ORACLE

Accessing OCI Object Storage with Pre-authenticated Links

December 2023, Version 1.0

Public

ORACLE

Purpose Statement

This paper provides guidance for navigating essential tasks within Oracle Cloud Infrastructure (OCI). Specifically, it provides step-by-step instructions for creating an Object Storage bucket, uploading a sample object to the bucket, and creating a pre-authenticated link for easy access to that object. Intended for developers and technical professionals who want practical information without the need for extensive coding, the paper provides users the knowledge and tools necessary to efficiently use these features within the OCI environment to facilitate effective data storage, retrieval, and access for various applications.

Disclaimer

ORACLE

Table of Contents

Introduction

This technical paper documents the key learnings from an immersive workshop focused on Oracle Cloud Infrastructure (OCI) Object Storage. This workshop delves into fundamental tasks essential for effective data management within OCI, providing practical insights for developers and technical professionals.

OCI Object Storage is a robust and scalable storage solution designed for internet-scale applications, offering high-performance capabilities while ensuring reliable and cost-efficient data durability. This service can store an unlimited amount of unstructured data, accommodating diverse content types such as analytic data, images, and videos.

Unlike traditional storage solutions, OCI Object Storage lets users securely store and retrieve data directly from the internet or within the cloud platform. Its regional nature ensures accessibility from anywhere, both within and outside the OCI context. Additionally, Object Storage provides multiple management interfaces, simplifying the process of storage management at scale.

Pre-authenticated requests provide a mechanism in Object Storage to allow access to a bucket or object without requiring the user to possess their own credentials. Access to the specified bucket or object persists as long as the initiator of the request holds the necessary permissions for resource access. For example, it allows an operations support user to upload backups to a bucket, or a business partner to retrieve quarterly financial reports from a bucket, all without possessing API keys.

When a pre-authenticated request is created, a distinctive web URL (link) is generated. Anyone who has this link can access the Object Storage resources outlined in the pre-authenticated request by using standard HTTP tools such as `curl` and `wget`.

This paper explores the following key objectives:

- **Create an Object Storage bucket**, which is a foundational component for organizing and managing data in Object Storage.
- **Upload a sample object** to the bucket, which provides insights into effective data transfer and storage practices in the Object Storage environment.
- **Create a pre-authenticated link** to access the object, which is a valuable feature for secure and convenient access to stored objects within Object Storage.

This paper is based on an Oracle LiveLabs workshop that covers certain aspects of OCI's Object Storage offerings and addresses limited offerings by Oracle. The details of the LiveLabs workshops are covered in the "Getting Started Resources" section of this paper.

Scope and Constraints for Pre-authenticated Requests

Before you perform the tasks in this paper, you should understand the following scope and limitations related to pre-authenticated requests:

- You can generate an unlimited number of pre-authenticated requests.
- A pre-authenticated request, when created for all objects within a bucket, allows users to upload an unrestricted quantity of objects to that specific bucket.
- An expiration date is required for each request, with no constraints on how far into the future you can set it.
- You can't edit an existing pre-authenticated request. If user access preferences or object listing changes are required, you must create another pre-authenticated request.

- By default, pre-authenticated requests for a bucket or objects with a prefix don't permit object listing. You must explicitly enable object listing when you create a pre-authenticated request.
- If a pre-authenticated request specifies a name prefix, users can perform `GET` and `PUT` actions only on objects with the specified prefix. Attempts to perform a `GET` or `PUT` action an object without the specified prefix or with a different prefix fail.
- The target and actions of a pre-authenticated request are determined by the creator's permissions, and changes to those permissions can affect the pre-authenticated request. However, the request is *not* tied to the creator's account login credentials. Therefore, changes to the creator's login credentials don't impact a pre-authenticated request.
- Deleting a pre-authenticated request ends user access to the associated bucket or object.
- Pre-authenticated requests don't give users the ability to delete buckets or objects.
- You can't delete a bucket or an object in a bucket that has pre-authenticated request associated with it.

To get started, you need access to an Oracle Cloud Infrastructure (OCI) tenancy. If you don't have an OCI tenancy created already, set one up by using the instructions in Get an Oracle.com Account.

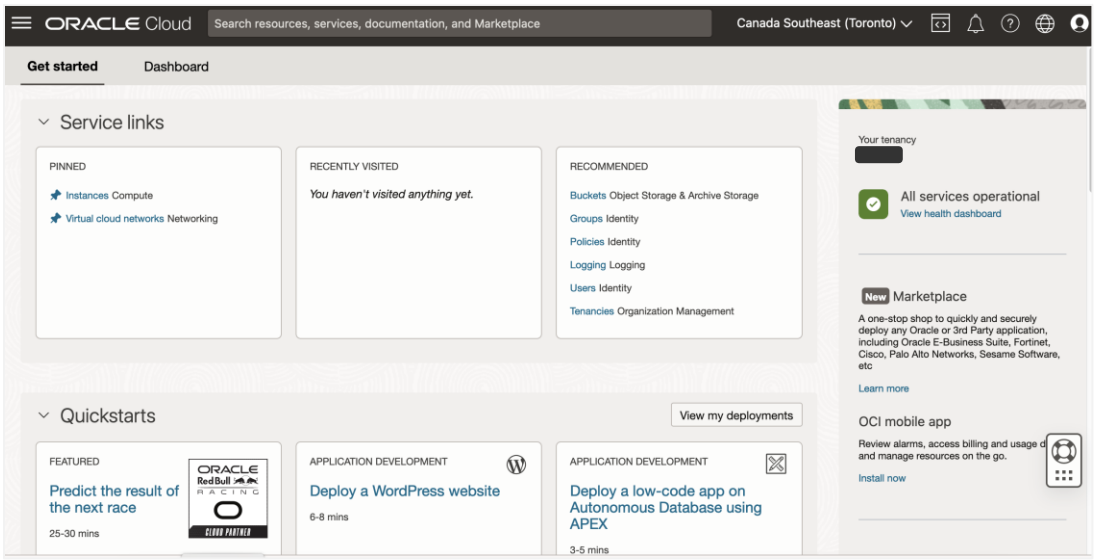
Alternatively, you can register on Oracle LiveLabs to access the Create an Object Storage Service workshop.

Access Object Storage and Create a Bucket

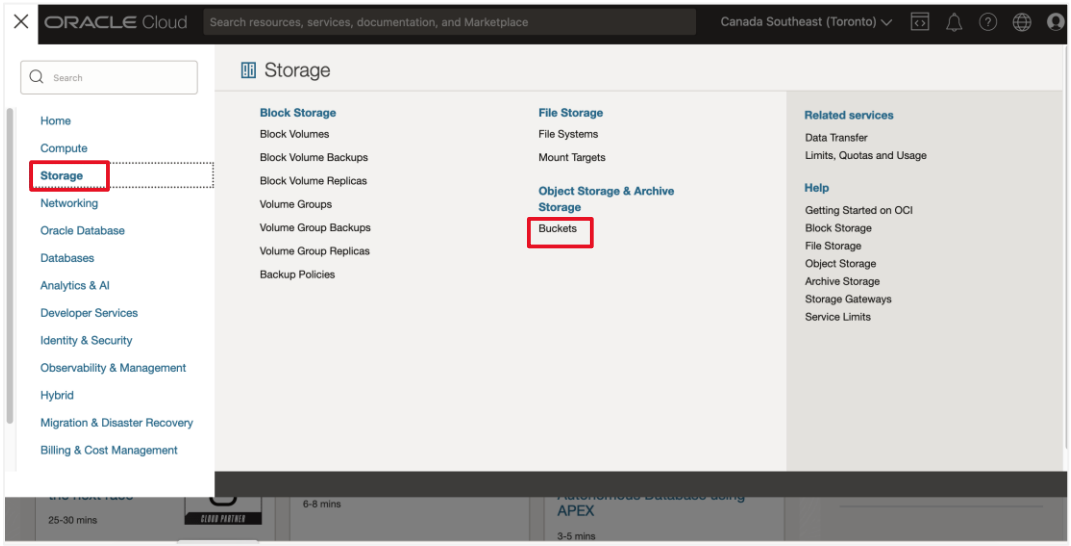
Sign in to OCI and create an Object Storage bucket.

1. Sign into the Oracle Cloud Console by using your cloud username and password, or the credentials provided in the Oracle LiveLabs workshop.

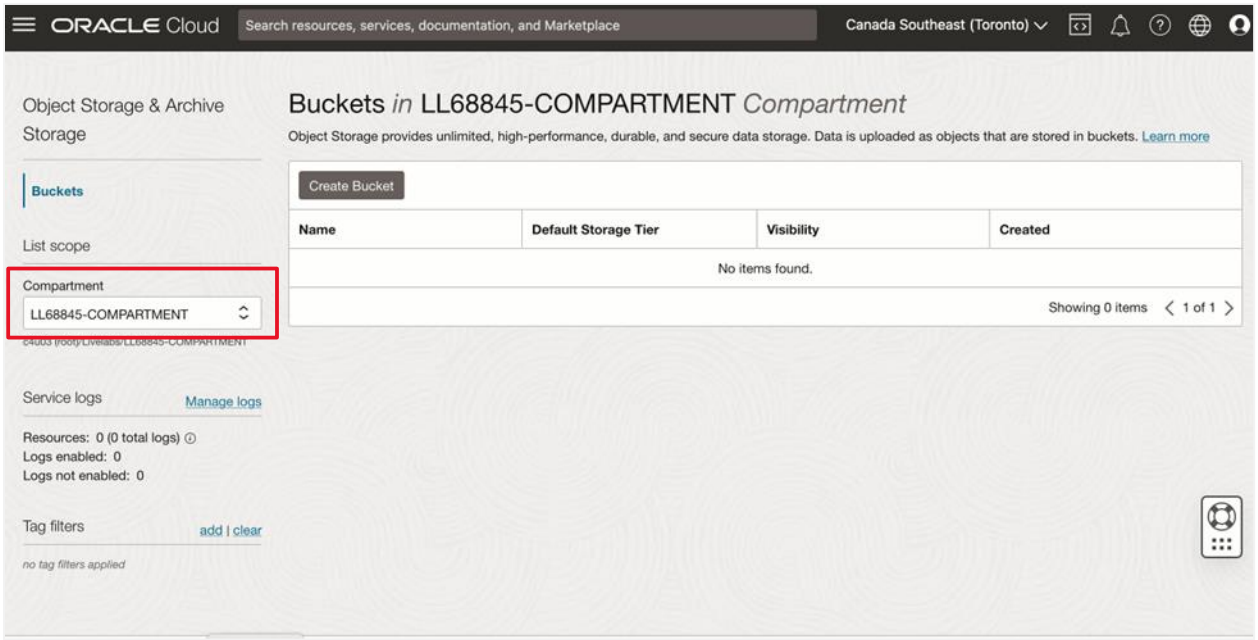
   The home page of the Console is displayed.



2. Click the navigation menu in the upper-left corner, select **Storage**, and then select **Buckets**.



The **Buckets** list page for the current compartment is displayed.



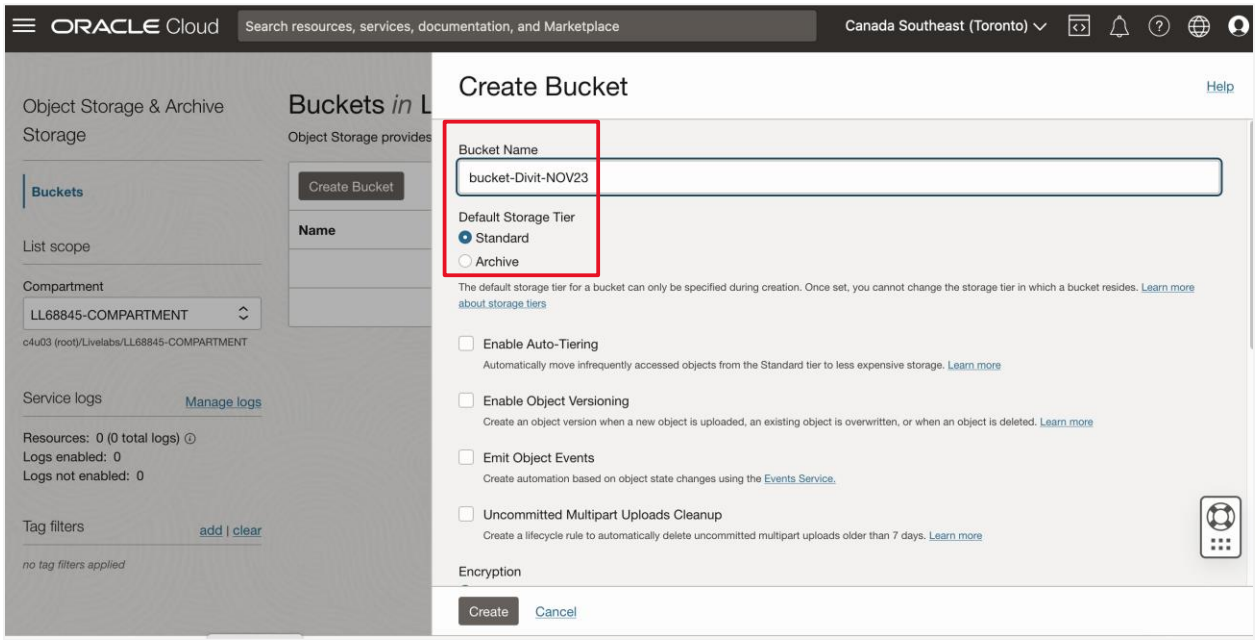
3. Ensure that you're in the compartment in which you want to create the bucket.

   You can view the compartment on the left-hand side of the page, under **List scope**.

   - If you're using the LiveLabs workshop, you can get your compartment ID from the login information page.
   - If you're not using LiveLabs workshop and have your own tenancy, select the compartment that you want to use from the list. The list displays all the compartments in the tenancy to which you have access.

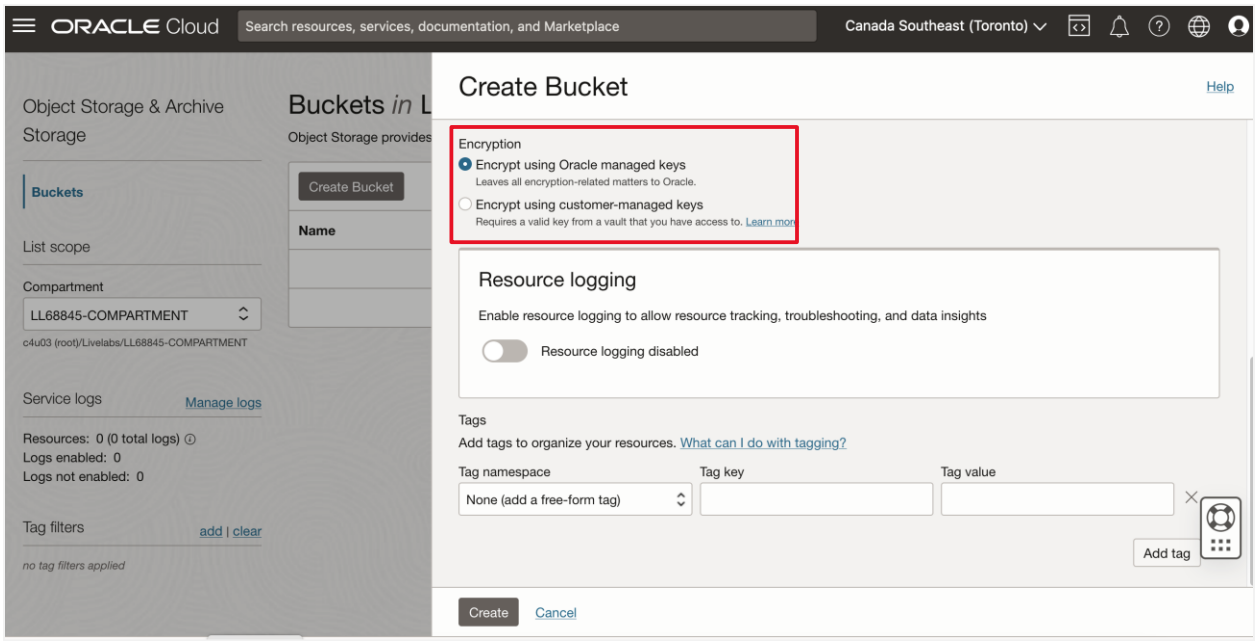
4. Click **Create Bucket**.

5. In the **Create Bucket** panel, specify the following details for the bucket:
   - **Bucket Name**: Enter a name for the storage bucket.
   - **Default Storage Tier**: Select **Standard**.



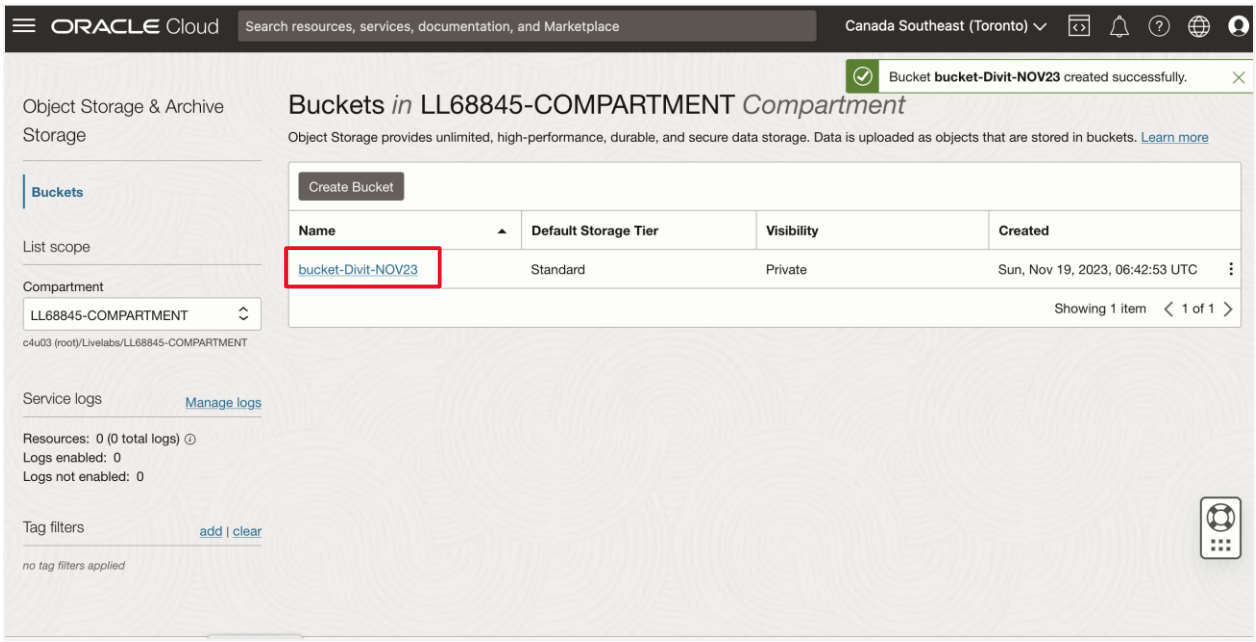
Under **Encryption**, you can select to have Oracle manage the encryption keys for you, or you can manage the keys by yourself. In this example, we're letting Oracle manage the keys for us.

6. Select **Encrypt using Oracle managed keys**.



7. Click **Create**.

   The bucket is created and is listed on the **Buckets** list page.



Upload an Object and Create a Pre-authenticated Link

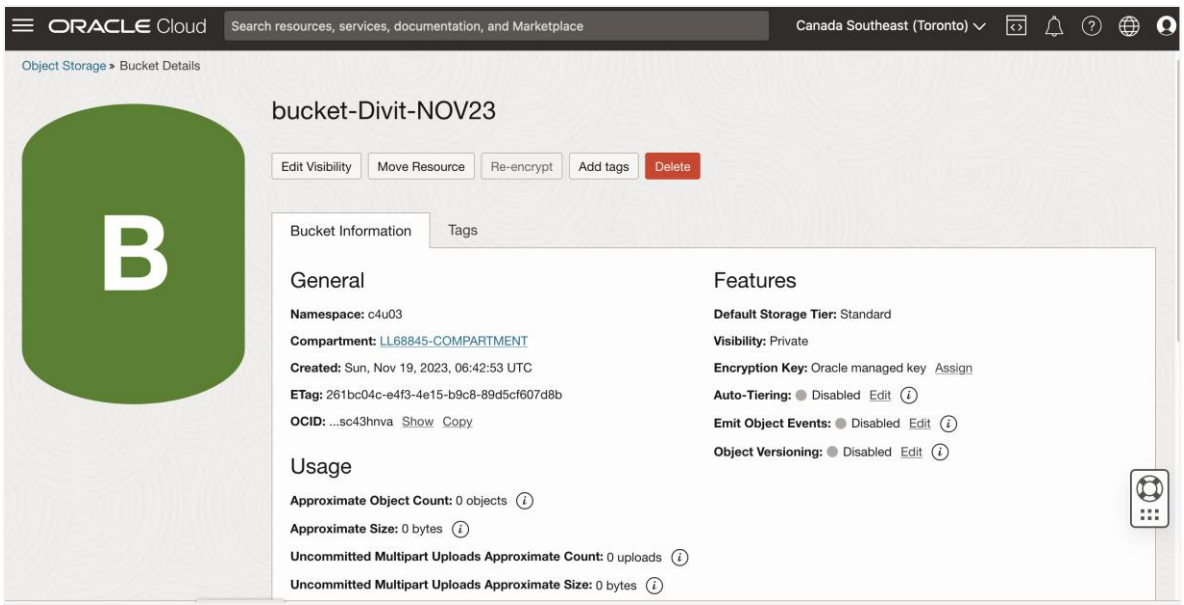
Now upload a sample object to the storage bucket, and request a pre-authenticated link to access it.

1. If you're using the LiveLabs workshop, download a *sample text file* to upload to the bucket that you created in the previous section. (You might need to right-click the link or page and select the "save as" option to download the `.txt` file.)

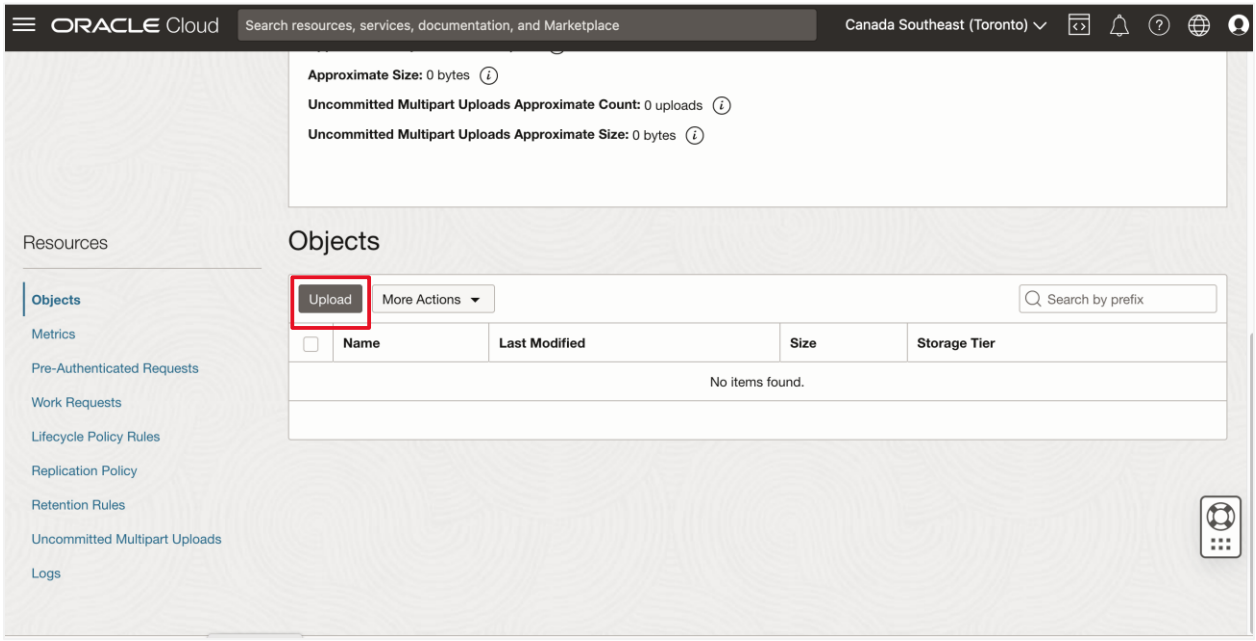
   Alternatively, you can choose to use any sample text file for the upload.

2. On the **Buckets** list page in the Oracle Cloud Console, click the name of the bucket that you created.

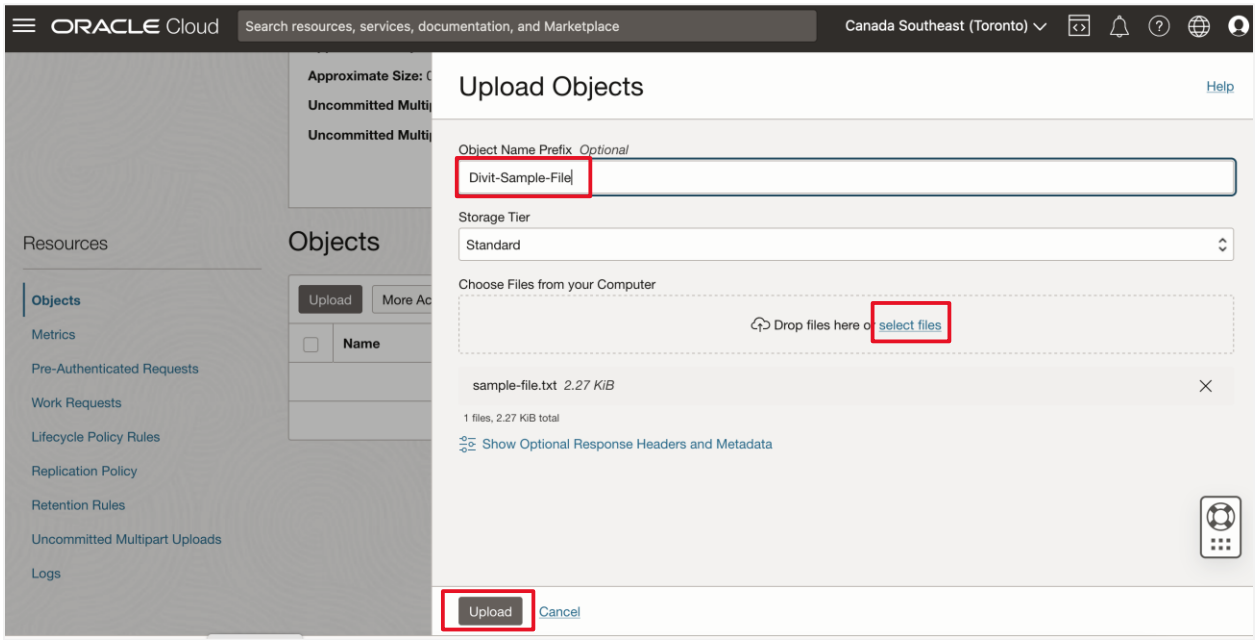
   The bucket details page is displayed.



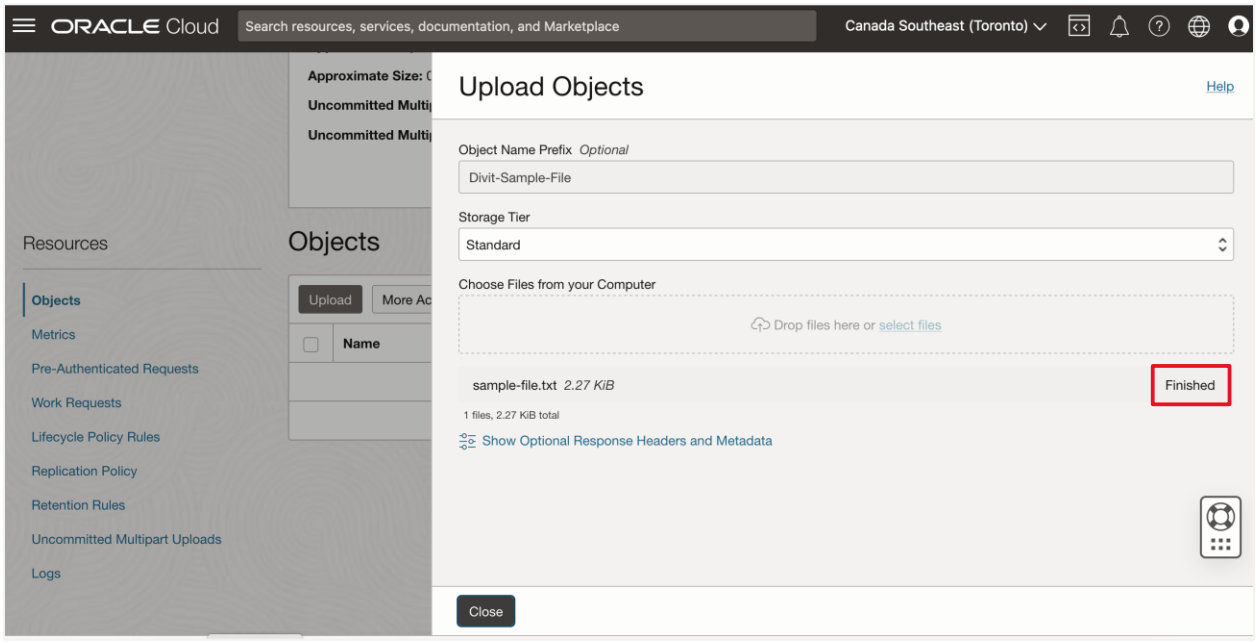
3. Under **Objects**, click **Upload**.



4. Click **select files** and select the `sample-file.txt` that you just downloaded or another sample text file that you want to use. Optionally, you can enter a name prefix for the objects that you upload. Then, click **Upload**.

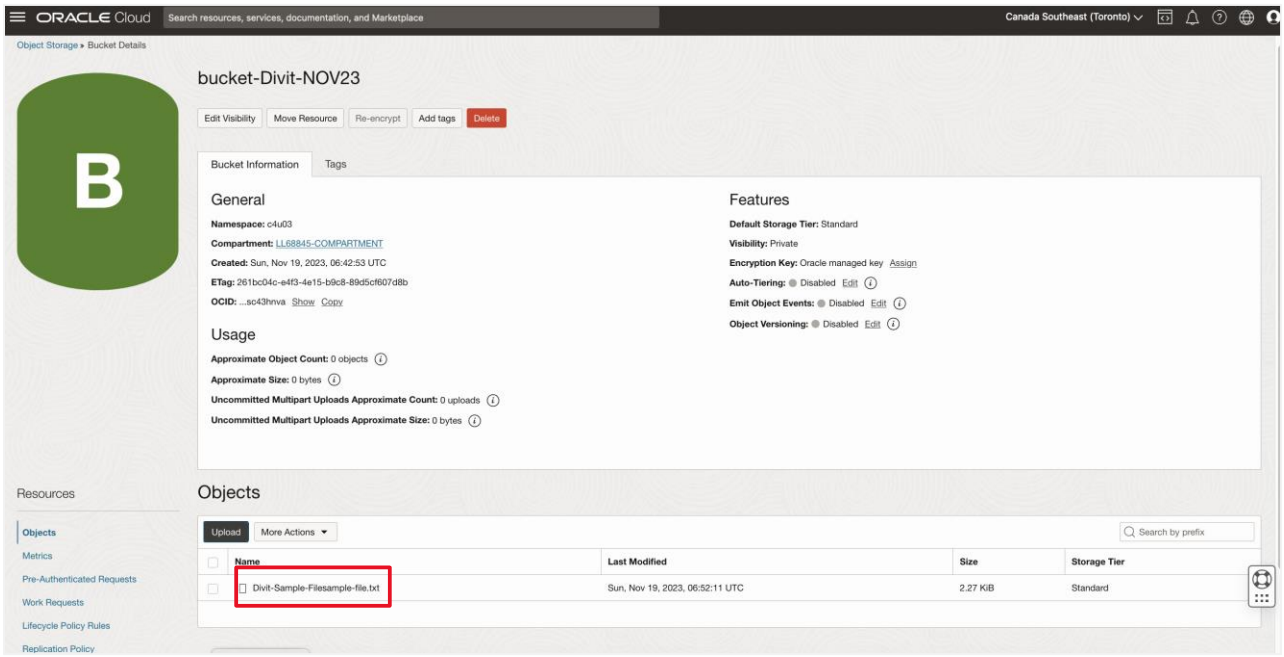


After the file is uploaded, its status is shown as **Finished**.

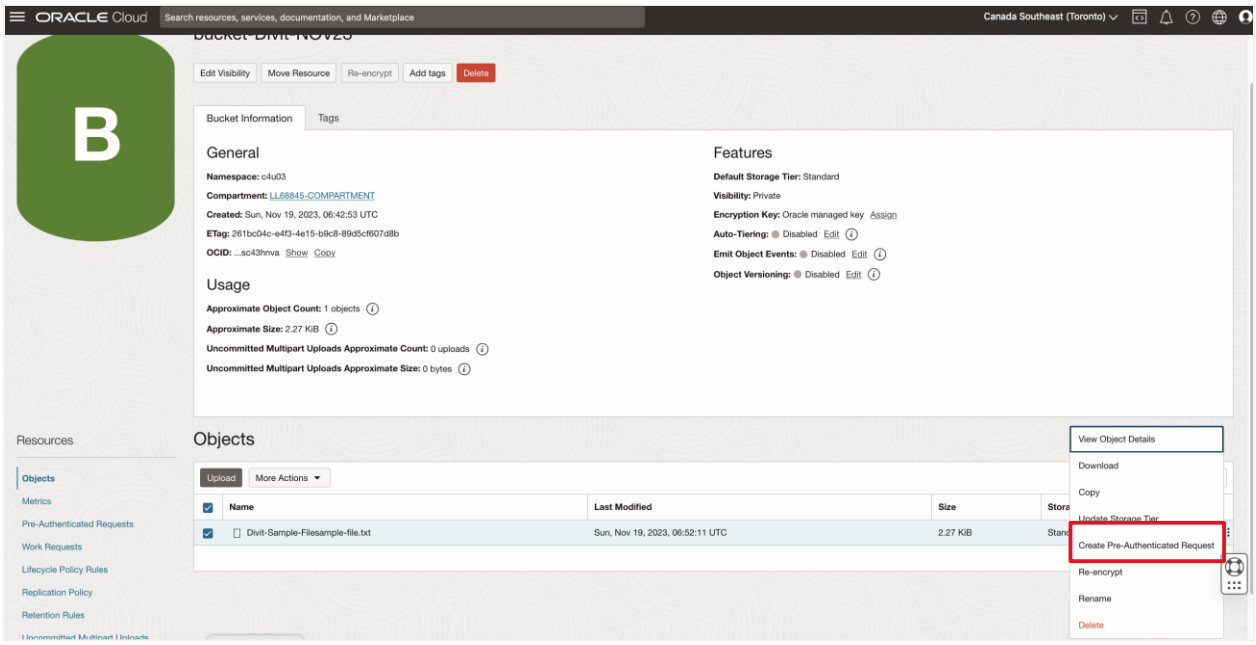


5. Click **Close**.

The file is listed under **Objects** in the bucket details page. If you chose to enter a prefix for the object names, that prefix is added to the file name.

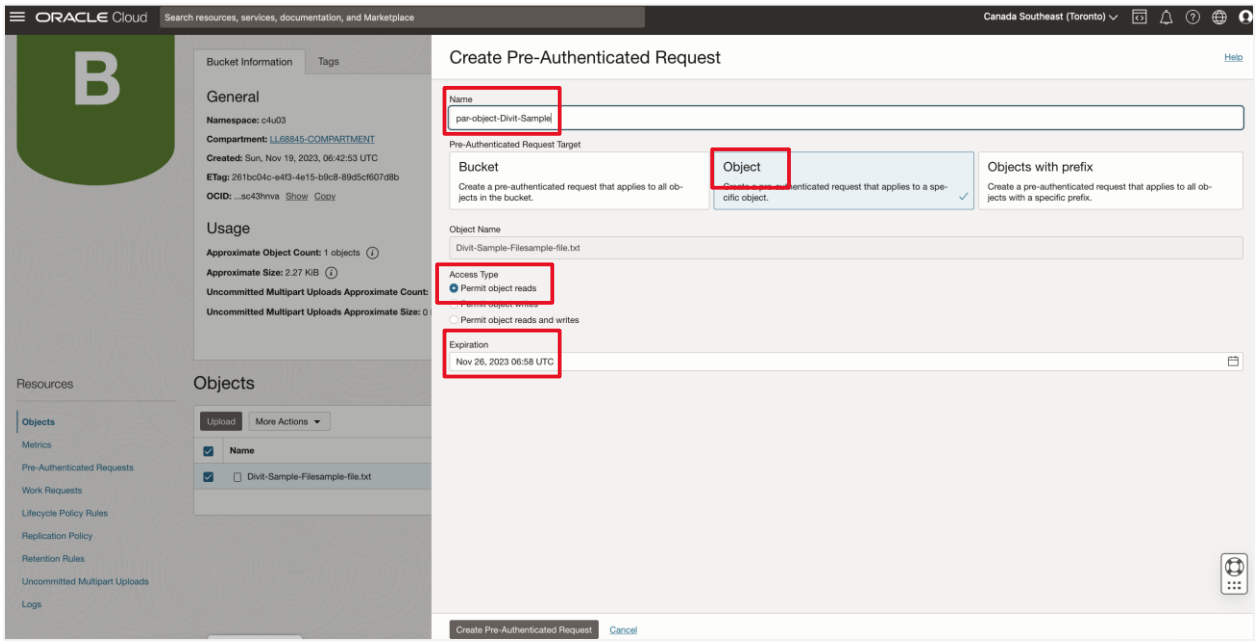


6. To create a web link that can be used to access the object without requiring any additional authentication, click the Actions menu to the right side of the object name, and select **Create Pre-Authenticated Request**.



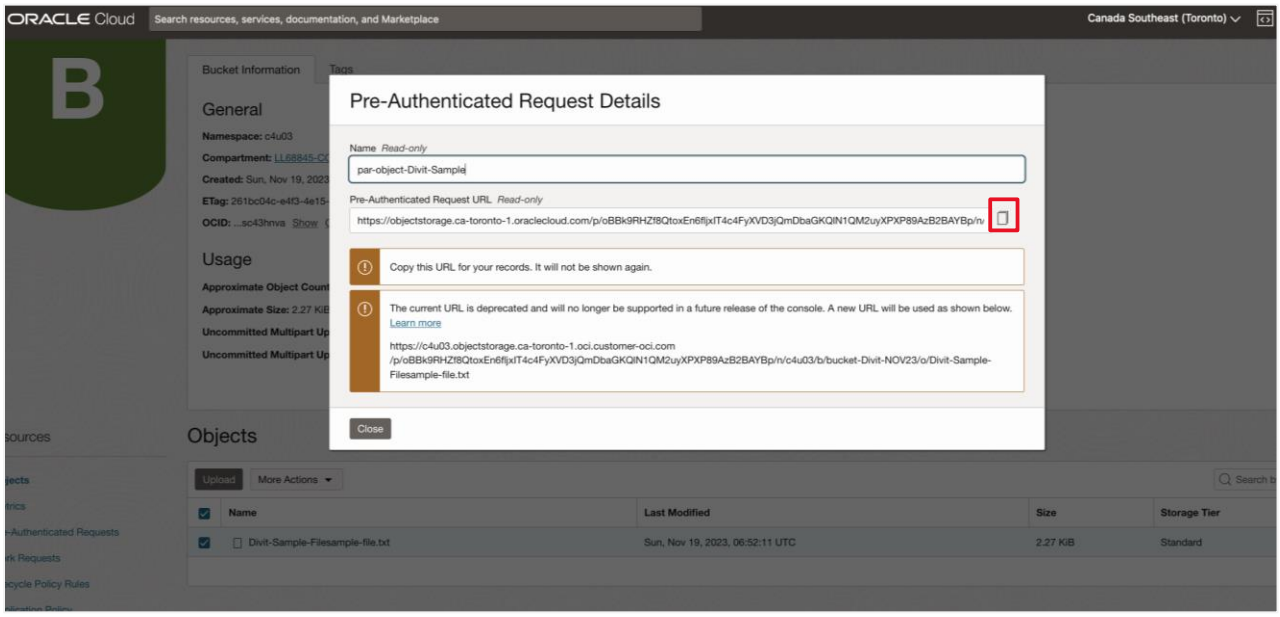
7. In the **Create Pre-Authenticated Request** panel, specify the following values:

- **Name**: Enter a descriptive name for the request.
- **Pre-Authenticated Request Target**: Select **Object**.
- **Access Type**: Select **Permit object reads**.
- **Expiration**: Enter an expiration date for the pre-authenticated link, or accept the default date.



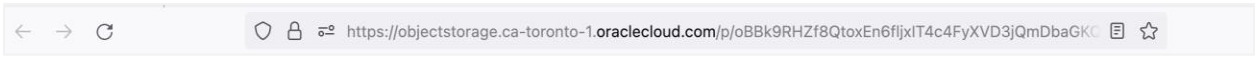
8. Click **Create Pre-Authenticated Request**.

   The request is created, and the request details dialog box is displayed.



9. Click the **Copy** icon to the right of the URL to copy the link. You must copy and save the link before closing the dialog box. The link can't be retrieved again.
10. After you copy the link, click **Close**.
11. Open a new browser window and paste the pre-authenticated link into the address bar.

    Because the sample file is a text file, it opens in a browser page.



Getting Started Resources

See the following resources to get started with OCI Object Storage.

General

- Product page
- Documentation

LiveLab workshop

- Create an Object Storage Service

Create an account on OCI: Get an Oracle.com Account

ORACLE

Conclusion

The Oracle Cloud Infrastructure (OCI) Object Storage service is an expansive, high-performance storage platform designed for internet-scale operations, ensuring both reliability and cost-effective data durability. This service has the capacity to store an unlimited volume of unstructured data, accommodating various content types, including analytical data and rich media such as images and videos. An innovative feature of Object Storage is the implementation of pre-authenticated requests, which provide users with access to a bucket or object without needing their own credentials. As long as the request creator retains permissions for resource access, users maintain uninterrupted access to the specified bucket or object. This feature enhances security and convenience in managing storage resources within the Object Storage service.

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle

Accessing OCI Object Storage with Pre-authenticated Links
Author: Divit Gupta