ORACLE

Configuring ZFS Storage for Cloud Snapshot Backups to OCI Object Store

Configuration Best Practices

July, 2020 | Version 3.0

DISCLAIMER

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

TABLE OF CONTENTS

INTRODUCTION

The Oracle ZFS Storage Appliance provides the ability to migrate data to Oracle Cloud Infrastructure (OCI) object storage either locally on premise or to OCI object storage.

Object storage is the primary method of storing large amounts of data in the cloud. With a flat namespace, it scales better than file system storage and supports extended metadata attributes that allow comprehensive search operations. Billions of objects can be stored when needed.

Cloud Snapshot Backups

The cloud snapshot backup feature of the Oracle ZFS Storage Appliance allows you to back up full and incremental snapshots from a local Oracle ZFS Storage Appliance to an object store target on another ZFS Storage Appliance as well as to cloud targets associated with an Oracle Cloud Infrastructure account. You can decide which snapshots are backed up to another appliance or to an actual cloud target.

OCI-Compatible Object Store On-Premise

The Oracle ZFS Storage Appliance also provides an OCI-compatible object storage that enables you to send cloud snapshots to local object storage on another ZFS Storage Appliance.

- Consistent OCI object store experience for OCI application testing and local storage
- Can apply ZFS data services and replication when storing cloud snapshots as objects on-premise
- Cloud snapshot backups are stored as objects in OCI cloud object storage and cannot be spun up or accessed over NFS or SMB

Use Cases

- Provides low-cost storage for snapshot backups
    - Snapshot backups can be scheduled through workflow
    - Provides recovery by restoring snapshots and rolling back
    - Provides recovery from accidental overwrite or malware like ransomware
- Provides archive storage for long-term data, such as business compliance requirements
- Provides tertiary backup storage on-premise
    - Cloud snapshots scheduled and stored in on-premise object storage
    - Not intended as complete DR solution
    - Snapshot of RMAN image copy supports database recovery

Advantages

Review the following advantages for storing or migrating data in a hybrid cloud environment with the ZFS Storage Appliance:

- Provides native cloud integration with OCI object storage
- Cloud snapshot backups are fully supported in the ZFS Appliance BUI, CLI, and REST interfaces and integrated with Analytics, alerts, logs, and authorization roles
- File system snapshots can be backed up to another on-premise ZFS Appliance or directly to OCI object storage
- Snapshot backups can be encrypted and compressed and if required, replicated to worldwide on-premise data centers

OVERVIEW

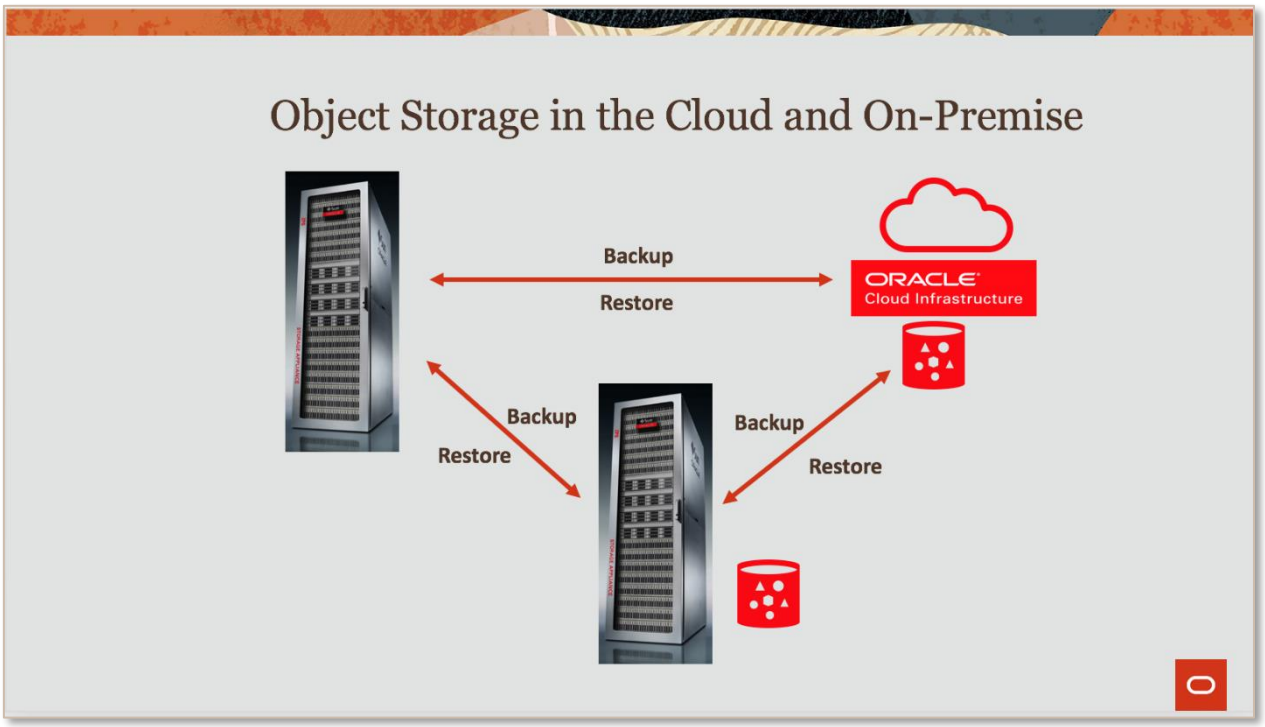
This document describes the following step-by-step instructions:

- Configuring a ZFSSA node as a cloud snapshot backup source system
- Configuring a second ZFSSSA node as an OCI target to receive a ZFS snapshot from the source ZFSSA node. Steps for storing on premise data encrypted and compressed are also provided.
- Deduplication on the ZFSSA target node can be enabled if the system supports deduplication. However, deduplication is generally recommended for full backups and you must consider the impact to critical workloads. If the primary workload of the ZFSSA target node is an object storage repository and performance is not a critical factor, you might consider enabling deduplication if it is supported.
- Configuring an OCI cloud target for archiving cloud snapshot backups
- Sending a ZFS cloud snapshot backup to OCI-compatible object storage

The source ZFS Storage node is defined as the host for data in the form of filesystems and LUNs from which a snapshot can be generated and subsequently pushed to the target:

- Target ZFS Storage node is defined as the recipient of snapshots sent from the source ZFS Storage node
- Source ZFS Storage node can send snapshots to OCI object storage (cloud)
- Source ZFSSA node sees the target ZFSSA node as an OCI bucket

The following is a context diagram of the environment.



The ZFS Appliance on the left takes on the role of the source from which shares and LUNs can be exposed to clients. The source can initiate a snapshot and then send that snapshot to the target ZFS Appliance, which is another node[1] over a defined network.

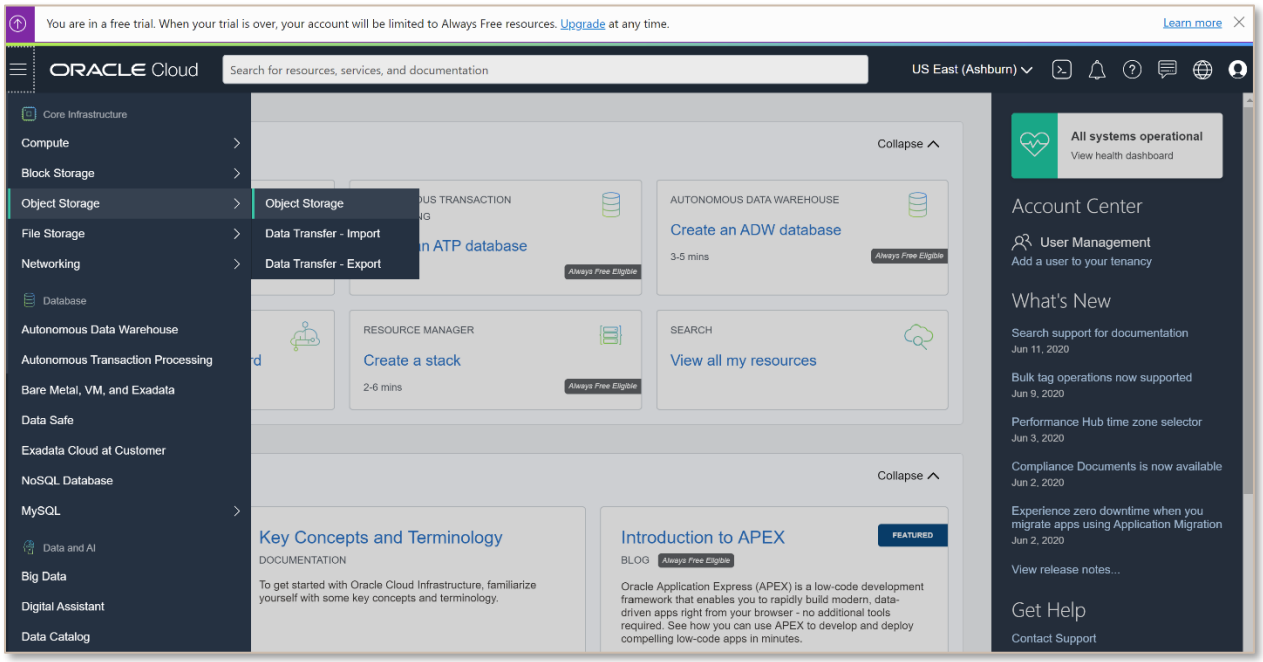
[1] This node may be a member of the ZFSSA cluster or could be a completed different ZFSSA.

ORACLE CLOUD INFRASTRUCTURE (OCI) OBJECT STORAGE

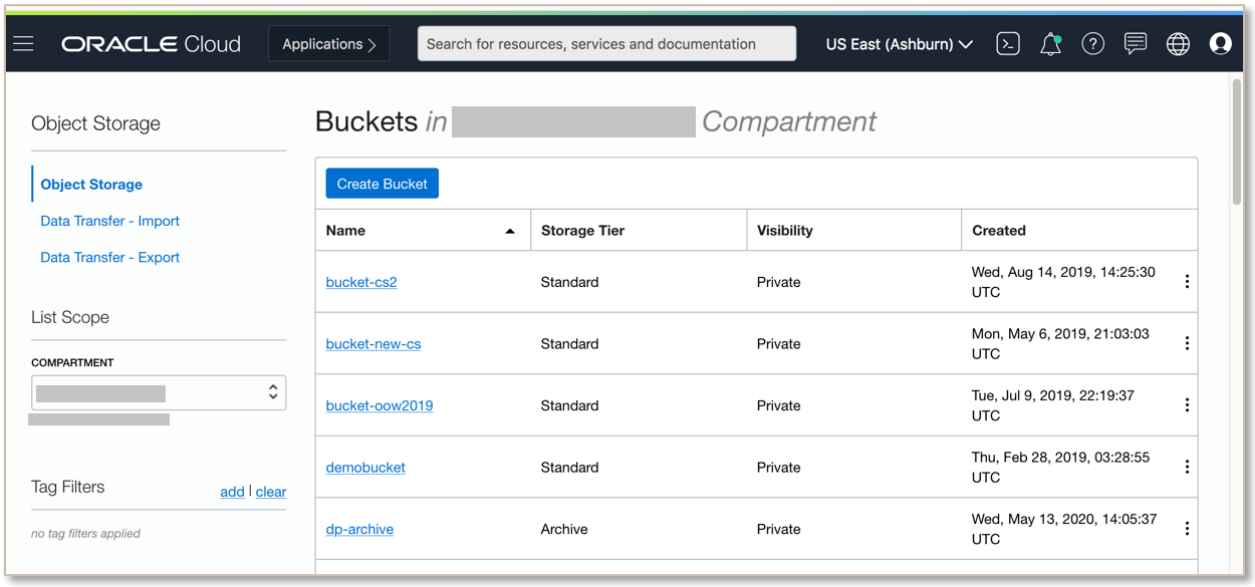
OCI provides a low-cost solution for data archival that integrates with on-premise ZFS Storage Appliance. OCI object storage provides both standard and archive tiers. When stored in either storage tier, data is encrypted automatically and cannot be disabled. Multiple cloud regions are available and data can be migrated between geographic regions.

Sign up for a free 30-day cloud trial to start an on-premise data migration to OCI object storage: https://www.oracle.com/cloud/free/

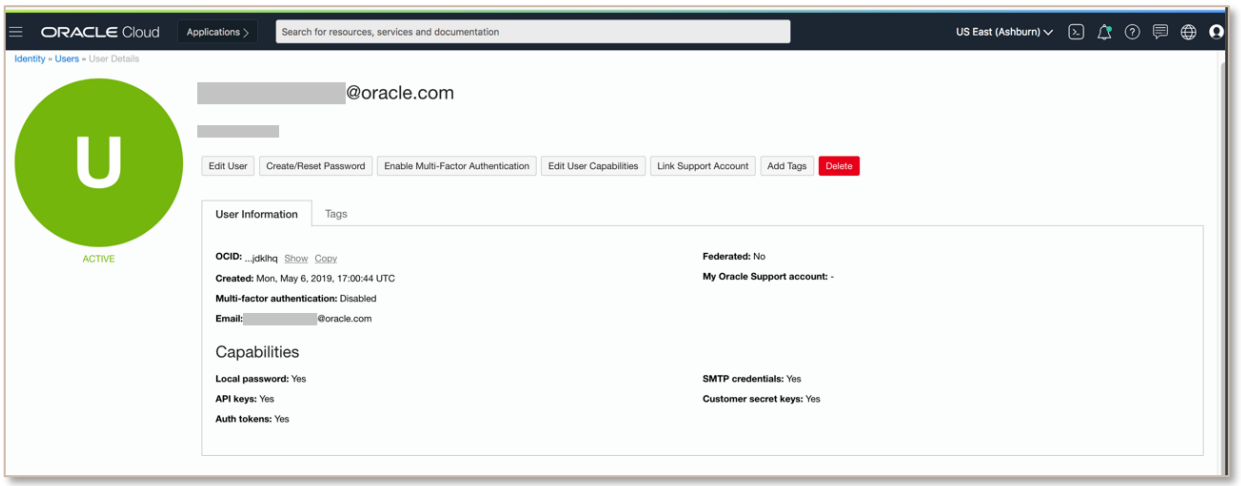
OCI provides the following management interfaces into all cloud components, including Object Storage. Select Object Storage from left panel under Oracle Cloud.



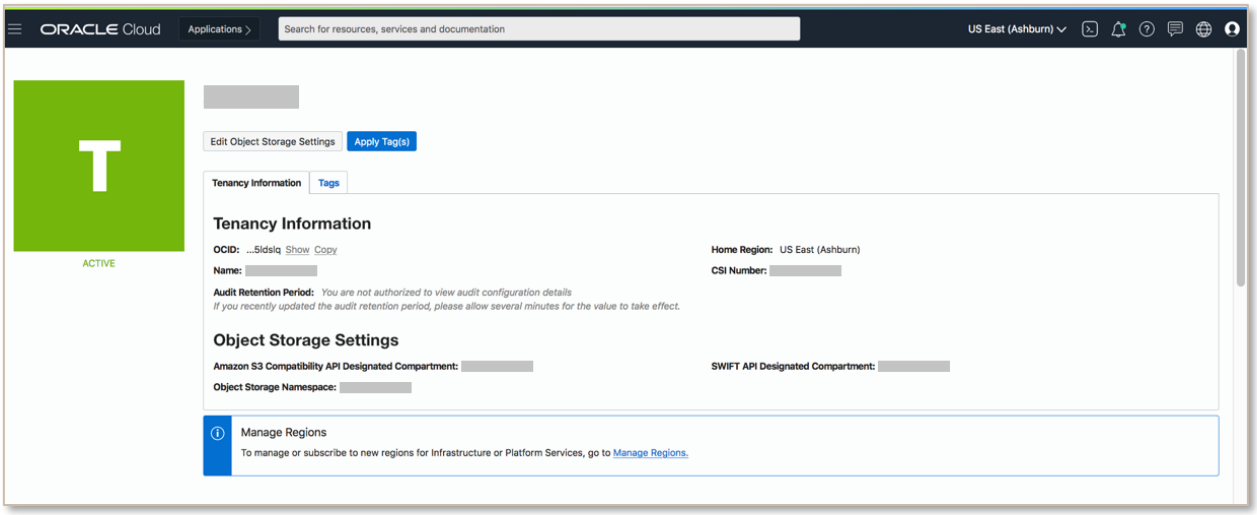
The OCI Object Storage interface provides a management view of your object storage tenancy and current compartment. Cloud storage buckets are created to store your data and can be reviewed accordingly. More options are available to provide cloud bucket details.



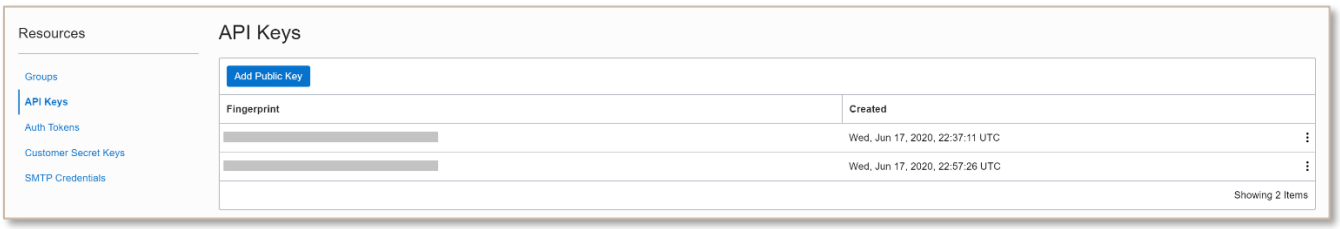
OCI Object Storage User profile screen includes user certificates that are created when the account is created. The OCID of the user is required when the cloud bucket target is created on the ZFS Storage Appliance.



Each OCI tenant is assigned one unique and uneditable Object Storage namespace that spans all compartments within a region. This is the OCI Tenancy screen that identifies the tenancy ID that was created when you create your OCI account. The tenancy OCID is required when the cloud bucket target is created on the on-premise ZFS Storage Appliance.



The public key (oci_api_key_public.pem) generated during OCI CLI installation needs to be uploaded in the OCI Object Storage User profile screen to grant the user access for CLI management. The fingerprint generated by the public key is required to modify and view objects on the ZFS Storage Appliance.



Summary Steps for OCI Cloud Object Storage Free Trial

» Review the summary steps below to set up your free OCI cloud storage trial. For information about OCI command line setup, see Part I: CLI Installation and Certificate Creation.
» Setup cloud account
» Sign into your account after it is activated
» Note the limitations of the object storage trial at the top of the screen
» Review user profile and tenancy information
» Select Object Storage from left menu under Oracle Cloud
» Select the (root) storage compartment that is created automatically in your tenancy
» Create a bucket with auto-generated name or give it a new name, if you prefer
    » Select standard tier
    » Oracle encryptions key
» From your local system, download and install OCI command line interface
    » From user profile screen, copy the certificates
    » Set up .oci config file
» Display the empty bucket with the OCI command line
» Do a test file migration with the OCI command line

GENERAL OVERVIEW

A summary of the configuration steps are as follows:

- **Part I: CLI installation and Certification Creation**
  - Install CLI
  - Create certificates
  - Generate fingerprint for the certificate
  - Create configuration file
- **Part II: ZFS Storage Appliance (both) – OCI Account Creation**
  - Create OCI account on both target and source
- **Part III: Local System and ZFS Storage Appliance (target) – OCI Target Creation**
  - Create encrypted project and share with compression enabled for the target destination
  - Create the target and bucket
  - List the bucket
- **Part IV: ZFS Storage Appliance (source) – OCI Cloud Service and Target Configuration**
  - Enable cloud service
  - Configure HTTP service
  - Create OCI-compatible target
- **Part V: ZFS Storage Appliance (both source and target) – Cloud Snapshot Backup and Restore**
  - Create a snapshot
  - Backup snapshot to on-premise ZFS Storage
  - Display the bucket content
  - Create second snapshot and send incremental backup to on-premise ZFS Storage
- **Part VI: Monitor Cloud Snapshot Backups and Object Store Bucket**
- **Part VII: Cloud Snapshot Backups Roles and Authorizations**
- **Part VIII: Automation and Customization Tips**
  - OCI command line simplification
  - Workflow installation and automation

Review the following components that are described in this document:

Component Description	Shortened Name	Purpose
Local system or laptop	local	Required to install and use the oci command line.
ZFS Storage Appliance #1	source appliance	ZFS Storage Appliance that is the source of the cloud snapshot backup
ZFS Storage Appliance #2	target appliance	ZFS Storage appliance that provides the OCI-compatible object storage target that is the destination of the cloud snapshot backups

PART I: CLI INSTALLATION AND CERTIFICATE CREATION

The detailed configuration steps are covered in subsequent numbered list items of this document.

1. **On the local system, install the CLI.**

   Specific configuration steps and visibility into the OCI-compatible object store must be completed with the OCI command interface that are installed on a local system like a server or laptop.

   The oci command line interface is installed on a local system, running at least python version 3.5+. The local system can be either Linux, Windows, or Mac. The CLI can be downloaded manually or using an installer script. Depending on your network configuration, you might need to set the following parameter to successfully download this interface: "export https_proxy=https://www-proxy.us.oracle.com:80"

   Once the environment variable has been defined as required, select one of the installation methods below.

   a) **Install CLI with installer script method.**

   ```
   local# bash -c "$(curl -L https://raw.githubusercontent.com/oracle/oci-cli/master/scripts/install/install.sh)"
   ```

   b) **Install CLI with manual method.**

   The manual process will use curl to download the install script after which, the installer is run with the options noted.

   ```
   local# curl -L -O https://raw.githubusercontent.com/oracle/oci-cli/master/scripts/install/install.sh
   local# ./install.sh --accept-all-defaults
   ```

2. **On the local system, create public and private keys (oci_api_key.pem and oci_api_key_public.pem).**

   - If you have a free cloud trial account set up and you want to create an OCI cloud target on a ZFS Storage Appliance, you would use the certificates that are accessible from the user profile section of your cloud account.
   - If you are creating an OCI-compatible object store target on a ZFS Storage Appliance, you will need to create the certificates as described below.

   Recall that PEM is a X.509 certificate (whose structure is defined using ASN.1), encoded using the ASN.1 DER (distinguished encoding rules), then run through Base64 encoding and stuck between plain-text anchor lines (BEGIN CERTIFICATE and END CERTIFICATE). The example below is in the context of the root account. Note that any account may be used although the default location of the bin, lib, and other support directories are relative to the account creating the certificates.

   - To generate the private and public keys, see this link: https://docs.cloud.oracle.com/iaas/Content/API/Concepts/apisigningkey.htm#How
   - General info can be found here.

   Steps:

   a) Change to the /root directory.
      - `local# cd /root`

   b) Create the .oci directory.
      - `local# mkdir .oci`

   c) Generate the private key with or without passphrase.
      - `local# openssl genrsa -out /root/.oci/oci_api_key.pem -aes128 2048`
      - `local# openssl genrsa -out /root/.oci/oci_api_key.pem 2048`

   d) Reduce permissions on the private key.
      - `local# chmod go-rwx /root/.oci/oci_api_key.pem`

   e) Generate the public key.

- local# **openssl rsa -pubout -in /root/.oci/oci_api_key.pem -out /root/.oci/oci_api_key_public.pem**

3. **On the local system, generate a fingerprint of the private key.**

```
local# openssl rsa -pubout -outform DER -in /root/.oci/oci_api_key.pem | openssl md5 -c
Enter pass phrase for /root/.oci/oci_api_key.pem:
writing RSA key
(stdin)= your-fingerprint
```

4. **On the local system, create the configuration file that will be used to create the target and will also be referenced in oci commands to monitor cloud snapshot backup information stored in the target.**

5. Using the information from the above steps, create .oci/config file similar to the following:

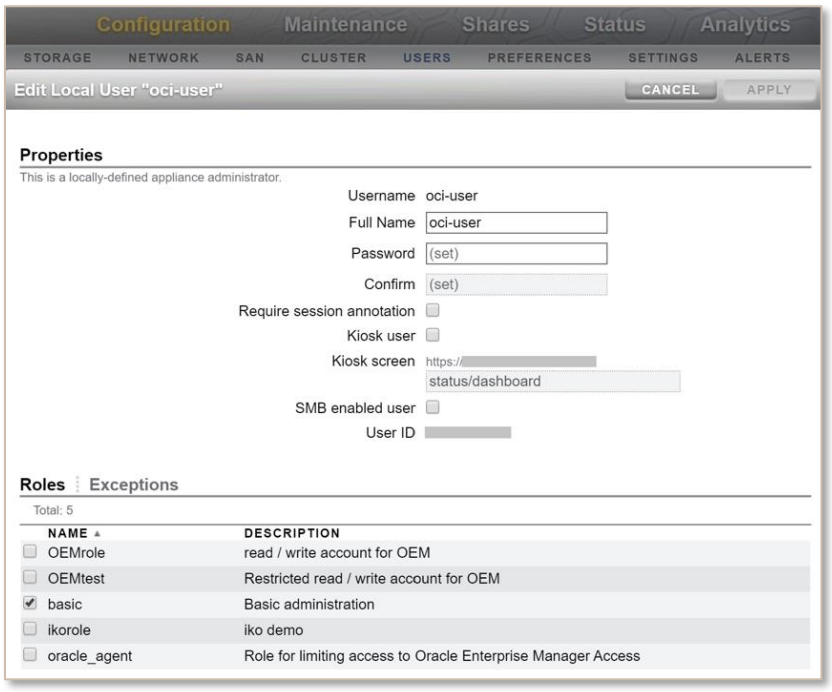
```
[DEFAULT]
user=user-OCID
fingerprint=your-fingerprint
key_file=/root/.oci/oci_api_key.pem
tenancy=tenancy-OCID
region=us-ashburn-1
```

For information on customizing the config file so that using the oci command line can be simplified, see Part VIII: Automation and Customization Tips.

PART II: ZFS STORAGE APPLIANCE (BOTH) – OCI ACCOUNT CREATION

1. **On the source appliance, create the oci-user account with the basic admin role.**
   - Go to Configuration→Users to create your oci-user account with selected “basic” role.

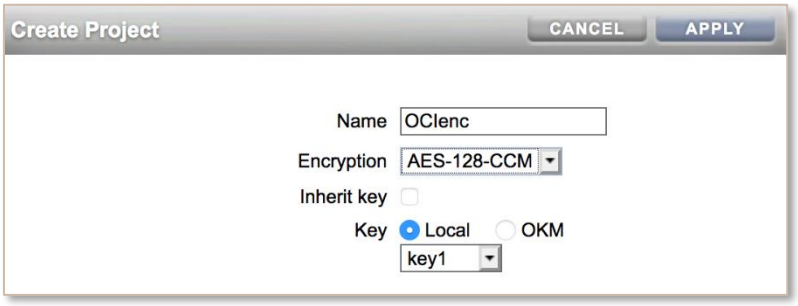
2. **On the target appliance, create the oci-user account with the basic admin role.**
   - Go to Configuration→Users to create your oci-user account with selected “basic” role.



PART III: LOCAL SYSTEM AND ZFS STORAGE APPLIANCE (TARGET) – OCI TARGET CREATION

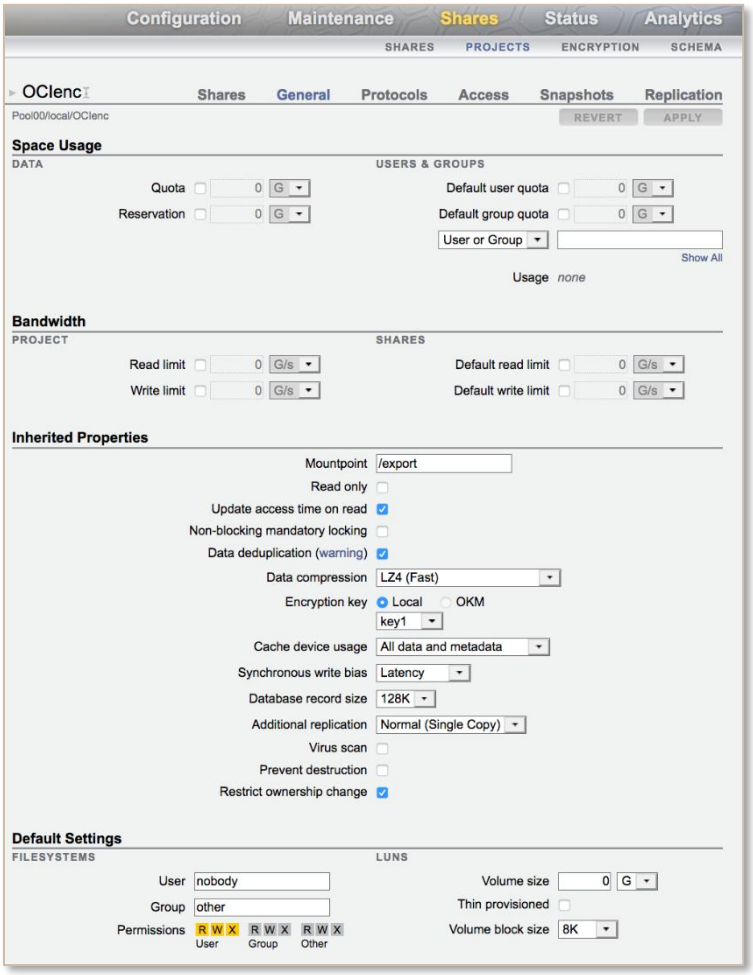
1. **On the target appliance, create an encrypted project for the share that will become the OCI-compatible object storage target.**

   The default encryption algorithm is AES-128-CCM. This provides strong encryption with good performance.

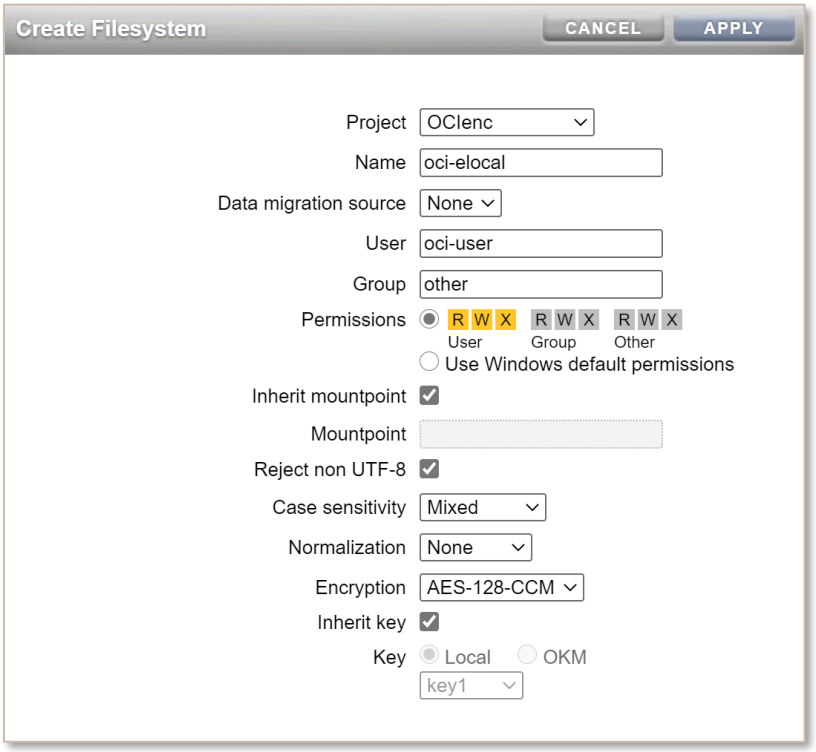


2. **On the target appliance, modify the default project "General" settings so that the share will be both encrypted and compressed. If the target appliance supports deduplication, you might consider testing it. In general, deduplication is only recommended for full backups.**

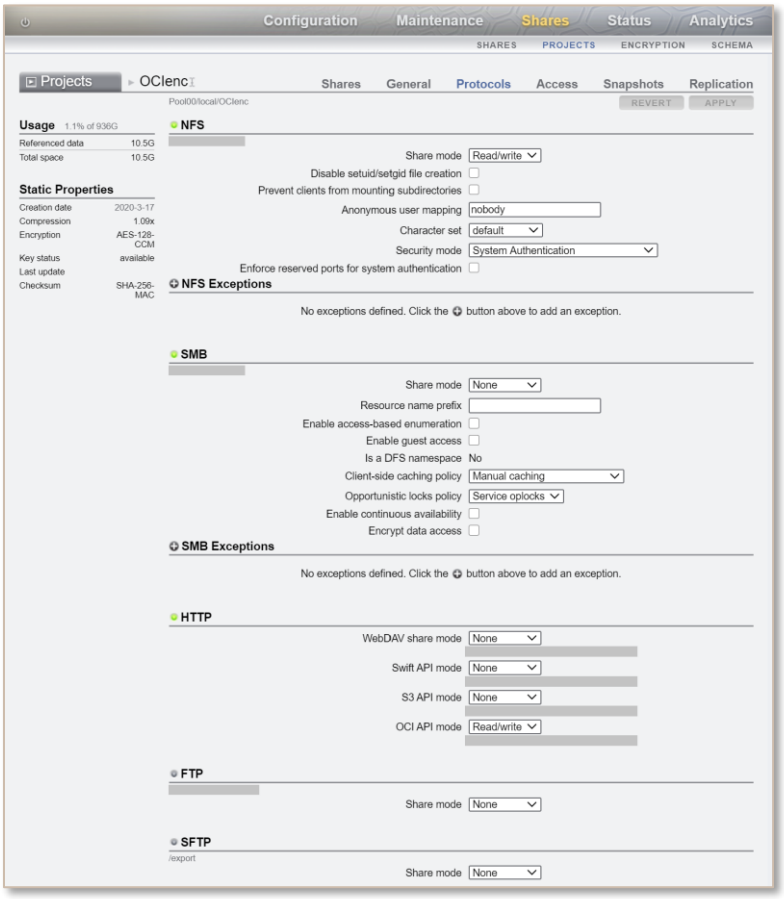
   - Select Data deduplication (optional)
   - Select Data compression: LZ4 (optional but recommended)



3. **On the target appliance, create the share that will become OCI-compatible object storage target. For example, oci-elocal.**
   a) From the OCI-enc project screen, select + Filesystems to create the share.
      i. Name the object storage target (i.e. oci-elocal)
      ii. Select user access (i.e. oci-user)



4. **On the target appliance, modify the default project "Protocols" settings to enable the share's OCI API mode.**
   - Select OCI API mode: Read/write



5. **Create the actual bucket for either the target system or for an OCI cloud target.**

   a) On the local system, use syntax similar to the following for the target system:

   ```
   local# oci os bucket create --endpoint "http://ZFSSA-name-or-IP/oci" -ns
   "export/oci-elocal" --config-file /root/.oci/config --name bucket --compartment-id
   export/oci-elocal
   ```

   b) On the local system, use syntax similar to the following to create an OCI cloud target:

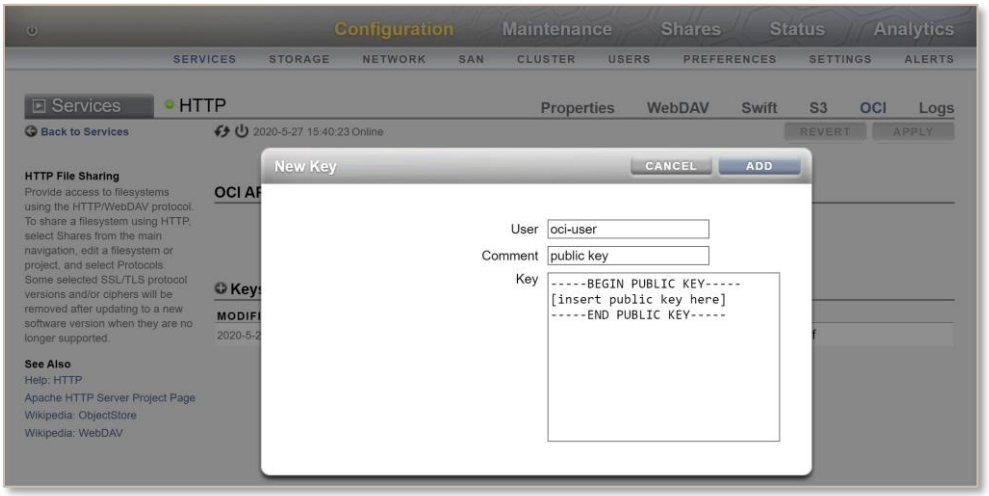
   ```
   local# oci os bucket create --endpoint "https://objectstorage.us-ashburn-
   1.oraclecloud.com" -ns "my-ns" --config-file /root/.oci/config --name cloudbucket --
   compartment-id export/oci-elocal
   ```

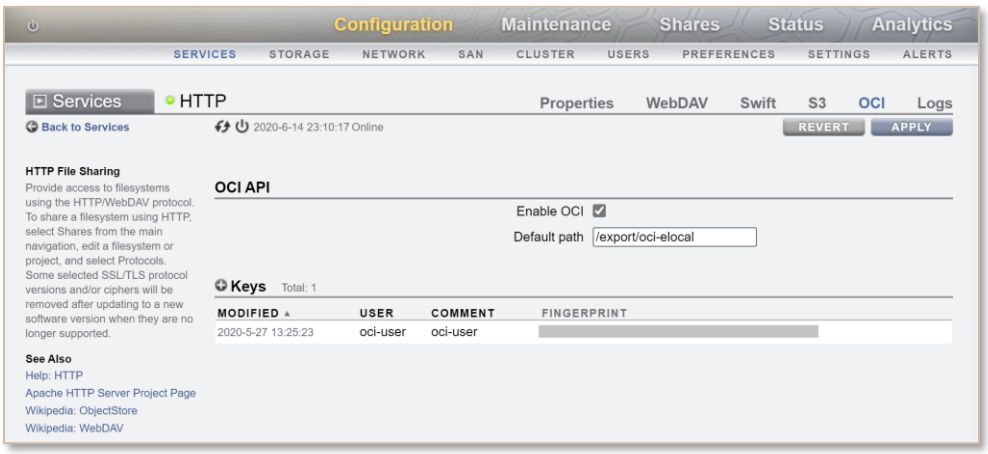
   For information about creating the config file, see Part VIII: Automation and Customization Tips.

6. **On the local system, list the bucket to confirm the bucket creation.**

   ```
   local# oci os object list -ns export/oci-elocal -bn bucket --endpoint http://ZFSSA-
   name-or-IP/oci
   ```

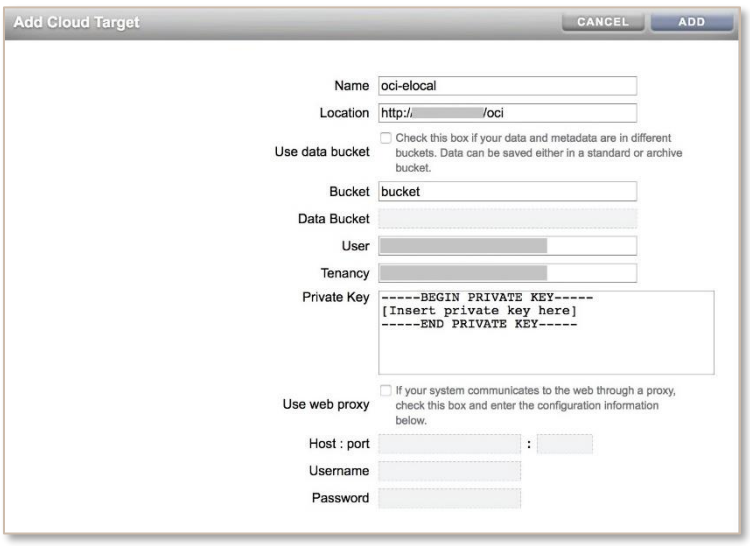
7. **On the target appliance, configure the HTTP service.**
   a) Select Configuration→Services→HTTP.
   b) Select the OCI tab.
   c) Select Enable OCI.
   d) Add default target/bucket location: /export/oci-elocal
   e) Add your public key.





8. **On the source appliance, create the OCI-compatible object storage target.**
   Provide information similar to the following:

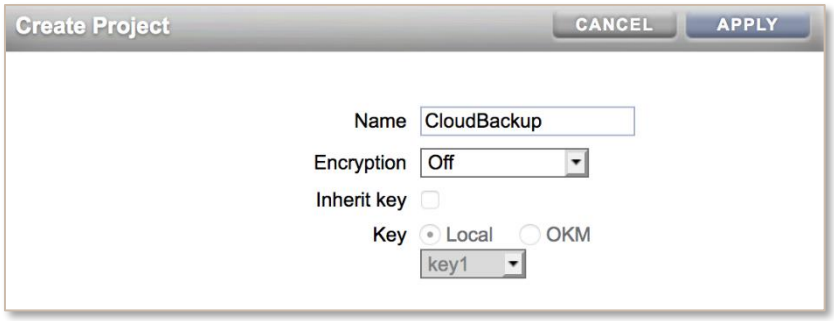
   a) Name: *oci-elocal*
   b) Location: *http://ZFSSA-name-or-IP/oci*
   c) Bucket: *bucket*
   d) User: *user-OCID*
   e) Tenancy: *tenancy-OCID*
   f) Private Key: *private key generated in Part I*



PART IV: ZFS STORAGE APPLIANCE (SOURCE) – OCI CLOUD SERVICE AND TARGET CONFIGURATION

1. **On the source appliance, create the project for the shares that will be used for the cloud snapshot backups. Use the initial project settings. For example:**

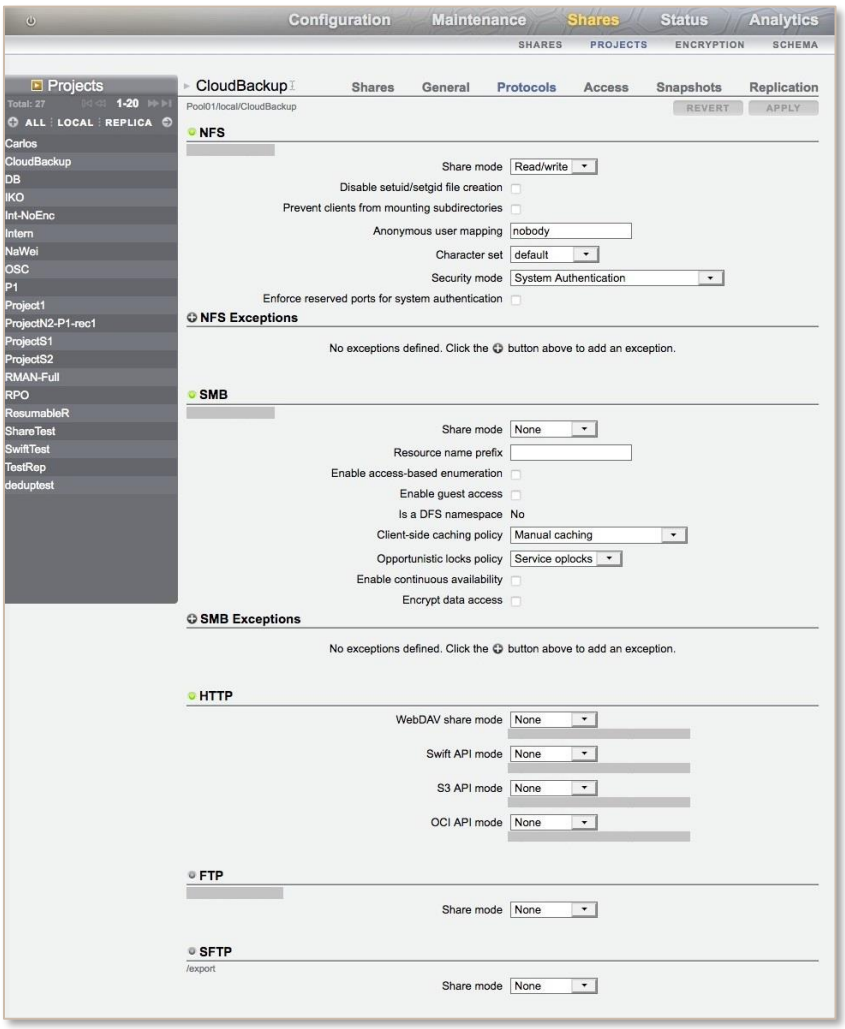
    a) Project name=CloudBackup
    b) Accept the other project defaults on the Create Project screen.



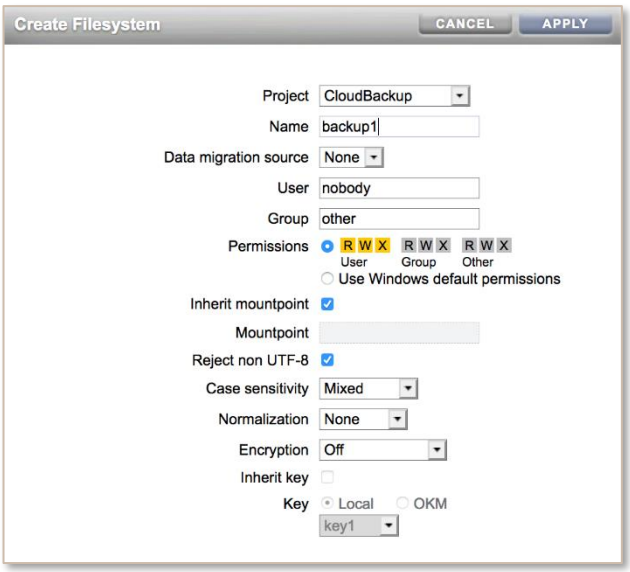
2. **On the source appliance, configure the project with the following settings. For example:**

    a) Select the General tab.
    b) Consider setting data compression=lz4 to reduce the size of data to be archived.
    c) Select the Protocols tab.

d) In the NFS section, select Share mode: Read/write. This step enables the ability to mount and write data in the share if needed. For example, modifying data to send full and incremental snapshot backups.



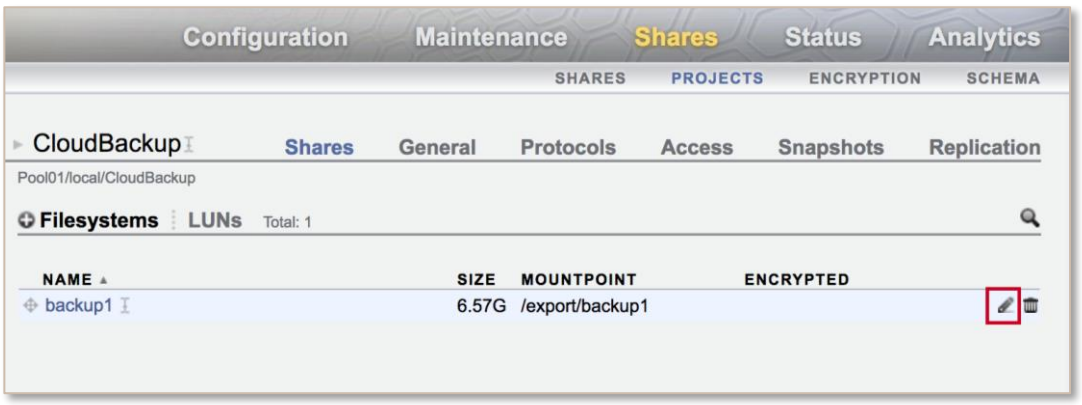
3. On the source appliance, create a share in the CloudBackup project. For example, “backup1”.



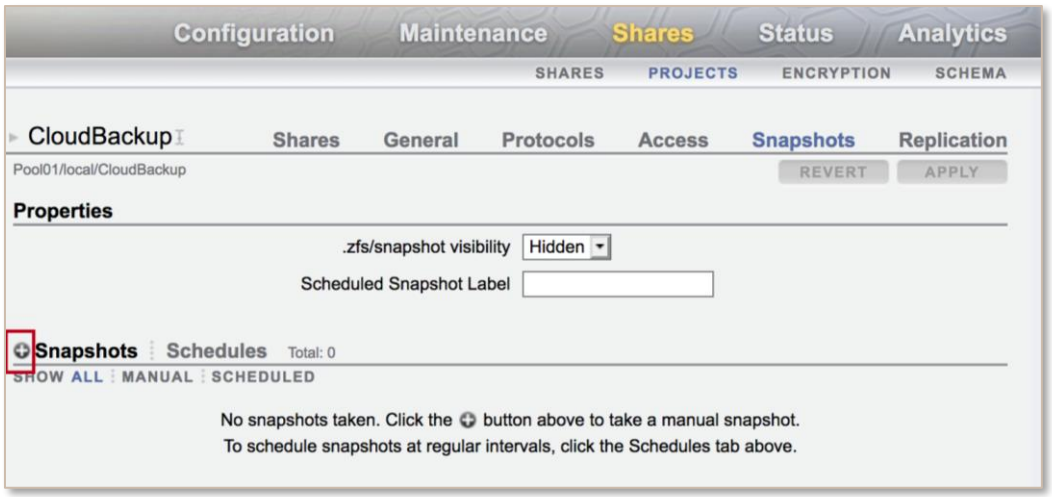
PART V: CLOUD SNAPSHOT BACKUP AND RESTORE

1. **On the source appliance, create a snapshot.**

   a) If the share is empty, write data in the share.
   b) Select share from which to create a snapshot and select the pencil icon.

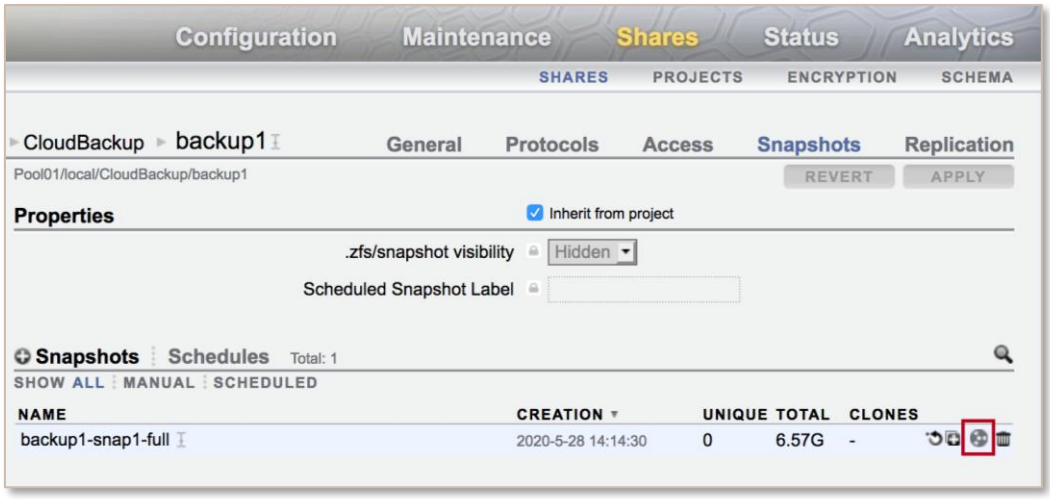


   c) Select the Shares→Snapshots tab and click the plus (+) icon to create a new snapshot. From the CloudBackup Shares screen, select the pencil icon. Then, select the Snapshots tab.

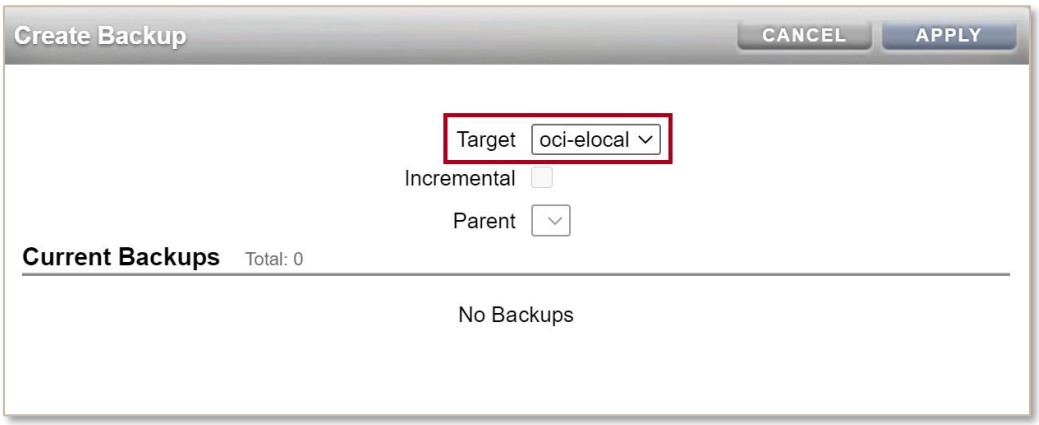


   d) Add a snapshot name and create the snapshot.

2. **On the source appliance, backup the snapshot to the OCI-compatible object storage on the target appliance.**
   a) Select the Snapshot tab of the share.
   b) Select the snapshot to back up by hovering to the right of the share and selecting the “Backup snapshot to cloud” icon.



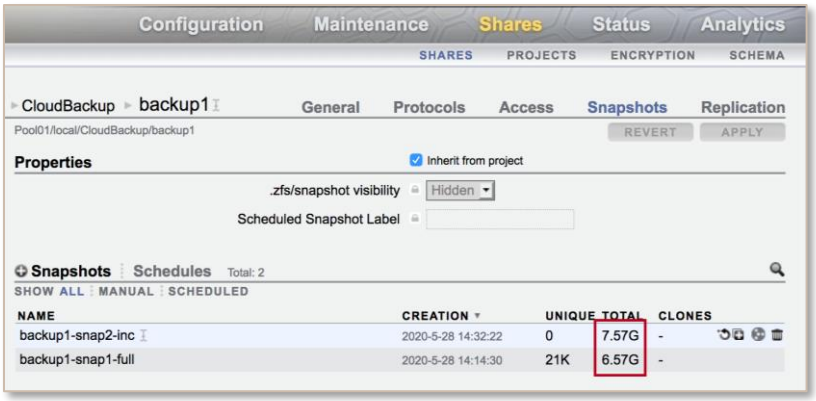
c) Select the cloud target to back up to and apply provided settings.



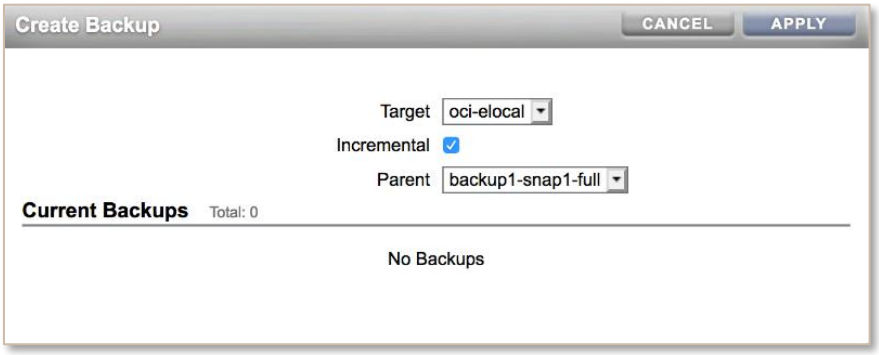
3. **Backup the incremental snapshot to the OCI-compatible object storage on the target appliance**.

a) Assuming the file system/share data is modified, create a new snapshot of selected.

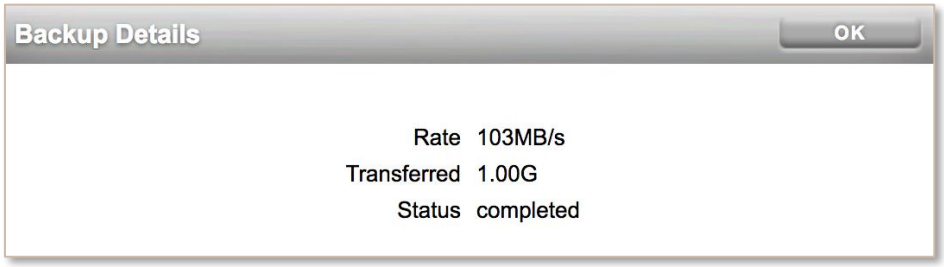
b) Note the difference in snapshot sizes.



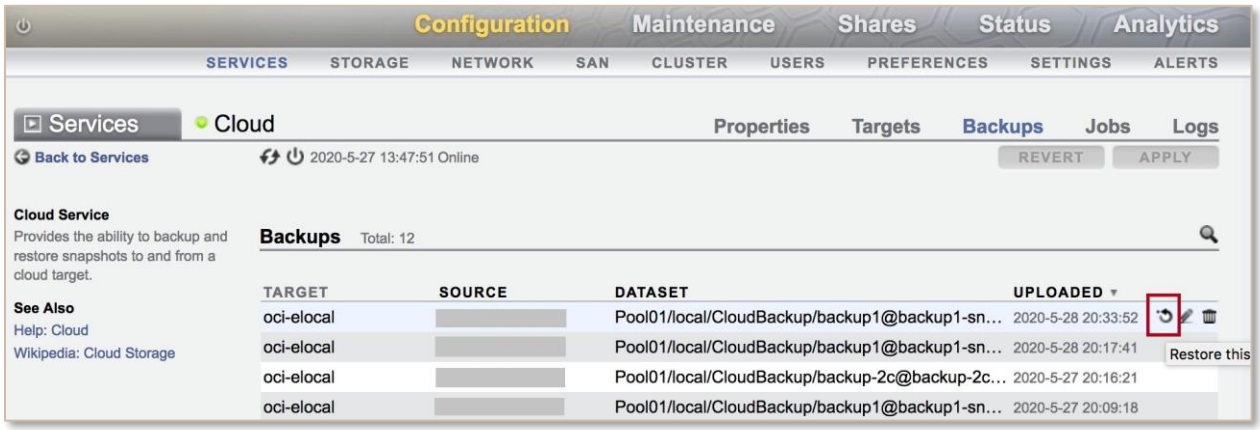
c) Select “Incremental” checkbox and assign its respective parent to only backup new data.



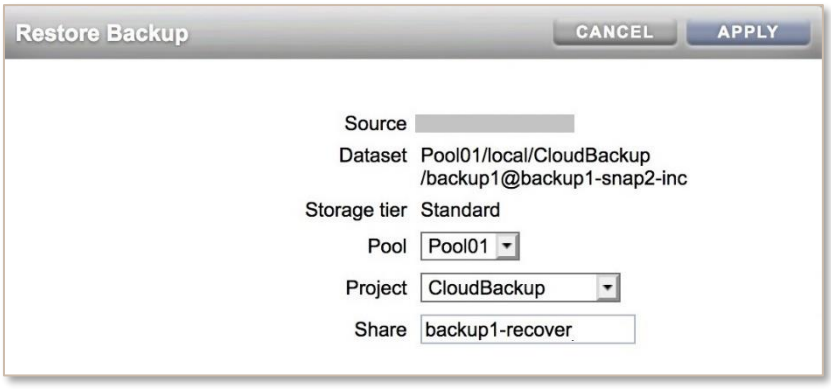
4. **Note that size of incremental snapshot backup transferred is only 1GB in size because only incremental changes are transferred.**



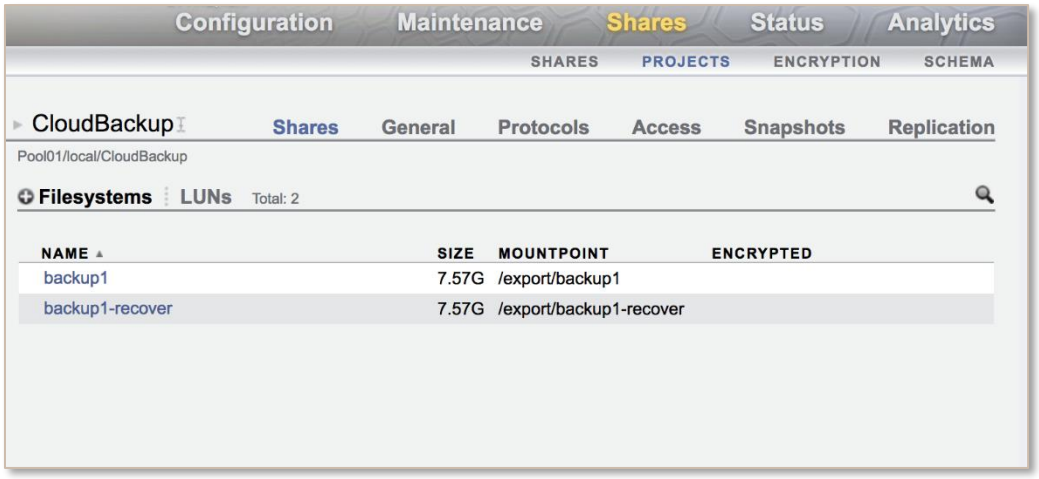
5. **Restore full and incremental cloud snapshot backup.**
   a) Go to Configuration→Services→Cloud→Backups, select backup and click “restore” icon.



b) Provide a new share name to restore the cloud snapshot backup.



6. **Go to Shares→CloudBackup. Confirm the cloud snapshot backup is restored.**



PART VI: MONITOR CLOUD SNAPSHOT BACKUPS AND OBJECT STORE BUCKET

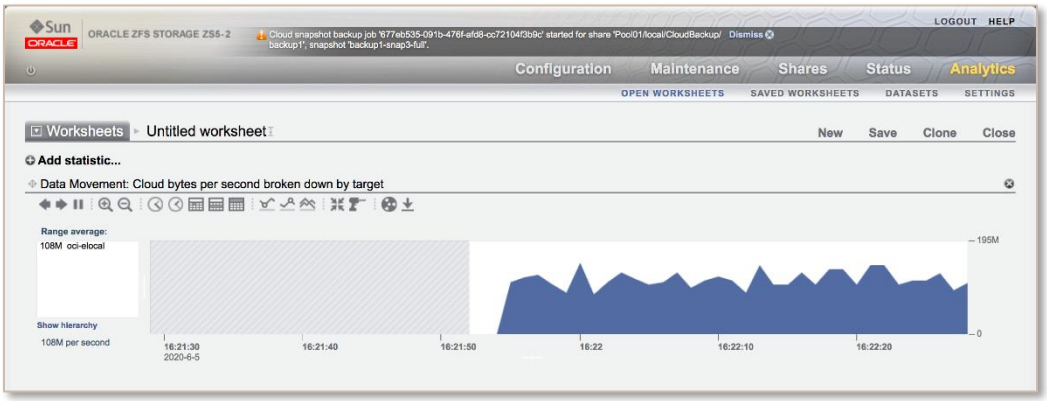
1. **Monitor cloud backup job with Analytics.**

   You can monitor cloud snapshot transfers with ZFS Storage Appliance Analytics.

   Cloud snapshot backup throughput performance between on-premise ZFS Storage Appliances will depend on network speed and connectivity.

   Backup throughput to OCI cloud object storage from on-premise storage will also depend upon connectivity. Our testing suggests approximately 100GB/hour. OCI's FastConnect feature provides a dedicated, private connection between your data center and OCI. FastConnect provides higher-bandwidth options, and a more reliable and consistent networking experience compared to internet-based connections.

   a) Go to Analytics and select + sign next to Add statistics. Select Cloud bytes or Cloud requests. For example:

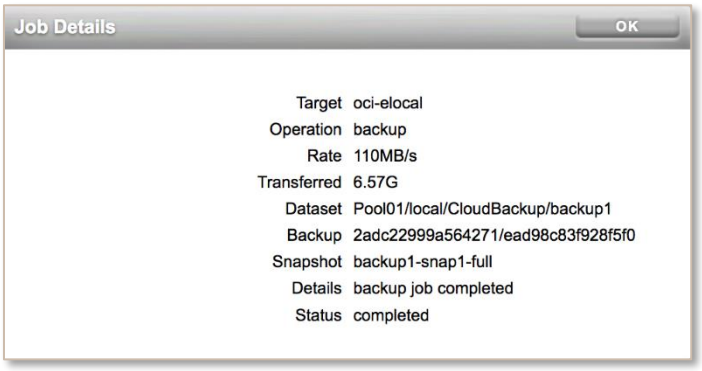


2. **Monitor cloud backup job details and alert information.**

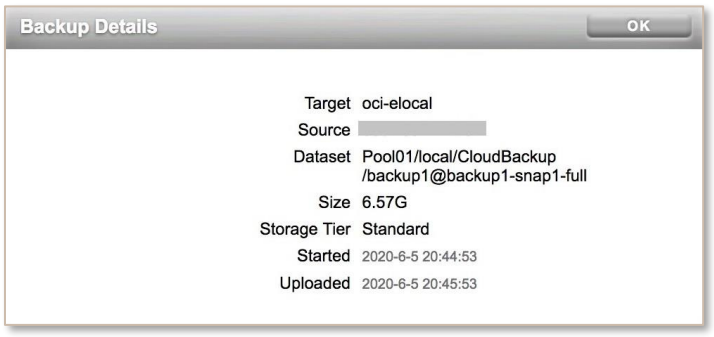
   Information about the current cloud snapshot backup job is detailed at the top of the BUI when then the job is in progress. Backup job details can also be displayed from Configuration→Services→Cloud→Backups or Configuration→ Services→Cloud→Jobs, which includes most recent backup jobs.

   Backup job details can also be reviewed in the alert logs in Maintenance→Logs.

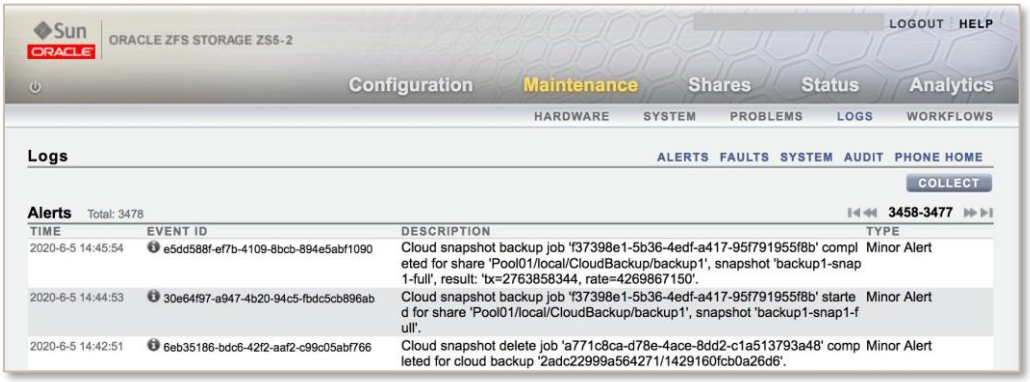
   a) On the source appliance, review details of last cloud snapshot backup job details in Configuration→ Services→Cloud→Jobs. Click the edit icon. For example:



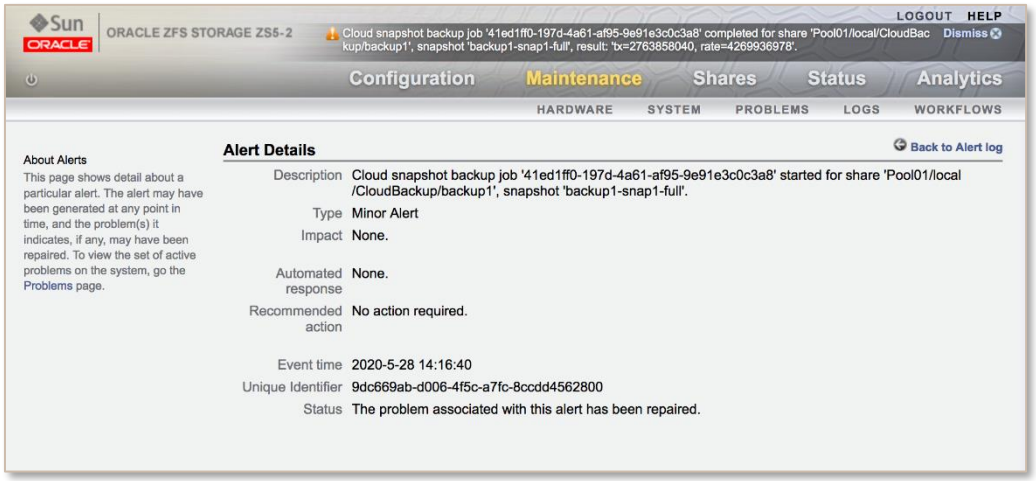
b) On the source appliance, review details of recent cloud snapshot backups in Configuration→ Services→Cloud→Backups. Click the edit icon. For example:



c) On the source appliance, review previous cloud snapshot backup entries in Maintenance→Logs. For example:



d) On the source appliance, select a cloud snapshot backup alert and click on the “show alert details” icon. For example:



3. Display OCI-compatible object storage bucket details.

The OCI-compatible object storage on an on-premise ZFS Storage Appliance does not include a management interface so visibility into the object storage bucket is through the oci command line interface.

Consider creating a config file so that oci command line syntax described below can be simplified. For more information, see Part VIII: Automation and Customization Tips.

a) On the local system, list the `oci-elocal` bucket contents. For example:

```
local# oci os object list --endpoint http://ZFSSA-name-or-IP/oci -ns /export/oci-elocal --bucket-name
bucket --limit 1000000 --output table --query 'data[*].{"Name":"name","Size":"size","Time
created":"time-created"}'
```

```
+-------------------------------------------------------------+-------+---------------------------+
| Name                                                        | Size  | Time created              |
+-------------------------------------------------------------+-------+---------------------------+
| zfs/target                                                  | 63    | 2020-05-27T17:25:25+00:00 |
| zfs/backups/18860d44a05efb7f/01d9aa3b984d8e7b/000000001     | 14852 | 2020-06-10T17:43:03+00:00 |
| zfs/log/6378714b-faac-4fbf-afb2-a42a7dd969d7/00000001       | 106   | 2020-06-09T22:14:01+00:00 |
| zfs/target                                                  | 63    | 2020-05-27T17:25:25+00:00 |
| zfs/log/7c6ccc16-9d6e-e254-cfc2-dd846a84b11a/00000227       | 109   | 2020-06-12T17:18:03+00:00 |
| zfs/manifests/18860d44a05efb7f/01d9aa3b984d8e7b             | 788   | 2020-06-10T17:43:03+00:00 |
| zfs/source/6378714b-faac-4fbf-afb2-a42a7dd969d7             | 204   | 2020-06-12T17:18:09+00:00 |
| zfs/source/7c6ccc16-9d6e-e254-cfc2-dd846a84b11a             | 205   | 2020-06-12T17:18:03+00:00 |
```

b) On the local system, listing the bucket contents of a cloud target can also be done with the same command. For example:

```
local# oci os object list  -endpoint "https://objectstorage.us-ashburn-1.oraclecloud.com" --ns
"my-ns" -name cloudbucket --limit 1000000 --output table --query
'data[*].{"Name":"name","Size":"size","Time created":"time-created"}'
```

```
+-----------------------------------------------------------------------------------+------------+---------------------------------+
| Name                                                                              | Size       | Time created                    |
+-----------------------------------------------------------------------------------+------------+---------------------------------+
| zfs/backups/2adc22999a564271/0d201319e7fdc6fc/000000001                           | 4503588    | 2020-04-21T13:17:50.718000+00:00 |
| zfs/backups/561f4abb58364785/e9add2fe76fa9a80/000000001                           | 1075000608 | 2020-03-05T21:47:09.644000+00:00 |
| zfs/backups/tar/300ec53b6405417f/f2c84bb0df547515/000000001                       | 188        | 2020-06-02T14:32:32.371000+00:00 |
| zfs/backups/tar/850338bd9d405668/41479dc3eb190073/000000001                       | 187        | 2020-03-24T21:02:55.192000+00:00 |
| zfs/backups/zfs/300ec53b6405417f/f2c84bb0df547515/000000001                       | 13128      | 2020-06-02T14:32:24.151000+00:00 |
| zfs/backups/zfs/850338bd9d405668/41479dc3eb190073/000000001                       | 13256      | 2020-03-24T21:02:48.717000+00:00 |
| zfs/backups/zfs/850338bd9d405668/c06f0305b9d3db20-41479dc3eb190073/000000001      | 3756       | 2020-03-24T21:03:16.441000+00:00 |
| zfs/dependencies/zfs/850338bd9d405668/41479dc3eb190073-c06f0305b9d3db20           | 0          | 2020-03-24T21:03:16.596000+00:00 |
| zfs/log/4c654cce-6cc1-4108-b3c9-f35b16e8a928/00000001                             | 107        | 2020-03-16T15:56:52.112000+00:00 |
```

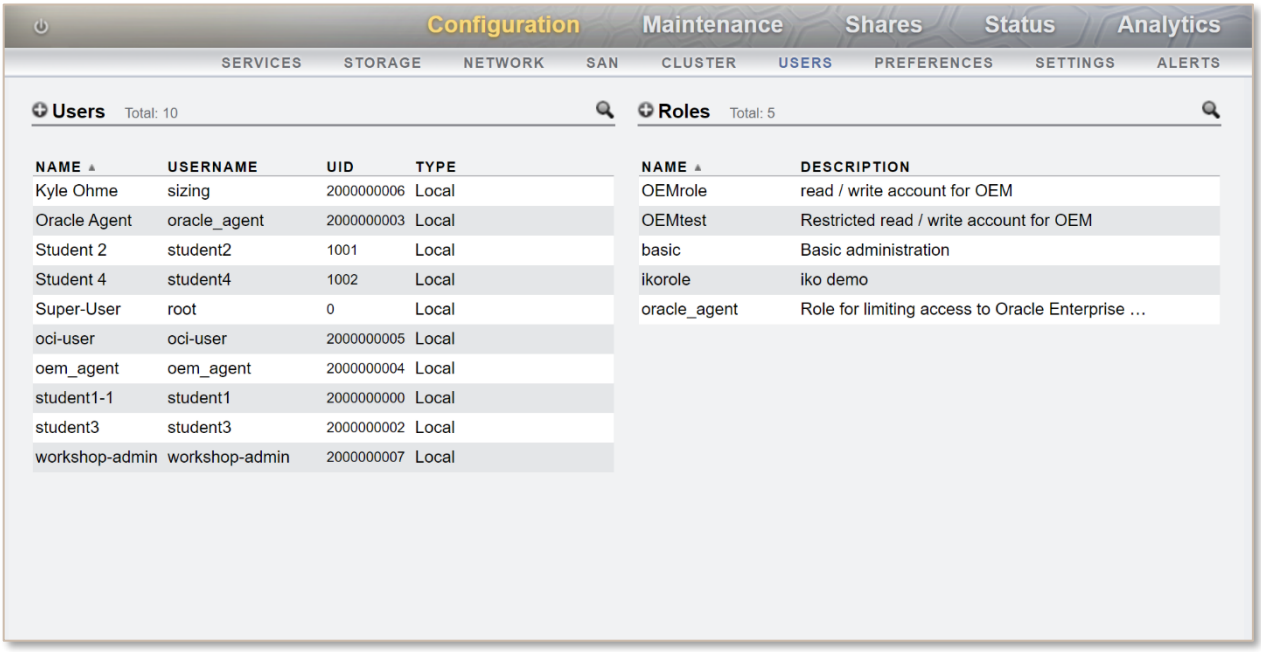
When a cloud snapshot backup is created, a unique ID string is generated that can be used to restore the snapshot. The above output is described as follows:

Component	Description
Name	zfs/backups – Identifies the snapshot backup ID zfs/dependences – identifies any incremental backup denoted with a /, which means that this backup cannot be removed unless the incremental backup snapshot is removed zfs/log – Identifies log data of the snapshot backup zfs/target – identifies the cloud snapshot target zfs/source – identifies the source name of the backup
Size	Cloud snapshot backup size in bytes
Time created	Identifies the date/time that the backup was created

PART VII: CLOUD SNAPSHOT BACKUPS ROLES AND AUTHORIZATION

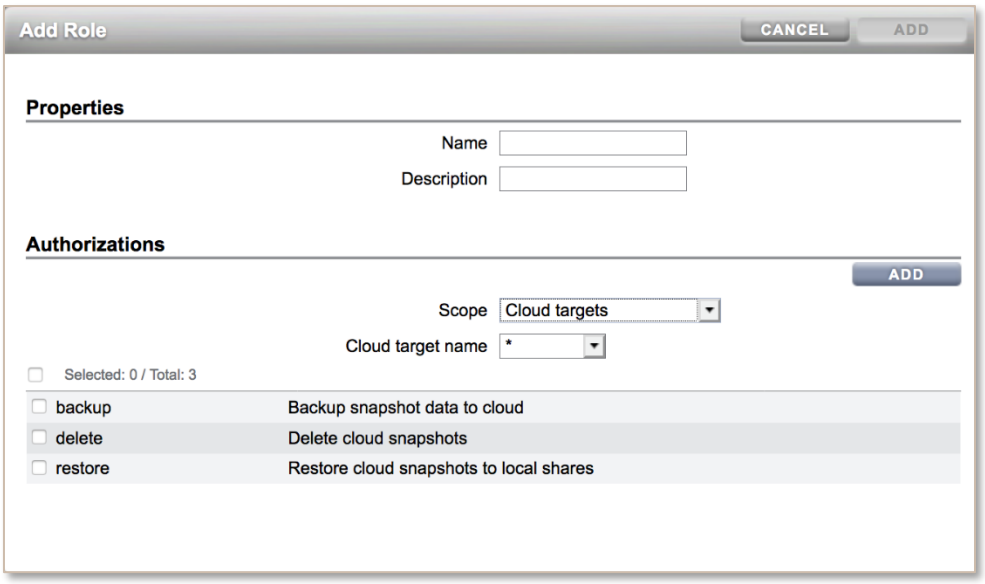
The ZFS Storage Appliance provides a pre-configured authorization (Cloud targets) so that you can determine who can add, remove, and restore cloud snapshot backups.

1. **Go to Configuration→Users and select + sign next to Roles.**



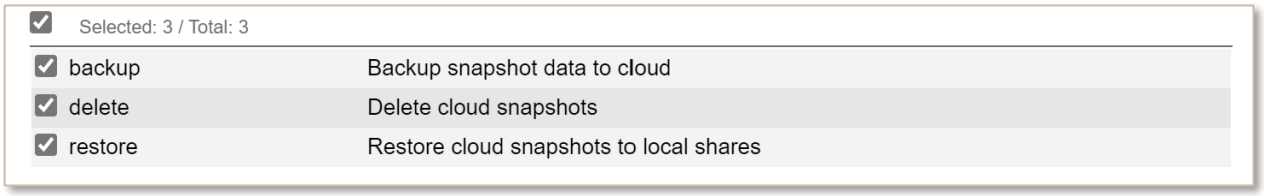
2. **Identify user name and description.**
3. **Restrict cloud target name, if necessary.**
4. **Select Cloud Targets from the Scope pulldown menu.**

5. **Select the backup, delete, or restore authorization.**

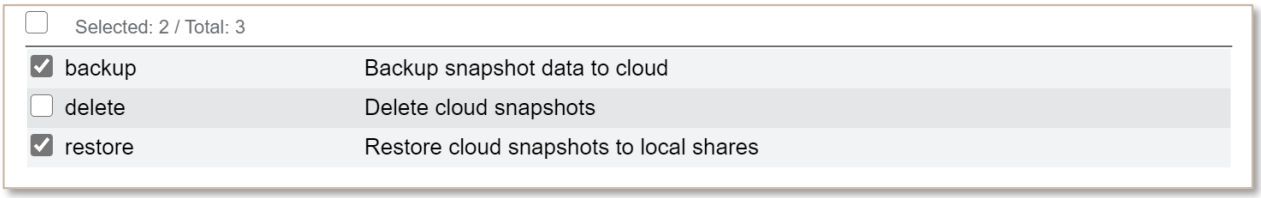


EXAMPLE: Cloud Snapshots Admin and Cloud Snapshots Operator permissions

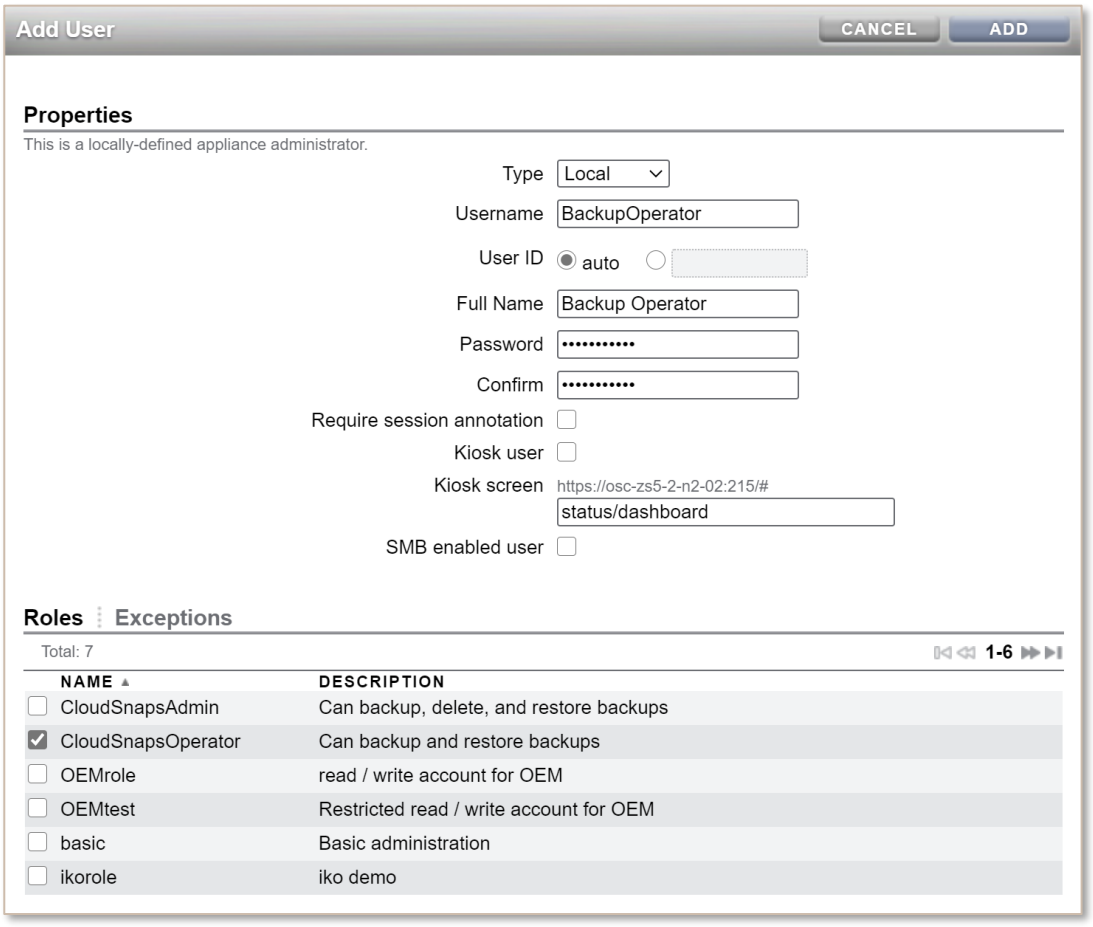
A Cloud Snapshots Admin could have the ability to backup, delete, and restore backups from a cloud target.



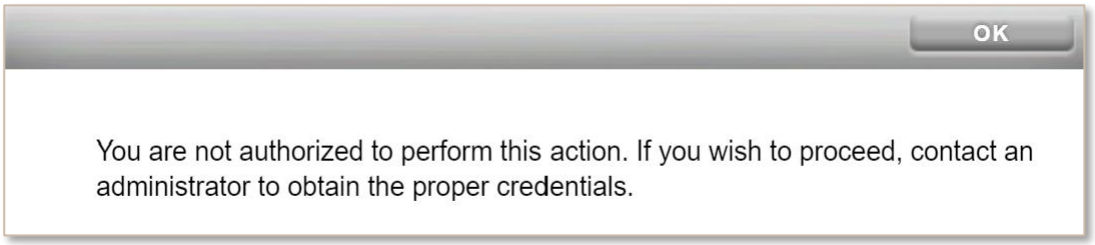
A Cloud Snapshots Operator could have the ability to backup and restore backups from a cloud target. This means the role does not have permission to delete backups.



6. **Create or modify an existing user and assign the proper role to allow cloud snapshot permissions.**



If a Cloud Snapshots Operator attempts to delete a backup, the system will prevent the request given the user does not have authorization to perform the action.



PART VIII: AUTOMATION AND CUSTOMIZATION TIPS

OCI Command Line Simplification

Because the OCI command line is used to create the target bucket and also monitor OCI object stores, you might consider setting up profiles to simplify the OCI command line execution.

Profiles can be used to facilitate command input when working with a specific target. Instead of using `–endpoint, –namespace, --compartment-id`, etc. to access a target, these configurations can be saved into a profile such that they can be called upon from a save file (for example, `--profile zfssa`).

The profile's settings are defined under its title (for example, `[zfssa]`). The .oci/config file can contain configuration such as: `user, fingerprint, key_file, tenancy,` and `region`. Similarly, the .oci/oci_cli_rc file (create file, if needed) can contain: `compartment_id, os.namespace,` and `endpoint`.

a) Create a profile in the config file by adding configurations like the following:

```
[zfssa]
user=user-OCID
fingerprint=your-fingerprint
key_file=selected-key-file-location
tenancy=tenancy-OCID
region=your-region
```

b) Create a profile in the oci_cli_rc file by adding configurations like the following:

```
[zfssa]
compartment_id=target-compartment-id
os.namespace=target-namespace
endpoint=https://ZFSSA-name-or-IP/oci
```

c) Use profiles to simplify any oci command. For example, these two commands are the same (given setup above):

- `local# oci os bucket create –endpoint "http://ZFSSA-name-or-IP/oci" --ns "target-namespace" –name bucket`
- `local# oci os bucket create --profile zfssa –name bucket`

Workflow Installation and Automation

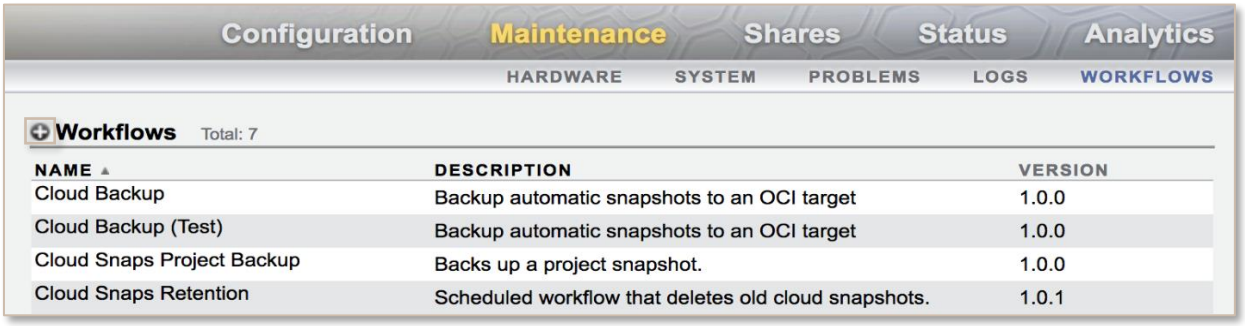
A workflow can be used to automate processes in the ZFS Storage Appliance. Through a script, a workflow can take in parameters to perform a scheduled or one-time execution of an action through the browser interface or CLI.

Creating workflows can assist you in managing cloud snapshot backups in OCI object storage. For example, you can leverage a workflow for scheduling cloud snapshot backups or for creating and scheduling a project-level cloud snapshot backup, and even to set a retention time for backups stored in OCI object storage.

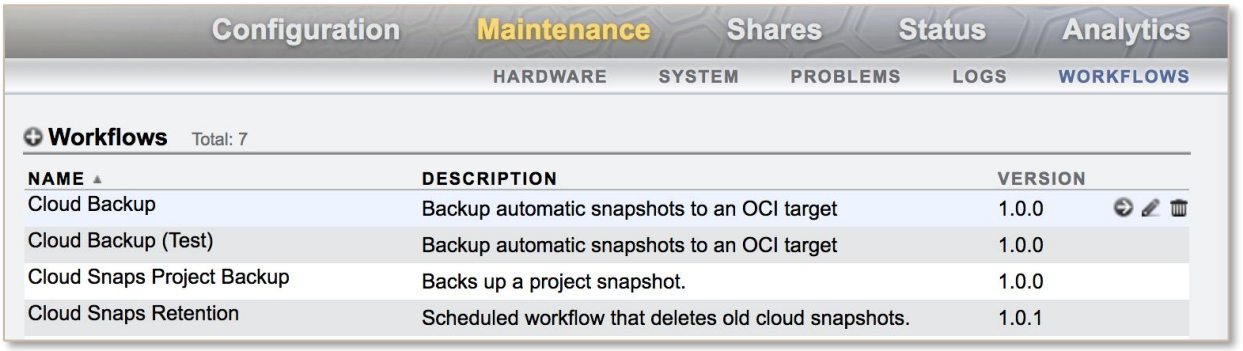
Workflow documentation can be found at: https://docs.oracle.com/cd/E91275_01/html/E91291/gokxv.html#scrolltoc.

1. On the source appliance, review workflow installation and execution from the BUI.

a) Go to Maintenance→Workflows and select + sign next to Workflows.



b) On the local system, select the workflow (.akwf) file to be used and upload it.
c) Press the "Execute Workflow" button to run workflow script.



2. On the source appliance, review the workflow CLI access and management.

Some workflows must be managed through the CLI, such as a scheduled workflow.

a) Access workflows from the CLI using the following command: > **`maintenance workflows ls`**

```
Workflows:

WORKFLOW     NAME                                  OWNER SETID ORIGIN              VERSION
workflow-000 Hello world                           root  false <local>             undefined
workflow-001 New share                             root  false <local>             undefined
workflow-002 Cloud Backup (Test)                   root  true  Oracle              1.0.0
workflow-003 Cloud Backup                          root  true  Oracle              1.0.0
workflow-004 Cloud Snaps Project Backup            root  false Oracle              1.0.0
workflow-005 Cloud Snaps Retention (Testing in Progress) root  true  Oracle
workflow-006 Cloud Snaps Retention                 root  true  Oracle              1.0.1
```

b) Select the desired workflow. For example, `> select workflow-002` and `ls` to display any available actions and properties.

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

July 2020
Authors: Cindy Swearingen, Stephanie Zambrana, Louis Romero, and Lillian Andersen