Using VMware Cloud Director Object Storage Extension as a Tenant User

24 FEB 2022

VMware Cloud Director Object Storage Extension 2.1.1

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

https://docs.vmware.com/

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

Contents

What is VMware Cloud Director Object Storage Extension

1

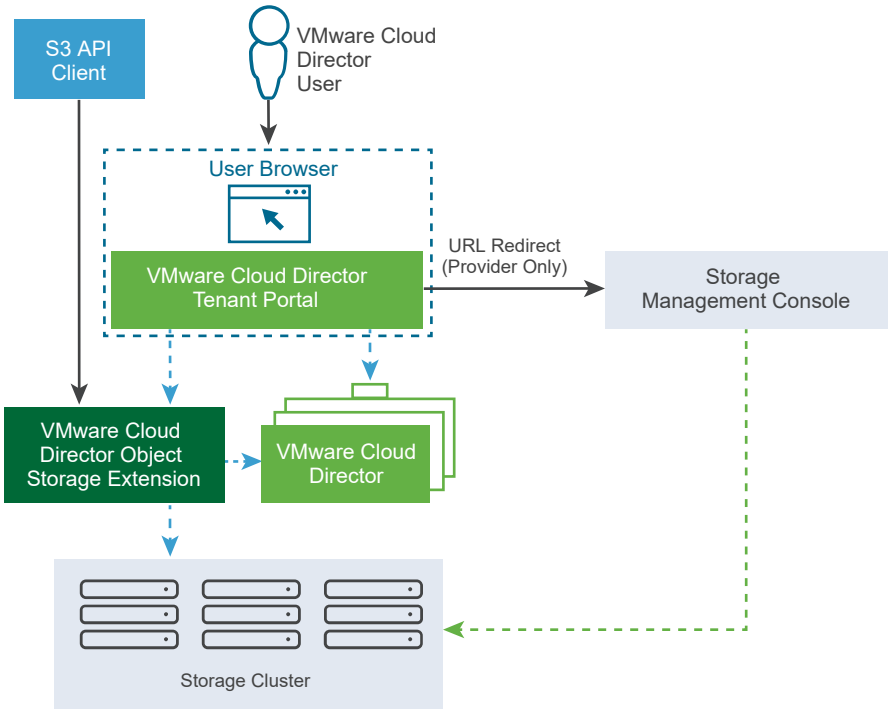
VMware Cloud Director Object Storage Extension is a standalone middleware service that provides object storage capabilities to VMware Cloud Director users. During the installation and configuration, the user interface of VMware Cloud Director Object Storage Extension registers as a plug-in to VMware Cloud Director. As a result, you can access VMware Cloud Director Object Storage Extension from the VMware Cloud Director cloud provider admin portal and the VMware Cloud Director tenant portal.

By integrating with VMware Cloud Director, VMware Cloud Director Object Storage Extension provides you the capability to store and share unstructured data within your VMware Cloud Director organization. You can also use VMware Cloud Director Object Storage Extension for backup and archiving purposes.

You can use VMware Cloud Director Object Storage Extension to store the following data types:

- Media files (images, audio, and video)
- Static Web content (HTML, CSS, JS, and ICO)
- Read-only documents (PDF)
- Backup and archives

The following diagram illustrates a high-level architecture of VMware Cloud Director Object Storage Extension.


S3 API Client
VMware Cloud Director User
User Browser
VMware Cloud Director Tenant Portal
URL Redirect (Provider Only)
Storage Management Console
VMware Cloud Director Object Storage Extension
VMware Cloud Director
Storage Cluster

Getting Started With VMware Cloud Director Object Storage Extension

2

When you log in to VMware Cloud Director Object Storage Extension for the first time, your inventory in VMware Cloud Director Object Storage Extension is empty and the **Getting Started** pages guide you through the first steps for working with buckets, vApps, and catalogs.

Understanding Buckets

Before you start uploading files to VMware Cloud Director Object Storage Extension, you must create a bucket. You can then upload any number of files to the bucket. A bucket is a logical unit of storage. Buckets are the fundamental containers in VMware Cloud Director Object Storage Extension.

You can access and manage buckets from the VMware Cloud Director Object Storage Extension user interface. See Chapter 3 Working with Buckets. Alternatively, you can use the S3 API that VMware Cloud Director Object Storage Extension supports. See Chapter 9 Working with VMware Cloud Director Object Storage Extension S3 API.

To organize and categorize your buckets, you can add multiple key-value pairs of tags to your buckets. For example, you can create a bucket to store financial reports from the financial department in your organization. You can tag this bucket with the following key-value pairs:

Key	Value
Department	*Finance*
Report	*Monthly*

Bucket names are globally unique and the namespace is shared between all VMware Cloud Director organizations. After you create a bucket, the name of that bucket cannot be used for another bucket in any of the VMware Cloud Director organizations until the bucket is deleted. Bucket names must adhere to the S3 bucket naming requirements. See Amazon S3 Bucket Naming Requirements.

Understanding Objects

Objects in VMware Cloud Director Object Storage Extension are the files that you upload to your buckets.

You can categorize objects within a bucket by adding key-value pairs of tags. If you are the owner of an object and have **Read** and **Write** permissions on the bucket that stores the object, you can add properties to the objects. You add the properties to the object by defining metadata in the form of a key-value pair.

Organization administrators can access and manage the objects that all users within their organization own. Organization users can access and manage the objects that they own and the objects that are shared with them.

You can preview image, text, PDF, audio, and video files directly in the user interface of VMware Cloud Director Object Storage Extension.

Understanding How to Work with vApps in VMware Cloud Director Object Storage Extension

A vApp is a package/container of multiple interoperating virtual machines that communicate over a network and use resources and services in your environment. The virtual machines in the vApp are managed as a unit and distributed in OVA and OVF format. With VMware Cloud Director Object Storage Extension, you can store the vApps that you do not use in your VMware Cloud Director environment. When you capture a vApp from VMware Cloud Director and move it to VMware Cloud Director Object Storage Extension, you copy the vApp data from the VMware Cloud Director datastore to the back-end storage appliance that VMware Cloud Director Object Storage Extension uses. By capturing a vApp from VMware Cloud Director, you do not copy the storage reservation to VMware Cloud Director Object Storage Extension.

Later, if you need any of the vApps that you captured and store in VMware Cloud Director Object Storage Extension, you can restore the vApps back to their original location. You can also download vApps as OVA files for backup and archiving purposes.

Understanding Catalogs in VMware Cloud Director Object Storage Extension

Catalogs in VMware Cloud Director Object Storage Extension are similar to the catalogs in VMware Cloud Director and act as containers for vApp and virtual machine templates.

You can upload ISO, OVA, OVF, and VMDK files to the VMware Cloud Director Object Storage Extension catalogs.

Catalogs in VMware Cloud Director Object Storage Extension can be used as external catalogs for VMware Cloud Director. An **organization administrator** can subscribe a VMware Cloud Director organization to a catalog in VMware Cloud Director Object Storage Extension. The subscription makes all files that are stored in VMware Cloud Director Object Storage Extension available to the VMware Cloud Director organization users without consuming any of the compute resources in the VMware Cloud Director environment. For information about subscribing your VMware Cloud Director organization to an external catalog, see Subscribe to an External Catalog in the *VMware Cloud Director Tenant Portal Guide*.

When you create a catalog in VMware Cloud Director Object Storage Extension, a bucket is also created and is reserved as a system bucket. You cannot manage that bucket the way you manage buckets created by users.

Understanding Security Credentials

VMware Cloud Director Object Storage Extension supports S3-compatible API and the AWS Signature V4 authentication. Security credentials are used for authenticating S3 API requests and consist of an access key and a secret key. VMware Cloud Director Object Storage Extension supports user and application types of security credentials.

With S3 API requests authenticated with user credentials, you can access and manage buckets and objects that you own or that are shared with you.

With S3 API requests authenticated with application credentials, you can access and manage objects at the bucket level.

This chapter includes the following topics:

Access the VMware Cloud Director Object Storage Extension Tenant Portal

You access the VMware Cloud Director Object Storage Extension tenant portal by using the VMware Cloud Director tenant portal.

Prerequisites

To access the VMware Cloud Director Object Storage Extension tenant portal, your VMware Cloud Director **system administrator** must activate VMware Cloud Director Object Storage Extension for your organization.

Procedure

1. In a Web browser, navigate to the VMware Cloud Director tenant portal URL of your organization.

   For example, `https://vcloud.example.com/tenant/myOrg`.

2. Enter your user name and password, and click **Log In**.
3. From the **More** drop-down menu, select **Object Storage**.

Results

The VMware Cloud Director Object Storage Extension tenant portal opens.

Roles and Rights in VMware Cloud Director Object Storage Extension

Any active VMware Cloud Director **organization user** can access VMware Cloud Director Object Storage Extension.

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

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

Table 2-1. 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	■ **General: Administrator View** ■ **Provider VDC: View** ■ **Organization VDC: View** ■ **UI Plugins: View**	None.
Tenant Administrator	■ **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**.

Starting with VMware Cloud Director Object Storage Extension 2.1, you can control the access to features for users in your organization by using subordinate roles. Subordinate roles determine if the tenant user can work with vApp, Catalog, and Kubernetes features in VMware Cloud Director Object Storage Extension. Organization administrators can assign subordinate roles to organization users. An **organization administrator** inherits all subordinate roles by default. An **organization user** does not have access to the vApp, Catalog, and Kubernetes features by default.

This subrole...	Allows you to...
vApp Contributor	Capture and restore vApps.
Catalog Contributor	Create, publish, and import catalogs.
Kubernetes Contributor	Backup and restore guest Kubernetes clusters.

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

Assign Subordinate Roles

To ensure users in your tenant organization can view vApp, Catalog, and Kubernetes features, you assign subordinate roles to the users.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. Click **Users**.
4. Next to the user account that you want to edit, click the ellipsis-vertical icon (⋮) and click **Edit Subordinate Roles**.
5. Select the subordinate roles that you want to add.

Click this role...	To...
vApp Contributor	Capture and restore vApps.
Catalog Contributor	Create, publish, and import catalogs.
Kubernetes Contributor	Backup and restore guest Kubernetes clusters.

6. Click **Save**.

Apply Server-Side Encryption

By default, VMware Cloud Director Object Storage Extension does not enforce any server-side encryption to the objects that users store in the underlying datastore. Optionally, an **organization administrator** can define a server-side encryption method to protect your data while it is stored in the data center of your **cloud provider**.

Your files are encrypted as VMware Cloud Director Object Storage Extension writes the data to disks in the data center and decrypts the data when you access it.

Changing the encryption method for your organization does not impact objects that exist in VMware Cloud Director Object Storage Extension.

Procedure

1 Log in to the VMware Cloud Director tenant portal.

2 From the **More** drop-down menu, select **Object Storage**.

3 Navigate to **Settings > Server-side Encryption** and click **Edit**.

4 Select the encryption type for your organization.

Encryption Type	Description
None	By default, VMware Cloud Director Object Storage Extension does not enforce a server-side encryption.
SSE-S3	A server-side encryption method that uses an AES-256 algorithm. An S3 server manages the primary keys.
SSE-C	Use this option, if the **organization administrator** wants to manage their own encryption algorithms and primary keys. If you select this encryption type, you must select the encryption algorithm and specify or generate an encryption key.

5 Select the **I understand the consequences** check box and click **Save**.

Working with Buckets

3

Buckets in VMware Cloud Director Object Storage Extension represent containers to which you upload files.

To store your data in VMware Cloud Director Object Storage Extension, you work with buckets and objects. Buckets are containers for objects. Objects are documents and files that you store in the buckets.

You create a bucket and then upload the objects to that bucket. When you no longer need a bucket, you can delete it.

Depending on your role, you can perform different operations with buckets.

As an ...	You can ...
organization user	create, edit, share, empty, and delete your own buckets.
organization administrator	create, edit, share, empty, and delete all buckets within your organization.

For each bucket, you can activate versioning. Versioning is a means of keeping multiple versions of an object in the same bucket. You use versioning to preserve, retrieve, and restore every version of every object stored in your buckets. With versioning, you can easily recover from both unintended user actions and application failures. You activate and deactivate versioning at the bucket level. You can activate or deactivate versioning during the creation of a bucket, or you can edit the versioning configuration later. By default, versioning is inactive. When you create a bucket, you can optionally activate the object lock feature. If the feature is active, versioning for the bucket is also active. If the object lock feature is active for a bucket, you cannot deactivate versioning for the bucket.

To protect an object version from accidental or malicious deletion, activate the object lock feature and set a retention policy when you create a bucket. If you do not activate the object lock feature during the creation of a bucket, you cannot activate the feature for this bucket later. There are three retention modes you can select from:

Retention Mode	Description
Governance Mode	A user with specific permissions can preview the retention policy.
Compliance Mode	The retention policy is not displayed to any user.
No Retention	Does not require the selection of a retention period. If you select this option, you can define the retention period later.

To categorize your buckets, you use the object tagging feature and assign tags to individual objects. A tag represents a key-value pair.

You can set a default bucket encryption so that all objects are encrypted when they are stored in the bucket. By default, VMware Cloud Director Object Storage Extension does not enforce any bucket-level encryption. You can define an encryption method at the bucket level. If both server-side encryption and bucket encryption are configured, the bucket encryption configuration takes precedence. If you enforce an object-level encryption through the VMware Cloud Director Object Storage ExtensionVMware Cloud Director Object Storage Extension API, the object-level encryption takes precedence over the bucket encryption configuration.

Encryption Method	Description
SSE-S3	A server-side encryption method that uses an AES-256 algorithm. An S3 server manages the primary keys.
None	By default, VMware Cloud Director Object Storage Extension does not enforce bucket-level encryption.

This chapter includes the following topics:

Create a Bucket

Before you can upload objects to VMware Cloud Director Object Storage Extension, you must create a bucket.

Prerequisites

- If you are using Cloudian HyperStore and want to use the object lock feature, verify that you upgraded Cloudian HyperStore to version 7.2.2.1 or later.
- Verify that the bucket name that you want to use adheres to the Amazon S3 Bucket Naming Requirements. Bucket names are globally unique across all VMware Cloud Director organizations.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. Click **Buckets > New Bucket**.
4. Enter a name of the bucket.
5. (Optional) To keep multiple versions of the objects that the bucket stores, turn on the **Activate Versioning** toggle.
6. (Optional) To prevent objects in the bucket from being deleted, turn on the **Object Lock** toggle.

   Note You can only activate the object lock feature during the creation of a bucket. If you activate the feature for a bucket, you cannot deactivate it later or suspend versioning for that bucket.

   a. Select the retention mode.

Option	Description
Governance Mode	A user with specific permissions can preview the retention policy.
Compliance Mode	The retention policy is not displayed to any user.
No Retention	Does not require the selection of a retention period. If you select this option, you can define the retention period later.

   b. Select the retention period.
7. Click **Save**.

Results

The new bucket appears in the **Buckets** pane and you can upload objects to it.

Bucket Logs

With bucket logs, you can record all activities at the bucket level.

When you configure bucket logging, you define a target bucket that stores the log files. Later, whenever you add, modify, or delete an object, VMware Cloud Director Object Storage Extension records the action in a log file.

To write bucket logs, VMware Cloud Director Object Storage Extension uses a dedicated log delivery account named System Logger. The log delivery account is a subject to the usual access control restrictions. When you configure bucket logging, VMware Cloud Director Object Storage Extension grants **Write of Bucket** and **Read of ACL** permissions on the target bucket to the System Logger account.

You can interact with log files the same way you interact with other objects in VMware Cloud Director Object Storage Extension. You can preview log files directly in VMware Cloud Director Object Storage Extension, or you can download the logs locally.

If VMware Cloud Director Object Storage Extension uses the ECS storage platform, bucket logging is impossible. The ECS storage platform does not support bucket logging.

If you use Cloudian HyperStore, you can work with bucket logs.

Activate Bucket Logging

To activate logging for a bucket, select a target bucket that stores the log files and optionally share the log files with other users.

Prerequisites

To activate bucket logging, verify that you have the required set of rights.

If you are an ...	You can ...
organization administrator	manage the logging configuration of buckets that users in your organization own.
organization user	manage the logging configuration of your own buckets.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. In the **Buckets** pane, click the name of the bucket that you want to edit.
4. Click **Properties**.
5. In the **Logging** card, click the text.
6. Enter the logging configuration details and click **Save**.
   a. Select the target bucket in which you want to store the log files.

      VMware Cloud Director Object Storage Extension grants **Write of Bucket** and **Read of ACL** permissions on the target bucket to the log delivery account named System Logger.

   b. (Optional) Enter a prefix for the log files.

c (Optional) To save the log files to a folder in the target bucket, select the **Prefix as a folder** check box.

d (Optional) Share the log files with other users.

- To share the log files with users within your tenant organization, use the toggle buttons in the **Tenant Users** row.
- To share the log files with authenticated users within all tenant organizations, use the toggle buttons in the **Authenticated Users** row.
- To share the log files with all users, use the toggle buttons in the **Public** row.
- To share the log files with specific users within your organization, click the **Add User** button, select the users with whom you want to share the log files, and use the toggle buttons in the corresponding row.

Results

Whenever an object is added or modified in the logging source bucket, VMware Cloud Director Object Storage Extension creates and adds a bucket log object to the logging target bucket. The owner of the log is the System Logger account.

Cross-Origin Resource Sharing Rules

Cross-origin resource sharing (CORS) is a mechanism for client web applications loaded in one domain to interact with resources in a different domain. With CORS, you can selectively allow cross-origin access to your VMware Cloud Director Object Storage Extension resources.

Using the VMware Cloud Director Object Storage Extension tenant portal, you can define multiple CORS rules at the bucket level.

CORS rules at the bucket level only take effect on virtual hosted-style S3 API requests. If you access resources using path-style S3 API requests, the global CORS rules take effect.

Create a Cross-Origin Resource Sharing Rule

Within a cross-origin resource sharing (CORS) rule, you define the allowed request origins, methods, headers, the maximum age of the request, and the exposed headers.

Prerequisites

To create CORS rules for a bucket, verify that you have the required set of rights.

If you are an ...	You can ...
organization administrator	can create CORS rules for the buckets that users in your organization own.
organization user	can create CORS rules for the buckets that you own.

Procedure

1 Log in to the VMware Cloud Director tenant portal.

2 From the **More** drop-down menu, select **Object Storage**.

3 In the **Buckets** pane, click the name of the bucket that you want to edit.

4 Click **Properties**.

5 In the **Cross-Origin Resource Sharing** section, click the text.

6 Enter the details of the rule.

   a Enter an ID for the rule or select the **Auto Generate** check box.

   b Enter the allowed request origins or select the **All Origins** check box.

   c Select the allowed request methods.

   d (Optional) Enter the allowed request headers.

   e (Optional) Enter the exposed headers.

   f (Optional) Enter the maximum age allowed for requests.

7 Save the current rule or add another rule.

   - To save the rule, click **Save**.
   - To add another rule, click **Add Rule** and complete step Step 6.

Sharing Buckets

You can share one bucket at a time.

To share a bucket, you can use access control lists or bucket policies.

Access control lists allow you to implement fine grained control over your buckets and the objects using the buckets. To share a bucket with an access control list, you edit the access permissions to the bucket by using the built-in canned access control lists, or by creating a custom access control list.

Bucket policies allow you to implement global control over your buckets. They can only be assigned to buckets but not to the objects in the bucket.

Access Control Lists

Use access control lists to manage access to buckets.

You can use access control lists to grant access to buckets. Access control lists define who has access to your buckets and what level of access they have. There are two types of access control lists:

- Canned access control lists are predefined.
- Custom access control lists can be modified to your needs.

Before you share a bucket using an access control list, you must verify that you have the required set of rights.

If you are an ...	You can ...
organization administrator	share buckets that users in your organization own.
organization user	share buckets that you own.

- Alternatively, the owner must assign one of the following sets of permissions for the bucket to your user account.
  - **Read of Bucket**, **Write of Bucket**, **Read of ACL**, and **Write of ACL**
  - **Read of Bucket**, **Read of ACL**, and **Write of ACL**
  - **Full Control**

Share a Bucket Using a Canned Access Control List

Canned access control lists are predefined, built-in access control lists that you can use to share buckets within your organization or publicly over the Internet.

Note Setting a canned access control list to a bucket overwrites existing permissions configuration for the bucket.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. In the **Buckets** pane, click the name of the bucket that you want to share.
4. On the **Permissions** tab, click **Set Canned ACL**.
5. Select a canned access control list name for the bucket and click **Set ACL**.

Option	Description
Private	Only the bucket owner and the **organization administrator** can access the bucket.
Public Read	Grants **Read** permissions on the bucket to all users.
Public Read/Write	Grants **Read** and **Write** permissions on the bucket to all users.
Authenticated Users Read	Grants **Read** permissions to all authenticated VMware Cloud Director users.
Tenant Read	Grants **Read** permissions on the bucket to all users within the VMware Cloud Director organization. If you use the ECS storage platform, this option is not available. If you use AWS S3, this option is not available.

Option	Description
Tenant Read/Write	Grants **Read** and **Write** permissions on the bucket to all users within the VMware Cloud Director organization. If you use ECS or AWS S3, this option is not available.
System Logger	To write bucket logs, VMware Cloud Director Object Storage Extension uses the System Logger account. Modifying the permissions of the System Logger account for a logging target bucket might result in failure to write bucket logs. For more information, see Bucket Logs. If you use the ECS storage platform, this option is not available.

Share a Bucket Using a Custom Access Control List

You can share buckets with users in your organization by creating a custom access control list.

The following table describes the available access control list options.

Option	Description
Full Control	Grants **Read** and **Write** permissions on the bucket, and **Read** and **Write** permissions for the access control list of the bucket.
Read of Bucket	Grants **Read** permissions on the bucket.
Write of Bucket	Grants **Write** permissions on the bucket.
Read of ACL	Grants **Read** permissions on the access control list of the bucket.
Write of ACL	Grants **Write** permissions on the access control list of the bucket.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. In the **Buckets** pane, click the name of the bucket that you want to share.
4. On the **Permissions** tab, click **Edit**.
5. Configure the required set of permissions for the bucket and click **Save**.
   - To share the bucket with users from your tenant organization, use the toggle buttons in the **Tenant Users** row.

     If you use the ECS storage platform, this option is not available.
   - To share the bucket with authenticated users from all tenant organizations, use the toggle buttons in the **Authenticated Users** row.
   - To share the bucket with all users, use the toggle buttons in the **Public** row.
   - To share the bucket with specific users within your organization, click the **Add User** button, select the user, and use the toggle buttons in the corresponding row.

- To write bucket logs, VMware Cloud Director Object Storage Extension uses the System Logger account. Modifying the permissions of the System Logger account for a logging target bucket might result in failure to write bucket logs. For more information, see Bucket Logs.

  If you use the ECS storage platform, this option is not available.

Bucket Policies

With bucket policies, you allow or deny an action to a resource in a bucket. You can also define conditions within a policy.

To grant access permissions to your bucket and the objects in it, you use bucket policies. Bucket policies are an important element in securing your buckets against unauthorized access.

Bucket policies consist of policy statements and are limited to 20 KB in size. You can create a single policy per bucket, but you can add multiple statements to a single policy.

Bucket policies use a JSON-based language. See Policies and Permissions in Amazon S3 .

VMware Cloud Director Object Storage Extension provides a policy editor that you can use instead of the JSON editor.

Only the bucket owner can create and edit bucket policies.

Create a Bucket Policy

To create a bucket policy, you define rules and conditions for accessing the objects in a bucket.

Prerequisites

To create a bucket policy, you must be the owner of the bucket.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. In the **Buckets** pane, click the name of the bucket that you want to edit.
4. On the **Permissions** tab, click text in the bucket policy area.
5. Enter the details of the policy and click **Save**.
   - You can use the policy editor to enter ID, effect, settings, and conditions for the policy.
   - You can use the JSON editor to enter the policy statements.
   - To create a **Public Read** or **Public Read/Write** policy, click the respective shortcut.

Lifecycle Rules

Use lifecycle rules to automize your data management.

Lifecycle rules are a way to reduce storage costs and the amount of time spent on managing your data. You define rules that instruct VMware Cloud Director Object Storage Extension to delete incomplete multipart uploads, set an expiration period for current or previous versions of objects, and clean up expired objects. You can define for the actions to take effect on all objects within a bucket, or to a subset of the objects within the bucket.

You can create, delete, edit, or deactivate lifecycle rules. Before taking any of these actions, verify that you have the required set of rights.

If you are an ...	You can ...
organization administrator	create, delete, and edit rules for the buckets of the users in your organization
organization user	create, delete, and edit rules for your own buckets

Create a Lifecycle Rule

Create a lifecycle rule to define automated actions to manage your data.

Prerequisites

Verify that you have the required set of rights to create a lifecycle rule for a bucket.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. In the **Buckets** pane, click the name of the bucket for which you want to create a rule.
4. On the **Lifecycle** tab, click **New Rule**.
5. To activate or deactivate the rule, move the **Status** slider.

   You can create an inactive rule and activate it later.
6. Select the scope of the rule.
   a. You can apply the rule to all objects in the bucket, or apply the rule to specific objects within the bucket.
   b. If you select to apply the rule to specific objects, enter a prefix for the objects to which the rule is applied.
   c. (Optional) To create a folder using the prefix you entered, select the **Prefix as a folder** check box.

7 Define the actions of the rule.

To create a lifecycle rule, define at least one action.

a Enter an expiration period for the current version of objects.

If you select this action, you cannot select the option to clean up the delete markers of expired objects.

b Enter an expiration period for previous versions of objects.

c To clean up the delete markers of expired object, select the check box.

If you select this action, you cannot select an expiration period for the current version of objects.

d To clean up incomplete multipart uploads, enter a waiting period and select the check box.

8 Click **Save**.

Synchronize a Bucket

To reflect the recent changes that are made in the back end, you can force the bucket-level synchronization between the VMware Cloud Director tenant portal and the back-end services.

Procedure

1 Log in to the VMware Cloud Director tenant portal.

2 From the **More** drop-down menu, select **Object Storage**.

3 In the **Buckets** pane, click the name of the bucket that you want to synchronize and click **Sync**.

Results

After the synchronization process completes, you can see all changes to the contents of the bucket.

Empty a Bucket

To clean up the inventory of VMware Cloud Director Object Storage Extension and to free storage space, you can empty a bucket. By emptying a bucket, you delete all objects from the bucket at once and preserve the access control configuration of the bucket.

Prerequisites

Verify that you have the required set of rights to empty a bucket.

- If you are an **organization administrator**, you can empty buckets that users in your organization own.
- If you are an **organization user**, you can delete a bucket if you are the owner of the bucket, or the owner must assign to your user account **Bucket Read** and **Bucket Write** permissions on the bucket.

Procedure

1 Log in to the VMware Cloud Director tenant portal.

2 From the **More** drop-down menu, select **Object Storage**.

3 In the **Buckets** pane, select the bucket that you want to empty.

4 Click **Empty**.

5 If versioning is active for the bucket, you can optionally select the **All versions** check box, so that all versions of all objects in the bucket are deleted.

   If you do not select the check box, you delete only the latest versions of the objects in the bucket.

6 To confirm the operation, click **Empty**.

Delete a Bucket

To clean up buckets that you no longer need from VMware Cloud Director Object Storage Extension, you can delete the buckets. You can delete one bucket at a time.

As an **organization user** you cannot delete shared buckets and reserved buckets that contain vApps and catalogs.

Prerequisites

- Verify that you have the required set of rights to delete a bucket.
  - If you are an **organization administrator**, you can delete buckets that users in your organization own.
  - If you are an **organization user**, you can only delete the buckets that you own.
- Verify that the bucket you want to delete does not store any objects.

Procedure

1 Log in to the VMware Cloud Director tenant portal.

2 From the **More** drop-down menu, select **Object Storage**.

3 In the **Buckets** pane, select the bucket that you want to delete.

4 Click **Delete** and confirm the deletion.

Working with Objects

4

Objects are the files that you upload to VMware Cloud Director Object Storage Extension. You manage objects by using the VMware Cloud Director Object Storage Extension tenant portal.

As an **organization user**, you work with the objects that you own. You can also operate with the objects that are shared with you. The operations that you can perform depend on the permissions that are assigned to your user account for a particular object.

As an **organization administrator**, you can manage the objects of all organization users using the privilege of the object owner.

This chapter includes the following topics:

Working with Folders

Starting with VMware Cloud Director Object Storage Extension 1.0.1 you can use folders and subfolders to group and organize objects.

How Do I Use Folders Within VMware Cloud Director Object Storage Extension Buckets

Buckets and objects are the primary resources in VMware Cloud Director Object Storage Extension. VMware Cloud Director Object Storage Extension has a flat structure with no hierarchy like in a file system. However, to achieve organizational simplicity, VMware Cloud Director Object Storage Extension supports the folder concept as a means of grouping objects. VMware Cloud Director Object Storage Extension supports the folder concept by using the full name of a folder as a prefix for the object names within the folder. In the context of folders, object names are called key names.

For example, you can create a folder called *monthly-reports* and store an object named *report-jan.xlsx* in the folder. The object is then stored with the key name *monthly-reports/report-jan.xlsx*, where *monthly-reports/* is the prefix.

You can create folders within folders but you cannot create buckets within buckets. You can directly upload objects to a folder. You can copy an object from a folder to a bucket. By using the VMware Cloud Director Object Storage Extension user interface, you cannot directly copy an object from one folder to another folder. To copy an object to another folder, use the *VMware Cloud Director Object Storage Extension API*. You can create and delete folders, but you cannot rename a folder. You cannot edit access permissions at the folder level.

Limitations for Catalog Buckets

When working with folders within catalog buckets, consider the following limitations:

- You can have only one level of folders. No subfolders are allowed.
- You can only upload OVA and ISO files to the main directory of a catalog bucket.
- You can only upload OVF and VMDK files to a folder in a catalog bucket.
- You can upload only one OVF file to a folder in a catalog bucket.

Create a Folder

To organize the objects in your buckets, you can create folders and group the objects as appropriate.

Once a folder is created, you cannot rename it.

Prerequisites

Verify that you have the required set of rights to create a folder in a bucket.

- If you are an **organization administrator**, you can create folders in the buckets that users in your organization own.
- If you are an **organization user**, to create a folder, you must be the owner of the bucket, or the owner of the bucket must assign **Read** and **Write** permissions for the bucket to your user account.

Procedure

1 Log in to the VMware Cloud Director tenant portal.

2 From the **More** drop-down menu, select **Object Storage**.

3 In the **Buckets** pane, navigate to the bucket in which you want to create a folder.

4 Click **Create Folder** and enter a name for the folder.

5 To create the folder, click **Create**.

Delete a Folder

To clean up the inventory of VMware Cloud Director Object Storage Extension and to free storage space, you can delete a folder. By deleting a folder, you delete all objects in the folder.

Prerequisites

Verify that you have the required set of rights to empty a bucket.

- If you are an **organization administrator**, you can delete folders that users in your organization own.
- If you are an **organization user**, to delete a folder, you must be the owner of the bucket that stores the folder, or the owner must assign to your user account **Bucket Read** and **Bucket Write** permissions on the bucket.

Procedure

1 Log in to the VMware Cloud Director tenant portal.

2 From the **More** drop-down menu, select **Object Storage**.

3 In the **Buckets** pane, click the name of the bucket that stores the folder that you want to delete.

4 If versioning is active for the bucket, hide object versions by using the Show Versions toggle button.

5 Select the folder that you want to delete.

6 From the **Actions** drop-down menu, select **Delete**.

7 If versioning is active for the bucket that stores the folder, you can optionally select the **All versions** check box.

   If you select the **All versions** check box, you delete all versions for all objects in the folder. If you do not select the check box, you delete only the latest versions of all objects in the folder.

8 To confirm the deletion, select the **Confirm deletion** check box and click **Delete**.

Upload Files to VMware Cloud Director Object Storage Extension

Objects in VMware Cloud Director Object Storage Extension are the files that you upload.

Important When uploading files to VMware Cloud Director Object Storage Extension, do not navigate out of the VMware Cloud Director Object Storage Extension tenant portal until the upload process completes. Leaving the VMware Cloud Director Object Storage Extension tenant portal within the same user session interrupts the upload process.

If you are using AWS S3, when you upload objects, you can select the storage class that best fits your needs. The following table describes the available storage classes and corresponding use cases.

Storage Class	Description
Standard	Default storage class. Best fit for general-purpose storage of frequently accessed data.
Reduced Redundancy	Provides the option to store noncritical, reproducible data at lower levels of redundancy than the standard storage.
Glacier	Best fit for short and mid-term archives.
Standard Infrequent Access (IA)	Best fit for long-lived and less frequently accessed data.
One Zone IA	Best fit for long-lived and less frequently accessed data that you store in a single zone.
Intelligent Tiering	Best fit for data with unknown or changing access patterns.
Glacier Deep Archive	Best fit for long-term archiving purposes.

For more information, see Amazon S3 Storage Classes and Amazon S3 Reduced Redundancy Storage.

Prerequisites

Verify that you have the required set of rights to upload files to a bucket.

- As an **organization administrator**, you can upload an object to the buckets that users in your organization own.
- As an **organization user**, you can upload an object if you are the owner of the bucket, or the owner must assign to your user account **Write of Bucket** permissions on the bucket .

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. In the **Buckets** pane, navigate to the bucket or folder to which you want to upload files.
4. Click **Upload**.

5 Select whether to overwrite the objects with the same name.

   By default, VMware Cloud Director Object Storage Extension overwrites files with the same name. If an object with the same name exists in the bucket and versioning is active for the bucket, you can upload a new version of the object.

6 (Optional) If you are using AWS S3, you can select the storage class.

7 Click the folder icon ( ), navigate to the files that you want to upload, and click **Upload**.

Add Tags and Metadata to an Object

To improve the categorization of objects in VMware Cloud Director Object Storage Extension, bucket owners can optionally add tags to individual objects. As a bucket owner, you can also add properties to objects by adding user-defined metadata. Both the object tags and the object metadata represent a key-value pair.

If a bucket owner adds tags to an object owned by another user, and the object owner does not have **FULL_CONTROL** privileges for the bucket, the object owner cannot edit the metadata of the object anymore.

If you use the Cloudian HyperStore storage platform, you can add tags to your objects. The ECS storage platform does not support tagging.

Important Adding metadata to an object overwrites the original object and resets permissions and other associations for the object.

You cannot edit the metadata of bucket log objects owned by the System Logger account.

Prerequisites

- Verify that you have the required set of rights to add tags to an object.
  - If you are an **organization administrator**, you can add tags to objects that users in your organization own.
  - If you are an **organization user**, you can add tags to objects, if you are the owner of the bucket that stores the object.
- Verify that you have the required set of rights to edit the metadata of an object.
  - If you are an **organization administrator**, to add metadata to an object, make sure that the object owner has **Write of Bucket** permissions on the bucket that stores the object.
  - If you are an **organization user**, to add metadata to an object, you must be the object owner and your user account must have **Write of Bucket** permissions.

Procedure

1 Log in to the VMware Cloud Director tenant portal.

2 From the **More** drop-down menu, select **Object Storage**.

3 In the **Buckets** pane, navigate to the bucket or folder that stores the object that you want to edit.

4 Click the name of the object that you want to edit.

5 Add a tag to the object

   a Click the link in the **Tags** section.

   b Enter a key-value for the tag.

   c Click **Save**.

6 Add metadata to the object.

   a Click the link in the **Metadata** section.

   b Enter a key-value for the metadata entry.

   c To indicate that you understand the effect of adding metadata to an object, select the check box.

   d Click **Save**.

Sharing Objects

By using the VMware Cloud Director Object Storage Extension tenant portal, you can share objects with specific users, or with all users within your tenant organization. You can also make objects public and share objects over the Internet.

You can share one object at a time. To share an object, you edit the access permissions of the object by using the built-in canned access control lists, or by creating a custom access control list.

If versioning is active for the bucket in which the object that you want to share resides, you can share a specific version of the object.

Share an Object by Using a Canned Access Control List

Canned access control lists are predefined, built-in access control lists that you can use to share objects within your organization or publicly over the Internet.

Note Setting a canned access control list to an object overwrites existing permissions configuration for the object.

Prerequisites

Verify that you have the required set of rights to share objects.

- If you are an **organization administrator**, you can share objects that users in your organization own.

- If you are an **organization user**, you can share objects, if you are the owner of the object, or the owner must assign either **Full Control**, or **Read of ACL** and **Write of ACL** permissions on the object.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. In the **Buckets** pane, navigate to the bucket or folder in which the object that you want to share resides.
4. If you want to share a specific version of the object, display all versions of the object by using the **Show Versions** toggle button.
5. Click the name of the object or the object version that you want to share.
6. On the **Permissions** tab, click **Set Canned ACL**.
7. Select a canned access control list name for the object and click **Set ACL**.

Option	Description
Private	Only the object owner and the **organization administrator** can access the object.
Public Read	Grants **read** permissions on the object to all users and makes the object public.
Public Read/Write	Grants **Read** and **Write** permissions on the object to all users.
Authenticated Users Read	Grants **Read** permissions to all authenticated VMware Cloud Director users.
Bucket Owner Read	Grants **Read** permissions on the object to the bucket owner.
Bucket Owner Full-Control	Grants **Full Control** permissions on the object to the bucket owner.
Tenant Read	Grants **Read** permissions on the object to all users that belong to the tenant organization. If you use AWS S3, this option is not available.

Share an Object by Using a Custom Access Control List

To share an object with specific users within or outside of your organization, you can create a custom access control list for the object that you want to share.

The following table describes the available access control list options.

Option	Description
`Full Control`	Grants **Read** permissions on the object and **Read**, and **Write** permissions on the access control list of the object.
`Read of Object`	Grants **Read** permissions for the object.

Option	Description
`Read of ACL`	Grants **Read** permissions for the access control list of the object.
`Write of ACL`	Grants **Write** permissions for the access control list of the object.

Prerequisites

Verify that you have the required set of rights to share objects.

- If you are an **organization administrator**, you can share objects that users in your organization own.
- If you are an **organization user**, you must be the owner of the object, or the owner must assign to your user account either **Full Control**, or **Read of ACL** and **Write of ACL** permissions on the object.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. In the **Buckets** pane, navigate to the bucket or folder that stores the object that you want to share.
4. If you want to share a specific version of the object, display all versions of the object by using the **Show Versions** toggle button.
5. Click the name of the object or the object version that you want to share.
6. On the **Permissions** tab, click **Edit**.
7. Configure the required set of permissions on the object and click **Save**.
   - To share the object with users from your tenant organization, use the toggle buttons in the **Tenant Users** row. If you use ECS or AWS S3, this option is not available.
   - To share the object with authenticated users from all tenant organizations, use the toggle buttons in the **Authenticated Users** row.
   - To share the object with all users, use the toggle buttons in the **Public** row.
   - To share the object with a specific user within your organization, click the **Add User** button, select the user from the drop-down menu, or enter the organization user name of the user, and use the toggle buttons in the corresponding row.

Copy an Object

You can copy objects from one bucket to another by using the VMware Cloud Director Object Storage Extension tenant portal.

If you are an **organization administrator** and you copy an object owned by one user to a bucket that another user owns, the owner of the destination bucket is permanently granted with **Read of Object** permissions on the source object.

Important When you copy files, do not navigate out of the VMware Cloud Director Object Storage Extension tenant portal until the process completes. Leaving the VMware Cloud Director Object Storage Extension tenant portal within the same user session interrupts the process.

Prerequisites

Verify that you have the required set of rights to copy an object.

- If you are an **organization administrator**, you can copy objects that users in your organization own.
- If you are an **organization user**, you must be the owner of the object, or the owner must assign **Read of Object** permissions on the object to your user account. To copy objects to buckets that other users own, use *VMware Cloud Director Object Storage Extension API Reference*.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. In the **Buckets** pane, navigate to the bucket or folder that stores the object that you want to copy.
4. Select the objects that you want to copy.
5. From the **Actions** drop-down menu, select **Copy to**.
6. Select the destination bucket.
7. If you use AWS S3, you can optionally change the storage class for the object.

   The following table describes the storage classes and the corresponding use cases.

Option	Description
Standard	Default storage class. Best fit for general-purpose storage of frequently accessed data.
Reduced Redundancy	Provides the option to store noncritical, reproducible data at lower levels of redundancy than the standard storage.
Glacier	Best fit for short and mid-term archives.
Standard Infrequent Access (IA)	Best fit for long-lived and less frequently accessed data.
One Zone IA	Best fit for long-lived and less frequently accessed data that you store in a single zone.
Intelligent Tiering	Best fit for data with unknown or changing access patterns.
Glacier Deep Archive	Best fit for long-term archiving purposes.

8 Select whether you want to overwrite the objects with the same name.

   By default, VMware Cloud Director Object Storage Extension overwrites files with the same name.

9 Confirm that you understand the effect of copying an object and click **Copy**.

Preview an Object

You can preview a list of file formats directly from the VMware Cloud Director Object Storage Extension tenant portal.

- Image files, such as JPEG, PNG, and GIF
- Text files, such as plain text, HTML, XML, and JSON
- Portable Document Format files (PDF)
- Audio and video files, such as MP4, MPEG, WAV, WebM

If versioning is active for the bucket that stores the object that you want to preview, you can preview a specific version of the object.

Prerequisites

Verify that you have the required set of rights to preview an object.

- If you are an **organization administrator**, you can preview all objects owned by or shared with users within your organization.
- If you are an **organization user**, you can preview objects that you own or that are shared with you. As an **organization user**, to preview objects, **Read of Object** permissions on the object must be assigned to your user account.

Procedure

1 Log in to the VMware Cloud Director tenant portal.

2 From the **More** drop-down menu, select **Object Storage**.

3 In the **Buckets** pane, navigate to the bucket or folder that stores the object you want to preview.

4 If you want to preview an earlier version of the object, display all versions of the object by using the **Show Versions** toggle button.

5 Click the name of the object or the object version that you want to preview.

6 Click **Preview**.

   A preview of the object appears in the VMware Cloud Director Object Storage Extension tenant portal.

Download an Object

You can download only one object at a time.

If versioning is active for the bucket that stores the object that you want to download, you can download a specific version of the object.

Prerequisites

Verify that you have the required set of rights to download an object.

- If you are an **organization administrator**, you can download all objects owned by or shared with users within your organization.
- If you are an **organization user**, to download objects, you must be the owner of the object, or **Read of Object** permissions must be assigned to your user account.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. In the **Buckets** pane, navigate to the bucket or folder that stores the object that you want to download.
4. If you want to download a specific version of the object, display all versions of the object by using the **Show Versions** toggle button.
5. Select the object or the object version that you want to download.
6. From the **Actions** drop-down menu, select **Download**.
7. Navigate to the location to which you want to download the object and click **Save**.

Results

After the download process completes, the file is available in the destination directory.

Restore an Archived Object

You can restore objects belonging to AWS S3 Glacier and Glacier Deep storage classes.

AWS S3 objects belong to one of four storage classes: Standard, Intelligent, Glacier and Glacier Deep. You can access objects from the Standard and Intelligent storage classes directly at any time. Objects from the Glacier and Glacier Deep storage classes are archived. To access them, you must restore them first.

Prerequisites

Verify that you have the required set of rights to restore an object.

- If you are an **organization administrator**, you can restore all objects owned by or shared with users within your organization.

- If you are an **organization user**, to restore objects, you must be the owner of the object, or **Read of Object** permissions must be assigned to your user account.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. In the **Buckets** pane, navigate to the bucket or folder that stores the object that you want to restore.
4. Click the **Show Versions** toggle button to display all versions of the object.
5. Click the ellipsis-vertical icon (⋮) next to the version of the object that you want to restore and click **Initiate Restore**.
6. Enter the duration for the availability of the restored object, select the retrieval tier, and click **Restore**.

Results

After the restore operation completes, you can access the object during the predefined availability period. To update the period, initiate a new restore operation.

Edit Object Lock Configuration at the Object Level

With the object lock feature, you prevent objects from being deleted from a bucket. You activate the feature at the bucket level during the bucket creation, but can edit the object lock configuration at the object level.

Prerequisites

- Verify that you have the required set of rights to edit the object lock configuration.
  - If you are an **organization administrator**, you can edit the objects lock configuration for objects that users in your organization own.
  - If you are an **organization user**, you can edit the objects lock configuration for objects, if you are the owner of the bucket that stores the object.
- Verify that the object lock feature is active for the bucket that stores the object that you want to edit. If the feature is not activated during the creation of the bucket that stores the object, you cannot edit the object lock configuration for the object.
- The object lock feature is supported for Dell ECS 3.6. If you are using 3.4 or earlier, you can not use the object lock feature.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.

3 In the **Buckets** pane, navigate to the bucket or folder that stores the object that you want to edit.

4 Click the name of the object that you want to edit.

5 On the **Properties** tab, click **Edit** in the **Object Lock** card.

6 Select the retention mode and enter the retention period.

Option	Description
Governance Mode	A user with specific permissions can preview the retention policy.
Compliance Mode	The retention policy is not displayed to any user.
No Retention	Does not require the selection of a retention period. If you select this option, you can define the retention period later.

7 Select the check box to activate legal hold and click **Save**.

Legal hold prevents the object from being deleted after the retention period expires.

Delete an Object

To free storage space in VMware Cloud Director Object Storage Extension, you can delete the objects that you no longer need. You can delete multiple objects simultaneously.

After you delete an object from VMware Cloud Director Object Storage Extension, you cannot restore it.

Prerequisites

Verify that you have the required set of rights to delete an object.

- If you are an **organization administrator**, you can delete objects that users in your organization own.
- If you are an **organization user**, to delete an object, you must be the owner of the object, or the owner must assign **Read of Bucket** and **Write of Bucket** permissions on the bucket that stores the object to your user account.

Procedure

1 Log in to the VMware Cloud Director tenant portal.

2 From the **More** drop-down menu, select **Object Storage**.

3 In the **Buckets** pane, navigate to the bucket or folder that stores the objects that you want to delete.

4 If you want to delete a specific version of an object, display all versions of the object by using the **Show Versions** toggle button.

5 Select the object or the object version that you want to delete.

6 From the **Actions** drop-down menu, select **Delete** and confirm the deletion.

Results

If versioning is not active for the bucket that stores the object you deleted, the object is deleted and cannot be restored. If versioning is active for the bucket and you do not select a specific version to be deleted, you delete only the last version of the object. To retrieve earlier versions of the object, use the **Show Versions** toggle button.

Working with Multiple Sites

5

The VMware Cloud Director Multisite feature allows a cloud 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.

For more information about the VMware Cloud Director Multisite feature, see the *VMware Cloud Director Cloud Provider Admin Portal Guide* and the *VMware Cloud Director Tenant Portal Guide*.

You can deploy and configure VMware Cloud Director Object Storage Extension within a multisite VMware Cloud Director environment. For more information about configuring VMware Cloud Director Object Storage Extension within a multisite VMware Cloud Director environment, see *Installing, Configuring, and Upgrading VMware Cloud Director Object Storage Extension*.

When VMware Cloud Director Object Storage Extension is configured within a multisite VMware Cloud Director environment, tenant users can preview and download objects in the remote site.

This chapter includes the following topics:

Preview an Object in a Remote Site

You can preview a list of file formats directly from the VMware Cloud Director Object Storage Extension tenant portal.

- Image files, such as JPEG, PNG, and GIF
- Text files, such as plain text, HTML, XML, and JSON
- Portable Document Format files (PDF)
- Audio and video files, such as MP4, MPEG, WAV, WebM

Prerequisites

Verify that you are the owner of the object in the remote site that you want to preview. In the remote site, you can only preview the objects that you own.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. In the upper-left corner of the **Buckets** pane, use the drop-down menu to select the remote site.
4. Navigate to the bucket or folder storing the object that you want to preview.
5. Click the name of the object that you want to preview.
6. Click **Preview**.

   A preview of the object appears in the VMware Cloud Director Object Storage Extension tenant portal.

Download an Object from a Remote Site

You can download objects from remote sites. You can download only one object at a time.

Prerequisites

Verify that you have the required set of rights to download an object.

- If you are an **organization administrator**, you can download the objects that are owned by or shared with users within your organization.
- If you are an **organization user**, to download objects, you must be the owner of the object, or you must have the **Read of Object** permission assigned to your user account.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. In the upper-left corner of the **Buckets** pane, use the drop-down menu to select the remote site.
4. Navigate to the bucket or folder storing the object that you want to download and select it.
5. From the **Actions** drop-down menu, select **Download**.
6. Navigate to the location to which you want to download the object and click **Save**.

Results

After the download process completes, the file is available in the destination directory.

Switch to a Remote Site

Organization users can only preview and download objects that they own from remote sites. To work with objects that are shared with you, or to perform other actions with the objects that you own from remote sites, you must switch to the remote site.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. In the upper-left corner of the **Buckets** pane, select the site to which you want to switch to.
4. Click the **pop-out** icon () next to the site to which you want to switch.

   The user interface of VMware Cloud Director Object Storage Extension in the remote site opens in a new browser window.

Backing up and Restoring Kubernetes Clusters

6

Get started backing up and restoring your Kubernetes clusters with VMware Cloud Director Object Storage Extension 2.1.

Backing up your clusters allows data to be restored from an earlier point in time if an unplanned event occurs. You can back up your entire Kubernetes cluster, or part of a cluster by backing up certain namespaces or labels.

VMware Cloud Director Object Storage Extension uses Velero, an open source tool, to back up and restore your Kubernetes resources and persistent volumes. VMware Cloud Director Object Storage Extension 2.1 supports vSphere persistent volumes only. To back up and restore persistent volumes, you need to install the Velero vSphere Plugin first. Please refer to the instructions on how to set up the plugin here -https://github.com/vmware-tanzu/velero-plugin-for-vsphere.

VMware Cloud Director Object Storage Extension supports backup and restore of Tanzu Kubernetes Grid clusters, CSE Native clusters, and external clusters. If you have activated Container Service Extension, all guest Kubernetes clusters are automatically listed under **Unprotected Clusters** in the **Kubernetes Tab**. You can also add external clusters through kubconfig files.

To start backing up your clusters, you must first activate the backup protection. You can set schedules to automatically kick off backups at recurring intervals or create one-time backups.

You can recover your Kubernetes cluster or your vSphere block volumes using the backup snapshots. A snapshot is an image of your cluster at a specific point in time.

This chapter includes the following topics:

- Remove a Kubernetes Cluster

Add an External Kubernetes Cluster

You can add external Kubernetes clusters for backup in VMware Cloud Director Object Storage Extension.

Prerequisites

- Verify that the Kubernetes version is 1.16 or above.
- Verify that the primary node's IP is reachable from the VMware Cloud Director Object Storage Extension backend server.
- Verify that the S3 endpoint can be reached by the external cluster's pod.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. Click **Kubernetes Clusters** and then **Unprotected Clusters**.
4. Click **Add External Cluster**.
5. Enter a name for the cluster.
6. Click **Select File** and select the kubconfig file.
7. Click **Save**.

   The external cluster is added under **Unprotected Clusters**.

What to do next

You must activate the protection to create a backup of the cluster that you added -Backing Up Kubernetes Clusters.

Backing Up Kubernetes Clusters

To back up your cluster, you must activate the backup protection. You can set a schedule to automatically kickoff backups at recurring intervals.

Activate the backup protection to start backing up your Kubernetes clusters. If you don't activate the **Backup Schedule**, the backup agent is deployed, but the cluster is not protected and no backup can be created. You can still edit the backup schedule later or do an on-demand backup.

Prerequisites

- To back up vSphere persistent backup volumes, you must install the Velero vSphere Plugin first - https://github.com/vmware-tanzu/velero-plugin-for-vsphere.

Procedure

1 Log in to the VMware Cloud Director tenant portal.
2 From the **More** drop-down menu, select **Object Storage**.
3 Click **Kubernetes Clusters** and then **Unprotected Clusters**.
4 Select the Kubernetes cluster that you want to back up and click **Start Protection**.
5 Click the **Backup Schedule** toggle switch to activate the scheduled backup.
6 Enter the **Backup Frequency** and **Backup TTL**.
7 Select the **Backup Scope**.
8 Select the **Backup Volume** if needed.
9 Click **Save**.

Edit the Backup Protection Policy

You can edit the backup settings of a protected cluster.

Procedure

1 Log in to the VMware Cloud Director tenant portal.
2 From the **More** drop-down menu, select **Object Storage**.
3 Click **Kubernetes Clusters** and then **Protected Clusters**.
4 Select the Kubernetes cluster that you want to edit and click **Action**.
5 Click **Edit Protection Policy**.
6 Make the according changes to the backup settings and click **Save**.

Create an On-Demand Backup

You can push one-time backups on demand.

Prerequisites

- To back up vSphere persistent backup volumes, you must install the Velero vSphere Plugin first - https://github.com/vmware-tanzu/velero-plugin-for-vsphere.

Procedure

1 Log in to the VMware Cloud Director tenant portal.
2 From the **More** drop-down menu, select **Object Storage**.
3 Click **Kubernetes Clusters** and then **Protected Clusters**.
4 Select the Kubernetes cluster that you want to back up and click **Backup**.
5 Enter the **Backup TTL**, **Backup Scope**, and **Backup Volume**.

6 Click **Backup**.

Delete a Kubernetes Backup Snapshot

You can delete a Kubernetes backup snapshot.

Procedure

1 Log in to the VMware Cloud Director tenant portal.

2 From the **More** drop-down menu, select **Object Storage**.

3 Click **Kubernetes Clusters** and then **Protected Clusters**.

4 Select a Kubernetes cluster and click **Action**.

5 Click **Delete**.

6 Select one of the snapshots and click **Delete**.

7 Click **Delete** again to confirm the deletion of the backup snapshot.

Restore a Kubernetes Cluster

You can restore Kubernetes clusters using the existing backup snapshots.

Procedure

1 Log in to the VMware Cloud Director tenant portal.

2 From the **More** drop-down menu, select **Object Storage**.

3 Click **Kubernetes Clusters** and then **Protected Clusters**.

4 Select the cluster that you want to restore and click **Restore**.

5 Select a snapshot and click **Restore**.

6 Click **Restore** to confirm.

Stop Kubernetes Backup Protection

You can stop the backup protection of protected Kubernetes clusters and delete all existing snapshots.

Procedure

1 Log in to the VMware Cloud Director tenant portal.

2 From the **More** drop-down menu, select **Object Storage**.

3 Click **Kubernetes Clusters** and then **Protected Clusters**.

4 Select the cluster that you want to stop protecting and click **Action**.

5 Click **Stop Protection**.

6 To delete all existing backups, select the check box.

7 Click **Stop**.

Results

The cluster is no longer protected and is listed in **Unprotected Clusters**.

Remove a Kubernetes Cluster

You can remove unprotected Kubernetes clusters fromVMware Cloud Director Object Storage Extension.

Only unprotected clusters can be removed from VMware Cloud Director Object Storage Extension To remove a cluster that is currently protected, you must stop the protection first and then remove the cluster.

Procedure

1 Log in to the VMware Cloud Director tenant portal.

2 From the **More** drop-down menu, select **Object Storage**.

3 Click **Kubernetes Clusters** and then **Unprotected Clusters**.

4 Select the cluster that you want to remove and then click **Remove**.

5 Click **Remove** to confirm that you want to remove the cluster.

Working with VMware Cloud Director Objects

7

With VMware Cloud Director Object Storage Extension, you can back up, restore, and share VMware Cloud Director vApps.

You can also create and publish VMware Cloud Director Object Storage Extension catalogs to VMware Cloud Director. Using the VMware Cloud Director Object Storage Extension catalogs, you can synchronize and share VMware Cloud Director catalogs.

This chapter includes the following topics:

Working with vApps in VMware Cloud Director Object Storage Extension

You can use VMware Cloud Director Object Storage Extension to store vApps that you do not currently use. This way, you can free storage space from VMware Cloud Director datastores. Later, you can restore the vApp back in the datastore and continue to use the same vApp in VMware Cloud Director.

Capture vApps

By capturing a vApp, you copy all data that the vApp consumes to VMware Cloud Director Object Storage Extension. By capturing a vApp, you create a backup copy of the data that the vApp contains. You can later restore the vApp back to its original location or download the vApp locally for archiving purposes.

By capturing a vApp, you do not copy the storage reservation from VMware Cloud Director to VMware Cloud Director Object Storage Extension.

You can capture up to 10 vApps simultaneously.

Prerequisites

- Verify that you have the required set of rights to capture vApps.
  - If you are an **organization administrator**, you have all required VMware Cloud Director rights to manage vApps.

  - If you are an **organization user**, verify that you have the **vApp: View VM Metrics** and **vApp: Download** rights assigned to your user account in VMware Cloud Director.
- Verify that the vApp you want to capture is powered off.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. In the **vApps** pane, click **Capture from data center**.
4. Select the vApps that you want to capture and click **Next**.
5. (Optional) Enter different names for the vApps and enter a description.
6. Click **Capture from data center**.

Results

After the capture task completes, the captured vApps are listed in the VMware Cloud Director Object Storage Extension tenant portal vApp list. You can share, download, delete, or restore the vApps.

Share a vApp

You can share vApps that are stored in VMware Cloud Director Object Storage Extension with other users within your organization or publicly over the Internet.

You can share one vApp at a time.

Prerequisites

Verify that you have the required set of rights to share a vApp.

- If you are an **organization administrator**, you can share all vApps that users in your organization own.
- If you are an **organization user**, to share a vApp as, you must be the vApp owner.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. In the **vApps** pane, click the vertical ellipsis icon (⋮) next to the vApp that you want to share and click **Share**.

4 Select the sharing status for the vApp and click **Set Sharing Status**.

Option	Description
Private	Only the object owner and the **organization administrator** can manage the vApp in VMware Cloud Director Object Storage Extension.
Tenant	Grants **read** permissions for the vApp to all users within the same organization. If you use the ECS storage platform, this option is not available.
Public	Grants **read** permissions for the vApp to all users.

Review Shared vApps

As an **organization user**, you can review all vApps that other users shared with you. As an **organization administrator**, you can review all the vApps within your organization.

If VMware Cloud Director Object Storage Extension is configured with AWS S3, you cannot review the list of shared vApps. AWS S3 does not support reviewing shared vApps.

Procedure

1 Log in to the VMware Cloud Director tenant portal.

2 From the **More** drop-down menu, select **Object Storage**.

3 In the **vApps** pane, click **Shared vApps**.

Download a vApp

For archiving purposes, or to save storage space in VMware Cloud Director Object Storage Extension, you can download vApps locally as an OVA file.

You can download one vApp at a time.

Prerequisites

Verify that you have the required set of rights to download a vApp.

- If you are an **organization administrator**, you can download all vApps that users in your organization own.
- If you are an **organization user**, to download a vApp as, you must be the vApp owner or the owner must share the vApp with you.

Procedure

1 Log in to the VMware Cloud Director tenant portal.

2 From the **More** drop-down menu, select **Object Storage**.

3 In the **vApps** pane, click the vertical ellipsis icon (⋮) next to the vApp that you want to download and click **Share**.

4 Select the location to which you want to download the vApp and start the download process.

Upload a vApp

You can upload an archived vApp to VMware Cloud Director Object Storage Extension and later restore, and use the vApp in VMware Cloud Director.

You can upload up to 10 vApps at once. The vApp files that you upload must have the OVA file extension.

Important When uploading files to VMware Cloud Director Object Storage Extension, do not navigate out of the VMware Cloud Director Object Storage Extension tenant portal until the upload process completes. Leaving the VMware Cloud Director Object Storage Extension tenant portal within the same user session interrupts the upload process.

Procedure

1 Log in to the VMware Cloud Director tenant portal.

2 From the **More** drop-down menu, select **Object Storage**.

3 In the **vApps** pane, click **Upload**.

4 Select whether you want to overwrite objects with the same name.

By default, VMware Cloud Director Object Storage Extension overwrites files with the same name.

5 Click the folder icon ( ), navigate to the files that you want to upload, and click **Upload**.

Import a vApp

You can import vApps from VMware Cloud Director Object Storage Extension directly to VMware Cloud Director using the VMware Cloud Director tenant portal.

Prerequisites

- Verify that you have the required set of rights to import vApps.
  - If you are an **organization administrator**, you have all required VMware Cloud Director rights to manage vApps.
  - If you are an **organization user**, verify that you have the **vApp: View VM Metrics** and **vApp: Download** rights assigned to your user account in VMware Cloud Director.
- Verify that the vApp you want to import is powered off.

Procedure

1 Log in to the VMware Cloud Director tenant portal.

2 Navigate to **Applications > Virtual Applications**.

3 From the **Actions** drop-down menu of the vApp that you want to import, select **Import from Object Storage**.

If multiple snapshots of the vApp are available, click **Import** next to the snapshot that you want to import.

4 Select one of the following options:

Option	Description
Import as New	You are transferred to the **Restore vApp to Cloud Director** page in VMware Cloud Director Object Storage Extension. You can optionally change the name and the target virtual data center for the restored vApp. Click **Restore** . The vApp is then imported to VMware Cloud Director as a new vApp.
Replace Current	The existing vApp in VMware Cloud Directoris replaced with a vApp from VMware Cloud Director Object Storage Extension.

5 Click **Import**.

Export a vApp

You can export vApps to VMware Cloud Director Object Storage Extension directly from VMware Cloud Director using the VMware Cloud Director tenant portal.

Prerequisites

- Verify that you have the required set of rights to export vApps.
  - If you are an **organization administrator**, you have all required VMware Cloud Director rights to manage vApps.
  - If you are an **organization user**, verify that you have the **vApp: View VM Metrics** and **vApp: Download** rights assigned to your user account in VMware Cloud Director.
- Verify that the vApp you want to export is powered off.

Procedure

1 Log in to the VMware Cloud Director tenant portal.

2 Navigate to **Applications > Virtual Applications**.

3 From the **Actions** drop-down menu of the vApp that you want to export, select **Export to Object Storage** and click **Export**.

Results

After you export the vApp, you can find a folder with the same name as the exported vApp in VMware Cloud Director Object Storage Extension. All exported vApps are listed inside that folder with a timestamp.

Restore a vApp

To use a vApp that you store in VMware Cloud Director Object Storage Extension, you restore the vApp back to a VMware Cloud Director virtual data center. You can restore one vApp at a time.

When you restore a vApp, you can edit the hardware properties of each virtual machine that the vApp contains.

Prerequisites

- Verify that you have the required set of rights to restore a vApp.
  - As an **organization administrator**, you have all required VMware Cloud Director rights to manage vApps.

    As an **organization administrator**, you can restore all vApps that users in your organization own.
  - As an **organization user**, verify that you have the **vApp: Upload**, **vApp: Create / Reconfigure**, and the **Organization vDC: View** permissions assigned to your user account in VMware Cloud Director.

    As an **organization user**, you can restore a vApp, if you are the vApp owner, or the owner has shared the vApp with you.
- Verify that the target organization virtual data center has enough compute resources to accommodate the vApp that you restore.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. In the **vApps** pane, click the vertical ellipsis icon next to the vApp that you want to restore and click **Restore to data center**.
4. Edit the settings of the vApp and the virtual machines and click **Restore**.
   a. (Optional) Edit the name of the vApp.
   b. Select the target virtual data center for the vApp.
   c. (Optional) Edit the hardware settings of the virtual machines that the vApp contains.

Results

After the restore task completes, the vApp is available in the inventory of VMware Cloud Director.

What to do next

You can start using the vApp in VMware Cloud Director.

If you no longer need a backup copy of the same vApp, you can delete the vApp from VMware Cloud Director Object Storage Extension.

Delete vApps

When you no longer need a vApp in VMware Cloud Director Object Storage Extension, you can delete it.

You can delete multiple vApps simultaneously. You cannot restore vApps that you delete from VMware Cloud Director Object Storage Extension.

Prerequisites

Verify that you have the required set of rights to delete vApps.

- If you are an **organization administrator**, you can delete all vApps that users in your organization own.
- If you are an **organization user**, to delete a vApp, you must be the vApp owner. **Organization users** cannot delete shared vApps.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. In the **vApps** pane, select the vApps that you want to delete.
4. From the **Actions** drop-down menu, select **Delete** and confirm the operation.

Results

The vApps that you delete are no longer stored in VMware Cloud Director Object Storage Extension.

Working with Catalogs

A catalog in VMware Cloud Director Object Storage Extension is a container for ISO, OVA, OVF, MF, and VMDK files.

Create a Catalog

When you create a catalog, VMware Cloud Director Object Storage Extension creates a catalog bucket and reserves it as a system bucket.

Although the catalog bucket appears in the **Buckets** pane in VMware Cloud Director Object Storage Extension, you cannot interact with catalog buckets the same way you interact with regular buckets. You interact with catalog buckets from the **Catalogs** pane.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. In the **Catalogs** pane, click **New Catalog**.

4 Enter a name for the catalog and click **Save**.

Results

The new catalog appears in the list of catalogs in the **Catalogs** pane.

What to do next

You can upload files to the catalog.

Create a Template in a Catalog

Templates are the folders within catalogs in VMware Cloud Director Object Storage Extension.

For every OVA file that you upload, VMware Cloud Director Object Storage Extension creates a folder with the OVA filename and extracts the OVF, MF, and VMDK files to the folder.

You can also manually create a template within a catalog and upload OVF and VMDK files to that folder.

Prerequisites

Verify that you have the required set of rights to create a template in a catalog.

- If you are an **organization administrator**, you can create templates in all catalogs that users in your organization own.
- If you are an **organization user**, you can create templates in catalogs that you own.

Procedure

1 Log in to the VMware Cloud Director tenant portal.

2 From the **More** drop-down menu, select **Object Storage**.

3 In the **Catalogs** pane, click the name of the catalog in which you want to create a template.

4 Click **Create Template**, enter a name for the template, and confirm the creation.

Upload Files to a Catalog

You can upload ISO and OVA files to a catalog in VMware Cloud Director Object Storage Extension.

For every OVA file that you upload, VMware Cloud Director Object Storage Extension creates a folder with the OVA filename and extracts the OVF, MF, and VMDK files to the folder. You cannot modify the objects in such folders, you can only delete them.

You can manually create a template within a catalog and upload OVF and VMDK files to that folder.

If you replace the OVA or ISO files within a published catalog, the operation increases the version of the vApp Template or the media item within the catalog.

You cannot upload OVF and VMDK files to the main directory of a catalog.

Important When uploading files to VMware Cloud Director Object Storage Extension, do not navigate out of the VMware Cloud Director Object Storage Extension tenant portal until the upload process completes. Leaving the VMware Cloud Director Object Storage Extension tenant portal within the same user session interrupts the upload process.

Prerequisites

Verify that you have the required set of rights to upload files to a catalog.

- If you are an **organization administrator**, you can upload files to all catalogs that users in your organization own.
- If you are an **organization user**, to upload files to a catalog, you must be the catalog owner.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. In the **Catalogs** pane, click the name of the catalog or the template to which you want to upload files.
4. Click **Upload**.
5. Click the folder icon ( ), navigate to the files that you want to upload, and click **Upload**.

Add a Catalog to VMware Cloud Director

If you created a catalog in VMware Cloud Director Object Storage Extension and uploaded media files to the catalog, you can add the catalog to the libraries of VMware Cloud Director. When you import a catalog to VMware Cloud Director, **organization users** can work with the catalog contents directly in VMware Cloud Director.

When you add a catalog from VMware Cloud Director Object Storage Extension to VMware Cloud Director, you create a catalog in VMware Cloud Director that contains all objects stored in the VMware Cloud Director Object Storage Extension catalog.

Prerequisites

Verify that you have the required set of rights to import catalogs to VMware Cloud Director.

- As an **organization administrator**, you have all required VMware Cloud Director rights to manage catalogs.
- As an **organization user**, verify that you have the following rights assigned to your user account in VMware Cloud Director:
  - **Catalog: Create / Delete a Catalog**
  - **Organization vDC: View**

- **Organization vDC Network: View Properties**

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. In the **Catalogs** pane, click the name of the catalog that you want to import and click **Add to libraries**.
4. (Optional) Change the catalog name.

   The name that you enter is used as the catalog name in VMware Cloud Director.
5. To start the process, click **Add to libraries**.

Results

After the task completes, you can start using the objects in the VMware Cloud Director tenant portal.

Publish a Catalog

When you publish a catalog, you make the catalog available for a subscription from VMware Cloud Director.

When you publish a catalog, VMware Cloud Director Object Storage Extension creates JSON files that contain all metadata and descriptors which the VMware Cloud Director catalogs require for an external subscription. For more information, see Subscribe to an External Catalog.

Prerequisites

Verify that you have the required set of rights to publish a catalog.

- If you are an **organization administrator**, you can publish all catalogs that users in your organization own.
- If you are an **organization user**, to publish a catalog, you must be the catalog owner.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. In the **Catalogs** pane, click the name of the catalog that you want to publish and click **Publish**.
4. Note the subscription URL and password, as you need them to configure the subscription in the VMware Cloud Director tenant portal.
5. Click **OK**.

What to do next

After the catalog publishing task completes, you can configure the subscription to the catalog.

Share a Catalog

You can share VMware Cloud Director Object Storage Extension catalogs with other users within your organization or publicly over the Internet.

Prerequisites

- Verify that you have the required set of rights to share a catalog.
  - If you are an **organization administrator**, you can share all catalogs that users in your organization own.
  - If you are an **organization user**, to share a catalog, you must be the catalog owner.
- Verify that the catalog you want to share is published. You cannot share catalogs that are not published.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. In the **Catalogs** pane, click the name of the catalog that you want to share.
4. From the **Actions** drop-down menu, select **Share**.
5. Select the sharing status for the catalog and click **Set Sharing Status**.

Option	Description
Private	Only the object owner and the **organization administrator** can manage the catalog in VMware Cloud Director Object Storage Extension.
Tenant	Grants all users within the same organization with **Read** permissions on the catalog. If you use the ECS storage platform, this option is not available.
Public	Grants all users with **Read** permissions on the catalog.

Review Shared Catalogs

As an **organization user**, you can review all catalogs that other users shared with you. As an **organization administrator**, you can review all the catalogs within your organization.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. In the **Catalogs** pane, click **Shared Catalogs**.

Unpublish a Catalog

When you unpublish a catalog, you restrict the subscription to the catalog from VMware Cloud Director and stop the existing subscriptions.

Prerequisites

Verify that you have the required set of rights to unpublish a catalog.

- If you are an **organization administrator**, you can unpublish all catalogs that users in your organization own.
- If you are an **organization user**, to unpublish a catalog, you must be the catalog owner.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. In the **Catalogs** pane, click the name of the catalog that you want to unpublish and click **Unpublish**.

Results

After the unpublishing task completes, subscription to the catalog from VMware Cloud Director is not possible.

Empty a Catalog

To clean up the inventory of VMware Cloud Director Object Storage Extension and to free storage space, you can empty a catalog. By emptying a catalog, you delete all objects from the catalog.

Prerequisites

- Verify that you have the required set of rights to empty a catalog.
  - If you are an **organization administrator**, you can empty all catalogs that users in your organization own.
  - If you are an **organization user**, to empty a catalog, you must be the catalog owner.
- Verify that the catalog you want to empty is not published. You cannot delete catalogs that are published for an external subscription.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. In the **Catalogs** pane, click the vertical ellipsis icon (⋮) next to the catalog that you want to empty.
4. Click **Empty** and confirm the operation.

Delete a Catalog

To clean up the inventory of VMware Cloud Director Object Storage Extension, you can delete the catalogs that you no longer need.

Prerequisites

- Verify that you have the required set of rights to delete a catalog.
  - If you are an **organization administrator**, you can delete all catalogs that users in your organization own.
  - If you are an **organization user**, to delete a catalog, you must be the catalog owner.
- Verify that the catalog you want to delete is not published. You cannot delete catalogs that are published for an external subscription.
- Verify that the catalog you want to delete does not store any objects. If there are objects in the catalog, first you must empty the catalog. See Empty a Catalog.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. In the **Catalogs** pane, click the vertical ellipsis icon (⋮) next to the catalog that you want to delete.
4. Click **Delete** and confirm the deletion.

Working with Security Credentials

8

Security credentials are a pair of an access key and a secret key. You use the keys pair for AWS Signature v4 authentication.

Cloudian HyperStore supports user and application types of security credentials. You can use the keys pair to authenticate S3 API requests and to access and manage objects and buckets.

With S3 API requests, authenticated with user credentials, you can manage all objects that you own or the objects that are shared with you.

With application credentials, you control the S3 API access at the bucket level.

If you use AWS S3 or ECS, you can only use user credentials to authenticate S3 API requests. With AWS S3 and ECS, each user account has a single pair of an access and secret keys.

You can rotate the user credential. The rotation only updates the secret key. When you rotate a user credential, the old secret key remains active for five minutes.

This chapter includes the following topics:

Working with User Credentials

Users own and manage their user credentials. VMware Cloud Director Object Storage Extension reserves one security credential for system management purposes. You cannot delete or deactivate that credential.

Organization administrators and **organization users** can use user credentials only to access and manage buckets and objects that they own or that are shared with them.

Create a User Credential

To manage your buckets and objects in VMware Cloud Director Object Storage Extension by using S3 API, create a user credential. By default, when you create a user credential, VMware Cloud Director Object Storage Extension activates the credential and you can use it right away.

You can create up to five user credentials.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. Select **Security Credentials > User Credentials** and click **Create**.

Results

A new security credential appears in the list of user credentials.

Activate or Deactivate a User Credential

To restrict or grant the S3 API access to your buckets and objects, you can activate and deactivate your user credentials.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. Select **Security Credentials > User Credentials** and select the user credential that you want to activate or deactivate.
4. Use the toggle button in the Status column and confirm the operation.

Delete a User Credential

To clean up the inventory of VMware Cloud Director Object Storage Extension, delete the user credentials that you no longer need.

Prerequisites

Verify that the user credential is deactivated. You cannot delete active user credentials.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. Select **Security Credentials > User Credentials** and select the user credential that you want to delete.
4. Click **Delete** and confirm the operation.

Working with Application Credentials

Users own and manage their application credentials.

Organization administrators and **organization users** can use application credentials only to access and manage buckets that they own.

Application credentials add constraints to the bucket access. With an application credential, an API client cannot create buckets or delete existing buckets. If you specify bucket names during the creation of application credentials, you only allow accessing and managing the specified bucket.

Create an Application Credential

To manage objects in a specific bucket or buckets by using S3 API, create an application credential. By default, when you create an application credential, VMware Cloud Director Object Storage Extension activates the credential and you can use it right away.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. Select **Security Credentials > Application Credentials** and click **Create**.
4. Enter a name for the application credential.
5. Select the buckets that can be accessed with the application credential and click **Create**.

Results

A new security credential appears in the list of application credentials.

Activate or Deactivate an Application Credential

To restrict or grant the S3 API access to your buckets, you can activate and deactivate your application credentials.

Procedure

1. Log in to the VMware Cloud Director tenant portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. Select **Security Credentials > Application Credentials** and select the application credential that you want to activate or deactivate.
4. Use the toggle button in the Status column and confirm the operation.

Delete an Application Credential

To clean up the inventory of VMware Cloud Director Object Storage Extension, delete the application credentials that you no longer need.

Prerequisites

Verify that the application credential is deactivated. You cannot delete active application credentials.

Procedure

1. Log in to the VMware Cloud Director tenant portal.

2 From the **More** drop-down menu, select **Object Storage**.

3 Select **Security Credentials > Application Credentials** and select the application credential that you want to delete.

4 Click **Delete** and confirm the operation.

Working with VMware Cloud Director Object Storage Extension S3 API

9

VMware Cloud Director Object Storage Extension provides a set of S3 compatible APIs for bucket and object operations.

The VMware Cloud Director Object Storage Extension API support AWS Signature v4, VMware Cloud Director authorization token, and JSON Web Token (JWT) authentication methods.

The VMware Cloud Director Object Storage Extension API support JSON and XML formats.

By default, the S3 APIs of VMware Cloud Director Object Storage Extension are available at `https://object-storage-extension-host-address/api/v1/s3`. Depending on the network configuration of your cloud provider, the address of VMware Cloud Director Object Storage Extension and the root path for the S3 API might be different from the default configuration.

The VMware Cloud Director Object Storage Extension S3 API documentation is available with the product at `https://object-storage-extension-host-address/docs` and in the VMware API Explorer at https://code.vmware.com/apis, under the VMware Cloud Director Object Storage Extension product category.

Using Security Credentials and VMware Cloud Director Object Storage Extension API

To see how you work with security credentials and VMware Cloud Director Object Storage Extension API, use the following example.

1. Create a user credential by using the VMware Cloud Director Object Storage Extension tenant portal.

   By default, newly created user credentials are activated during creation.
2. Copy the access and secret keys.
3. Note the name of a bucket as it is displayed in the VMware Cloud Director Object Storage Extension tenant portal.
4. In your API client, use the AWS Signature authentication method to authenticate your API request by entering the API endpoint and the access and security keys.

   For example, enter the following connection information:

API Endpoint	**https://*Cloud-Director-Object-Storage-Extension-IP-Andreas*:443/api/v1/s3**
Access key	**5a5af54cf34a172a511f**
Secret key	**omSG+UXSoyD1fbdFt0iia3I8I+f0QLSiIn5wpq1L**

5 To list all buckets owned by the owner of the user credential, run an S3 API **GET** request .

For example:

```
GET /api/v1/s3/ HTTP/1.1
Host: vCloud-Director-Object-Storage-Extension-IP-addres:443
Accept: application/xml
X-Amz-Content-Sha256: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
X-Amz-Date: 20190717T014259Z
Authorization: AWS4-HMAC-SHA256 Credential=5a5af54cf34a172a511f/20190717/us-
east-1/s3/aws4_request, SignedHeaders=accept;host;x-amz-content-sha256;x-amz-date,
Signature=a1a0cfdc34fd4275f567ef673f14d8ff963242d29c13515506a3a913e7f38415
cache-control: no-cache
```

The system returns the following XML representation of the contents of the bucket:

```
<listBucketResult>
        <Name>bucket-name</Name>
        <KeyCount>1</KeyCount>
        <MaxKeys>1000</MaxKeys>
        <Contents>
            <Key>object-name</Key>
            <Owner>
                <ID>system-id-of-the-user</>
                <DisplayName>display-name-of-the-user</DisplayName>
            </Owner>
            <StorageClass>Storage-Class</StorageClass>
            <Size>object-size-in-KB</Size>
            <LastModified>last-modified-date</LastModified>
        </Contents>
        <IsTruncated>true-or-false</IsTruncated>
        <ContinuationToken>1-or-0</ContinuationToken>
</listBucketResult>
```

To obtain a user or an application credential, see Chapter 8 Working with Security Credentials.

Apply a Cloudian Storage Policy

10

When using the Cloudian Platform, you can apply custom storage policies, created by your provider admin.

Storage policies ensure that your data is protected and highly available. A default storage policy is applied to all tenants. Your provider administrator can create custom storage policies for tenants who use the Cloudian platform.

Procedure

1 Log in to the VMware Cloud Director tenant portal.

2 From the **More** drop-down menu, select **Object Storage**.

3 Click **Settings** and then **Storage Policy**.

4 Click **Edit**.

5 Select **Specific Storage Policy** and then select a storage policy from the drop-down menu.

6 Click **Save**.