Using VMware Cloud Director Object Storage Extension as a Cloud Provider

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

Working with VMware Cloud Director Object Storage Extension as a Cloud Provider

1

Cloud providers with the VMware Cloud Director **System Administrator** user role can manage VMware Cloud Director Object Storage Extension.

By using the VMware Cloud Director Object Storage Extension cloud provider admin portal, you can activate or deactivate VMware Cloud Director Object Storage Extension for a tenant organization.

By using the `ose` command-line utility, you can manage and reconfigure VMware Cloud Director Object Storage Extension. For example, you can change the logging level or change the public network port.

To manage and monitor the underlying storage, use the storage management console of your storage vendor.

Access VMware Cloud Director Object Storage Extension

2

You access the VMware Cloud Director Object Storage Extension cloud provider admin portal from VMware Cloud Director cloud provider admin portal.

During the configuration of VMware Cloud Director Object Storage Extension, the user interface of VMware Cloud Director Object Storage Extension registers as a plug-in to VMware Cloud Director.

Prerequisites

- Verify that VMware Cloud Director Object Storage Extension is configured properly.
- Verify that your user profile in VMware Cloud Director has a **System Administrator** role assigned.

Procedure

1. In a browser, go to the VMware Cloud Director cloud provider admin portal URL.

   For example, `https://vcloud.example.com/provider`.

2. Log in with the **System Administrator** user name and password.
3. From the **More** drop-down menu, select **Object Storage**.

Access the AWS Console

3

If you configured VMware Cloud Director Object Storage Extension with AWS S3, you can manage and monitor your AWS environment in the AWS Console.

Procedure

1. Log in to the VMware Cloud Director cloud provider admin portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. On the **Platform** tab, click the pop-out icon ().

   The AWS Console opens in a new tab of your Web browser.

Access the ECS Management Console

4

If you configured VMware Cloud Director Object Storage Extension with the ECS storage platform, you can manage and monitor the ECS components and services by using the ECS Management Console.

Procedure

1. Log in to the VMware Cloud Director cloud provider admin portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. On the **Platform** tab, click the pop-out icon ().

   The ECS Management Console opens in a new tab of your Web browser.
4. Enter your credentials and log in.

Access the Cloudian Management Console

5

If you configured VMware Cloud Director Object Storage Extension with the Cloudian storage platform, you can manage and monitor the Cloudian components and service by using the Cloudian Management Console.

For information about using the Cloudian Management Console, see the Cloudian HyperStore Administration Guide.

Procedure

1. Log in to the VMware Cloud Director cloud provider admin portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. On the **Platform** tab, click the pop-out icon ().

Results

The Cloudian Management Console opens in a new tab of your Web browser.

Onboarding VMware Cloud Director Organizations and Users to AWS

6

When you onboard VMware Cloud Director organization users to AWS, you create an association between an AWS account and a VMware Cloud Director organization.

When you associate a VMware Cloud Director organization with an AWS account, all VMware Cloud Director organization users share the same AWS storage.

To onboard VMware Cloud Director organization users to AWS, you can invite an existing AWS account, create an AWS account, share an AWS account between multiple VMware Cloud Director organizations, or reuse an existing AWS account.

This chapter includes the following topics:

Invite an AWS User Account

You can invite an existing AWS user account to start using VMware Cloud Director Object Storage Extension.

Inviting an AWS user to VMware Cloud Director Object Storage Extension requires actions on both the cloud provider and the AWS account owner sides. The cloud provider sends an invitation to the AWS account owner. The invitation is communicated to the AWS account over email and within the AWS Console.

After the AWS account owner accepts the invitation, and performs the required actions in the AWS Console, VMware Cloud Director Object Storage Extension verifies if:

- The invited account authorized the AWS payer account to provision the invited account.
- The invited account is authorized to use AWS S3.

Once the verification completes, the AWS user account is active and can use VMware Cloud Director Object Storage Extension.

Prerequisites

Verify that VMware Cloud Director Object Storage Extension is inactive for the VMware Cloud Director organization to which you want to invite a user account.

Procedure

1 Log in to the VMware Cloud Director cloud provider admin portal.

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

3 On the **Tenants** tab, click the name of the tenant organization to which you want to invite an AWS user.

4 In the storage platform card, click **Manage Account**.

5 Select **Invite Account** and click **Next**.

6 Enter the AWS account ID and the account email.

7 (Optional) Enter a note to the invitation.

8 Click **Invite**.

An invitation is sent to the user in the AWS Console and a notification with instructions is sent over email. The invitation is active for 15 days. If the user does not accept or reject the invitation during the period, the invitation automatically canceled.

The invitation that is sent to the account contains instructions for acceptance. To use VMware Cloud Director Object Storage Extension with AWS S3, the owner of the invited AWS account must do the following three actions in the AWS Console:

a Accept the invitation.

b Allow the AWS payer account to provision additional roles to the invited account. For more information see Creating the OrganizationAccountAccessRole in an invited member account.

c Activate AWS S3.

Once the user completes the actions, VMware Cloud Director Object Storage Extension verifies and automatically activates the AWS user account. The tenant can start using VMware Cloud Director Object Storage Extension with AWS S3.

9 (Optional) While waiting for a response from the tenant user, you can perform the following three actions:

- To get the latest status of the invitation from AWS, click **Sync Status**.
- To send a reminder to the invited account over email, click **Remind by email**.

  Your default email client opens with a predefined email template that you can send to the tenant user. You can edit the text of the email as required.
- To cancel the invitation, click **Cancel Invitation**.

Create an AWS User Account

When onboarding VMware Cloud Director organization users to AWS, you can create a new AWS account with an email and appoint it as the owner of the VMware Cloud Director tenant organization.

When you create a new user account, you only need a valid email address of the user for which you want to create an AWS account. VMware Cloud Director Object Storage Extension creates the AWS user account, assigns all required permissions, and activates AWS S3 for the user account.

Prerequisites

- Verify that VMware Cloud Director Object Storage Extension is inactive for the VMware Cloud Director organization within which you want to create a user account.
- Verify that the email of the user that you want to onboard does not already have an AWS account.

Procedure

1. Log in to the VMware Cloud Director cloud provider admin portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. On the **Tenants** tab, click the name of the tenant organization within which you want to create an AWS account.
4. In the storage platform card, click **Manage Account**.
5. Select **Create** and click **Next**.
6. Enter the email address for the AWS user account and click **Create**.

   Creating and configuring the AWS account takes a few minutes.
7. (Optional) To retrieve the latest status of the account creation and configuration, click **Sync Status**.

Results

Once the account is created and configured, VMware Cloud Director Object Storage Extension automatically activates the AWS user account and the tenant can start using VMware Cloud Director Object Storage Extension with AWS S3.

Share an AWS User Account

By sharing an AWS user account, VMware Cloud Director users that belong to different organizations can share the same AWS S3 storage.

All VMware Cloud Director organization users that belong to a single organization can see and work with all buckets and objects that belong to the associated AWS account.

If you use the same AWS account to onboard more than one VMware Cloud Director organization, all users from the associated VMware Cloud Director organizations share the same storage.

If an AWS account is shared, you can see the VMware Cloud Director organization that share the account from the storage platform card at **Tenants >** ***Tenant-Organization-Name***.

Sharing an AWS account is a best practice for organization users that work in the same department and must work with the same objects. For example, organization users from the financial and human resources departments of a company that provide input to the same quarterly report.

You can share an AWS account across VMware Cloud Director organizations within a multisite deployment. When sharing and AWS account, you can associate VMware Cloud Director organizations from remote sites with the AWS account.

Prerequisites

Verify that VMware Cloud Director Object Storage Extension is inactive for the VMware Cloud Director organization within which you want to share a user account.

Procedure

1. Log in to the VMware Cloud Director cloud provider admin portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. On the **Tenants** tab, click the name of the tenant organization within which you want to share an AWS account.
4. In the storage platform card, click **Manage Account**.
5. Select **Share** and click **Next**.
6. Select an AWS account from the drop-down menu and click **Assign**.

   Configuring a sharing of an AWS account takes a few minutes.
7. (Optional) To retrieve the latest status of the account sharing configuration, click **Sync Status**.

Results

Once the shared account is configured, the organization user can start using VMware Cloud Director Object Storage Extension with AWS S3.

Reuse an AWS User Account

By reusing an AWS account, you use an existing AWS account that is not associated with a VMware Cloud Director organization from the AWS root organization pool to provide access to VMware Cloud Director Object Storage Extension to a VMware Cloud Director organization user.

Prerequisites

Verify that VMware Cloud Director Object Storage Extension is inactive for the VMware Cloud Director organization within which you want to reuse a user account.

Procedure

1. Log in to the VMware Cloud Director cloud provider admin portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. On the **Tenants** tab, click the name of the tenant organization within which you want to reuse an AWS account.
4. In the storage platform card, click **Manage Account**.
5. Select **Reuse** and click **Next**.
6. From the drop-down menu, select the AWS account that you want to reuse.
7. (Optional) To clean up all existing buckets of the account, select the check box.

   Cleaning up buckets and objects from AWS S3 is time consuming. You can close the dialog box and come back to the **Tenants** tab to review the progress.

   Note If the cleanup operation fails, resetting the AWS account fails as well.
8. Click **Assign**.

   Configuring a reuse of an AWS account takes a few minutes.
9. (Optional) To retrieve the latest status of the account reuse configuration, click **Sync Status**.

Results

Once the reused account is configured, the organization user can start using VMware Cloud Director Object Storage Extension with AWS S3.

Reset an AWS User Account

To remove the association between an AWS account and a VMware Cloud Director organization, you can reset the AWS account.

If the AWS account is shared between VMware Cloud Director organizations, you cannot clean up buckets and objects from AWS S3.

If the AWS account is associated with a single VMware Cloud Director organization, you can optionally clean up all buckets and objects that the account owns from AWS S3. If you choose not to clean up the buckets and objects that the account owns, the resources remain stored in AWS S3.

Prerequisites

Verify that VMware Cloud Director Object Storage Extension is inactive for the VMware Cloud Director organization to which the user account belongs.

Procedure

1. Log in to the VMware Cloud Director cloud provider admin portal.

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

3 On the **Tenants** tab, click the name of the tenant organization to which the AWS account belongs.

4 In the storage platform card, click **Reset Tenant**.

5 (Optional) To remove all buckets and objects from AWS S3, select Clean up all buckets.

   Cleaning up buckets and objects from AWS S3 is time consuming. You can close the dialog box and come back to the **Tenants** tab to review the progress.

   Note If the cleanup operation fails, resetting the AWS account also fails.

Results

While the operation runs, the status is **Purging**. Once the operation completes successfully, the status changes to **Deactivated**. If resetting the account fails, the status changes to **Abnormal** and an error message indicates what the issue might be.

If this account is reused or invited, the account is released from the organization unit and is moved to the root organization pool.

If the account is invited, the account is removed from the root organization pool.

What to do next

If the account is reused or invited, you can reuse this account again and provide access to VMware Cloud Director Object Storage Extension to another VMware Cloud Director organization user. See Reuse an AWS User Account.

If the account is invited, you cannot reuse it. To provide access to VMware Cloud Director Object Storage Extension to the same AWS account, invite the account again. See Invite an AWS User Account.

Onboarding VMware Cloud Director Organizations and Users to an On-Premise Storage Platform

7

You onboard VMware Cloud Director organization users to a storage platform, for example ECS or Cloudian, by activating VMware Cloud Director Object Storage Extension for a VMware Cloud Director organization for the first time.

When you activate VMware Cloud Director Object Storage Extension for a VMware Cloud Director organization for the first time, an equivalent group is created in the underlying storage platform. The group in the storage platform is the equivalent of a VMware Cloud Director organization. Initially, the group does not contain any users. When an organization user of VMware Cloud Director creates a bucket and uploads an object to VMware Cloud Director Object Storage Extension for the first time, a storage user is created in the corresponding group in the storage platform.

When you deactivate VMware Cloud Director Object Storage Extension for a VMware Cloud Director organization, the organization users cannot access VMware Cloud Director Object Storage Extension, but the buckets and objects that the users created are retained.

If you deactivate and delete an organization user from VMware Cloud Director, the storage user remains active and the object storage data is retained in the storage platform. When you delete an organization user from VMware Cloud Director, you can transfer only the VMware Cloud Director resources to another organization user. To clean up the object storage data of a deleted organization user, use the storage management console.

To restore the access to the resources for the organization users, activate VMware Cloud Director Object Storage Extension.

See Activating and Deactivating VMware Cloud Director Object Storage Extension for a Tenant Organization .

Managing Tenant Organizations

8

To activate or deactivate VMware Cloud Director Object Storage Extension for a VMware Cloud Director organization, use the VMware Cloud Director Object Storage Extension cloud provider admin portal.

To manage storage quotas, rating plans, and other storage platform features for a tenant organization, use the storage management console provided by your storage vendor, that is the AWS Console, the Cloudian Management Console, or the ECS Management Console.

This chapter includes the following topics:

Activating and Deactivating VMware Cloud Director Object Storage Extension for a Tenant Organization

By activating or deactivating VMware Cloud Director Object Storage Extension for a tenant organization, you control the access of organization users to VMware Cloud Director Object Storage Extension.

Activate VMware Cloud Director Object Storage Extension for a Tenant Organization

By activating VMware Cloud Director Object Storage Extension for a tenant organization, you provide the users in the organization with access to VMware Cloud Director Object Storage Extension.

Procedure

1. Log in to the VMware Cloud Director cloud provider admin portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. On the **Tenants** tab, click the name of the tenant organization for which you want to activate VMware Cloud Director Object Storage Extension.

4 Turn the toggle on for the selected tenant organization.

5 To create mapping between the tenant organization and a storage tenant, select a storage tenant ID from the drop-down menu.

6 Click **Activate**.

Deactivate VMware Cloud Director Object Storage Extension for a Tenant Organization

By deactivating VMware Cloud Director Object Storage Extension for a tenant organization, you restrict the access to object storage resources for the users in the organization.

Procedure

1 Log in to the VMware Cloud Director cloud provider admin portal.

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

3 On the **Tenants** tab, click the name of the tenant organization for which you want to deactivate VMware Cloud Director Object Storage Extension.

4 Turn the toggle off for the selected tenant organization.

5 To confirm the operation, click **Deactivate**.

Edit Tenant Mapping Configuration

You can edit the mapping between the VMware Cloud Director and the storage platform tenant entities.

When you first activate VMware Cloud Director Object Storage Extension for a tenant organization, VMware Cloud Director Object Storage Extension creates an equivalent group in the underlying storage platform. When the storage tenant is created, VMware Cloud Director Object Storage Extension maps it to the VMware Cloud Director tenant organization. You can change the mapping configuration.

If you have vendor-specific object storage data (buckets and objects) in your data center, before you start using VMware Cloud Director Object Storage Extension, you can introduce the existing data to VMware Cloud Director Object Storage Extension by editing the tenant mapping.

By configuring the tenant mapping, you can also use one storage tenant for multiple VMware Cloud Director tenant organizations.

You can map multiple VMware Cloud Director tenant organization to the same storage group, for example, to share the storage for tenant organizations within a multisite VMware Cloud Director environment. A best practice is to create a standalone storage group in your storage platform and then map tenant organizations to it. It is not a best practice to map one tenant organization to the default storage group of another tenant organization.

When you edit the default tenant mapping configuration, consider the following constraints:

- For example, by default *tenant1* is mapped to *storage1*. If you edit the mapping for *tenant1* and map it to *storage2*, you cannot map another tenant to *storage1*.
- For example, by default *tenant1* is mapped to *storage1*. If you map *tenant2* to *storage1*, you cannot map *tenant1* to another storage.

Prerequisites

Verify that you deactivated VMware Cloud Director Object Storage Extension for the tenant organization for which you want to edit the mapping configuration. See Deactivate VMware Cloud Director Object Storage Extension for a Tenant Organization.

Procedure

1. Log in to the VMware Cloud Director cloud provider admin portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. On the **Tenants** tab, click the name of the tenant organization for which you want to edit the mapping configuration.
4. In the storage platform card, click the note icon ( ) next to the storage tenant ID.
5. Enter the storage tenant ID that you want to map to the tenant organization, or select it from the drop-down menu, and click **Save**.

What to do next

Activate VMware Cloud Director Object Storage Extension for the tenant organization. See Activate VMware Cloud Director Object Storage Extension for a Tenant Organization .

Manage a Storage Tenant Organization

You can manage the storage tenant organizations by using the management console of the storage vendor that you use. To ease your navigation in the management console of your vendor, you can use the VMware Cloud Director Object Storage Extension tenant portal and access a specific tenant organization directly in the management console of the vendor.

Within the storage management console, you can manage storage quotas, rating plans, and other storage platform features at the tenant organization level.

Procedure

1. Log in to the VMware Cloud Director cloud provider admin portal.
2. From the **More** drop-down menu, select **Object Storage**.
3. On the **Tenants** tab, click the name of the tenant organization that you want to manage.

4 Click the pop-out icon () in the upper right corner of the storage platform card and confirm the operation.

Results

You are redirected to the management console of the storage platform.

VMware Cloud Director Object Storage Extension Administration

9

You can use the `ose` command-line utility to change the configuration of VMware Cloud Director Object Storage Extension and to troubleshoot problems.

Reconfiguring VMware Cloud Director Object Storage Extension requires you to stop the VMware Cloud Director Object Storage Extension service, perform the operation that you want, and start the service again.

This chapter includes the following topics:

Cloudian Storage Policies

Cloud providers can create and assign custom storage policies for tenants who use the Cloudian platform.

A storage policy is a set of rules that define how data can be managed and distributed within the organization. VMware Cloud Director Object Storage Extension offers a default storage policy. In addition, you can create custom storage policies if your tenants use the Cloudian platform. Tenants can then apply these policies when creating buckets and objects. Use storage policies to protect your data and to avoid data losses if any type of failure occurs. Storage policies make your data highly available.

Based on the number of data centers in your environment, different data protection methods are available to select from when creating the storage policy. In VMware Cloud Director Object Storage Extension, there are three distribution methods, also called distribution schemes.

- Replication

- Erasure Coding Across Data Centers
- Replicated Erasure Coding

Replication

Replication is the process in which data is copied to multiple locations. The system creates a configurable number of copies of each data object, and each copy is stored on a different node. There is no limitation of the data centers that can be used. Replication within a single data center or replication across multiple data centers are both supported, if the number of copies is not greater than the number of the nodes. When creating a replication storage policy, you should always specify at least two copies.

For example, with 4x replication, 4 copies of each object are created, and each copy is stored on a different node. This can be done within a single data center, or across multiple data centers.

Figure 9-1. Replication within a single data center

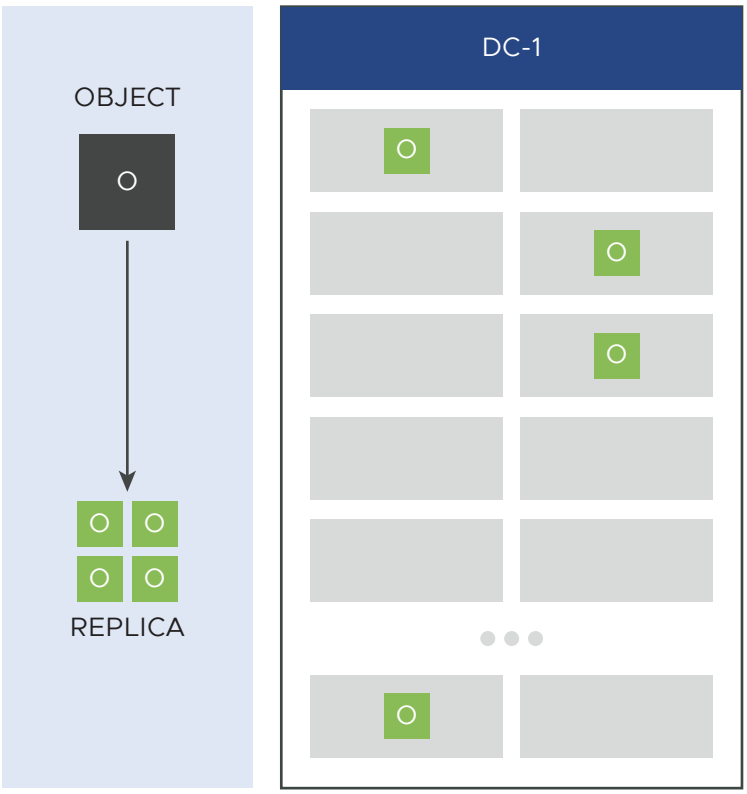


Figure 9-2. Replication across multiple data centers

Erasure Coding Across Data Centers

Erasure coding breaks data into a configurable number of data fragments, known as the "k" value, plus a configurable number of parity fragments - the "m" value. The fragments are distributed across a set of storage systems, with each fragment stored on a different node. Choosing the right configuration for you, depends on how many nodes you have in your data center. A minimum of three data centers and six nodes is required.

When you access an object, it is reassembled using the stored fragments. If a data or parity fragment is lost or corrupted, the object can be decoded from any "k" number of fragments and the object remains readable even if a "m" number of nodes are unavailable.

The diagram shows an object divided into eight fragments, each stored on a different node in three data centers.

Figure 9-3. Erasure coding across data centers

The following table lists the erasure coding "k" + "m" configuration that is currently supported by VMware Cloud Director Object Storage Extension 2.1.1.

Table 9-1. Erasure Coding Distribution Configuration

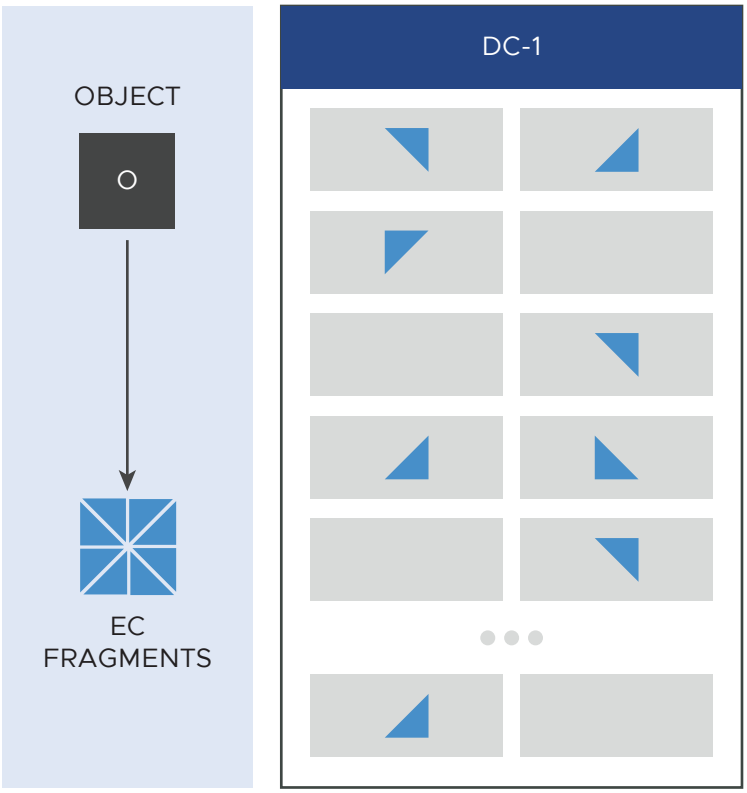
Number of participating data centers	Supported "k" + "m"	Fragments Distribution
3	5+4	3 fragments per DC
	7+5	4 fragments per DC
4	8+4	3 fragments per DC
5	6+4	2 fragments per DC
6	8+4	2 fragments per DC
	7+5	2 fragments per DC
7	10+4	2 fragments per DC
8	10+6	2 fragments per DC
9	10+8	2 fragments per DC

Replicated Erasure Coding

Replicated erasure coding is a distribution method that falls between the replication and erasure coding methods. The system creates copies, or replicas, of the data object. The number of copies must be equal to the number of data centers selected. Each copy is then broken into fragments, the same way the erasure coding method works, and the fragments are distributed within a single data center, or across multiple data centers.

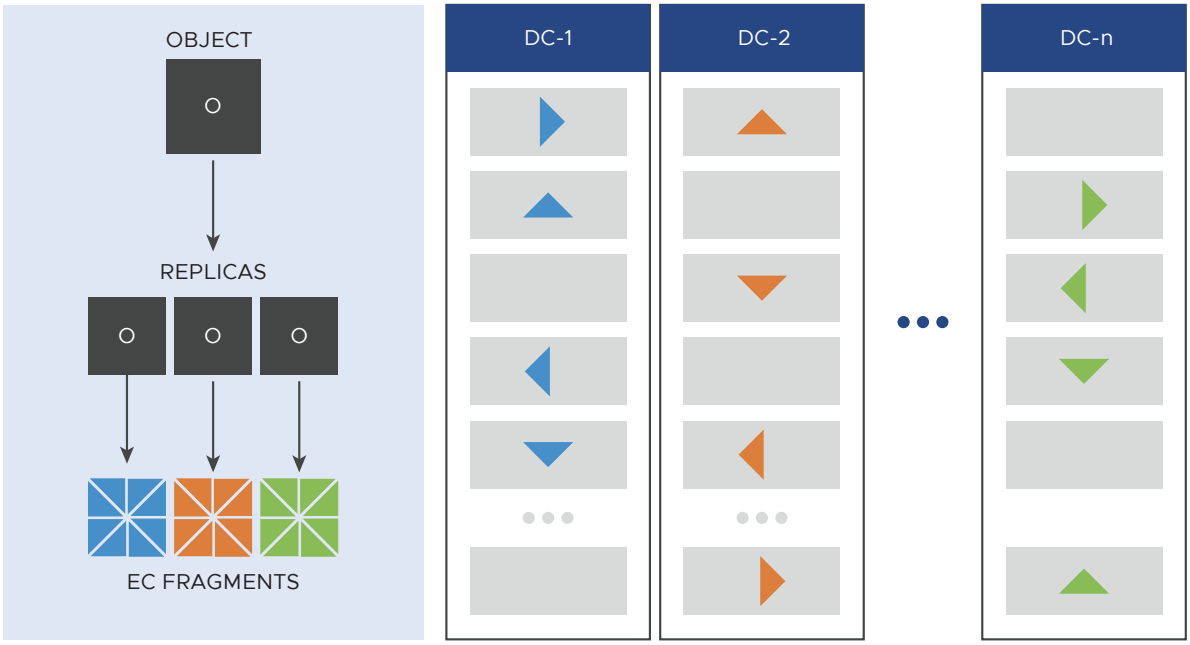
When you have only one data center available, the replicated erasure coding method works the same as erasure coding. The data object is split into fragments, which are then distributed within the data center, each on a separate node.

Figure 9-4. Replicated erasure coding within a single data center



When you select replicated erasure coding across multiple data centers as your preferred distribution method, copies of the data object are created first - three copies for three data centers. Each copy is then broken into fragments, which are then distributed across the data centers, each on a separate node.

Figure 9-5. Replicated erasure coding across multiple data centers



The following table lists the replicated erasure coding "k" + "m" configuration that is currently supported by VMware Cloud Director Object Storage Extension 2.1.1.

Table 9-2. Replicated Erasure Coding Distribution Configuration

Supported "k" + "m" configuration
4+2
6+2
8+2
9+3
12+4

Create a storage policy

You can create storage policies for tenants who use the Cloudian platform.

Prerequisites

- You can create storage policies for tenants who use the Cloudian platform only.
- The Cloudian HyperStore version must be 7.2.4.10+ or 7.3.1+.
- The Erasure Coding distribution scheme requires a minimum of 3 data centers and 6 nodes. Verify that your environment supports this configuration, if you want to use the Erasure Coding method.

Procedure

1 Log in to the VMware Cloud Director cloud provider admin portal.

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

3 Click **Tenants** and then **Storage Policies**.

4 Click **New Storage Policy**.

5 Enter a name for the storage policy.

6 Select the data centers that you want to use.

7 Select your preferred **Distribution Scheme**.

If you select...	You must...
Replication	1. Enter the **Replicas Count** - the count must not be larger than the total number of nodes available. 2. Select a **Datacenter Assignment** - this option decides how the replicas can be distributed across the data centers. 3. Click **Create**.
Replicated Erasure Coding	1. Select your preferred Erasure Coding "k"+"m" value configuration. 2. Click **Create**.
Erasure Coding	

Delete a storage policy

You can delete the Cloudian storage policies that you created.

Prerequisites

- You cannot delete a storage policy that is assigned to a tenant or a bucket.
- You cannot delete a storage policy that is currently used as a default system policy.

Procedure

1 Log in to the VMware Cloud Director cloud provider admin portal.

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

3 Click **Tenants** and then **Storage Policies**.

4 Click the ⋮ and then **Delete**.

5 Click **Delete** again.

Edit Roles

As a cloud provider, you can add rights to the predefined roles in VMware Cloud Director Object Storage Extension.

You can edit the predefined roles in VMware Cloud Director Object Storage Extension by adding rights. Each of the three predefined roles - provider administrator, tenant administrator and tenant user, has a default set of rights which cannot be deleted.

Procedure

1 Log in to the VMware Cloud Director cloud provider admin portal.

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

3 Navigate to **Settings** and click **Roles**.

4 Click the vertical ellipsis icon (⋮) next to the role that you want to edit. Click **Edit**.

5 Select the rights that you want to add.

6 Click **Save**.

Global Bucket Synchronization

Bucket synchronization ensures that all buckets are automatically updated.

Bucket synchronization ensures that all buckets are up to date and every object that gets uploaded through the platform, is visible in the UI. You can schedule a synchronization task at the organization level to reflect any recent changes made in the back end. You can also configure a bucket synchronization for multisite tenants only and sync buckets between associated sites that do not share the same data server or the same data base.

You can do an on-demand synchronization with the Sync Now option, or schedule a bucket synchronization at a specific point in time.

Bucket synchronization can be a resource intensive task. VMware Cloud Director Object Storage Extension offers the Scope and Threshold options to provide control over the resources. You can configure those options to optimize the synchronization task.

Configure Bucket Synchronization

You can configure a bucket synchronization for tenant organizations and for multisite tenants.

Prerequisites

Verify that the tenant organizations that you want to synchronize are active.

Procedure

1 Log in to the VMware Cloud Director cloud provider admin portal.

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

3 Navigate to **Tenants > Bucket Synchronization** and click **Configure**.

4 Click the toggle button to activate synchronization scheduling.

5 Enter **Sync Interval** and **Object** as required.

6 Select the **Tenant Scope** and click **Save**.

Edit Global Cross-Origin Resource Sharing Configuration

Cross-origin resource sharing (CORS) is a mechanism for client web applications loaded in one domain to interact with resources in a different domain.

By using the VMware Cloud Director Object Storage Extension user interface, you can edit the global CORS settings at the system level. Tenant users can set individual CORS rules at the bucket level.

By default, global CORS settings do not allow cross-origin S3 API requests. To manage CORS rules at the bucket level, deactivate the global settings or set an allowlist, then configure CORS rules by using the VMware Cloud Director Object Storage Extension tenant portal. See Working with Cross-Origin Resource Sharing Rules.

Procedure

1 Log in to the VMware Cloud Director cloud provider admin portal.

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

3 In the **Settings** tab, click **Edit**.

4 Select a CORS configuration and click **Save**.

There are three CORS configuration options.

Option	Description
Deactivate Global CORS	Cross-origin access to buckets depends on the CORS rules of the individual bucket.
Activate Global CORS with any Origin	Cross-origin access to buckets is allowed for all requests.
Activate Global CORS with Custom Origin Allowlist	Cross-origin access to buckets is allowed for requests from the origins that you specify. Access requests from other origins depend on the CORS rules of the individual bucket.

Change the Root Logging Level of VMware Cloud Director Object Storage Extension

To collect more troubleshooting information, you can change the root logging level of VMware Cloud Director Object Storage Extension to `debug`.

Important Setting the root logging level to `debug` causes the log capacity to fill faster.

Procedure

1 Open an SSH connection to the VMware Cloud Director Object Storage Extension machine.

2 Change the logging level to `debug`.

```
ose service restart --debug
```

Change the Public Network Port

By default, VMware Cloud Director Object Storage Extension is configured to use port 443 for external communication. You can change the public port by using the `ose` command-line utility.

Procedure

1 Open an SSH connection to the VMware Cloud Director Object Storage Extension machine.

2 Change the public network port to 8443.

```
ose args set --k=server.port --v=8443
```

3 Restart the VMware Cloud Director Object Storage Extension service.

```
ose service restart
```

Deactivate the SSL Certificate Validation for the S3 Service

For testing and development purposes, you can deactivate the SSL certificate validation that the VMware Cloud Director Object Storage Extension API performs.

The VMware Cloud Director tenant portal requires an SSL certificate validation. When the SSL certificate validation is inactive, you cannot access VMware Cloud Director Object Storage Extension by using the VMware Cloud Director tenant portal.

Procedure

1 Open an SSH connection to the VMware Cloud Director Object Storage Extension machine.

2 Restart the VMware Cloud Director Object Storage Extension service and deactivate the SSL certificate validation.

```
ose service restart --nossl
```

Generate a Support Bundle

To help diagnose problems, you might need to generate system and runtime information, and support bundle collections of log files.

The following table describes the contents of the support bundle:

Name	Description
`command.txt`	Text file with details about the support bundle. Contains start date, end date, and target directory for the support bundle, as defined during generation.
`config.txt`	Text file with configuration details. The system token, passwords, and the signature and fingerprint of the SSL certificate are excluded.
`log`	Directory that contains the following VMware Cloud Director Object Storage Extension logs: ■ VMware Cloud Director Object Storage Extension Keeper Service Logs ■ Access Logs ■ Default Logs ■ System Logs ■ Organization Unit (OU) Logs
`db`	Directory that contains the schema history and the hibernate sequence for the database.

Procedure

1 Open an SSH connection to the VMware Cloud Director Object Storage Extension machine.

2 To generate the support bundle, run the following command:

```
ose support --start start-date --end end-date
```

You can optionally append the `--start` and `--end` arguments.

The `--start` argument defines the start time for the logs to be collected. The default value is 2018-01-01.

The `--end` argument defines the end time for the logs to be collected. If not specified, the end date is the current date.

For the `--start` and the `--end` arguments values, enter the date in the YYYY-MM-DD format.

```
ose support --start 2020-03-12 --end 2020-05-24
```

Results

The support bundle is generated and saved to the `/opt/vmware/voss/support` directory of the VMware Cloud Director Object Storage Extension machine.