Dell PowerScale: CloudPools and ECS

Architectural Overview, Considerations, and Best Practices

May 2023

H14775.8

White Paper

Abstract

This white paper provides an overview of Dell PowerScale CloudPools software in OneFS 9.4.0.0. It describes its policy-based capabilities that can reduce costs and optimize storage by automatically moving infrequently accessed data to Dell ECS storage.

Dell Technologies

Copyright

Contents

Executive summary

Overview

This white paper describes how Dell PowerScale CloudPools software in OneFS 9.4.0.0 integrates with Dell ECS storage. The paper covers the following topics:

- CloudPools solution architectural overview
- CloudPools 2.0 introduction with a focus on the following improvements:
  - AWS signature v4 authentication support
  - Dell PowerScale NDMP and Dell PowerScale SyncIQ support
  - Non-Disruptive Upgrade (NDU) support
  - Snapshot efficiency
  - Sparse files handling
  - Quota management
  - Anti-virus integration
  - WORM integration
- General considerations and best practices for a CloudPools implementation
- CloudPools reporting, commands, and troubleshooting

Audience

This white paper is intended for experienced system administrators, storage administrators, and solution architects interested in learning how CloudPools works and understanding the CloudPools solution architecture, considerations, and best practices.

This guide assumes the reader has a working knowledge of:

- Network-attached storage (NAS) systems
- The Dell PowerScale scale-out storage architecture and the Dell PowerScale OneFS operating system
- The Dell ECS architecture

Readers should also be familiar with PowerScale and ECS documentation resources including:

- Dell PowerScale OneFS release notes, available on Dell Support, containing important information about resolved and known issues
- Dell PowerScale OneFS Best Practices
- Dell ECS General Best Practices

Revisions

Date	Description
March 2017	Initial release
April 2019	Rewritten and added details for CloudPools 2.0
October 2019	Updated snapshot efficiency and best practices

Date	Description
June 2020	Updated best practices
October 2020	Updated CloudPools operations
April 2021	Updated best practices
October 2021	Updated performance
April 2022	• Updated template • Updated reporting
May 2023	Updated best practices

We value your feedback

Dell Technologies and the authors of this document welcome your feedback on this document. Contact the Dell Technologies team by email.

Author: Jason He

Note: For links to other documentation for this topic, see the PowerScale Info Hub.

CloudPools solution architecture overview

Overview

The OneFS CloudPools feature allows tiering cold or infrequently accessed data to lower-cost cloud storage. It is built on the Dell PowerScale SmartPools file pool policy framework, which provides granular control of file placement on a PowerScale cluster.

CloudPools extends the PowerScale namespace to the private cloud, Dell ECS, as illustrated in the following figure. It allows applications and users to seamlessly retain access to data through the same network path and protocols regardless of where the file data physically resides.

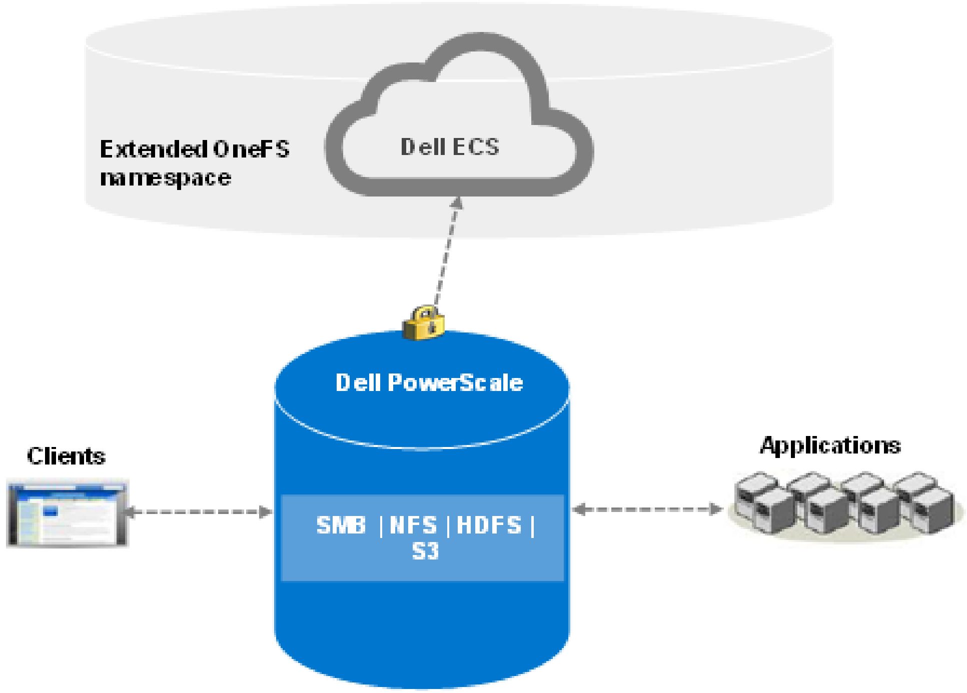


Figure 1. **CloudPools solution architecture**

Note: A SmartPools license and a CloudPools license are required on each node of the PowerScale cluster. Dell Isilon OneFS version 8.0.0 or later is required for CloudPools 1.0. Dell Isilon OneFS version 8.2.0 or later is required for CloudPools 2.0.

Policies are defined on the PowerScale cluster and drive the tiering of data. Clients can access the archived data through various protocols including SMB, NFS, HDFS, and S3.

PowerScale

This section describes key CloudPools concepts including:

- SmartPools
- SmartLink files
- File pool policies

SmartPools

SmartPools is the OneFS data tiering framework, of which CloudPools is an extension. SmartPools alone tiers data between different node types within a PowerScale cluster. CloudPools also adds to tier data outside of a PowerScale cluster.

SmartLink files

Although file data is moved to cloud storage, the files remain visible in OneFS. After file data has been archived to the cloud storage, the file is truncated to an 8 KB file. The 8 KB file is called a SmartLink file or stub file. Each SmartLink file contains a data cache and a map. The data cache is used to retain a portion of the file data locally, and the map points to all cloud objects.

The following figure shows the contents of a SmartLink file and the mapping to cloud objects.

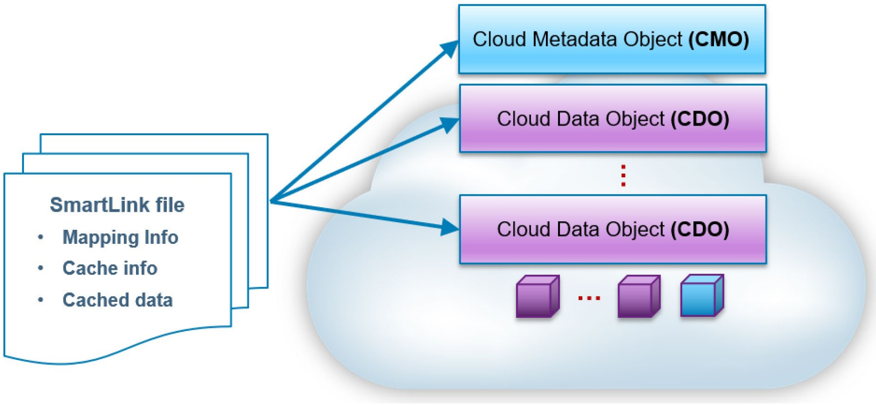


Figure 2. **SmartLink file**

File pool policies

Both CloudPools and SmartPools use the file pool policy engine to define which data on a cluster should live on which tier or be archived to a cloud storage target. The SmartPools and CloudPools job has a customizable schedule that runs once a day by default. If files match the criteria specified in a file pool policy, the content of those files is moved to cloud storage when the job runs. A SmartLink file that contains information about where to retrieve the data is left behind on the PowerScale cluster. In CloudPools 1.0, the SmartLink file is sometimes referred to as a stub, which is a unique construct that does not behave like a normal file. In CloudPools 2.0, the SmartLink file is an actual file that contains pointers to the CloudPool target where the data resides.

Key options when configuring a file pool policy include:

- Encryption
- Compression
- File matching criteria
- Local data cache
- Date Retention

Encryption

CloudPools provides an option to encrypt data before the data is sent to the cloud storage. It uses the PowerScale key management module for data encryption and uses AES-256 as the encryption algorithm. The benefit of encryption is that only encrypted data is being sent over the network.

Compression

CloudPools provides an option to compress data before the data is sent to the cloud storage. It implements block-level compression using the zlib compression library. CloudPools does not compress data that is already compressed.

File-matching criteria

When files match a file pool policy, CloudPools moves the file data to the cloud storage. File-matching criteria enable defining a logical group of files as a file pool for CloudPools. The criteria define which data should be archived to cloud storage.

File matching criteria include:

- File name
- Path
- File type
- File attribute
- Modified
- Accessed
- Metadata changed
- Created
- Size

Any number of file-matching criteria can be added to refine a file pool policy for CloudPools.

Local data cache

Caching is used to support local reading and writing of SmartLink files. It reduces bandwidth costs by eliminating repeated fetching of file data for repeated reads and writes to optimize performance.

Note: The data cache is used for temporarily caching file data from the cloud storage on PowerScale disk storage for files that have been moved off cluster by CloudPools.

The local data cache is always the authoritative source for data. CloudPools looks for data in the local data cache first. If the file being accessed is not in the local data cache, CloudPools fetches the data from the cloud. CloudPools writes the updated file data in the local cache first and periodically sends the updated file data to the cloud.

CloudPools provides the following configurable data cache settings:

- **Cache expiration:** This option is used to specify the number of days until OneFS purges expired cache information in SmartLink files. The default value is one day.
- **Writeback frequency:** This option is used to specify the interval at which OneFS writes the data stored in the cache of SmartLink files to the cloud. The default value is nine hours.
- **Cache read ahead:** This option is used to specify the cache read ahead strategy for cloud objects (partial or full). The default value is partial.
- **Accessibility:** This option is used to specify how data is cached in SmartLink files when a user or application accesses a SmartLink file on the PowerScale cluster. Values are **cached** (default) and **no cache**.

Data retention

Data retention is a concept used to determine how long to keep cloud objects on the cloud storage. There are three different retention periods:

- **Cloud data retention period:** This option is used to specify the length of time cloud objects are retained after the files have been fully recalled or deleted. The default value is one week.
- **Incremental backup retention period for NDMP incremental backup and SyncIQ:** This option is used to specify the length of time that CloudPools retains cloud objects referenced by a SmartLink file. And SyncIQ replicates the SmartLink file or NDMP backs up the SmartLink file using an incremental NDMP backup. The default value is five years.
- **Full backup retention period for NDMP only:** This option is used to specify the length of time that OneFS retains cloud data referenced by a SmartLink file. And NDMP backs up the SmartLink file using a full NDMP backup. The default value is five years.

Note: If more than one period applies to a file, the longest period is applied.

ECS

This section describes the following cloud objects in ECS:

- Cloud metadata object
- Cloud data object

Cloud metadata object

A cloud metadata object (CMO) is a CloudPools object in ECS that is used for supportability purposes.

Cloud data object

A cloud data object (CDO) is a CloudPools object that stores file data in ECS. File data is split into 2 MB chunks to optimize performance before sending it to ECS. The chunk is called a CDO. If file data is less than the chunk size, the CDO size is equal to the size of the file data.

Note: The chunk size is 1 MB in CloudPools 1.0 and versions before OneFS 8.2.0.

CloudPools operations

This section describes the workflow of CloudPools operations:

- Archive
- Recall
- Read
- Update

Archive

The archive operation is the CloudPools process of moving file data from the local PowerScale cluster to cloud storage. Files are archived either using the SmartPools Job or from the command line. The CloudPools archive process can be paused or resumed. See Commands for details.

The following figure shows the workflow of the CloudPools archive.

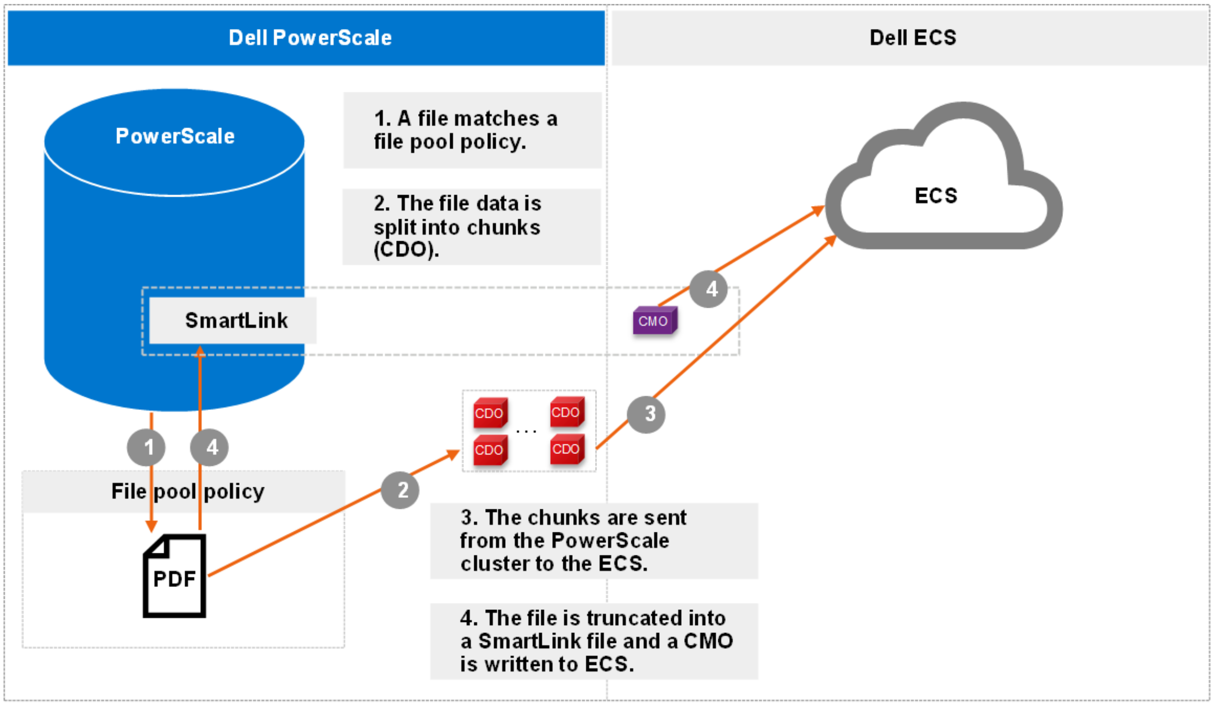

Dell PowerScale
Dell ECS
PowerScale
1. A file matches a file pool policy.
2. The file data is split into chunks (CDO).
SmartLink
CMO
4
ECS
CDO
CDO
CDO
CDO
3
1
4
File pool policy
2
PDF
3. The chunks are sent from the PowerScale cluster to the ECS.
4. The file is truncated into a SmartLink file and a CMO is written to ECS.

Figure 3. **Archive workflow**

More workflow details include:

- The file pool policy in step 1 specifies a cloud target and cloud-specific parameters. Policy examples, as described in File pool policies, include:
  - Encryption
  - Compression
  - Local data cache
  - Data retention
- When chunks are sent from the PowerScale cluster to Dell ECS in step 3, a checksum is applied for each chunk to ensure data integrity.

Recall

The recall operation is the CloudPools process of reversing the archive process. It replaces the SmartLink file by restoring the original file data on the PowerScale cluster and removing the cloud objects in ECS. The recall process can only be performed using the command line. The CloudPools recall process can be paused or resumed. See Commands for detailed instructions on commands.

The following figure shows the workflow of CloudPools recall.

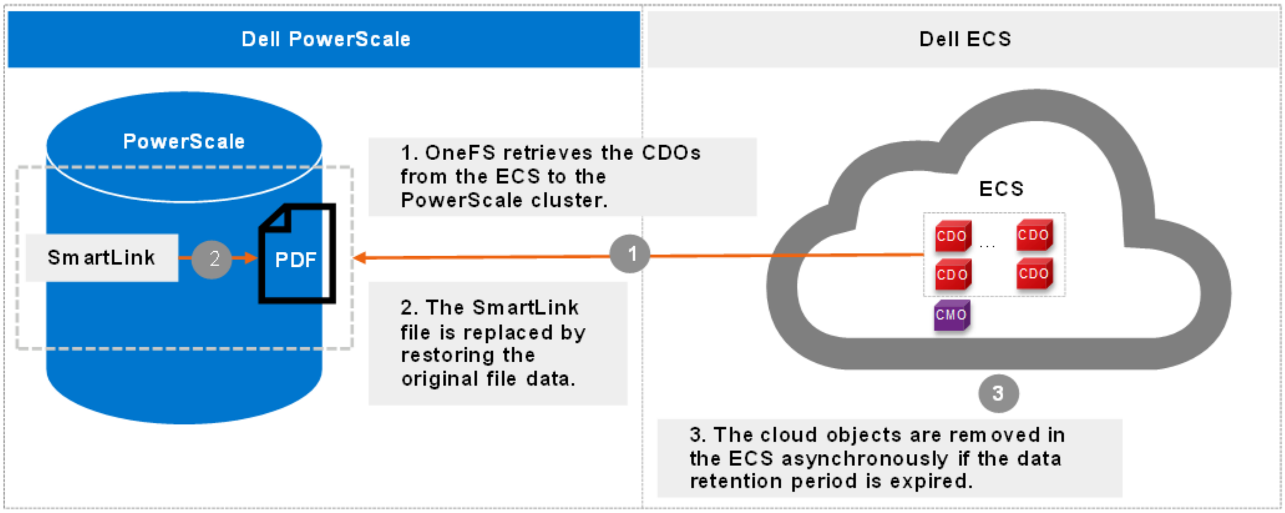

Dell PowerScale
Dell ECS
PowerScale
SmartLink
2
PDF
1
1. OneFS retrieves the CDOs from the ECS to the PowerScale cluster.
2. The SmartLink file is replaced by restoring the original file data.
ECS
CDO
CDO
CDO
CDO
CMO
3
3. The cloud objects are removed in the ECS asynchronously if the data retention period is expired.

Figure 4. **Recall workflow**

Read

The read operation is the CloudPools process of client data access, known as inline access. When a client opens a file for read, the blocks will be added to the cache in the associated SmartLink file by default. The cache can be disabled by setting the accessibility. For more detail, see File pool policies.

The following figure shows the workflow of CloudPools read by default.

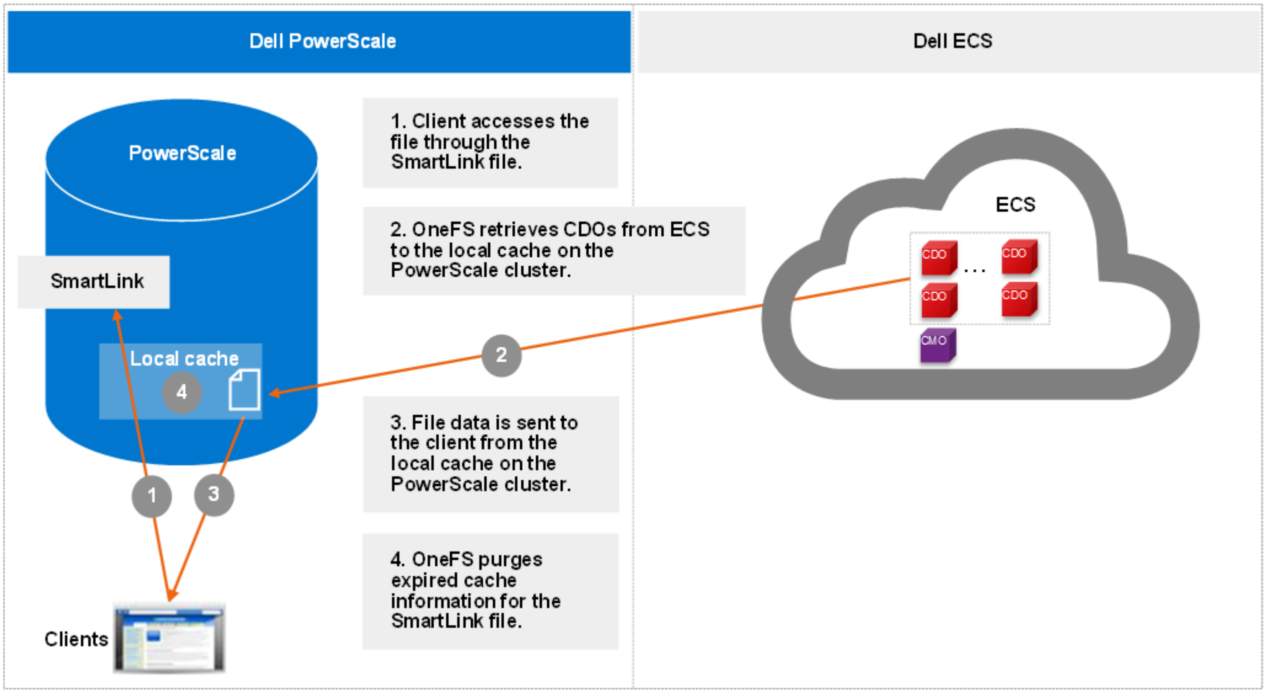

Dell PowerScale
Dell ECS
PowerScale
SmartLink
Local cache
4
1
3
2
Clients
ECS
CDO
CDO
CDO
CDO
CMO
1. Client accesses the file through the SmartLink file.
2. OneFS retrieves CDOs from ECS to the local cache on the PowerScale cluster.
3. File data is sent to the client from the local cache on the PowerScale cluster.
4. OneFS purges expired cache information for the SmartLink file.

Figure 5. **Read workflow**

Starting from OneFS 9.1.0.0, cloud object cache is introduced to enhance CloudPools functions for communicating with cloud. In step 1, OneFS looks for data in the object cache first and OneFS retrieves data from the object cache if the data is already in the object cache. Cloud object cache reduces the number of requests to the ECS when reading a file.

Prior to OneFS 9.1.0.0, OneFS looks for data in the local data cache first in step 1. It moves to step 3 if the data is already in the local data cache.

Note: Cloud object cache is per node. Each node maintains its own object cache on the cluster.

Update

The update operation is the CloudPools process that occurs when clients update data. When clients change to a SmartLink file, CloudPools first writes the changes in the data local cache and then periodically sends the updated file data to ECS. The space used by the cache is temporary and configurable. For more information, see File pool policies.

The following figure shows the workflow of the CloudPools update.

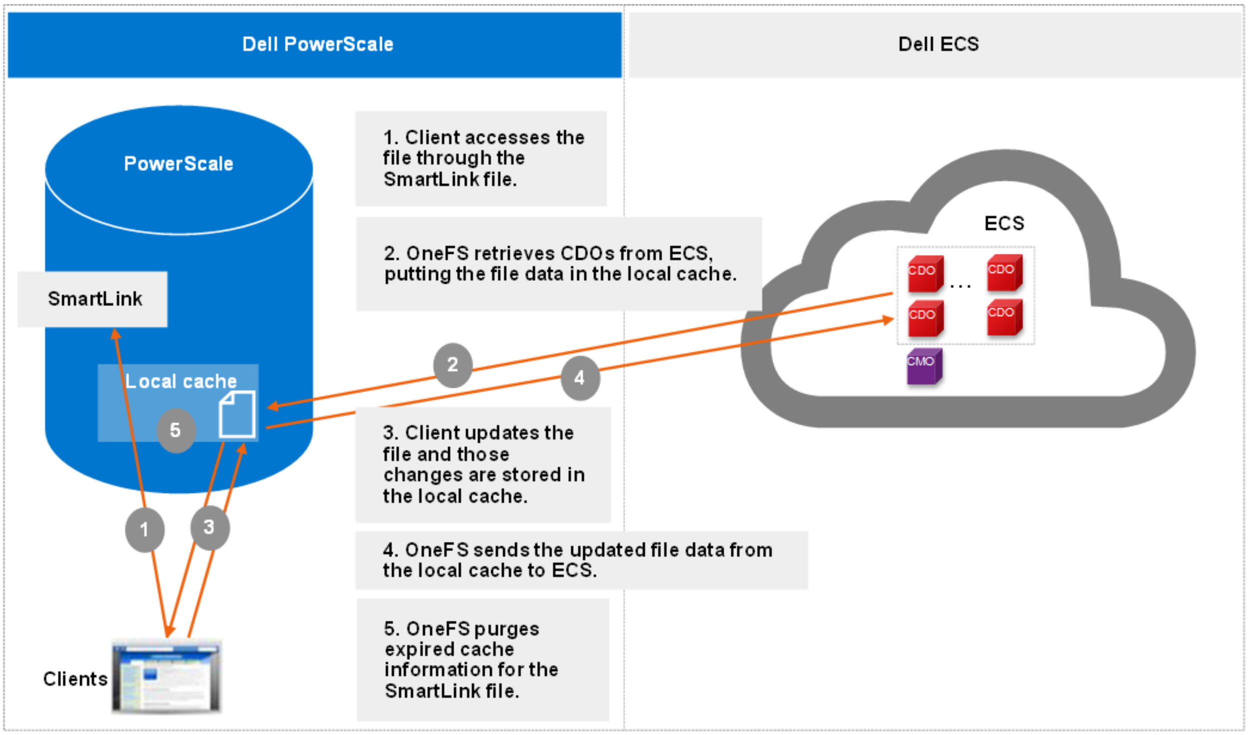

Dell PowerScale
Dell ECS
PowerScale
SmartLink
Local cache
Clients
ECS
CDO
CDO
CDO
CDO
CMO
1
2
3
4
5
1. Client accesses the file through the SmartLink file.
2. OneFS retrieves CDOs from ECS, putting the file data in the local cache.
3. Client updates the file and those changes are stored in the local cache.
4. OneFS sends the updated file data from the local cache to ECS.
5. OneFS purges expired cache information for the SmartLink file.

Figure 6. **Update workflow**

CloudPools 2.0

Introduction

CloudPools 2.0 is the next generation of CloudPools, released in OneFS 8.2.0. This section describes the following improvements in CloudPools 2.0:

- AWS signature v4 authentication support
- NDMP and SyncIQ support
- Non-Disruptive Upgrade (NDU) support
- Snapshot efficiency
- Sparse files handling
- Quota management
- Anti-virus integration
- WORM integration

AWS signature v4 authentication support

CloudPools 2.0 supports AWS signature version 4 (V4) with signature version 2 (V2). V4 provides an extra level of security for authentication with the enhanced algorithm and no action required from end users. For more information about V4, see the article Authenticating Requests: AWS Signature V4.

CloudPools 2.0 handles the compatibility of Dell PowerScale SyncIQ for data replication and NDMP for data backup and restore. When the source and target PowerScale clusters use different authentication versions, consider the following information:

- With **SyncIQ**, when the source PowerScale cluster is running OneFS 8.2.0 and the target PowerScale cluster is running a version of OneFS earlier than OneFS 8.2.0:
  - If the CloudPools cloud storage account is using V2 or V4 on the source PowerScale cluster, V2 is used on the target PowerScale cluster.
- With **NDMP,** when files are restored from tape to the target PowerScale cluster:
  - If the CloudPools cloud storage account is using V4 on the target PowerScale cluster, V4 is used.
  - If the CloudPools cloud storage account is using V2 on the target PowerScale cluster, V2 is used.
- With **NDU,** when upgrading OneFS to version 8.2.0:
  - Once the PowerScale cluster is COMMITTED to OneFS 8.2.0, it automatically begins using V4.
  - CloudPools cloud storage accounts cannot use V4 in the UPGRADED state if the version prior to the OneFS 8.2.0 upgrade did not support V4.

Note: A patch can be installed on OneFS 8.1.2 to support AWS signature V4 authentication. Contact your Dell representative if you plan to install the patch.

NDMP and SyncIQ support

When the CloudPools version differs between the source cluster and the target PowerScale cluster, the CloudPools cross-version compatibility is handled.

NDMP and SyncIQ provide two types of copy or backup: shallow copy and deep copy. For more information about NDMP and SyncIQ protection, see the white paper High Availability and Data Protection with Dell PowerScale Scale-out NAS.

- **Shallow copy (SC)/backup:** Replicates or backs up SmartLink files to the target PowerScale cluster or tape as SmartLink files without file data.
- **Deep copy (DC)/backup:** Replicates or backs up SmartLink files to the target PowerScale cluster or tape as regular files or unarchived files. The backup or replication will be slower than normal. Disk space will be consumed on the target cluster for replicating data.

The following table shows the CloudPools and OneFS mapping information. CloudPools 2.0 is released along with OneFS 8.2.0. CloudPools 1.0 is running in OneFS 8.0.x or 8.1.x.

Table 1. CloudPools and OneFS mapping information

OneFS version	CloudPools version
OneFS 8.0.x/OneFS 8.1.x	CloudPools 1.0
OneFS 8.2.0 or higher	CloudPools 2.0

The following table shows the NDMP and SyncIQ supported use cases when different versions of CloudPools are running on the source and target clusters. As noted in the table, if CloudPools 2.0 is running on the source PowerScale cluster and CloudPools 1.0 is running on the target PowerScale cluster, shallow copies are not allowed.

Table 2. NDMP and SyncIQ supported use cases with CloudPools

Source	Target	SC NDMP	DC NDMP	SC SyncIQ replication	DC SyncIQ replication
CloudPools 1.0	CloudPools 2.0	Support	Support	Support	Support
CloudPools 2.0	CloudPools 1.0	No Support	Support	No Support	Support

Nondisruptive upgrade support

When a cluster that has been using CloudPools 1.0 is upgraded to OneFS 8.2.0 or higher, a new CHANGEOVER process is initiated automatically after the upgrade commit. The process ensures a smooth transition from CloudPools 1.0 to CloudPools 2.0. CloudPools 2.0 is ready to use once the upgrade state is committed. For more information about upgrade states, see the white paper PowerScale Non-Disruptive Upgrade (NDU) Best Practices.

Snapshot efficiency

Prior to OneFS 8.2.0, CloudPools 1.0 supported archiving files with existing snapshots. However, CloudPools 1.0 had a limitation when archiving files that have existing snapshots: the copy-on-writes (CoW) process copied the entire contents of the file into the snapshot. Archiving files with existing snapshots therefore did not save space on the PowerScale cluster until the previously CoW-created snapshots expired. CloudPools 1.0 offers an option (Uncheck Archive files with snapshots in WebUI) to skip such files with snapshots. A user might have not chosen to archive files with snapshots if the previously CoW-created snapshots had long retentions. This case is to avoid creating another copy on cloud storage where the retention period meant it would persist on PowerScale storage anyway.

CloudPools 2.0 eliminates CoW on the primary data source PowerScale cluster when archiving files with snapshots to the cloud. The file data is only stored in the cloud storage, which saves space on the PowerScale cluster. For more information about data CoW for snapshots, see the white paper Data Protection with Dell PowerScale SnapshotIQ.

However, CloudPools 2.0 does not archive files on the target cluster in a SyncIQ relationship. In an environment with long snapshot retentions and an expectation that the same snapshots are maintained in both clusters. It is possible for storage usage on a target cluster to grow larger than the storage on the primary cluster which has CloudPools enabled. For space efficiency, a user with requirements for long snapshot retentions on two clusters in a SyncIQ relationship might choose to use natively tiered PowerScale archive storage, rather than CloudPools.

SnapshotIQ can take read-only, point-in-time copies of any directory or subdirectory within OneFS. A file in one directory can be either a regular file or a SmartLink file before creating a snapshot. A regular file can be truncated to a SmartLink file after archiving its file data to the cloud. A SmartLink file can be converted to a regular file after recalling its file data to the PowerScale cluster. When a snapshot is taken, it preserves the exact state of a file system at that instant. A file in the snapshot directory (/ifs/.snapshot) is a

SmartLink file if the same file in the source directory is a SmartLink file. A file in the snapshot directory is a regular file if the same file in the source directory is a regular file. The earlier version of data can be accessed later in the snapshot directory.

The following scenarios address CloudPools 2.0 and snapshots. HEAD is the current version of a SmartLink file in the source directory.

- The file is already a SmartLink file in the source directory before creating a snapshot.
  - Scenario 1: Update HEAD
  - Scenario 2: Update HEAD multiple times and a new snapshot is created between multiple updates
  - Scenario 3: Read file data from a snapshot
- The file is still a regular file in the source directory before creating a snapshot. Then, the regular file is archived to the cloud after a snapshot creation.
  - Scenario 4: Update HEAD
  - Scenario 5: Read file data from a snapshot

Scenario 1

When updating HEAD (SmartLink files in snapshot), a new SmartLink is generated for HEAD when updating HEAD and write-back to the cloud. Cache for HEAD will be empty once its own cache expires. For the workflow of updating a SmartLink file, see Update. The original version SmartLink file is still used for the next snapshot of HEAD. This scenario does not cause the snapshot space to grow. The following figure shows the process of scenario 1 to update HEAD when SmartLink files are in the snapshot directory.

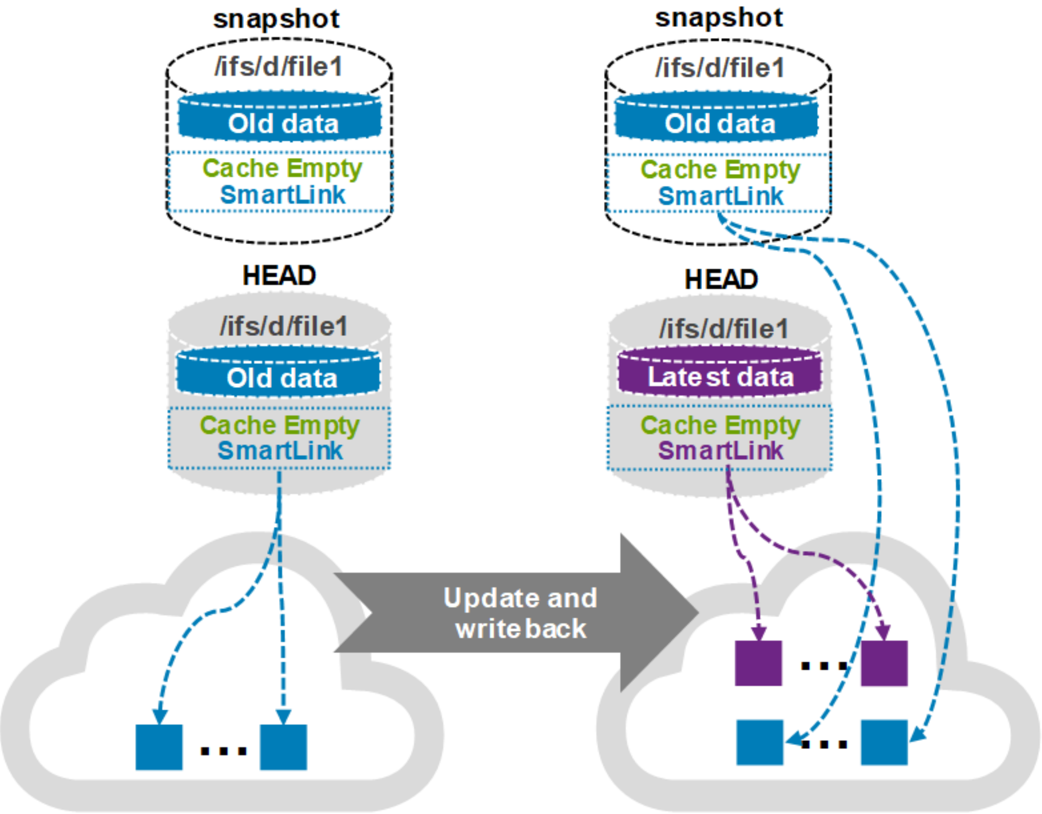


Figure 7. **Scenario 1: Update HEAD when SmartLink files are in the snapshot directory**

Scenario 2

This scenario describes updating HEAD multiple times, and a new snapshot is created between multiple updates (SmartLink files in snapshot). For example, a user updates HEAD (the first update) while a new (most recent) snapshot is created before the first update write-back is made to the cloud. Then, another user updates (the second update) HEAD again after the new (most recent) snapshot is created. Now there are two snapshots: one snapshot is the next snapshot of HEAD, the other is the most recent snapshot of HEAD.

When a snapshot is taken, it preserves the exact state of a file system at that instant. Data for the next snapshot of HEAD is the old data that is already archived to the cloud and its cache is empty. Data for the most recent snapshot is the new data (old data with the first update). Its cache is dirty before the new data write-back is made to the cloud. Data for HEAD is the latest data and its cache is dirty before the latest data write-back is made to the cloud. The latest data contains old data with the first update and the second update. A new version SmartLink is generated for the most recent snapshot after the new data write-back is made to the cloud (write-back in the snapshot). The new data contains old data with the first update. Also, a new version SmartLink is generated for HEAD after the latest data write-back is made to the cloud (write-back in HEAD). Cache for the most recent snapshot or HEAD becomes empty once its own cache expires. Now, all file data is only stored on the cloud and saves space on the PowerScale cluster. Users can read file data from its own SmartLink file at any time.

The following figure shows the process of scenario 2.

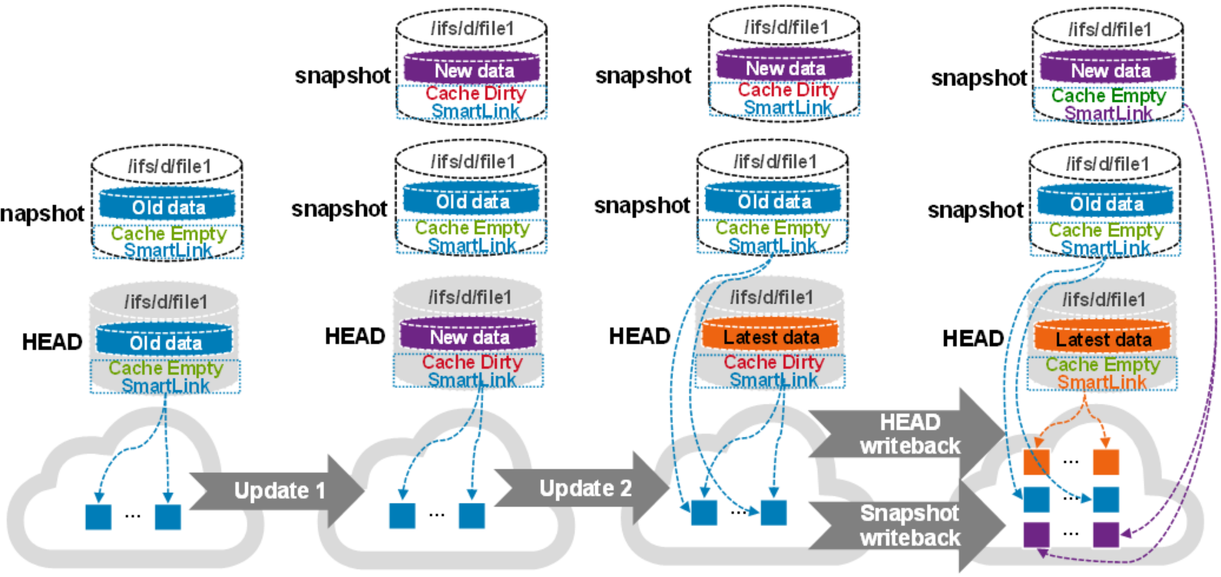


Figure 8. **Scenario 2: Update HEAD multiple times and perform a write-back in the snapshot**

Scenario 3

This scenario describes reading file data from a snapshot (SmartLink files in snapshot). The files in the next snapshot and HEAD use the same version of SmartLink file when not updating HEAD after the snapshot is created. This scenario is no different than reading the same file from HEAD or the next snapshot of HEAD. For the workflow of reading a SmartLink file, see Read. The same local data cache is used when reading the same file from HEAD and the next snapshot of HEAD simultaneously. This scenario does not cause the snapshot space to grow. The file in the snapshot directory uses its version of SmartLink file when updating HEAD and performing a write-back to the cloud like in scenario 1 or scenario 2. Users can read earlier versions of file data in the snapshot directory. The snapshot space could grow temporarily for cache data, and the grown space is released once its own cache expires.

Scenario 4

In this scenario, when updating HEAD (regular files in snapshot). A SmartLink file is used for HEAD, and a regular file is used for the same file in the next snapshot of HEAD. A new SmartLink file is generated for HEAD when updating HEAD and performing a write-back to the cloud. The cache for HEAD is empty once its own cache expires. Meanwhile, OneFS enables the Block Allocation Manager Cache Manager (BCM) on the regular file in the next snapshot of HEAD. BCM contains the metadata of mapping to cloud objects for the regular file in the next snapshot of HEAD. This scenario does not cause the snapshot space to grow.

The following figure shows scenario 4.

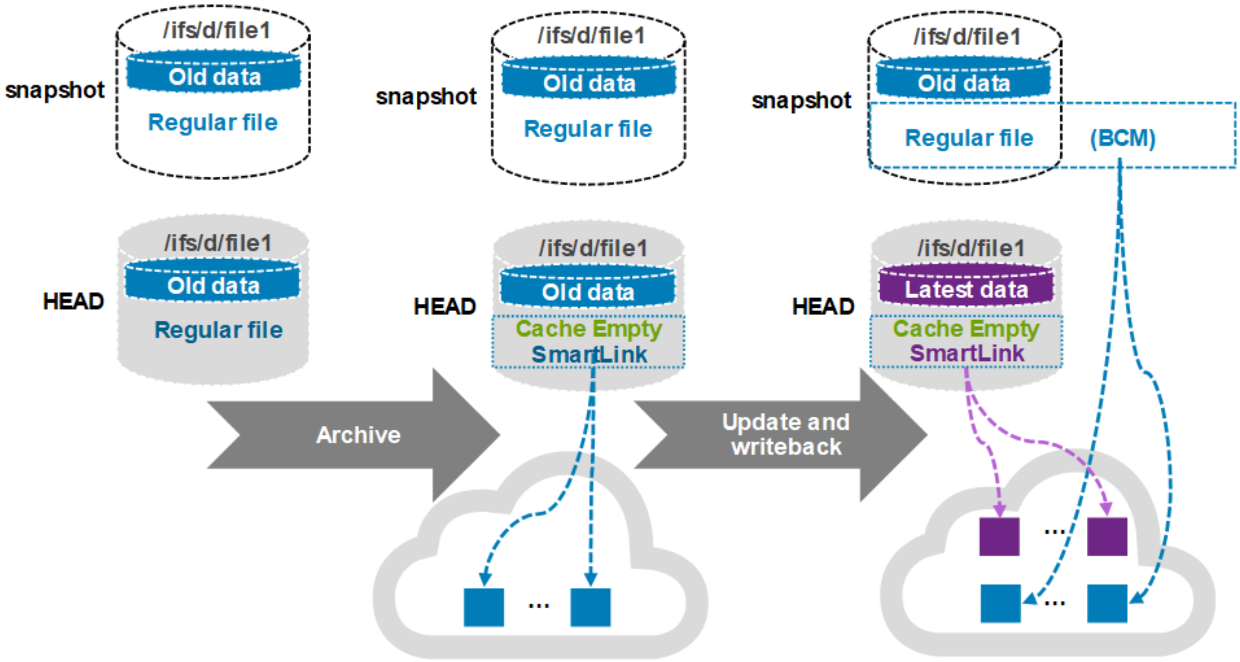


Figure 9. **Scenario 4: Update HEAD when regular files are in the snapshot directory**

Scenario 5

In this scenario, when reading file data from a snapshot (regular files in snapshot). File data is the same for HEAD (SmartLink file) and the same file (regular file) in the next snapshot of HEAD when not updating HEAD after the snapshot creation. File data is read from HEAD when reading the same file in the next snapshot of HEAD. This scenario does not cause the snapshot space to grow. The file in the next snapshot of HEAD is a regular file (enabled BCM). And the file has the earlier version of data when updating HEAD and performing a write-back to the cloud like in scenario 4. The earlier version of data is retrieved from the cloud by BCM. File data is stored on the PowerScale cluster when reading the earlier version of data from the regular file in the next snapshot of HEAD. The snapshot space grows, and the grown space is not released unless the snapshot is deleted.

Note: In OneFS 8.2.0, CloudPools 2.0 supports write-back in a snapshot. See Scenario 3 for details. However, CloudPools 2.0 does not support archiving and recalling files in the snapshot directory. Consider the case when there is already file data in a snapshot on a cluster running a OneFS release earlier than OneFS 8.2.0. That data takes up storage space on the PowerScale cluster, and then the cluster is upgraded to OneFS 8.2.0. Because CloudPools 2.0 does not support archiving files in snapshots to the cloud, the storage space for this snapshot cannot be released when the cluster is upgraded.

If SyncIQ or NDMP backs up the SmartLink files, the mapping file data should be retrieved from the cloud using the backup copy of the SmartLink file. If the backup retention has not expired, the CDOs of the mapping file data cannot be deleted even though the snapshot has been deleted. The reason is that the SmartLink file backup still references the CDOs of the mapping file data. When the backup retention period has expired and the CDOs of the mapping file data are no longer used, the CDOs of the mapping file data are deleted. For more information about data retention, see Data retention. If SyncIQ or NDMP does not back up SmartLink files, the CDOs of the mapping file data are deleted for SmartLink files after the snapshot is deleted.

Users can revert a snapshot or access snapshot data through the snapshots directory (/ifs/.snapshot). The main methods for restoring data from a snapshot are as follows:

- Revert a snapshot through the SnapRevert job.
- Restore a file or directory using Microsoft Shadow Copy Client on Windows or cp command on Linux.
- Clone a file from a snapshot (CloudPools does not support cloning a file from a snapshot).

For details on restoring snapshot data, see the administration guide OneFS 8.2.0 Web Administration Guide. CloudPools does not support cloning a file from a snapshot. The other two methods for restoring data from a snapshot in a CloudPools environment are described as follows.

When using the SnapRevert job to restore data from a snapshot, it reverts a directory back to the state it was in when a snapshot was taken. For example, there is a /ifs/test directory including a regular.txt regular file, and a smartlink.txt SmartLink file that has its file data archived to the cloud. A snap01 snapshot is created on the /ifs/test directory, and updates are made on the two files. The regular.txt file is then archived to the cloud, and it is truncated to a SmartLink file. Then, the SmartLink file smartlink.txt is recalled and it is converted to a regular file. If the snapshot snap01 is restored, it overwrites the files in directory /ifs/test. The regular.txt file reverts to a regular file, and the smartlink.txt reverts to a SmartLink file. The directory /ifs/test is reverted to the state it was in when snap01 was taken.

When using Microsoft Shadow Copy Client on Windows or the cp command on Linux, the file data is retrieved from the cloud through SmartLink files in a snapshot. This copy operation will create new regular files. That means extra space is required for the new regular files restored from a snapshot.

Sparse files handling

CloudPools 2.0 provides a new sparse file format to improve handling of empty blocks. With this improvement, sparse zeros are not in CloudPools operations, reducing network utilization and space on the cloud target.

Note: No cloud objects are written when archiving full sparse files (fully empty blocks).

Quota management

In OneFS 8.2.0, quotas present actual space consumed on the PowerScale cluster.

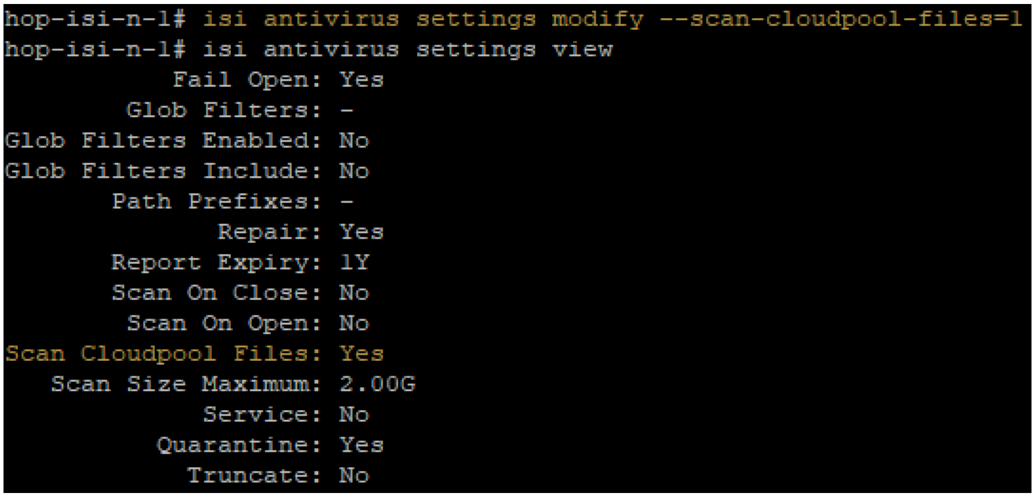
For example, there is a directory or user quota of 500 GB and it is reporting 400 GB used. 200 GB of files are archived from the PowerScale cluster to cloud. Moving data to the cloud reduces the quota's measured node space consumption. In OneFS releases earlier than 8.2.0, the amount of data that has been archived to the cloud frees the quota. And the quota shows 200 GB (400 GB to 200 GB) used out of 500 GB. That means the user or directory quota can exceed the set limit (500 GB). In OneFS 8.2.0, the application logical size integrated with CloudPools 2.0 measures the true capacity consumption even if data is archived from the PowerScale cluster to the cloud. And the quota shows 400 GB used out of 500 GB through the application logical size. That means the user or directory quota cannot exceed the set limit of 500 GB.

For more information about the new Dell PowerScale SmartQuotas reporting capabilities in OneFS 8.2.0, see the white paper Storage Quota Management and Provisioning with Dell PowerScale SmartQuotas.

Anti-virus integration

In OneFS releases earlier than OneFS 8.2.0, SmartLink files were skipped for anti-virus scanning.

In OneFS 8.2.0, CloudPools 2.0 provides a configurable option for anti-virus scanning of SmartLink files. The file data is retrieved from the cloud and cached on the cluster for the scan only if the option is enabled. The scan will be slower than normal. As shown in the following figure, the **Scan Cloudpool Files** option is configured and verified using the command line.



```
hop-isi-n-1# isi antivirus settings modify --scan-cloudpool-files=1
hop-isi-n-1# isi antivirus settings view
           Fail Open: Yes
        Glob Filters: -
Glob Filters Enabled: No
Glob Filters Include: No
       Path Prefixes: -
              Repair: Yes
       Report Expiry: 1Y
       Scan On Close: No
        Scan On Open: No
Scan Cloudpool Files: Yes
   Scan Size Maximum: 2.00G
             Service: No
          Quarantine: Yes
            Truncate: No
```

Figure 10. **Enable scanning of CloudPool files**

Note: The Scan Cloudpool Files option is disabled by default, which means SmartLink files are skipped when scanning a directory which includes SmartLink files.

WORM integration

Dell PowerScale SmartLock is an optional software feature of OneFS that enables SEC 17-a4 data compliance. In enterprise mode, individual directories can be set up as Write Once, Read Many (WORM) directories. And the data is immutable by everyone except the root account on the cluster once the files have been committed. A PowerScale cluster can also be set up in compliance mode where the root account on the cluster is removed. And no user can change or delete data in WORM-locked folders.

Before OneFS 8.2.0, SmartLink files were not allowed in both enterprise and compliance modes. In OneFS 8.2.0, CloudPools 2.0 and SmartLock integration is as follows:

- **Compliance mode**: SmartLink files are not allowed in compliance mode.
- **Enterprise mode**: SmartLink files are allowed in enterprise mode.
    - Enterprise mode can be enabled on a directory with SmartLink files.

- SmartLink files can be moved into an Enterprise mode directory which prevents modifying or deleting the SmartLink files.
- SmartLink files can be recalled from the cloud to the PowerScale cluster once they are committed.

Best practices for PowerScale storage and ECS

Introduction

This section focuses on the considerations and best practices for configuring CloudPools and ECS.

PowerScale configuration

This section includes considerations and best practices for configuring CloudPools.

CloudPools settings

CloudPools settings can be changed either on the CloudPools setting tab or on a per-file-pool policy from the OneFS WebUI. It is highly recommended to change these settings on a per-file-pool policy. The following list includes general considerations and best practices for CloudPools settings.

- **Encryption:** Encryption is an option that can be enabled either on the PowerScale cluster or on ECS. The recommendation is to enable encryption on the PowerScale cluster instead of on ECS. If the average CPU is high (greater than 70%) on the PowerScale cluster, the encryption can be enabled on ECS instead of on the PowerScale cluster. Encryption adds an additional load on the PowerScale cluster. Encryption can also impact the CloudPools archive and recall performance.
- **Compression:** Compression is an option that can be enabled on the PowerScale cluster, in which file data is compressed before sending it to ECS. ECS will automatically compress the file data if it has not already been compressed to optimize space utilization. If network bandwidth is a concern, the recommendation is to enable compression on the PowerScale cluster to save network resources. When the compression is disabled on the PowerScale cluster, ECS will automatically compress the file data. Compression adds an additional load on the PowerScale cluster which means it might take more time to archive files from PowerScale storage to ECS.
- **Data retention:** The recommendation is to explicitly set the data retention for the file data being archived from the PowerScale cluster to ECS. If the SmartLink files are backed up with SyncIQ or NDMP, the data retention defines how long the cloud objects remain on the ECS. Once the retention period has passed, the PowerScale cluster sends a delete command to ECS. The ECS marks the associated cloud objects for deletion. The delete process is asynchronous and the space is not reclaimed until garbage collection completes. This process is a low-priority background process, which might take days to fully reclaim the space depending on how busy the system is.
- **Local data cache:** If the storage space is limited on the PowerScale cluster, the recommendation is to set lower values for the Writeback Frequency and Cache Expiration. This option reduces the time to keep file data in the local data cache and frees up storage space sooner on the PowerScale cluster.

File pool policy

File pool policies define what data will be archived from the PowerScale cluster to ECS. Consider the following details about file pool policies:

- Ensure the priority of file pool policies is set appropriately. Multiple file pool policies can be created for the same cloud storage account. When the SmartPools job runs, it processes file pool policies in priority order.
- In terms of freeing up storage space on the PowerScale cluster, the recommendation is not to archive small files that are less than 32 KB in size.
- If the files need to be updated frequently, the recommendation is not to archive those files.
- Previous versions of OneFS 8.2.0, OneFS supports up to 128 file pool policies (SmartPools and CloudPools combined). OneFS 8.2.0 and later supports up to 256 file pool policies. The recommendation is not to exceed 30 file pool policies per PowerScale cluster.
- If the file pool policy is updated, it has no impact on the files already archived. It will only affect the files to be archived when the SmartPools job next runs.
- If multiple file pool policies are configured for CloudPools, it is recommended to configure the same number of CloudPools storage accounts, CloudPools on PowerScale, and replication groups on ECS. Each of the file pool policies targets a different bucket and keeps data separated.
- Archiving based on **Modified** or **Created times** rather than **Accessed time**, which results in files that are used often including applications, libraries and scripts. So, care should be taken to exclude these types of files from being archived to the cloud, which would result in delays for clients/users loading these applications. One example is archiving users' home directories and the home directories contain files that are created once but accessed often.

Other considerations

More considerations include:

- **Deduplication:** CloudPools can archive deduped files from a PowerScale cluster to cloud storage. However, un-deduped files will be created when recalling those files from the cloud to the PowerScale cluster. For more information about deduplication within OneFS, see the white paper Next Generation Storage Efficiency with Dell PowerScale SmartDedupe.
- **Small file storage efficiency (SFSE):** CloudPools and SFSE cannot work together. For PowerScale clusters using CloudPools, any SmartLink files cannot be containerized or packed. It is best practice to not archive small files that will be optimized using SFSE. The efficiencies gained from implementing SFSE for small files outweigh the storage advantages gained from archiving them to the cloud using CloudPools. For more information about the Small File Storage Efficiency feature of OneFS, see the white paper Dell PowerScale OneFS Storage Efficiency.
- **Network proxy:** When a PowerScale cluster cannot connect to the CloudPool storage target directly, network proxy servers can be configured for an alternate path to connect to the cloud storage.

- **SmartConnect:** If users access SmartLink files regularly through a specific node, clogging the inline access path might impact client performance. You can configure PowerScale SmartConnect for load-balancing connections for the cluster. For more information about SmartConnect, see the white paper Dell PowerScale Network Design Considerations.
- **Cloud storage account:** Do not delete a cloud storage account that is in use by archived files. Any attempt to open a SmartLink file associated with a deleted account will fail. In addition, NDMP backup and restore and SyncIQ failover and failback will fail when a cloud storage account has been deleted.
- **Cloud objects and data retention:** Cloud objects are crucial for SmartLink files. Any attempt to open a SmartLink file associated with deleted cloud objects will fail. OneFS checks data retention and the reference count for cloud objects before garbage collection. When data retention has expired and there is no reference count for cloud objects, cloud objects will be deleted through garbage collection. Data retention is a concept used to determine the Date of Death (DoD) setting for objects that support a SmartLink file. DoD is used to trigger garbage collection only if the reference count is zero for a file on the cluster only. The reference count is a concept used to determine whether cloud objects are associated with SmartLink files, including SmartLink files in the snapshots, SyncIQ backup, and NDMP backup. The considerations include:
    - Data retention periods include Cloud data retention period, Incremental backup retention period for NDMP incremental backup and SyncIQ, and Full backup retention period for NDMP only. If more than one period applies to a SmartLink file, the longest period is applied.
    - If a SmartLink file is unchanged through multiple SyncIQ backups or NDMP backups, its data retention will remain unchanged.
    - Data retention is set or updated on any event that changes the backed up version of a file or the state of the SmartLink file.
    - If a SmartLink file is changed and incrementally backed up, its data retention will be set by calculating the current time plus incremental backup retention period.
    - If a SmartLink file is recalled, the reference count will be removed, and its data retention will be set by calculating the current time plus cloud data retention period. Its cloud objects will be deleted through garbage collection after its data retention has expired.
    - If a SmartLink file is deleted, its data retention will be set by calculating the current time plus cloud data retention period. If cloud objects are still associated with snapshots, SyncIQ backup, or NDMP backup, its cloud objects will not be deleted through garbage collection after its data retention has expired.
- **OneFS upgrade (CloudPools 1.0 to CloudPools 2.0):** Before beginning the upgrade, check the OneFS CloudPools upgrade path information shown in the following table. See ECS configuration to ensure that proper configurations of DNS, Load balancer, ECS BaseURL, and CloudPools URI are accurate.

Table 3. OneFS CloudPools upgrade path

Installed OneFS version (CloudPools 1.0)	Upgrade to OneFS version (CloudPools 2.0)			
	8.2.0	8.2.1 with May 2020 RUPs	8.2.2 with May 2020 RUPs	9.x
8.0.x or 8.1.x	Strongly discouraged	OK if needed but recommend 8.2.2	Strongly recommended	Strongly recommended

Note: Contact your Dell representative if you plan to upgrade OneFS to 8.2.0.

In a SyncIQ environment with unidirectional replication, the SyncIQ target cluster should be upgraded before the source cluster. The reason is that OneFS allows the CloudPools-1.0-formatted SmartLink files to be converted into CloudPools-2.0-formatted SmartLink files through a post-upgrade SmartLink conversion process. Otherwise, SyncIQ policy need to be reconfigured to **deep copy** but deep copy will cause archived file content to read from the cloud and replicated. In a SyncIQ environment with bi-directional replication, it is recommended to disable SyncIQ on both source and target clusters and upgrade both source and target clusters simultaneously. You can then reenable SyncIQ on both source and target clusters once the OneFS upgrades have been committed on both source and target clusters. Depending on the number of SmartLink files on the target DR cluster and the processing power of that cluster, the SmartLink conversion process can take considerable time.

Note: No need to stop SyncIQ and Snapshot during the upgrade in a SyncIQ environment with unidirectional replication. SyncIQ must resynchronize all converted stub files, it might take SyncIQ some time to catch up with all the changes.

To check the status of the SmartLink upgrade process, run the following command, substituting the appropriate job number.

```
# isi cloud job view 6
              ID: 6
              Description: Update SmartLink file formats
              Effective State: running
             Type: smartlink-upgrade
             Operation State: running
             Job State: running
             Create Time: 2019-08-23T14:20:26
         State Change Time: 2019-09-17T09:56:08
         Completion Time: -
         Job Engine Job: -
         Job Engine State: -
         Total Files: 21907433
         Total Canceled: 0
         Total Failed: 61
         Total Pending: 318672
         Total Staged: 0
         Total Processing: 48
         Total Succeeded: 21588652
```

Note: CloudPools recall jobs will not run while SmartLink upgrade or conversion is in progress.

For Not All Nodes on Network (NANON) cluster, it is recommended to get the unconnected nodes connected to the network before starting the SmartLink conversion. Also, you need disable SnapDelete until the SmartLink conversion is completed.

ECS configuration

Before configuring CloudPools on a PowerScale cluster, the ECS environment needs to be configured properly. The ECS S3 interface that CloudPools uses is backwards compatible with previous versions of ECS. Therefore, customers can upgrade their ECS versions and CloudPools will continue to function normally if the OneFS version stays the same.

General considerations and best practices when configuring ECS for CloudPools include:

- **Virtual data center (VDC):** If the cloud data needs to be protected using ECS Geo-replication, see Protecting cloud data. Multiple VDC should be created and federated together.
- **Replication group:** The option *Replicate to All Sites* need to be configured appropriately when creating replication group. This option cannot be changed after the replication has been created.
- **Namespace:** Namespace creation is exclusively for CloudPools. The following options must be considered.
    - **Server-side encryption:** The encryption needs to be configured appropriately when creating the namespace. This option cannot be changed after the namespace is created.

  - **Replication group:** The Replication Group needs to be configured appropriately when creating the namespace. This option cannot be changed after the namespace is created. The default replication group is selected by default.
  - **Retention policy:** The retention period should not be created on the namespace. The best practice is to set the data retention in the file pool policy on the PowerScale cluster.
  - **Namespace Quota and Default Bucket Quota**: The quota should not be enabled.
  - **Access during outage (ADO):** For Geo-replication, ensure Access During Outage is enabled.

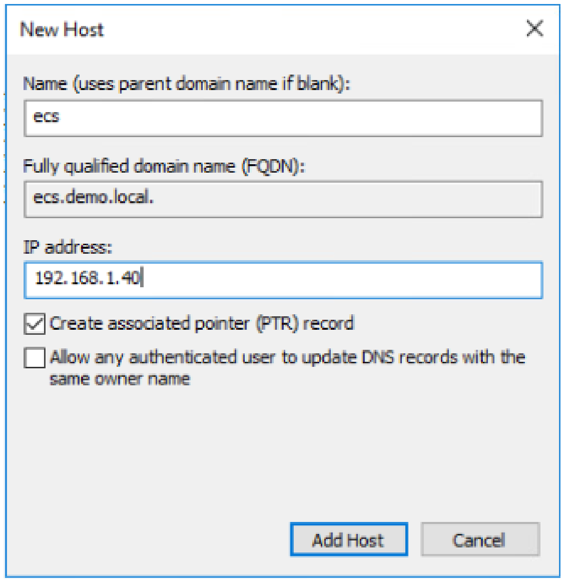
- **Bucket:** The retention period should not be created on a bucket. The best practice is to set the data retention in the file pool policy on the PowerScale cluster.
- **Base URL:** CloudPools 2.0 uses virtual host style bucket addressing by default. For virtual host style, see the ECS Administrator's Guide. A base URL needs to be created on ECS for the virtual host style bucket addressing. The base URL should be the FQDN of the CNAME (alias) for the load balancer virtual IP (VIP) and used for CloudPools URI.
- **Load balancer:** A hardware or software load balancer can evenly distribute the load across all ECS nodes. The Load balancer VIP must have a DNS entry to resolve the virtual host style address. A CNAME and wildcard and an A record need to be created on the DNS servers for the load balancer VIP. The procedure for configuring DNS depends on your DNS server or DNS provider. For example, DNS is set up on a Windows server, Table 4 and Table 5 show the DNS entries created for ECS. Sample screenshots of this configuration are shown in Figure 11 and Figure 12.

Table 4. An A record example

Name	Record type	FQDN	IP address	Comment
ecs	A	ecs.demo.local	192.168.1.10	The FQDN of the load balancer is ecs.demo.local.

Table 5. A CNAME and wildcard entry

Name	Record type	FQDN	FQDN for target host	Comment
cloudpools_uri	CNAME	cloudpools_uri.demo.local	ecs.demo.local	If you create an SSL certificate for the ECS S3 service, it must have the wildcard entry on the name of the certificate. And the non-wildcard version as a Subject Alternate Name.
*.cloudpools_uri	CNAME	*.cloudpools_uri.demo.local	ecs.demo.local	This option is used for virtual host addressing for a bucket. For example: mybucket.ecs.demo.local



New Host

Name (uses parent domain name if blank): ecs

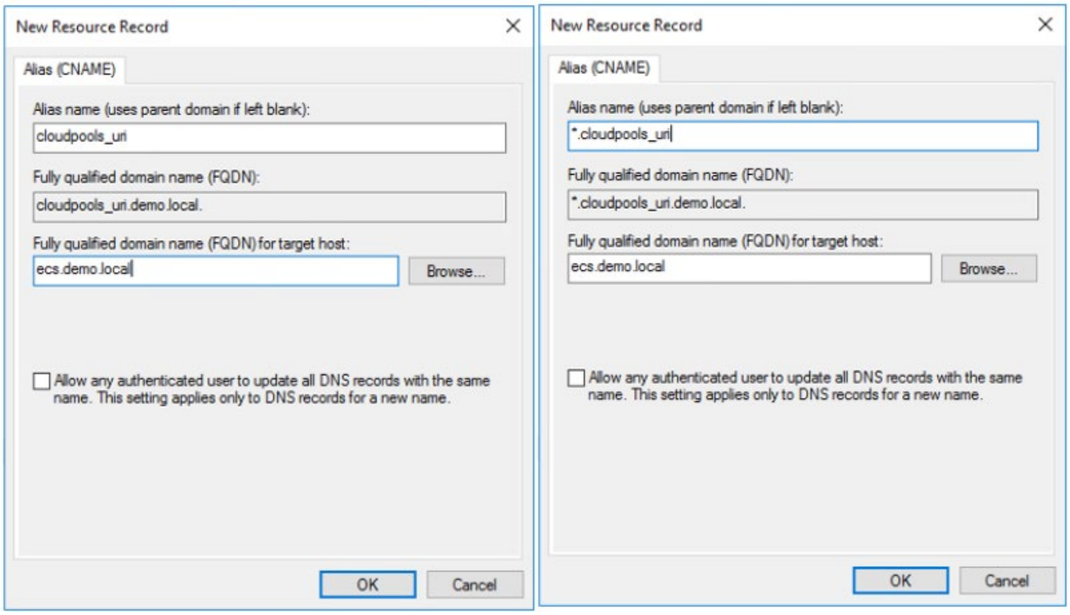
Fully qualified domain name (FQDN): ecs.demo.local.

IP address: 192.168.1.40

☑ Create associated pointer (PTR) record

□ Allow any authenticated user to update DNS records with the same owner name

Figure 11. **An A record**



New Resource Record

Alias (CNAME)

Alias name (uses parent domain if left blank): cloudpools_uri

Fully qualified domain name (FQDN): cloudpools_uri.demo.local.

Fully qualified domain name (FQDN) for target host: ecs.demo.local

□ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

New Resource Record

Alias (CNAME)

Alias name (uses parent domain if left blank): *.cloudpools_uri

Fully qualified domain name (FQDN): *.cloudpools_uri.demo.local.

Fully qualified domain name (FQDN) for target host: ecs.demo.local

□ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

Figure 12. **A CNAME and wildcard DNS entry**

Note: A load balancer is a must for CloudPools 2.0 and ECS.

Protecting SmartLink files

SmartLink files are the sole means to access file data stored in ECS, so ensure that you protect them from accidental deletion.

This section discusses using SyncIQ and NDMP to back up SmartLink files.

Note: SmartLink files cannot be backed up using a copy command, such as secure copy (scp).

SyncIQ

SyncIQ is CloudPools-aware but consider the guidance in Snapshot efficiency, especially where snapshot retention periods on the target cluster will be long.

SyncIQ policies support two types of data replication for CloudPools:

- **Shallow copy:** This option is used to replicate files as SmartLink files without file data from source PowerScale cluster to target PowerScale cluster.
- **Deep copy:** This option is used to replicate files as regular files or unarchived files from source PowerScale cluster to target PowerScale cluster.

For information about cross-version compatibility of CloudPools, see NDMP and SyncIQ support.

SyncIQ, SmartPools, and CloudPools licenses are required on both the source and target PowerScale cluster. It is highly recommended to setup a scheduled SyncIQ backup of the SmartLink files. For more information about SyncIQ, see the white paper Dell PowerScale SyncIQ: Architecture, Configuration, and Considerations.

When SyncIQ replicates SmartLink files, it also replicates the local cache state and unsynchronized cache data from the source PowerScale cluster to the target PowerScale cluster. Figure 13 shows the SyncIQ replication when replicating directories including SmartLink files and unarchived normal files. Both unidirectional and bi-directional replication are supported. Appendix A: Step-by-step configuration example provides steps for failing over to a secondary PowerScale cluster and failing back to a primary PowerScale cluster.

Note: OneFS manages cloud access at the cluster level and does not support managing cloud access at the directory level. You need to remove cloud access on the source cluster and add cloud access on the target cluster when failing over a SyncIQ directory containing SmartLink files to a target cluster. If there are multiple CloudPools storage accounts, removing/adding cloud access will impact all CloudPools storage accounts on the source/target cluster.

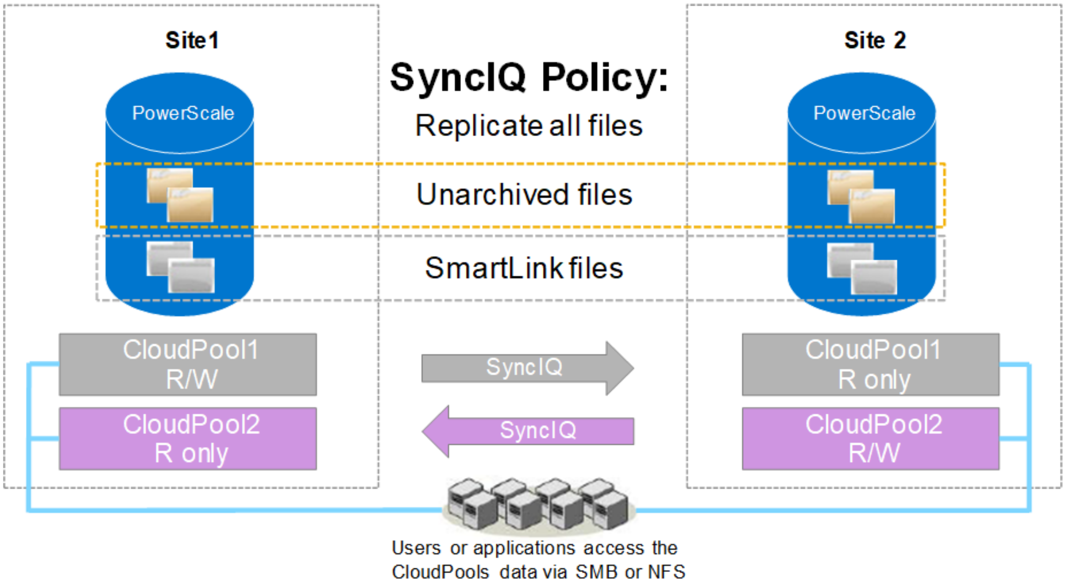


Figure 13. **SyncIQ replication**

Note: If encryption is enabled in a file pool policy for CloudPools, SyncIQ also replicates all the relevant encryption keys to the secondary PowerScale cluster along with the SmartLink files.

NDMP

NDMP is also CloudPools-aware and supports three backup and restore methods for CloudPools:

- **DeepCopy:** This option is used to back up files as regular files or unarchived files. Files can only be restored as regular files.
- **ShallowCopy:** This option is used to back up files as SmartLink files without file data. Files can only be restored as SmartLink files.
- **ComboCopy:** This option is used to back up files as SmartLink files with file data. Files can be restored as regular files or SmartLink files.

For information about cross-version compatibility of CloudPools, see NDMP and SyncIQ support.

It is possible to update the file data and send the updated data to the cloud storage. Multiple version SmartLink files can be backed up to tapes using NDMP, and multiple versions of CDOs are protected on ECS under the data retention setting. You can restore a specific version of a SmartLink file from tapes to a PowerScale cluster and continue to access (read or update) the file like before.

Note: If encryption is enabled in the file pool policy for CloudPools, NDMP also backs up all the relevant encryption keys to tapes along with the SmartLink files.

Protecting cloud data

ECS supports geo-replication which provides access to the cloud data from multiple sites. Geo-replication requires:

- More than one ECS federated together
- A replication group configured with more than one VDC
- A namespace is configured for CloudPools which uses the replication group with more than one VDC

When files have been archived from a PowerScale cluster to ECS, the cloud data will automatically be replicated to another ECS asynchronously. As shown in the following figure, ECS geo-replication works together with CloudPools.

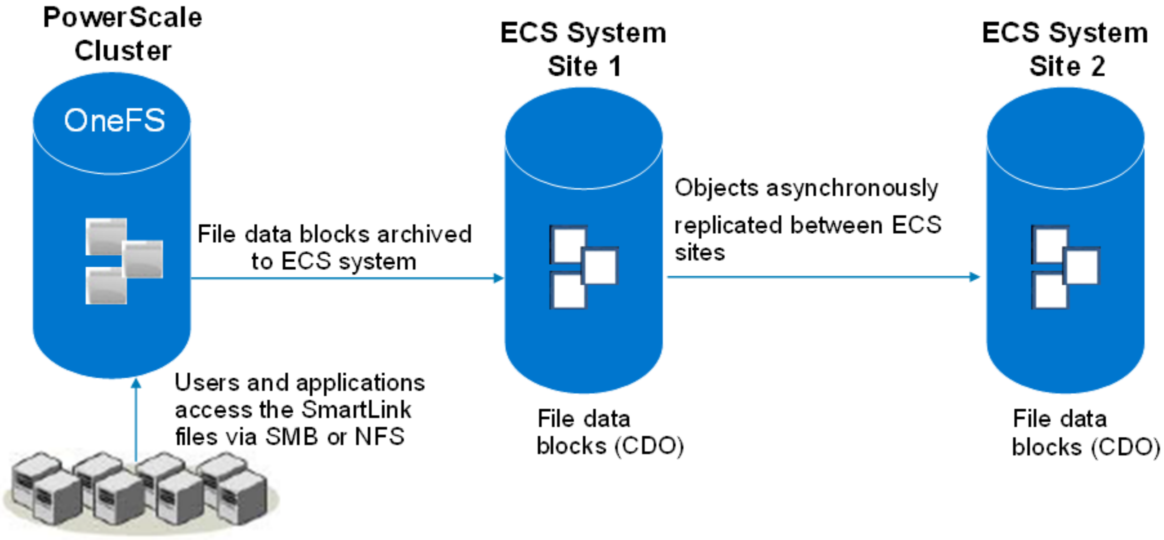

PowerScale Cluster
OneFS
ECS System Site 1
ECS System Site 2
File data blocks archived to ECS system
Objects asynchronously replicated between ECS sites
Users and applications access the SmartLink files via SMB or NFS
File data blocks (CDO)
File data blocks (CDO)

Figure 14. **ECS geo-replication works together with CloudPools**

Note: Cloud data is compressed when replicating the data from one ECS to another. Any encrypted data will remain encrypted when replicating the data.

It is recommended to enable Access During Outage (ADO) on the CloudPools buckets and configure a load balancer for the primary and secondary ECS. This configuration help you continue to access cloud data when the primary ECS has an outage. If the primary ECS comes back, any changes will be asynchronously replicated back to the primary ECS.

For the steps on failover to secondary ECS and failback to primary ECS, see Appendix A: Step-by-step configuration example.

Combining SyncIQ with ECS Geo-Replication

SyncIQ and ECS Geo-Replication work together to protect your data access in the event you have a site-wide failure. Also, the site contains both the PowerScale and ECS primary systems as illustrated in the following figure.

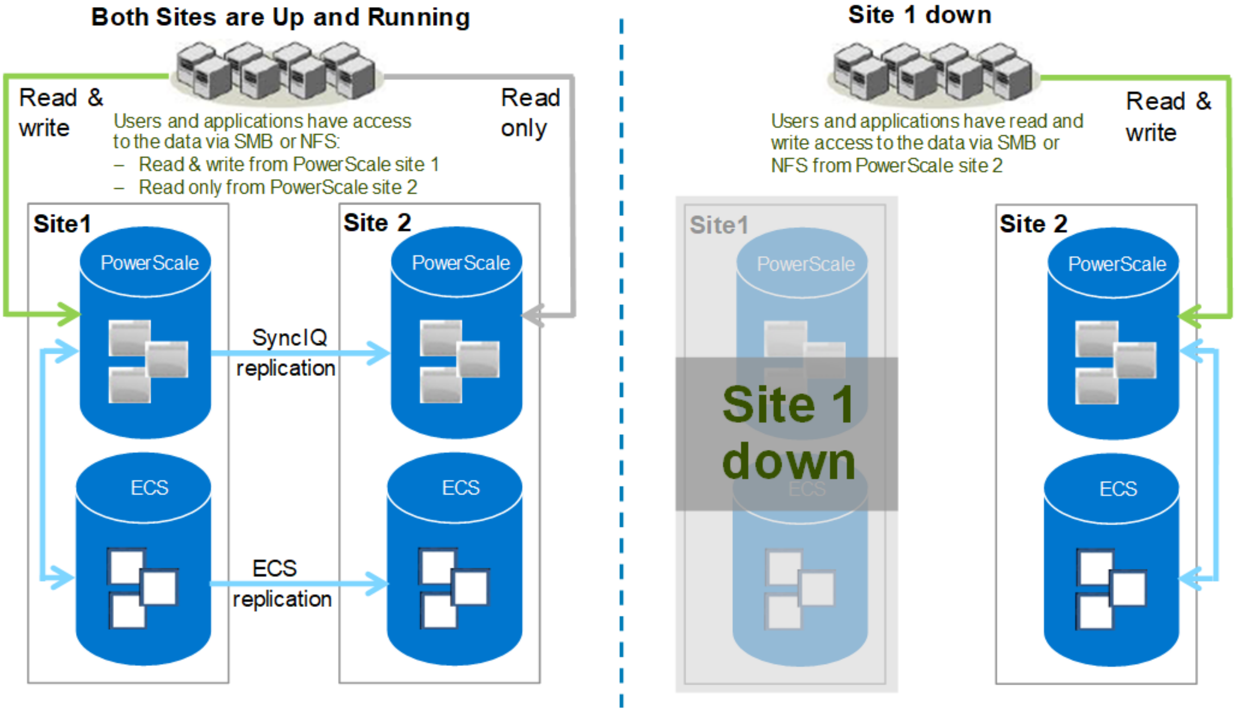

Both Sites are Up and Running
Read & write
Users and applications have access to the data via SMB or NFS:
– Read & write from PowerScale site 1
– Read only from PowerScale site 2
Read only
Site1
Site 2
PowerScale
PowerScale
SyncIQ replication
ECS
ECS
ECS replication
Site 1 down
Users and applications have read and write access to the data via SMB or NFS from PowerScale site 2
Read & write
Site1
PowerScale
Site 1 down
ECS
Site 2
PowerScale
ECS

Figure 15. **Data Remains Accessible After Site-Wide Failure of Both ECS System and PowerScale Cluster**

You can use SyncIQ and ECS Replication Group to configure a multisite architecture, with each site replicating to the other site. The following figure shows an example of a two-site configuration whereby each site has a PowerScale cluster and ECS system that replicate to each other.

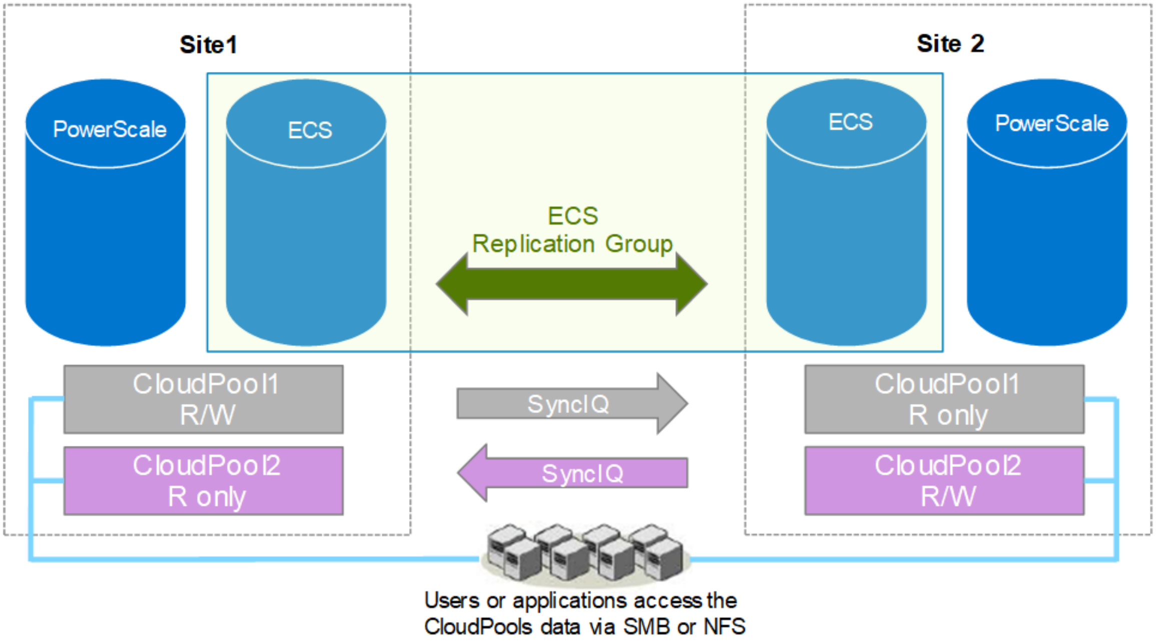


Figure 16. **Two Site CloudPools and SyncIQ Configuration**

In this configuration, CloudPool1 tiers data from Site1 PowerScale cluster to Site1 ECS system. Similarly, Site2 has a CloudPool2 that tiers data to its local ECS system. It then uses SyncIQ and the ECS replication group to replicate data between sites. It is strongly recommended that the OneFS version of Site1 and Site2 are consistent. If the OneFS versions of Site1 and Site2 are not consistent, see NDMP and SyncIQ support. In this scenario, all data access is performed locally. If there is a site-wide failure, fail over operations can make both CloudPool1 and CloudPool2 data available from the available site.

Performance

CloudPools is designed to move cold data from primary storage to the cloud. It is deliberately slow to ensure that it does not compete with things that are performance sensitive like SMB and NFS user activity. By default, CloudPools is using 10 threads per node which balances CloudPools CPU usage with other cluster functions. It is recommended to use the default number of threads for typical workloads. CloudPools does provide an option to modify the number of archive and recall threads. However, modifying the number of archive and recall threads can improve archive and recall performance but can also have significant impact on the CPU load of your system.

Here is as an example, the test is archiving and recalling 1 GB files between a four node Dell Isilon H500 cluster. The H500 cluster is connected using a physical server load balancer to a five node Dell ECS EX300 system. All equipment is connected on the same 10-Gigabit Ethernet network. With this configuration, it achieves ~ 261 MB/s (~ 65 MB/s per H500 node) for archive. It achieves ~702 MB/s (~ 175 MB/s per H500 node) for recall throughput of 1 GB files. The results are based on ideal test scenarios where there is no other load was on the systems or network. Typical environments would have additional loads on the systems, and so there will have different performance results.

Note: Contact your Dell representative if you want to configure higher number of threads.

CloudPools archive and recall performance are highly dependent upon many factors, such as the network bandwidth between the PowerScale cluster and the ECS system, available system resources and file size. These performance considerations would be:

- The CloudPools archive and recall performance have increased as the file size increases. However, it has minor effect on archive when file size is greater than or equal to 10 MB. It has negligible effect on recall when file size is greater than or equal to 10 MB.
- The CloudPools archive and recall performance have increased as the thread counts increase. However, it has negligible effect on archive and recall when the number of threads per PowerScale node is greater than or equal to 40.
- For a single large file, it has negligible effect on archive and recall regardless of the file size or number of threads per node. A single thread manages a single file transfer on a single node.
- Starting from OneFS 9.3.0.0, CloudPools creates Likewise sparks to drive the read of each CDO from the cloud. This enhancement can cache multiple chunks or CDOs of a stub file concurrently to improve CloudPools read and recall performance.
- It has negligible effect on archive and recall performance regardless of number of file pool policies or jobs.
- With the expansion of PowerScale nodes, CloudPools archive and recall performance has increased, but not linearly.
- CloudPools archive and recall performance have increased as the ECS appliance becomes more powerful.
- For a single, heterogeneous cluster, it has a minor impact on CloudPools archive performance, and a large impact on CloudPools recall performance. The archive and recall performance are better when data is stored in the tier 1 node pool. The setting **Data Storage Target** of a file pool policy can determine the node pool for recall. However, the node pool cannot be changed for inline read. The node pool for a stub is used for inline read for this stub.
- Not All Nodes on Network (NANON) cluster has a large impact on CloudPools archive and recall performance.

Reporting

Introduction

This section describes reporting for CloudPools network stats and includes the following topics:

- CloudPools network stats
- Query network stats by CloudPools account

- Query network stats by file pool policy
- Query history network stats
- Cloud statistics namespace with CloudPools

CloudPools network stats

CloudPools network stats collect every network transaction and provide network activity statistics from connections to the cloud storage. The network activity statistics include bytes In, bytes Out, and the number of GET, PUT, and DELETE operations. CloudPools network stats are available in two categories:

- Per CloudPools account
- Per file pool policy

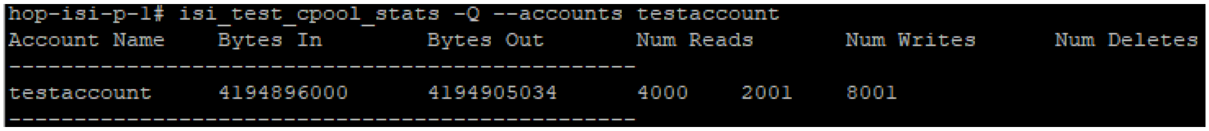
Note: CloudPools network stats do not provide file statistics, such as the file list being archived or recalled.

Query network stats by CloudPools account

Run the following command to check the CloudPools network stats by CloudPools account.

```
isi_test_cpool_stats -Q --accounts <account_name>
```

The following figure shows an example of current CloudPools network stats by CloudPools account.



```
hop-isi-p-1# isi_test_cpool_stats -Q --accounts testaccount
Account Name    Bytes In        Bytes Out       Num Reads       Num Writes      Num Deletes
------------------------------------------------
testaccount     4194896000      4194905034      4000    2001    8001
------------------------------------------------
```

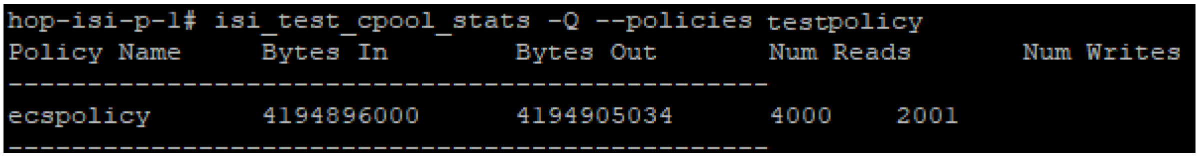
Figure 17. **Network stats by CloudPools account**

Query network stats by file pool policy

Run the following command to check the CloudPools network stats by file pool policy.

```
isi_test_cpool_stats -Q --policies <policy_name>
```

The following figure shows an example of current CloudPools network stats by file pool policy.



```
hop-isi-p-1# isi_test_cpool_stats -Q --policies testpolicy
Policy Name     Bytes In        Bytes Out       Num Reads       Num Writes
------------------------------------------------
ecspolicy       4194896000      4194905034      4000    2001
------------------------------------------------
```

Figure 18. **Network stats by file pool policy**

Note: The command output does not include the number of deletes by file pool policy.

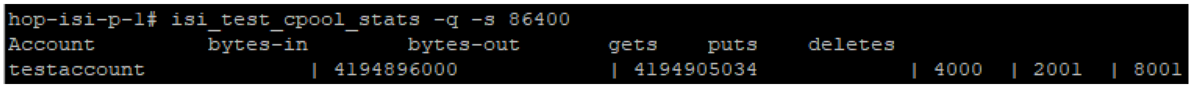
Query history network stats

Run the following command to check the history CloudPools network stats.

```
isi_test_cpool_stats -q -s <number of seconds in the past to start
stat query>
```

Use the **s** parameter to define the number of seconds in the past. For example, set it as 86,400 to query CloudPools network stats over the last day.

The following figure shows an example of CloudPools network stats over the last day.



```
hop-isi-p-1# isi_test_cpool_stats -q -s 86400
Account         bytes-in        bytes-out       gets    puts    deletes
testaccount             | 4194896000            | 4194905034            | 4000  | 2001  | 8001
```

Figure 19. **Network stats last day**

Run the following command to flush stats from memory to database and get the latest CloudPools history network stats.

```
isi_test_cpool_stats -f
```

Cloud statistics namespace with CloudPools

The cloud statistics namespace with CloudPools is added in OneFS 9.4.0.0. This feature leverages existing OneFS daemons and systems to track statistics about CloudPools activities. The statistics include bytes In, bytes Out, and the number of Reads, Writes, and Deletions. CloudPools statistics are available in two categories:

- Per CloudPools account
- Per file pool policy

Note: The cloud statistics namespace with CloudPools do not provide file statistics, such as the file list being archived or recalled.

You can run the **isi statistics cloud** command to view statistics about CloudPools activities. For more information about **isi statistics cloud** command, see the document PowerScale OneFS 9.4.0.0 CLI Command Reference.

Commands and troubleshooting

Introduction

This section describes CloudPools commands and troubleshooting methodologies.

Commands

This CloudPools operations and job monitoring commands discussed in this section include:

- CloudPools archive
- CloudPools recall
- CloudPools monitoring

CloudPools archive

Run the following command to archive files from a PowerScale cluster to the cloud on demand.

```
isi cloud archive <file name> --recursive [true | false] --policy
<policy name>
```

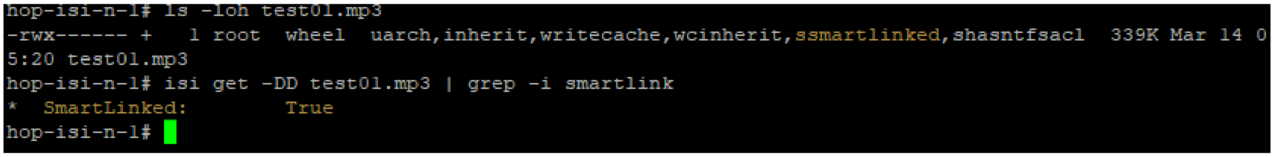
Parameters:

- **<file name>:** File name to be archived

- **--recursive:** Whether the archive should apply recursively to nested directories
- **--policy:** Policy name to be used with archiving

Run either of the following two commands to check whether the file is a SmartLink file or not, as shown in Figure 20.

```
ls -loh <file name>
isi get -DD <file name> | grep -i smartlink
```



```
hop-isi-n-1# ls -loh test01.mp3
-rwx------ +   1 root  wheel  uarch,inherit,writecache,wcinherit,ssmartlinked,shasntfsacl  339K Mar 14 0
5:20 test01.mp3
hop-isi-n-1# isi get -DD test01.mp3 | grep -i smartlink
*  SmartLinked:        True
hop-isi-n-1#
```

Figure 20. **SmartLink file**

CloudPools recall

Run the following command to recall files from the cloud to a PowerScale cluster on demand.

```
isi cloud recall <files> --recursive [true | false]
```

Parameters:

- **<file name>:** File name to be archived
- **--recursive:** Whether the archive should apply recursively to nested directories

CloudPools job monitoring

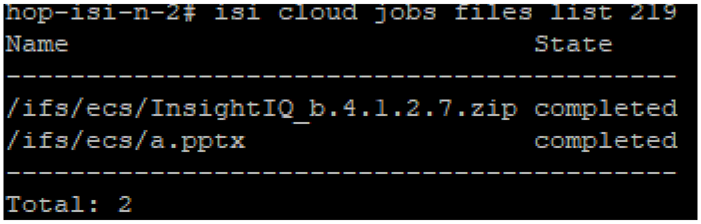
To check the CloudPools job status, run the following command.

```
isi cloud jobs list
```

To check the archive or recall file list status for a specific CloudPools job, run the following command.

```
isi cloud jobs files list <job id>
```

As shown in Figure 21, the job id can be found by running the command `isi cloud jobs list`.



```
hop-isi-n-2# isi cloud jobs files list 219
Name                               State
-------------------------------------------
/ifs/ecs/InsightIQ_b.4.1.2.7.zip completed
/ifs/ecs/a.pptx                    completed
-------------------------------------------
Total: 2
```

Figure 21. **File list of specific CloudPools job**

Note: The output of `isi cloud jobs files list <job id>` shows only the file name and state for specific CloudPools jobs.

To perform additional actions, run the following commands:

- Pause a CloudPools job:

  ```
  isi cloud jobs pause <job id>
  ```

- Resume a paused CloudPools job:

  ```
  isi cloud jobs resume <job id>
  ```

- Cancel a CloudPools job:

  ```
  isi cloud jobs cancel <job id>
  ```

- Check the file list state of writing updated data to the cloud (job id is 1), which is an internal CloudPools job and always running:

  ```
  isi cloud jobs files list 1
  ```

Note: The CloudPools system jobs should not be paused except temporarily for troubleshooting. No jobs should be left paused for an indefinite time.

Troubleshooting

This section describes various CloudPools troubleshooting methodologies, which include:

- CloudPools state
- CloudPools logs

CloudPools state

To check the CloudPools storage account state, use the following command:

```
isi cloud accounts view <cloudpools storage account name>
```

To check the CloudPool state, run the following command:

```
isi cloud pools view <cloud pool name>
```

To check the file pool policy state, run the following command:

```
isi filepool policies view <filepool policy name>
```

CloudPools logs

Check the CloudPools log if needed. The location of CloudPools logs is as follows:

- Most normal daemon log is at /var/log/isi_cpool_d.log
- The log of IO to the cloud is at /var/log/isi_cpool_io_d.log
- Key management log is at /var/log/isi_km_d.log

CloudPools job (Job Engine) log is at `/var/log/isi_job_d.log`

Appendix A: Step-by-step configuration example

Introduction

This appendix describes a step-by-step configuration example for CloudPools and ECS and includes the following topics:

- ECS configuration
- Load Balancer configuration
- PowerScale configuration
- SmartLink files and cloud data protection

ECS configuration

This section describes the ECS configuration for CloudPools, which includes:

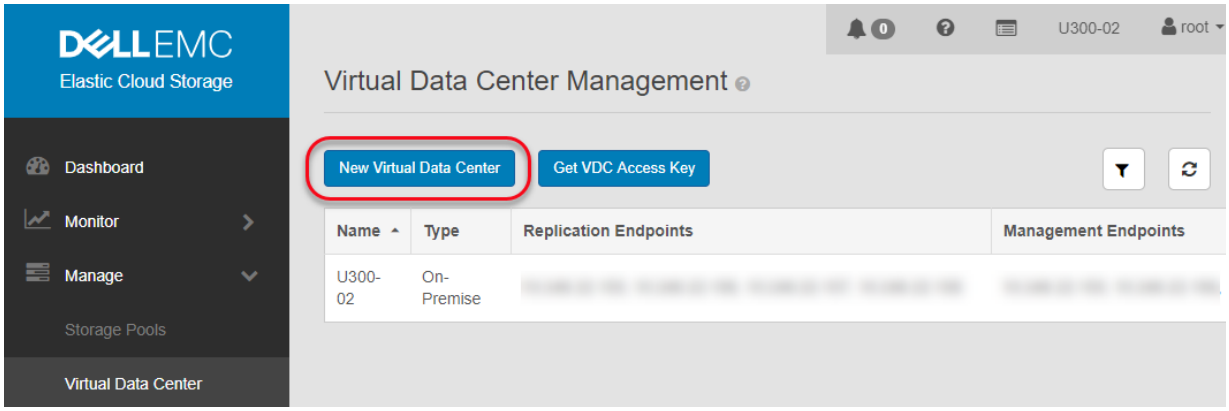
- Virtual data center creation
- Replication group creation
- Namespace creation
- Object user creation
- Base URL creation

The example ECS configuration is a general guide when ECS is used for CloudPools. It does not cover all details of ECS configuration for other use cases. Consult the ECS Administrator's Guide for more details on ECS configuration.

Virtual data center

This section describes the steps how to create a Virtual Data Center on ECS.

1. Log in to the ECS portal, go to **Manage** > **Virtual Data Center,** and click **New Virtual Data Center** as shown in the following figure.



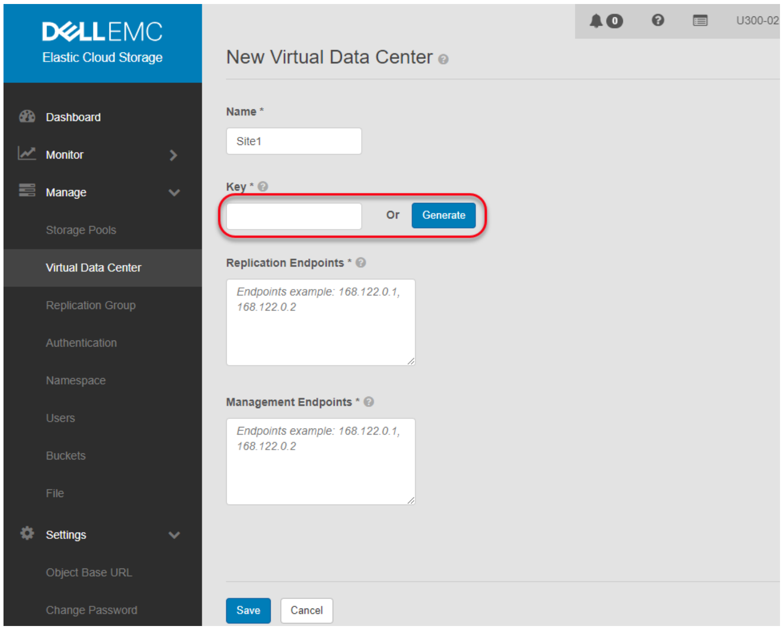
Name	Type	Replication Endpoints	Management Endpoints
U300-02	On-Premise	[redacted]	[redacted]

Figure 22. **New Virtual Data Center**

2. From the **New Virtual Data Center** page as shown in Figure 23, the minimum information is as follows:

   - **Name**: Type a name to identify the virtual data center.
   - **Key**: Type a key or generate a new key.
   - **Replication and Management endpoints**: The endpoints should contain a comma-separated listing of each node’s IP address. This option can either be

the node's public IP address or a separate replication or management network for each node. If network separation is not configured, both replication and management endpoints will be the same.



New Virtual Data Center

Name *: Site1

Key *: Or Generate

Replication Endpoints *: Endpoints example: 168.122.0.1, 168.122.0.2

Management Endpoints *: Endpoints example: 168.122.0.1, 168.122.0.2

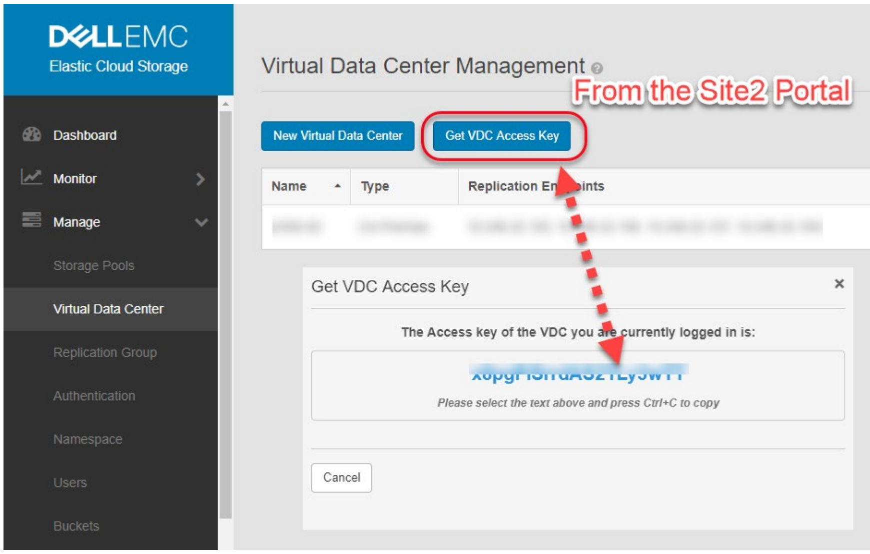
Save Cancel

Figure 23. **New Virtual Data Center page**

3. Click **Save** to create a new virtual data center.

If you want the cloud data to be replicated to a second site, you have to setup multiple virtual data centers (VDC) that are federated together. The steps to create multiple VDCs are as follows.

1. Log in to the **second** ECS portal and go to **Manage** > **Virtual Data Center**. Select **Get VDC Access Key** as shown in the following figure and copy the **VDC Access Key.** You will need it in the next step. Also make note of the second site's replication and management IP addresses.



Virtual Data Center Management

Name	Type	Replication Endpoints
[redacted]	[redacted]	[redacted]

Get VDC Access Key

The Access key of the VDC you are currently logged in is:

[redacted]

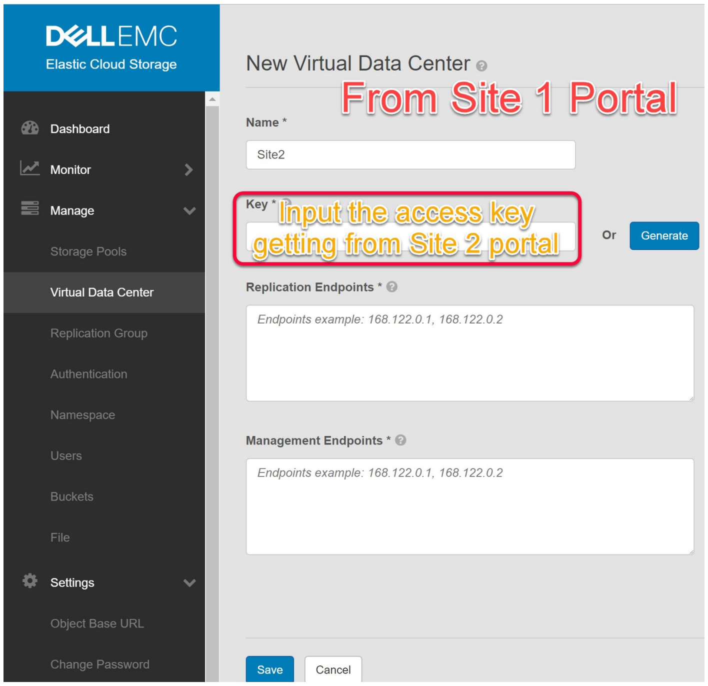
Please select the text above and press Ctrl+C to copy

Cancel

Figure 24. **Get VDC Access Key from the Second ECS**

2. Log in to the **primary** ECS portal and go to **Manage** > **Virtual Data Center.** Select **New Virtual Data Center** as shown in Figure 25. The minimum information is as follows:

   - **Name:** Type a name to identify the virtual data center.
   - **Key**: Type the key copied from the second ECS portal in step 1.
   - **Replication and Management endpoints**: The endpoints should contain a comma-separated listing of each node in the second site's IP address. This option can either be the node's public IP address or if a separate replication or management network for each node. If network separation is not configured, both replication and management endpoints will be the same.



New Virtual Data Center

From Site 1 Portal

Name *: Site2

Key *

Input the access key getting from Site 2 portal

Replication Endpoints *: *Endpoints example: 168.122.0.1, 168.122.0.2*

Management Endpoints *: *Endpoints example: 168.122.0.1, 168.122.0.2*

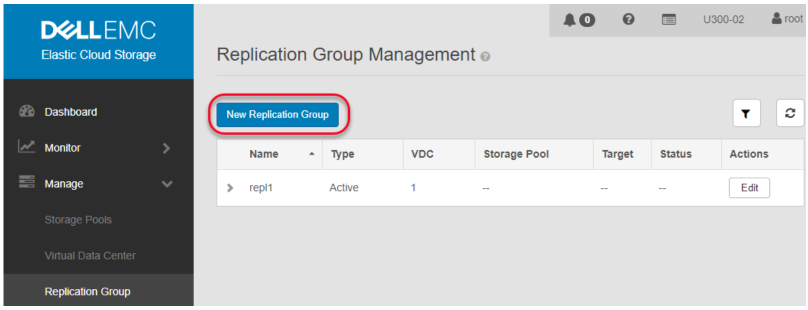
Figure 25. **Create a VDC on primary ECS**

3. Click **Save** to create a new virtual data center.

Replication group

This section describes the steps how to create replication group on ECS.

1. Log in to the ECS portal and go to **Manage** > **Replication Group**. Click the **New Replication Group** button as shown in the following figure.

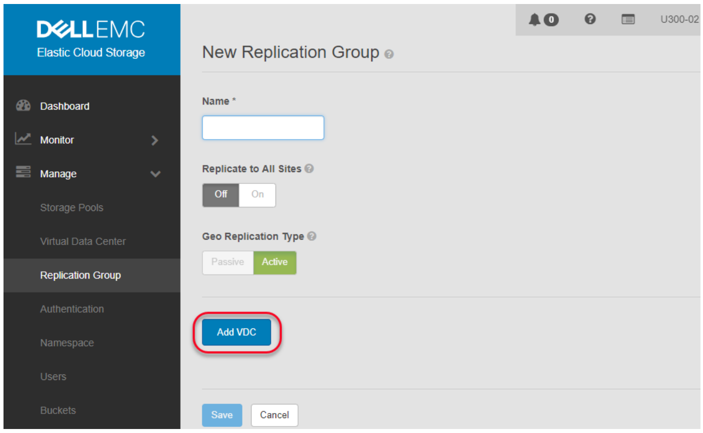


Replication Group Management

Name	Type	VDC	Storage Pool	Target	Status	Actions
repl1	Active	1	--	--	--	Edit

Figure 26. **New Replication Group**

2. From the **New Replication Group** page as shown in Figure 27, the minimum information is as follows:
   - **Name**: Type a name to identify the replication group.
   - **Replicate to All Site**: Select the replication level preference by enabling or disabling "Replicate to All Sites":
     - **Enable**: This option is used to replicate data to all sites or VDCs in the replication group. If your replication group has four sites that would mean four copies are stored, one at each site. This option offers the highest data durability but has the lowest space efficiency.
     - **Disable**: This option is used to maintain one additional copy of data at another site. Regardless of the number of sites you will always have two copies of the data.
   - **Add VDC**: The setting is ignored for single site replication groups. Add the appropriate virtual data centers and storage pools.



New Replication Group

Name *

Replicate to All Sites: Off [✓ Off] On

Geo Replication Type: Passive [✓ Active]

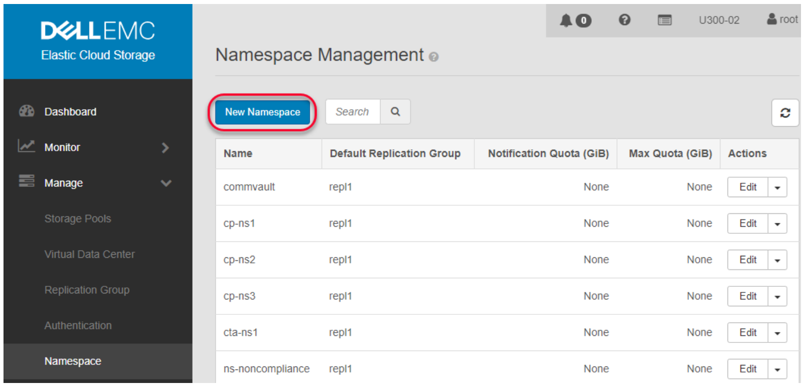
Figure 27. **Configure New Replication Group**

3. Click **Save** to create a replication group.

Namespace

This section describes the steps how to create a namespace on ECS.

1. Log in to the ECS portal, go to **Manage** > **Namespace,** and click **New Namespace** as shown in the following figure.



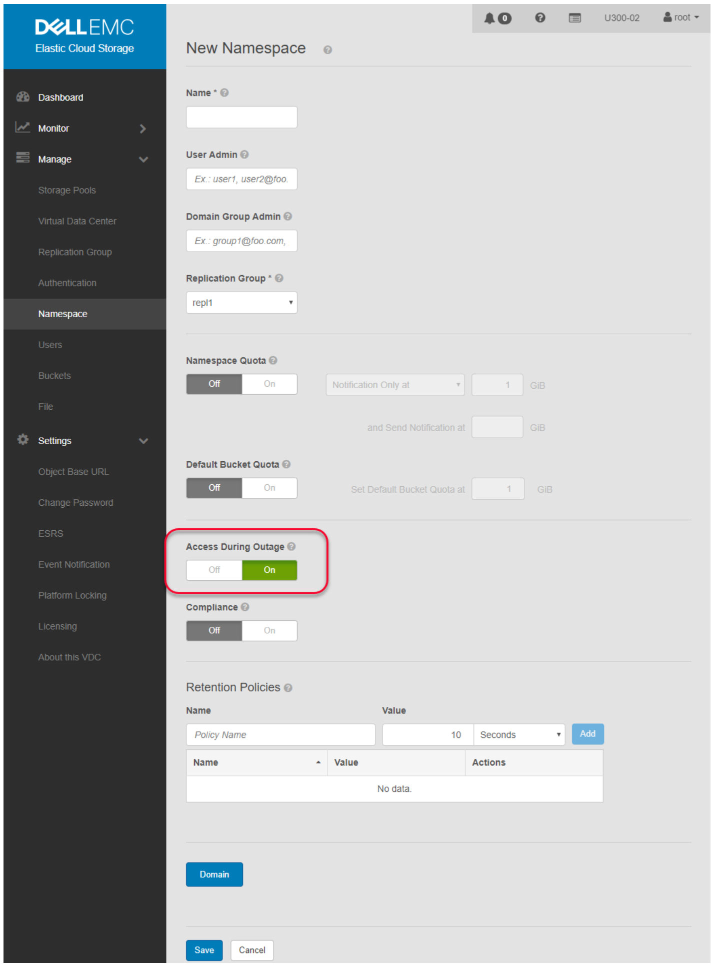
Namespace Management

Name	Default Replication Group	Notification Quota (GiB)	Max Quota (GiB)	Actions
commvault	repl1	None	None	Edit
cp-ns1	repl1	None	None	Edit
cp-ns2	repl1	None	None	Edit
cp-ns3	repl1	None	None	Edit
cta-ns1	repl1	None	None	Edit
ns-noncompliance	repl1	None	None	Edit

Figure 28. **New Namespace**

2. From the **New Namespace** page as shown in Figure 29, the minimum information is as follows:

   - **Name**: Type a name to identify the namespace.
   - **Replication group**: The replication group will determine if the CloudPools data will be replicated to other ECS sites or not.
   - **Server-side Encryption**: If you require the ECS cluster to perform server-side encryption, you must enable it. It cannot be changed after the namespace is created.
   - **Retention Policies:** It is recommended not to enable file system, CAS, or Bucket Retention Periods for CloudPools buckets.
   - **Namespace Quota:** It is recommended not to enable quota for CloudPools namespace.
   - **Default Bucket Quota:** It is recommended not to enable quota for CloudPools bucket.
   - **Access During Outage**: It is recommended to enable **Access During Outage**. See the ECS Administrator's Guide for more details on Access During Outage.



New Namespace

Name *

User Admin: Ex.: user1, user2@foo.

Domain Group Admin: Ex.: group1@foo.com,

Replication Group *: repl1

Namespace Quota: [✓ Off] On — Notification Only at 1 GiB — and Send Notification at GiB

Default Bucket Quota: [✓ Off] On — Set Default Bucket Quota at 1 GiB

Access During Outage: Off [✓ On]

Compliance: [✓ Off] On

Retention Policies

Name: Policy Name — Value: 10 Seconds

Name	Value	Actions
No data.		

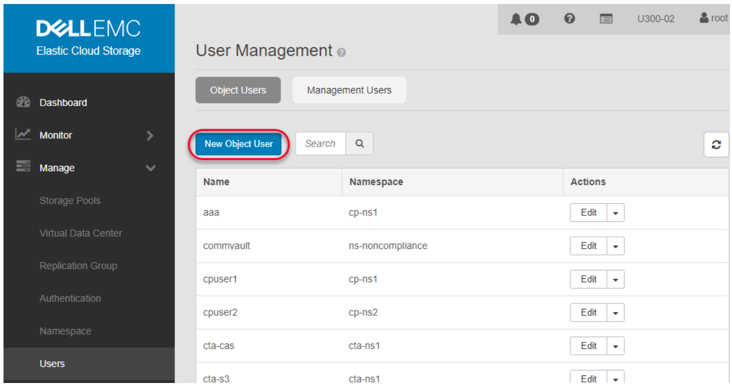
Figure 29. **Configure New Namespace**

3. Click **Save** to create a namespace.

Object user

This section describes the steps how to create an object user on ECS.

1. Log in to ECS portal, go to **Manage** > **Users,** and click **New Object User** as shown in the following figure.

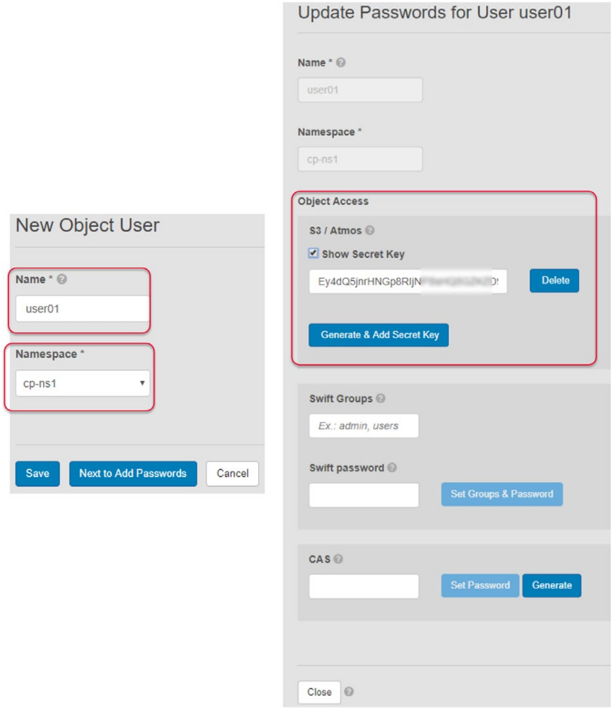


User Management

Name	Namespace	Actions
aaa	cp-ns1	Edit
commvault	ns-noncompliance	Edit
cpuser1	cp-ns1	Edit
cpuser2	cp-ns2	Edit
cta-cas	cta-ns1	Edit
cta-s3	cta-ns1	Edit

Figure 30. **New Object User**

2. From the **New Object User** page, as shown in Figure 31, the minimum information is as follows:
   - **Name**: Type a name to identify the object user.
   - **Namespace**: Select a namespace you want to use by the object user and click **Next to Add Passwords.**
   - **Generate & Add Secret Key**: This option generates the password of the object user. You need this information to configure CloudPools on the PowerScale cluster.



New Object User

Name * user01

Namespace * cp-ns1

Update Passwords for User user01

Name * user01

Namespace * cp-ns1

Object Access

S3 / Atmos

☑ Show Secret Key

Ey4dQ5jnrHNGp8RIjN[redacted]

Swift Groups

Swift password

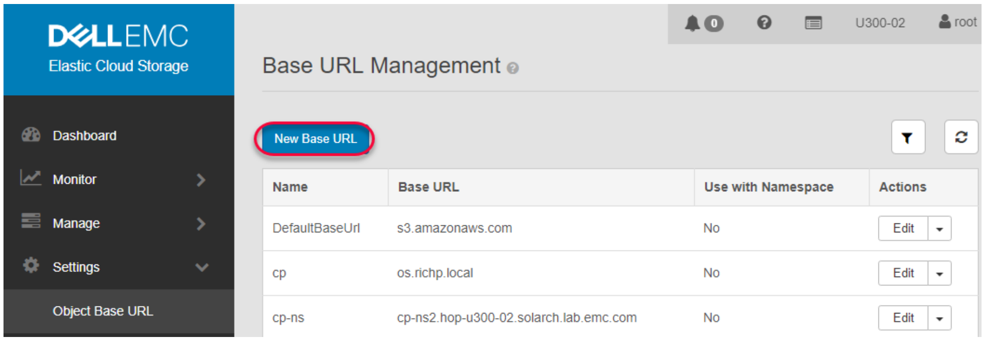
CAS

Figure 31. **Configure New Object User**

Base URL

This section describes the steps how to create a base URL on ECS.

1. Log in to ECS portal, go to **Settings** > **Object Base URL,** and click **New Base URL** as shown in the following figure.

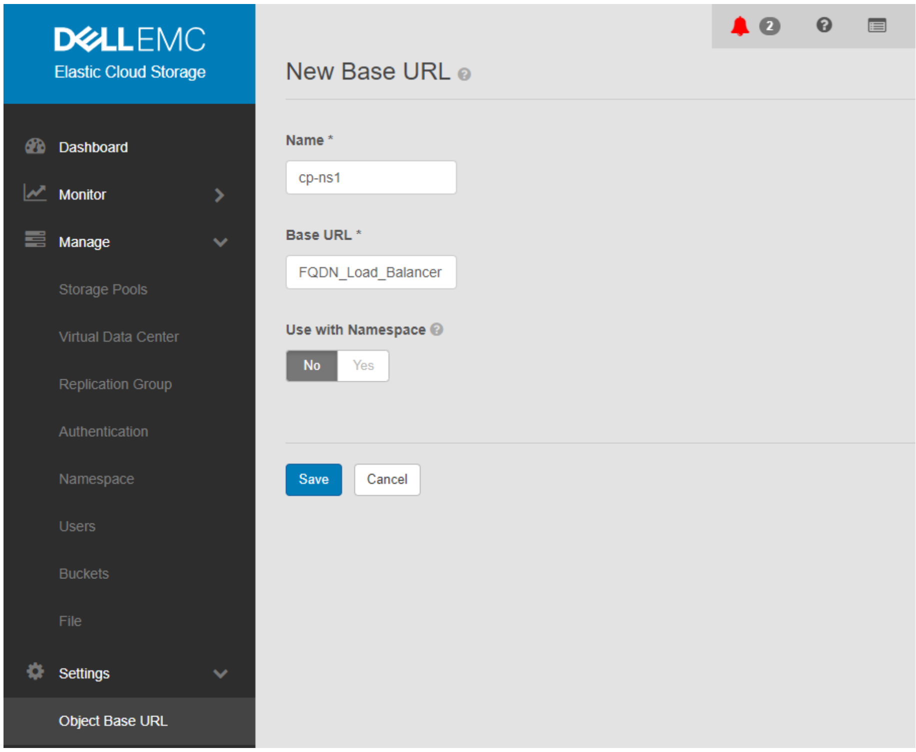


Name	Base URL	Use with Namespace	Actions
DefaultBaseUrl	s3.amazonaws.com	No	Edit
cp	os.richp.local	No	Edit
cp-ns	cp-ns2.hop-u300-02.solarch.lab.emc.com	No	Edit

Figure 32. **New Base URL**

2. From the **New Base URL** page as shown in Figure 33, the minimum information is as follows:

   - **Name**: Type a name to identify the base URL.
   - **Base URL**: This option is needed to configure the load balancer and DNS. See Base URL and Load balancer, which describe the URL when configuring the cloud storage account on the PowerScale cluster.



Name *
cp-ns1

Base URL *
FQDN_Load_Balancer

Use with Namespace
[✓ No] Yes

Figure 33. **Base URL creation**

3. Click **Save** to create a base URL.

Load balancer

A load balancer balances traffic to the various ECS nodes from the PowerScale cluster. A load balancer can provide better performance and throughput for CloudPools. There are hardware and software load balancer options available. See the following deployment documents for the configuration of load balancer.

- ECS with HAProxy
- ECS with NGINX (OpenResty)
- ECS with F5
- ECS with KEMP

Note: A load balancer is required for CloudPools 2.0 and ECS.

PowerScale configuration

This section describes the CloudPools configuration on a PowerScale cluster, which includes:

- License verification
- Cloud storage account creation
- CloudPool creation
- File pool policy creation
- Running of SmartPools job for CloudPools
- SyncIQ policy creation

Verify licensing

This section describes how to verify licensing on the PowerScale system.

1. Log in to the OneFS WebUI and go to **Cluster Management** > **Licensing** as shown in Figure 34.
2. Verify that both the CloudPools and SmartPools license status is **Activated**.

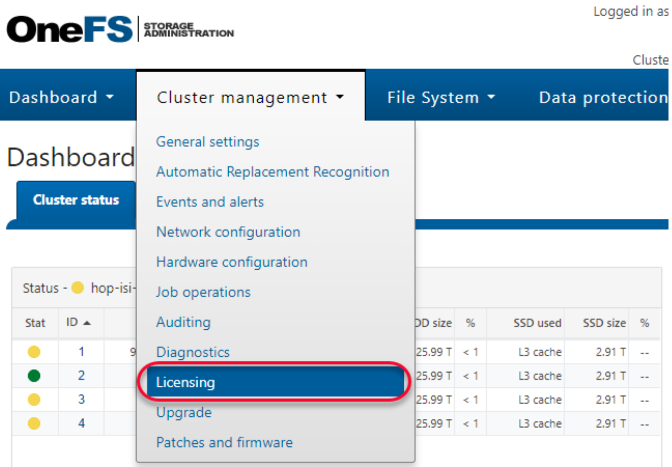
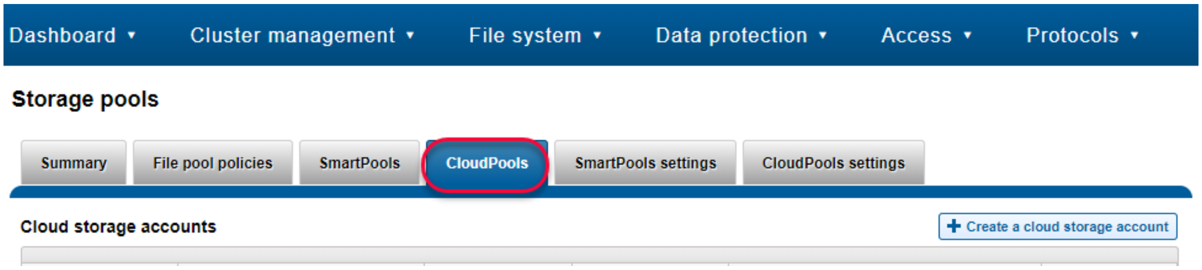


Figure 34. **Verifying licenses**

Cloud storage account

This section describes how to create a cloud storage account on a PowerScale cluster.

1. Log in to the OneFS WebUI and go to **File System** > **Storage Pools**. Click **CloudPools** as shown in the following figure.



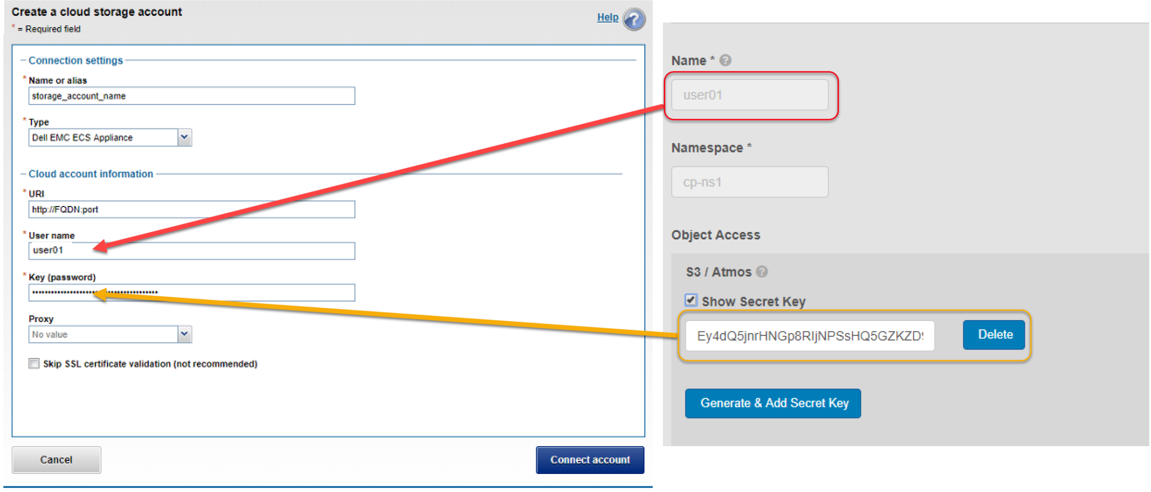
Storage pools

Cloud storage accounts

Figure 35. **CloudPools**

2. Click the **Create a Cloud Storage Account** button, from the **Create a Cloud Storage Account** page as shown in Figure 36. The minimum information is as follows:

   - **Name or alias**: Type a name to identify the cloud storage account.
   - **Type**: Select Dell ECS Appliance.
   - **URL:** Type the FQDN as your own (you can use the base URL created on ECS).
   - **User name**: Type the object username created on ECS.
   - **Key (password)**: Type the secret key of object user.



Create a cloud storage account
* = Required field

Connection settings

* Name or alias: storage_account_name

* Type: Dell EMC ECS Appliance

Cloud account information

* URI: http://FQDN:port

* User name: user01

* Key (password): ••

Proxy: No value

□ Skip SSL certificate validation (not recommended)

Name *: user01

Namespace *: cp-ns1

Object Access

S3 / Atmos

☑ Show Secret Key

Ey4dQ5jnrHNGp8RIjNPSsHQ5GZKZD!

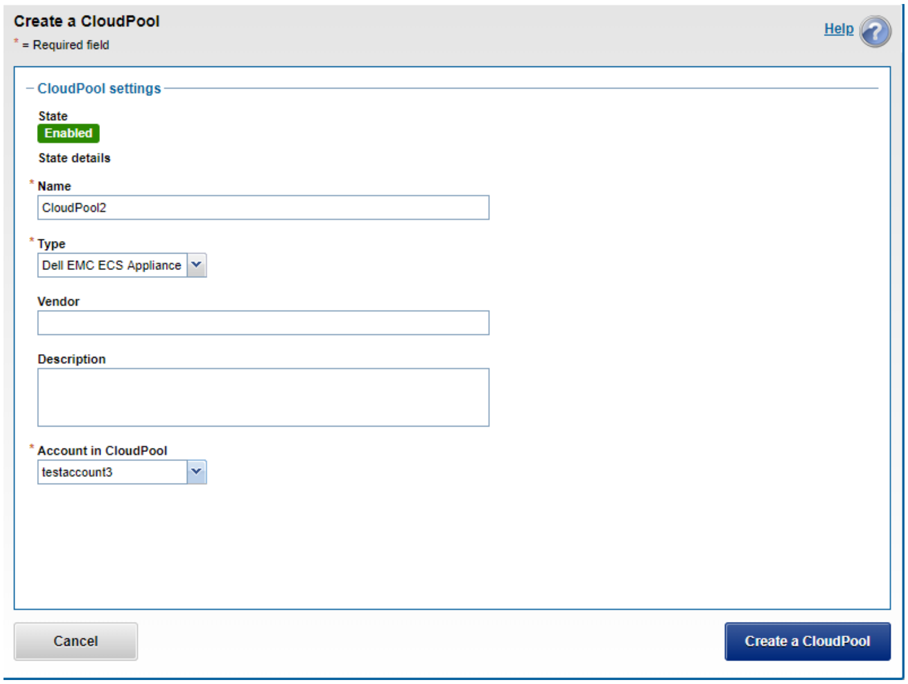
Figure 36. **Create a cloud storage account**

3. Click **Connect account** to create a cloud storage account. This operation results in two buckets being created in ECS. One bucket will start with a **d** as a container to store the CDOs, and the other will start with an **m** as a container to store the associated metadata.

CloudPool

This section describes the steps how to create a CloudPool on a PowerScale cluster.

1. Log in to the OneFS WebUI and go to **File System** > **Storage Pools.** Click **CloudPools** as shown in Figure 35.
2. Click the **Create a CloudPool** button, from the **Create a CloudPool** page as shown in Figure 37. The minimum information is as follows:
   - **Name**: Type a name to identify the CloudPool.
   - **Type**: Select Dell ECS Appliance.
   - **Account in CloudPool**: Select the cloud storage account as your own.



Create a CloudPool

* = Required field

CloudPool settings

State: Enabled

State details

* Name: CloudPool2

* Type: Dell EMC ECS Appliance

Vendor:

Description:

* Account in CloudPool: testaccount3

Figure 37. **Create a CloudPool**

3. Click **Create a CloudPool** to create a CloudPool.

File pool policy

This section describes the steps to create a file pool policy on a PowerScale cluster.

1. Log in to the OneFS WebUI and go to **File System** > **Storage Pools**. Click **File Pool Policies** as shown in the following figure.

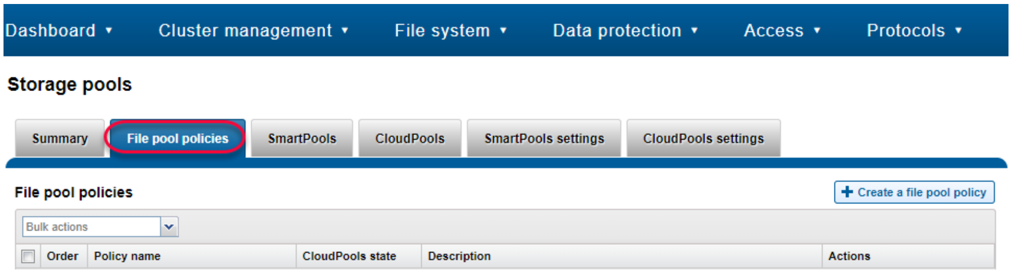
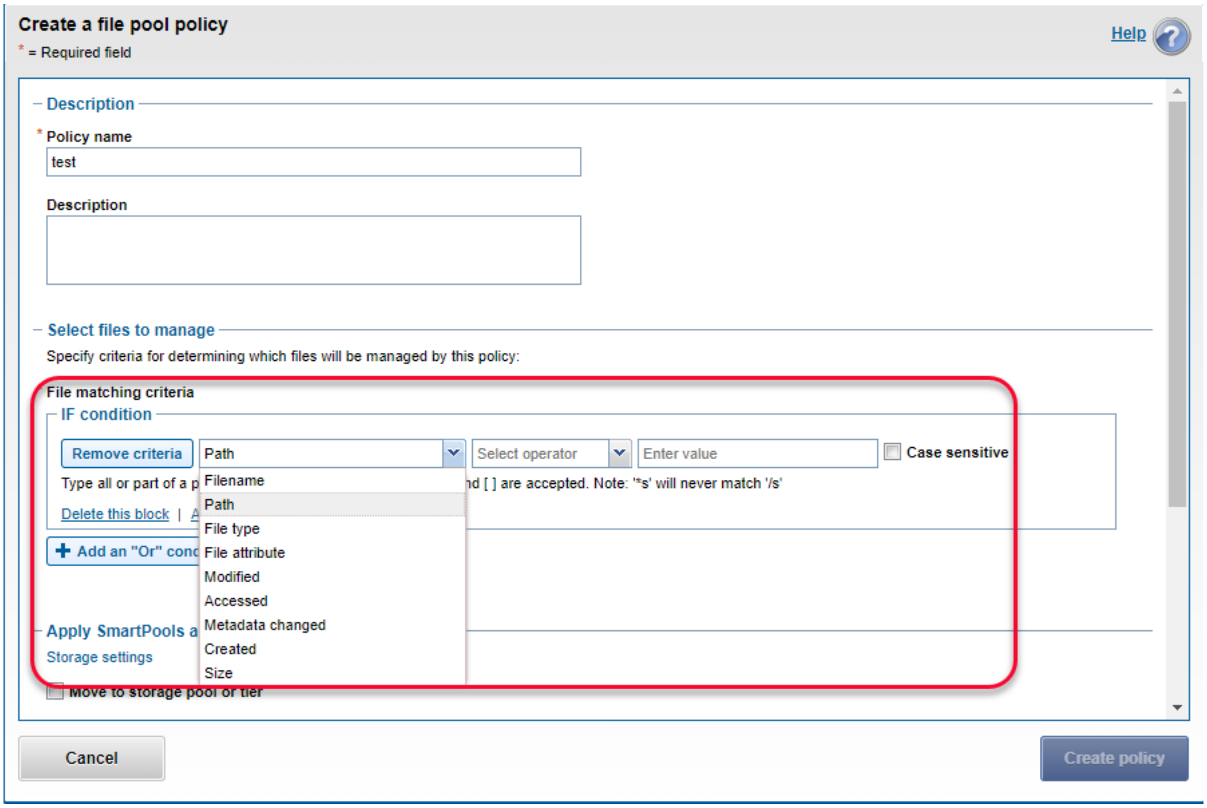


Figure 38. **Create a file pool policy**

2. Click the **Create a File Pool Policy** button, from the **Create a file pool policy** page as shown in Figure 39 and Figure 40. The minimum information is as follows:
    - **Policy Name**: Type a name to identify the file pool policy.
    - **File Matching Criteria**: Define a logical group of files for CloudPools. See File-matching criteria.
    - **Move to cloud storage**: Select the specific CloudPool as the CloudPool storage target.
    - **Data retention settings:** Set the data retention as your own. See Data retention.



Create a file pool policy

* = Required field

Description

* Policy name: test

Description

Select files to manage

Specify criteria for determining which files will be managed by this policy:

File matching criteria

IF condition

Path | Select operator | Enter value | □ Case sensitive

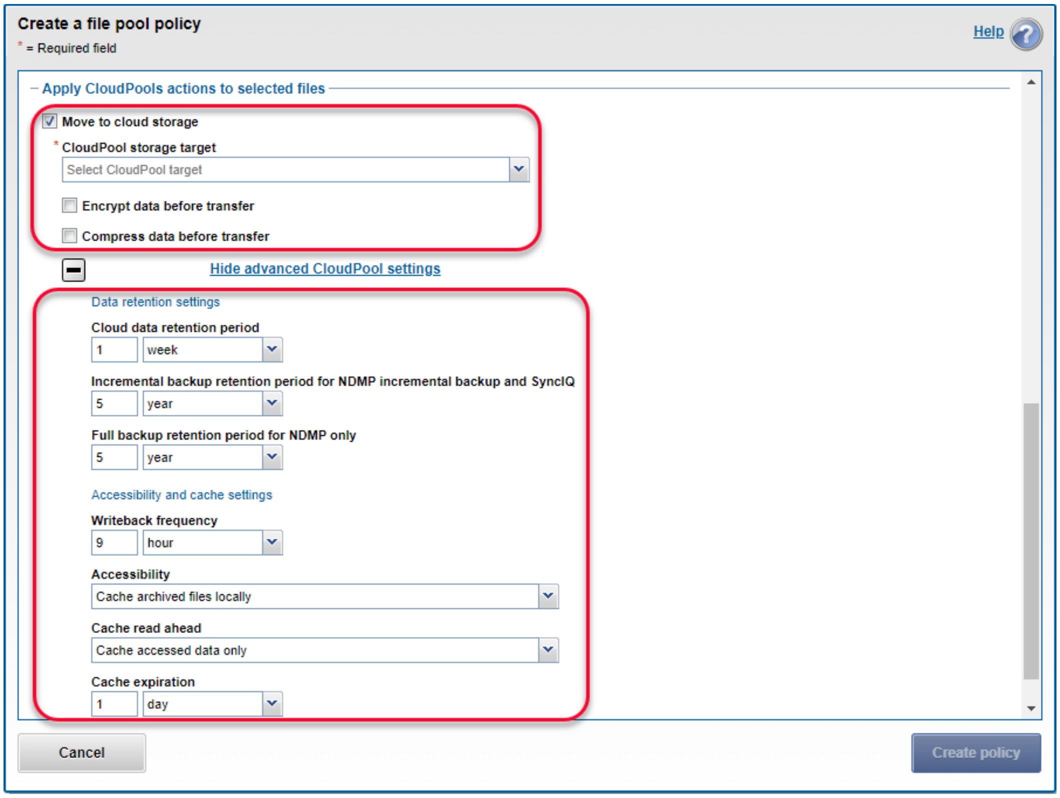
Type all or part of a p … nd [ ] are accepted. Note: '*s' will never match '/s'

Apply SmartPools a…

Storage settings

□ Move to storage pool or tier

Figure 39. **Create a file pool policy**



Create a file pool policy

* = Required field

Apply CloudPools actions to selected files

☑ Move to cloud storage

* CloudPool storage target: Select CloudPool target

□ Encrypt data before transfer

□ Compress data before transfer

Data retention settings

Cloud data retention period: 1 week

Incremental backup retention period for NDMP incremental backup and SyncIQ: 5 year

Full backup retention period for NDMP only: 5 year

Accessibility and cache settings

Writeback frequency: 9 hour

Accessibility: Cache archived files locally

Cache read ahead: Cache accessed data only

Cache expiration: 1 day

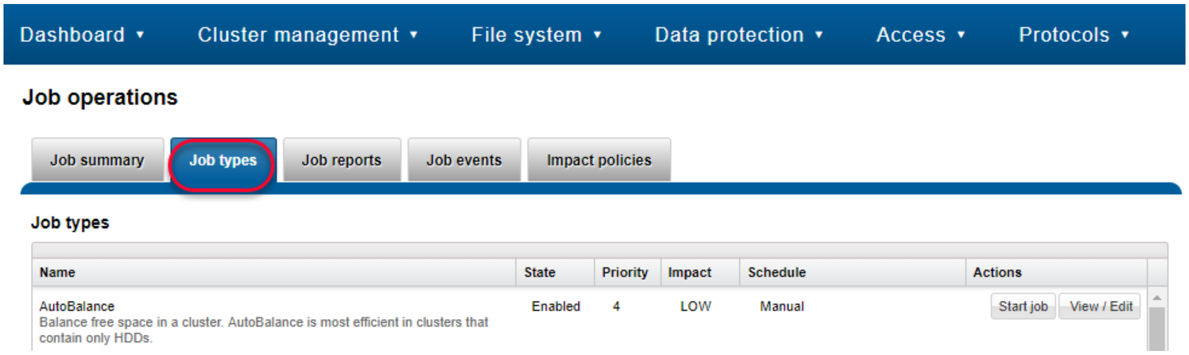
Figure 40. **Create a file pool policy (continued)**

3. Click **Create policy** to create a file pool policy.

Run SmartPools job for CloudPools

This section describes how to run the SmartPools job for CloudPools on a PowerScale cluster.

1. Log in to the OneFS WebUI and go to **Cluster management** > **Job operations**. Click **Job types** as shown in the following figure.

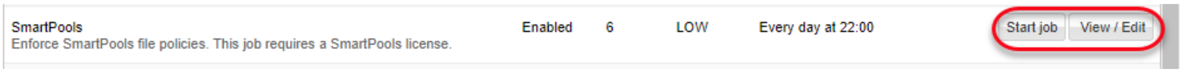


Job types

Name	State	Priority	Impact	Schedule	Actions
AutoBalance Balance free space in a cluster. AutoBalance is most efficient in clusters that contain only HDDs.	Enabled	4	LOW	Manual	Start job View / Edit

Figure 41. **Job types**

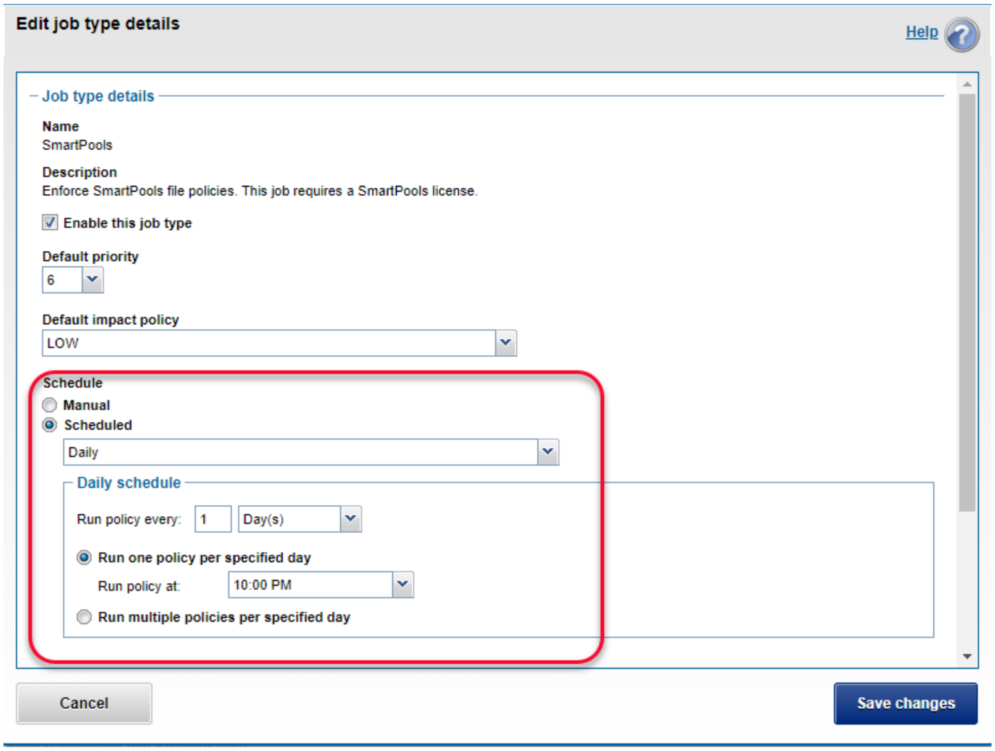
2. Select the **SmartPools** item and click **Edit** as shown in the following figure.



SmartPools Enforce SmartPools file policies. This job requires a SmartPools license.	Enabled	6	LOW	Every day at 22:00	Start job View / Edit

Figure 42. **SmartPools job**

3. From the **Edit job type details** page as shown in Figure 43, you can:
   - Enable or disable the job
   - Set the priority of the job
   - Set the impact policy
   - Set the job schedule as manual or scheduled as your own



Edit job type details

Job type details

Name
SmartPools

Description
Enforce SmartPools file policies. This job requires a SmartPools license.

☑ Enable this job type

Default priority: 6

Default impact policy: LOW

Schedule
○ Manual
● Scheduled
Daily

Daily schedule
Run policy every: 1 Day(s)
● Run one policy per specified day
Run policy at: 10:00 PM
○ Run multiple policies per specified day

Figure 43. **Edit job type details**

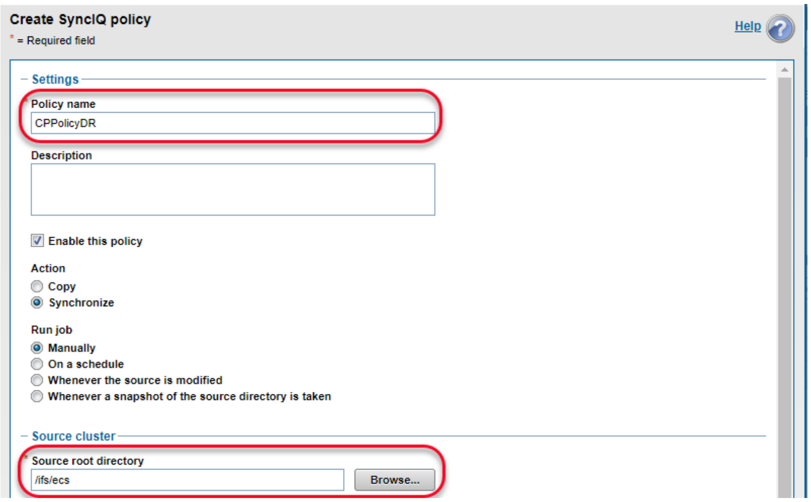
4. Click **Start job** as shown in Figure 42 to run the file pool policy to archive files from the PowerScale cluster to ECS. If you want to start a specific file pool policy job manually, see Commands and troubleshooting.

SyncIQ policy

This section describes how to create a SyncIQ policy on the PowerScale cluster.

1. Log in to the OneFS WebUI and go to **Cluster Management** > **Licensing** as shown in Figure 34. Verify that the CloudPools, SmartPools, and SyncIQ license status are **Activated**.
2. Go to **Data Protection** > **SyncIQ** > **Policies** and click the **Create a SyncIQ policy** button as shown in Figure 44 and Figure 45. The minimum information is as follows:
   - **Policy name:** Type a name to identify the policy name.
   - **Source root directory**: Type the directory name from source PowerScale cluster you want to replicate to the target PowerScale cluster.
   - **Target host**: Type the IP or name of the target PowerScale cluster.

- **Target directory**: Type the directory name from the target PowerScale cluster you want to store the data replicated from the source PowerScale cluster.
- **Deep copy for CloudPools**: Select the type you want to use.



Create SyncIQ policy
* = Required field
Help

Settings

Policy name
CPPolicyDR

Description

☑ Enable this policy

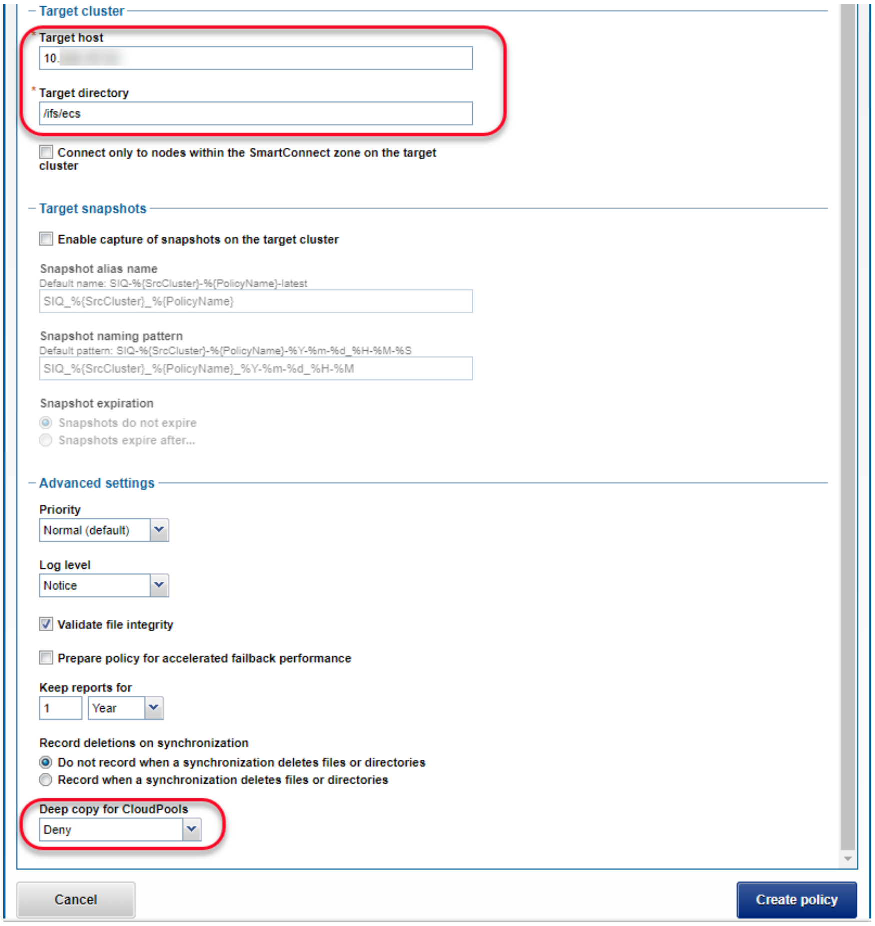
Action
○ Copy
● Synchronize

Run job
● Manually
○ On a schedule
○ Whenever the source is modified
○ Whenever a snapshot of the source directory is taken

Source cluster

* Source root directory
/ifs/ecs
Browse...

Figure 44. **Create SyncIQ policy**



Target cluster

* Target host
10.[redacted]

* Target directory
/ifs/ecs

□ Connect only to nodes within the SmartConnect zone on the target cluster

Target snapshots

□ Enable capture of snapshots on the target cluster

Snapshot alias name
Default name: SIQ-%{SrcCluster}-%{PolicyName}-latest
SIQ_%{SrcCluster}_%{PolicyName}

Snapshot naming pattern
Default pattern: SIQ-%{SrcCluster}-%{PolicyName}-%Y-%m-%d_%H-%M-%S
SIQ_%{SrcCluster}_%{PolicyName}_%Y-%m-%d_%H-%M

Snapshot expiration
● Snapshots do not expire
○ Snapshots expire after...

Advanced settings

Priority
Normal (default)

Log level
Notice

☑ Validate file integrity

□ Prepare policy for accelerated failback performance

Keep reports for
1 Year

Record deletions on synchronization
● Do not record when a synchronization deletes files or directories
○ Record when a synchronization deletes files or directories

Deep copy for CloudPools
Deny

Cancel
Create policy

Figure 45. **Create SyncIQ policy (continued)**

3. Click **Create policy** to create a SyncIQ policy.

SmartLink files and cloud data protection

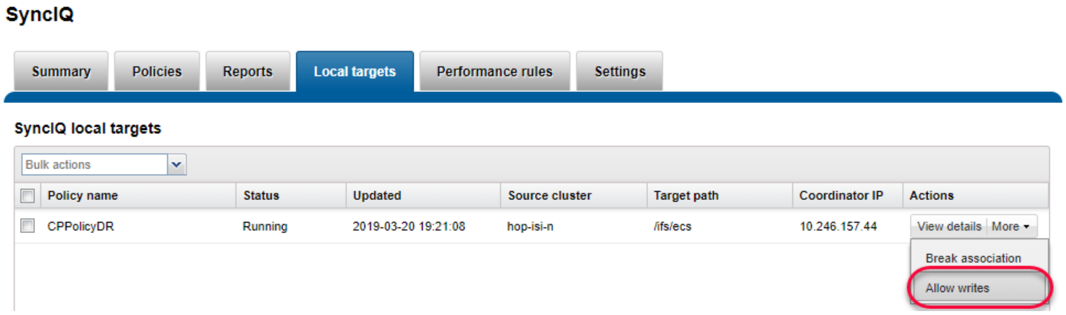
This section describes an example to protect SmartLink files and cloud data. Ensure that you have already configured ECS geo-replication and SyncIQ on the PowerScale clusters, which include:

- Fail over to the secondary PowerScale cluster
- Failback to the primary PowerScale cluster
- Fail over to the secondary ECS
- Failback to the primary ECS

Fail over to the secondary PowerScale cluster

This section describes the steps required to fail over to the secondary PowerScale cluster.

1. Log in to the **secondary** OneFS WebUI and go to **Data Protection** > **SyncIQ.** Click **Local Targets** on the policy that you want to failover and select **More** > **Allow Writes** as shown in the following figure. This operation will grant read/write access to the data on the primary PowerScale cluster being replicated to the secondary PowerScale cluster.



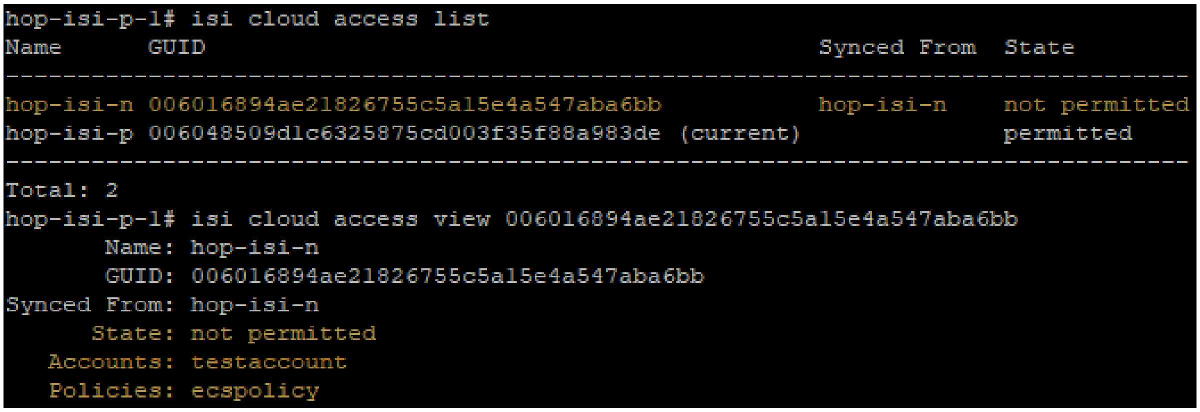
SyncIQ local targets

□ Policy name	Status	Updated	Source cluster	Target path	Coordinator IP	Actions
□ CPPolicyDR	Running	2019-03-20 19:21:08	hop-isi-n	/ifs/ecs	10.246.157.44	View details More

Figure 46. **Allow writes on secondary cluster**

Note: If the primary PowerScale cluster is still online, you need stop all writes to the replication policy's directory.

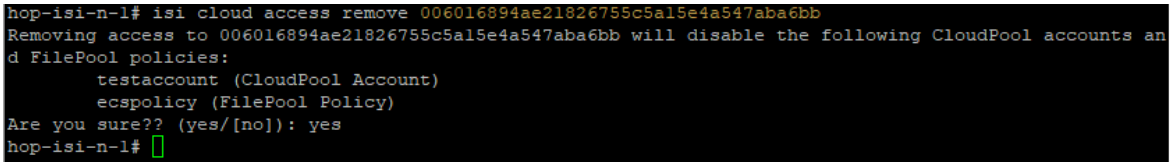
2. Check and change cloud access. Log in to the PowerScale clusters using SSH. To identify the CloudPools GUID, run the commands `isi cloud access list` and `isi cloud access view <GUID>`. The following figure shows the cloud access status on the secondary PowerScale cluster.



```
hop-isi-p-1# isi cloud access list
Name       GUID                                          Synced From  State
-----------------------------------------------------------------------------------
hop-isi-n  006016894ae21826755c5a15e4a547aba6bb          hop-isi-n    not permitted
hop-isi-p  006048509d1c6325875cd003f35f88a983de (current)              permitted
-----------------------------------------------------------------------------------
Total: 2
hop-isi-p-1# isi cloud access view 006016894ae21826755c5a15e4a547aba6bb
       Name: hop-isi-n
       GUID: 006016894ae21826755c5a15e4a547aba6bb
Synced From: hop-isi-n
      State: not permitted
   Accounts: testaccount
   Policies: ecspolicy
```

Figure 47. **Identify CloudPools GUID to be transferred**

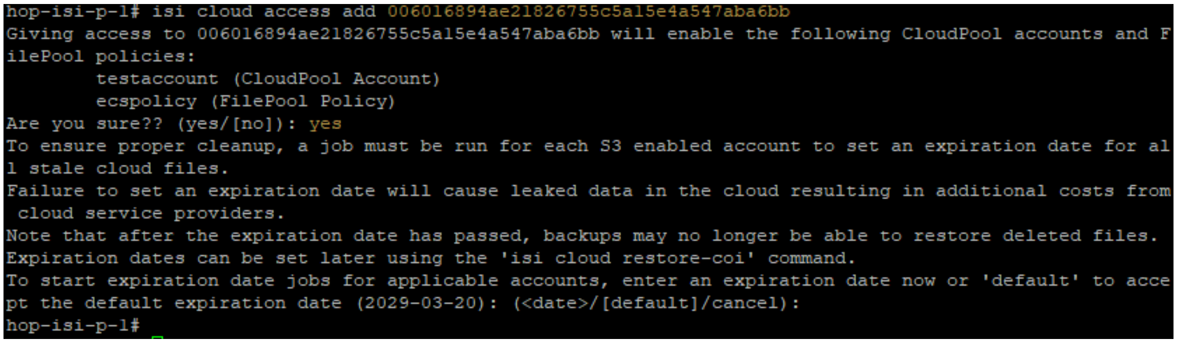
3. On the **primary** PowerScale cluster, remove the cloud write permission by running the command `isi cloud access remove <GUID>`, as shown in the following figure. This operation disables the file pool policy, CloudPool, and cloud storage account on the primary PowerScale cluster.



```
hop-isi-n-1# isi cloud access remove 006016894ae21826755c5a15e4a547aba6bb
Removing access to 006016894ae21826755c5a15e4a547aba6bb will disable the following CloudPool accounts an
d FilePool policies:
        testaccount (CloudPool Account)
        ecspolicy (FilePool Policy)
Are you sure?? (yes/[no]): yes
hop-isi-n-1# 
```

Figure 48. **Remove Cloud write access on the primary PowerScale cluster**

4. On the **secondary** PowerScale cluster, add the cloud write permission by running the command `isi cloud access add <GUID>`, as shown in the following figure. This operation enables file pool policy, CloudPool, and cloud storage account on the secondary PowerScale cluster.



```
hop-isi-p-1# isi cloud access add 006016894ae21826755c5a15e4a547aba6bb
Giving access to 006016894ae21826755c5a15e4a547aba6bb will enable the following CloudPool accounts and F
ilePool policies:
        testaccount (CloudPool Account)
        ecspolicy (FilePool Policy)
Are you sure?? (yes/[no]): yes
To ensure proper cleanup, a job must be run for each S3 enabled account to set an expiration date for al
l stale cloud files.
Failure to set an expiration date will cause leaked data in the cloud resulting in additional costs from
 cloud service providers.
Note that after the expiration date has passed, backups may no longer be able to restore deleted files.
Expiration dates can be set later using the 'isi cloud restore-coi' command.
To start expiration date jobs for applicable accounts, enter an expiration date now or 'default' to acce
pt the default expiration date (2029-03-20): (<date>/[default]/cancel):
hop-isi-p-1# 
```

Figure 49. **Add Cloud write access on the secondary PowerScale cluster**

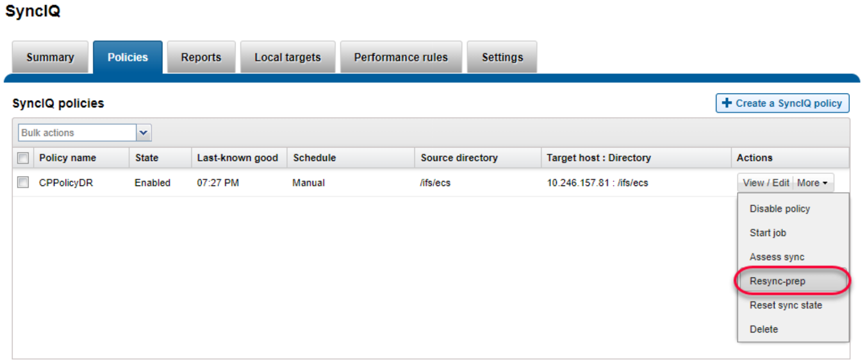
Note: Do not allow write access to the CloudPools from more than one PowerScale cluster.

The SyncIQ failover is complete.

Fail back to primary PowerScale cluster

This section describes the steps required to fail back to the primary PowerScale cluster.

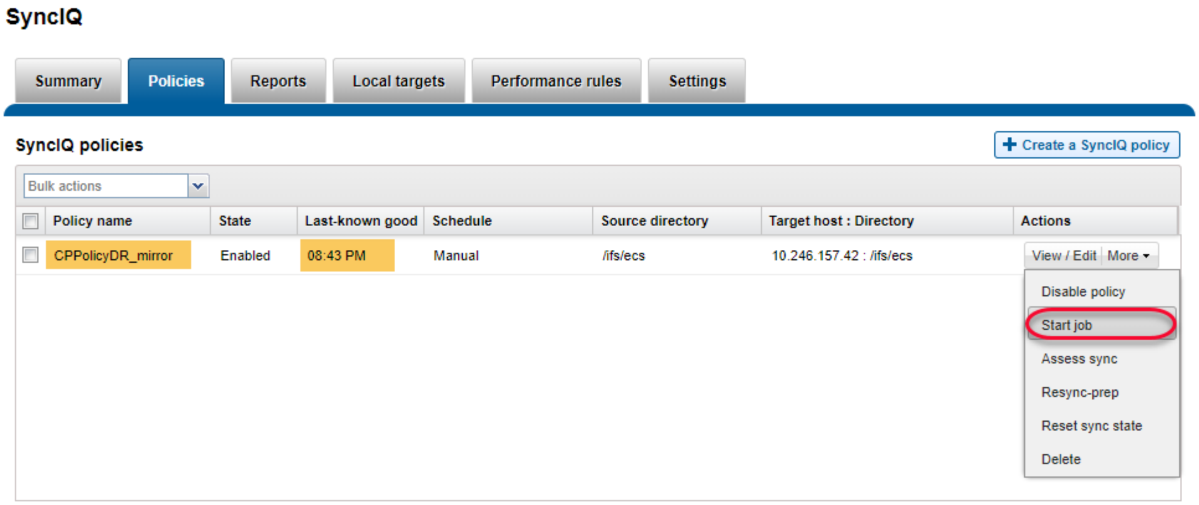
1. Log in to the **primary** OneFS WebUI and go to **Data Protection** > **SyncIQ**. Click **Policies** on the policy that you want to failback and select **More** > **Resync-prep** as shown in the following figure. This operation will create a SyncIQ replication mirror policy on the secondary PowerScale cluster.



	Policy name	State	Last-known good	Schedule	Source directory	Target host : Directory	Actions
□	CPPolicyDR	Enabled	07:27 PM	Manual	/ifs/ecs	10.246.157.81 : /ifs/ecs	View / Edit More ▾

Figure 50. **Resync prep SyncIQ policy on primary PowerScale cluster**

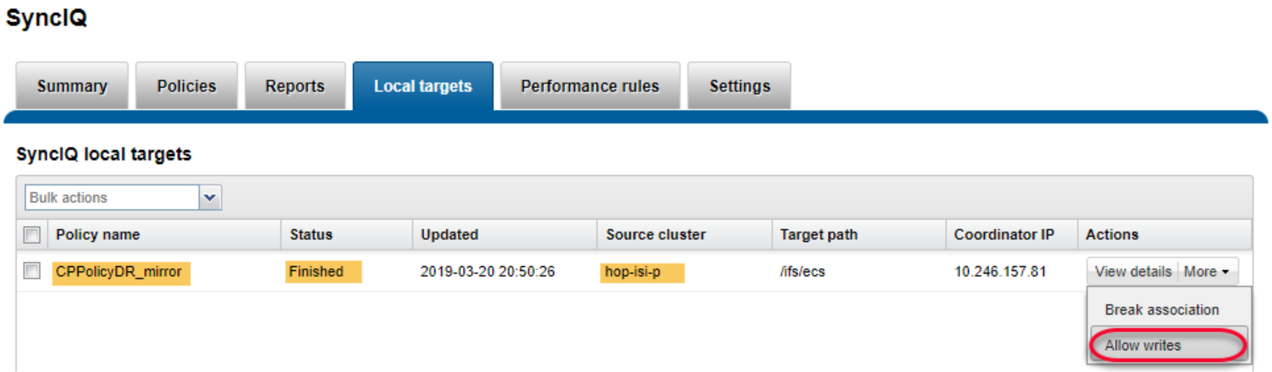
2. Log in to the **secondary** OneFS WebUI and go to **Data Protection** > **SyncIQ** > **Policies**. On the replication mirror policy that you want to failover and select **More** > **Start Job** as shown in the following figure. This operation will sync any changes that have been written to the secondary PowerScale cluster back to the primary PowerScale cluster.



Policy name	State	Last-known good	Schedule	Source directory	Target host : Directory	Actions
CPPolicyDR_mirror	Enabled	08:43 PM	Manual	/ifs/ecs	10.246.157.42 : /ifs/ecs	View / Edit More

Figure 51. **Sync data from secondary PowerScale cluster to primary PowerScale cluster**

3. Log in to the **primary** OneFS WebUI and go to **Data Protection** > **SyncIQ**. Click **Local Targets** on the policy that you want to failover and select **More** > **Allow Writes** as shown in the following figure. This operation will grant read/write access to the replication directory back to the primary PowerScale cluster and change the secondary PowerScale cluster's access to this directory as read-only.

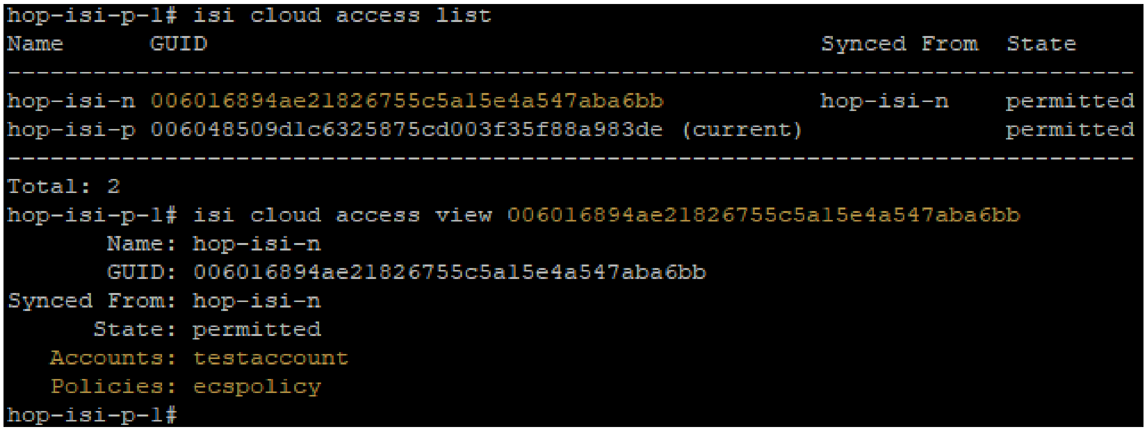


Policy name	Status	Updated	Source cluster	Target path	Coordinator IP	Actions
CPPolicyDR_mirror	Finished	2019-03-20 20:50:26	hop-isi-p	/ifs/ecs	10.246.157.81	View details More

Figure 52. **Allow writes on primary PowerScale cluster to SyncIQ replication directory**

Note: If the secondary PowerScale cluster is still online, you need stop all writes to the replication policy's directory. To perform a final replication from the secondary PowerScale cluster to the primary PowerScale cluster to ensure both sites are synchronized.

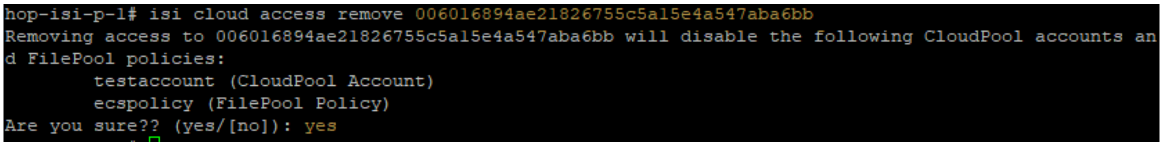
4. Check and change cloud access. Log in to the PowerScale clusters using SSH. To identify the CloudPools GUID, run the commands `isi cloud access list` and `isi cloud access view <GUID>`. The following figure shows how to display the cloud access status on the secondary PowerScale cluster.



```
hop-isi-p-1# isi cloud access list
Name       GUID                                              Synced From  State
-------------------------------------------------------------------------------
hop-isi-n 006016894ae21826755c5a15e4a547aba6bb          hop-isi-n    permitted
hop-isi-p 006048509d1c6325875cd003f35f88a983de (current)              permitted
-------------------------------------------------------------------------------
Total: 2
hop-isi-p-1# isi cloud access view 006016894ae21826755c5a15e4a547aba6bb
       Name: hop-isi-n
       GUID: 006016894ae21826755c5a15e4a547aba6bb
Synced From: hop-isi-n
      State: permitted
   Accounts: testaccount
   Policies: ecspolicy
hop-isi-p-1#
```

Figure 53. **Identify GUID for CloudPools account and file pool policy**

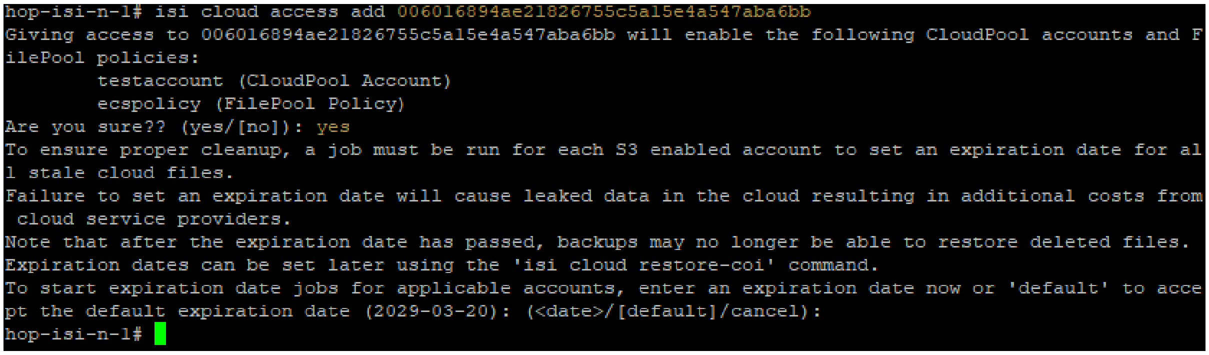
5. On the **secondary** PowerScale cluster, remove the cloud write permission by running the command `isi cloud access remove <GUID>`, as shown in the following figure. This operation disables the file pool policy, CloudPool, and cloud storage account on the secondary PowerScale cluster.



```
hop-isi-p-1# isi cloud access remove 006016894ae21826755c5a15e4a547aba6bb
Removing access to 006016894ae21826755c5a15e4a547aba6bb will disable the following CloudPool accounts an
d FilePool policies:
        testaccount (CloudPool Account)
        ecspolicy (FilePool Policy)
Are you sure?? (yes/[no]): yes
```

Figure 54. **Remove cloud write access on the secondary PowerScale cluster**

6. On the **primary** PowerScale cluster, you can add cloud write permission by running the command `isi cloud access add <GUID>`, as shown in the following figure. This operation enables file pool policy, CloudPool, and cloud storage account on the primary PowerScale cluster.



```
hop-isi-n-1# isi cloud access add 006016894ae21826755c5a15e4a547aba6bb
Giving access to 006016894ae21826755c5a15e4a547aba6bb will enable the following CloudPool accounts and F
ilePool policies:
        testaccount (CloudPool Account)
        ecspolicy (FilePool Policy)
Are you sure?? (yes/[no]): yes
To ensure proper cleanup, a job must be run for each S3 enabled account to set an expiration date for al
l stale cloud files.
Failure to set an expiration date will cause leaked data in the cloud resulting in additional costs from
 cloud service providers.
Note that after the expiration date has passed, backups may no longer be able to restore deleted files.
Expiration dates can be set later using the 'isi cloud restore-coi' command.
To start expiration date jobs for applicable accounts, enter an expiration date now or 'default' to acce
pt the default expiration date (2029-03-20): (<date>/[default]/cancel):
hop-isi-n-1#
```

Figure 55. **Give the primary PowerScale cluster cloud write access**

Note: Do not allow write access to the CloudPools from more than one PowerScale clusters.

7. Log in to the **secondary** OneFS WebUI and go to **Data Protection** > **SyncIQ**. Click **Policies** on the policy that you want to failback and select **More** > **Resync-prep**. This operation will disable the SyncIQ replication mirror policy on the secondary PowerScale cluster and place the secondary PowerScale cluster back into read-only mode. In addition, this operation will enable the SyncIQ replication policy on the primary PowerScale cluster.

The SyncIQ failback is complete.

Fail over to secondary ECS

By default, all ECS sites in a replication group have read/write access to the buckets. If the primary ECS site is unavailable, the cloud data is still available to the PowerScale cluster.

A load balancer needs to be configured for all ECS sites. It can recognize whether the primary ECS is unavailable or not. If so, the load balancer will automatically direct requests to the secondary ECS. It might take several minutes to connect to the secondary ECS.

HAProxy HTTP connections example:

```
option httpchk GET /?ping HTTP/1.1\r\nHost:\ haproxy\r\nX-Emc-
Namespace:\ foo
option allbackups
server node1S1 <Node 1 IP address of primary ECS>:9020 check inter
10000 rise 2 fall 5
server node1S2 <Node 1 IP address of secondary ECS>:9020 check
backup inter 10000 rise 2 fall 5
```

This server node1S1 line tells the load balancer to check if the S3 service is up and running on the primary ECS node. It performs a health check using the command stated in the option httpchk line. If the health check fails, the service is unavailable on the primary ECS. The allbackups line tells HAProxy to direct traffic to the secondary ECS nodes configured with the backup option, such as server node1S2.

Note: Cloud data might be lost if the updated cloud data is not completely replicated to the secondary ECS.

Fail back to primary ECS

If the primary ECS comes back online, the load balancer can recognize that the primary ECS is back online. It automatically directs requests to the primary ECS. It might take several minutes to connect the primary ECS.

Appendix B: Technical support and resources

Resources

Dell.com/support is focused on meeting customer needs with proven services and support.

The Dell Technologies Info Hub provides expertise that helps to ensure customer success on Dell storage platforms.

The following list provides links to documents and other assets that are referenced in this paper. It also provides links to other resources that might be helpful in the deployment of CloudPools on PowerScale:

- OneFS CloudPools Administration Guide
- OneFS Technical Overview
- Next Generation Storage Efficiency with Dell PowerScale SmartDedupe
- Dell PowerScale OneFS Storage Efficiency
- Dell PowerScale SyncIQ: Architecture, Configuration, and Considerations
- High Availability and Data Protection with Dell PowerScale Scale-out NAS
- Storage Quota Management and Provisioning with Dell PowerScale SmartQuotas
- PowerScale Non-Disruptive Upgrade (NDU) Best Practices
- Data Protection with Dell PowerScale SnapshotIQ
- Dell PowerScale: Network Design Considerations
- Dell ECS Administrator's Guide