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
Contents

1 About Installing, Configuring and Upgrading VMware vCloud Availability in the Cloud 5

Updated Information 6

2 Overview of VMware vCloud Availability 7
   Cloud Deployment Architecture 8
   VMware vCloud Availability Services 10

3 Installing and Configuring VMware vCloud Availability 13
   VMware vCloud Availability Requirements 13
      VMware vCloud Availability Users and Services Requirements 13
      VMware vCloud Availability Deployment Requirements 15
      VMware vCloud Availability Network Port Configuration 16
      vCloud Availability Management Endpoints 19
   Deploy VMware vCloud Availability Services Using the vSphere Client 20
   Deploying VMware vCloud Availability Services with OVF Tool 22
      Defining OVF Tool Parameters for VMware vCloud Availability Services Deployment 22
      Deploy VMware vCloud Availability Services Using the OVF Tool 23
   Configure vCloud Availability Services 25
      Configure a vCloud Availability Replication Manager 26
      Configure a vCloud Availability vApp Replication Manager 27
      Configure vCloud Availability Replicator Appliance 29
      Register a vCloud Availability Replicator with a vCloud Availability Replication Manager in the Same Site 30
   Configure vCloud Availability Tunnel 30
   Enable vCloud Availability Tunnel 32
   Restart Services 32
   Configuring the Customer Experience Improvement Program 33
      Categories of Information That VMware Receives 33
      Join or Leave the Customer Experience Improvement Program 33

4 Upgrading vCloud Availability 35
   Order of Upgrading vCloud Availability Components 35
   Upgrade vCloud Availability Components by Using Default Repository 36
   Upgrade VMware vCloud Availability by Using an ISO Image 37
   Upgrade vCloud Availability Components by Using a Specified Repository 38
   Install the vCloud Availability Plug-In for vCloud Director 39
Start Working with vCloud Availability 3.0 40

5 Managing VMware vCloud Availability 42
   Pair Cloud Sites 42
   Re-Pair Cloud Sites 43
   Add a New vCloud Availability Replicator 44
   Certificate Management in VMware vCloud Availability 45
      Regenerate a Self-Signed Certificate 45
      Upload a CA-Signed Certificate 46
      Replacing vCloud Availability Services Certificates 46
   Certificate Management in the External Infrastructure 51
      Configure VMware vCloud Availability with a Renewed vCloud Director Endpoint or Certificate 51
      Configure VMware vCloud Availability with a Renewed Lookup Service Certificate on a Platform Services Controller 52
   Collect VMware vCloud Availability Usage Information 54
   Collect VMware vCloud Availability Storage Consumption Information 56
   Free up Disk Space on the vCloud Availability Appliance 58
   Troubleshooting VMware vCloud Availability 59
      Update a Network Time Protocol Configuration 59
      Cannot Access the vCloud Availability Portal Through vCloud Director 60
      Collecting Support Bundles for the vCloud Availability Components 61
About Installing, Configuring and Upgrading VMware vCloud Availability in the Cloud

The Installing, Configuring and Upgrading VMware vCloud Availability in the Cloud document provides information on how to install, configure, upgrade, and administer the VMware vCloud Availability solution from the service provider side.

Intended Audience

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

- VMware vSphere®
- VMware vCloud Director®
- VMware vCloud® Availability
- Secure Shell (SSH)
- Bash Scripting

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

This *Installing, Configuring and Upgrading VMware vCloud Availability in the Cloud* document is updated with each release of the product or when necessary.

This table provides the update history of the *Installing, Configuring and Upgrading VMware vCloud Availability in the Cloud* document.

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7 MAY 2019</td>
<td>Added the following topics:</td>
</tr>
<tr>
<td></td>
<td>- Configure VMware vCloud Availability with a Renewed vCloud Director Endpoint or Certificate</td>
</tr>
<tr>
<td></td>
<td>- Free up Disk Space on the vCloud Availability Appliance</td>
</tr>
<tr>
<td></td>
<td>Updated the information in the following topics:</td>
</tr>
<tr>
<td></td>
<td>- VMware vCloud Availability Network Port Configuration</td>
</tr>
<tr>
<td></td>
<td>- Configure VMware vCloud Availability with a Renewed Lookup Service Certificate on a Platform Services Controller</td>
</tr>
<tr>
<td>18 APR 2019</td>
<td>Added the following topics:</td>
</tr>
<tr>
<td></td>
<td>- vCloud Availability Management Endpoints</td>
</tr>
<tr>
<td></td>
<td>- Regenerate a Self-Signed Certificate</td>
</tr>
<tr>
<td></td>
<td>- Upload a CA-Signed Certificate</td>
</tr>
<tr>
<td></td>
<td>- Replacing vCloud Availability Services Certificates</td>
</tr>
<tr>
<td></td>
<td>Updated the information in the following topics:</td>
</tr>
<tr>
<td></td>
<td>- VMware vCloud Availability Network Port Configuration</td>
</tr>
<tr>
<td></td>
<td>- Replace the Certificate of the vCloud Availability vApp Replication Manager Service</td>
</tr>
<tr>
<td></td>
<td>- Replace the Certificate of the vCloud Availability Replication Manager Service</td>
</tr>
<tr>
<td></td>
<td>- Replace the Certificate of the vCloud Availability Replicator Service</td>
</tr>
<tr>
<td></td>
<td>- Replace the Certificate of the vCloud Availability Tunnel Service</td>
</tr>
<tr>
<td>11 APR 2019</td>
<td>Initial release.</td>
</tr>
</tbody>
</table>
Overview of VMware vCloud Availability

The VMware vCloud Availability solution provides replication and failover capabilities for vCloud Director and vCenter Server workloads at both VM and vApp level.

The service operates through a VMware Cloud Provider Program, and depending on the installation type, it provides recovery for cloud and on-premises environments. The VMware vCloud Availability provides:

- Replication management and monitoring of replications from and to a cloud site.
- Failback recovered in the cloud workloads to the on-premises site.
- Migration of protected VMs in the cloud site back to the on-premises appliance.
- Self-service protection and failover workflows per virtual machine (VM).
- Single installation package as a Photon-based virtual appliance.
- The capability of each deployment to serve as both source and recovery vCloud Director instance (site). There are no dedicated source and destination sites.
- Symmetrical replication flow that can be started from either the source or the recovery vCloud Director site.
- Replication and recovery of vApps and VMs between vCloud Director sites.
- Using a single-site vCloud Availability installation, you can migrate vApps and VMs between Virtual Data Centers that belong to a single vCloud Director Organization.
- Built-in Secure Tunneling requires no incoming open ports on the on-premises site.
- Integration with existing vSphere environments.
- Multi-tenant support.
- Built-in encryption or encryption and compression of replication traffic.
- Support for multiple vCenter Server and ESXi versions.

This chapter includes the following topics:

- Cloud Deployment Architecture
- VMware vCloud Availability Services
Cloud Deployment Architecture

The cloud deployment architecture of the VMware vCloud Availability solution relies on symmetrical replication operations between cloud environments.

In a single cloud environment, the vCloud Availability Replicator, the vCloud Availability Replication Manager, the vCloud Availability vApp Replication Manager, and the vCloud Availability Tunnel operate together to support the 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.

Test and Development Deployment

For test and development purposes, you can employ the simplest architecture where all four VMware vCloud Availability services are deployed and configured on a single appliance.
The components with no color in the following diagrams represent existing components in the vCloud Director environments. The remaining colored cells represent VMware vCloud Availability services that you deploy during VMware vCloud Availability installation and configuration procedures.
Production Deployment

For production deployments, you deploy and configure a vCloud Availability Tunnel appliance and an appliance that hosts the vCloud Availability vApp Replication Manager, and vCloud Availability Replication Manager services. You deploy and configure dedicated vCloud Availability Replicator appliance or appliances.

VMware vCloud Availability Services

VMware vCloud Availability solution is composed of services that can coexist in the same virtual appliance or in dedicated appliances.
Table 2-1. vCloud Availability Services Definitions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud Availability Replicator</td>
<td>Exposes the low-level HBR primitives as REST APIs.</td>
</tr>
<tr>
<td>vCloud Availability Replication Manager</td>
<td>A management service operating on the vCenter Server level. It understands the vCenter Server level concepts for starting the replication workflow for the virtual machines.</td>
</tr>
<tr>
<td>vCloud Availability vApp Replication Manager with embedded vCloud Availability Portal</td>
<td>Provides the main interface for the cloud and on-prem replication operations. It understands the vCloud Director level concepts and works with vApps and virtual machines. The embedded vCloud Availability Portal provides tenants (vCloud Availability Portal) and service providers (vCloud Availability Service Provider Portal) with a graphic user interface to facilitate the management of the VMware vCloud Availability solution. It also provides overall system and workload information.</td>
</tr>
<tr>
<td>vSphere Replication Server and vSphere Replication Filter</td>
<td>The replication server receives and records delta information for each replicated virtual machine. During the cloud-to-cloud replication, delta information is sent from one ESXi host to another ESXi host.</td>
</tr>
<tr>
<td>vCloud Availability Tunnel</td>
<td>Simplifies provider networking setup by channeling all incoming and outgoing traffic for a site through a single point - the vCloud Availability Tunnel appliance. The traffic is both management and monitoring for the replication data (LWD traffic).</td>
</tr>
<tr>
<td>Lightweight Delta Protocol Service (LWD Proxy)</td>
<td>The proprietary replication protocol service ensures that each incoming replication data stream comes only from the authorized source LWD Proxy instance, and each outgoing replication data stream goes only to an authorized destination LWD Proxy instance.</td>
</tr>
</tbody>
</table>

Table 2-2. Additional Services Definitions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud Director</td>
<td>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.</td>
</tr>
<tr>
<td>VMware Platform Services Controller®</td>
<td>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.</td>
</tr>
</tbody>
</table>

The VMware vCloud Availability services provide a management interface for configuration and administration purposes.

You perform initial configuration of VMware vCloud Availability services by using the vCloud Availability Replication Manager, vCloud Availability Replicator, and vCloud Availability vApp Replication Manager management interfaces.

You cannot access the vCloud Availability Portal before finishing the initial VMware vCloud Availability configuration.

You can find the configuration and log files for the VMware vCloud Availability services at the following locations.
Table 2-3. Configuration Files Location

<table>
<thead>
<tr>
<th>Service</th>
<th>Default Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud Availability Replication Manager</td>
<td>/opt/vmware/h4/manager/config/application.properties</td>
</tr>
<tr>
<td>vCloud Availability Replicator</td>
<td>/opt/vmware/h4/replicator/config/application.properties</td>
</tr>
<tr>
<td>vCloud Availability vApp Replication Manager</td>
<td>/opt/vmware/h4/cloud/config/application.properties</td>
</tr>
<tr>
<td>vCloud Availability Tunnel</td>
<td>/opt/vmware/h4/tunnel/config/application.properties</td>
</tr>
</tbody>
</table>

Table 2-4. Log Files Location

<table>
<thead>
<tr>
<th>Service</th>
<th>Default Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud Availability Replication Manager</td>
<td>/opt/vmware/h4/manager/log/manager.log</td>
</tr>
<tr>
<td>vCloud Availability Replicator</td>
<td>/opt/vmware/h4/replicator/log/replicator.log</td>
</tr>
<tr>
<td>vCloud Availability vApp Replication Manager</td>
<td>/opt/vmware/h4/cloud/log/cloud.log</td>
</tr>
<tr>
<td>vCloud Availability Tunnel</td>
<td>/opt/vmware/h4/tunnel/log/tunnel.log</td>
</tr>
</tbody>
</table>
Installing and Configuring VMware vCloud Availability

You first deploy the VMware vCloud Availability services and then perform initial configuration of each service so that all of the solution components are visible and able to connect.

This chapter includes the following topics:

- VMware vCloud Availability Requirements
- Deploy VMware vCloud Availability Services Using the vSphere Client
- Deploying VMware vCloud Availability Services with OVF Tool
- Configure vCloud Availability Services
- Configuring the Customer Experience Improvement Program

VMware vCloud Availability Requirements

Before you start deploying and configuring VMware vCloud Availability services, verify that your cloud environment meets the specific requirements.

VMware vCloud Availability Users and Services Requirements

Before you start deploying and configuring vCloud Availability, verify that the users and the services comply with the following requirements.

vCloud Availability vApp Replication Manager Users Requirements

The vCloud Availability vApp Replication Manager distinguishes between admin users and regular users. To start a session with administrator privileges, the credentials you enter for both of the vCloud Director sites must belong to the ADMINISTRATORS or VRADMINISTRATORS group. For example, the Administrator@vSphere.local single sign-on user you enter when logging into the management portal, is a member of the ADMINISTRATORS group.

VMware vCloud Availability User Sessions Requirements

Each vCloud Availability user session is guaranteed to have a vCloud Director user and vCloud Director organization associated with the session.
To manage VMware vCloud Availability objects and the local vCloud Availability vApp Replication Manager appliance as a service provider, you start a user session as a vCloud Director **system administrator** by using vCloud Director user name and password. **System administrator** users can manage any local and monitor any remote VMware vCloud Availability inventory object. To manage VMware vCloud Availability objects in the remote sites, you must authenticate as a system administrator to the remote site.

To perform disaster recovery operations and manage local VMware vCloud Availability objects as a tenant user, you start a user session as a vCloud Director organization administrator by using vCloud Director credentials. As an organization administrator, you can perform disaster recovery operations in the local site, you can manage any local VMware vCloud Availability object, and can monitor any remote VMware vCloud Availability object that belongs to the respective vCloud Director organization. To manage remote VMware vCloud Availability objects, you must authenticate to the corresponding remote organization.

For more information about authenticating to remote sites, see the *Authenticate to Remote Sites as a Service Provider* and *Authenticate to Remote Sites as a Tenant* topics in vCloud Availability User's Guide.

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

**Table 3-1. vCloud Availability vApp Replication Manager Replication Operations with Required Sessions**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Incoming Replication</th>
<th>Outgoing Replication</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Required Session on</td>
<td>Required Session on</td>
</tr>
<tr>
<td></td>
<td>Source Site</td>
<td>Destination Site</td>
</tr>
<tr>
<td>start</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>stop</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>reconfigure</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>failover</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>migrate</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>sync</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>pause</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>resume</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>reverse</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>failover test</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>failover test cleanup</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Services Connectivity**

- The vCloud Availability vApp Replication Manager must have TCP access to vCloud Director, vCloud Availability Replication Manager, vCenter Server, or PSC (depending on where the Lookup Service is hosted).
The vCloud Availability Replication Manager must have TCP access to the Lookup Service and all the vCloud Availability Replicator appliances in both local, and remote sites.

The vCloud Availability Replicator must have TCP access to the vCloud Availability Replication Manager, vCenter Server, and the Lookup Service.

For information on network requirements, see VMware vCloud Availability Network Port Configurations.

**Supported Topologies**

The resource vCenter Server instances within a vCloud Director site must be within the same single sign-on domain. All vCloud Availability Replicator, vCloud Availability Replication Manager, vCloud Availability vApp Replication Manager, and vCloud Availability Tunnel appliances within the respective site must be configured with that same single sign-on domain.

For information about the interoperability between vCloud Availability and vCenter Server, see VMware Product Interoperability Matrices.

**VMware vCloud Availability Deployment Requirements**

Before you start deploying and configuring VMware vCloud Availability services, verify that your environment complies with the following requirements.

### Deployment Types and Hardware Requirements

You install all VMware vCloud Availability services in a cloud site by using a single installation OVA package for cloud deployment. Use the same OVA package to deploy vCloud Availability appliances in all your cloud sites.

Depending on your scale and deployment goals, you can select various deployment types. The following table describes the different deployment types and hardware requirements.

**Table 3-2. VMware vCloud Availability Cloud Deployment Types**

<table>
<thead>
<tr>
<th>Deployment Type</th>
<th>Description</th>
<th>Hardware Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Combined Appliance</td>
<td>All-in-one deployment type that is suitable for testing, evaluation, and</td>
<td>4 vCPUs, 6 GB RAM, 10</td>
</tr>
<tr>
<td></td>
<td>small-scale environments. Includes the following services:</td>
<td>GB Storage</td>
</tr>
<tr>
<td></td>
<td>• vCloud Availability Replication Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• vCloud Availability Replicator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• vCloud Availability vApp Replication Manager with embedded</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vCloud Availability Portal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• vCloud Availability Tunnel</td>
<td></td>
</tr>
<tr>
<td></td>
<td>You deploy a single appliance with all VMware vCloud Availability services</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ready for configuration.</td>
<td></td>
</tr>
<tr>
<td>Cloud Replication</td>
<td>A single appliance that contains the following services:</td>
<td>2 vCPUs, 4 GB RAM, 10</td>
</tr>
<tr>
<td></td>
<td>• vCloud Availability Replication Manager</td>
<td>GB Storage</td>
</tr>
<tr>
<td></td>
<td>• vCloud Availability vApp Replication Manager with embedded</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vCloud Availability Portal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>You deploy it to configure replications from and to vCloud Director.</td>
<td></td>
</tr>
</tbody>
</table>
Table 3-2. VMware vCloud Availability Cloud Deployment Types (Continued)

<table>
<thead>
<tr>
<th>Deployment Type</th>
<th>Description</th>
<th>Hardware Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Replicator</td>
<td>Deploys a dedicated vCloud Availability Replicator appliance suitable for large-scale environments. It handles replication traffic for a site. You can have more than one replicator per site.</td>
<td>4 vCPUs&lt;br&gt;6 GB RAM&lt;br&gt;10 GB Storage</td>
</tr>
<tr>
<td>Cloud Tunnel</td>
<td>Deploys a vCloud Availability Tunnel appliance.</td>
<td>2 vCPUs&lt;br&gt;2 GB RAM&lt;br&gt;10 GB Storage</td>
</tr>
</tbody>
</table>

You use a single installation OVA package for deployment of vCloud Availability on-premises. When installing the on-prem OVA package, you are not present with a choice of a deployment type. Only vCloud Availability replicator appliance deploys on-premises.

Other Deployment Requirements

- If your ESXi hosts have more than one vmkernel network interface (vmk), make sure that vSphere Replication NFC Traffic is enabled. This setting is required for routing the replication traffic.

  An ESXi host may have a dedicated vmk for replication traffic in its own broadcast domain. If vSphere Replication NFC Traffic is enabled on the dedicated vmk interface, the vCloud Availability Replicator must be connected to the same broadcast domain. The vSphere Replication NFC Traffic cannot be routed if it is not in the default TCP stack.

  If vSphere Replication NFC Traffic is not enabled, you might get timeout errors during the replication setup or reconfiguration. For more information about enabling vSphere Replication NFC Traffic, see Set Up a VMkernel Adapter for vSphere Replication Traffic on a Target Host in the VMware vSphere Replication Administration Guide.

- You deploy a vCloud Availability vApp Replication Manager per vCloud Director server group (installation). Within the server group there might be, for example, a vCD cell and a resource vCenter Server with at least one ESXi host.

- The VMware vCloud Availability services perform a host name certificate verification. Therefore, it is expected that the CommonName or at least one of the entries in the Subject Alternative Name of the vCloud Director certificate matches the vCloud Director address (FQDN or IP) that is used during vCloud Director registration.

VMware vCloud Availability Network Port Configuration

To ensure VMware vCloud Availability services can communicate within a single site and between source and destination sites, make sure that the required network ports are opened.
The following diagram shows the data flow between network ports and the ports numbers through a typical deployment on the cloud sites.

The following table shows the firewall rules required in a cloud site for VMware vCloud Availability services communication.
### Table 3-3. Firewall Rules for Local Site Connection

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud Availability Replicator</td>
<td>ESXi Hosts</td>
<td>90</td>
<td>TCP and UDP</td>
<td>Used by the vCloud Availability Replicator service for replication traffic to the destination ESXi hosts.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>80</td>
<td>TCP</td>
<td></td>
</tr>
<tr>
<td>vCloud Availability Replicator</td>
<td>VMware Platform Services Controller®</td>
<td>44</td>
<td>TCP</td>
<td>Used for single sign-on and Lookup Service communication when vSphere 5.5 or later is used in the respective site.</td>
</tr>
<tr>
<td>vCloud Availability Replicator</td>
<td>vCenter Server</td>
<td>44</td>
<td>TCP</td>
<td>Used by the local vCloud Availability vApp Replication Manager service or the vCloud Availability Replicator service for communication with the local vCenter Server.</td>
</tr>
<tr>
<td>vCloud Availability Replicator</td>
<td>vCloud Availability vApp Replication Manager</td>
<td>80</td>
<td>TCP</td>
<td>Used for vCloud Availability vApp Replication Manager management from the vCloud Availability Replicator.</td>
</tr>
<tr>
<td>vCloud Availability Replicator</td>
<td>vCloud Availability Tunnel</td>
<td>80</td>
<td>TCP</td>
<td>Used for vCloud Availability Tunnel management from the vCloud Availability Replicator.</td>
</tr>
<tr>
<td>vCloud Availability vApp Replication Manager</td>
<td>VMware Platform Services Controller®</td>
<td>44</td>
<td>TCP</td>
<td>Used for single sign-on and Lookup Service communication when vSphere 5.5 or later is used in the respective site.</td>
</tr>
<tr>
<td>vCloud Availability vApp Replication Manager</td>
<td>vCloud Director</td>
<td>44</td>
<td>TCP</td>
<td>Used for vCloud Director management from the vCloud Availability vApp Replication Manager.</td>
</tr>
<tr>
<td>vCloud Availability vApp Replication Manager</td>
<td>vCloud Availability Replicator</td>
<td>80</td>
<td>TCP</td>
<td>Used for vCloud Availability Replicator management from the vCloud Availability vApp Replication Manager.</td>
</tr>
<tr>
<td>vCloud Availability vApp Replication Manager</td>
<td>vCloud Availability Tunnel</td>
<td>80</td>
<td>TCP</td>
<td>Used for vCloud Availability Tunnel management from the vCloud Availability vApp Replication Manager.</td>
</tr>
<tr>
<td>vCloud Availability Tunnel</td>
<td>vCloud Availability Replicator</td>
<td>80</td>
<td>TCP</td>
<td>Used for vCloud Availability Replicator management from the vCloud Availability Tunnel.</td>
</tr>
<tr>
<td>vCloud Availability Tunnel</td>
<td>vCloud Availability vApp Replication Manager</td>
<td>80</td>
<td>TCP</td>
<td>Used for vCloud Availability vApp Replication Manager service management from the vCloud Availability Tunnel appliance.</td>
</tr>
</tbody>
</table>
### Table 3-3. Firewall Rules for Local Site Connection (Continued)

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud Availability Tunnel</td>
<td>VMware Platform Services Controller</td>
<td>44</td>
<td>TCP</td>
<td>Used for VMware Platform Services Controller communication management from the vCloud Availability vApp Replication Manager and vCloud Availability Replicator.</td>
</tr>
<tr>
<td>ESXi Hosts</td>
<td>vCloud Availability Replicator</td>
<td>31</td>
<td>TCP</td>
<td>Used by the ESXi hosts for replication traffic to the destination vCloud Availability Replicator service.</td>
</tr>
<tr>
<td>Firewall</td>
<td>vCloud Availability Tunnel</td>
<td>80</td>
<td>TCP</td>
<td>Used for redirecting external traffic management to the vCloud Availability Tunnel service.</td>
</tr>
</tbody>
</table>

The following table shows the port configuration required for an external communication.

### Table 3-4. Firewall Rules for External Communication

<table>
<thead>
<tr>
<th>Original Destination</th>
<th>Translated Destination</th>
<th>Original Destination Port</th>
<th>Translated Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Network/Up link Interface</td>
<td>vCloud Availability Tunnel</td>
<td>443</td>
<td>8048</td>
<td>TCP</td>
<td>Used for incoming replication management and replication data traffic from the public network to the vCloud Availability Tunnel. The tunnel then reroutes the traffic to the local services.</td>
</tr>
</tbody>
</table>

### vCloud Availability Management Endpoints

According to the deployment method, use the following management ports when accessing each of the vCloud Availability services.

**Combined Appliance**

The following table lists the management interface addresses with ports that the vCloud Availability services use when deployed and configured on a single combined appliance.

### Table 3-5. Services Management Endpoints on a Combined Appliance

<table>
<thead>
<tr>
<th>Component</th>
<th>Management Endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud Availability vApp Replication Manager</td>
<td><a href="https://Appliance%E2%80%93IP%E2%80%93Address/ui/admin">https://Appliance–IP–Address/ui/admin</a></td>
</tr>
<tr>
<td>vCloud Availability Replication Manager</td>
<td><a href="https://Appliance%E2%80%93IP%E2%80%93Address:8441/ui/admin">https://Appliance–IP–Address:8441/ui/admin</a></td>
</tr>
</tbody>
</table>
Table 3-5. Services Management Endpoints on a Combined Appliance (Continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Management Endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud Availability Replicator</td>
<td><a href="https://Appliance-IP-Address:8440/ui/admin">https://Appliance-IP-Address:8440/ui/admin</a></td>
</tr>
<tr>
<td>vCloud Availability Tunnel</td>
<td><a href="https://Appliance-IP-Address:8442/ui/admin">https://Appliance-IP-Address:8442/ui/admin</a></td>
</tr>
</tbody>
</table>

Dedicated Appliance

The following table lists the management interface addresses with ports that the vCloud Availability services use when each is deployed and configured on a dedicated appliance.

Table 3-6. Services Management Endpoints on Dedicated Appliances

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Component</th>
<th>Management Endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>vCloud Availability Replication Manager</td>
<td><a href="https://Replication-Management-Appliance-IP-Address:8441/ui/admin">https://Replication-Management-Appliance-IP-Address:8441/ui/admin</a></td>
</tr>
<tr>
<td>Cloud Replicator</td>
<td>vCloud Availability Replicator</td>
<td><a href="https://Replicator-Appliance-IP-Address/ui/admin">https://Replicator-Appliance-IP-Address/ui/admin</a></td>
</tr>
<tr>
<td>Cloud Tunnel</td>
<td>vCloud Availability Tunnel</td>
<td><a href="https://Tunnel-Appliance-IP-Address/ui/admin">https://Tunnel-Appliance-IP-Address/ui/admin</a></td>
</tr>
</tbody>
</table>

Deploy VMware vCloud Availability Services Using the vSphere Client

You install all VMware vCloud Availability services by using a single installation OVA package.

Use the same OVA package to deploy VMware vCloud Availability appliances in all your cloud sites.

Prerequisites

- Download the installation vCloud Availability 3.0 Appliance for Cloud Providers (vCloud-Availability-release_number-xxx-build_number_OVF10.ova) file that contains all VMware vCloud Availability appliances binaries.
- Verify that you installed the Client Integration Plug-in so that you can use the Deploy OVF Template option in the vSphere Client.

Procedure

1. Log in to the vSphere Client.
2. Right-click the target location, for example data center, folder, cluster, resource pool, or host, where you want to deploy the VMware vCloud Availability services.
3. From the drop-down menu, select Deploy OVF Template.

The Deploy OVF Template wizard opens.
4 In the Select source page, browse to the vCloud Availability 3.0 Appliance for Cloud Providers (VMware-vCloud-Availability-release_number-xxx-build_number_OVF10.ova) file location and click Next.

5 Review the OVF template details and click Next.

6 Accept the terms in the license agreement and click Next.

7 Enter a name for the deployed appliance.

8 Select a data center, or data center folder that contains the host, or cluster on which you want to deploy the appliance, and click Next.

9 Select a deployment type and click Next.

Table 3-7. VMware vCloud Availability Deployment Types

<table>
<thead>
<tr>
<th>Deployment Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| Combined Appliance      | All-in-one deployment type that is suitable for testing, evaluation, and small-scale environments. Includes the following services:  
|                         |   vCloud Availability Replication Manager                                                      |
|                         |   vCloud Availability Replicator                                                               |
|                         |   vCloud Availability vApp Replication Manager with embedded vCloud Availability Portal         |
|                         |   vCloud Availability Tunnel                                                                   |
|                         | You deploy a single appliance with all VMware vCloud Availability services ready for configuration. |
| Cloud Replication Manager| Deploys a single appliance that contains the following services:  
|                         |   vCloud Availability Replication Manager                                                      |
|                         |   vCloud Availability vApp Replication Manager with embedded vCloud Availability Portal         |
| Cloud Replicator        | Deploys a dedicated vCloud Availability Replicator appliance.                                   |
| Cloud Tunnel            | Deploys a dedicated vCloud Availability Tunnel appliance.                                       |

10 Select a host, or cluster as a destination on which you want the appliance to run, and click Next.

11 Select the virtual disk format and the storage policy for the appliance from the drop-down menu.

12 (Optional) Configure the network settings and click Next.
13 Customize the deployment properties of the VMware vCloud Availability appliance and click **Next**.

a  Enter and confirm the password for the **root** user for the appliance.

You can use this password only once and must change the **root** user password after you log in for the first time.

b  Select the **Enable SSH** check box.

c  In the **NTP Server** section, enter the NTP server address that the appliance uses.

**Important** Make sure that vCenter Server, ESXi, vCloud Director, the Platform Services Controller, and all VMware vCloud Availability appliances use the same NTP server.

14 (Optional) Review all the settings and select **Power on after deployment**.

15 To begin the OVA installation process, click **Finish**.

The **Recent Tasks** page shows the status for initializing the OVF deployment on the target host.

**What to do next**

If you did not select the **Enable SSH** option during deployment, you can reconfigure the appliance. For more information, see [https://kb.vmware.com/s/article/59197](https://kb.vmware.com/s/article/59197).

---

**Deploying VMware vCloud Availability Services with OVF Tool**

To deploy VMware vCloud Availability services by using the VMware OVF Tool, define deployment parameters and run a deployment script.

**Defining OVF Tool Parameters for VMware vCloud Availability Services Deployment**

Before you deploy VMware vCloud Availability services, you must define the specific OVF Tool parameters for deployment.

The following table describes the parameters you must define when deploying VMware vCloud Availability services by using the OVF Tool scripts.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OVA</td>
<td>The local client path to the installation OVA package. For example, OVA=&quot;local_client_path/VMware-vCloud-Availability-release_number-xxx-build_number_OVF10.ova&quot;.</td>
</tr>
<tr>
<td>VMNAME</td>
<td>Virtual machine name.</td>
</tr>
<tr>
<td>VSPHERE_DATASTORE</td>
<td>The VSPHERE_DATASTORE value is the datastore name as it is displayed in the vSphere Web Client.</td>
</tr>
<tr>
<td>VSPHERE_NETWORK</td>
<td>The name of the network on which the appliance to run.</td>
</tr>
<tr>
<td>VSPHERE_ADDRESS</td>
<td>The IP address of the vCenter Server instance on which you deploy the appliance.</td>
</tr>
<tr>
<td>VSPHERE_USER</td>
<td>User name for a vCenter Server administrator.</td>
</tr>
</tbody>
</table>
Deploy VMware vCloud Availability Services Using the OVF Tool

To deploy VMware vCloud Availability services, define deployment parameters in your OVF Tool user session, and run the deployment script.

You install all VMware vCloud Availability services by using a single installation OVA package. Use the same OVA package to deploy VMware vCloud Availability appliances in all your cloud sites.

**Prerequisites**

- Download the installation vCloud Availability 3.0 Appliance for Cloud Providers (VMware-vCloud-Availability-release_number-xxx-build_number_OVF10.ova) file that contains all VMware vCloud Availability appliances binaries.
- Verify that you have the OVF Tool installed and configured.

**Procedure**

1. Open an SSH session to the server where the OVF Tool is installed and configured.
2. Define deployment parameters in the OVF Tool console by running the following commands.

```bash
# VMNAME="Name-to-be-Assigned-to-the-VM"
# VSPHERE_DATASTORE="vSphere-datastore"
# VSPHERE_NETWORK="VM-Network"
# OVA="local_client_path/VMware-vCloud-Availability-release_number-xxx-build_number_OVF10.ova"
# VSPHERE_USER="vCenter-Server-admin-user"
# VSPHERE_USER_PASSWORD="vCenter-Server-admin-user-password"
```
3 Deploy a VMware vCloud Availability appliance.

The value you set for the \(--deploymentOption\) argument controls the deployment type for the appliance you deploy. The following table lists the deployment types and the corresponding values for the OVF Tool \(--deploymentOption\) argument.

### Table 3-8. VMware vCloud Availability Deployment Types and OVF Tool Deployment Options

<table>
<thead>
<tr>
<th>Deployment types</th>
<th>OVF Tool Deployment Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Combined Appliance | combined | All-in-one deployment type that is suitable for testing, evaluation, and small-scale environments. Includes the following services:  
- vCloud Availability Replication Manager  
- vCloud Availability Replicator  
- vCloud Availability vApp Replication Manager with embedded vCloud Availability Portal  
- vCloud Availability Tunnel  
You deploy a single appliance with all VMware vCloud Availability services ready for configuration. |
| Cloud Replication Management | cloud | Deploys a single appliance that contains the following services:  
- vCloud Availability Replication Manager  
- vCloud Availability vApp Replication Manager with embedded vCloud Availability Portal  
Cloud Replicator | replicator | Deploys a dedicated vCloud Availability Replicator appliance. |
| Cloud Tunnel | tunnel | Deploys a dedicated vCloud Availability Tunnel appliance. |

The following example command deploys a **Combined** VMware vCloud Availability appliance and sets a static IP address.

```
# ./ovftool/ovftool --name="${VMNAME}" --datastore="${VSPHERE_DATASTORE}" --acceptAllEulas  
--powerOn --X:enableHiddenProperties --X:injectOvfEnv --X:waitForIp  
--ipAllocationPolicy=fixedPolicy --deploymentOption=combined --machineOutput --noSSLVerify  
--overwrite --powerOffTarget "--net:VM Network=${VSPHERE_NETWORK}" --diskMode=thin  
--prop:guestinfo.cis.appliance.root.password='Your-Root-Password'  
--prop:guestinfo.cis.appliance.ssh.enabled=True  
--prop:guestinfo.cis.appliance.net.ntp='Your-ntp-server-ip-address'  
--prop:vami.DNS.VMware_vCloud_Availability='Your-DNS-Server-Address'  
--prop:vami.domain.VMware_vCloud_Availability='Your-Domain-Name'  
--prop:vami.gateway.VMware_vCloud_Availability='Your-Gateway-IP-Address'  
--prop:vami.ip0.VMware_vCloud_Availability='IP-to-be-Assigned-to-the-Appliance'  
--prop:vami.netmask0.VMware_vCloud_Availability='Your-Netmask-Address'  
--prop:vami.searchpath.VMware_vCloud_Availability='Your-Search-Path-Address'  
"${OVA}" "vi://${VSPHERE_USER}:${VSPHERE_USER_PASSWORD}@${VSPHERE_ADDRESS}${VSPHERE_LOCATOR}"```

The system prints the IP address of the VMware vCloud Availability appliance.
Configure vCloud Availability Services

To configure the VMware vCloud Availability solution, you perform an initial configuration of the vCloud Availability Replication Manager, vCloud Availability vApp Replication Manager, vCloud Availability Replicator and vCloud Availability Tunnel, register the services within a single site, then pair your cloud sites.

After you configure all VMware vCloud Availability services in one or more cloud sites, you can log in to the vCloud Availability Portal at https://vApp-Replication-Manager-IP-address/ui/login. Tenant user names are in the user@org format.

A best practice is to configure all services in one site, then register the vCloud Availability Replicator with the vCloud Availability Replication Manager in the same site. Then perform the initial configuration and registration on the second site.

During the configuration of a vCloud Availability service, you can open that service management interface, go to the System Monitoring tab and validate if the setup of the particular entry completed successfully. Red entries indicate incomplete setup. When services are configured successfully, all entries are green in the System Monitoring tab in the vCloud Availability vApp Replication Manager service management interface.

Procedure

1. **Configure a vCloud Availability Replication Manager**
   - To configure a vCloud Availability Replication Manager, register the vCloud Availability Replication Manager appliance to a Lookup service.

2. **Configure a vCloud Availability vApp Replication Manager**
   - To configure a vCloud Availability vApp Replication Manager, enter a site name to be used as an identifier and register the vCloud Availability vApp Replication Manager to a Lookup service. Then set up the vCloud Availability Replication Manager and the vCloud Director.

3. **Configure vCloud Availability Replicator Appliance**
   - To configure the vCloud Availability Replicator, you first register the vCloud Availability Replicator appliance to a Lookup service. Then you add the vCloud Availability Replicator to the vCloud Availability Replication Manager.

4. **Register a vCloud Availability Replicator with a vCloud Availability Replication Manager in the Same Site**
   - You register a vCloud Availability Replicator to a vCloud Availability Replication Manager in the same site, so that the two services can work together.

5. **Configure vCloud Availability Tunnel**
   - You configure the vCloud Availability Tunnel to allow for remote sites to communicate with the tunnel on its public port.
Enable vCloud Availability Tunnel

You enable vCloud Availability Tunnel service by using the vCloud Availability vApp Replication Manager and register the vCloud Availability Tunnel connectivity in all your cloud sites before pairing an on-premise site with your cloud site.

Restart Services

You restart all VMware vCloud Availability services available in a single appliance in the cloud site. Services that are in dedicated appliances are restarted separately for each appliance.

Configure a vCloud Availability Replication Manager

To configure a vCloud Availability Replication Manager, register the vCloud Availability Replication Manager appliance to a Lookup service.

Procedure

1. In a Web browser, go to https://Replication-Management-Appliance-IP-Address:8441/ui/admin.
   The vCloud Availability Replication Manager service management interface login page opens.
2. If you are prompted for Client Certificate, click Cancel.
3. Log in by using the root user password that you set during the OVA deployment.
   The vCloud Availability Appliance Password window displays.
4. Change the initial root user password.
   a. Enter the initial root user password set during the OVA deployment.
   b. Enter and confirm a new password. Create a secured password with a minimum of eight characters and containing at least one of each of the following characters:
      - Lowercase: a b c
      - Uppercase: A B C
      - Numeric: 1 2 3
      - Special: & # %
   c. Click Apply.
      The Getting Started tab displays.
5. Navigate to the Configuration tab and click Edit against the Lookup service address entry.
   The Lookup Service Details window displays.
6. Enter a valid Lookup service address and click Apply.
   Enter the lookup service address in the following format https://Lookup-Service-IP-address:443/lookupservice/sdk.
7 To complete the configuration, accept the SSL certificate of the Lookup service.

8 Log out of the vCloud Availability Replication Manager.

What to do next
You can now perform an initial configuration of the vCloud Availability vApp Replication Manager.

**Configure a vCloud Availability vApp Replication Manager**

To configure a vCloud Availability vApp Replication Manager, enter a site name to be used as an identifier and register the vCloud Availability vApp Replication Manager to a Lookup service. Then set up the vCloud Availability Replication Manager and the vCloud Director.

**Procedure**

1 In a Web browser, go to https://Replication-Management-Appliance-IP-Address/ui/admin.
   The vCloud Availability vApp Replication Manager service management interface login page opens.

2 If you are prompted for Client Certificate, click Cancel.

3 Log in as root.
   You are redirected to the Getting Started tab.

4 Click Run initial setup wizard.
   The Initial Setup wizard displays.

5 Enter a Site name, optionally enter a Site Description, and click Next.
   Important Note the site name that you enter, as it is used as an identifier and cannot be changed later.

6 Enter the tunnel address for the Public API endpoint, optionally add description, and click Next.
   You can use the tunnel default port 8048.

7 Enter a valid Lookup service address, your single sign-on user name and password, and click Next.
   Enter the Lookup service address in the following format https://Lookup-Service-IP-address:443/lookupservice/sdk.

8 Accept the SSL certificate of the Lookup service.
9 Set up vCloud Director.
   a Select the configuration type.
      If you select Discover the vCloud Director Service address automatically, skip this step.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Discover the vCloud Director Service address automatically | By default, this option is selected. Use the option if the following configurations are present in your environment:  
   - vCloud Director is federated with a previously specified lookup service.  
   - There is only one registered vCloud Director in the lookup service.  
   - The single sign-on user belongs to the System administrator group in vCloud Director. |
| Enter details for the vCloud Director Service manually | Select this option, if your vCloud Director instance is not federated with a previously specified Lookup service or if multiple vCloud Director instances are registered to the Lookup service.               |

b Enter the vCloud Director URL in the following format: https://vCloud Director-IP-Address:443/api.

c Enter a vCloud Director System administrator user name and password, and click Next.
   For example administrator@system, where system is the name of the system organization of vCloud Director.

   The vCloud Director certificate details display.

d Accept the vCloud Director SSL certificate.

10 Enter a valid VMware vCloud Availability license key and click Next.

11 Select or deselect the Join the VMware Customer Experience Improvement Program check box to either join or leave the program and click Next.
   VMware’s Customer Experience Improvement Program provides VMware with information that enables VMware to improve its products and services, to fix problems, and to advise you on how best to deploy and use our products.
   You are redirected to the Ready To Complete page.

12 Review the vCloud Availability vApp Replication Manager configuration summary and click Finish.

13 (Optional) To check what other configurations are required to complete the vCloud Availability vApp Replication Manager service configuration successfully, select the System Monitoring tab, and locate the alerts.

What to do next
Add vCloud Availability Replicator instances and configure the settings for tunnel connectivity.
Configure vCloud Availability Replicator Appliance

To configure the vCloud Availability Replicator, you first register the vCloud Availability Replicator appliance to a Lookup service. Then you add the vCloud Availability Replicator to the vCloud Availability Replication Manager.

Procedure

1. Log in to the vCloud Availability Replicator service management interface.
   a. Open a Web browser and depending on your deployment type, navigate to the following management endpoint.

<table>
<thead>
<tr>
<th>Deployment type</th>
<th>Management Endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Combined Appliance</td>
<td><a href="https://Appliance-IP-Address:8440/ui/admin">https://Appliance-IP-Address:8440/ui/admin</a></td>
</tr>
<tr>
<td>Cloud Replicator</td>
<td><a href="https://Replicator-Appliance-IP-Address/ui/admin">https://Replicator-Appliance-IP-Address/ui/admin</a></td>
</tr>
</tbody>
</table>

   b. Log in by using your root user credentials.

2. Change the initial root user password.
   a. Enter the initial root user password set during the OVA deployment.
   b. Enter and confirm a new password.
      Create a secured password with a minimum of eight characters and containing at least one of each of the following characters:
      - Lowercase: a b c
      - Uppercase: A B C
      - Numeric: 1 2 3
      - Special: & # %
   c. Click Apply.
      The Getting Started tab displays.

3. Click Configure Lookup Service.
   The Lookup Service Details window displays.

4. Enter the Lookup service address and click Apply.
   Enter the Lookup service address in the following format https://Lookup-Service-IP-address:443/lookupservice/sdk.

5. Accept the SSL certificate of the Lookup service and log out.

What to do next
You can now register the vCloud Availability Replicator with the vCloud Availability Replication Manager.
Register a vCloud Availability Replicator with a vCloud Availability Replication Manager in the Same Site

You register a vCloud Availability Replicator to a vCloud Availability Replication Manager in the same site, so that the two services can work together.

Prerequisites

Verify that you have configured a vCloud Availability Replicator appliance and a vCloud Availability Replication Manager appliance in the same site.

Procedure

1. In a Web browser, go to https://Replication-Management-Appliance-IP-Address:8441/ui/admin.

   The vCloud Availability Replication Manager service management interface login page opens.

2. Log in as root.

3. In the Replicators tab, click New.

   The New Replicator wizard displays.

4. Enter the vCloud Availability Replicator details and click Add.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site</td>
<td>Select the site where the vCloud Availability Replicator is deployed.</td>
</tr>
<tr>
<td>Description</td>
<td>You can optionally add a description for the vCloud Availability Replicator</td>
</tr>
<tr>
<td></td>
<td>that you are registering.</td>
</tr>
<tr>
<td>API URL</td>
<td>The vCloud Availability Replicator API endpoint address.</td>
</tr>
<tr>
<td>Appliance Password</td>
<td>The root user password for the vCloud Availability Replicator appliance.</td>
</tr>
<tr>
<td>SSO User Name</td>
<td>A user assigned with administrative privileges for the local site single sign-on</td>
</tr>
<tr>
<td></td>
<td>domain, for example <a href="mailto:Administrator@VSPHERE.LOCAL">Administrator@VSPHERE.LOCAL</a>.</td>
</tr>
<tr>
<td>SSO Password</td>
<td>The password for the administrative user.</td>
</tr>
</tbody>
</table>

   If you enter the vCloud Availability Replicator FQDN, for example eu-2.replicator.com, the vCloud Availability Replication Manager service management interface displays the vCloud Availability Replicator appliance IP address instead of the FQDN.

5. To complete the registration, accept the vCloud Availability Replicator SSL certificate.

   When the status icon turns green in the Replicators administration pane, the new vCloud Availability Replicator is added to the vCloud Availability Replication Manager.

Configure vCloud Availability Tunnel

You configure the vCloud Availability Tunnel to allow for remote sites to communicate with the tunnel on its public port.
Procedure

1. Log in to the vCloud Availability Tunnel service management interface.
   a. Open a Web browser and depending on your deployment type, navigate to the following management endpoint.

<table>
<thead>
<tr>
<th>Deployment type</th>
<th>Management Endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Combined Appliance</td>
<td><a href="https://Appliance-IP-Address:8442.ui/admin">https://Appliance-IP-Address:8442.ui/admin</a></td>
</tr>
<tr>
<td>Cloud Tunnel Appliance</td>
<td><a href="https://Tunnel-Appliance-IP-Address/ui/admin">https://Tunnel-Appliance-IP-Address/ui/admin</a></td>
</tr>
</tbody>
</table>

   b. Log in by using your root user credentials.

2. Change the initial root user password.
   a. Enter the initial root user password set during the OVA deployment.
   b. Enter and confirm a new password.

      Create a secured password with a minimum of eight characters and containing at least one of each of the following characters:

      - Lowercase: a b c
      - Uppercase: A B C
      - Numeric: 1 2 3
      - Special: & # %

   c. Click Apply.

      The Getting Started tab displays.

3. On the Configuration tab, click Edit against the Lookup service address entry.

   The Lookup Service Details window displays.

4. Enter the lookup service address and click Apply.

   Enter the lookup service address in the https://Lookup-Service-IP-address:443/lookupservice/sdk format.

5. Accept the SSL certificate of the Lookup service and log out.

   The Lookup service address appears in both Site details and System Monitoring > Service status panes.

What to do next

Enable the tunneling service for VMware vCloud Availability services communication.
Enable vCloud Availability Tunnel

You enable vCloud Availability Tunnel service by using the vCloud Availability vApp Replication Manager and register the vCloud Availability Tunnel connectivity in all your cloud sites before pairing an on-premise site with your cloud site.

Prerequisites

- For all cloud sites, verify that you have locally registered the vCloud Availability Replicator to a vCloud Availability Replication Manager.
- Configure the deployed vCloud Availability Tunnel appliance by setting up a Lookup service address.

Procedure

1. In Web browser, go to https://Replication-Management-Appliance-IP-Address/ui/admin and log in as root.
2. Navigate to the Configuration tab and click Edit against the Tunnel address entry. The Tunneling Settings window appears.
3. Edit the vCloud Availability Tunnel settings and click Apply.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable tunneling for vCloud Availability services communication</td>
<td>Enable vCloud Availability Tunnel.</td>
</tr>
<tr>
<td>Tunnel address</td>
<td>Enter the local vCloud Availability Tunnel service API endpoint. By default, this address is with port 8047. For example, <a href="https://Tunnel-Appliance-IP-address:8047">https://Tunnel-Appliance-IP-address:8047</a>.</td>
</tr>
<tr>
<td>Appliance user</td>
<td>The vCloud Availability Tunnel appliance root user.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the vCloud Availability Tunnel appliance root user.</td>
</tr>
</tbody>
</table>

4. Accept the vCloud Availability Tunnel SSL certificate.
5. Restart all services in order to apply the tunnel configuration.

For your dedicated vCloud Availability Replicator appliances, you must restart the vCloud Availability Replicator service on every vCloud Availability Replicator appliance in the site.

Restart Services

You restart all VMware vCloud Availability services available in a single appliance in the cloud site. Services that are in dedicated appliances are restarted separately for each appliance.
Procedure

1. Restart vCloud Availability vApp Replication Manager service.
      The vCloud Availability vApp Replication Manager service management interface login page displays.
   b. Log in and select System Monitoring.
   c. Click Restart Service.
   d. Confirm the restart by clicking Restart in the pop-up window.

2. Restart vCloud Availability Replicator service.
   a. In a Web browser, go to https://Replicator-Appliance-IP-Address/ui/admin.
      The vCloud Availability Replicator service login page displays.
   b. Log in and select System Monitoring.
   c. Click Restart Service.
   d. Confirm the restart by clicking Restart in the pop-up window.

Configuring the Customer Experience Improvement Program

When you choose to participate in the Customer Experience Improvement Program (CEIP), VMware receives anonymous information to improve the quality, reliability, and functionality of VMware products and services.

Categories of Information That VMware Receives

This product participates in the VMware Customer Experience Improvement Program (CEIP).

Details regarding the data collected by CEIP and the purposes for which it is used by VMware are available at the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html.

To join or leave the CEIP for this product, see Join or Leave the Customer Experience Improvement Program.

Join or Leave the Customer Experience Improvement Program

You can choose to join the Customer Experience Improvement Program (CEIP), or leave the CEIP at any time.

Prerequisites

Verify that your user profile is assigned System Administrator privileges.
Procedure

1  Log in to the VMware vCloud Availability portal as a **System administrator**. For more information, see the *Accessing the vCloud Availability Portal as a Service Provider* topic in the *vCloud Availability User’s Guide*.

2  Navigate to **Configuration > System Settings > Participate in CEIP** and click **Edit**.

3  Select or deselete the **Join the VMware Customer Experience Improvement Program** checkbox to either join or leave the program and click **Apply**.
Upgrading vCloud Availability

You upgrade vCloud Availability components by using the service management interface of each of its components.

To upgrade to VMware vCloud Availability 3.0, you can configure vCloud Availability components to download the upgrade packages from the following sources.

- Download from the default VMware repository.
- Download from an ISO image file that is mounted to the CD-ROM drive of the component appliance.
- Download from a local repository, on which you have uploaded the upgrade package.

The following table describes all possible options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Default Repository</td>
<td>Use the default VMware repository when your environment allows an external Internet access. This option is configured by default.</td>
</tr>
<tr>
<td>Use CDROM Updates</td>
<td>Use the CD-ROM drive of a vCloud Availability appliance when your environment does not allow an external Internet access.</td>
</tr>
<tr>
<td>Use Specified Repository</td>
<td>Use a specified local repository as a content mirror when your environment does not allow external Internet access and vCloud Availability appliances are deployed to multiple datastores.</td>
</tr>
</tbody>
</table>

This chapter includes the following topics:

- Order of Upgrading vCloud Availability Components
- Upgrade vCloud Availability Components by Using Default Repository
- Upgrade VMware vCloud Availability by Using an ISO Image
- Upgrade vCloud Availability Components by Using a Specified Repository
- Install the vCloud Availability Plug-In for vCloud Director
- Start Working with vCloud Availability 3.0

Order of Upgrading vCloud Availability Components

To upgrade VMware vCloud Availability, you must upgrade vCloud Availability components in a specific order.
Upgrade vCloud Availability components in the local site and then upgrade all components in the remote site. During the upgrade, you might observe replication interruptions and Recovery Point Objective (RPO) violations.

Upgrade your vCloud Availability components in the following order:

1. Upgrade all vCloud Availability vApp Replication Manager instances.
2. Upgrade all vCloud Availability Replication Manager instances.
3. Upgrade all vCloud Availability Replicator instances.
4. Upgrade all vCloud Availability Tunnel instances.

### Upgrade vCloud Availability Components by Using Default Repository

You can configure vCloud Availability components to use the default VMware repository for the upgrade.

#### Procedure

1. Log in to the service management interface for the vCloud Availability component as root.

   You access service management interfaces for vCloud Availability components in a Web browser. The following table lists the services management interface addresses of vCloud Availability 1.5 components.

<table>
<thead>
<tr>
<th>VMware vCloud Availability Component</th>
<th>Management Interface Address and Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud Availability vApp Replication Manager</td>
<td><a href="https://Appliance-IP-Address:8046/ui/admin">https://Appliance-IP-Address:8046/ui/admin</a></td>
</tr>
<tr>
<td>vCloud Availability Replication Manager</td>
<td><a href="https://Appliance-IP-Address:8044/ui/admin">https://Appliance-IP-Address:8044/ui/admin</a></td>
</tr>
<tr>
<td>vCloud Availability Replicator</td>
<td><a href="https://Appliance-IP-Address:8043/ui/admin">https://Appliance-IP-Address:8043/ui/admin</a></td>
</tr>
<tr>
<td>vCloud Availability Tunnel</td>
<td><a href="https://Appliance-IP-Address:8047/ui/admin">https://Appliance-IP-Address:8047/ui/admin</a></td>
</tr>
</tbody>
</table>

2. Install updates.

   a. On the Configuration tab, click Edit against the Update repository entry.
   b. Select Use Default Repository and click Apply.
   c. Click Check for update against the Product version entry.
   d. Click Update and wait for the update to install.

   The appliance restarts automatically.

#### What to do next

After you upgrade all vCloud Availability components in all cloud sites, finalize the upgrade by carrying out the post-upgrade configuration. For more information, see Start Working with vCloud Availability 3.0.
Upgrade VMware vCloud Availability by Using an ISO Image

You can configure vCloud Availability components to download the upgrade package from an ISO image file that is mounted to the CD-ROM drive of the component appliance.

Procedure

1. Download the vCloud Availability 3.0 Appliance for Cloud Providers (VMware-vCloud-Availability-XXX-build_number.iso) image from the vCloud Availability official VMware download site.

2. Copy the ISO image file to a datastore that is accessible from the vCenter Server instance that you use with vCloud Availability.

3. Mount the ISO file to a vCloud Availability appliance.
   a. Log in to the vSphere Client on the site where you want to upgrade vCloud Availability.
   b. In the Home page, click **Hosts and Clusters**.
   c. Right-click the virtual machine that hosts the vCloud Availability component and select **Edit Settings**.
   d. On the **Virtual Hardware** tab, select **CD/DVD Drive > Datastore ISO File**.
   e. Follow the prompts to add the CD/DVD drive to the vCloud Availability virtual machine and select the **Connected** option.

4. Log in to the service management interface for the vCloud Availability component as **root**.

You access service management interfaces for vCloud Availability components in a Web browser. The following table lists the services management interface addresses of vCloud Availability 1.5 components.

<table>
<thead>
<tr>
<th>VMware vCloud Availability Component</th>
<th>Management Interface Address and Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud Availability vApp Replication Manager</td>
<td><a href="https://Appliance-IP-Address:8046/ui/admin">https://Appliance-IP-Address:8046/ui/admin</a></td>
</tr>
<tr>
<td>vCloud Availability Replication Manager</td>
<td><a href="https://Appliance-IP-Address:8044/ui/admin">https://Appliance-IP-Address:8044/ui/admin</a></td>
</tr>
<tr>
<td>vCloud Availability Replicator</td>
<td><a href="https://Appliance-IP-Address:8043/ui/admin">https://Appliance-IP-Address:8043/ui/admin</a></td>
</tr>
<tr>
<td>vCloud Availability Tunnel</td>
<td><a href="https://Appliance-IP-Address:8047/ui/admin">https://Appliance-IP-Address:8047/ui/admin</a></td>
</tr>
</tbody>
</table>

5. Install updates.
   a. On the **Configuration** tab, click **Edit** against the **Update repository** entry.
   b. Select the **Use CDROM Updates** option and click **Apply**.
c Click **Check for update** against the **Product version** entry.
d Click **Update** and wait for the update to install.
The appliance restarts automatically.

6 Unmount the ISO image.
   a In the vSphere Client, shut down the virtual machine that hosts the vCloud Availability component.
b Right-click the virtual machine and select **Edit Settings**.
c In the **Virtual Hardware** tab, select **CD/DVD Drive** and deselect **Connected** and **Connect At Power On**.
d Power on the virtual machine.

**What to do next**

After you upgrade all vCloud Availability components in all sites, you finalize the upgrade by carrying out the post-upgrade configuration. For more information, see [Start Working with vCloud Availability 3.0](#).

**Upgrade vCloud Availability Components by Using a Specified Repository**

You can configure vCloud Availability components to use a local repository for an upgrade.

**Procedure**

1 Prepare the local repository for upgrades.
   a Install and configure a local Web server.
b Download the vCloud Availability 3.0 Appliance for Cloud Providers (VMware-vCloud-Availability-XXX-build_number.iso) file from the official VMware download site.
c Mount the ISO image and copy the update directory to the local Web server.
   The update directory should contain **manifest** and **package-pool** directories.

2 Log in to the service management interface for the vCloud Availability component as **root**.

You access service management interfaces for vCloud Availability components in a Web browser. The following table lists the services management interface addresses of vCloud Availability 1.5 components.

**Table 4-3. Services Management Interface Addresses**

<table>
<thead>
<tr>
<th>VMware vCloud Availability Component</th>
<th>Management Interface Address and Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud Availability vApp Replication Manager</td>
<td><a href="https://Appliance-IP-Address:8046/ui/admin">https://Appliance-IP-Address:8046/ui/admin</a></td>
</tr>
<tr>
<td>vCloud Availability Replication Manager</td>
<td><a href="https://Appliance-IP-Address:8044/ui/admin">https://Appliance-IP-Address:8044/ui/admin</a></td>
</tr>
<tr>
<td>vCloud Availability Replicator</td>
<td><a href="https://Appliance-IP-Address:8043/ui/admin">https://Appliance-IP-Address:8043/ui/admin</a></td>
</tr>
<tr>
<td>vCloud Availability Tunnel</td>
<td><a href="https://Appliance-IP-Address:8047/ui/admin">https://Appliance-IP-Address:8047/ui/admin</a></td>
</tr>
</tbody>
</table>
3 Install updates.
   a On the Configuration tab, click Edit against the Update repository entry.
   b Select the Use Specified Repository option.
   c Enter the URL address of the local repository by pointing to the update directory of the local Web server.
      For example, http://local-Web-server-address/update.
   d To authenticate to the repository, enter your user name and password.
   e Click Apply.
   f Click Check for update against the Product version entry.
   g Click Update and wait for the update to install.
      The appliance restarts automatically.

What to do next

After you upgrade all vCloud Availability components in all sites, you finalize the upgrade by carrying out the post-upgrade configuration. For more information, see Start Working with vCloud Availability 3.0.

Install the vCloud Availability Plug-In for vCloud Director

To access the vCloud Availability Portal from the vCloud Director Service Provider Admin Portal and the vCloud Director Tenant Portal, you must install the vCloud Availability plug-in for vCloud Director.

Procedure

1 Log in to the vCloud Availability Service Provider Portal.
   a In a Web browser, go to https://vApp-Replication-Manager-IP-address/ui/admin.
   b Log in as root.
2 Install the vCloud Availability plug-in for vCloud Director.
   a Navigate to the Configuration tab and click Edit against the vCloud Director address entry.
   b Select the configuration type and click Apply.
      If you select Discover the vCloud Director Service address automatically, proceed to Step 3.
      If you select Enter details for the vCloud Director Service manually, proceed to Step 2c.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Discover the vCloud Director Service address automatically | By default, this option is selected. Use the option if the following configurations are present in your environment:  
  ▪ vCloud Director is federated with a previously specified Lookup service.  
  ▪ There is only one registered vCloud Director in the Lookup service.  
  ▪ The single sign-on user belongs to the System administrator group in vCloud Director.  |
| Enter details for the vCloud Director Service manually | Select this option, if your vCloud Director instance is not federated with a previously specified Lookup service or if multiple vCloud Director instances are registered to the Lookup service.  |

c Enter the vCloud Director URL in the following format: https://vCloud Director-IP-address:443/api.
d Enter a vCloud Director System administrator user name and password, and click Next.
   For example administrator@system, where system is the name of the system organization of vCloud Director.
   The vCloud Director certificate details display.
e To finish the vCloud Director configuration, accept the vCloud Director SSL certificate.

3 In the System Monitoring tab, click Restart Service and confirm the operation.
You successfully installed the vCloud Availability plug-in for vCloud Director and can access the vCloud Availability Portal directly from the vCloud Director user interface.

Start Working with vCloud Availability 3.0
After you upgrade all vCloud Availability components in the local and the remote sites, to start working with vCloud Availability 3.0, verify that the trust between the sites is preserved, enter a valid license key, and configure replication policies in the local and the remote sites.

Procedure
1 Log in to the vCloud Availability Service Provider Portal.
   a In a Web browser, go to https://vApp-Replication-Manager-IP-address/ui/admin.
   b Log in as root.
2 Enable the vCloud Availability Tunnel service.

**Note** If you set up the tunneling before performing the upgrade, skip this step.

- a In the **Configuration** tab, click **Edit** against the **Tunnel address** entry.
- b In the **System Monitoring** tab, click **Restart Service**.

Perform this step for all vCloud Availability services.

3 Reestablish the trust between the sites.

See **Re-Pair Cloud Sites**.

4 Enter a valid vCloud Availability license key.

- a In the **Configuration** tab, click **Edit** against the **License key** entry.
- b Enter your license key and click **Apply**.
- c Verify that there are no errors for the **License key** entry.

5 Set up the NTP server.

- a Open an SSH connection to the vCloud Availability vApp Replication Manager appliance.
- b Log in as **root**.
- c Open the `/etc/systemd/timesyncd.conf` file by using a text editor.
- d To set or update the NTP server of the appliance, modify the following entry.

```
NTP= NTP-Server-Address
```

- e Save the changes and exit the text editor.
- f Restart the time synchronization service by running the following command.

```
$ systemctl restart systemd-timesyncd
```

6 Create custom replication policies or enable configuring replication in the default policy.

To configure new replications, the policies that are assigned to the source and the destination organizations must allow incoming and outgoing replications.

You successfully upgraded vCloud Availability and can start configuring replications. For more information, see the **vCloud Availability User's Guide**.
Management and administrative tasks occur after you install and configure the vCloud Availability solution and include changes to the provisioned environment and routine administration and maintenance procedures.

This chapter includes the following topics:

- Pair Cloud Sites
- Re-Pair Cloud Sites
- Add a New vCloud Availability Replicator
- Certificate Management in VMware vCloud Availability
- Certificate Management in the External Infrastructure
- Collect VMware vCloud Availability Usage Information
- Collect VMware vCloud Availability Storage Consumption Information
- Free up Disk Space on the vCloud Availability Appliance
- Troubleshooting VMware vCloud Availability

**Pair Cloud Sites**

By pairing your cloud sites, you establish a trust between vCloud Availability vApp Replication Manager instances in two different sites.

You can initiate pairing from either of the cloud sites.

**Prerequisites**

Verify that you configured the following services in both sites between which you establish a trust:

- vCloud Availability vApp Replication Manager
- vCloud Availability Replication Manager
- vCloud Availability Replicator
- vCloud Availability Tunnel
Procedure

1. In a Web browser, go to https://vApp-Replication-Manager-IP-address/ui/login.
2. Log in as root.
3. Select the Sites tab and click New Pairing.
4. Pair the cloud sites.
   a. In the New Pairing window, enter the name of the remote site.
      Note: Use the remote site name that you previously defined.
   b. Enter the Endpoint URL of the remote site.
      Enter the public IP address of the vCloud Availability Tunnel appliance in the remote site with port 443. For example, https://Tunnel-Appliance–Public–IP–address:443.
   c. To pair the local with the remote site, enable Remote appliance credentials and enter the root user password of the vCloud Availability vApp Replication Manager appliance.
      To pair the sites with Remote appliance credentials disabled, you must repeat the procedure on your remote site.
   d. Click Pair.
   e. To complete the pairing, accept the SSL certificate of the remote vCloud Availability vApp Replication Manager appliance.
5. To verify that the trust between the two sites is successfully established, navigate to Sites and confirm that the new site is listed and there are no errors or warnings.

What to do next

Before you can configure replications, you must create a custom replication policy and assign it to the source and destination vCloud Director organizations, or edit the default replication policy for both organizations. The replication policy that is assigned to the source and destination organizations must allow replications. For more information, see Working with Replication Policies chapter.

Re-Pair Cloud Sites

After you register a vCloud Availability Replicator, replace the vCloud Availability vApp Replication Manager certificate, or upgrade VMware vCloud Availability, you must reestablish the trust between the cloud sites.

You can initiate the trust reestablishment from either of the sites between which you establish a trust.

Procedure

1. In a Web browser, go to https://vApp–Replication–Manager–IP–address/ui/login.
2. Log in as root.
   The vCloud Availability Provider portal displays.
3. Select the Sites tab and click the peer site within the Cloud sites pane.

4. Click Repair.

   The Update Pairing window displays.

5. (Optional) Change the current tunnel address and description.

6. Enable the Remote appliance credentials if not already enabled.

7. Enter the root user password of the remote vCloud Availability vApp Replication Manager appliance and click Update.

8. To complete the trust reestablishment, accept the SSL certificate of the remote vCloud Availability vApp Replication Manager appliance.

You reestablished the cloud sites trust and can configure new incoming and outgoing replications between the sites.

### Add a New vCloud Availability Replicator

Depending on your deployment requirements, you can add vCloud Availability Replicator instances to your vCloud Availability environment.

#### Prerequisites

- Deploy a new vCloud Availability Replicator appliance. For more information, see Deploy VMware vCloud Availability Services Using the vSphere Client and Deploy VMware vCloud Availability Services Using the OVF Tool.
- Configure the new vCloud Availability Replicator appliance. For more information, see Configure vCloud Availability Replicator Appliance.
- Register the new vCloud Availability Replicator appliance to the local vCloud Availability Replication Manager. For more information, see Register a vCloud Availability Replicator with a vCloud Availability Replication Manager in the Same Site.

#### Procedure

1. Add a vCloud Availability Replicator.
   a. In a Web browser, go to https://Replication-Manager-IP-address:8441/ui/admin.
      
      The vCloud Availability Replication Manager service management interface login page displays.
   b. Log in as root.
   c. In the Replicators tab, click New.
      
      The New Replicator wizard displays.
   d. Select the site to which you add the new vCloud Availability Replicator instance.
e  (Optional) Add a description for the vCloud Availability Replicator.

f  In the API URL text box, enter the vCloud Availability Replicator appliance address and port 443.
   For example, https://Replicator-Appliance-IP-address:443.

g  Enter the appliance root password that you set during the initial vCloud Availability Replicator configuration.

h  Enter the single sign-on domain administrator user name and password.
   For example, administrator@vsphere.local.

i  Click Add.

j  To complete the addition, accept the vCloud Availability Replicator SSL certificate.

2  Register the vCloud Availability Tunnel appliance to the new vCloud Availability Replicator by re-enabling the tunnel.
   a  On the Configuration tab, click Edit against the tunnel address entry.
   b  Enter your credentials for the tunnel appliance and click Apply.

A new vCloud Availability Replicator instance is added to your vCloud Availability environment.

**What to do next**

To use the new vCloud Availability Replicator instance, reestablish the trust between cloud sites. See Repair Cloud Sites. To add another vCloud Availability Replicator, repeat this procedure.

**Certificate Management in VMware vCloud Availability**

You can regenerate a self-signed certificate or import a CA-signed certificate to replace the certificate for every VMware vCloud Availability service.

**Regenerate a Self-Signed Certificate**

When the SSL certificate of a vCloud Availability service expires, you use the service management interface of that service to regenerate the certificate.

**Procedure**

1  In a Web browser, go to the vCloud Availability service management interface at https://Appliance-IP-Address:port/ui/admin.

2  Log in as root.

3  On the Configuration tab, click Regenerate against the Certificate entry.

4  Confirm the operation by clicking Apply.

Regenerating the SSL certificate of the vCloud Availability service restarts all vCloud Availability services that run on the same appliance.
What to do next

If you must refer to your old certificate, you can locate it at /opt/vmware/h4/<service type>/config/keystore.p12.bak, where <service type> can be cloud, manager, replicator, or tunnel.

Upload a CA-Signed Certificate

You can configure vCloud Availability services to work with a CA-signed certificate.

You upload a CA-signed SSL certificate to authenticate the vCloud Availability service so that the Web browser does not show a certificate prompt every time users log in to the vCloud Availability service management interface over HTTPS.

Procedure

1 In a Web browser, go to the vCloud Availability service management interface at https://Appliance-IP-Address:port/ui/admin.
2 Log in as root.
3 On the Configuration tab, click Import against the Certificate entry.
4 Enter the password that protects the PKCS#12 keystore and the private key.
5 Click Browse and select the PKCS#12 key and the corresponding certificate.

   Note The PKCS#12 file must contain one entry with a private key, the associated certificate and, optionally, the certificate chain.

6 Click Apply.

Uploading the CA-signed certificate of the vCloud Availability service restarts all services that run on the same appliance.

What to do next

If you must refer to the old certificate, you can locate it at /opt/vmware/h4/<service type>/config/keystore.p12.bkp, where <service type> can be cloud, manager, replicator, or tunnel.

Replacing vCloud Availability Services Certificates

When you renew or replace the certificate of a vCloud Availability service, you must reconfigure the remaining services of the VMware vCloud Availability to work with the new certificate.

Replace the Certificate of the vCloud Availability vApp Replication Manager Service

When the certificate of the vCloud Availability vApp Replication Manager service expires, you must replace it with the new self-signed or CA-signed certificate.
Regenerating the SSL certificate or uploading a CA-signed certificate of the vCloud Availability vApp Replication Manager service breaks the trust between the cloud and on-premises sites.

After you replace the certificate of the vCloud Availability vApp Replication Manager service, you must reestablish the trust between the cloud and on-premises sites.

**Important** After re-pairing the cloud sites, you must manually re-pair all on-premises sites. To configure the vCloud Availability on-premises appliance, see the *Installing and Configuring vCloud Availability On-Premises* document.

**Procedure**

1. Log in to vCloud Availability vApp Replication Manager by using the service management interface.
   a. Open a Web browser and navigate to `https://Appliance-IP-Address/ui/admin`.
   b. Log in by using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>root_user_password</td>
</tr>
</tbody>
</table>

2. Generate or upload a new certificate.
   For more information, see Regenerate a Self-Signed Certificate or Upload a CA-Signed Certificate.

3. Re-enable the tunnel.
   For more information, see Enable vCloud Availability Tunnel.

4. In the service management interface of the vCloud Availability vApp Replication Manager appliance, navigate to the Sites tab.

5. Select a cloud site and click Repair.
   **Note** You must perform this step for each cloud site.
   For more information, see Re-Pair Cloud Sites.

6. Re-pair all on-premises sites with the cloud sites.
   To configure the vCloud Availability on-premises appliance, see the *Installing and Configuring vCloud Availability On-Premises* document.

**Replace the Certificate of the vCloud Availability Replication Manager Service**

When the certificate of the vCloud Availability Replication Manager service expires, you replace it with the new self-signed or CA-signed certificate.

Replacing the certificate of the vCloud Availability Replication Manager service breaks the trust between all vCloud Availability Replicator instances in the local, remote cloud, and remote on-premises sites.
After you replace the certificate of the vCloud Availability Replication Manager service, to re-pair the registration of vCloud Availability Replicator instances in the remote site, reestablish the trust between the cloud sites.

**Important** After re-pairing the cloud sites, you must manually re-pair all on-premises sites. To configure the vCloud Availability on-premises appliance, see the *Installing and Configuring vCloud Availability On-Premises* document.

**Procedure**

1. Log in to vCloud Availability Replication Manager by using the service management interface.
   a. Open a Web browser and navigate to `https://Appliance-IP-Address:8441/ui/admin`.
   b. Log in by using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>root_user_password</td>
</tr>
</tbody>
</table>

2. Generate or upload a new certificate.
   For more information, see *Regenerate a Self-Signed Certificate* or *Upload a CA-Signed Certificate*.

3. Re-pair the registration of vCloud Availability Replicator instances to the vCloud Availability Replication Manager service in the local site.
   a. Log in to the service management interface of the vCloud Availability Replicator appliance again.

      Enter the service address in the format `https://Replication-Manager-IP-address:8441/ui/admin`.

      On the **System Monitoring** tab all vCloud Availability Replicator instances are Offline.

   b. On the **Replicators** tab, select a vCloud Availability Replicator instance and click **Repair**.

   c. Enter details of the vCloud Availability Replicator instance and click **Apply**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance Password</td>
<td>The root user password for the vCloud Availability Replicator appliance.</td>
</tr>
<tr>
<td>SSO User Name</td>
<td>A user assigned with administrative privileges for the local site single sign-on domain, for example <em><a href="mailto:Administrator@VSPHERE.LOCAL">Administrator@VSPHERE.LOCAL</a></em>.</td>
</tr>
<tr>
<td>SSO Password</td>
<td>The password for the administrative user.</td>
</tr>
</tbody>
</table>

   d. Accept the SSL certificate of the vCloud Availability Replicator service.

   e. Repeat steps b to d for all vCloud Availability Replicator instances that are registered to the vCloud Availability Replication Manager service in the local site.

   f. After you repair the registrations for all vCloud Availability Replicator instances, verify that no connectivity errors are reported on the **System Monitoring** tab.
4 In the service management interface of the vCloud Availability vApp Replication Manager appliance, navigate to the Sites tab.

5 Select a cloud site and click Repair.

   Note You must perform this step for each cloud site.

   For more information, see Re-Pair Cloud Sites.

6 Re-pair all on-premises sites with the cloud sites.

   To configure the vCloud Availability on-premises appliance, see the Installing and Configuring vCloud Availability On-Premises document.

You successfully renewed the certificate of the vCloud Availability Replication Manager service and reestablished the trust between the clouds, and on-premises sites.

**Replace the Certificate of the vCloud Availability Replicator Service**

When the certificate of the vCloud Availability Replicator service expires, you replace it with the new self-signed or CA-signed certificate.

Regenerating the SSL certificate or uploading a CA-signed certificate of the vCloud Availability Replicator service breaks the registration of the vCloud Availability Replicator service to the vCloud Availability Replication Manager instance in the local and remote sites.

After you renew the certificate of the vCloud Availability Replicator service, to repair the registration to the vCloud Availability Replication Manager instance in the remote site, reestablish the trust between the cloud sites.

**Procedure**

1 Log in to the vCloud Availability Replicator service management interface.
   
   a Open a Web browser and depending on your deployment type, navigate to the following management endpoint.

<table>
<thead>
<tr>
<th>Deployment type</th>
<th>Management Endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Combined Appliance</td>
<td><a href="https://Appliance-IP-Address:8440/ui/admin">https://Appliance-IP-Address:8440/ui/admin</a></td>
</tr>
<tr>
<td>Cloud Replicator</td>
<td><a href="https://Replicator-Appliance-IP-Address/ui/admin">https://Replicator-Appliance-IP-Address/ui/admin</a></td>
</tr>
</tbody>
</table>

   b Log in by using your root user credentials.

2 Generate or upload a new certificate.

   For more information, see Regenerate a Self-Signed Certificate or Upload a CA-Signed Certificate.
3 Re-pair the registration of vCloud Availability Replicator instances to the vCloud Availability Replication Manager service in the local site.

   a Log in to the service management interface of the vCloud Availability Replication Manager appliance again.

   Enter the service address in the format https://Replication-Manager-IP-address:8441/ui/admin.

   On the System Monitoring tab all vCloud Availability Replicator instances are Offline.

   b On the Replicators tab, select a vCloud Availability Replicator instance and click Repair.

   c Enter details of the vCloud Availability Replicator instance and click Apply.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance Password</td>
<td>The root user password for the vCloud Availability Replicator appliance.</td>
</tr>
<tr>
<td>SSO User Name</td>
<td>A user assigned with administrative privileges for the local site single sign-on domain, for example <a href="mailto:Administrator@VSPHERE.LOCAL">Administrator@VSPHERE.LOCAL</a>.</td>
</tr>
<tr>
<td>SSO Password</td>
<td>The password for the administrative user.</td>
</tr>
</tbody>
</table>

   d Accept the SSL certificate of the vCloud Availability Replicator service.

   e Repeat steps b to d for all vCloud Availability Replicator instances that are registered to the vCloud Availability Replication Manager service in the local site.

   f After you repair the registrations for all vCloud Availability Replicator instances, verify that no connectivity errors are reported on the System Monitoring tab.

4 In the service management interface of the vCloud Availability vApp Replication Manager appliance, navigate to the Sites tab.

5 Select a cloud site and click Repair.

   **Note** You must perform this step for each cloud site.

   For more information, see Re-Pair Cloud Sites.

You successfully renewed the certificate of the vCloud Availability Replicator service.

**Replace the Certificate of the vCloud Availability Tunnel Service**

When the certificate of the vCloud Availability Tunnel service expires, you replace it with a new self-signed or a CA-signed certificate.

You replace the certificate and perform a service configuration of the vCloud Availability Tunnel appliance only in cloud sites.

   **Important** After re-pairing the cloud sites, you must manually re-pair all on-premises sites. To configure the vCloud Availability on-premises appliance, see the Installing and Configuring vCloud Availability On-Premises document.
Procedure

1. Log in to the vCloud Availability Tunnel service management interface.
   a. Open a Web browser and depending on your deployment type, navigate to the following management endpoint.

<table>
<thead>
<tr>
<th>Deployment type</th>
<th>Management Endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Combined Appliance</td>
<td><a href="https://Appliance-IP-Address:8442/ui/admin">https://Appliance-IP-Address:8442/ui/admin</a></td>
</tr>
<tr>
<td>Cloud Tunnel Appliance</td>
<td><a href="https://Tunnel-Appliance-IP-Address/ui/admin">https://Tunnel-Appliance-IP-Address/ui/admin</a></td>
</tr>
</tbody>
</table>

   b. Log in by using your root user credentials.

2. Generate or upload a new certificate.
   For more information, see Regenerate a Self-Signed Certificate or Upload a CA-Signed Certificate.

3. Re-enable the tunnel.
   For more information, see Enable vCloud Availability Tunnel.

4. In the service management interface of the vCloud Availability vApp Replication Manager appliance, navigate to the Sites tab.

5. Select a cloud site and click Repair.
   
   **Note** You must perform this step for each cloud site.

   For more information, see Re-Pair Cloud Sites.

6. Re-pair all on-premises sites with the cloud sites.
   
   To configure the vCloud Availability on-premises appliance, see the Installing and Configuring vCloud Availability On-Premises document.

You successfully renewed the certificate of the vCloud Availability Tunnel service.

Certificate Management in the External Infrastructure

After renewing or replacing the SSL certificate of the vCenter Server Lookup service on a Platform Services Controller or changing the vCloud Director endpoint or its certificate, you must configure the VMware vCloud Availability services to work with the new certificate.

Configure VMware vCloud Availability with a Renewed vCloud Director Endpoint or Certificate

If you renew the vCloud Director SSL certificate or change the vCloud Director endpoint, you must perform additional steps to ensure that the vCloud Availability vApp Replication Manager can communicate with vCloud Director.
Prerequisites

- Follow this procedure if you manually configured the vCloud Director details in vCloud Availability vApp Replication Manager.
- If you selected **Discover vCloud Director Service address automatically**, verify that the vCloud Director details in the lookup service are updated and skip this procedure.
- Verify that you successfully renewed the vCloud Director SSL certificate. For more information, see VMware KB 1026309.

Procedure

1. In a Web browser, open the vCloud Availability vApp Replication Manager configuration portal by navigating to `https://vApp-Replication-Manager-IP-address:8441/ui/admin`.
2. Log in as the **root** user.
3. In the left pane, click **Configuration**.
4. Under **Service endpoints**, next to **vCloud Director address** click **Edit**.
5. On the **vCloud Director Details** page, click **Apply**.
   - The details of the new certificate appear.
6. Verify that the details of the certificate are correct, and click **Accept**.
7. In the left pane, click **System Monitoring**.
8. Under **System health**, click **Restart service**.

**Configure VMware vCloud Availability with a Renewed Lookup Service Certificate on a Platform Services Controller**

If you renew the vCenter Server Lookup service certificate on a Platform Services Controller instance, you must configure the VMware vCloud Availability components to work with the renewed certificate.

Prerequisites

- Verify that you have successfully renewed the Platform Services Controller certificate and that the vCenter Server Lookup service is updated to use the renewed certificate. For more information, see `https://kb.vmware.com/s/article/2118939`.
- Verify that all components in your environment that depend on the vCenter Server registration in the vCenter Server Lookup service are configured to trust the renewed certificate. An example of such a component is NSX Manager.
Procedure

1 Configure the vCloud Availability Replicator to work with the renewed Platform Services Controller certificate.

   If you are not using the Combined deployment type and have dedicated vCloud Availability Replicator appliances, repeat this step for all vCloud Availability Replicator instances.

   a In a Web browser, open the vCloud Availability Replicator service management interface by navigating to https://Replicator–Appliance–IP:8440/ui/admin.
   b Log in as the root user.
   c In the left pane, click Configuration.
   d Under Service endpoints, next to Lookup service address click Edit.
   e In the Lookup Service Details dialog box, enter the Lookup service address and click Apply.
   The details of the renewed vCenter Server Lookup service certificate appear.
   f To complete the vCloud Availability Replicator configuration, accept the renewed vCenter Server Lookup service certificate.

2 Configure the vCloud Availability Replication Manager to work with the renewed Platform Services Controller certificate.

   a In a Web browser, open the vCloud Availability Replication Manager service management interface by navigating to https://Replication–Manager–IP-address:8441/ui/admin.
   b Log in as the root user.
   c In the left pane, click Configuration.
   d Under Service endpoints, next to Lookup service address click Edit.
   e In the Lookup Service Details dialog box, enter the Lookup service address and click Apply.
   The details of the renewed vCenter Server Lookup service certificate appear.
   f To complete the vCloud Availability Replicator configuration, accept the renewed vCenter Server Lookup service certificate.

3 Configure the vCloud Availability vApp Replication Manager to work with the renewed Platform Services Controller certificate.

   a In a Web browser, open the vCloud Availability vApp Replication Manager service management interface by navigating to https://vApp–Replication–Manager–IP-address:8441/ui/admin.
   b Log in as the root user.
   c In the left pane, click Configuration.
   d Under Service endpoints, next to Lookup service address click Edit.
e In the **Lookup Service Details** dialog box, enter the Lookup service address and click **Apply**.

The details of the renewed vCenter Server Lookup service certificate appear.

f To complete the vCloud Availability vApp Replication Manager configuration, accept the renewed vCenter Server Lookup service certificate.

**Collect VMware vCloud Availability Usage Information**

This procedure outlines extracting usage information from your vCloud Availability installation. You can use the exported information for reporting purposes.

**Procedure**

1 Log in to the vCloud Availability vApp Replication Manager appliance console as **root**.

   ```bash
   $ c4 loginroot C4-Root-Password
   ```

2 (Optional) Retrieve information about the usage-report script.

   ```bash
   $ usage-report --help
   ```

3 Generate the vCloud Availability usage report.

   ```bash
   $ usage-report --output /tmp/report_summary.tsv --details /tmp/report_details.tsv
   ```

The vCloud Availability usage report consists of two .tsv files. The /tmp/report_summary.tsv file contains information about the total incoming replications and information about incoming replications aggregated by Organizations and by vDC.

The /tmp/report_summary.tsv file contains information about individual incoming replications in the following format:

```
# vCloud Availability Usage Report

Incoming replication counts

<table>
<thead>
<tr>
<th>Replication type</th>
<th>Total count</th>
<th>Cloud to cloud replications</th>
<th>Cloud to cloud migrations</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere to cloud replications</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>vSphere to cloud migrations</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total incoming vApp replications</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Newly started incoming vApp replications</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Carried over incoming vApp replications</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Total incoming VM replications</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Newly started incoming VM replications</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Carried over incoming VM replications</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
```

Incoming vApp replications by org
<table>
<thead>
<tr>
<th>Org</th>
<th>Org Id</th>
<th>Total count</th>
<th>Cloud to cloud replications</th>
<th>Cloud to cloud migrations</th>
<th>vSphere to cloud replications</th>
<th>vSphere to cloud migrations</th>
</tr>
</thead>
<tbody>
<tr>
<td>s2Org</td>
<td>223137fb-48bf-4da2-93d0-a493abbf48e8</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Incoming VM replications by org

<table>
<thead>
<tr>
<th>Org</th>
<th>Org Id</th>
<th>Total count</th>
<th>Cloud to cloud replications</th>
<th>Cloud to cloud migrations</th>
<th>vSphere to cloud replications</th>
<th>vSphere to cloud migrations</th>
</tr>
</thead>
<tbody>
<tr>
<td>s2Org</td>
<td>223137fb-48bf-4da2-93d0-a493abbf48e8</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Incoming vApp replications by vDC

<table>
<thead>
<tr>
<th>vDC</th>
<th>vDC Id</th>
<th>Org</th>
<th>Total count</th>
<th>Cloud to cloud replications</th>
<th>Cloud to cloud migrations</th>
<th>vSphere to cloud replications</th>
<th>vSphere to cloud migrations</th>
</tr>
</thead>
<tbody>
<tr>
<td>vdc_s2Org</td>
<td>64275c6d-dbcc-477c-8b8d-7325a2d0b4bc</td>
<td>s2Org</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Incoming VM replications by vDC

<table>
<thead>
<tr>
<th>vDC</th>
<th>vDC Id</th>
<th>Org</th>
<th>Total count</th>
<th>Cloud to cloud replications</th>
<th>Cloud to cloud migrations</th>
<th>vSphere to cloud replications</th>
<th>vSphere to cloud migrations</th>
</tr>
</thead>
<tbody>
<tr>
<td>vdc_s2Org</td>
<td>64275c6d-dbcc-477c-8b8d-7325a2d0b4bc</td>
<td>s2Org</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

The `/tmp/report_details.tsv` file contains information about individual incoming replications in the following format:

```
# vCloud Availability Detailed Usage Report

generatedOn     2019-03-14 14:26:17.349716
buildVersion    3.0.0.21637380-f95e12bb4
localSite       site2
instanceId      96eebcce-bed0-487e-8283-3b547c3b9591

Incoming replication counts

<table>
<thead>
<tr>
<th>Replication type</th>
<th>Total count</th>
<th>Cloud to cloud replications</th>
<th>Cloud to cloud migrations</th>
</tr>
</thead>
<tbody>
<tr>
<td>migrations</td>
<td>vSphere to cloud replications</td>
<td>vSphere to cloud migrations</td>
<td></td>
</tr>
<tr>
<td>Total incoming vApp replications</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Newly started incoming vApp replications</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Carried over incoming vApp replications</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total incoming VM replications</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Newly started incoming VM replications</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Carried over incoming VM replications</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Incoming VM Replications

<table>
<thead>
<tr>
<th>Replication Type</th>
<th>Migration/Replication</th>
<th>vApp Name</th>
<th>vApp Id</th>
<th>VM Name</th>
<th>VM Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replication ID</td>
<td>Source Site</td>
<td>Source Org</td>
<td>Source vDC Id</td>
<td>Source vDC</td>
<td>Destination</td>
</tr>
<tr>
<td>Site</td>
<td>Destination Org Id</td>
<td>Destination Org</td>
<td>Destination vDC Id</td>
<td>Destination vDC</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>--------------------</td>
<td>------------------</td>
<td>--------------------</td>
<td>-----------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>r001</td>
<td>245f4a0a-461d-448b-bea2-b0ac4f4f8ae</td>
<td>r001</td>
<td>a2f0d59a-0e88b-455a-82ad-1368253c16dd</td>
<td>C4-b65aa776-5d47-4108-9ea0-009062044b8d</td>
</tr>
<tr>
<td></td>
<td>223137fb-48bf-4da2-93d0-a493abbf48e8</td>
<td>site1</td>
<td>s10rg</td>
<td>b9c72f0b-fc0d-4f5a-beb9-fb60f89b6a67</td>
<td>vdc_s10rg</td>
</tr>
<tr>
<td></td>
<td>64275c6d-dbcc-477c-88b8d-7325a2d0b4bc</td>
<td>vdc_s20rg</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>r001c</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>C4--2206a568-7c16-4688-844f-fd98d7e8d357</td>
</tr>
<tr>
<td></td>
<td>none</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>mouse</td>
</tr>
<tr>
<td></td>
<td>onprem1</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>onprem1</td>
</tr>
<tr>
<td></td>
<td>s223137fb-48bf-4da2-93d0-a493abbf48e8</td>
<td>site2</td>
<td>64275c6d-dbcc-477c-88b8d-7325a2d0b4bc</td>
<td>vdc_s20rg</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vdc_s20rg</td>
<td>vsphere-to-cloud</td>
<td>replication</td>
<td>mouse</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>vsphere-to-cloud</td>
<td>migration</td>
<td>r001c</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

4. Download the vCloud Availability usage report locally.

```bash
$ scp /tmp/report_summary.tsv /tmp/report_details.tsv user@your-host:/download-target-location
```

5. (Optional) Remove the generated reports from the vCloud Availability vApp Replication Manager appliance.

```bash
$ rm /tmp/report_summary.tsv /tmp/report_details.tsv
```

---

**Collect VMware vCloud Availability Storage Consumption Information**

This procedure outlines extracting storage consumption information from your vCloud Availability installation. You can use the exported information for reporting purposes.

To aggregate a detailed monthly storage consumption report, create daily snapshots by using the `storage-report -s` command. At the end of the reporting period, generate an aggregated storage consumption report by using the `storage-report` script. The `storage-report` script reads all storage consumption snapshots that you created and generates an aggregated report of the average storage consumption.

**Procedure**

1. Log in to the vCloud Availability vApp Replication Manager appliance console as **root**.

   ```bash
   $ c4 loginroot C4-Root-Password
   ```

2. Create a storage consumption snapshot.

   ```bash
   $ storage-report -s
   ```

   The `storage-report -s` script saves the storage consumption information at the time the script runs.
The system returns the storage consumption snapshot data in the following format:

```
# vCloud Availability - snapshot Storage Consumption Report

generatedOn  2018-09-11 08:28:34.474680
productName   vsphere Replication Cloud (C4)
buildVersion  1.5.0.1126-b60fa40
localSite     site2
instanceId    86f3279d-4119-4c0a-9a30-7295c8dca4d1

Storage consumption by org
Org     Org Id  Storage consumed        Number of PITs
s2Org   c6415681-9456-4051-88bd-5b3ebf75f610    10486784        0

Storage consumption by vDC
vDC     vDC Id  Org     Storage consumed        Number of PITs
vdc_s2Org       f5aed876-4d62-4c35-9d3d-9c3065a8bdfb    s2Org   10486784        0

# End of report.
```

3 (Optional) Retrieve more information about the `storage-report` script.

```
$ storage-report --help
```

4 Generate the vCloud Availability storage consumption report.

```
$ storage-report --output /tmp/storage_report.tsv
```

Running the `storage-report` script deletes all previously created snapshots. Run the `storage-report` script in the end of a reporting period to aggregate storage snapshots for the ending reporting period and prepare the system for the next reporting period.

The aggregated storage consumption report uses the following format:

```
# vCloud Availability - aggregated Storage Consumption Report

generatedOn  2018-09-11 08:28:58.288823
productName   vsphere Replication Cloud (C4)
buildVersion  1.5.0.1126-b60fa40
localSite     site2
instanceId    86f3279d-4119-4c0a-9a30-7295c8dca4d1

Storage consumption by org (avg)
Org     Org Id  Storage consumed        Number of PITs
s2Org   c6415681-9456-4051-88bd-5b3ebf75f610    10486784        0

Storage consumption by vDC (avg)
vDC     vDC Id  Org     Storage consumed        Number of PITs
vdc_s2Org       f5aed876-4d62-4c35-9d3d-9c3065a8bdfb    s2Org   10486784        0

# End of report.
```
5 Download the vCloud Availability storage consumption report locally.

```
$ scp /tmp/storage_report.tsv user@your-host:/download-target-location
```

6 (Optional) Remove the generated reports from the vCloud Availability vApp Replication Manager appliance.

```
$ rm /tmp/storage_report.tsv
```

**Free up Disk Space on the vCloud Availability Appliance**

If the available disk space on the vCloud Availability appliance is low, you can remove obsolete or unnecessary files.

**Procedure**

1 Clear the vCloud Availability appliance service logs.
   a Log in to the vCloud Availability appliance by using a Secure Shell (SSH) client and authenticate as the root user.
   b Navigate to the following folders and remove the service logs that are old or unnecessary.
      - `/opt/vmware/h4/cloud/log`
      - `/opt/vmware/h4/manager/log`
      - `/opt/vmware/h4/replicator/log`
      - `/opt/vmware/h4/tunnel/log`

2 Clear the vCloud Availability appliance support bundles.
   a In a Web browser, navigate to `https://Appliance-IP-Address/ui/admin` and log in with the root user.
   b In the left pane, click Support and delete all unnecessary support bundles.
   c Log in to the vCloud Availability appliance by using a Secure Shell (SSH) client and authenticate as the root user.
   d Navigate to the following folders and remove the support bundles that are not available under the Support bundles page.
      - `/opt/vmware/h4/cloud/support`
      - `/opt/vmware/h4/manager/support`
      - `/opt/vmware/h4/replicator/support`
      - `/opt/vmware/h4/tunnel/support`
3 If you have a dedicated Cloud Replicator appliance, remove the core dumps.
   a Log in to the Cloud Replicator appliance by using a Secure Shell (SSH) client and authenticate as the root user.
   b Navigate to the /var/core/ folder and remove the HBR core* files.

You see that the available disk space on the vCloud Availability appliance is increased.

What to do next
You can check the /var/log and the /tmp folders for unnecessary files and delete them.

Troubleshooting VMware vCloud Availability
Known troubleshooting information can help you diagnose and correct problems in your disaster recovery environment.

Update a Network Time Protocol Configuration
You update the Network Time Protocol (NTP) configuration by using the appliance console.

Problem
If you use different NTP servers for components in your disaster recovery environment, you might encounter connection or authentication problems.

Cause
To avoid connection or authentication problems, the following components of your disaster recovery environment must use the same time synchronization configuration:

- All vCenter Server instances in the source and destination sites
- All ESXi hosts in the source and destination sites
- Platform Services Controller instances in the source and destination sites
- All vCloud Availability appliances in the source and destination sites

Solution
1 Log in to the affected vCloud Availability appliance.
   a Open an SSH connection to the affected appliance.
   b Log in as root.
2 Set the NTP server.
   a Open the /etc/systemd/timesyncd.conf file by using a text editor.
   b To set or update the NTP server of the appliance, modify the following entry.

   \[\text{NTP= NTP-Server-Address}\]
c Save the changes and exit the text editor.

d Restart the time synchronization service by running the following command.

$ systemctl restart systemd-timesyncd

What to do next

Set or update the same NTP configuration in all vCloud Availability appliances.

**Cannot Access the vCloud Availability Portal Through vCloud Director**

You cannot access the vCloud Availability Portal through the vCloud Director Service Provider Admin Portal and the vCloud Director Tenant Portal.

**Problem**

The Availability option is not available in the vCloud Director Service Provider Admin Portal and in the vCloud Director Tenant Portal, or clicking it does not open the vCloud Availability Portal. In the vCloud Availability logs, you see the following error: Unable to register vCAV plugin in vCD.

**Cause**

Connectivity problems during the initial configuration of vCloud Availability might prevent the vCloud Availability plug-in from registering with vCloud Director.

**Solution**

1 Log in to the vCloud Availability Service Provider Portal.
   a Open a Web browser and navigate to https://vApp-Replication-Manager-IP-address/ui/admin.
   b Log in with your root user credentials.
Register the vCloud Availability plug-in with vCloud Director.

a On the Configuration tab, next to the vCloud Director address click Edit.

b Select the configuration type and click Apply.

- If you select Discover the vCloud Director Service address automatically, proceed to Step 3.
- If you select Enter details for the vCloud Director Service manually, proceed to Step 2c.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Discover the vCloud Director Service address automatically | By default, this option is selected. Use the option if the following configurations are present in your environment:  
  - vCloud Director is federated with a previously specified Lookup service.  
  - There is only one registered vCloud Director in the Lookup service.  
  - The single sign-on user belongs to the System administrator group in vCloud Director. |
| Enter details for the vCloud Director Service manually | Select this option, if your vCloud Director instance is not federated with a previously specified Lookup service or if multiple vCloud Director instances are registered with the Lookup service. |

c Enter the vCloud Director URL in the following format: https://vCloud Director-IP-Address:443/api.

d Enter a vCloud Director System administrator user name and password, and click Apply.

For example, administrator@system, where system is the name of the system organization of vCloud Director.

The vCloud Director certificate details display.

e To complete the vCloud Director configuration, accept the vCloud Director SSL certificate.

3 On the System Monitoring tab, click Restart Service and confirm the operation.

Collecting Support Bundles for the vCloud Availability Components

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

Collecting a Support Bundle from vCenter Server

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

1 In a Web browser, navigate to
2 Enter root user name and password, and click Enter. The download starts.

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

Collecting a Support Bundle from vCloud Director
To collect the vCloud Director support bundle, establish an SSH connection to one of the vCloud Director VMs and run the following command:

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

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

Collecting a Support Bundle from vCloud Availability Replicator
To collect the support bundle for vCloud Availability Replicator, perform the following steps:

1 In a Web browser, go to https://Replicator–Appliance–IP:8440/ui/admin. The vCloud Availability Replicator service management interface login page opens.
2 Log in as root.
3 Go to Support.
4 Click Generate New and confirm the operation by clicking Generate. A pop-up window indicating the process progress appears.
5 To save the support bundle file locally, select the bundle and confirm by clicking Download.

Collecting a Support Bundle from vCloud Availability Replication Manager
To collect the support bundle for vCloud Availability Replication Manager, perform the following steps:

1 In a Web browser, go to https://Replication–Manager–IP–address:8441/ui/admin. The vCloud Availability Replication Manager service management interface login page opens.
2 Log in as root.
3 Go to Support.
4 Click Generate New and confirm the operation by clicking Generate. A pop-up window indicating the process progress appears.
5 To save the support bundle file locally, select the bundle and confirm by clicking Download.

The vCloud Availability Replication Manager support bundle includes support bundles from all connected vCloud Availability Replicator instances.
Collecting a Support Bundle from vCloud Availability vApp Replication Manager

To collect the support bundle for vCloud Availability vApp Replication Manager by using the appliance graphic user interface, perform the following steps:

1. In a Web browser, go to https://vApp-Replication-Manager-IP-address/ui/login.
   The vCloud Availability vApp Replication Manager service management interface login page opens.
2. Log in as root.
3. Go to Support.
4. Click Generate New and confirm the operation by clicking Generate.
   A pop-up window indicating the process progress appears.
5. To save the support bundle file locally, select the bundle and confirm by clicking Download.

Collecting vCloud Availability Logs by Using Command Line Interface

To collect the support bundle for vCloud Availability vApp Replication Manager by using the appliance command-line interface, perform the following steps:

1. Create an SSH connection to the vCloud Availability vApp Replication Manager and log in as root.
2. Create a folder to store the support bundles.

   # mkdir bundles

3. Run the /opt/vmware/h4/bin/support-bundle.py script.
   You must provide the deployment type of your appliance and the output folder as arguments to the script. If you deployed a combined type appliance, the script collects all logs from the virtual machine. If you used other deployment types, you must create an SSH connection to each vCloud Availability appliance and run the script providing the respective deployment type and output folder as arguments. Following is an example of the command used to collect logs from a combined appliance:

   # /opt/vmware/h4/bin/support-bundle.py combined ./bundles

Upon a successful creation of the support bundle file, you receive the following message:
The support bundle was successfully generated at /root/bundles/bundle-YYYY-MM-DD_HH-mm-SS-Time-Zone(combined)-bundle-YYYY-MM-DD_HH-mm-SS-Time-Zone.tar.bz2.

4. Copy the logs archive to your machine.