

VMware Cloud Director Object Storage Extension 2.1.1 Release Notes

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

Copyright © 2023 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

- 1** Introduction 4
- 2** What's New 5
- 3** Upgrade 6
- 4** Resolved Issues 7
- 5** Caveats and Limitations 8
- 6** Product Documentation 9
- 7** Known Issues 10

Introduction

1

VMware Cloud Director Object Storage Extension 2.1.1 | 24 FEB 2022 | Build 19362139

Check for additions and updates to these release notes.

What's New

2

VMware Cloud Director Object Storage Extension version 2.1.1 includes the following new features:

- **Object lock and object tagging for Dell ECS 3.6 users**

VMware Cloud Director Object Storage Extension 2.1.1 introduces new user mapping for tenants who use Dell ECS 3.6. VMware Cloud Director tenant users are now mapped to ECS Identity and Access Management (IAM) users and no longer to ECS object users.

You can upgrade user mapping with a single click in the cloud provider portal. The upgrade is optional.

The upgrade of user mapping allows you to use the object lock and object tagging features. The object lock feature protects an object version from accidental or malicious deletion. You activate the object lock and set a retention policy when you create a bucket. Object tagging allows users to categorize buckets by assigning tags to individual objects using key-value pairs.

- **Support for additional operating systems**

This release adds support for the following operating systems:

- Photon OS 3 and later
- Ubuntu 18 and later
- Debian 10 and later

For more information on how to install VMware Cloud Director Object Storage Extension, see [Installing and Configuring VMware Cloud Director Object Storage Extension](#).

Upgrade

3

You can upgrade directly to VMware Cloud Director Object Storage Extension 2.1.1 from versions 2.1 and 2.0. See [Upgrading VMware Cloud Director Object Storage Extension](#).

Resolved Issues

4

- **Restore from a vApp backup times out**

If the vApp backup contains NVRAM files, the restoring of the backup fails with a `Timed Out` error.

- **The usage of the S3 HEAD request method on a folder causes the service to fail with an error**

When a folder contains huge objects, repeated calls of the HEAD method on the folder leads to an `OutOfMemoryError`.

- **Sync Now option does not work when synchronizing buckets**

When objects or folders are uploaded through the S3 API, the changes are not showing up in VMware Cloud Director Object Storage Extension after clicking the Sync Now button.

Caveats and Limitations

5

- **If you are using ECS storage, S3 API, or the Find a Bucket feature, you cannot visit a bucket that belongs to a different tenant organization in the ECS platform.**
- **Bucket synchronization supports up to 10 million objects per a single synchronization job**
When the cloud provider enables bucket synchronization for a tenant in the provider portal, the synchronization can support up to 10 million objects for the tenant. VMware Cloud Director Object Storage Extension 2.1 does not support the synchronization for more than 10 million objects per a single bucket synchronization job.
- **VMware Cloud Director and the underlying storage systems have different limitations on user names. To use VMware Cloud Director Object Storage Extension, user names must comply with both the requirements of VMware Cloud Director and the underlying storage system. A best practice is to use short user names (under 50 bytes) and to use alphanumeric characters.**
 - If you are using Clouidian storage, the maximum length of user IDs is 255 bytes.
 - If you are using Dell ECS 3.4 or earlier, the maximum length of user IDs is 91 bytes.
 - If you are using Dell ECS 3.6, the maximum length of user IDs is 64 bytes.
- **S3 API requests authenticated with application credentials do not support the following use cases:**
 - Accessing a shared bucket if another user grants you permissions for the bucket.
 - Deleting multiple objects simultaneously with a single API request.
 - Copying objects from buckets that you own.

Product Documentation

6

All documentation is available on the [VMware Cloud Director Object Storage Extension Documentation](#) page.

Known Issues

7

- **You cannot log in to VMware Cloud Director Object Storage Extension as a service administrator**

When you try to log in to VMware Cloud Director Object Storage Extension as a service administrator, the login is unsuccessful. The problem is observed on a random basis and it occurs if you have multiple groups which are mapped to multiple VMware Cloud Director roles.

Workaround: Log in to VMware Cloud Director Object Storage Extension with a user that has a single group, mapped to their VMware Cloud Director role.

- **You cannot push images to the VMware Harbor Registry**

When you try to push an image to the VMware Harbor Registry and the VMware Harbor Registry server uses VMware Cloud Director Object Storage Extension S3 as a backend storage, the process fails. The problem is observed when VMware Harbor Registry is configured with VMware Cloud Director Object Storage Extension S3 endpoint and credentials.

Workaround: Request a hotfix from VMware.

- **Bucket synchronization does not synchronize all objects when object paths contain special symbols**

VMware Cloud Director Object Storage Extension synchronizes the first 1,000 objects to the database. Special symbols include characters that might be encoded in the URL.

Workaround: None.

- **You cannot create a bucket policy with a UI-generated service instance ID**

When you try to create a bucket policy and use the UI to generate the service instance ID, the process fails.

Workaround: Create the service instance ID manually and ensure it does not include the hyphen symbol (-) .

- **The S3 service of VMware Cloud Object Storage Extension is unavailable**

When you start or view VMware Cloud Object Storage Extension, the VMware Cloud Object Storage Extension service is active, but the S3 service is unavailable, with the following error message in the log file:

```
S3_TOKEN_AUTH_ERROR
```

The issue is observed if the time gap between the S3 client and the VMware Cloud Object Storage Extension VM is over 20 seconds.

Workaround 1: Change the gap time between the S3 client and the VMware Cloud Object Storage Extension VM to less than 20 seconds, for example, NTP for the VMware Cloud Object Storage Extension VM.

Workaround 2: Run the command `oss.s3.request-expire-time=3600` and restart the VMware Cloud Object Storage Extension service.

- **Object versioning does not work for the third party object storage integration with VMware Cloud Director by Object Storage Interoperability Service (OSIS)**

If the third party object storage system designs object version ID longer than 40 chars, the mapping to Object Storage Extension fails and object versioning cannot work.

Workaround: None.

- **The third party adapter for Object Storage Interoperability Service (OSIS) cannot run successfully**

If the third party object storage adapter for OSIS does not implement the API `/api/v1/console`, the OSIS adapter cannot run successfully.

Workaround: Implement `/api/v1/console` with a blank link.

- **Object count metrics on the bucket do not reflect the correct value**

When a tenant user uploads multiple objects to a bucket, the object count on the bucket properties displays a lower number than the actual number of objects.

Workaround: Click the **SYNC** button on the bucket.

- **You cannot unprotect a Kubernetes cluster which is disconnected from Object Storage Extension**

When a tenant administrator tries to unprotect a protected Kubernetes cluster, which is disconnected from Object Storage Extension, the operation fails.

Workaround 1: Re-connect the Kubernetes cluster to Object Storage Extension.

Workaround 2: Delete the relevant records in the Object Storage Extension database tables `external_cluster_info` and `cluster_protection_info`.

- **Third-party object storage platforms cannot be integrated with OSIS when S3 is configured with HTTPS**

When using a third-party object storage platform, which is integrated with OSIS (Object Storage Interoperability Service), the bucket creation fails due to the backend trust anchors error for SSL certificates.

Workaround: Configure third-party object storage S3 with HTTP or request a hotfix from VMware.

- **For DELL ECS platform, creating two buckets with the same name across two different tenants results in an overwriting of the existing bucket in the first tenant**

When you create a bucket with the same name across different tenants, the initial bucket is replicated along with the content of the bucket. This content can then be managed by all of these users.

Workaround: Request a hotfix upon 2.1.1.1 from VMware.

- **The Access Key and Secret Key pair is not displayed immediately after a tenant user logs in to VMware Cloud Director portal when using the DELL ECS platform**

When a tenant user onboards to VMware Object Storage Extension for the first time, the access key and secret key pair is not displayed immediately in the Security Credentials tab.

Workaround: When the user creates a bucket in the Buckets tab, the access key and the secret key pair is displayed.

- **Some tenant users cannot create buckets**

When using the ECS platform, some tenant users cannot create buckets if their corresponding IAM user in ECS has been removed manually by the ECS administrator.

Workaround: Remove the corresponding user records from the VMware Cloud Director Object Storage Extension database.

- **Tenant users that log in with OpenID Connect cannot make S3 API calls**

When tenant users log in to VMware Cloud Director with OpenID Connect and they have been assigned a "Defer to Identity Provider" global role in VMware Cloud Director, they cannot access the S3 API by using the Access Key and Secret Key from the Security Credentials.

Workaround: Make the S3 API calls to the underlying object storage clusters directly with the same Access Key and Secret Key.

- **Object lock feature does not work on Cloudian 7.4+**

You cannot use the object lock feature if you use Cloudian 7.4 or later.

Workaround: You can perform object lock operations in Cloudian S3 or in the Cloudian Management Console.

- **Tenant administrators cannot edit subordinate roles when they log in with OpenID Connect**

When tenant administrators log in to VMware Cloud Director with OpenID Connect and they have been assigned a "Defer to Identity Provider" global role in VMware Cloud Director, they cannot edit subordinate roles for other tenant users.

Workaround: Log in to VMware Cloud Director with another authentication method.

- **You cannot back up and restore Kubernetes clusters if you use Dell ECS**

If the backend is configured with DELL ECS, the Kubernetes cluster protection button in the tenant portal is inactive.

Workaround: Protect the cluster using the VMware Cloud Director Object Storage Extension API call.

- **Unable to add catalogs from VMware Cloud Director Object Storage Extension to VMware Cloud Director libraries for Cloud Director 10.3 and later**

When tenant users create a new catalog and click "Add to libraries" to upload an object, the import of the object fails.

Workaround: None

- **The Permissions and Lifecycle tabs in the tenant portal are not displayed**

Tenant users that are mapped to IAM of ECS 3.6 or later cannot view the Permissions and Lifecycle tabs in the VMware Cloud Director Object Storage Extensions tenant portal.

Workaround: None

- **Kubernetes clusters are not listed in VMware Cloud Director Object Storage Extension for Container Service Extension (CSE) 3.2 and later**

When a tenant administrator tries to back up a Kubernetes cluster for CSE 3.2 or later, the tenant cannot see the Kubernetes clusters list in VMware Cloud Director Object Storage Extension.

Workaround:

- a Go to the CSE UI plugin.
- b Select the Kubernetes cluster and download the kubeconfig file to your local system.
- c Go to **Object Storage > Kubernetes**.
- d Click **Add External Cluster Now**.
- e Enter a name for the cluster and select the kubeconfig file from your local system.

The cluster is now listed in the Kubernetes Clusters tab.

- **Synchronization tasks of buckets with more than 60 thousand objects fail with a timeout error**

When you try to sync a bucket that contains more than 60 thousand objects, the synchronization task expires after 24 hours.

Workaround: Click the Sync Now button repeatedly until the synchronization task completes successfully.