Abstract
This white paper provides an overview of Dell EMC™ Isilon™ CloudPools software in OneFS™ 8.2.0 and describes its policy-based capabilities that can reduce costs and optimize storage by automatically moving infrequently accessed data to Dell EMC ECS storage.

April 2019
Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 2017</td>
<td>Initial release</td>
</tr>
<tr>
<td>April 2019</td>
<td>Rewritten and added details for CloudPools 2.0</td>
</tr>
</tbody>
</table>

Acknowledgements

This paper was produced by the following:

Author: Jason He (Jason.He@dell.com)
# Table of contents

Revisions........................................................................................................................................... 2
Acknowledgements............................................................................................................................... 2
Table of contents ................................................................................................................................... 3
Executive summary................................................................................................................................. 6
Audience................................................................................................................................................ 6
We value your feedback......................................................................................................................... 6

1 CloudPools solution architectural overview ..................................................................................... 7
   1.1 Isilon ............................................................................................................................................... 7
   1.1.1 SmartPools ................................................................................................................................ 7
   1.1.2 SmartLink files ........................................................................................................................... 8
   1.1.3 File pool policies ....................................................................................................................... 8
   1.2 ECS ............................................................................................................................................... 10
   1.2.1 Cloud metadata object............................................................................................................. 10
   1.2.2 Cloud data object...................................................................................................................... 10
   1.3 CloudPools operations ............................................................................................................... 10
      1.3.1 Archive ................................................................................................................................. 10
      1.3.2 Recall ..................................................................................................................................... 11
      1.3.3 Read ....................................................................................................................................... 12
      1.3.4 Update .................................................................................................................................... 13

2 CloudPools 2.0 ..................................................................................................................................... 15
   2.1 AWS signature v4 authentication support ................................................................................... 15
   2.2 NDMP and SyncIQ support .......................................................................................................... 15
   2.3 Non-disruptive upgrade support ................................................................................................. 16
   2.4 Snapshot efficiency ...................................................................................................................... 16
   2.5 Sparse files handling .................................................................................................................... 17
   2.6 Quota management ...................................................................................................................... 17
   2.7 Anti-virus integration ................................................................................................................... 18
   2.8 WORM integration ....................................................................................................................... 19

3 Considerations and best practices ...................................................................................................... 20
   3.1 Isilon configuration ...................................................................................................................... 20
      3.1.1 CloudPools settings ............................................................................................................. 20
      3.1.2 File pool policy .................................................................................................................... 20
   3.1.3 Other considerations ............................................................................................................. 21
   3.2 ECS configuration ....................................................................................................................... 21
# Table of contents

3.3 Protecting SmartLink files........................................................................................................... 22
3.3.1 Isilon SyncIQ...................................................................................................................................... 22
3.3.2 Isilon NDMP ............................................................................................................................... 23
3.4 Protecting cloud data...................................................................................................................... 24

4 Reporting........................................................................................................................................... 25
4.1 CloudPools network stats introduction ....................................................................................... 25
4.2 Query network stats by CloudPools account ................................................................................. 25
4.3 Query network stats by file pool policy ....................................................................................... 25
4.4 Query history network stats ....................................................................................................... 26

5 Commands and troubleshooting ..................................................................................................... 27
5.1 Commands ....................................................................................................................................... 27
5.1.1 CloudPools archive .................................................................................................................. 27
5.1.2 CloudPools recall ..................................................................................................................... 27
5.1.3 CloudPools job monitoring ..................................................................................................... 27
5.2 Troubleshooting ............................................................................................................................. 28
5.2.1 CloudPools state ..................................................................................................................... 28
5.2.2 CloudPools logs ....................................................................................................................... 29

A Step-by-step configuration example ................................................................................................. 30
A.1 ECS configuration .......................................................................................................................... 30
A.1.1 Virtual data center ................................................................................................................... 30
A.1.2 Replication group ..................................................................................................................... 34
A.1.3 Namespace ............................................................................................................................... 35
A.1.4 Object user ............................................................................................................................... 37
A.1.5 Base URL .................................................................................................................................. 38
A.2 Load balancer ............................................................................................................................... 40
A.3 Isilon configuration ........................................................................................................................ 40
A.3.1 Verify licensing ........................................................................................................................ 40
A.3.2 Cloud storage account .......................................................................................................... 41
A.3.3 CloudPool .................................................................................................................................. 42
A.3.4 File pool policy ........................................................................................................................ 42
A.3.5 Run SmartPools job for CloudPools ...................................................................................... 44
A.3.6 SyncIQ policy ........................................................................................................................... 46
A.4 SmartLink files and cloud data protection .................................................................................... 47
A.4.1 Fail over to the secondary Isilon cluster ................................................................................ 48
A.4.2 Fail back to primary Isilon cluster ......................................................................................... 49
A.4.3 Fail over to secondary ECS ..................................................................................................... 52
Table of contents

A.4.4 Fail back to primary ECS ........................................................................................................52
B  Technical support and resources ..............................................................................................53
  B.1  Related resources ................................................................................................................53
Executive summary

This white paper provides information about how Dell EMC™ Isilon™ CloudPools software in OneFS™ 8.2.0 integrated with Dell EMC ECS storage and it covers the following topics:

- CloudPools solution architectural overview
- CloudPools 2.0 introduction with a focus on the following improvements:
  - 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
- 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 the following:

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

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

- Dell EMC Community Network info hubs
- Dell EMC OneFS release notes, which are available on the Dell EMC support network and contain important information about resolved and known issues
- [Dell EMC Isilon OneFS Best Practices](#)
- [Dell EMC ECS General Best Practices](#)

We value your feedback

Dell EMC and the authors of this document welcome your feedback on the white paper.

Authors: Jason He ([Jason.He@dell.com](mailto:Jason.He@dell.com))
CloudPools solution architectural overview

CloudPools is a feature of Isilon OneFS that provides the capabilities to tier cold or infrequently accessed data to lower-cost cloud storage. It is built on the Isilon OneFS SmartPools file pool policy framework, which provides granular control of file placement on an Isilon cluster.

As shown in Figure 1, CloudPools extends the Isilon namespace to the private cloud, Dell EMC ECS. 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.

![CloudPools solution architecture](image)

**Figure 1**  CloudPools solution architecture

**Note:** A SmartPools license and a CloudPools license are required on each node of the Isilon cluster. A minimum of OneFS 8.0.0 is required for CloudPools 1.0, and OneFS 8.2.0 for CloudPools 2.0.

The tiering of data is driven by policies defined on the Isilon cluster. The archived data can be accessed by clients through a variety of protocols including SMB, NFS, HDFS, and SWIFT.

1.1 Isilon

This section describes key CloudPools concepts, which include:

- SmartPools
- SmartLink files
- File pool policies

1.1.1 SmartPools

SmartPools is the OneFS data tiering framework, of which CloudPools is an extension. SmartPools alone provides the ability to tier data between different node types within an Isilon cluster. CloudPools adds the ability to tier data outside of an Isilon cluster.
1.1.2 SmartLink files

Although file data is moved to the cloud storage, the files remain visible in OneFS. After file data has been archived to the cloud storage, the file gets truncated to an 8KB file. The 8KB file is called 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. The map points to all cloud objects.

Figure 2 shows the contents of a SmartLink file and the mapping cloud objects.

1.1.3 File pool policies

Both CloudPools and SmartPools use the file pool policy engine to define what 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 are moved to the cloud storage during the job execution, and a SmartLink file is left behind on the Isilon cluster that contains information about where to go to retrieve the data. In CloudPools 1.0, the SmartLink file sometimes referred to as a stub, 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.

This section describes the key options when configuring a file pool policy, which include:

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

1.1.3.1 Encryption

CloudPools provides an option to encrypt data before it is sent to the cloud storage. It leverages the Isilon 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.

1.1.3.2 Compression

CloudPools provides an option to compress data before it is sent to the cloud storage. It implements block level compression using the zlib compression library. CloudPools will not compress data that is already compressed.
1.1.3.3 File matching criteria
When files match a file pool policy, CloudPools moves the file data to the cloud storage. File matching criteria enable you to define a logical group of files as a file pool for CloudPools. It defines what data should be archived to the cloud storage.

File matching criteria include the following:

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

You can add any number of file matching criteria to refine a file pool policy for CloudPools.

1.1.3.4 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 Isilon disk storage for files that have been moved off cluster via CloudPools.

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

CloudPools provides the following four configurable data cache settings:

- **Cache Expiration:** Specifies the number of days until OneFS purges expired cache information in SmartLink files. The default value is one day.
- **Writeback Frequency:** Specifies 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:** Specifies the cache read ahead strategy for cloud objects (partial or full). The default value is partial.
- **Accessibility:** Specifies how data is cached in SmartLink files when a user or application accesses a SmartLink file on the Isilon cluster. Values are cached and no cache. The default value is cached.

1.1.3.5 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:** Specifies the length of time cloud objects is retained after the files have been fully recalled or deleted. The default value is one week.
CloudPools solution architectural overview

- **Incremental Backup Retention Period for NDMP Incremental Backup and SyncIQ**: Specifies the length of time that CloudPools retains cloud objects referenced by a SmartLink file that has been replicated by SyncIQ or an incremental NDMP backup. The default value is five years.

- **Full Backup Retention Period for NDMP Only**: Specifies the length of time that OneFS retains cloud data referenced by a SmartLink file that has been backed up by a full NDMP backup. The default value is five years.

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

---

1.2 **ECS**

This section describes cloud objects in ECS:

- Cloud metadata object
- Cloud data object

1.2.1 **Cloud metadata object**

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

1.2.2 **Cloud data object**

A cloud data object (CDO) is a CloudPools object that stores file data in ECS. File data is split into 2MB 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 or prior to OneFS 8.2.0.

---

1.3 **CloudPools operations**

This section describes the workflow of CloudPools operations:

- Archive
- Recall
- Read
- Update

1.3.1 **Archive**

Archive operation is the CloudPools process of moving file data from the local Isilon cluster to the cloud storage. Files can be archived either using the SmartPools Job or from the command line. You can pause and resume the CloudPools archive process. Refer to the section **commands** for details.
CloudPools solution architectural overview

Figure 3 shows the workflow of CloudPools archive. The steps involved are listed below:

1. A file is found that matches a file pool policy, which specifies a cloud target and cloud specific parameters. For example, encryption, compression, local data cache and data retention.
2. The file data is split into chunks called Cloud Data Objects (CDO).
3. The chunks are sent from the Isilon cluster to ECS system. A checksum is applied for each chunk to ensure data integrity.
4. The file is truncated into a SmartLink file on the Isilon cluster and a Cloud Metadata Object (CMO) is written to ECS system.

1.3.2 Recall

Recall operation is the CloudPools process of reversing the archive process. It will replace the SmartLink file by restoring the original file data on the Isilon cluster and removing the cloud objects in ECS. The recall process can only be performed using the command line. You can pause and resume the CloudPools recall process. Refer to the section commands for detailed instructions.
Figure 4 shows the workflow of CloudPools recall. The steps are listed below:

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

### 1.3.3 Read

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. This can be disabled by setting the accessibility. For more detail, refer to the section local data cache.

Figure 5 shows the workflow of CloudPools read by default. The steps are listed below:

1. Client accesses the file through the SmartLink file. OneFS looks for data in the local data cache first and moves to step 3 if the data is already in the local data cache.
2. OneFS retrieves the CDOs from the ECS to the Isilon cluster, putting the file data in the data local cache.
3. The file data is sent to the clients from the data local cache on the Isilon cluster.
4. OneFS purges expired cache information for the SmartLink file.
Update operation is the CloudPools process that occurs when clients update data. When clients make changes 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, refer to the section local data cache.

Figure 6 shows the workflow of the CloudPools update. The steps are listed below:

1. Client accesses the file through the SmartLink file.
2. OneFS retrieves CDOs from the ECS system to the Isilon cluster, putting the file data in the local cache.
3. The 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 system.
5. OneFS purges expired cache information for the SmartLink file.
CloudPools solution architectural overview

Isilon Cluster

1. Client accesses the file through the SmartLink file

2. OneFS retrieves CDOs from the ECS system, 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 system

5. OneFS purges expired cache information for the SmartLink file

ECS System

Figure 6  Update workflow
2 CloudPools 2.0

CloudPools 2.0 is the next generation of CloudPools, released in OneFS 8.2.0. This chapter will describe 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

2.1 AWS signature v4 authentication support

CloudPools 2.0 supports AWS signature version 4 (V4) in conjunction 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 on V4, refer to the link Authenticating Requests: AWS Signature V4.

CloudPools 2.0 handles the compatibility of SyncIQ for data replication and NDMP for data backup/restore. When the source and target Isilon clusters use different authentication versions, the following are the considerations for CloudPools:

- **SyncIQ**: When the source Isilon cluster is running OneFS 8.2.0 and the target Isilon cluster is running a version of OneFS prior to OneFS 8.2.0.
  - If CloudPools cloud storage account is using V2 or V4 on the source Isilon cluster, V2 will be used on the target Isilon cluster.

- **NDMP**: When files are restored from tape to the target Isilon cluster.
  - If CloudPools cloud storage account is using V4 on the target Isilon cluster, V4 will be used.
  - If CloudPools cloud storage account is using V2 on the target Isilon cluster, V2 will be used.

- **NDU**: When OneFS is upgraded to 8.2.0.
  - Once the Isilon cluster is COMMITTED to OneFS 8.2.0, it will automatically start 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 will be released to support V4 in OneFS 8.1.2.

2.2 NDMP and SyncIQ support

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

NDMP and SyncIQ provide the following two types of copy or backup: Shallow and Deep Copy Backups. For more information on NDMP and SyncIQ protection, refer to the white paper High Availability and Data Protection with Dell EMC Isilon Scale-out NAS.
**Shallow Copy (SC)/Backup:** Replicate or back up SmartLink files to the target Isilon cluster or tape as SmartLink files without file data.

**Deep Copy (DC)/Backup:** Replicate or back up SmartLink files to the target Isilon cluster or tape as regular files or unarchived files.

Table 1 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>
<thead>
<tr>
<th>OneFS version</th>
<th>CloudPools version</th>
</tr>
</thead>
<tbody>
<tr>
<td>OneFS 8.0.x/OneFS 8.1.x</td>
<td>CloudPools 1.0</td>
</tr>
<tr>
<td>OneFS 8.2.0 or higher</td>
<td>CloudPools 2.0</td>
</tr>
</tbody>
</table>

Table 2 shows the NDMP and SyncIQ supported use cases when running different version of CloudPools on the source and target clusters. As noted below, if CloudPools 2.0 is running on the source Isilon cluster and CloudPools 1.0 is running on the target Isilon cluster, Shallow copies are not allowed.

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>SC NDMP</th>
<th>DC NDMP</th>
<th>SC SyncIQ Replication</th>
<th>DC SyncIQ Replication</th>
</tr>
</thead>
<tbody>
<tr>
<td>CloudPools 1.0</td>
<td>CloudPools 2.0</td>
<td>Support</td>
<td>Support</td>
<td>Support</td>
<td>Support</td>
</tr>
<tr>
<td>CloudPools 2.0</td>
<td>CloudPools 1.0</td>
<td>No Support</td>
<td>Support</td>
<td>No Support</td>
<td>Support</td>
</tr>
</tbody>
</table>

### 2.3 Non-disruptive 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 post upgrade commit. The process ensures a smooth transition from CloudPools 1.0 to CloudPools 2.0. CloudPools 2.0 will be ready to use once the upgrade state is committed. For more information on upgrade states, refer to the white paper *Isilon Non-Disruptive Upgrade (NDU) Best Practices*.

The recommendation is to ensure no SyncIQ or NDMP jobs are running before upgrading OneFS to 8.2, otherwise the CHANGEOVER process will not continue until the SyncIQ and NDMP jobs complete.

### 2.4 Snapshot efficiency

CloudPools 2.0 eliminates data copy-on-write (CoW) when archiving files with snapshots from an Isilon cluster to the cloud. The file data is only stored in the cloud storage which saves space on the Isilon cluster. For more information on data CoW for snapshots, refer to the white paper *Next Generation Data Protection with OneFS SnapshotIQ*.

When SmartLink files are updated by users, the updated file data will be sent to the cloud storage. The snapshot only has a reference to the old file data. Both the modified and old file data are only stored in the cloud storage, so the storage space is saved on the Isilon cluster.
You can restore a file to a regular file from the snapshot directly in the case when the SmartLink file has been deleted. The file data will be retrieved from the cloud during the file restoration. And the regular file can be archived again from the Isilon cluster to the cloud storage.

If the SmartLink files are backed up by SyncIQ or NDMP before being updated, the old file data can be recalled from the cloud using the backup copy of the SmartLink file. If the backup retention has not expired, the CDOs of the old file data cannot be deleted even though the snapshot has been deleted. Because the CDOs of the old file data are still referenced by the SmartLink file backup. When the backup retention period has expired and the CDOs of the old file data are no longer used, the CDOs of the old file data will be deleted. For more information on data retention, refer to the section data retention.

If SmartLink files are not backed up by SyncIQ or NDMP before updating occurs on the SmartLink file, the CDOs of the old file data will be deleted after the snapshot is deleted.

Figure 7 shows how CloudPools 2.0 integrates with SnapshotIQ.

2.5 Sparse files handling

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

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

2.6 Quota management

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

For example, if you have a directory or user quota of 500GB and it is reporting 400GB used, then you archive 200GB files from the Isilon cluster to cloud. Moving data to the cloud reduces quotas measured node space consumption. In prior to OneFS 8.2.0, the quota is freed by the amount of data that has been archived to the
CloudPools 2.0

Cloud and your quota will show 200GB (400 - 200) used out of 500GB. That means the user or directory quota can exceed the set limit (500GB). In OneFS 8.2.0, application logical size integrated with CloudPools 2.0 measures the true capacity consumption even if data is archived from the Isilon cluster to the cloud, and your quota will show 400GB used out of 500GB through the application logical size. That means the user or directory quota cannot exceed the set limit (500GB).

For more information on the new SmartQuota reporting capabilities in OneFS 8.2.0, refer to the white paper Storage Quota Management and Provisioning with Dell EMC Isilon SmartQuotas.

2.7 Anti-virus integration

In prior to OneFS 8.2.0, SmartLink files were skipped for the anti-virus scanning.

In OneFS 8.2.0, CloudPools 2.0 provides a configurable option for anti-virus scanning of the SmartLink files. The file data will be retrieved from the cloud and cached on the cluster for the scan only if the option is enabled. As shown in Figure 8, the Scan Cloudpool Files option is configured and verified using the command line.

```
hop-isi-n-l# is1 antiviru$ settings modify --scan-cloudpool-files=1
hop-isi-n-l# is1 antiviru$ 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 8 Enable Scan 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.
2.8 WORM integration

SmartLock is an optional software feature of OneFS that enables SEC 17-a4 data compliance. In what is referred to as Enterprise Mode, individual directories can be set up as WORM (Write Once, Read Many) and the data is immutable by everyone except the root account on the cluster once the files have been committed. You can also set up an Isilon cluster in what is called Compliance Mode, where the root account on the cluster is removed and no one can change or delete data in WORM locked folders.

In prior to OneFS 8.2.0, SmartLink files are not allowed in both Enterprise mode and Compliance mode. In OneFS 8.2.0, details about CloudPools 2.0 and SmartLock integration is listed below:

- **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 Isilon cluster once they are committed.
Chapter 3: Considerations and best practices

This section focuses on the considerations and best practices of how to configure Isilon CloudPools and ECS.

3.1 Isilon configuration

This section will focus on the considerations and best practices of how to configure Isilon CloudPools properly.

3.1.1 CloudPools settings

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

- **Encryption**: Encryption is an option that can be enabled either on the Isilon cluster or on the ECS. The recommendation is to enable encryption on the Isilon cluster instead of on the ECS. If the average CPU is high (>70%) on Isilon cluster, the encryption can be enabled on ECS instead of on the Isilon cluster. It is important to note that encryption adds an additional load on the Isilon cluster. Encryption can also impact the CloudPools archive and recall performance.

- **Compression**: Compression is an option that can be enabled on the Isilon cluster, and then file data will be 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 Isilon cluster to save network resources. When the compression is disabled on the Isilon cluster, ECS will automatically compress the file data. It is important to note that compression adds an additional load on the Isilon cluster which means it might take more time to archive files from Isilon to ECS.

- **Data Retention**: The recommendation is to explicitly set the data retention for the file data being archived from the Isilon cluster to ECS. If the SmartLink files are backed up via SyncIQ or NDMP, the data retention defines how long the cloud objects remain on the ECS. Once the retention period has passed, the Isilon cluster sends a delete command to ECS. The ECS will mark the associated cloud objects for deletion. The delete process is asynchronous and the space will not be reclaimed until garbage collection completes. This is a low priority background process, which may 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 Isilon cluster, the recommendation is to set lower values for the Writeback Frequency and Cache Expiration. This will reduce the time to keep file data in the local data cache and free up storage space sooner on the Isilon cluster.

3.1.2 File pool policy

File pool policies are the mechanism to define what data will be archived from the Isilon cluster to ECS. The considerations are listed below:

- 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 Isilon cluster, the recommendation is not to archive small files that are <30KB in size.
- If the files need to be updated frequently, the recommendation is not to archive those files.
- OneFS supports a maximum of 128 file pool policies (SmartPools and CloudPools combined). The recommendation is not to exceed 30 file pool policies per Isilon 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 run.

3.1.3 Other considerations

- **Deduplication**: CloudPools can archive deduped files from an Isilon cluster to cloud storage. However, un-deduped files will be created when recalling those files from the cloud to the Isilon cluster. For more information on deduplication within OneFS, refer to the white paper [Storage Efficiency with Dell EMC Isilon SmartDedupe](#).

- **Small File Storage Efficiency (SFSE)**: CloudPools and SFSE cannot work together. For Isilon clusters using CloudPools, any SmartLink files cannot be containerized or packed. It is best practice to not archive small files that you intend to optimize using SFSE. The efficiencies gained from implementing SFSE for small files, will outweigh the storage advantages gained from archiving them to the cloud using CloudPools. For more information on the Small File Storage Efficiency feature of OneFS, refer to the white paper [Dell EMC Isilon OneFS Storage Efficiency for Healthcare PACS](#).

- **Network Proxy**: When an Isilon cluster cannot connect to the CloudPool storage target directly, network proxy servers can be configured for an alternate path to connect the cloud storage.

- **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.

3.2 ECS configuration

Before configuring Isilon CloudPools on an Isilon cluster, the ECS environment needs to be configured properly. The following are the general considerations and best practices when configuring ECS for CloudPools.

- **Virtual Data Center (VDC)**: If the cloud data needs to be protected using ECS Geo-replication, refer to the section [ECS geo-replication](#). 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 cannot be changed after the replication has been created.

- **Namespace**: Namespace creation is exclusively for CloudPools. The following options need to be considered.
  - **Server-side Encryption**: The encryption need to be configured appropriately when creating the namespace, this cannot be changed after the namespace is created.
  - **Replication Group**: The Replication Group need to be configured appropriately when creating the namespace, this 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 Isilon cluster.
  - **Access During Outage (ADO)**: For Geo-replication, make sure 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 Isilon cluster.

- **Base URL**: CloudPools 2.0 only uses virtual host style bucket addressing. For virtual host style, refer to the [ECS Administrator's Guide](#). A base URL need to be created on ECS for the virtual host style bucket addressing. The base URL should be the FQDN of the load balancer virtual IP (VIP).
Considerations and best practices

- **Load Balancer**: A hardware or software load balancer can evenly distribute the load across all ECS nodes. Load balancer VIP must have a DNS entry to resolve the virtual host style address. As shown in Figure 9, a CNAME/wildcard and an A record need to be created on the DNS servers for the load balancer VIP.

![DNS entry](Figure 9)

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

### 3.3 Protecting SmartLink files

SmartLink files are the sole means to access file data stored in ECS. It is important to protect SmartLink files from accidental deletion.

In this section, Isilon SyncIQ and NDMP are discussed for the backup of SmartLink files.

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

#### 3.3.1 Isilon SyncIQ

SyncIQ is CloudPools aware. SyncIQ policies support two types of data replication for CloudPools:

- **Shallow copy**: Replicate files as SmartLink files without file data from source Isilon cluster to target Isilon cluster.
- **Deep copy**: Replicate files as regular files or unarchived files from source Isilon cluster to target Isilon cluster.

For the cross-version compatibility of CloudPools, refer to the section [NDMP and SyncIQ support](#).

SyncIQ, SmartPools, and CloudPools licenses are required on both source and target Isilon cluster. It is highly recommended to setup a scheduled SyncIQ backup of the SmartLink files. For more on Isilon SyncIQ, refer to the white paper [Dell EMC Isilon SyncIQ: Architecture, Configuration, and Considerations](#).

When SyncIQ replicates SmartLink files, it also replicates local cache state and unsynchronized cache data from the source Isilon cluster to the target Isilon cluster. Figure 10 shows the SyncIQ replication when replicating a directory including SmartLink files and unarchived normal files. For the steps on failover to a secondary Isilon cluster and failback to a primary Isilon cluster, please refer to Appendix A.
Considerations and best practices

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

3.3.2 Isilon NDMP

NDMP is CloudPools aware. Isilon NDMP supports three types of backup and restore for CloudPools:

- **DeepCopy**: Back up files as regular files or unarchived files, and files can only be restored as regular files.
- **ShallowCopy**: Back up files as SmartLink files without file data, and files can only be restored as SmartLink files.
- **ComboCopy**: Back up files as SmartLink files with file data, and files can be restored as regular files or SmartLink files.

For the cross-version compatibility of CloudPools, refer to the section [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 version CDOs will be protected on ECS under the data retention setting. You can restore a specific version of a SmartLink file from tapes to an Isilon cluster and continue to access (read/update) the file like before.

Note: If encryption is enabled in the file pool policy for CloudPools, NDMP will also back up all the relevant encryption keys to tapes along with the SmartLink files.
### 3.4 Protecting cloud data

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

- 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 an Isilon cluster to ECS, the cloud data will automatically be replicated to another ECS asynchronously. As shown in Figure 11, ECS geo-replication works together with CloudPools.

![Diagram of ECS geo-replication with CloudPools](image)

**Figure 11** 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.

If Access During Outage (ADO) is enabled on the CloudPools buckets and a load balancer is also configured for the primary and secondary ECS, cloud data can continue to be accessed 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, please refer to Appendix A.
4 Reporting

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

- CloudPools network stats introduction
- Query network stats by CloudPools account
- Query network stats by file pool policy
- Query history network stats

4.1 CloudPools network stats introduction

CloudPools network stats collect every network transaction. They 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/DELETE operations. You can get the CloudPools network stats in the following 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.

4.2 Query network stats by CloudPools account

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

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

Figure 12 below shows an example of current CloudPools network stats by CloudPools account.

![Network stats by CloudPools account](image1.png)

**Figure 12** Network stats by CloudPools account

4.3 Query network stats by file pool policy

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

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

Figure 13 below shows an example of current CloudPools network stats by file pool policy.

![Network stats by file pool policy](image2.png)

**Figure 13** Network stats by file pool policy

**Note:** The number of delete operations by policy is not displayed by the file pool policy.
4.4 Query history network stats

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

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

You can define the number of seconds in the past with the parameter `s`. For example, set it as 86,400 to query CloudPools network stats in the last day.

Figure 14 below shows an example of CloudPools network stats in the last day.

```
hop-isi-p-1# isi_test_cpool_stats -q -s 86400
Account   Bytes-in   bytes-out   gets  puts  deletes
testaccount  4194996000  4194993034  4000  2001  8001
```

Figure 14  Network stats last day

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

```bash
isi_test_cpool_stats -f
```
5 **Commands and troubleshooting**

This section describes CloudPools commands and troubleshooting methodologies.

### 5.1 Commands

This section describes CloudPools operations and job monitoring commands, which include:

- CloudPools archive
- CloudPools recall
- CloudPools monitoring

#### 5.1.1 CloudPools archive

Run the following command to archive files from an Isilon 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 15.

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

**Figure 15** SmartLink file

#### 5.1.2 CloudPools recall

Run the following command to recall files from the cloud to an Isilon 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.

#### 5.1.3 CloudPools job monitoring

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

```
isi cloud jobs list
```
To check the archive or recall file list status for a specific CloudPools job, use the following command. As shown in Figure 16, the job id can be found using the command `isi cloud jobs list`.

`isi cloud jobs files list <job id>`

![File list of specific CloudPools job](image)

**Figure 16** File list of specific CloudPools job

*Note:* The output of the command only shows the file name and state for specific CloudPools job.

To pause a CloudPools job, use the following command:

`isi cloud jobs pause <job id>`

To resume a paused CloudPools job, use the following command:

`isi cloud jobs resume <job id>`

To cancel a CloudPools job, use the following command:

`isi cloud jobs cancel <job id>`

Run the following command to 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`

### 5.2 Troubleshooting

This section describes various CloudPools troubleshooting methodologies, which include:

- CloudPools state
- CloudPools logs

#### 5.2.1 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, use the following command:

`isi clouds pools view <cloud pool name>`

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

`isi filepool policies view <filepool policy name>`
5.2.2 CloudPools logs

Check the CloudPools logs if needed. The location of CloudPools logs are 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
A  Step-by-step configuration example

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

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

A.1  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 that follows is designed to be a general guide when the purpose of the ECS is to be used by CloudPools. It does not cover all the details of ECS configuration for other use cases. Consult the ECS Administrator's Guide for more details on ECS configuration.

A.1.1  Virtual data center

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

1. Log in to the ECS portal, navigate to Manage > Virtual Data Center, and click New Virtual Data Center as shown in the Figure 17.

![New Virtual Data Center](image)

Figure 17  New Virtual Data Center
Step-by-step configuration example

2. From the **New Virtual Data Center** page as shown in Figure 18, 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 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 page](image)

*Figure 18  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 following are the steps to create multiple VDC.

1. Log in to the **second** ECS portal and navigate to **Manage > Virtual Data Center**. Select **Get VDC Access Key** as shown in the Figure 19 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.

![Image](image-url)  
**Figure 19**  Get VDC Access Key from the Second ECS
2. Log in to the primary ECS portal and navigate to Manage > Virtual Data Center. Select New Virtual Data Center as shown in Figure 20. 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 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.

![Figure 20](image_url) Create a VDC on primary ECS

3. Click **Save** to create a new virtual data center.
A.1.2 Replication group

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

1. Log in to the ECS portal and navigate to Manage > Replication Group. Click the New Replication Group button as shown in the Figure 21.

![New Replication Group](image)

**Figure 21** New Replication Group

2. From the New Replication Group page as shown in Figure 22, 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**: Replicates data to all sites/VDCs in the replication group. If your replication group has four sites that would mean four copies are stored, one at each site. This offers the highest data durability but has the lowest space efficiency.
  - **Disable**: Maintains one additional copy of data at another site. Regardless of the number of sites you will always have 2 copies of the data.
- **Add VDC**: The setting is ignored for single site replication groups. Add the appropriate virtual data centers and storage pools.
3. Click **Save** to create a new replication group.

### A.1.3 Namespace

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

1. Log in to the ECS portal, navigate to **Manage > Namespace**, and click **New Namespace** as shown in Figure 23.
2. From the **New Namespace** page as shown in Figure 24, 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 cannot be changed after the namespace created.
   - **Retention Policies**: It is recommended not to enable file system, CAS or Bucket Retention Periods for CloudPools buckets.
   - **Access During Outage**: It is recommended to enable **Access During Outage**. See the [ECS Administrator's Guide](#) for more details on Access During Outage.

![Figure 24 Configure New Namespace](image-url)
3. Click **Save** to create a new namespace.

### A.1.4 Object user

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

1. Log in to ECS portal, navigate to **Manage > Users**, and click **New Object User** as shown in Figure 25.

![New Object User](image)

**Figure 25** New Object User

2. From the **New Object User** page as shown in the Figure 26, 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 will generate the password of the object user, you will need this to configure CloudPools on the Isilon cluster.
A.1.5 Base URL

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

1. Log in to ECS portal, navigate to Settings > Object Base URL, and click New Base URL as shown in Figure 27.

Figure 26 Configure New Object User
Step-by-step configuration example

2. From the **New Base URL** page as shown in Figure 28, the minimum information is as follows:
   - **Name**: Type a name to identify the base URL.
   - **Base URL**: This is needed to configure the load balancer and DNS. See the section **Base URL** and **Load Balancer**, which describes the URL when configuring the cloud storage account on the Isilon cluster.

3. Click **Save** to create a new base URL.
A.2 Load balancer

A load balancer balances traffic to the various ECS nodes from the Isilon cluster. A load balancer can provide much better performance and throughput for CloudPools. There are many hardware and software load balancer options available. See the [ECS with HAProxy Load Balancer](#) for the configuration of load balancer.

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

A.3 Isilon configuration

This section describes the CloudPools configuration on an Isilon cluster, which include:

- Verify licensing
- Cloud storage account creation
- CloudPool creation
- File pool policy creation
- Run SmartPools job for CloudPools
- SyncIQ policy creation

A.3.1 Verify licensing

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

1. Log in to the Isilon OneFS WebUI and navigate to **Cluster Management > Licensing** as shown in Figure 29.
2. Verify that both the CloudPools and SmartPools license status is **Activated**.

![Figure 29 Verifying licenses](#)
A.3.2 Cloud storage account

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

1. Log in to the Isilon OneFS WebUI and navigate to File System > Storage Pools. Click CloudPools as shown in Figure 30.

2. Click the + Create a Cloud Storage Account button, from the Create a Cloud Storage Account page as shown in the Figure 31. The minimum information is as follows:
   - Name or alias: Type a name to identify the cloud storage account.
   - Type: Select Dell EMC ECS Appliance.
   - URL: Type the FQDN as your own (you can use the base URL created on ECS).
   - User name: Type the object user name created on ECS.
   - Key (password): Type the secret key of object user.

3. Click Connect account to create a cloud storage account. This results in two buckets being created in ECS; one will start with a “d” as a container to store the CDO’s, and the other will start with an “m” as a container to store the associated metadata.
A.3.3 CloudPool

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

1. Log in to the Isilon OneFS WebUI and navigate to **File System > Storage Pools**. Click **CloudPools** as shown in Figure 30.

2. Click the **+ Create a CloudPool** button, from the **Create a CloudPool** page as shown in Figure 32. The minimum information is as follows:
   - **Name**: Type a name to identify the CloudPool.
   - **Type**: Select Dell EMC ECS Appliance.
   - **Account in CloudPool**: Select the cloud storage account as your own.

![Create a CloudPool](image)

Figure 32 Create a CloudPool

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

A.3.4 File pool policy

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

1. Log in to the Isilon OneFS WebUI and navigate to **File System > Storage Pools**. Click **File Pool Policies** as shown in Figure 33.
Step-by-step configuration example

2. Click the + Create a File Pool Policy button, from the Create a file pool policy page as shown in Figure 34 and Figure 35. 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 the section 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 the section data retention settings.

![Create a file pool policy](image-url)
Step-by-step configuration example

Figure 35  Create a file pool policy (continued)

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

A.3.5  Run SmartPools job for CloudPools

This section describes how to run the SmartPools job for CloudPools on an Isilon cluster.

1. Log in to the Isilon OneFS WebUI and navigate to **Cluster management > Job operations**. Click **Job types** as shown in the Figure 36.

Figure 36  Job types
Step-by-step configuration example

2. Select the **SmartPools** item and click **Edit** as shown in the Figure 37.

![Figure 37 SmartPools job](image)

3. From the **Edit job type details** page as shown in Figure 38, you can perform the following:
   - 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

![Figure 38 Edit job type details](image)

4. Click **Start job** as shown in Figure 37 to run the file pool policy to archive files from the Isilon cluster to ECS. If you want to start a specific file pool policy job manually, refer to the section **commands and troubleshooting**.
A.3.6 **SyncIQ policy**

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

1. Log in to the Isilon OneFS WebUI and navigate to **Cluster Management > Licensing** as shown in Figure 29 above. Verify that the CloudPools, SmartPools, and SyncIQ license status is **Activated**.

2. Navigate to **Data Protection > SyncIQ > Policies** and click the **+ Create a SyncIQ policy** button as shown in Figure 39 and Figure 40. 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 Isilon cluster you want to replicate to the target Isilon cluster.
   - **Target host**: Type the IP or name of the target Isilon cluster.
   - **Target directory**: Type the directory name from the target Isilon cluster you want to store the data replicated from the source Isilon cluster.
   - **Deep copy for CloudPools**: Select the type you want to use.

![Create SyncIQ policy](image_url)
3. Click **Create policy** to create a SyncIQ policy.

### A.4 SmartLink files and cloud data protection

This section describes an example to protect SmartLink files and cloud data. You need ensure that you have already configured ECS geo-replication and SyncIQ on the Isilon clusters, which includes the following:

- Failover to the secondary Isilon cluster
- Failback to the primary Isilon cluster
- Failover to the secondary ECS
- Failback to the primary ECS
A.4.1 Fail over to the secondary Isilon cluster

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

1. Log in to the **secondary** Isilon OneFS WebUI and navigate to **Data Protection > SyncIQ**. Click **Local Targets** on the policy that you want to failover, and select **More > Allow Writes** as shown in Figure 41. This will grant read/write access to the data on the primary Isilon cluster being replicated to the secondary Isilon cluster.

![SyncIQ](image)

Figure 41 Allow writes on secondary cluster

**Note:** If your primary Isilon 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 Isilon clusters using SSH. To identify the CloudPools GUID, use the commands `isi cloud access list` and `isi cloud access view <GUID>`. Figure 42 shows the cloud access status on the secondary Isilon cluster.

![Cloud access list](image)

Figure 42 Identify CloudPools GUID to be transferred

3. On the **primary** Isilon cluster, remove the cloud write permission using the command `isi cloud access remove <GUID>` as shown in Figure 43. This will disable the file pool policy, CloudPool, and cloud storage account on the primary Isilon cluster.

![Cloud access remove](image)

Figure 43 Remove Cloud write access on the primary Isilon cluster
4. On the secondary Isilon cluster, add the cloud write permission using the command `isi cloud access add <GUID>` as shown in Figure 44. This will enable file pool policy, CloudPool, and cloud storage account on the secondary Isilon cluster.

```
# Example command
oci-cloud access add 09e0189f7a26e75c0686e5a47abab0b
```

![Figure 44: Add Cloud write access on the secondary Isilon cluster](image)

**Note:** It is important to not allow write access to the CloudPools from more than one Isilon cluster.

The SyncIQ failover is complete.

### A.4.2 Fail back to primary Isilon cluster

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

1. Log in to the primary Isilon OneFS WebUI and navigate to Data Protection > SyncIQ. Click Policies on the policy that you want to fail back, and select More > Resync-prep as shown in Figure 45. This will create a SyncIQ replication mirror policy on the secondary Isilon cluster.

![Figure 45: Resync prep SyncIQ policy on primary Isilon cluster](image)

2. Log in to the secondary Isilon OneFS WebUI and navigate to Data Protection > SyncIQ > Policies. On the replication mirror policy that you want to fail over, and select More > Start Job as shown in Figure 46. This will sync any changes that have been written to the secondary Isilon cluster back to the primary Isilon cluster.
Step-by-step configuration example

SyncIQ

SyncIQ policies

<table>
<thead>
<tr>
<th>Policy name</th>
<th>State</th>
<th>Last known good</th>
<th>Schedule</th>
<th>Source directory</th>
<th>Target host : Directory</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFPolicyDR_minor</td>
<td>Enabled</td>
<td>08:45 PM</td>
<td>Manual</td>
<td>/ifs/</td>
<td>10.246.157.42 /ifs/</td>
<td>Start job</td>
</tr>
</tbody>
</table>

Figure 46  Sync data from secondary Isilon cluster to primary Isilon cluster

3. Log in to the primary Isilon OneFS WebUI and navigate to Data Protection > SyncIQ. Click Local Targets on the policy that you want to fail over, and select More > Allow Writes as shown in Figure 47. This will grant read/write access to the replication directory back to the primary Isilon cluster and change the secondary Isilon cluster's access to this directory as read only.

SyncIQ

SyncIQ local targets

<table>
<thead>
<tr>
<th>Policy name</th>
<th>Status</th>
<th>Updated</th>
<th>Source cluster</th>
<th>Target path</th>
<th>Coordinator IP</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFPolicyDR_minor</td>
<td></td>
<td>2019-03-20 20:59:26</td>
<td>hopscotch</td>
<td>/ifs/</td>
<td>10.246.157.81</td>
<td>Start job</td>
</tr>
</tbody>
</table>

Figure 47  Allow writes on primary Isilon cluster to SyncIQ replication directory

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

4. Check and change cloud access. Log in to the Isilon clusters using SSH. To identify the CloudPools GUID, use the commands \texttt{isi cloud access list} and \texttt{isi cloud access view <GUID>}. Figure 48 shows how to display the cloud access status on the secondary Isilon cluster.
Step-by-step configuration example

**Identify GUID for CloudPools account and file pool policy**

5. **On the secondary Isilon cluster**, remove the cloud write permission using the command `isi cloud access remove <GUID>` as shown in Figure 49. This will disable the file pool policy, CloudPool, and cloud storage account on the secondary Isilon cluster.

**Remove cloud write access on the secondary Isilon cluster**

6. **On the primary Isilon cluster**, you can add cloud write permission using the command `isi cloud access add <GUID>` as shown in Figure 50. This will enable file pool policy, CloudPool, and cloud storage account on the primary Isilon cluster.

**Give the primary Isilon cluster cloud write access**

**Note:** It is important to not allow write access to the CloudPools from more than one Isilon clusters.

The SyncIQ failback is complete.
A.4.3 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 Isilon cluster.

The load balancer need to be configured for all ECS sites. It can recognize whether the primary ECS is unavailable or not. If so, this will automatically direct requests to the secondary ECS. It may 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 health check using the command stated in the option `httpchk` line. If the health check fail, 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 may be lost if the updated cloud data is not replicated to the secondary ECS completely.

A.4.4 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 may take several minutes to connect the primary ECS.
Technical support and resources

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

**Storage technical documents and videos** provide expertise that helps to ensure customer success on Dell EMC storage platforms.

## B.1 Related resources

Below is a list of documents and other assets that are referenced in this paper along with other resources that may be helpful in your deployment of CloudPools on Isilon.

1. **Dell EMC Isilon CloudPools and ECS (CloudPools 1.0)**
2. **OneFS CloudPools Administration Guide**
3. **OneFS Technical Overview**
4. **OneFS 8.1.0 CLI Administration Guide**
5. **OneFS 8.1.0 CLI Command Reference**
6. **OneFS 8.1.0 Web Administration Guide**
7. **Storage Efficiency with Dell EMC Isilon SmartDedupe**
8. **Dell EMC Isilon OneFS Storage Efficiency for Healthcare PACS**
9. **Dell EMC Isilon SyncIQ: Architecture, Configuration, and Considerations**
10. **High Availability and Data Protection with Dell EMC Isilon Scale-out NAS**
11. **Storage Quota Management and Provisioning with Dell EMC Isilon SmartQuotas**
12. **Isilon Non-Disruptive Upgrade (NDU) Best Practices**
13. **Next Generation Data Protection with OneFS SnapshotIQ**
14. **Dell EMC ECS Administrator's Guide**