You can append the option to every command that you run on the vCloud Availability Installer Appliance.

Prepare the vCloud Availability Installer Appliance for Upgrading to vCloud Availability 1.0.1

You can simplify the deployment of individual components by defining installation variables or by creating a registry file on your vCloud Availability Installer Appliance.

Both ways to deploy and configure vCloud Availability are displayed for your reference. The installation using variables is presented in the left column of the table in each step, containing standard installation and configuration commands. The installation with simple commands, using a vCloud Availability Installer Appliance registry file, is presented in the right column of the table in each step.

Procedure

1 Create protected password files on your vCloud Availability Installer Appliance.

OS credentials are stored in text files in `~/.ssh` directory for all appliances. The files are only accessible to the system **root** user for security purposes. You provide the path to the respective password file during installation and configuration steps.

Note The *appliances-root-password* is the **root** password that is set for the vCloud Availability appliances that you create during installation procedures. The following example uses the same **root** password for all vCloud Availability appliances. You can set different passwords for all appliances, by creating a dedicated password file in the `~/.ssh` directory. Provide the path to the correct password file in the respective installation and configuration step.

Standard Command	Command Using Registry

`# mkdir ~/.ssh`
`# chmod 0700 ~/.ssh`
`# echo 'appliances-root-password' > ~/.ssh/.root`
`# echo 'vcd-password' > ~/.ssh/.vcd`
`# echo 'sso-password' > ~/.ssh/.sso`
`# echo 'management-vsphere-password' > ~/.ssh/.vsphere.mgmt`
`# find ~/.ssh -type f -name '.*' -print0 | xargs -0 chmod 0600`
	`# mkdir ~/.ssh`
	`# chmod 0700 ~/.ssh`
	`# echo 'appliances-root-password' > ~/.ssh/.root`
	`# find ~/.ssh -type f -name '.*' -print0 | xargs -0 chmod 0600`

2 Define installation variables.

Management vSphere details refer to the path of the environment managed by the service providers that is not available to tenant users. The resource vSphere environment details relate to the path of the environment that tenants use. In the current example, the deployment environment consists of one management vSphere instance and two resource vSphere instances.

Important The *Variables* listed in the table are used as an example. Update values to match your environment.

Define Installation Variables

```
# export MGMT_VSPHERE_ADDRESS=mgmt-vsphere-address
# export MGMT_VSPHERE_USER=mgmt-vsphere-admin-user
# export MGMT_VSPHERE_LOCATOR='mgmt-locator'
# export MGMT_VSPHERE_DATASTORE='mgmt-datastore'
# export MGMT_VSPHERE_NETWORK='mgmt-network'

# export VSPHERE01_ADDRESS=vsphere-01-address
# export VSPHERE01_PLACEMENT_LOCATOR=vsphere-01-locator
# export VSPHERE01_PLACEMENT_DATASTORE=vsphere-01-datastore
# export VSPHERE01_PLACEMENT_NETWORK=vsphere-01-network


# export VSPHERE02_ADDRESS=vsphere-02-address
# export VSPHERE02_PLACEMENT_LOCATOR=vsphere-02-locator
# export VSPHERE02_PLACEMENT_DATASTORE=vsphere-02-datastore
# export VSPHERE02_PLACEMENT_NETWORK=vsphere-02-network


# export VCD_ADDRESS=vcd-01-address
# export VCD_USER=root@system
# export SSO_USER=administrator@vsphere.local
```

Create Registry File

1 Create a **~/.vcav/registry** file to hold installation variables. Update the values to match your environment.

```
vsphere mgmt-vsphere-name
    address mgmt-vsphere-address
    api-port 443
    api-user admin-user
    api-password admin-user-password
    placement-locator mgmt-locator
    placement-datastore mgmt-datastore
    placement-network mgmt-network

vsphere vsphere-01-name
    address vsphere-01-address
    api-port 443
    api-user vsphere-01-admin-user
    api-password vsphere-01-admin-password
    placement-locator vsphere-01-locator
    placement-datastore vsphere-01-datastore
    placement-network vsphere-01-network

vsphere vsphere-02-name
    address vsphere-02-address
    api-port 443
    api-user vsphere-02-admin-user
    api-password admin-user-password
    placement-locator vsphere-02-locator
    placement-datastore vsphere-02-datastore
    placement-network vsphere-02-network

VCD vcd-01-name
    address vcd-01-address
    api-port 443
    api-user root@System
    api-password vcd-root-password
    sso-user administrator@vsphere.local
    sso-password sso-password
```

2 Update the file permissions

```
# chmod 0600 ~/.vcav/registry
```

Add Trusted Thumbprints to the vCloud Availability Installer Appliance

The vCloud Availability Installer Appliance must be able to verify the thumbprint of the vCenter Server and vCloud Director hosts that it works with.

To achieve this, you first import the SSL certificate thumbprint of these hosts into the vCloud Availability Installer Appliance, by running the `vcav trust add` command. The command displays the thumbprint that you are importing. For security purposes, you must verify that the displayed thumbprint matches the actual server certificate.

If the SSL certificate of one of the servers changes, rerun the `vcav trust add` command for that host.

Procedure

1 Create a trust between your vSphere instances and the vCloud Availability Installer Appliance.

Repeat this step for every vCenter Server.

a

Standard Command	Command Using Registry
`# vcav trust add --address= $VSPHERE01_ADDRESS --port=443 --accept-all`	`# vcav trust add --vsphere=vsphere-01-name --accept-all`

b

Standard Command	Command Using Registry
`# vcav trust add --address= $VSPHERE02_ADDRESS --port=443 --accept-all`	`# vcav trust add --vsphere=vsphere-02-name --accept-all`

c

Standard Command	Command Using Registry
`# vcav trust add --address= $MGMT_VSPHERE_ADDRESS --port=443 --accept-all`	`# vcav trust add --vsphere=mgmt-vsphere-name --accept-all`

2 Create a trust with vCloud Director.

Standard Command	Command Using Registry
`# vcav trust add --address=$VCD_ADDRESS --port=443 --accept-all`	`# vcav trust add --vcd=vcd-01-name --accept-all`

Connect to vCloud Availability Appliances

Establish a trusted connection between the vCloud Availability Installer Appliance and the remaining vCloud Availability components.

Prerequisites

Verify that you have installed and configured the following vCloud Availability components to support all vCloud Availability services.

- vSphere Replication Manager
- vSphere Replication Cloud Service Host
- vSphere Replication Server
- Cassandra Host
- RabbitMQ Host

Procedure

1 Connect to vSphere Replication Manager.

Repeat the step for every vSphere Replication Manager in your environment.

a Configure the SSH connectivity.

Standard Command	Command Using Registry

`# vcav vsphere trust-ssh \`
`--vsphere-address=$VSPHERE01_ADDRESS \`
`--vsphere-user=$SSO_USER \`
`--vsphere-password-file=~/.ssh/.sso \`
`--vm-name=HMS01-name \`
`--root-password-file=~/.ssh/.root \`
`--vm-address=HMS01-address`
	`# vcav vsphere trust-ssh \`
	`--vsphere=vsphere-o1-name \`
	`--vm-name=HMS01-name \`
	`--root-password-file=~/.ssh/.root \`
	`--vm-address=HMS01-address`

b Connect to vSphere Replication Manager.

```
# vcav hms connect \
--root-password-file=~/.ssh/.root \
--vm-address=HMS01-address
```

c Verify that the connection is successfully established.

Standard Command	Command Using Registry

`# vcav hms check \`
`--hms-address=HMS01-address \`
`--vsphere-address=$VSPHERE01_ADDRESS \`
`--vsphere-user=$SSO_USER \`
`--vsphere-password-file=~/.ssh/.sso \`
`--vcd-address=vcd-01-address \`
`--vcd-user=root@system \`
`--vcd-password-file=~/.ssh/.vcd \`
`--sso-user=administrator@vsphere.local \`
`--sso-password-file=~/.ssh/.sso`
	`# vcav hms check \`
	`--hms-address=HMS01-address \`
	`--vsphere=vsphere-o1-name \`
	`--vcd=vcd-01-name`

If the connection is successfully established, the system returns an **OK** message.

2 Create a trusted connection with your RabbitMQ host.

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

3 Create a trusted connection with your Cassandra host.

```
# vcav trust add --address=cassandra-address --port=9042 --accept-all
```

4 Connect to vSphere Replication Cloud Service Host.

Repeat the step for every vSphere Replication Cloud Service host in your environment.

a Configure the SSH connectivity.

Standard Command

```
# vcav vsphere trust-ssh \
--vsphere-address=mgmt-vsphere-address \
--vsphere-user=mgmt-vsphere-user \
--vsphere-password-
file=~/.ssh/.vsphere.mgmt \
--vm-name=HCS01-address \
--root-password-file=~/.ssh/.root \
--vm-address=HCS01-address
```

Command Using Registry

```
# vcav vsphere trust-ssh \
--vsphere=mgmt-vsphere-name \
--vm-name=HCS01-name \
--root-password-file=~/.ssh/.root \
--vm-address=HCS01-address
```

b Connect to vSphere Replication Cloud Service Host.

```
# vcav hcs connect --root-password-file=~/.ssh/.root --vm-address=HCS01-address
```

c Verify that the connection is successfully established.

Standard Command

```
# vcav hcs check \
--hcs-address=HCS01-address \
--vcd-address=vcd-01-address \
--vcd-user=root@system \
--vcd-password-file=~/.ssh/.vcd \
--sso-user=administrator@vsphere.local \
--sso-password-file=~/.ssh/.sso \
--vsphere-address-list=vsphere-01-address
```

Command Using Registry

```
# vcav hcs check \
--hcs-address=HCS01-address \
--vcd=vcd-01-address \
--vsphere-registry-list=vsphere-01-address
```

If the connection is successfully established, the system returns an **OK** message.

5 Connect to vSphere Replication Server.

a Configure the SSH connectivity.

Repeat this step for every vSphere Replication Server in your environment.

Standard Command

```
# vcav vsphere trust-ssh \
--vsphere-address=$VSPHERE01_ADDRESS \
--vsphere-user=$SSO_USER \
--vsphere-password-file=~/.ssh/.sso \
--vm-name=HBR01-name \
--root-password-file=~/.ssh/.root \
--vm-address=HBR01-address
```

Command Using Registry

```
# vcav vsphere trust-ssh \
--vsphere=vsphere-o1-name \
--vm-name=HBR01-name \
--root-password-file=~/.ssh/.root \
--vm-address=HBR01-address
```

b Connect to vSphere Replication Server.

```
# vcav hbr connect --root-password-file=~/.ssh/.root --vm-address=HBR01-address
```

Create vCloud Availability Portal Host

The vCloud Availability Portal provides a graphic user interface to facilitate the management of vCloud Availability operations.

The vCloud Availability Portal back end (PBE) scales horizontally. You can deploy a new vCloud Availability Portal instance on demand connected to the same load balancer that all the vCloud Availability Portal instances are under. The load balancer must support sticky sessions, so that the same PBE instance processes user requests within a session. This setting ensures that all the information displayed in the vCloud Availability Portal is consistent.

Depending on the number of concurrent sessions that the vCloud Availability Portal is expected to host, you can deploy `small`, `medium`, or `large` vCloud Availability Portal host. The vCloud Availability Portal sends requests to a vCloud Director instance and receives data from the same vCloud Director instance. To host the maximum number of concurrent sessions, ensure that the vCloud Director database can use similar compute resources that you allocate to the vCloud Availability Portal host. You can find details about the vCloud Availability Portal deployment types in the following table.

Table 8-2. vCloud Availability Portal Host Deployment Types

Deployment Type	Description
`Small`	Deploys an appliance with 2 CPUs, 2 GB of memory, 10 GB of disk space, and 512 MB of Java Virtual Memory. Suitable for hosting up to 150 concurrent sessions.
`Medium`	Deploys an appliance with 2 CPUs, 4 GB of memory, 10 GB of disk space, and 1.5 GB of Java Virtual Memory. Suitable for hosting up to 400 concurrent sessions.
`Large`	Deploys an appliance with 4 CPUs, 6 GB of memory, 10 GB of disk space, and 3 GB of Java Virtual Memory. Suitable for hosting up to 800 concurrent sessions.

Procedure

1 Create a vCloud Availability Portal host by running the following command.

Important The `--deployment-type` argument in the following command defines the compute resources that you allocate to the vCloud Availability Portal host. By default, the value is `small`. You can change the value depending on your requirements.

Standard Command	Command Using Registry

`# vcav vcd-ui create \`
`--ovf-url=vcloud-availability-for-vcd-ui-ova-1.0.1.2-xxx-build_number.ova \`
`--deployment-type=small \`
`--vsphere-address=$MGMT_VSPHERE_ADDRESS \`
`--vsphere-user=$MGMT_VSPHERE_USER \`
`--vsphere-password-file=~/.ssh/.vsphere.mgmt \`
`"--network=$MGMT_VSPHERE_NETWORK" \`
`"--vsphere-locator=$MGMT_VSPHERE_LOCATOR" \`
`--datastore=$MGMT_VSPHERE_DATASTORE \`
`--ntp=pool.ntp.org \`
`--root-password-file=~/.ssh/.root \`
`--vm-name=ui01-name`
	`# vcav vcd-ui create \`
	`--ovf-url=vcloud-availability-for-vcd-ui-ova-1.0.1.2-xxx-build_number.ova \`
	`--deployment-type=small \`
	`--vsphere=mgmt-vsphere-name \`
	`--ntp=pool.ntp.org \`
	`--root-password-file=~/.ssh/.root \`
	`--vm-name=ui01-name`

The IP address of the new vCloud Availability Portal virtual machine is displayed. Write it down because you need it during the configuration.

2 Set a variable to the address of the created virtual machine.

Standard Command	Command Using Registry
`# UI01_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=ui01-name``	`# UI01_ADDRESS=`vcav vsphere get-ip \` `--vsphere=mgmt-vsphere-name \` `"--network=mgmt-network" \` `--vm-name=ui01-name``

3 Update the `truststore` file with the vCloud Availability Portal virtual machine credentials.

```
# echo 'Portal-VM-Password' > ~/.ssh/.truststore

# chmod 0600 ~/.ssh/.truststore
```

4 If you use Fully Qualified Domain Names (FQDN) to access and manage appliances, you must verify that the DNS record matches the vCloud Availability Portal IP address, and trusts the SSH certificate for this FQDN.

   a Check the DNS server to ensure that the entry matches the IP address of the vCloud Availability Portal host.

   b Run the `trust-ssh` command to trust the certificate for the vCloud Availability Portal FQDN.

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 \`
`--root-password-file=~/.ssh/.root \`
`--vm-name=ui01-name \`
`--vm-address=ui01-FQDN`
	`# vcav vsphere trust-ssh \`
	`--vsphere=mgmt-vsphere-name \`
	`--root-password-file=~/.ssh/.root \`
	`--vm-name=ui01-name \`
	`--vm-address=ui01-FQDN`

Configure vCloud Availability Portal Host

Procedure

1 Configure the vCloud Availability Portal host by running the following command.

   In the following example the vCloud Availability Portal is configured to operate with a new generated self-signed SSL certificate. You can set up the vCloud Availability Portal to use an externally signed SSL certificate, by replacing the `--keep-self-signed-certificate` argument with `--https-certificate=/file-path-to-certificate-file` and `--https-key=/file-path-to-certificate-public-key`. The vCloud Availability Portal appliance provides the certificate and key files to an `nginx` process.

Standard Command	Command Using Registry

`# vcav vcd-ui configure \`
`--ui-address=$UI01_ADDRESS \`
`--keep-self-signed-certificate \`
`--truststore-password-file=~/.ssh/.truststore \`
`--vcd-address=$VCD_ADDRESS \`
`--vcd-user=$VCD_USER \`
`--vcd-password-file=~/.ssh/.vcd \`
`--sso-user=administrator@vsphere.local \`
`--sso-password-file=~/.ssh/.sso`
	`# vcav vcd-ui configure \`
	`--ui-address=$UI01_ADDRESS \`
	`--keep-self-signed-certificate \`
	`--truststore-password-file=~/.ssh/.truststore \`
	`--vcd=vcd-01-name`

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

2 You allocate small, medium, and large sizes of Java Virtual Memory (JVM) to the vCloud Availability Portal service process during the deployment of the vCloud Availability Portal host. You can change the allocated JVM by following the procedure bellow. You must complete steps Step 2d and Step 2g for medium and large deployments. For more information about the vCloud Availability Portal deployment types and related JVM configuration, see Create vCloud Availability Portal Host. You can optionally update the allocated JVM by editing the `nginx.conf` file by completing the following steps.

a Use SSH to connect to the vCloud Availability Portal host.

b Use a text editor to open the `/opt/vmware/conf/vcav-ui/nginx/nginx.conf` file.

c The initial size of the memory allocation pool is defined in the following line. Change the numeric value to designate more JVM to the vCloud Availability Portal host.

```
jvm_options "-Xms1024m";
```

d The following line defines the maximum size of memory allocation pool for the `nginx` process. The numeric value must be equal to or greater than the numeric value you defined in the previous step.

Important This step required for medium and large vCloud Availability Portal deployments.

```
jvm_options "-Xmx1024m";
```

e You can optionally uncomment the following lines to enable JVM heap dump and define the heap dump file path.

```
jvm_options "-XX:+HeapDumpOnOutOfMemoryError";
jvm_options "-XX:HeapDumpPath=/opt/vmware/logs/vcav-ui/jvm.hprof";
```

f By default, the maximum number of concurrent client sessions is set to 1024. To increase this number, use a text editor to open the `/usr/lib/systemd/system/vcav-ui.service` and add the following line after the `[Service]` line.

```
LimitNOFILE=8192
```

g Restart the vCloud Availability Portal service to complete this configuration, by running the following command.

Important This step required for medium and large vCloud Availability Portal deployments.

```
systemctl restart vcav-ui
```

3 Configure the `nginx` process to run for a `non-root` user.

The vCloud Availability Portal host `nginx` process runs under the system `root` user by default. You can change the user that the `nginx` process uses by modifying the vCloud Availability Portal service script. You can skip this step, if you do not want to edit the `nginx` process user.

a Use SSH to connect to the vCloud Availability Portal host as `root`.

b Stop the vCloud Availability Portal service by running the following command.

```
# systemctl stop vcav-ui
```

c Use a text editor to modify the `/usr/lib/systemd/system/vcav-ui.service` file, by adding `User=`*`new-user-name`* line after the `[Service]` line.

d Change the line that provides the `PID` file location to read `PIDFile=/opt/vmware/logs/vcav-ui/vcav-ui.pid`.

e Using a text editor open the `/opt/vmware/conf/vcav-ui/nginx/nginx.conf` and change the line that provides the `PID` file location to read `pid /opt/vmware/logs/vcav-ui/vcav-ui.pid`.

f Change the ownership of the log files that the service uses by running the following commands.

```
# chown -R new-user-name /opt/vmware/logs/vcav-ui

# chown -R new-user-name /opt/vmware/vcav-ui/logs
```

g Start the vCloud Availability Portal service by running the following command.

```
# systemctl start vcav-ui
```

4 Assign a domain name to your vCloud Availability Portal host.

It is a best practice to assign a domain name to your vCloud Availability Portal VM for production deployments.

5 Verify that the vCloud Availability Portal is configured correctly, by running the following command.

```
'curl -k https://$UI01_ADDREESS:8443/
```

Backing up the vCloud Availability Solution

9

You can back up and recover the vCloud Availability 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 solution.

Table 9-1. Backup Strategy for vCloud Availability 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, see Backing up and Restoring the Platform Services Controller in *vSphere Installation and Setup*.
vRealize Orchestrator Appliance	Combine VM level backups with external database backups.
RabbitMQ Server	Run stateless VM level backups.
Cassandra Server	Run VM level backups.

10 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.

This chapter includes the following topics:

- Key Features
- vRealize Orchestrator Plug-Ins
- vRealize Orchestrator Plug-In for vSphere Replication and vCloud Availability

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.

vRealize Orchestrator Plug-In for vSphere Replication and vCloud Availability

Users and tenants of vCloud Availability 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 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
  c. From vCloud Availability to an on-premise vCenter Server data center
- Reverse replication workflow:
  a. From vCloud Availability to an on-premise vCenter Server data center

- Planned migration workflow:
  a From an on-premise vCenter Server data center to vCloud Availability
  b From vCloud Availability to an on-premise vCenter Server data center
- Test Recovery workflow:
  a From an on-premise vCenter Server data center to vCloud Availability
  b From vCloud Availability to an on-premise vCenter Server data center
- Cleanup of test instances:
  a From an on-premise vCenter Server data center to vCloud Availability
  b From vCloud Availability to an on-premise vCenter Server data center
- Real Recovery Workflow:
  a From vCloud Availability to an on-premise vCenter Server data center
  b From an on-premise vCenter Server data center to vCloud Availability
- Unconfigure a Replication workflow:
  a Between on-premise vCenter Server data centers
  b From an on-premise vCenter Server data center to vCloud Availability
  c From vCloud Availability 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
  b Clean up test recovery for a virtual machine replicated to vCloud Availability
  c Real Recovery for a virtual machine replicated to vCloud Availability

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

Day 2 Operations

11

Day 2 operations happen post provisioning and include routine maintenance tasks and changes to the virtual environment. For vCloud Availability, 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 version 1.0.1.1 and above, to support these operations.

- Day 2 Operations Scripts

  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.

- Password Management

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

- Certificate Management

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

- Diagnostic Information

  Getting diagnostic information for vCloud Availability deployments requires a careful collection of the logs from each component.

Day 2 Operations Scripts

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 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`. If a disk cannot be found in vCloud Director, add the following two parameters to search for a disk in vCenter Server: ■ `--sso-user=`*`$SSO_USER`* ■ `--sso-password-file=`*`~/.ssh/.sso`*
`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.

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 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.

Password Management

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

Handling Password Changes of Infrastructure Components

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

3 Configure vCloud Availability Administration Portal with the New Password

After you configure vCloud Availability, you must also configure vCloud Availability Administration Portal.

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 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 vCloud Availability Administration Portal with the New Password

After you configure vCloud Availability, you must also configure vCloud Availability Administration Portal.

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.

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.

For more information on changing the password for a vCloud Director database, see Update Database Connection Properties.

What to do next

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

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]
```

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 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 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 vCloud Availability Administration Portal 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 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 Portal Host Root User

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

Prerequisites

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

Procedure

1. Connect to the vCloud Availability 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 Portal host, you must edit the corresponding truststore password file with the new root password.

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

You can change the password for the root user for the vCloud Availability Administration 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 Administration 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 Administration 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 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 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 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 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 components.

Add an Updated vSphere Machine SSL Certificate to vCloud Availability

To add an updated vSphere machine SSL certificate to vCloud Availability, 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 does not use an SSL port for the AMQP protocol, the `vcav hcs configure` operation returns an error.

Note You can add the `--amqp-port=`*`port-number`* argument to override the vCloud Director port and point the AMQP service to an SSL port.

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 instance.

Updating Tenant vSphere Certificates

To update the vSphere machine SSL certificate, you must reconfigure all vSphere Replication Server instances.

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

Add an Updated vSphere Machine SSL Certificate to a vSphere Replication Server

To add an updated vSphere machine SSL certificate to a vSphere Replication Server, you must re-register all vSphere Replication Server instances with the vSphere SSO service.

Important You must perform the following steps for all vSphere Replication Server instances.

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. In a Web browser, navigate to the vSphere Replication virtual appliance management interface (VAMI) on the following URL.

   `https://(appliance hostname or IP address):5480`

2. Log in with *root* privileges.
3. Navigate to **VR > Configuration**.
4. To add the new vSphere machine SSL certificate, re-register the vSphere Replication Server with the vSphere lookup service.
   a. Enter the **SSO Administrator** user name in the text box.
   b. Enter the **Password** in the text box.
   c. In the **Actions** pane, click **Save and Restart Service**.

   A **Successfully save the configuration** message appears.
5. Verify that the vSphere Replication Server is properly re-registered.
   a. Log in to the vSphere Web Client as an **administrator**.
   b. Navigate to **Manage > vSphere Replication > Replication Servers**.
   c. Verify that the status of the vSphere Replication Server is **Connected**.

      You might have to wait several minutes until the vSphere Replication Server becomes available.

You have successfully added an updated vSphere machine SSL certificate to a vSphere Replication Server 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, see Create and Import a Signed SSL certificate in the *vCloud Director Installation and Upgrade Guide.*
2. Update the vCloud Director public endpoint configuration. For more information, see Customize Public Endpoints in 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 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 Portal hosts to use the new vCenter Server 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 Using a 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 Cassandra Installation and Configuration.

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	Command Using Registry

`# 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=$SSO_USER \`
`--sso-password-file=~/.ssh/.sso`
	`# vcav cassandra register \`
	`--hcs-address=hcs-IP-address \`
	`--cassandra-address=$CASSANDRA_ADDRESS \`
	`--cassandra-port=9042 \`
	`--vcd=vcd-01-name`

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

Standard Command	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 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 RabbitMQ Installation and Configuration.

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 Portal Host Certificate

To update the vCloud Availability 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 Portal certificate, complete the following steps.

1 To verify that you are replacing the correct vCloud Availability 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 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	Command Using Registry

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

To update the vCloud Availability Administration 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 Administration Portal certificate, complete the following steps.

1 To verify that you are replacing the correct vCloud Availability Administration 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 Administration 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.

Diagnostic Information

Getting diagnostic information for vCloud Availability deployments requires a careful collection of the logs from each component.

Because there are various different components on both the service provider and tenant installations, troubleshooting relies on careful investigation of the configuration and logs generated by each component. These logs then must be examined in tandem to identify the errors.

Service Provider Diagnostics

Due to the large number of different components used to support the vCloud Availability 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.

Component Versions

To get the deployed version of the vCloud Availability components, you have to create an SSH connection and run the following command on the VM hosting the component:

```
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.

Collect Logs Using vCloud Availability Installer Appliance

The vCloud Availability Installer Appliance provides an easy way to collect logs from all 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

To generate logs from vCloud Availability Installer Appliance 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
```

Run the script for every vSphere Replication Manager and vSphere Replication Cloud Service host you want to collect logs from.

Once generated, the logs are downloaded and stored in `/tmp` folder on the vCloud Availability Installer Appliance.

vCloud Availability Portal Logs

The vCloud Availability Portal log files are at `/opt/vmware/logs/vcav-ui`.

Table 11-1. vCloud Availability Portal Log Files

Filename	Description
`access.log`	This file is generated by the `nginx` process and contains external request and response statuses.
`dr2c.log`	This file is generated by the vCloud Availability Portal and contains the following: ■ Routing information ■ Details for requests to vCloud Director ■ Details for responses from vCloud Director ■ Other runtime information
`error.log`	This file is generated by the `nginx` process and contains unhandled runtime errors.

vCloud Availability Administration Portal Logs

The vCloud Availability Administration Portal log files are at `/opt/vmware/vcav-smp/logs`.

Table 11-2. vCloud Availability Administration Portal Log Files

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

Support Bundles

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.

vCenter Server

You can generate the vCenter Server 6.0 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.

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`

vSphere Repication 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.

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.

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.

Log File Location

If you are not using the support bundle capability, you can collect diagnostic information manually. The following table lists the log locations for all the components.

Table 11-3. Log File Location for Service Provider Components

Component	Log Location
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	`/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 Portal	`/opt/vmware/logs/vcav-ui`
vCloud Availability Administration 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`

Tenant Diagnostics

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.

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.

Support Bundles

Support bundles are generated automatically and contain product-specific logs, configuration files, and data appropriate to the situation.

vSphere Repication Appliance

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) on the following URL.

   `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

Log File Locations

If you are not using the support bundle capability, you can collect diagnostic information manually. The following table lists the log locations for all the components.

Table 11-4. Log File Location for Tenant Components

Component	Log Location
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.

Useful Operations

12

Useful operations for administering a vCloud Availability for vCloud Director.

- vCloud Availability Installer Appliance Useful Operations

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

- Register vCloud Director with Shared SSO

  Register vCloud Director with Shared SSO to which all backing resource vCenter Servers are registered.

- Securing vSphere Replication Server Traffic

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

vCloud Availability Installer Appliance Useful Operations

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

- Useful Commands
- Create Containers for Test and Development Environments

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

- Docker Operations

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

- Configure Service Provider vCloud Director Organizations

  Each Organization VDC must be enabled for replication, before configuring tenant environment.

Useful Commands

`Get-ip`

If you need the IP address of any of the vCloud Availability host VMs, you can run the following command.

Standard Command	Command Using Registry

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

The IP address is displayed.

Connect

If you lose connectivity to any of the VMs hosting vCloud Availability services, you can reconnect the component by using vCloud Availability scripts.

Reconnect to vSphere Replication Management Server

To reconfigure the SSH connectivity, 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=hms-VM-name`
`--root-password-file=~/.ssh/.root`
`--vm-address=hms-address`
	`# vcav vsphere trust-ssh \`
	`--vsphere=mgmt-vsphere-name \`
	`--vm-name=hms-VM-name \`
	`--root-password-file=~/.ssh/.root \`
	`--vm-address=hms-address`

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

Standard Command	Command Using Registry

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

Reconnect to vSphere Replication Cloud Service host VM

To reconfigure the SSH connectivity, 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 your vSphere Replication Cloud Service host 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 \`
	`--root-password-file=~/.ssh/.root \`
	`--vm-address=hcs-address`

Reconnect to vSphere Replication host VM

To reconfigure the SSH connectivity, 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 your vSphere Replication host 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 \`
	`--root-password-file=~/.ssh/.root \`
	`--vm-address=hbr-address`

Docker Host

To connect to your Docker host virtual machine, run the following command.

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

Reconfigure

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

A use case for the `reconfigure` command is adding vCenter Server to the vCloud Availability 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 Management server and vSphere Replication servers to your new vCenter Server instance. For more information, see Installing vCloud Availability.

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.

Create 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 Cassandra Installation and Configuration. For more information about installing and configuring RabbitMQ hosts for production, seeRabbitMQ Installation and Configuration.

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 ReplicationCloud 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.

Docker Operations

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 amqp01 rabbitmqctl list_users

# docker exec cassandra01 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.

Configure Service Provider vCloud Director Organizations

Each Organization VDC must be enabled for replication, before configuring tenant environment.

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 Configure vSphere Replication Cloud Service.

Procedure

- Enable Organization VDC for replication using the vCloud Availability Installer Appliance.

Standard Command	Command Using Registry

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

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

Register vCloud Director with Shared SSO

Register vCloud Director with Shared SSO to which all backing resource vCenter Servers are registered.

Procedure

- Register VCD with the lookup service of the tenant VC through REST API.

```
PUT https://<vcd ip>:<port>/api/admin/extension/settings/lookupService
Accept: application/*+xml;version=6.0
Content-Type: application/*+xml;version=6.0
<LookupServiceParams xmlns="http://www.vmware.com/vcloud/extension/v1.5"
xmlns:vcloud_v1.5="http://www.vmware.com/vcloud/v1.5"
userName="SSO_ADMIN_USER" password="SSO_ADMIN_USER_PASS"><LookupServiceUrl>https://{SSO_URL_IP}:
{SSO_PORT}/lookupservice/sdk</LookupServiceUrl>
</LookupServiceParams>
```

Note Here onwards vCloud Director can be accessed only with this URL `https://VCD IP or hostname/cloud/login.jsp`.

Enable SSO in vCloud Director UI: **Administration > Federation > Use vSphere Single Sign On**

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.

Using the vCloud API Schema Reference

13

The API provides access to the vCloud Availability service including failover, testing failover and failback, enabling the operations to be scripted or controlled through an external process.

Using the API interface you can integrate operations with other services and systems, including integration into Web and command-line control systems.

This chapter includes the following topics:

- API Workflow
- vCloud Director for Connection and Authentication
- vSphere Replication Server Registration Example
- Enabling Replication Example

API Workflow

Configuration and recovery of protected virtual machines uses a fixed process through the API service

To configure and recover virtual machines protected by the service, perform the following tasks in vSphere Replication and service provider environment:

1. Using the vSphere Replication Appliance, specifically the vCenter Server Web Client UI extension, replicate the virtual machines that you plan to protect from your source site to the Service Provider.

   You must initiate replication to the cloud by using vSphere Replication at your source site because replication between your source site and the cloud is not symmetrical. You can initiate a replication to the cloud from your source site but, for security reasons, you cannot communicate with the virtual machines at your source site from the cloud.
2. After replicating your virtual machines to the cloud, call the APIs to list the replications.
3. Using API calls test recovery for a virtual machine and cleanup the test after you run it.
4. If your source site becomes unavailable, recover your virtual machines by using failback API calls.

vCloud Director for Connection and Authentication

Before starting management through the API, a suitable connection and authentication process must be followed, and then the generated token must be used for further calls.

Table 13-1. vCloud Director Operations for Connection and Authentication.

Operation	Description	Headers
GET /api/versions	Every cloud has a login URL that a client can obtain by making an unauthenticated `GET` request to the vCloud Director API/versions URL. The response to this request also lists vCloud API versions that the server supports. Each version of the vCloud API that the server supports has its own login URL. You can find the URL in the `LoginUrl` element of response.	
POST /api/sessions	Authenticates a user and creates a Session object that contains the URLs from which that user can begin browsing. Users who authenticate to the integrated identity provider use basic HTTP authentication. If the request is successful, the server returns HTTP response code 200 (OK) and headers that include an authorization header of the form: `x-vcloud-authorization: token` This header must be included in each subsequent vCloud API request. The `Session` element returned from a successful login contains one or more URLs from which you can begin browsing.	Authorization: Basic encoded-credentials. Accept: `application/*+xml;version=5.5` All requests must include an HTTP Accept header that designates the vCloud API version that the client supports. Supply credentials like: `user@organization:password` `User` is the login name. `Organization` is the name of an organization of which the user is a member. `Password` is the user profile password. You must supply these credentials in a MIME Base64 encoding.

vSphere Replication Server Registration Example

Registering a vSphere Replication Server instance into a vCloud Availability deployment uses multiple steps and calls to the Web service API.

The following steps show the sample process using a combination of the `curl` tool and shell variables to compose the required requests to register a new vSphere Replication Server instance.

Prerequisites

When using the Web services API, you can use any tool that can set and request the required information. In the example below, the command-line tool `curl`. The process requires multiple steps, first to obtain the authorization, then the registration URL, and finally the call that performs the registration.

Procedure

1 Create variables that you use in the rest of the registration process:

```
VCD_IP=<IP address or FQDN for the vCD host>
VRS_IP=<IP address or FQDN for the VRS host>
VRS_THUMBPRINT=`openssl s_client -connect $VRS_IP:5480 \
    -tls1 -verify 0 </dev/null 2>/dev/null | \
openssl x509 -fingerprint -noout | grep Fingerprint | \
head -n1 | \awk -F= '{print $2}'`
```

This step configures the IP address of the vSphere Replication Server instance, and the fingerprint required to access the information.

2 Generate variables to be used to hold information for the first access to the API:

```
CONTENT="regVRS-content.txt"
HEADERS="regVRS-headers.txt"
ACCEPT='Accept: application/*+xml;version=5.6'
USER='root@system'
PASS='ca$hc0w'
```

The `$CONTENT` variable is a file, to which the information is returned. The `$HEADERS` is the header material used to supply authentication and supported returned types.

3 Authenticate with the vCD API by using `curl` with the previously set variables.

```
$ curl -k -o "$CONTENT" -D "$HEADERS" -X POST --user "$USER:$PASS" -H "$ACCEPT" "https://$
{VCD_IP}/api/sessions"
```

The information returned from this call is placed into the two files reference by the variables. One containing the headers, and the other the body.

4 You can confirm that the process finishes successfully by checking the content of the header file:

```
$ head -n1 $HEADERS
```

The returned header contains a successful HTTP result code `200`, for example `HTTP/1.1 200 OK`.

5 Extract the authorization code from the returned header information. The code must be provided in future requests to authenticate the operations.

```
$ grep x-vcloud-authorization "$HEADERS" | awk -F : '{print $2}' | tr -d ' '
```

6 Create a variable containing the return authorization code:

```
$ VCD_COOKIE=93f2f3f0c07a4355b3466812ddf9987e
```

7 Obtain the URL for the VIM server by submitting another curl request, using the authorization code:

```
$ curl -k -o "$CONTENT" -D "$HEADERS" \
    -H "x-vcloud-authorization: $VCD_COOKIE" \
    -H "$ACCEPT" \
    https://${VCD_IP}/api/admin/extension/vimServerReferences
```

The returned header contains a successful HTTP result code `200`.

8 Extract the `VimServerReference` from the returned data:

```
$ cat $CONTENT | grep "vmext:VimServerReference" | awk -F\" '{print $2}'
```

9 Set the returned value into a variable:

```
$VIM_URL=https://10.158.12.163/api/admin/extension/vimServer/f88ce1f6-f8f3-489b-9f32-fac50b035f2b
```

10 Build the request body:

```
ACCEPT='Accept: application/*+xml;version=6.0;vr-version=3.0'
REGVRS_BODY="<?xml version=\"1.0\" encoding=\"UTF-8\" standalone=\"yes\"?>
<ns2:ManageVrServerParams xmlns=\"http://www.vmware.com/vcloud/v1.5\"
xmlns:ns2=\"http://www.vmware.com/vr/v6.0\">
    <ns2:VrThumbprint>${VRS_THUMBPRINT}</ns2:VrThumbprint>
    <ns2:VrManagementURI>https://${VRS_IP}:8123</ns2:VrManagementURI>
<ns2:VrTrafficPort>31031</ns2:VrTrafficPort>
</ns2:ManageVrServerParams>"
```

11 Submit the request using the compiled request body:

```
$ curl -k -o "$CONTENT" -D "$HEADERS" \
    -X POST --data-binary "$REGVRS_BODY" \
    -H "x-vcloud-authorization: $VCD_COOKIE" \
    -H "Content-Type: application/vnd.vmware.hcs.registerVrServerParams+xml" \
    -H "$ACCEPT" ${VIM_URL}/action/registerVrServer
```

The returned header contains a successful HTTP result code `200`.

12 Extract the URL required to perform the registration:

```
$ cat $CONTENT | grep Link | grep "application/vnd.vmware.vcloud.task+xml" | awk -F\" '{print $4}'
# TASK_URL=https://10.158.12.163/api/task/49e6347e-0382-4843-b494-2eea01e77229
```

13 To perform the registration, submit the final request:

```
$ curl -k -o "$CONTENT" -D "$HEADERS" \
    -H "x-vcloud-authorization: $VCD_COOKIE" -H "$ACCEPT" $TASK_URL
```

The returned header contains a successful HTTP result code `200`.

What to do next

Examine the content of the returned information and verify that the progress is `100` and that there are no errors listed.

Enabling Replication Example

Enabling replication for a virtual machine a vCloud Availability deployment uses multiple steps and calls to the Web service API.

During the replication enablement process, the steps are completed by a vCloud Director administrator.

Note The following procedure contains long, single commands that should be run as one. There are breaks in the command for better visibility marked with "\". "#" marks the beginning of a new command.

Prerequisites

When using the Web services API, you can use any tool that can set and request the required information. In the example below, the command-line tool curl. The process requires multiple steps, first to obtain the authorization, then the registration URL, and finally the call that performs the registration.

Procedure

1 Create some variables that are used in the rest of the process:

```
CONTENT="regOrg-content.txt"
HEADERS="regOrg-headers.txt"
ACCEPT='Accept: application/*+xml;version=5.6'
USER='administrator@System'
PASS='.s3cr3tP@ssw0rd!'
VCD_IP=10.158.12.128
```

2 Authenticate with the vCD API by using `curl` with the previously set variables. You use the authorization token returned in all further commands.

```
# curl -k -o "$CONTENT" -D "$HEADERS" -X POST --user "$USER:$PASS" \
 -H "$ACCEPT" "https://${VCD_IP}/api/sessions"
```

3 Extract the authorization code from the returned header information:

```
# head -n1 $HEADERS

# grep x-vcloud-authorization "$HEADERS" | awk -F : '{print $2}' | tr -d ' '
```

4 Set a variable to contain the authorization code:

```
# VCD_COOKIE=93f2f3f0c07a4355b3466812ddf9987e
```

5 To identify the correct organization where the replication will be enabled, obtain a list of configured organizations:

```
# curl –k –o "$CONTENT" –D "$HEADERS" \
 –H "x–vcloud–authorization: $VCD_COOKIE" \
 –H "$ACCEPT" https://${VCD_IP}/api/org
```

6 Extract the organization:

```
# head –n1 $HEADERS

# cat $CONTENT | grep "application/vnd.vmware.vcloud.org+xml" | awk –F\" '{print $4 ":" $2}'
```

7 Obtain a list of the VDCs within the organization:

```
# curl –k –o "$CONTENT" –D "$HEADERS" –H "x–vcloud–authorization: $VCD_COOKIE" \
  –H "$ACCEPT" https://10.158.12.163/api/org/0be6ca24–5769–413e–b121–2d7290310dcb

# head –n1 $HEADERS

# cat $CONTENT | grep "application/vnd.vmware.vcloud.vdc+xml" | awk –F\" '{print $6 ":" $4}'
```

8 To enable a replication to the selected organization, obtain the registration URL required:

```
# curl –k –o "$CONTENT" –D "$HEADERS" –H "x–vcloud–authorization: $VCD_COOKIE" \
  –H "$ACCEPT" https://10.158.12.163/api/vdc/0de76523–a3ec–4b90–878d–007527127ce0

# head –n1 $HEADERS

# cat $CONTENT | grep "enableReplication" | awk –F\" '{print $4}'
```

9 Enable a replication by submitting a POST request using the URL retrieved in the previous step.

```
# curl –k –o "$CONTENT" –D "$HEADERS" –X POST –H "x–vcloud–authorization: $VCD_COOKIE" \
  –H "$ACCEPT" \
  https://10.158.12.163/api/vdc/0de76523–a3ec–4b90–878d–007527127ce0/action/enableReplication

# head –n1 $HEADERS

# cat $CONTENT | grep Link | grep "application/vnd.vmware.vcloud.task+xml" | \
  awk –F\" '{print $4}'
```

10 Confirm that the task finishes successfully to enable a replication.

```
# curl –k –o "$CONTENT" –D "$HEADERS" –H "x–vcloud–authorization: $VCD_COOKIE" \
  –H "$ACCEPT" https://10.158.12.163/api/task/49e6347e–0382–4843–b494–2eea01e77229

# head –n1 $HEADERS

# cat $CONTENT
```

Replication is now be enabled. If the task fails, look for the error, correct, and try to enable a replication again.