

Installing, Configuring, and Upgrading VMware Cloud Director Object Storage Extension

17 NOV 2022

VMware Cloud Director Object Storage Extension 2.2

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

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

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

Copyright © 2022 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

- 1 What is VMware Cloud Director Object Storage Extension 4**
- 2 Deploying VMware Cloud Director Object Storage Extension 8**
 - Before you begin 9
 - Network ports configuration 11
 - AWS S3 Configuration Requirements 14
 - ECS Deployment Requirements 15
 - Cloudian Deployment Requirements 15
 - Configuring and Managing Multisite and Multi-region Deployments 17
 - Multisite and Multi-region Topologies 17
- 3 Installing and Configuring VMware Cloud Director Object Storage Extension 22**
 - VMware Cloud Director Object Storage Extension Command-Line Interface Reference 23
 - Install VMware Cloud Director Object Storage Extension 29
 - Configuring VMware Cloud Director Object Storage Extension 34
 - Configuring VMware Cloud Director Object Storage Extension with AWS 34
 - Configure VMware Cloud Director Object Storage Extension with ECS 37
 - Configure VMware Cloud Director Object Storage Extension with Cloudian HyperStore 40
 - Configure VMware Cloud Director Object Storage Extension with OSIS compliant object storage 43
 - Configure Additional VMware Cloud Director Object Storage Extension Instances Behind a Load Balancer 45
- 4 Uninstall VMware Cloud Director Object Storage Extension 46**
- 5 Upgrading VMware Cloud Director Object Storage Extension 48**
 - Prepare the Database for Upgrade 49

What is VMware Cloud Director Object Storage Extension

1

VMware Cloud Director Object Storage Extension is a standalone middleware service that you install in your data center to provide object storage capabilities to the users of VMware Cloud Director.

Architecture of VMware Cloud Director Object Storage Extension

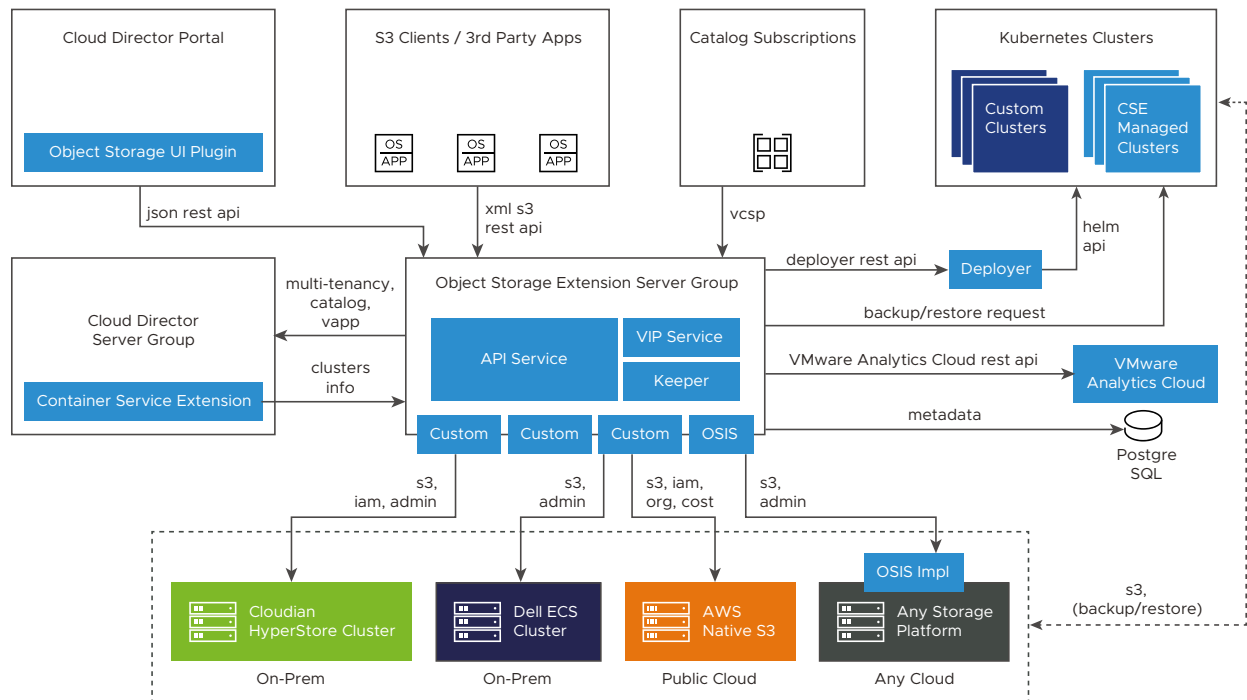
During installation and configuration, the user interface of VMware Cloud Director Object Storage Extension registers as a user interface plug-in to VMware Cloud Director by using the Portal Extensibility Framework. As a result, you can access the user interface of VMware Cloud Director Object Storage Extension directly from the VMware Cloud Director cloud provider admin portal as a system administrator and from the VMware Cloud Director tenant portal as an organization user.

You can configure VMware Cloud Director Object Storage Extension to work with AWS S3. You can also use the Object Storage Interoperability Service and configure VMware Cloud Director Object Storage Extension with any S3-compatible storage platform. VMware Cloud Director Object Storage Extension can still run on top of a Cloudfire HyperStore or a Dell EMC ECS storage cluster.

You can switch between storage platforms that you use with VMware Cloud Director Object Storage Extension, but cannot use two storage platforms at the same time.

An instance of VMware Cloud Director Object Storage Extension can work with a single instance of VMware Cloud Director or a single VMware Cloud Director server group.

The following diagram illustrates the architecture of VMware Cloud Director Object Storage Extension and the network connections between the components.



Components of VMware Cloud Director Object Storage Extension

VMware Cloud Director Object Storage Extension consists of four components.

Table 1-1. Components of VMware Cloud Director Object Storage Extension

Component	Description
Object Storage Interoperability Service (OSIS)	The service used for integrating any S3-compatible storage platform to VMware Cloud Director Object Storage Extension.
VMware Cloud Director Object Storage Extension Service	The public service of VMware Cloud Director Object Storage Extension that provides the APIs for the data path and the control path on port 443.

Table 1-1. Components of VMware Cloud Director Object Storage Extension (continued)

Component	Description
VMware Cloud Director Object Storage Extension Keeper (<code>voss-keeper</code>) Service	<p>The system service for the VMware Cloud Director Object Storage Extension service and the <code>ose</code> command-line utility. The <code>voss-keeper</code> service runs as a system service and you can manage it by using the <code>systemctl</code> command-line utility.</p> <p>Stopping the <code>voss-keeper</code> service also stops the VMware Cloud Director Object Storage Extension service on port 443.</p> <ul style="list-style-type: none"> ■ Installs and starts the VMware Cloud Director Object Storage Extension middleware service and the user interface plug-in. ■ Monitors the health of the Java daemon that VMware Cloud Director Object Storage Extension uses. ■ Synchronizes the configuration between VMware Cloud Director Object Storage Extension nodes within a cluster. ■ Installs and starts the internal virtual IP translation server.
Command-Line Utility (<code>ose</code>)	Contains the scripts required for configuring VMware Cloud Director Object Storage Extension and starting or stopping the Java daemon.
VMware Internationalization Protocol Service	This is an internal service that translates text strings within the user interface of VMware Cloud Director Object Storage Extension. The service runs as a system service and you can manage it by using the <code>systemctl</code> command-line utility.

Roles and Rights in VMware Cloud Director Object Storage Extension

Any user with an account that is activated from VMware Cloud Director perspective can access VMware Cloud Director Object Storage Extension.

The items you see and the actions you can perform depend on the rights assigned to your user profile within a VMware Cloud Director organization.

The rights assigned to your user profile in VMware Cloud Director define your user role in VMware Cloud Director Object Storage Extension.

The following table contains the mapping between VMware Cloud Director rights and VMware Cloud Director Object Storage Extension roles.

Table 1-2. Mapping Between VMware Cloud Director Rights and VMware Cloud Director Object Storage Extension Roles

VMware Cloud Director Object Storage Extension Tenant Portal Role	VMware Cloud Director Rights	Notes
Provider Administrator	<ul style="list-style-type: none"> ■ General: Administrator View ■ Provider VDC: View ■ Organization VDC: View ■ UI Plugins: View 	None.
Tenant Administrator	<ul style="list-style-type: none"> ■ General: Administrator View ■ Organization VDC: View ■ UI Plugins: View 	Tenant administrators in VMware Cloud Director Object Storage Extension must not have the Provider VDC: View role assigned to their user account in VMware Cloud Director. If you assign the Provider VDC: View role to a Tenant Administrator , the user role in VMware Cloud Director Object Storage Extension changes to Provider Administrator .
Tenant User	UI Plugins: View	Tenant users in VMware Cloud Director Object Storage Extension must not have the General: Administrator View and the General: Administrator View roles assigned to their user account in VMware Cloud Director. If you assign these roles to a Tenant User , the user role in VMware Cloud Director Object Storage Extension changes to Tenant Administrator .

For information about the predefined roles and their rights in VMware Cloud Director, see [Predefined Roles and Their Rights](#).

Deploying VMware Cloud Director Object Storage Extension

2

You install VMware Cloud Director Object Storage Extension on a Linux operating system.

VMware Cloud Director Object Storage Extension supports a list of Linux distributions and versions:

- CentOS Linux 8
- CentOS Linux 7
- Red Hat Enterprise Linux 7 or later
- Oracle Linux 7 or later
- Photon OS 3 or later
- Ubuntu 18 or later
- Debian 10 or later

To run VMware Cloud Director Object Storage Extension on a virtual machine, install Java JRE 8 or later.

Deployment Types and Hardware Requirements

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

Deployment Type	What to do?	VMware Cloud Director Object Storage Extension Hardware Requirements
Small	<p>Deploy a virtual storage appliance to your compute cluster. The compute cluster is where your tenant workloads are running.</p> <p>Deploy VMware Cloud Director Object Storage Extension to your management cluster. The management cluster is where your VMware Cloud Director cells are running.</p>	<ul style="list-style-type: none"> ■ 4 Core CPU ■ 8 GB RAM ■ 120 GB free disk space
Medium	<p>Deploy a virtual storage appliance to a dedicated ESXi host with large local disks.</p> <p>Deploy VMware Cloud Director Object Storage Extension to your management cluster. The management cluster is where your VMware Cloud Director cells are running.</p>	<ul style="list-style-type: none"> ■ 8 Core CPU ■ 8 GB RAM ■ 120 GB Free Disk Space
Large	<p>Configure storage platform services on a supported physical appliance.</p> <p>Deploy VMware Cloud Director Object Storage Extension to your management cluster. The management cluster is where your VMware Cloud Director cells are running.</p>	<ul style="list-style-type: none"> ■ 12 Core CPU ■ 12 GB RAM ■ 120 GB Free Disk Space

Read the following topics next:

- [Before you begin](#)
- [Network ports configuration](#)
- [AWS S3 Configuration Requirements](#)
- [ECS Deployment Requirements](#)
- [Clouddian Deployment Requirements](#)
- [Configuring and Managing Multisite and Multi-region Deployments](#)

Before you begin

Before you deploy VMware Cloud Director Object Storage Extension, you must prepare your environment. VMware Cloud Director Object Storage Extension requires specific external components of specific versions.

The following table lists the software components and the supported versions of the components that you must deploy and configure.

Required Component	Supported Versions
VMware Cloud Director	<ul style="list-style-type: none"> ■ 10.3 ■ 10.4 ■ 10.5 <p>Note To work with VMware Cloud Director Object Storage Extension, the VMware Cloud Director instance you use must support VMware Cloud Director cloud provider admin portal and VMware Cloud Director tenant portal.</p>
Cloudian HyperStore	<p>If you are deploying VMware Cloud Director Object Storage Extension on top of Cloudian HyperStore, a cluster of at least 3 Cloudian HyperStore nodes is required.</p> <p>You can configure VMware Cloud Director Object Storage Extension with Cloudian HyperStore versions 7.4 or later.</p> <p>To use multiple regions in VMware Cloud Director Object Storage Extension, you need Cloudian HyperStore version 7.4.2 or later.</p> <p>For more information about the requirements specific to Cloudian HyperStore, see Cloudian Deployment Requirements.</p>
Dell EMC ECS	<p>If you are deploying VMware Cloud Director Object Storage Extension on top of ECS, a cluster of at least 3 ECS nodes is required.</p> <p>VMware Cloud Director Object Storage Extension supports ECS versions 3.6 or later.</p> <p>For more information about the requirements specific to ECS, see ECS Deployment Requirements.</p>
Database	<p>PostgreSQL versions 10 to 14.</p> <p>Note The encoding and collation setting of the PostgreSQL database can affect the object synchronization from the storage platform. Verify that the encoding of database is UTF8, and the collation is <code>en_US.UTF-8</code>.</p> <p>If the locale of the OS where your Postgres database is deployed does not contain <code>en_US.UTF-8</code>, or you are not sure which collation method to set, you can set collation to the default value <code>c</code>.</p>

VMware Cloud Director Object Storage Extension requires a dedicated database instance and a database user that has sufficient privileges to create tables and change database schemas.

VMware Cloud Director Object Storage Extension does not require the RabbitMQ message bus for communication with VMware Cloud Director.

Make sure that the clocks of all VMware Cloud Director Object Storage Extension and storage platform nodes are synchronized. As a best practice, you can use the same Network Time Protocol (NTP) server.

Requirements for Virtual Hosted-Style S3 API Request

When you make an S3 API request, you can use path-style URI, for example `https://<ose-host>/<bucket>/<object>`, or `https://<ose-host>/api/v1/s3/<bucket>/<object>`. You can also use the virtual hosted-style URI, for example, `https://<bucket>.<s3-ose-host>/<object>`.

When you set the S3 API endpoint, you can use the following patterns:

- `https://<your-org-domain.com>`
- `https://s3.<region-name-here>.<your-org-domain.com>`
- `https://s3.<your-org-domain.com>`

To support virtual hosted-style S3 API requests, make sure the hostname of your VMware Cloud Director Object Storage Extension instance starts with `s3.` and that your DNS server can route virtual hosted-style requests.

For example, the hostname of your VMware Cloud Director Object Storage Extension instance is *example.com*. To route virtual hosted-style requests, add the following hostname mapping to DNS entries:

From	To
<code>*.s3.example.com</code>	<code>example.com</code>
<code>s3.example.com</code>	<code>example.com</code>

Network ports configuration

Ensure that the required network ports are open for the VMware Cloud Director Object Storage Extension services communication.

Table 2-1. Ports and Protocols Required for the VMware Cloud Director Object Storage Extension Services

Source	Destination	Port	Protocol	Description
VMware Cloud Director Object Storage Extension	AWS S3 Service, AWS Organizations Service, AWS IAM Service, and AWS Security Token Service	443	TCP	Used for communication between VMware Cloud Director Object Storage Extension and AWS services.
VMware Cloud Director cloud provider admin portal, VMware Cloud Director tenant portal, or an S3 client	VMware Cloud Director Object Storage Extension	443	TCP	The public API port of VMware Cloud Director Object Storage Extension.

Table 2-1. Ports and Protocols Required for the VMware Cloud Director Object Storage Extension Services (continued)

Source	Destination	Port	Protocol	Description
Kubernetes cluster to be protected	Docker Hub	443	TCP	Used when the Kubernetes cluster pulls Velero Docker images.
Kubernetes cluster to be protected	VMware Cloud Director Object Storage Extension	443	TCP	Used when the Kubernetes cluster performs a backup and restore with the VMware Cloud Director Object Storage Extension S3 endpoint.
VMware Cloud Director Object Storage Extension	VMware Cloud Director	443	TCP	Used for interactions with VMware Cloud Director.
VMware Cloud Director Object Storage Extension	ECS	443	TCP	Used for communication between VMware Cloud Director Object Storage Extension and the ECS Management Console .
VMware Cloud Director Object Storage Extension	Cloudian HyperStore	443, 80 (optional)	TCP	Used for communication between VMware Cloud Director Object Storage Extension and the Cloudian S3 Service.
VMware Cloud Director Object Storage Extension	ECS	4443	TCP	Used for communication between VMware Cloud Director Object Storage Extension and the ECS Admin Service.
VMware Cloud Director Object Storage Extension	ECS	4443	TCP	Used for communication between VMware Cloud Director Object Storage Extension and the ECS S3 Service.

Table 2-1. Ports and Protocols Required for the VMware Cloud Director Object Storage Extension Services (continued)

Source	Destination	Port	Protocol	Description
The <code>osse</code> utility on the Linux machine	VMware Cloud Director Object Storage Extension	5198	TCP	Used for configuring the VMware Cloud Director Object Storage Extension Keeper service (<code>voss-keeper</code>).
VMware Cloud Director Object Storage Extension	PostgreSQL Server	5432	TCP	Used for communication between the PostgreSQL database and VMware Cloud Director Object Storage Extension.
VMware Cloud Director Object Storage Extension	Kubernetes cluster to be protected	6443	TCP	Used when VMware Cloud Director Object Storage Extension deploys Velero to the Kubernetes cluster.
VMware Cloud Director Object Storage Extension	VMware Cloud Director Object Storage Extension	8091	TCP	Used for the translation-related communication between the VMware Cloud Director Object Storage Extension Service Java daemon and the internal VMware internationalization protocol Java daemon.
VMware Cloud Director Object Storage Extension	Cloudian HyperStore	8443	TCP	Used for communication between VMware Cloud Director Object Storage Extension and the Cloudian Management Console.

Table 2-1. Ports and Protocols Required for the VMware Cloud Director Object Storage Extension Services (continued)

Source	Destination	Port	Protocol	Description
VMware Cloud Director Object Storage Extension	Cloudian HyperStore	16443, 16080 (optional)	TCP	Used for communication between VMware Cloud Director Object Storage Extension and the Cloudian IAM Service.
VMware Cloud Director Object Storage Extension	Cloudian HyperStore	19443	TCP	Used for communication between VMware Cloud Director Object Storage Extension and the Cloudian Admin Service.

AWS S3 Configuration Requirements

To configure VMware Cloud Director Object Storage Extension with AWS S3, you need a payer AWS account.

Create an Identity and Access (IAM) user for your AWS payer account and use the IAM user to establish the connection between AWS and VMware Cloud Director Object Storage Extension instead.

Assign the following permission to the IAM user:

- **Amazon S3 Full Access**
- **AWS Organizations Full Access**
- **AWS IAM Full Access**
- **AWS STS Full Access**
- **AWS Key Management Service Power User**

To configure VMware Cloud Director Object Storage Extension with AWS S3, make sure that VMware Cloud Director Object Storage Extension has outbound access to AWS services.

Terminology Mapping

The AWS S3 terminology somewhat differs from the VMware Cloud Director Object Storage Extension terminology. The following table describes the mapping between different terms.

VMware Cloud Director Object Storage Extension Term	AWS S3 Term	Description
System Administrator	AWS Payer Account	The user account used by the cloud provider to configure and manage the service.
Tenant Organization	Organization Unit	The entity that a cloud provider creates to consolidate user accounts and compute resources. For more information about AWS Organizations, see https://docs.aws.amazon.com/organizations/latest/userguide/orgs_introduction.html .
Organization User	Identity and Access (IAM) User	The end user that consumes services. In AWS, each organization unit contains a default account. All IAM users in the organization unit belong to the default account.

ECS Deployment Requirements

If you want to deploy VMware Cloud Director Object Storage Extension on top of an ECS cluster, the ECS cluster must meet specific criteria.

Following is a list of the ECS components that you must deploy.

- An ECS Admin Service HTTPS API endpoint accessible from the internal network of VMware Cloud Director. By default, the endpoint is configured to use port 4443.
- ECS S3 Service accessible from the internal network of VMware Cloud Director. By default, the S3 service uses port 9021 for SSL communication.
- ECS Management Console accessible from external networks.

The object lock and the object tagging features for ECS are supported from ECS version 3.6.

To synchronize the clocks of all VMware Cloud Director Object Storage Extension and ECS nodes, use the same NTP server.

Cloudian Deployment Requirements

If you want to deploy VMware Cloud Director Object Storage Extension on top of a Cloudian cluster, the Cloudian cluster must meet specific requirements.

Required Cloudian Components

Following is a list of the Cloudian components that you must deploy.

- A Cloudian HyperStore cluster with at least three nodes.

- A Cloudian HyperStore Admin Service HTTPS API endpoint accessible from the internal network of VMware Cloud Director. By default, the endpoint is configured to use port 19443.
- Cloudian HyperStore S3 Service accessible from the internal network of VMware Cloud Director. By default, the S3 service uses port 443 for SSL communication.
- Cloudian HyperStore Identity and Access Management Service (IAM) accessible from the internal network of VMware Cloud Director. By default, the IAM service uses port 16443 for SSL communication.
- Cloudian Management Console accessible from external networks.

Required Configuration of Cloudian Components

VMware Cloud Director Object Storage Extension requires specific configurations of the Cloudian components in your environment.

Following is a list of specific configurations of Cloudian components that VMware Cloud Director Object Storage Extension requires.

- Activate single sign-on (SSO) and provide a unique shared key for the Cloudian Management Console. Note the shared key and the SSO login user, as you need them during the configuration of VMware Cloud Director Object Storage Extension.
- To meet the VMware Cloud Director user-mapping requirements, increase the maximum length of Cloudian HyperStore user IDs from 64 bytes to 255 bytes.
- Activate HyperStore Identity and Access Manager.
- Activate Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols on the S3 endpoint.
- Activate shared buckets lists.
- By default, Cloudian HyperStore is configured with an open HTTP port used for the S3 API communication. Use the Cloudian HyperStore HTTP port with VMware Cloud Director Object Storage Extension only if performance is more important than security. If your tenants need to use the SSE-C encryption type, an opened HTTPS port is required.
- Create a default storage policy. For more information, see *Getting Started with a New HyperStore System* in the *Cloudian HyperStore Admin Guide*.

To use the multi-region feature, you need Cloudian HyperStore version 7.4.1.3 or 7.5.1.

To synchronize the clocks of all VMware Cloud Director Object Storage Extension and Cloudian nodes, use the same NTP server.

For information about installing, configuring, and scaling Cloudian components for integration with VMware Cloud Director Object Storage Extension, see <https://cloudian.com/vmware-docs/>.

Configuring and Managing Multisite and Multi-region Deployments

You can deploy and configure VMware Cloud Director Object Storage Extension within a multisite VMware Cloud Director architecture, and within a multi-region architecture.

Multisite Deployment

A site refers to a VMware Cloud Director instance, which runs within a standalone geolocation. The VMware Cloud Director multisite feature enables a service provider or a tenant of multiple, geographically distributed VMware Cloud Director installations (server groups) to manage and monitor those installations and their organizations as single entities.

By configuring VMware Cloud Director Object Storage Extension within a multisite architecture, you enable tenant users to preview and download objects in remote sites.

With the multisite feature, you achieve high availability and provide a single point of data access for organization users.

Multi-region Deployment

A region refers to an object storage cluster, which runs within a standalone geolocation, with a unique S3 API endpoint. The VMware Cloud Director Object Storage Extension multi-region feature allows the cloud provider to group multiple regions of object storage clusters to a central management plane, on a single VMware Cloud Director site, or across multiple VMware Cloud Director sites.

By grouping multi-region object storage clusters, you can activate S3 regions for specific tenant organizations and tenant users can create buckets within the multi-regions.

VMware Cloud Director Object Storage Extension 2.2 supports the multi-region feature on the Cloudian platform.

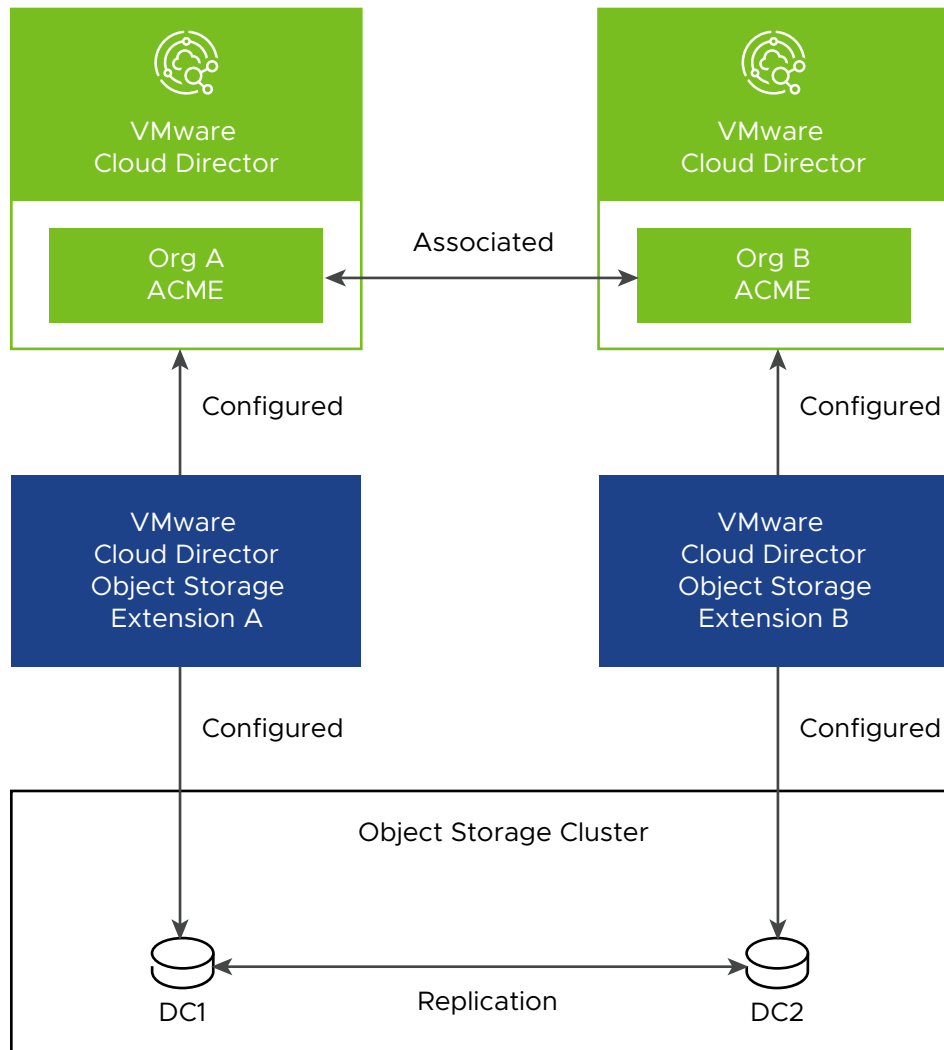
Multisite and Multi-region Topologies

You can configure multisite VMware Cloud Director instances with multi-region object storage clusters within the following configurations:

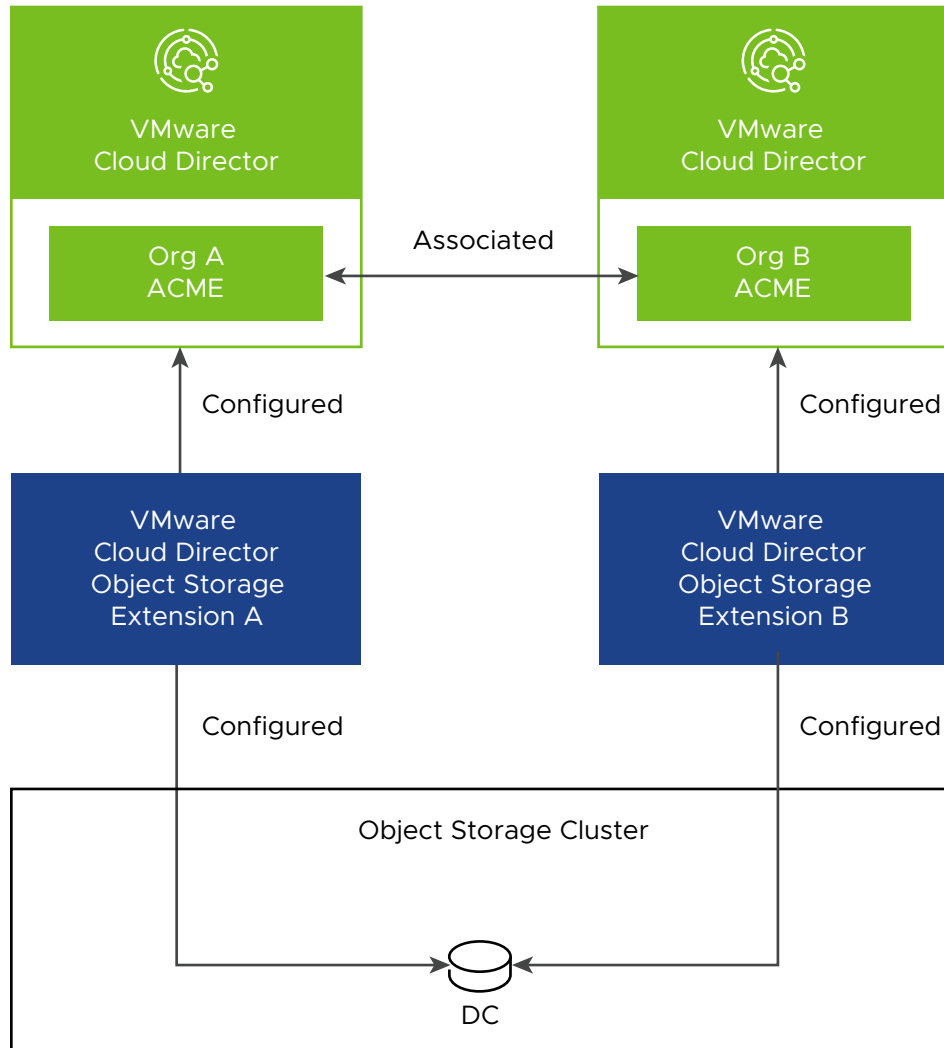
- Multisite single region topology
- Single site multi-region topology
- Multisite multi-region topology

Multisite Single Region Topology

Within a multisite architecture, you can configure VMware Cloud Director Object Storage Extension instances with a standalone virtual data center in each site. The following diagram illustrates the architecture.



You can also configure VMware Cloud Director Object Storage Extension instances in different sites to use a single virtual data center. The following diagram illustrates the architecture.



When you configure the multisite feature, you create a cluster of multiple VMware Cloud Director Object Storage Extension instances to create an availability zone. You can group the VMware Cloud Director Object Storage Extension instances together only in a single region. A region is a collection of compute resources in a geographic area. Regions are isolated and independent of one another. VMware Cloud Director Object Storage Extension does not support multi-region architectures.

You can share the same buckets and objects across tenant organizations within a multisite environment. To share buckets and objects across sites, map all tenant organizations to the same storage group. See [Edit Tenant Mapping Configuration](#).

Multisite Deployment Requirements for VMware Cloud Director Object Storage Extension

When you configure the multisite feature with VMware Cloud Director Object Storage Extension, consider the following requirements.

- Associate the VMware Cloud Director sites that you want to use in the multisite environment. For more information, see the *VMware Cloud Director Service Provider Admin Portal Guide*.

- Deploy and configure a VMware Cloud Director Object Storage Extension instance in each site.
- You can share your storage platform cluster across sites, or you can deploy and configure all required storage components in each site.
- Join the storage clusters into a distribution group.

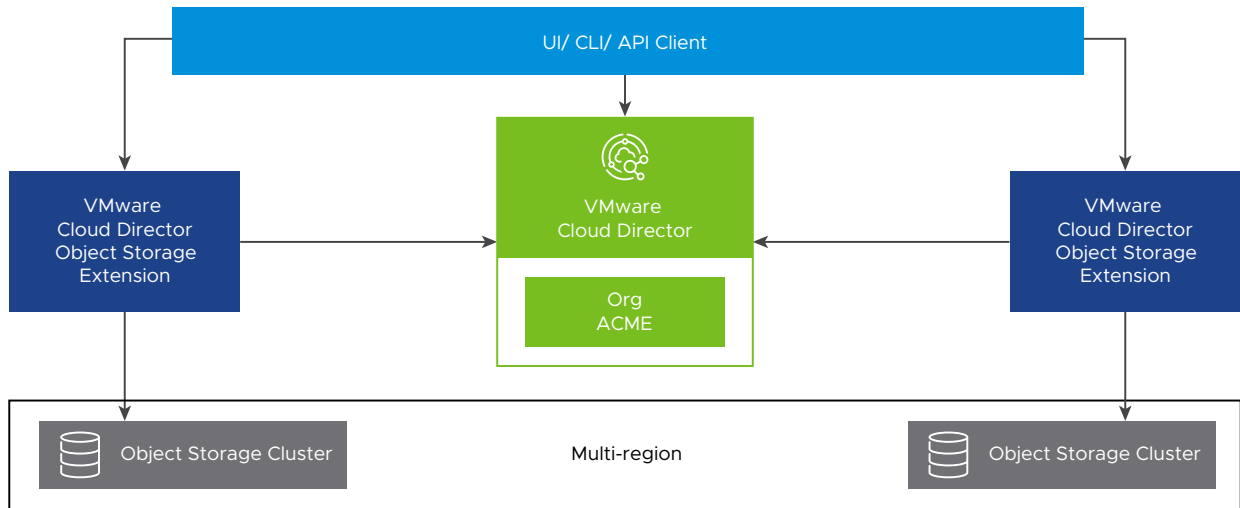
For Cloudian HyperStore, set up a storage policy with a multi-DC data distribution group.

For ECS, set up replication groups across the virtual data centers.

- For AWS S3, use the same AWS payer account to configure VMware Cloud Director Object Storage Extension. Also, make sure that all VMware Cloud Director Object Storage Extension sites are configured with an AWS S3 endpoint in the same region.

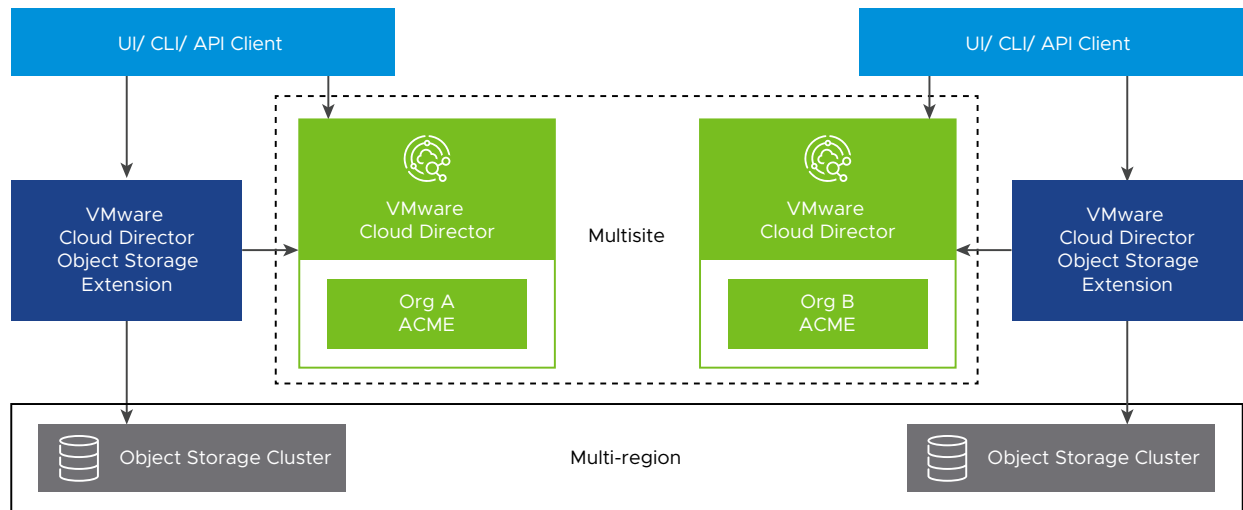
Single Site Multi-region Topology

When you deploy multi-region object storage clusters, you can deploy one VMware Cloud Director Object Storage Extension server to each object storage cluster. You can connect multiple VMware Cloud Director Object Storage Extension servers to the same VMware Cloud Director site. The following diagram illustrates the architecture.



Multisite Multi-Region Topology

When you deploy multi-region object storage clusters, you can associate multi-region object storage to multisite VMware Cloud Director instances. You can deploy one VMware Cloud Director Object Storage Extension server to each object storage cluster. The VMware Cloud Director Object Storage Extension servers connect to the multisite VMware Cloud Director Object Storage Extension. On both the local and remote sites, tenant users can use multi-region object storage with a multisite VMware Cloud Director topology. The following diagram illustrates the architecture.



Installing and Configuring VMware Cloud Director Object Storage Extension

3

You can install VMware Cloud Director Object Storage Extension on different Linux distributions.

The VMware Cloud Director Object Storage Extension installation and configuration consist of deploying and configuring not only the VMware Cloud Director Object Storage Extension services, but also of configuring all external components to work with VMware Cloud Director Object Storage Extension.

For scaling purposes, you can deploy and configure multiple instances of VMware Cloud Director Object Storage Extension behind a load balancer.

Following is a list of the steps you take to install and configure VMware Cloud Director Object Storage Extension:

- 1 Install the VMware Cloud Director Object Storage Extension installation package.
- 2 Import an externally signed SSL certificate to VMware Cloud Director Object Storage Extension.
- 3 Connect to a preconfigured database.
- 4 Connect to an instance of VMware Cloud Director.
- 5 Configure the VMware Cloud Director Object Storage Extension endpoint region information.
- 6 Install the VMware Cloud Director Object Storage Extension user interface.
- 7 Start the Kubernetes Backup and Restore service.
- 8 Configure the connection to the storage platform components or the AWS services.

Read the following topics next:

- [VMware Cloud Director Object Storage Extension Command-Line Interface Reference](#)
- [Install VMware Cloud Director Object Storage Extension](#)
- [Configuring VMware Cloud Director Object Storage Extension](#)
- [Configure Additional VMware Cloud Director Object Storage Extension Instances Behind a Load Balancer](#)

VMware Cloud Director Object Storage Extension

Command-Line Interface Reference

The following table describes the `ose` command-line interface scripts.

Script	Description
<code>ose</code>	Returns details about the <code>ose</code> command-line utility.
<code>ose --version</code>	Returns the version of VMware Cloud Director Object Storage Extension that you run.
<code>ose show</code>	Returns all VMware Cloud Director Object Storage Extension configuration details. You can optionally add the <code>--with-secret</code> argument and the system returns the passwords that you set during installation and configuration.
SSL Certificate Management Scripts	
<code>ose cert gen</code>	Generates a new self-signed SSL certificate for the VMware Cloud Director Object Storage Extension service. The <code>--cn</code> and <code>--secret</code> arguments are required. The <code>--cn</code> argument value, must be the common name of the VMware Cloud Director Object Storage Extension host. The <code>--secret</code> argument value must be the password of the keystore.
<code>ose cert import</code>	Imports an externally signed SSL certificate. The <code>--path</code> and <code>--secret</code> arguments are required. The <code>--path</code> argument value must be the full path to the <code>.p12</code> certificate file. The <code>--secret</code> argument value must be the password of the keystore. You can optionally add the <code>--force</code> argument to avoid the password validation.
<code>ose cert show</code>	Returns details about the SSL certificate that VMware Cloud Director Object Storage Extension uses. You can optionally add the <code>--with-secret</code> argument to get the password of the keystore.
Database Configuration Scripts	
<code>ose db set</code>	Configures a connection between your database instance and VMware Cloud Director Object Storage Extension. The <code>--url</code> , <code>--user</code> , and <code>--secret</code> arguments are required. The <code>--url</code> argument value must be the URL of your database instance. The <code>--user</code> and <code>--secret</code> arguments values must be the credentials of the database user. You can use the <code>--ssl-mode</code> parameter to set the SSL mode of the database. You can use the <code>--ssl-cert-path</code> to set the SSL certificate filepath for the database instance. You can optionally add the <code>--force</code> argument to avoid the password validation.

Script	Description
<code>ose db show</code>	Returns details about the database configuration. You can optionally add the <code>--with-secret</code> argument to get the password of the database user.
VMware Cloud Director Configuration Scripts	
<code>ose director set</code>	Configures a connection between VMware Cloud Director and VMware Cloud Director Object Storage Extension. The <code>--url</code> , <code>--user</code> , and <code>--secret</code> arguments are required. The <code>--url</code> argument value must be the URL of your VMware Cloud Director instance. The <code>--user</code> and <code>--secret</code> arguments values must be the credentials of a VMware Cloud Director system administrator. You can optionally add the <code>--force</code> argument to avoid the password validation.
<code>ose director show</code>	Returns details about the VMware Cloud Director configuration. You can optionally add the <code>--with-secret</code> argument to get the password of the VMware Cloud Director user account.
<code>ose endpoint set</code>	Sets the URL and the region name for the VMware Cloud Director Object Storage Extension endpoint.
<code>ose ui install</code>	Installs the VMware Cloud Director Object Storage Extension user interface plug-in for VMware Cloud Director.
<code>ose ui uninstall</code>	Uninstalls the VMware Cloud Director Object Storage Extension user interface plug-in for VMware Cloud Director.
<code>ose ui show</code>	Returns details about the configuration of the VMware Cloud Director Object Storage Extension user interface plug-in for VMware Cloud Director.
Storage Platform Configuration Scripts	
<code>ose platforms enable</code>	Allows VMware Cloud Director Object Storage Extension to work with either Cloudian or ECS storage platforms. To activate the Cloudian storage platform, run the <code>ose platforms enable cloudian</code> script. To activate the ECS storage platform, run the <code>ose platforms enable ecs</code> script. To activate the AWS S3 storage service, run the <code>ose platforms enable amazon</code> script. To activate the Object Storage Interoperability Service, run the <code>ose platforms enable osis</code> script. The <code>--name</code> argument is required and defines a unique name for the Object Storage Interoperability Service instance.
<code>ose platforms show</code>	Returns details about the platform that is configured for use in VMware Cloud Director Object Storage Extension.
AWS S3 Configuration Scripts	

Script	Description
<code>ose amazon set</code>	<p>Configures the connection to AWS S3.</p> <p>The <code>--region</code>, <code>--access-key</code>, and <code>--secret-key</code> arguments are required.</p> <p>The <code>--region</code> argument value must be the region of the AWS payer account.</p> <p>The <code>--access-key</code> and <code>--secret-key</code> values must be the access and secret keys of the AWS payer account.</p>
<code>ose amazon show</code>	<p>Returns details about the AWS S3 configuration.</p> <p>You can optionally add the <code>--with-secret</code> argument to get the secret key of the AWS payer account.</p>
Cloudian Configuration Scripts	
<code>ose cloudian admin set</code>	<p>Configures a connection between the Cloudian Admin service and VMware Cloud Director Object Storage Extension.</p> <p>The <code>--url</code>, <code>--user</code>, and <code>--secret</code> arguments are required.</p> <p>The <code>--url</code> argument value must be the URL of the Cloudian Admin service.</p> <p>The <code>--user</code> and <code>--secret</code> arguments values must be the credentials of a Cloudian Admin service administrator user.</p> <p>You can optionally add the <code>--force</code> argument to avoid the password validation.</p>
<code>ose cloudian s3 set</code>	<p>Configures a connection between the Cloudian S3 service and VMware Cloud Director Object Storage Extension.</p> <p>The <code>--url</code> argument is required and the value must be the FQDN or the IP address of the S3 service.</p> <p>If you use the FQDN, make sure that you correctly configure the S3 Service domain in the Cloudian HyperStore cluster. Also, make sure that your DNS server can route all bucket requests from the virtual to the actual S3 Service host. For example, from <i>bucket-name.hyper-store-s3-host</i> to <i>hyper-store-s3-host</i>. If you use the IP address of the S3 Service, no domain and virtual host route settings are required.</p>
<code>ose cloudian iam set</code>	<p>Configures a connection between the Cloudian IAM service and VMware Cloud Director Object Storage Extension.</p> <p>The <code>--url</code> argument is required and the value must be the URL of the Cloudian IAM service.</p>
<code>ose cloudian console set</code>	<p>Configures the connection between the Cloudian Management Console and VMware Cloud Director Object Storage Extension.</p> <p>The <code>--url</code>, <code>--user</code>, and <code>--secret</code> arguments are required.</p> <p>The <code>--url</code> argument value must be the URL of the Cloudian Management Console.</p> <p>The <code>--user</code> argument value must be the user name of a Cloudian system administrator.</p> <p>The <code>--secret</code> argument value must be the single sign-on shared key that is configured in the Cloudian Management Console.</p> <p>You can optionally add the <code>--force</code> argument to avoid the password validation.</p>

Script	Description
<code>ose cloudian show</code>	Returns details about the configuration of Cloudian components. You can optionally add the <code>--with-secret</code> argument to get the passwords of the Cloudian user accounts.
ECS Configuration Scripts	
<code>ose ecs admin set</code>	Configures a connection between the ECS Admin service and VMware Cloud Director Object Storage Extension. The <code>--url</code> , <code>--user</code> , and <code>--secret</code> arguments are required. The <code>--url</code> argument value must be the URL of the ECS Admin service. The <code>--user</code> and <code>--secret</code> arguments values must be the credentials of an ECS Admin service administrator user. You can optionally add the <code>--force</code> argument to avoid the password validation.
<code>ose ecs s3 set</code>	Configures a connection between the ECS S3 service and VMware Cloud Director Object Storage Extension. The <code>--url</code> argument is required. The argument value must be the FQDN or the IP address of the S3 service. Make sure that your DNS server can route all bucket requests from the virtual to the actual S3 service host. For example, from <i>bucket-name.hyper-store-s3-host</i> to <i>hyper-store-s3-host</i> . If you use the IP address of the S3 service, no domain and virtual host route settings are required.
<code>ose ecs console set</code>	Configures a connection between the ECS Management Console and VMware Cloud Director Object Storage Extension. The <code>--url</code> , <code>--user</code> , and <code>--secret</code> arguments are required. The <code>--url</code> argument value must be the URL of the ECS Management Console. The <code>--user</code> and <code>--secret</code> arguments values must be the credentials of an ECS administrator user. You can optionally add the <code>--force</code> argument to avoid the password validation.
<code>ose ecs show</code>	Returns details about the configuration of ECS components. You can optionally add the <code>--with-secret</code> argument to get the passwords of the ECS user accounts.
Object Storage Interoperability Service Configuration Scripts	

Script	Description
<code>ose osis admin set</code>	<p>Configures a connection between VMware Cloud Director Object Storage Extension and the admin service of the Object Storage Interoperability Service instance.</p> <p>The <code>--name</code>, <code>--url</code>, <code>--user</code>, and <code>--secret</code> arguments are required.</p> <p>The <code>--name</code> argument value must be the name of the Object Storage Interoperability Service instance.</p> <p>The <code>--url</code> argument value must be the URL of the Object Storage Interoperability Service admin service.</p> <p>The <code>--user</code> and <code>--secret</code> arguments values must be the credentials of an Object Storage Interoperability Service admin service administrator user.</p> <p>You can optionally add the <code>--force</code> argument to avoid the password validation.</p>
<code>ose osis s3 set</code>	<p>Configures a connection between the Object Storage Interoperability Service S3 service and VMware Cloud Director Object Storage Extension.</p> <p>The <code>--name</code> argument is required and the value must be the name of the Object Storage Interoperability Service instance.</p> <p>The <code>--url</code> argument is required and the value must be the FQDN or the IP address of the S3 service.</p>
VMware Cloud Director Object Storage Extension Service Configuration Scripts	
<code>ose args set</code>	<p>Sets VMware Cloud Director Object Storage Extension service arguments. Service arguments are a key-value pair. Use the <code>--k</code> and <code>--v</code> arguments to define the key and value.</p> <p>The <code>--k</code> argument value must be the key and the <code>--v</code> argument value must be the value.</p>
<code>ose args get</code>	<p>Returns details about a VMware Cloud Director Object Storage Extension service argument.</p> <p>Use the <code>--k</code> argument to retrieve service arguments by their key.</p>
<code>ose args del</code>	<p>Deletes VMware Cloud Director Object Storage Extension service arguments.</p> <p>Use the <code>--k</code> argument to delete service arguments by their key.</p>
<code>ose args show</code>	Returns details about all VMware Cloud Director Object Storage Extension service argument.
<code>ose service start</code>	<p>Starts the VMware Cloud Director Object Storage Extension service.</p> <p>You can optionally add the <code>--debug</code> argument to change the service logging level to <code>debug</code>.</p>
<code>ose service stop</code>	Stops the VMware Cloud Director Object Storage Extension service.
<code>ose service restart</code>	<p>Restarts the VMware Cloud Director Object Storage Extension service.</p> <p>You can optionally add the <code>--debug</code> argument to change the service logging level to <code>debug</code>.</p>
<code>ose service show</code>	Returns the VMware Cloud Director Object Storage Extension service status and configuration.

Script	Description
Kubernetes Backup and Restore Scripts	
<code>ose k8s-br start</code>	Starts the VMware Cloud Director Object Storage Extension Kubernetes backup and restore service.
<code>ose k8s-br show</code>	Returns the VMware Cloud Director Object Storage Extension Kubernetes backup and restore service status.
<code>ose k8s-br stop</code>	Stops the VMware Cloud Director Object Storage Extension Kubernetes backup and restore service.
Data Migration Scripts	
<code>ose migration start</code>	Starts data migration from VMware Cloud Director Object Storage Extension version 1.0 to version 1.0.1 or from version 1.0 to version 1.5. To restart the process, rerun the script with the <code>--force</code> argument.
<code>ose migration show</code>	Returns details about the migration progress.
Configuration Scripts	
<code>ose config validate</code>	Validates the configuration of VMware Cloud Director Object Storage Extension.
<code>ose config export</code>	Exports the configuration of VMware Cloud Director Object Storage Extension to a JSON file. The <code>--file</code> and <code>--secret</code> arguments are required. The <code>--file</code> argument value must be the export filename. The <code>--secret</code> argument value must be the password of a VMware Cloud Director system administrator.
<code>ose config import</code>	Imports the configuration of VMware Cloud Director Object Storage Extension from a JSON file. The <code>--path</code> and <code>--secret</code> arguments are required. The <code>--file</code> argument value must be the source directory for the import. The <code>--secret</code> argument value must be the password of a VMware Cloud Director system administrator.
Administration Scripts	
<code>ose support</code>	Generates a support bundle. The <code>--start</code> argument is optional and defines the start time for the logs to be collected. The default value is 2018-01-01. The <code>--end</code> argument is optional and defines the end time for the logs to be collected. If not specified, the end date is the current date. For the <code>--start</code> and the <code>--end</code> arguments values, enter the date in the YYYY-MM-DD format.
Java Virtual Machine (JVM) Configuration Scripts	
<code>ose jvmargs set</code>	Configures the JVM arguments. Use the <code>-v</code> argument to define the JVM arguments. For example, to set an HTTP proxy, run the following command: <code>ose jvmargs -v "Dhttp.proxyHost=proxy.cloud.com -Dhttp.proxyPort=3128"</code> .

Script	Description
<code>ose jvmargs delete</code>	Deletes the JVM arguments configuration.
<code>ose jvmargs show</code>	Returns details about the JVM arguments configuration.

Install VMware Cloud Director Object Storage Extension

To install VMware Cloud Director Object Storage Extension, deploy an installation package to a target Linux virtual machine and use the `ose` command-line utility to configure VMware Cloud Director Object Storage Extension and the external components.

For security purposes, VMware Cloud Director Object Storage Extension validates the complexity of all passwords. When you set passwords by using the `ose` command-line utility, make sure that the password contains:

- At least eight characters
- Minimum one uppercase character
- Minimum one lowercase character
- Minimum one numeric digit character
- Minimum one non-alphanumeric character.

Use only visible ASCII characters. Do not use space and non-printing control characters, such as BEL or NUL.

VMware Cloud Director Object Storage Extension performs a password validation as part of the execution of the following scripts:

- `ose cert import`
- `ose director set`
- `ose db set`

For testing purposes, you can avoid the password validation by adding the `--force` argument to the script that you run.

Prerequisites

- Verify that your target environment and target machine meet the deployment and hardware requirements. See [Chapter 2 Deploying VMware Cloud Director Object Storage Extension](#).
- Verify that you have a dedicated database instance and a database user that has enough privileges to create tables and change schemas.
- Verify that the installation package is uploaded to the `/temp` directory of the target machine.
- Verify that you have installed Openssl 1.x on the target machine.

Procedure

- 1 Open an SSH connection to the target machine and log in as **root**.
- 2 Install VMware Cloud Director Object Storage Extension from the installation package.

For this Linux distribution...	Use this command...
CentOS, Red Hat Enterprise Linux, Oracle Linux	<code>yum install /temp/vmware-ose-2.2-17852793.el7.x86_64.rpm</code>
Photon OS	<code>rpm -ivh /temp/vmware-ose-2.2-52392538.ph3.x86_64.rpm</code>
Ubuntu, Debian	<code>sudo apt-get install /temp/vmware-ose_\${v.v.v-\$nnnnnnnn}.deb</code>

The VMware Cloud Director Object Storage Extension Keeper Service starts immediately after the installation package is installed.

Important If you are deploying the installation package as part of upgrading VMware Cloud Director Object Storage Extension, do not perform any further command-line configuration steps. Keep the VMware Cloud Director Object Storage Extension server running for about a minute and continue the upgrade process. See [Chapter 5 Upgrading VMware Cloud Director Object Storage Extension](#).

If you are deploying the installation package as part of a clean installation of VMware Cloud Director Object Storage Extension, proceed to the next step.

- 3 Verify that the `ose` command-line utility works, by running the following command:

For this Linux distribution...	Use this command...
CentOS, Red Hat Enterprise Linux, Photon OS, Oracle Linux	<code>ose -h</code>
Ubuntu, Debian	<code>sudo ose -h</code>

The system returns help information about the `ose` command-line utility.

4 Import an externally signed SSL certificate.

- a Prepare the PKCS 12 keystore with the externally signed certificate and a unique alias by running the `export` command.

For this Linux distribution...	Use this command...
CentOS, Red Hat Enterprise Linux, Photon OS, Oracle Linux	<pre>openssl pkcs12 -export -in cert-file-name.cer -inkey s3.key -CAfile CA-cert-file-name.cer -passout pass:password -out PKCS-file-name.p12 -chain -name unique-cert-alias</pre>
Ubuntu, Debian	<pre>sudo openssl pkcs12 -export -in cert-file-name.cer -inkey s3.key -CAfile CA-cert-file-name.cer -passout pass:password -out PKCS-file-name.p12 -chain -name unique-cert-alias</pre>

In the current example, the `openssl` tool is used for exporting the certificate. You can use an alternative tool.

For example:

```
openssl pkcs12 -export -in s3.cer -inkey s3.key -CAfile CA.cer -passout pass:ChangeIt!
-out s3.p12 -chain -name s3
```

- b Import the certificate to your PKCS12 keystore by running the `import` command.

For this Linux distribution...	Use this command...
CentOS, Photon OS, Oracle Linux	<pre>ose cert import --path path-to-keystore-file --secret 'password-of-the-keystore'</pre>
Red Hat Enterprise Linux	<pre>ose config import -file ph3config -secret vmware</pre>
Ubuntu, Debian	<pre>sudo ose cert import --path path-to-keystore-file -- secret 'password-of-the-keystore'</pre>

If the password that you enter contains a single quote character ('), run the command without the `--secret` argument. The system prompts you to enter the password on a new line.

For example:

```
ose cert import --path ./ose-service.p12 --secret 'ChangeIt!'
```

for RPM packages or

```
sudo ose cert import --path ./ose-service.p12 --secret 'ChangeIt!'
```

for DEB packages.

- a For testing purposes, instead of importing a certificate, you can generate a self-signed SSL certificate by running the following command:

For this Linux distribution...	Use this command...
CentOS, Red Hat Enterprise Linux, Photon OS, Oracle Linux	<code>ose cert gen --cn common-name-of-` --secret <i>certificate-password</i></code>
Ubuntu, Debian	<code>sudo ose cert gen --cn common-name-of-ose-host --secret <i>certificate-password</i></code>

For example, `ose cert gen --cn s3.acme.com`.

5 Configure the database connection.

For this Linux distribution...	Use this command...
CentOS, Red Hat Enterprise Linux, Photon OS, Oracle Linux	<code>ose db set --url jdbc:postgresql://db_host:db_port/db_instance --user 'db-user' --secret 'db-password'</code>
Ubuntu, Debian	<code>sudo ose db set --url jdbc:postgresql://db_host:db_port/db_instance --user 'db-user' --secret 'db-password'</code>

If the password that you enter contains a single quote character ('), run the command without the `--secret` argument. The system prompts you to enter the password on a new line.

For example:

```
ose db set --url jdbc:postgresql://localhost:5432/ossdb --user oseadmin --secret
'ChangeIt!'
```

6 Configure the connection to VMware Cloud Director.

For this Linux distribution...	Use this command...
CentOS, Red Hat Enterprise Linux, Photon OS, Oracle Linux	<code>ose director set --url vcd-url --user vcd-sysadmin-user@system --secret 'vcd-sysadmin-password'</code>
Ubuntu, Debian	<code>sudo ose director set --url vcd-url --user vcd-sysadmin-user@system --secret 'vcd-sysadmin-password'</code>

Important For the `--user` argument value, if you are installing VMware Cloud Director Object Storage Extension to a multisite VMware Cloud Director environment, make sure that the **system administrator** account can log in to all sites.

The system administrator user name that you enter must be with an `@system` suffix.

For example:

```
ose director set --url https://vcd.acme.com --user vcd-admin-user@system --secret
'ChangeIt!'
```

If the password you enter contains a single quote character ('), run the command without the `--secret` argument and the system prompts you to enter the password in a new line.

- 7 If you want to use the Kubernetes backup and restore feature, you must start the service.

For this Linux distribution...	Use this command...
CentOS, Red Hat Enterprise Linux, Photon OS, Oracle Linux	<code>ose k8s-br start</code>
Ubuntu, Debian	<code>sudo ose k8s-br start</code>

- 8 Set the URL and region for the VMware Cloud Director Object Storage Extension endpoint.

For this Linux distribution...	Use this command...
CentOS, Red Hat Enterprise Linux, Photon OS, Oracle Linux	<code>ose endpoint set --url=ose-host-url</code>
Ubuntu, Debian	<code>sudo ose endpoint set --url=ose-host-url</code>

Here, *ose-host-url* is the public server endpoint of VMware Cloud Director Object Storage Extension. Typically, the public server endpoint is the HTTPS URL of the VMware Cloud Director Object Storage Extension host on port 443. The URL becomes available after you complete the configuration and start the VMware Cloud Director Object Storage Extension service. Make sure that the URL is open for a public access.

If you deploy multiple instances of VMware Cloud Director Object Storage Extension behind a load balancer, the *ose-host-url* must be the public FQDN of VMware Cloud Director Object Storage Extension.

- 9 Install the VMware Cloud Director Object Storage Extension user interface plug-in.

For this Linux distribution...	Use this command...
CentOS, Red Hat Enterprise Linux, Photon OS, Oracle Linux	<code>ose ui install</code>
Ubuntu, Debian	<code>sudo ose ui install</code>

What to do next

Configure VMware Cloud Director Object Storage Extension with a Cloudian HyperStore or an ECS cluster.

Configuring VMware Cloud Director Object Storage Extension

You can configure VMware Cloud Director Object Storage Extension with AWS S3, with a Dell EMC ECS, with a Cloudian HyperStore cluster, or with any S3 compliant object storage cluster that implements the Object Storage Interoperability Service (OSIS) interface.

If you are using an S3 compliant object storage cluster other than AWS, Cloudian HyperStore or DELL ECS, you can integrate VMware Cloud Director Object Storage Extension by implementing the Object Storage Interoperability Service (OSIS) interface. For more information, please refer to [Object Storage Interoperability Service Development Guide](#).

After you deploy VMware Cloud Director Object Storage Extension and configure the connections to VMware Cloud Director and your dedicated database, you configure the connections to the underlying storage platform or service.

Configuring VMware Cloud Director Object Storage Extension with AWS

Before you configure VMware Cloud Director Object Storage Extension with AWS, activate policy types for the AWS organization. You must also assign the **AWS STS Full Access** privileges for the AWS organization to the AWS IAM user that you use for the configuration of VMware Cloud Director Object Storage Extension.

After you prepare your AWS environment, you configure VMware Cloud Director Object Storage Extension with AWS by establishing connections between VMware Cloud Director Object Storage Extension and AWS services.

Prepare Your AWS Environment for Configuration

Before you configure VMware Cloud Director Object Storage Extension with AWS, activate policy types in your AWS organization and create a specific policy for the IAM user that you use for the configuration with VMware Cloud Director Object Storage Extension.

Procedure

- 1 Activate policy types for the AWS organization that you will configure with VMware Cloud Director Object Storage Extension.

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_enable-disable.html

- 2 Create a policy with **AWS STS Full Access** privileges.
 - a In a Web browser, go to the AWS IAM Console at <https://console.aws.amazon.com/iam/home> and sign in.
 - b On the **Access Management** tab, in the left navigation pane, click **Policies**.
 - c In the details pane on the right side, click **Create Policy**.

- d If you use the visual editor, select **STS Service**, **All STS actions**, and **All Resources**.

If you use the JSON editor, enter the following string:

```
{
  "Version": "YYYY-MM-DD",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:*",
      "Resource": "*"
    }
  ]
}
```

- e Click **Review Policy**.

- f To save the policy, enter a name for the policy, for example, **STSTFullAccess**.

- 3 Assign permissions to the IAM user that you will use for configuring VMware Cloud Director Object Storage Extension with AWS.

Important It is advised that you create an Identity and Access Management (IAM) user for your AWS payer account and use the IAM user to establish the connection between AWS and VMware Cloud Director Object Storage Extension instead.

Assign the following permission to the IAM user:

- **Amazon S3 Full Access**
 - **AWS Organizations Full Access**
 - **AWS IAM Full Access**
 - **AWS STS Full Access** (user-defined)
 - **AWS Key Management Service Power User**
-

For more information, see https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_change-permissions.html.

What to do next

You can now configure VMware Cloud Director Object Storage Extension with AWS.

Configure VMware Cloud Director Object Storage Extension with AWS

To configure VMware Cloud Director Object Storage Extension with AWS, you provide the region, the secret, and the access keys of your AWS payer account.

When you configure VMware Cloud Director Object Storage Extension with AWS, you establish the connection to the following AWS services:

- Identity and Access Management (IAM) Service
- Simple Storage Service (S3)

- Security Token Service (STS)
- Organization Service

Prerequisites

- Verify that you prepared your AWS environment for configuration with VMware Cloud Director Object Storage Extension. See [Prepare Your AWS Environment for Configuration](#).
- Verify that VMware Cloud Director Object Storage Extension has outbound access to AWS services.

Procedure

- 1 Open an SSH connection to the machine on which you installed VMware Cloud Director Object Storage Extension.
- 2 Start the VMware Cloud Director Object Storage Extension Keeper service.

```
systemctl start voss-keeper
```

- 3 Configure the connection to AWS S3.

```
ose amazon set --region aws-payer-account-region --access-key account-access-key --secret-key account-secret-key
```

For example:

```
ose amazon set --region us-east-1 --access-key AKIAIOSFODNN7EXAMPLE --secret-key wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
```

- 4 Allow the use of AWS S3.

```
ose platforms enable amazon
```

- 5 Validate the configuration.

```
ose config validate
```

If all components are successfully configured, the system returns the following message:

```
+-----+-----+-----+-----+
|           Name           | Required | Connectivity | Detail |
+=====+=====+=====+=====+
|           Database       |         Y |         Normal |        |
+-----+-----+-----+-----+
|           Certificate     |         Y |         Normal |        |
+-----+-----+-----+-----+
|         Cloud Director   |         Y |         Normal |        |
+-----+-----+-----+-----+
|        Platform - AWS    |         Y |         Normal |        |
+-----+-----+-----+-----+
|      AWS IAM service     |         Y |         Normal |        |
```

AWS S3 service		Y	Normal		
AWS STS service		Y	Normal		
AWS Organization service		Y	Normal		

If the system returns an error, review the log file at `/opt/vmware/voss/log`.

6 Verify the status of the VMware Cloud Director Object Storage Extension service.

```
ose service show
```

If the VMware Cloud Director Object Storage Extension service runs as expected, the system returns a `Running` status and configuration details.

If you receive an error message, you can start the VMware Cloud Director Object Storage Extension service in debugging mode by adding the `--debug` argument and troubleshoot the problem.

7 Start VMware Cloud Director Object Storage Extension services.

```
ose service start
```

8 (Optional) Get configuration details.

```
ose amazon show
```

The system returns the AWS configuration details.

Configure VMware Cloud Director Object Storage Extension with ECS

Configuring VMware Cloud Director Object Storage Extension with an ECS cluster consists of establishing a connection between VMware Cloud Director Object Storage Extension and ECS services.

For security purposes, VMware Cloud Director Object Storage Extension validates the complexity of all passwords. When you set passwords by using the `ose` command-line utility, make sure that the password contains:

- At least eight characters
- Minimum one uppercase character
- Minimum one lowercase character
- Minimum one numeric digit character
- Minimum one non-alphanumeric character.

Use only visible ASCII characters. Do not use space and non-printing control characters, such as BEL or NUL.

VMware Cloud Director Object Storage Extension performs a password validation as part of the execution of the following scripts:

- `ose ecs admin set`
- `ose ecs console set`

For testing purposes, you can avoid the password validation by adding the `--force` argument to the command that you run.

Prerequisites

Verify that your ECS configuration meets the deployment requirements of VMware Cloud Director Object Storage Extension. See [ECS Deployment Requirements](#).

Procedure

- 1 Open an SSH connection to the machine on which you installed VMware Cloud Director Object Storage Extension.
- 2 Start the VMware Cloud Director Object Storage Extension Keeper service.

```
systemctl start voss-keeper
```

- 3 Configure the connection to the ECS Admin Service HTTPS API endpoint.

```
ose ecs admin set --url ecs-admin-service-url --user admin-user --secret 'password'
```

If the password that you enter contains a single quote character ('), run the command without the `--secret` argument and the system prompts you to enter the password on a new line.

For example:

```
ose ecs admin set --url https://object-storage.acme.com:19443 --user sysadmin --secret 'ChangeIt!'
```

- 4 Configure the connection to the ECS Management Console.

```
ose ecs console set --url ecs-console-url --user admin-user --secret admin-user-pass
```

For example:

```
ose ecs console set --url https://object-storage.acme.com:8443 --user admin --secret 'ChangeIt!'
```

- 5 Configure the connection to the ECS S3 Service.

```
ose ecs s3 set ecs-s3-url
```

To configure the connection, use the FQDN or the IP address of the S3 Service. If you use the FQDN, make sure that you correctly configure the S3 Service domain in the ECS cluster. Also, make sure that your DNS server can route all bucket requests from the virtual to the actual S3 Service host. For example, from *bucket-name.ecs-s3-host* to *ecs-s3-host*. If you use the IP address of the S3 Service, no domain and virtual host route settings are required.

For example:

```
ose ecs s3 set https://object-storage.acme.com:443
```

6 Allow the use of the ECS platform.

ose platforms enable ecs

7 Validate the configuration.

```
ose config validate
```

If all components are successfully configured, the system returns the following message:

Name	Required	Connectivity	Detail
Database	Y	Normal	
Certificate	Y	Normal	
Cloud Director	Y	Normal	
Platform - ECS	Y	Normal	
ECS Admin Service	Y	Normal	
ECS Console Service	N	Normal	

```
| ECS S3 Service | Y | Normal |
|
+-----+-----+-----+
+
```

If the system returns an error, review the log file at `/opt/vmware/voss/log`.

8 Verify the status of the VMware Cloud Director Object Storage Extension service.

```
ose service show
```

If the VMware Cloud Director Object Storage Extension service runs as expected, the system returns a `Running` status and configuration details.

If you receive an error message, you can start the VMware Cloud Director Object Storage Extension service in debugging mode by adding the `--debug` argument and troubleshoot the problem.

9 Start VMware Cloud Director Object Storage Extension services.

```
ose service start
```

10 (Optional) Get configuration details.

```
ose ecs show
```

The system returns the ECS configuration details.

Configure VMware Cloud Director Object Storage Extension with Cloudian HyperStore

Configuring VMware Cloud Director Object Storage Extension with a Cloudian HyperStore cluster consists of establishing a connection between the VMware Cloud Director Object Storage Extension and Cloudian HyperStore services.

For security purposes, VMware Cloud Director Object Storage Extension validates the complexity of all passwords. When you set passwords using the `ose` command-line utility, make sure that the password complies with the following requirements:

- At least eight characters in length
- Minimum one uppercase character
- Minimum one lowercase character
- Minimum one numeric digit character
- Minimum one non-alphanumeric character. Use only visible American Standard Code for Information Interchange (ASCII) characters. Do not use space and non-printing control characters, such as BEL or NUL.

VMware Cloud Director Object Storage Extension performs a password validation as part of the execution of the following scripts:

- `ose cloudian admin set`
- `ose cloudian console set`

For testing purposes, you can avoid the password validation by adding the `--force` argument to the command that you run.

Prerequisites

- Verify that you deployed VMware Cloud Director Object Storage Extension and configured connections to VMware Cloud Director and to your database.
- Verify that you upgraded your Cloudian HyperStore to version 7.1.6 or 7.2.
- Verify that you increased the maximum length of Cloudian HyperStore user IDs from 64 bytes to 255 bytes. See [Before you begin](#) and [Cloudian Deployment Requirements](#).

Procedure

- 1 Open an SSH connection to the machine on which you installed VMware Cloud Director Object Storage Extension.
- 2 Start the VMware Cloud Director Object Storage Extension Keeper service.

```
systemctl start voss-keeper
```

- 3 Configure the connection to the Cloudian HyperStore Admin Service HTTPS API endpoint.

```
ose cloudian admin set --url hyperstore-admin-url --user admin-user --secret 'password'
```

If the password you enter contains a single quote character ('), run the command without the `--secret` argument and the system prompts you to enter the password in a new line.

For example:

```
ose cloudian admin set --url https://object-storage.acme.com:19443 --user sysadmin --secret 'ChangeIt!'
```

- 4 Configure the connection to the Cloudian HyperStore S3 Service.

```
ose cloudian s3 set your-hyperstore-s3-url
```

To configure the connection, use the FQDN or the IP address of the S3 Service. If you use the FQDN, make sure that the S3 Service URL matches the Service domain setting in Cloudian HyperStore. According to Cloudian HyperStore requirements, the format you must use is `https://s3-<your-region>.<your-hyperstore-host>`. Also, make sure that your DNS server can route all bucket requests from the virtual to the actual S3 Service host. For example, from `<any-bucket-name>.<your-hyperstore-host>` to `<your-hyperstore-host>`. If you use the IP address of the S3 Service, no domain and virtual host route settings are required.

For example:

```
ose cloudian s3 set https://s3-regionA.hyperstore.local
```

5 Configure the connection to the Cloudian HyperStore IAM Service.

```
ose cloudian iam set hyper-store-iam-url
```

For example:

```
ose cloudian iam set http://object-storage.acme.com:16443
```

6 Configure the connection to the Cloudian Management Console.

```
ose cloudian console set --url hyperstore-cmc-url --user admin-user --secret cmc-sso-shared-key
```

The user name that you enter must be the user name of a valid system administrator user. For the `--secret` argument value, enter the single sign-on shared key that is configured in the Cloudian Management Console.

For example:

```
ose cloudian console set --url https://object-storage.acme.com:8443 --user admin --secret UinqeMQA9FAWy8zbDqWTLBRRg23U72xBWi
```

7 Allow the use of the Cloudian HyperStore platform.

```
ose platforms enable cloudian
```

8 Validate the configuration of VMware Cloud Director Object Storage Extension .

```
ose config validate
```

If all components are successfully configured, the system returns the following message:

```
+-----+-----+-----+-----+
+
+      Name      | Required | Connectivity |      Detail
+-----+-----+-----+-----+
+
+      Database  |        Y |        Normal |
+-----+-----+-----+-----+
+
+      Certificate |        Y |        Normal |
+-----+-----+-----+-----+
+
+      Cloud Director |        Y |        Normal |
+-----+-----+-----+-----+
```

```

+
| Platform - Cloudian | Y | Normal |
|
+-----+-----+-----+
+
| Cloudian Admin Service | Y | Normal |
|
+-----+-----+-----+
+
| Cloudian S3 Service | Y | Normal |
|
+-----+-----+-----+
+

```

If the system returns an error, review the log file at `/opt/vmware/voss/log`.

9 Verify the status of the VMware Cloud Director Object Storage Extension service.

```
ose service show
```

If the VMware Cloud Director Object Storage Extension service runs as expected, the system returns a `Running` status and configuration details.

If you receive an error message, you can start the VMware Cloud Director Object Storage Extension service in debugging mode by adding the `--debug` argument and troubleshoot the problem.

10 Start VMware Cloud Director Object Storage Extension services.

```
ose service start
```

11 (Optional) Get configuration details.

```
ose cloudian show
```

The system returns the Cloudian HyperStore configuration details.

Configure VMware Cloud Director Object Storage Extension with OSIS compliant object storage

Integrate any S3-compliant object storage platform by configuring Object Storage Interoperability Service (OSIS).

Prerequisites

- Before you can configure VMware Cloud Director Object Storage Extension to work with a third-party object storage platform, verify that you have developed an OSIS adapter for the platform. See the [VMware Object Storage Interoperability Service - Development Guide](#).
- Verify that you have obtained the OSIS adapter name. See [Get the OSIS adapter name](#).

Get the OSIS adapter name

Before you can integrate OSIS, you must obtain the OSIS adapter name.

Procedure

- 1 Start the OSIS adapter and verify that it is running.
- 2 Get the platform information by using a tool like cURL or Postman. See the [Object Storage Interoperability Service API Reference Guide](#).

For example, `curl -k https://osis-adapter-api-server/api/info`

In the response, the property `platform_name` displays the adapter name. The property `auth_modes` displays the supported authentication modes.

How to configure VMware Cloud Director Object Storage Extension with OSIS compliant object storage

OSIS defines a set of management API specifications for VMware Cloud Director Object Storage Extension.

OSIS allows VMware Cloud Director Object Storage Extension to communicate with third-party object storage platforms and exchange tenant and user information.

Procedure

- 1 Configure the OSIS API connection.

```
ose osis admin set --name OSIS-adapter-name --url https://osis-adapter-api-server --user
username --secret
password
```

- 2 (Optional) If the authentication mode for OSIS is with a bearer API token, set a refresh token.

```
ose args set --k oss.platform.OSIS-adapter-name.admin.refresh-token --v refresh-token
```

- a To determine the authentication mode of OSIS, run the OSIS API GET `/api/info` and view the `auth_modes` property.

- 3 Configure the third-party object storage platform S3 endpoint.

```
ose osis s3 set --name OSIS-adapter-name --url https://platform-S3-endpoint
```

- 4 Switch to the third-party object storage platform.

```
ose platforms enable osis --name OSIS-adapter-name
```

- 5 Restart the VMware Cloud Director Object Storage Extension service.

```
ose service restart
```

Results

You can now allow tenant organizations to use the new third-party object storage platform.

Configure Additional VMware Cloud Director Object Storage Extension Instances Behind a Load Balancer

For scaling purposes, you can deploy additional instances of VMware Cloud Director Object Storage Extension behind the load balancer in your environment.

Prerequisites

Verify that you deployed additional node or nodes of VMware Cloud Director Object Storage Extension. See [Install VMware Cloud Director Object Storage Extension](#).

Procedure

- 1 Open SSH connections to the first instance of VMware Cloud Director Object Storage Extension that you deployed and to the additional nodes that you are configuring with the same load balancer.
- 2 Export the configuration from the initially deployed VMware Cloud Director Object Storage Extension.

```
ose config export --file="configuration-file-name" --secret="vcd-sys-admin-pass"
```

The script exports the configuration to an encrypted text file in the `root` directory.

For the `--file` argument value, enter the export filename. For the `--secret` argument value, enter the password of a VMware Cloud Director system administrator.

- 3 Copy the configuration file to the additional VMware Cloud Director Object Storage Extension instances that you configure.
- 4 Import the configuration to the additional instances of VMware Cloud Director Object Storage Extension.

```
ose config import --file="path-to-the-configuration-file" --secret="vcd-sys-admin-pass"
```

Here, the `--file` argument value, is the source directory for the import. The `--secret` argument value is the password of a VMware Cloud Director system administrator.

- 5 Restart the VMware Cloud Director Object Storage Extension Keeper service on the additional nodes of VMware Cloud Director Object Storage Extension.

```
systemctl restart voss-keeper
```

Uninstall VMware Cloud Director Object Storage Extension

4

To upgrade or clean up your testing or development environment, you can uninstall VMware Cloud Director Object Storage Extension. When you uninstall VMware Cloud Director Object Storage Extension, you remove the software binaries. The configuration and log files remain in the file system of the host machine.

Procedure

- 1 Open an SSH connection to the VMware Cloud Director Object Storage Extension machine.
- 2 Stop the VMware Cloud Director Object Storage Extension Keeper service.

```
systemctl stop voss-keeper
```

- 3 Uninstall VMware Cloud Director Object Storage Extension.

- ◆ If you are uninstalling VMware Cloud Director Object Storage Extension 2.2, run one of the following commands, depending on your Linux distribution:

For this Linux distribution...	Use this command...
CentOS, RHEL, Photon OS, Oracle Linux	<pre>rpm -e vmware-ose</pre>
Ubuntu, Debian	<pre>sudo apt-get remove vmware-ose</pre>

- ◆ If you are uninstalling VMware Cloud Director Object Storage Extension 1.5, 2.0, 2.1 or 2.1.1, run the following command:

```
rpm -e vmware-ose
```

- ◆ If you are uninstalling VMware Cloud Director Object Storage Extension 1.0.X, run the following command:

```
rpm -e vmware-voss
```

The script stops VMware Cloud Director Object Storage Extension services and removes the software binaries from the host machine.

- 4 (Optional) After you uninstall VMware Cloud Director Object Storage Extension binaries, the configuration files remain in `/opt/vmware/voss` and the log files remain in `/opt/vmware/vip`. You can delete the directories by running the following command:

```
sudo rm -rf /opt/vmware/voss /opt/vmware/vip root-user-password
```

Upgrading VMware Cloud Director Object Storage Extension

5

You can upgrade to VMware Cloud Director Object Storage Extension 2.2 directly from versions 2.X.

VMware Cloud Director Object Storage Extension is distributed as an RPM installation file with a name in the format `vmware-ose-v.v.v-nnnnnnnn.el7.x86_64.rpm`, where *v.v.v* is the product version and *nnnnnnnn* is the build number. For example, `vmware-ose--1.0.0-24012158.el7.x86_64.rpm`.

If you are upgrading from version 1.X, first upgrade your environment to version 2.X, and then upgrade to VMware Cloud Director Object Storage Extension 2.2.

If you are upgrading a multisite environment, to avoid service downtime, upgrade VMware Cloud Director Object Storage Extension instances one by one.

Upgrading from VMware Cloud Director Object Storage Extension 2.X

To upgrade from version 2.X, run the following commands:

For CentOS, RHEL, Photon OS, and Oracle Linux:

```
rpm -e vmware-ose
rpm -ivh vmware-ose-v.v.v-nnnnnnnn.el7.x86_64
ose endpoint set --url=YOUR_OSE_FQDN --region=YOUR_S3_REGION_NAME
ose ui install
ose service restart
```

For Ubuntu and Debian:

```
sudo apt-get remove vmware-ose
sudo apt-get install /temp/vmware-ose_v.v.v-nnnnnnnn.deb
ose endpoint set --url=YOUR_OSE_FQDN --region=YOUR_S3_REGION_NAME
ose ui install
ose service restart
```


Upgrading from VMware Cloud Director Object Storage Extension 1.X

To upgrade from version 1.X, do the following:

- 1 Uninstall the earlier version of the software from the host machine. See [Chapter 4 Uninstall VMware Cloud Director Object Storage Extension](#).
- 2 Prepare your database before upgrading to version 2.2. See [Prepare the Database for Upgrade](#).
- 3 Install the new RPM package. See [Install VMware Cloud Director Object Storage Extension](#).
- 4 Run a data migration script. See [Migrate VMware Cloud Director Object Storage Extension Data](#).

Read the following topics next:

- [Prepare the Database for Upgrade](#)

Prepare the Database for Upgrade

To prepare your database for upgrading to version 2.2, remove the `conname` constraint from the `bucket_info` table.

Prerequisites

- Verify that the old version of VMware Cloud Director Object Storage Extension is uninstalled.
- Verify that you upgraded your PostgreSQL database to version 9.5 or later.
- Verify that you backed up your database.

Procedure

- 1 Log in to the PostgreSQL database as a database administrator.
- 2 Retrieve the OID of the `conname` constraint for the `bucket_info` table.

```
SELECT conname
FROM pg_constraint
WHERE conrelid =
    (SELECT oid
     FROM pg_class
     WHERE relname like 'bucket_info');
```

The system returns the OID string. For example, `ukb9c15fhp50s53gs8pntjaq5qt`. Copy the OID so that you can use it in the next step.

- 3 Remove the constraints from the `bucket_info` table.

```
ALTER TABLE bucket_info
    DROP CONSTRAINT IF EXISTS {OID};
```

4 (Optional) Delete the tables that are not used in VMware Cloud Director Object Storage Extension 2.2.

```
DROP TABLE IF EXISTS um_storage_can_id;  
  
DROP TABLE IF EXISTS um_storage_user_id;  
  
DROP TABLE IF EXISTS pwc_object_info;
```

Results

Your PostgreSQL database is prepared for the upgrade to VMware Cloud Director Object Storage Extension 2.2.