ISILON CLOUDPOOLS AND ELASTIC CLOUD STORAGE

ABSTRACT

CloudPools is a feature of Isilon's OneFS that provides off-cluster tiering of infrequently accessed data to cloud storage. This white paper explains how CloudPools work with Elastic Cloud Storage (ECS). It includes an architectural overview, availability options, best practice recommendations and a step-by-step configuration example.

March 2017
The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © 2017 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA, 5/17, White Paper H14775.1

Dell Inc. believes the information in this document is accurate as of its publication date. The information is subject to change without notice.
TABLE OF CONTENTS

EXECUTIVE SUMMARY ........................................................................................................... 5
AUDIENCE................................................................................................................................. 5

ARCHITECTURAL OVERVIEW ................................................................................................. 6
High Availability ....................................................................................................................... 10
Configuring CloudPools on Multiple Sites............................................................................. 14
Encryption ............................................................................................................................... 14
SmartQuota ............................................................................................................................. 15
SmartLock ............................................................................................................................... 15
Dedupe ................................................................................................................................... 15
Cloning ................................................................................................................................... 15
Client-Based Tools .................................................................................................................. 15
SmartLink File Access Directly From The Isilon cluster ....................................................... 15
Alternate Data Streams ......................................................................................................... 15
SMB Oplock .......................................................................................................................... 15

REQUIREMENTS .................................................................................................................... 16

BEST PRACTICES .................................................................................................................... 16
ECS Settings ............................................................................................................................ 16
Load Balancer ......................................................................................................................... 16
CloudPools Settings ............................................................................................................... 16
File Pool Policies .................................................................................................................... 18
Encryption ............................................................................................................................... 19
Compression ............................................................................................................................ 19
Snapshots ................................................................................................................................ 20
Protecting SmartLink Files .................................................................................................... 20
Deleting a Cloud Storage Account ......................................................................................... 20
Architectural Considerations .................................................................................................. 20

PERFORMANCE ..................................................................................................................... 21

PROOF-OF-CONCEPT TESTING RECOMMENDATIONS .................................................... 21

STEP-BY-STEP CONFIGURATION EXAMPLE ..................................................................... 22
ECS Configuration .................................................................................................................... 22
Optional Load Balancer .......................................................................................................... 28
Isilon Configuration ......................................................................................................................... 29
Optional: Setup DR to Protect Access to CloudPools Data Using SyncIQ ................................. 35

FAILOVER / FAILBACK EXAMPLES .......................................................................................... 37
  Failover to Secondary Isilon Cluster .......................................................................................... 37
  Failback to Primary Isilon Cluster ............................................................................................. 39
  Failover to Secondary ECS Site ................................................................................................. 42

SUMMARY ..................................................................................................................................... 43

REVISION HISTORY .................................................................................................................... 43
EXECUTIVE SUMMARY
In any enterprise, the need to store ever increasing amounts of data continues to grow year over year. As the volume of aging data increases enterprises need to reduce their retention costs, while freeing up primary storage for more frequently accessed data. Dell EMC Isilon CloudPools software provides policy-based automated tiering that lets you seamlessly integrate with the cloud as an additional storage tier for the Isilon cluster at your data center. This allows you to address rapid data growth and optimize data center storage resources by using the cloud as a highly economical storage tier with massive storage capacity.

CloudPools uses custom policies that include built-in security that transparently moves less active data automatically from an Isilon system to a lower cost cloud storage solution. Importantly, although data has moved it is completely transparent to applications and users whose access remains unchanged.

Dell EMC Elastic Cloud Storage (ECS) is a massively scalable enterprise-grade private cloud solution that provides extremely high levels of storage efficiency, resiliency and simplicity. All data is automatically balanced which optimizes capacity and performance and allows for performance to scale with capacity growth.

Because both products are developed and supported by Dell EMC you gain all the benefits of a solution that has been fully tested together as well as single vendor support.

Additional benefits of combining Isilon and ECS together with CloudPools include:

- Reclaim space on existing Isilon primary storage systems
- Reduce on-going primary and backup storage acquisition costs
- Remove static data out of the recurring backup process
- Reduce management and operation costs
- Co-location benefits such as lower data residency risks, lower networking costs as well as lower latency

Further you can easily configure geographic replication to ensure your data is available from multiple sites in case of site-wide failures.

In summary, CloudPools enables you to optimize storage resources and gain cloud scale storage capacity while reducing overall storage costs.

AUDIENCE
This white paper is intended for architects and administrators interested in learning how CloudPools work, architectural best practices as well as built in options for multi-site availability. There is also a step-by-step configuration example to show how easy it is to configure.

Although CloudPools support a number of public and private cloud targets including Dell EMC Isilon, Dell EMC ECS, Virtustream Storage Cloud, Amazon AWS, and Microsoft Azure, this paper focuses on integration with ECS.
ARCHITECTURAL OVERVIEW

CloudPools is a feature of Isilon’s OneFS that provides off-cluster tiering of cold or infrequently accessed data to cloud storage. It uses file pool policies to govern the placement and retention of tiered or archived files. Figure 1 shows how CloudPools extend the Isilon namespace to the cloud allowing applications and users to seamlessly retain access the data via the same network path and protocols regardless of where the data physically resides.

Figure 1) CloudPools Overview

The tiering of data is driven by policies defined on the Isilon cluster using configuration management options such as a Web UI, CLI or PAPI. Some CloudPools storage options include:

- Encryption and Proxy Support: To secure data that will be sent to the cloud, CloudPools can encrypt the data as well send it via a proxy before sending it to the ECS cloud.
- Compression: In order to optimize network performance files can be compressed before being sent to the cloud.
- On disk cache: Can reduce bandwidth cost by eliminating fetching of file contents for repeated read/writes
- Data retention policies: defines how long data should live in the cloud

Data archived to the cloud can be accessed by clients via a variety of protocols including SMB, NFS, HDFS and SWIFT.

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, for example between X410 nodes to NL410 nodes. CloudPools adds the ability to tier data outside of an Isilon cluster.

The SmartPools data tiering framework enables multiple levels of performance, protection, and storage density within the same file system. This allows you to define the value of the data within your workflows based on policies, and automatically aligns data to the appropriate price/performance tier over time.

With SmartPools, data movement is seamless, and with file-level granularity and control via automated policies, manual control, or API interface, you can tune performance, data layout, storage tier alignment, and protection settings – all with minimal impact to your end-users.

File Pool Policies

Both CloudPools and SmartPools use the same file pool policy engine to define which data on a cluster should live on which tier, or be archived to the cloud. The SmartPools and CloudPools job has a customizable schedule that runs once a day by default. If data matches the criteria specified in a policy, those files are moved to the desired cloud storage repository during that particular job run.
Cloud Data Object (CDO)

In order to optimize performance of objects being sent to the cloud, files are split into 1MB chunks called Cloud Data Objects (CDO). If a file is less than 1MB in size, the CDO size is equal to the size of the file. The CDOs are moved to the ECS cloud.

SmartLink (Stub)

After a files' data has been archived to the cloud, the file on the Isilon system gets truncated to an 8KB SmartLink file (called a stub file in OneFS 8.0). Each SmartLink file contains metadata that records the specific instructions (contained in the file pool policy) used to archive the file. In addition each SmartLink file contains a data cache and a map. The data cache is used to retain a portion of the file data locally (for faster local access). The map points to all cloud data objects used to store the file. Figure 2 shows the contents of a SmartLinked file and the objects stored in the cloud (ECS system).

Figure 2) SmartLink Files

Note: With default replication settings after file data has been flushed from cache the SmartLink files consume ~26K (8K * 3 times replication + metadata).

Archiving Files to ECS

Archiving is the process of copying files from the local Isilon cluster to a remote account set up in ECS. Files can be archived either using the SmartPools Job or from the command line.

File pool policies are used to set selection criteria for files, specify a cloud target, and optionally cloud-specific attributes. When a file pool policy is configured, the system queues the policy in a SmartPools job that is run by the OneFS Job Engine. When the job runs, the system looks for files matching the pattern specified in each file pool policy. When a file matches a file pool policy that contains cloud-specific parameters, CloudPools copies the file data to the designated cloud target. After the file data is copied, its copied content is removed, leaving behind the SmartLink on the Isilon cluster.

Figure 3 shows the basic workflow – in this case the policy is defined to select files older than 6 months and to archive them to the ECS system.

Figure 3) Archive Workflow from Isilon to ECS
Protocol Access

The SmartLink files provide users and applications transparent access to the tiered/archived data. Client applications continue unchanged when CloudPools are in effect; the only difference in accessing an archived file would be the increase in time to retrieve it from the cloud. Data stored in the ECS cluster is accessible by Isilon clients using SMB, NFS, HDFS, and SWIFT protocols. Note that the data cannot be accessed directly from the ECS system.

Figure 4 shows how users and applications access the data from the Isilon cluster. Unbeknownst to them they are actually accessing SmartLink files which fetch the requested blocks from the ECS system and return them to the requested user or application.

Local Data Cache

Caching is used to support read/write of the SmartLinked files. It reduces bandwidth cost by eliminating fetching of file contents for repeated read/writes, and increases the write performance for SmartLinked files. The local cache will contain:

- Archived file updates: If an archived file is updated, CloudPools first writes those changes in the local cache and then periodically sends the updated file data to the ECS system.
- Data read by the client if read ahead is enabled

The local data cache is always the authoritative source for data. CloudPools always looks for data in the local cache first. Only if the portion of the file(s) being accessed is not in the local data cache, CloudPools fetches the data from ECS. CloudPools provides configurable settings:

- Cache Expiration: specifies how long since last access time to retain archived data in the local data cache.
- Write-back frequency: specifies how often archived file updates are written to the ECS system
- Cache read ahead: whether to cache only the part of an archived file being read or the entire file
- Accessibility: whether to cache archived file locally or not during a read operation
Logical Space Usage

The goal of tiering is to free up space on your Isilon systems consumed by less frequently accessed data. The main activities that affect space usage by CloudPools are archiving, reading, updating and recall.

- **Archive**: during the archive process, file data is broken up into 1 MB chunks and sent to the ECS system. The original on-cluster file is replaced by a SmartLinked (stub) file which takes up 8 KB of space on the Isilon system.

- **Read**: refers to client data access, also known as inline access. When a client opens a file for read, by default, the blocks read will be added to the cache in the associated SmartLink file; this can be disabled by setting the accessibility option to not cache archived files. Optionally, cache read ahead can be enabled, which will read the entire file into cache instead of just the portion being requested. Space taken up will be equivalent to the size stored in cache plus the SmartLink file which contains the mapping information to the full file data in ECS. The space used by the cache is temporary; the cache expiration setting determines how long the system retains cache information in SmartLink files.

- **Recall**: restores the full file to the Isilon cluster and overwrites its associated SmartLink file. This will also completely remove the associated CDO from the ECS system. Recall can only be performed on the Isilon cluster using the CLI command `isi cloud recall`.

- **Update**: if a user makes changes to an archived file, CloudPools first writes those changes in the local cache and then periodically sends the updated file data to the ECS system. The space used by the cache is temporary; the cache expiration setting determines how long the system retains cache information in SmartLink files.

Figure 5 shows an example of space usage after a 2 MB file is archived to ECS, then after 100KB is read and finally after the entire file is recalled back to the Isilon system. This example is using default cache and accessibility configuration options.

---

**CloudPools Data Retention**

When data is archived to an ECS system, the advanced CloudPools settings defined in the file pool policy assign a retention period to the cloud data. The retention period is used to determine how long to keep the cloud data objects (CDO) for a file whose SmartLink file has been deleted. There are three different retention periods; if more than one applies to a file then the one that is the longest is applicable:

- **Cloud Data Retention Period**: this determines how long to keep CDO after the SmartLink file has been deleted. This default is one week.

- **Incremental Backup Retention Period**: this is applicable for both incremental NDMP backups as well as SyncIQ® replications that include SmartLink files. Here again if the SmartLink file is deleted on the primary Isilon system you still want to have access to the associated cloud objects in the case where you restore the SmartLink files from either the SyncIQ destination or from NDMP incremental backup. This default is 5 years.
- **Full Backup Retention Period:** this is applicable for NDMP full backups containing SmartLink files. The default is five years. If the SmartLink file is deleted locally you still want to retain the cloud data objects so that if you perform a restore of the full NDMP backup, the recovered SmartLink files still have access to the associated data in the ECS system.

Once the retention period on the file has passed, then the Isilon cluster sends a delete command to ECS who will mark the associated objects for deletion. The user’s view of system utilization, through metering and chargeback reports is updated asynchronously and will reflect the reduced object count and capacity. The space however will not be reclaimed until garbage collection completes for the associated ECS chunks. This is a low priority background process that can take five or more days to fully reclaim the space depending on how busy the system is.

Let’s walk through an example:

1) File pool policy sets the following retention policies:
   - Full Backup Retention: 5 years
   - Incremental Backup Retention: 3 years
   - Cloud Data Retention: 1 week

2) File1 is archived.

3) Incremental backup is run that includes File1’s SmartLink file.

4) One year passes and File1’s SmartLink file is deleted.

5) Given the retention policies, the Isilon cluster will send a delete command to the ECS system three years later. This means the associated cloud data objects would be retained on the ECS system for three years after the SmartLink file was deleted.

### HIGH AVAILABILITY

Both Isilon and ECS are enterprise storage solutions that are designed to survive the loss of nodes and disks. By utilizing different levels of erasure coding and mirroring ECS and Isilon are able to provide high levels of data protection with low storage overhead. They also provide options that offer protection against site wide failures. With CloudPools it is important to not only ensure resiliency of the data stored in the ECS system but also the SmartLink files since these are necessary to provide access to the data stored in the ECS system.

#### Protecting SmartLink Files

The only way to protect SmartLink files, and therefore access to the data stored in the ECS system in the event of an Isilon cluster failure is via a SmartLink aware backup utility – namely NDMP or SyncIQ. Traditional copy commands will not work; the resultant file will be corrupted.

If you have only a single site or limited WAN bandwidth between sites you may choose to protect the SmartLink data using NDMP backups. NDMP-based backup solutions will back up the SmartLink files without recalling the files however, it can take a significant amount of time to fully complete a restore of this data.

If you have multiple Isilon sites it is recommended to replicate the data using SyncIQ. SyncIQ is a licensed feature that enables you to have a consistent replica of your data on another Isilon cluster. This provides a simple way to quickly regain full access to data in the ECS system in the case of an Isilon site failure.

SyncIQ uses directory level policies to determine what data to replicate between Isilon sites as well as the replication frequency. You can setup policies that can replicate all files in a particular directory, exclude certain directories or you can choose to exclude specific files. Note: Although excluding specific files can be configured by selecting file matching criteria within a SyncIQ policy, it is not recommended since it will prevent you from being able to perform a failback operation.

SyncIQ is CloudPools aware; and if the OneFS version on the target cluster is 8.0 and higher, it recognizes SmartLink files and by default, replicates them without pulling down the data from the ECS system. The directory you are replicating can contain a combination of unarchived files as well as SmartLink files. When SyncIQ replicates SmartLink files it also replicates secondary information associated with a SmartLink file such as local cache state and unsynchronized cache data.
Note: If your destination Isilon cluster is pre-OneFS 8.0, or you have a specific reason that you need to replicate full file data to the second Isilon cluster then you can select the SyncIQ policy option “Deep Copy”. Enabling deep copy can significantly increase the amount of time to complete replication.

Figure 6 shows how both unarchived and SmartLinked files are replicated using the SyncIQ policy that specifies to replicate all files from /ifs/images from site 1 to site 2.

Figure 6) SyncIQ Replication

SyncIQ supports two types of replication policies: copy and synchronization. Copy policies are mainly used for archival purposes and only maintain recent versions of files stored on the source cluster; they do not support failback. For CloudPools it is more common to use a synchronization policy which maintains an exact replica of the source directory on the target cluster and support fail over and fail back operations.

In normal operation, SyncIQ only allows write access to replicated data on the source Isilon cluster. The target Isilon cluster will have only read access to the data, regardless of whether it is stored locally or has been archived by CloudPools.

In the event the source Isilon site has an outage, fail over operations can be run by transferring write permission to the target site and redirecting users and applications to the secondary cluster where they can continue to access, view and modify their data. If the source system comes back online fail back operations can be run. During failback, any changes made to the data on the secondary cluster are resynced to the primary cluster by means of a replication job using a mirror policy. After the changes are successfully copied back, the write permission can be taken away from the secondary cluster and given back to the source.

Note: The target cluster must be running a minimum OneFS version of 8.0 in order to replicate the SmartLink files. If it is running less than 8.0, deep (full) copy is only possible. Both clusters must be licensed for SyncIQ, SmartPools and CloudPools in order to provide correct replication, failover, and failback.

Note: If you are encrypting the data being sent to ECS, both SyncIQ and NDMP will also sync all the relevant encryption keys to the secondary cluster or backup target along with the SmartLinks.

Caution:
- Do not break an association between the source and target clusters unless you want this removed permanently. This can result in either a full or large differential replication to occur the next time you run the replication policy.
- Be cautious of making changes such as changing the DNS record of the target cluster. This can cause an error condition that effectively breaks the association between source and target clusters. This can result in either a full or large differential replication to occur the next time you run the replication policy. We recommend contacting Dell EMC support before making configuration changes that affect how the clusters connect together.
Protecting the Data Stored in the ECS System

ECS includes support for geo-replication which provides access to data from multiple sites as well as data redundancy in case of site failure. This requires:

- more than one ECS site is federated together
- a replication group is configured with more than one ECS site (known as a Virtual Data Center or VDC)
- namespace to be used for CloudPools is configured with a replication group that has more than one VDC

See the configuration example later in this document for step-by-step details on how to configure this.

Once configured any data sent to the ECS system from CloudPools will automatically be replicated to the other site(s) configured in the replication group. Replication to the other site(s) is an asynchronous process. Chunks are added to a queue to be sent over and worker I/O threads continuously process the queue until it is empty. The site that receives replicated chunks will be responsible for local data protection (erasure coding and triple-mirroring).

Figure 7 shows how ECS geo-replication works with CloudPools data.

Figure 7) Protecting Data Stored in the ECS System with Automatic Replication between ECS Sites

NOTE: Data is compressed when sent to other site and any data encrypted using D@RE will also remain encrypted when sent.

In a geo-replicated environment where you have ECS encryption enabled, when a new ECS system joins an existing system (referred to as a federation), the master key is extracted using the public-private key of the existing system and encrypted using the new public-private key pair generated from the new system that joined the federation. From this point on, the master key is global and known to both systems within the federation.

In the event the ECS site that is the Isilon CloudPools target has an outage:

- the CloudPools account may need to be changed to point to the second ECS system unless redirection is done by something like a load balancer that can detect the site failure and redirect traffic to the backup site
- data can continue to be accessed (read, created and updated) if “access during outage” (ADO) is enabled in ECS on the CloudPools buckets

If the site comes back online any changes made while it was down will be asynchronously replicated back to it. If the failure is permanent you should perform failover operations using the ECS UI. As an example, in the previous figure, if “access during outage” is enabled on the CloudPools buckets and Site 1 was unavailable, the Cloud Storage Account could continue to archive, read and recall the CloudPools data from ECS Site 2.
Combining Isilon SyncIQ with ECS Geo-Replication

SyncIQ and ECS Geo-Replication work together to protect your data access in the event that you have a site wide failure that contains both the Isilon and ECS primary systems as illustrated in Figure 8.

Figure 8) Data Remains Accessible After Site-Wide Failure of Both ECS System and Isilon Cluster
CONFIGURING CLOUDPOOLS ON MULTIPLE SITES

You can use SyncIQ and ECS Replication Group to configure a multi-site architecture, with each site replicating to the other site. Figure 9 shows an example of a two site configuration whereby each site has an Isilon cluster and ECS system that replicate to each other.

Figure 9) Two Site CloudPools and SyncIQ Configuration

In this configuration CloudPool1 tiers data from Site1 Isilon cluster to Site1 ECS system. Similarly Site2 has a CloudPool2 that tiers data to its local ECS system. It then uses SyncIQ and ECS replication group to replicate data between sites. In this scenario all data access is performed locally however in the event of a site-wide failure fail over operations can make both CloudPools’ data available from the site that remains available.

ENCRIPTION

Both Isilon and ECS provide options to encrypt data. Isilon encryption is a configurable user-option in the Cloud Pool Policy. When a file is archived to the cloud, and encryption is enabled, each Cloud Data Object (CDO) is encrypted by a Data Encryption Key (DEK). Each DEK is in turn encrypted by the Master Encryption Key (MEK). This MEK is stored in OneFS’ key management system and there is one MEK per cluster. The encrypted DEK is stored along with the MEK’s ID in the Cloud Management Object (CMO) for a file. The CMO is stored in the cloud along with the CDOs for a file. When the file is recalled from the cloud, the file chunks are decrypted. Cached data is therefore decrypted. AES256 is used in cloud pool encryption. Encryption is transparent to the end-user. The encryption keys are managed on the Isilon side using the OneFS key management system.

For Failover or Disaster recovery purposes, it is highly recommended to use SyncIQ to copy the SmartLinks from the primary Isilon cluster (The cluster that has moved the data to ECS) to a secondary cluster. SyncIQ (and NDMP) is aware of CloudPools and syncs all the relevant encryption keys to the secondary cluster (or backup target) along with the SmartLinks.

ECS version 2.2 and later provides a licensed option for adding Data at Rest Encryption (D@RE) which provides server side encryption (SSE) and supports S3 encryption semantics, e.g. x-amz-server-side-encryption. In CloudPools when D@RE is enabled on ECS, key management is done automatically. Server-side encryption (SSE) encrypts data inline prior to it being stored on disk. SSE follows the FIPS-140-2 Level 1 compliance, AES256 algorithm.
SYNCIQ
SyncIQ, is SmartLink aware and will replicate SmartLink files to a destination cluster. During a failover scenario, the target cluster is connected to the cloud and the users will have seamless access to on premise and tiered files (requires both clusters have proper licenses and minimum OneFS 8.0).

SNAPSHOTIQ
Files with existing snapshots can be moved to the cloud target using CloudPools however it will not result in space savings on Isilon until all the snapshots pointing to the file have expired.

SMARTQUOTA
SmartQuota monitors and enforces administrator-defined storage limits within an Isilon cluster; it does not enforce a limit on the amount of user or directory space used by data archived to ECS. An archived file is only charged for the space used by the SmartLink file, thus CloudPools has the effect of allowing user and/or directories to logically, but not physically, exceed the quota space in SmartQuota on the Isilon cluster.

It is therefore important to be aware that for recalled files, the full file size counts against quotas. As an example, if a 1G file is archived, only the remaining SmartLink file size is counted against the quota. If the file is recalled, the full 1G will be counted against the quota. As such, it is recommended to only recall files as needed and then if appropriate re-archive them so as to not exceed quotas.

Space usage can also temporarily be affected if you are caching cloud data in SmartLink files when a user or application accesses a SmartLink file on the cluster.

SMARTLOCK
CloudPools does not support archiving or recalling files that are SmartLock protected. If an environment contains SmartLock directories, they should be excluded from being archived using appropriate policy settings.

DEDUPE
It is possible to SmartLink an already de-duped file. However, recalling the data will create a 'un-de-duped' file.

CLONING
Cloning of SmartLink files is prevented.

NDMP-BASED BACKUP
NDMP-Based backup solutions will back up the SmartLinks without recalling the files.

CLIENT-BASED TOOLS
Avoid running SMB or NFS client-based tools such as AVScan or a backup application as this causes the file data stored in ECS to be fully cached back to the SmartLink files.

SMARTLINK FILE ACCESS DIRECTLY FROM THE ISILON CLUSTER
SmartLink files can only be read or written by clients. You cannot edit or read a SmartLink file directly on the Isilon cluster. The following commands are also blocked on SmartLink files on the Isilon cluster: tar, gzip, scp, AVscan and job engine jobs.

ALTERNATE DATA STREAMS
If a file has one or more alternate data streams (ADS), like other files, the file’s contents are archived and recalled by CloudPools. Any ADS data will be included as part of the SmartLink for the file.

SMB OPLOCK
SMB Oplock (lease/notification) does not work in cases where you create a file with the SUPERCEDE flag, and the file already exists and is archived.
**REQUIREMENTS**

CloudPools is a licensed OneFS feature that requires both a CloudPools and SmartPools license.

A minimum of OneFS 8.0 is required.

**BEST PRACTICES**

This section details specific recommendations for architecting a CloudPools configuration to ECS.

**ECS SETTINGS**

When configuring ECS for use as a CloudPools destination there are some best practice configurations that should be followed. These include:

- **Virtual Data Center**: If you want your data to be replicated to a second site you must setup multiple virtual data centers (VDC) that are federated together.

- **Replication Group**: Ensure you have a replication group that is configured with your preference for replication level by enabling or disabling “Replicate to All Sites”; this can’t be changed after the replication group is created.

- **Namespace configuration:**
  - Create a namespace that will be exclusively for CloudPools.
  - **Server-side encryption**: Before configuring a namespace the administrator should determine if they require ECS to encrypt the data (see Encryption section below for details). If so, then encryption must be enabled when creating the namespace, it can’t be enabled or disabled after the namespace is created.
  - **Replication group**: Ensure you select a replication group that is configured with your preference for replication level. The default replication group selected when creating the namespace will be the one used by the CloudPools account to automatically create the buckets, this can’t be changed after the bucket is created.
  - **Retention Policy**: Since data is only available as long as the Isilon SmartLink exists it is recommended to not configure a retention period on the namespace, instead let the file pool policy control this.

- **Bucket configuration**: Since data is only available as long as the Isilon SmartLink exists there is no benefit to retaining objects beyond this time. Therefore, it is recommended to not configure a retention period on the namespace, instead let the file pool policy control this.

**LOAD BALANCER**

CloudPools connects to ECS using a single hostname or IP address. Therefore, it is recommended to use a scalable load balancer to evenly distribute the load across all ECS nodes.

**CLOUDPOOLS SETTINGS**

CloudPools provides settings to modify data retention settings as well as accessibility and cache settings.

These settings can be modified in the default template or on a per file policy basis. The default settings used when you create a file pool policy come from the Cloud Pools Settings tab in the Storage Pools section of the UI as illustrated in Figure 10. Because the default settings are good for most file pool policies it is not recommended to change the default template which is available in the CloudPools Settings tab in the Storage Pools section of the UI.

*Figure 10) Do Not Modify CloudPools Template Settings*
Instead, if any changes to these settings are preferred, they should be changed on a per file pool policy basis which can be found in the advanced section of the CloudPools options in the file pool policy as illustrated in Figure 11.

Figure 11) Advanced CloudPools Settings in the File Pool Policy

**Data Retention Settings**

It is recommended to explicitly set the retention settings for the data being moved by CloudPools to ECS. Even if the SmartLinks are getting backed up via SyncIQ or NDMP and your environment has specific retention settings for those backups, the retention settings set on the file pool policy configuration will be applied to the data stored in ECS.
Local Cache Settings

Caching is used to support read/write of the SmartLinked files. It helps in reducing bandwidth cost by eliminating fetching of file contents for repeated read/writes. It helps in increasing the write performance for SmartLinked files. The local data cache is always the authoritative source for data. CloudPools always looks for data in the local cache first. Only if the portion of the file(s) being accessed is not in the local data cache, CloudPools goes and fetches the data over WAN. CloudPools also provides configurable settings to expire the cache if no writes have happened. It also has a configurable setting for write-back to the cloud in case the cached data gets modified.

If the disk space on the source Isilon is limited, then it is recommended to reduce the ‘Writeback Frequency’ and ‘Cache Expiration’ values in the CloudPools settings to lower numbers. This will reduce the amount of time that data (both dirty and clean) stays in the cache and thereby, frees up disk space sooner.

Snapshots

Since data contained in a snapshot does not provide space savings on the Isilon system, it is recommended to exclude snapshot files by unchecking the default CloudPools setting “Archive files with snapshots”.

FILE POOL POLICIES

File pool policies are the mechanism to define the dataset that will be moved to ECS. It is therefore, important to create policies optimally.

- Ensure the priority of your custom file pool policies is set appropriately. When the SmartPools system job runs, it processes the file pool policies in descending order according to their position in the file pool policy list. You can set custom policies higher or lower priority by moving it up or down in the list.

- When creating a file pool policy for CloudPools, it is recommended to explicitly set the retention settings. Even if the SmartLinks are getting backed up via SyncIQ or NDMP and your environment has specific retention settings for those backups, the retention settings set on the file pool policy configuration will be applied to the data stored in ECS.

- CloudPools are most effective at space savings on larger files. It is recommended to not archive files that are <30K in size.

- It is recommended to not archive files that users or applications will continue to make modifications to. Using timestamps in your file pool policy provides an efficient way to determine what data is best suited to archive to ECS. As an example specifying file-matching criteria for files that haven’t been modified for more than a defined period of time.

- In order to avoid superfluous error messages, avoid including directories that run Antivirus software. The anti-virus software will generate error messages on the SmartLink files. If you do include these directories you should make a note that these messages can be safely ignored.

- OneFS supports a maximum of 128 file pool policies (SmartPools and CloudPools combined) although it is recommended not to exceed 30 file pool policies per Isilon cluster.

- Within a file pool policy that archives files to ECS you can control where the locally-retained SmartLink files are stored by specifying a SmartPools target as well as a CloudPools target.

- Changing file matching criteria only affects what files will be archived to ECS, it has no impact on files already archived to ECS. As an example if your file pool policy archived files that hadn’t been accessed in 6 months all files matching that criterion would be archived to ECS. If later you modified the file pool policy to instead archive files that hadn’t been accessed in 1 year it would not recall any of the files that have already been archived to ECS regardless of if they meet the new file matching criteria. Further if you modified a file that is already archived to ECS, so that its last modified time is recent, the file will be updated however will remain in ECS.

- When you recall a file from cloud storage, the full file is restored to its original directory. If the file pool policy that originally archived the file to the cloud is still in effect, the next time the SmartPools job runs, the recalled file is archived to the cloud again. If you do not want the recalled file to be re-archived, you can move the file to a different directory that would not be affected by the file pool policy, or you can modify or delete the policy.
**ENCRYPTION**

Encryption is an option that can be performed either on the Isilon system prior to data being sent to ECS, or on the ECS system itself, it shouldn’t be done on both. Unless your Isilon system averages high CPU (>70%) the recommendation would be to enable encryption on the Isilon file pool policy instead of on the ECS namespace. This adds the value of having only encrypted data being sent over the network.

Encryption can be enabled on a per file pool policy basis on the Isilon cluster in the CloudPools settings section of the file pool policy as illustrated in Figure 12.

Figure 12) Enabling Encryption in the File Pool Policy

![Create a File Pool Policy](image)

It is important to note that encryption adds additional load on the system performing the encryption and can also impact the archive and recall speed.

**COMPRESSION**

CloudPools provides an option to compress data before it is sent to the ECS system. If network bandwidth is a concern then enabling CloudPools compression can help. If not then the ECS system will automatically compress the data in order to optimize space utilization.

Compression can be enabled on a per file pool policy basis on the Isilon cluster in the CloudPools settings section of the file pool policy as illustrated in Figure 13.

Figure 13) Enabling Compression in File Pool Policies

![Create a File Pool Policy](image)

Both CloudPools and ECS skip compression attempts on data that have previously been compressed thus saving system resources attempting to compress the same data again.

It is important to note that, encryption and compression though highly useful features can create additional load on the Isilon cluster and the time to archive data to ECS may increase.
SNAPSHOTS
Files with existing snapshots when moved to the cloud using CloudPools will not result in space savings on Isilon until all the snapshots pointing to the file have expired. It is therefore recommended to uncheck the default CloudPools setting that allows excluding files with existing snapshots from being archived. After the Snapshots expire, the next time the file pool policy runs, these files will be moved to the ECS system and you will get space savings on the Isilon system. In order to gain the most benefit from tiering data to the ECS system, it is recommended to regularly delete older snapshots that are no longer needed on your Isilon system.

Figure 14 illustrates how to uncheck the option to archive files with snapshots.

Figure 14) Uncheck Archive Files with Snapshots

CloudPools also supports SnapRevert for SmartLink files. If a SnapRevert job is run against a directory that has files moved to the ECS storage, this will result in the original files being restored on the Isilon system. CloudPools will also remove any cloud data that was recreated on the Isilon system as a result of the SnapRevert job running.

PROTECTING SMARTLINK FILES
SmartLinks are the sole means of accessing the data stored in ECS. It is therefore important to protect the SmartLinks from accidental deletion as well as for failover/disaster recovery purposes. It is highly recommended to setup a scheduled SyncIQ backup of the SmartLinks for at least once a day to a second Isilon cluster. Optionally, the SmartLinks can also be backed up using traditional NDMP backups.

Note: Do not use copy commands such as scp (secure copy) to copy a SmartLink file from one cluster to another, the resultant file is corrupted.

DELETING A 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.

ARCHITECTURAL CONSIDERATIONS
- Do not activate CloudPools while your system is actively performing a OneFS rolling upgrade.
- It is important that all the nodes in the Isilon cluster have network connectivity to the ECS system. If one of the nodes does not have network connectivity the archiving process can hang.
- If your ECS system is not on the same network as your Isilon system starting with OneFS 8.0.1 CloudPools can be configured to work with a proxy server.
PERFORMANCE

Archive and recall performance is highly dependent upon many factors including the network bandwidth between the Isilon cluster and the ECS system, available system resources and file size. However, as an example we tested archiving and recalling 1GB files between an Isilon X210 cluster connected via a load balancer to a four node ECS U2800 system all connected on the same 10GB network as illustrated in Figure 15.

Figure 15) CloudPools Test Setup

With this configuration we achieved near linear scalability on our tests of a three, four and five node Isilon X210 cluster showing ~100MB/s/Isilon node for archive and ~85MB/s/Isilon node for recall throughput of 1 GB files. These results were achieved in the specific configuration stated. Typical environments would have additional load on the systems and may include network latency and as such will have different performance results.

Running one or many file pool policies in parallel does not impact the total archive and recall throughput. As an example if you wanted to archive 100GB of data, running one file pool policy would provide the same throughput as running two policies each against 50GB of data.

CloudPools defaults to 10 threads per node which balances CloudPool CPU usage with other cluster functions. While we recommend the default number of threads for typical workloads CloudPools does provide an option to modify the number of archive and recall threads. 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. Before making any changes to thread count you should consider the following:

- Increasing thread count will not have any impact if your infrastructure does not have sufficient network bandwidth to accommodate the increased archive and recall throughput.

- Do not increase archive thread count if you have other high priority activity on your Isilon cluster during archive times or CPU usage is >50% already during archive times.

- Do not increase recall thread count unless you want to prioritize recall performance; doing so increases CPU usage on the cluster for recall operations during which time it can impact the performance of other cluster jobs.

- Do not make changes to thread count in production until you have tested this change and fully understand the impact on your environment.

In our testing, we found setting archive threads to 20 and recall threads to 40 to be ideal although we had sufficient network bandwidth to handle the load and no other higher priority activity required the CPU during these times.

If you want to configure higher number of threads please contact support.

PROOF-OF-CONCEPT TESTING RECOMMENDATIONS

If you plan to run tests before implementing CloudPools into production it is recommended to modify the retention periods to low values (perhaps 1 day) on the file pool policies you are using so as not to keep the CDOs longer than needed. Remember to then set appropriately before implementing in production.
**STEP-BY-STEP CONFIGURATION EXAMPLE**

CloudPools is extremely easy to setup and manage simply requiring:

1. ECS Web UI: Namespace and Object User with S3 credentials
2. Isilon Web UI or CLI:
   
   a. Cloud Storage Account: To set the credentials required to connect to ECS. Also automates creating buckets on the ECS system that will contain the data archived by CloudPools.
   
   b. Cloud Pool: A logical container containing the previously created account
   
   c. File Pool Policies: Policies that define what data needs to be tiered from Isilon to ECS

This section provides an example of how to configure ECS and Isilon and setup CloudPools.

**ECS CONFIGURATION**

ECS requires a storage pool, virtual data center, replication group, namespace and an object user with a S3 password. If these aren’t already created follow these instructions to create them. If they are you can skip ahead to the Isilon configuration section.

From the ECS UI login as a user assigned to the system admin role.

**Step 1: Storage Pools**

Storage pools are used to group nodes and their associated disks within a single site. If physical separation is required for different data or business units multiple storage pools can be created within the same site. Data will be distributed across nodes within a storage pool. As an example, if you had 16 nodes and you wanted to physically isolate sales data from engineering data, providing more space for engineering data, you would setup two storage pools. You could assign nodes 1 – 4 to the sales storage pool and nodes 5 – 16 to the engineering storage pool.

If a storage pool containing the nodes you want to have the CloudPools data written to is not already created, select New Storage Pool.

**Figure 16) Create a New Storage Pool**

![Create a New Storage Pool](image)

Give the storage pool a name and from the available nodes, click on the + icon next to the nodes you would like to be used to store the CloudPools data. Storage pools require a minimum of four nodes. Optionally you can enable cold storage which uses an erasure coding with higher efficiency and requires a minimum of six nodes. See the [ECS Administrator’s Guide](#) for more details on cold storage and erasure coding schemes.

**Figure 17) Add Nodes to Storage Pool**

![Add Nodes to Storage Pool](image)
Step 2: Virtual Data Center

A virtual data centers (VDC) is a logical construct that contains a collection of ECS nodes that are managed as a single unit; typically a VDC contains all ECS nodes within a single site.

If a VDC containing the IP addresses for the nodes you want to have the CloudPools data written to is not already created, select New Virtual Data Center.

Figure 18) Create a New Virtual Data Center

Provide the following:

- A name for the virtual data center.
- 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 if a separate replication or management network is configured this will be that IP addresses for each node. If network separation is not configured, both replication and management endpoints will be the same.
- Select to generate a key.

If you wish to setup multiple sites refer to the ECS Administrator’s Guide for details on adding additional VDCs to a federation.

Figure 19) Configure New Virtual Data Center
Optional: Second Site Configuration

If you want your data to be replicated to a second site you will have to setup multiple virtual data centers (VDC) that are federated together.

Login to the second site’s portal and configure your storage pool. Then navigate to Manage → Virtual Data Center and select Get VDC Access Key. **Warning:** Do not create a new VDC here.

Figure 20) Get VDC Access Key from the Second Site

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.

Login to the first site’s portal and navigate to Manage → Virtual Data Center and select New Virtual Data Center. From here provide the following:

- A name for the second virtual data center.
- Paste the VDC Access Key that you copied from site 2 here
- 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 is configured this will be that IP addresses for each node. If network separation is not configured, both replication and management endpoints will be the same.

Figure 21) Create VDC for Second Site
Step 3: Replication Group

A replication group is a logical construct that defines if data within a storage pool is only written locally or if it can be replicated to other sites or virtual data centers.

If a replication group isn’t configured the way you want to have the CloudPools data availability setup, select New Replication Group.

Figure 22) Select New Replication Group

Provide the following:

- Give the replication group a name.
- If you plan to have multiple sites (multiple VDCs) that you want the data to replication to, select your 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 performance & data durability but has the lowest space efficiency
  - Disable: maintains one additional copy of data at another site in the VDC. Regardless of the number of sites you will always have 2 copies of the data
  - The setting is ignored for single site replication groups.
- Add the appropriate virtual data centers and storage pools.

See the ECS Administrator’s Guide for more details on replication groups.

Figure 23) Configure Replication Group
Step 4: Namespace

A namespace is a logical construct that provides tenant isolation. Users from one namespace can only access objects within their own namespace, they can’t access objects that reside in another namespace. It is recommended to create a namespace that is dedicated to CloudPools usage.

If a namespace isn’t configured for the CloudPools data, select New Namespace.

Figure 24) Select New Namespace

At a minimum you will have to provide a name for the namespace and a replication group. The replication group will determine if the CloudPools data sent to this namespace will be replicated to other ECS sites or not. It is recommended to enable “Access During Outage” so that you are able to access the data in the event of the primary ECS site being unavailable temporarily. If this is left as disabled then the data will be unavailable to be read until either the primary site comes back online or is determined to be permanently unavailable and failover operations complete. See the [ECS Administrator’s Guide](#) for more details on “Access During Outage”.

If you require the ECS system to perform server-side encryption you must enable it during the namespace creation, it can’t be changed later. Also, it is recommended not to enable file system, CAS or Bucket Retention Periods for CloudPools buckets.

Figure 25) Configure Namespace
Step 5: Object Users

Object users are end-users of the ECS object store. Objects users are defined by a username and a secret key (like a password) that they use to gain read write access to the ECS namespace. You will need to create an object user that will be used by the CloudPools to read and write data to the ECS object store. It is recommended that this user be dedicated to CloudPools access and not used to access other data written to the namespace by other means.

If an object user with S3 password isn’t configured for the namespace the CloudPools data will be written to, select New Object User.

Figure 26) Select New Object User

Provide the following:

- Give the object user a name.
- Provide it a namespace that it will be given permission to use
- Select Next to Add Passwords
- Select Generate & Add Password
- Keep a copy of the user name and the password that is generated, you will need this to configure CloudPools on the Isilon system.

Figure 27) Create New Object User and Generate S3 Password
OPTIONAL LOAD BALANCER

Although not required it is recommended to configure a load balancer that balances traffic to the various ECS nodes from the Isilon system. Without a load balancer all CloudPools traffic would go through a single ECS node. As such adding a load balancer can provide much better performance and throughput for the CloudPools. There are many hardware and software load balancer options available; here are a couple of quick configuration examples for two popular software load balancers.

Example: HAProxy

Modify the haproxy.cfg file and add the following lines to the bottom. Depending on how you prefer to connect to the ECS system you can add just port 9020 for HTTP interface or port 9021 for HTTPS interface.

Substitute <Node # S1 IP address> with each node in site 1’s external IP address, ex. if node1 site 1’s IP is 10.100.10.4 it would read: server node1 10.100.10.4:9020 check inter 10000 rise 2 fall 5

Substitute <Node # S2 IP address> with each node in site 2’s external IP address

For HTTP connections add:

# ECS S3 API HTTP Interface 9020

listen ECS_S3_API

  bind 0.0.0.0:9020 #This binds all the IPs on the load balancer, you can select a specific IP if you prefer
  balance roundrobin #You can use a different algorithm if you prefer such as leastconn
  option httpchk GET /?ping HTTP/1.1\r\nHost:\haproxy\r\nX-Emc-Namespace:foo
  option allbackups

server node1S1 <Node 1 S1 IP address>:9020 check inter 10000 rise 2 fall 5
server node2S1 <Node 2 S1 IP address>:9020 check inter 10000 rise 2 fall 5
server node3S1 <Node 3 S1 IP address>:9020 check inter 10000 rise 2 fall 5
server node4S1 <Node 4 S1 IP address>:9020 check inter 10000 rise 2 fall 5
server node1S2 <Node 1 S2 IP address>:9020 check backup inter 10000 rise 2 fall 5 # used in case of site 1 unavailability
server node2S2 <Node 2 S2 IP address>:9020 check backup inter 10000 rise 2 fall 5 # used in case of site 1 unavailability
server node3S2 <Node 3 S2 IP address>:9020 check backup inter 10000 rise 2 fall 5 # used in case of site 1 unavailability
server node4S2 <Node 4 S2 IP address>:9020 check backup inter 10000 rise 2 fall 5 # used in case of site 1 unavailability

You may also want to configure multi-threading by adding nbproc as an option under global settings. I used an nbproc value equal to the number of CPU cores in the HAProxy system. This also requires the daemon be running. Here is an example of what was added to the global section of haproxy.cfg:

global
  nbproc 20
  daemon

Note: the values after 9020 are optional and the lines for site 2 are used for access to ECS in the event ECS site 1 in unavailability
Note: for HTTPS connections duplicate the lines shown above but substitute 9020 with 9021 and change the listen line to
ECS_S3S_API. Also, the certificate would need to be on the system hosting the load balancer. As an example it would include
the following changes:

# ECS S3 API HTTPS interface 9021

listen ECS_S3S_API

bind 0.0.0.0:9021 #This binds all the IPs on the load balancer, you can select a specific IP if you prefer

server node1 <Node 1 S1 IP address>:9021 check inter 10000 rise 2 fall 5 #The values used after port 9021 are optional

Example: NGinX

Modify the nginx.conf configuration file to add the following: (substitute <Node # IP address> with each node’s external IP address, ex.
server node1 10.100.10.4:9020)

```bash
http {
  upstream ecs {
    server <Node 1 IP address>:9020;
    server <Node 2 IP address>:9020;
    server <Node 3 IP address>:9020;
    server <Node 4 IP address>:9020;
  }
  server {
    listen 80;
  }
}
```

ISILON CONFIGURATION

Isilon CloudPools are simple to setup requiring appropriate licensing and the creation of a Cloud Storage Account, a CloudPool, and a
File Pool Policy. Here is a sample configuration.

Step 1: Verify Licensing

Isilon requires both a SmartPools and a CloudPools license. Navigate to Cluster Management → Licensing and verify that both the
CloudPools and SmartPools license status is Activated.

Figure 28) Check Isilon Licensing and Verify CloudPools and SmartPools License Status Shows Activated
Step 2: Create a Cloud Storage Account and CloudPools

Isilon requires both a Cloud Storage Account and CloudPools to be created. Navigate to File System → Storage Pools.

Figure 29) Navigate to Storage Pools

Next navigate to the CloudPools tab where you can create a Cloud Storage Account followed by a CloudPool.

Figure 30) First Create a Cloud Storage Account Followed by a CloudPool
A Cloud Storage Account provides Isilon with specifics on how to access the ECS system. For the URI use port 9020 for http or 9021 for https. If you are using a load balancer then use the IP address of the load balancer here, if not then use the IP address of one of the ECS nodes. The user name and key are the name of the object user and its S3 password that was generated when we created a user in ECS.

Figure 31) Create a Cloud Storage Account That Connects to the ECS System

This results in two buckets being created in the ECS namespace we previously configured. One will start with a "d" and will be a container for the data the CloudPools sends over and the other will start with an "m" and be used to store the associated metadata. The bucket will use the default replication group and access during outage settings for the namespace it is associated with.

Now you can create a CloudPool which you configure to use the Cloud Storage Account you just configured.

Figure 32) Create a CloudPool Using the Previously Configured Cloud Storage Account
Step 3: Create a File Pool Policy

Now you can create a file pool policy that will determine the rules for what data gets sent to the ECS system. Navigate to File System → Storage Pools → File Pool Policies and select Create a File Pool Policy.

Figure 33) Create a File Pool Policy

File Pool Policies define what files you want to have moved to the ECS system and any CloudPools actions you want applied to these files.

You start out by selecting the criteria for what files you want the policy to manage. This includes:

- filename
- path
- file type
- custom user-defined file attribute
- last modification time
- last accessed time
- last metadata modification time
- creation date
- size

You can add any number of file matching criteria to refine the policy to best define the data that you want the CloudPools Policy to manage.

Next you can select which CloudPools Storage Target you want to use, this is the CloudPools Storage Account that you previously configured. Optionally, you can also specify SmartPools Actions to be applied on the selected files. Since we have configured to move data to the cloud, these actions will only be applied to the SmartLink files.

You can also select if you want the data to be encrypted or compressed prior to being moved to the ECS system.

There are also retention and cache setting options available in the advanced CloudPools settings. For more details on these and other File Pool Policy options refer to the OneFS Web Administration Guide specific to your OneFS release.
OneFS applies file pool policies in order, the first policy that matches a file controls how that file is handled. Given this you may want to evaluate if changing the order of the policy is necessary after the file pool policy is created.
Step 4: Run a File Pool Policy

By default this file pool policy is configured as a low impact background job with a priority level of 6 that will run on a default schedule that runs one policy per day starting at 10 pm. You can change the job parameters as needed by navigating to Cluster Management → Job Operations → Job Types and then editing the SmartPools job type details.

Figure 35) Edit SmartPools Job Parameters

If you want to start a specific file pool policy job manually you can run the following command substituting <files> with the individual file names or path that you want to run the policy on and <PolicyName> with the name of the specific file pool policy you created previously.

`isi cloud archive <files> --policy=<PolicyName>`

You can check that the job has completed by running the following command:

`isi cloud job list`
It may showing a status of running indicating the archive job is currently running. If so, continue to run the job list command until you see a status of completed which indicates the archive job completed.

You can validate the file archived successfully by looking running the following command on the directory that you archived and ensuring the archived files have a ssmartlinked (or stubbed) flag.

`ls -loh <path to file directory that was archived>`

Here is a sample output of a file that has successfully been archived:

```
-rwxrwxrwx + 1 root wheel inherit,writecache,wcinherit,ssmartlinked,shasntfsacl,hasads 1.0M Mar 11 01:03 scalable.rtf
```

**OPTIONAL: SETUP DR TO PROTECT ACCESS TO CLOUDPOOLS DATA USING SYNClQ**

Once data is written to CloudPools the only access method is by means of the SmartLink files. Therefore it is highly recommended that you backup these SmartLink files via SyncIQ or traditional NDMP backup.

SyncIQ will replicate the SmartLink files to a secondary Isilon cluster which will provide access to the CloudPools data in case the primary Isilon cluster becomes unavailable. Below is a sample configuration to configure SyncIQ with the CloudPools you previously configured. For complete details on SyncIQ configuration refer to the Isilon OneFS Web Administration Guide.

**Step 1: Validate Proper Licensing**

First ensure both of your systems have the proper licenses activated. To do this, on both clusters navigate to Cluster Management → Licensing and verify that they both have the CloudPools, SmartPools and SyncIQ license status as Activated.

**Step 2: Create a SyncIQ Policy**

You need to create a SyncIQ policy on the primary cluster. This will be used to replicate the SmartLinks from the primary to the second cluster. Navigate to Data Protection → SyncIQ. From here open the Policies tab and select Create a SyncIQ Policy.
At a minimum the policy requires the following:

- a policy name
- source cluster details
- target cluster details

Figure 38) Configure SyncIQ Policy

Note: Although you can set file matching criteria it is not recommended since it will prevent you from being able to perform a failback operation.
You can now start the SyncIQ policy job.

Figure 39) Start SyncIQ Policy Job

You can check the status of the job in the SyncIQ reports tab on the source/primary cluster.

Once this job completes the secondary Isilon cluster will show a local copy of the cloud storage account, CloudPools and file pool policy created in a state of disabled. This is because only one is active and the second passive. You will also see the target directory is created on this secondary cluster and it contains all of the data from this directory. This will include file data that wasn’t sent to the cloud as well as the SmartLinks for data that was sent to the cloud.

FAILOVER / FAILBACK EXAMPLES

FAILOVER TO SECONDARY ISILON CLUSTER

By setting up SyncIQ replication to a secondary cluster you have provided a way to retain access to the data stored in the ECS cloud in the event that the primary Isilon cluster becomes unavailable. Both Isilon clusters have read access to the data being replicated with SyncIQ between sites regardless of whether it is stored locally or on an ECS system. However, only one Isilon cluster can write to the Isilon directory being replicated and to the ECS system. In the event of a site failure write access must be transferred to the secondary cluster for both the SyncIQ replication directory as well as the ECS CloudPools account. To change write access to the secondary cluster (failover) you would follow these steps:

Step 1: Perform a SyncIQ Failover

The first step in performing a CloudPools site failover is to do a SyncIQ failover. This will grant read/write access to the data on the Isilon cluster that is being replicated to the secondary Isilon cluster. This includes all the files in the directory being replicated with SyncIQ including the SmartLink files for the data stored on the ECS system.

Note: If your primary Isilon cluster is still online first stop all writes to the replication policy’s path and modify the replication policy so that it is set to run manually before performing a SyncIQ failover.

From the secondary Isilon cluster navigate to Data Protection > SyncIQ > Local Targets. On the policy that you want to failover select More > Allow Writes.

Figure 40) Perform a SyncIQ Failover
If your failover is temporary, perhaps you are doing system maintenance on Cluster 1, you can skip step 2 below. Users and applications can view and edit all files including those stored in ECS. Any changes they make to files stored in ECS will be stored in Cluster 2’s local cache and as part of failback these changes will be copied to Cluster 1 and then the next time the file pool policy runs the changes will be written to ECS.

**Step 2: Change CloudPools Access to Secondary Isilon Cluster**

In order to maintain consistency of the data stored in the ECS system CloudPools allow read write access from only one Isilon cluster. Up until now your primary site has read/write access and the secondary site has read only access to the data stored in the ECS system. If your primary site is unavailable for an extended period of time you have the option of providing the secondary site with write access to the data stored in the ECS system.

To transfer ECS write permission to your secondary Isilon cluster you need to ssh into the Isilon clusters using a tool such as putty or mRemoteNG. First login to one of the Isilon clusters and copy the CloudPools GUID for the CloudPools account you want to transfer using the command `isi cloud access list`. If there are multiple CloudPools GUIDs being shown you can get more details by running the command `isi cloud access view <GUID>` where <GUID> is the GUID shown from the previous list command. Copy the CloudPools GUID that shows the correct file pool policy and cloud storage account.

It is important to not allow write access to the CloudPools from more than one Isilon cluster at a time. If you are performing a planned shutdown or transfer then you start by removing write permission to the CloudPools Account on the primary Isilon cluster. This will disable the file pool policy, CloudPools and Cloud Storage Account on the primary Isilon system. To do this ssh into the **primary** Isilon cluster and run `isi cloud access remove <GUID>` replacing <GUID> with the GUID identified in the previous list command. If the primary Isilon cluster is already unavailable and will be for an extended period of time you can skip this step and move on to adding access.
Now you can add write access to the CloudPools from the secondary Isilon cluster. This will enable file pool policy, CloudPools and Cloud Storage Account on the secondary Isilon system and allow it to run the file pool policy that archives data to the ECS system. To do this ssh into the secondary Isilon cluster and run `isi cloud access add <GUID>` with the GUID identified in the previous list command.

Figure 43) Add CloudPools Write Access to Secondary Isilon Cluster

```
Cluster2.1# isi cloud access add 000e1e83f0e0d2abf95d771ee7a131ca82
Giving access to 000e1e83f0e0d2abf95d771ee7a131ca82 will enable the following CloudPool accounts and FilePool policies:
   CP1 (CloudPool Account)
   CPPolicy1 (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 all 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 accept the default expiration date (2027-01-17): (<date>/[default]/cancel):
Cluster2-1#
```

Now that failover is complete you can change the SyncIQ replication policy back to its original schedule.

FAILBACK TO PRIMARY ISILON CLUSTER

If the primary Isilon cluster becomes available you may wish to failback. You start by failing back SyncIQ policy and then CloudPools. The SyncIQ failback includes migrating data that clients have modified on the secondary Isilon cluster and returning replication and write access to the SyncIQ directory. The CloudPools failback involves changing write permission back to the primary Isilon cluster.

SYNCIQ FAILBACK

Step1: Create a SyncIQ Replication Mirror Policy on the Secondary Isilon Cluster

In order to perform a SyncIQ failback you need to start by creating a SyncIQ replication mirror policy on the secondary Isilon cluster. To do this login to the primary Isilon cluster UI and navigate to Data Protection > SyncIQ > Policies. For the SyncIQ policy that you want to failback select More > Resync-prep.

Figure 44) Resync Prep SyncIQ Policy on Primary Isilon Cluster
Step 2: Sync Data on the Secondary Isilon Cluster with the Primary Isilon Cluster

Next you will want to sync any changes that have been written to the secondary Isilon clusters replication directory back to the primary Isilon cluster. To perform this login to the secondary Isilon cluster’s UI and navigate to Data Protection > SyncIQ > Policies. On the replication mirror policy that you want to failover select More > Start Job.

Figure 45) Sync Data from Secondary Isilon Cluster to Primary Isilon Cluster

Step 3: Perform SyncIQ Failback

Before initiating a SyncIQ failback operation it is recommended:

1) Stop client writes to the replication directory

2) Perform a final replication from the secondary Isilon cluster to the primary Isilon cluster to ensure both sites are in sync. To accomplish this rerun the previous step, from secondary Isilon cluster select SyncIQ replication mirror policy and select Start Job. Wait for this job to complete, you can see the status in the reports tab.

3) Take note of the current SyncIQ replication policy and then change it to run manually.

Now you are ready to perform a SyncIQ failback. 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. This includes all the files in the directory being replicated with SyncIQ including the SmartLink files for the data stored on the ECS system.

From the primary Isilon cluster navigate to Data Protection > SyncIQ > Local Targets. On the policy that you want to failover select More > Allow Writes.

Figure 46) Allow Writes on Primary Isilon Cluster to SyncIQ Replication Directory
Then on the secondary Isilon cluster navigate to Data Protection > SyncIQ > Policies. Beside the replication mirror policy that is failing over select More > Resync-prep. This will put the secondary Isilon cluster back into read-only mode and ensure that the data sets are consistent on both the primary and secondary Isilon clusters. Although not required, you can also delete the SyncIQ mirror policy on the secondary Isilon cluster by selecting More > Delete after the failback has completed successfully.

Failback is now complete. You can redirect your clients back to accessing their data from the primary Isilon cluster. If necessary you can also change the SyncIQ replication policy back to the desired schedule.

CLOUDPOOLS FAILBACK

Now that you have successfully changed the write access to the SyncIQ replication directory back to the primary Isilon cluster you now need to change the write access to the ECS system back as well.

Note: This is only necessary if during failover you changed CloudPools access to the secondary Isilon cluster (failover Step 2).

Step1: Disable Write Access to the ECS System on the Secondary Isilon Cluster

In order to maintain consistency of the data stored in the ECS system CloudPools allow read write access from only one Isilon cluster. Currently your secondary site has read/write access and the primary site has read only access to the data stored in the ECS system.

To transfer ECS write permission back to your primary Isilon cluster you need to ssh into the secondary Isilon cluster using a tool such as putty or mRemoteNG. Identify the GUID for the CloudPools Account and File Pool Policy you want to transfer using the command isi cloud access list. If there are multiple CloudPools GUIDs being shown you can get more details by running the command isi cloud access view <GUID> where <GUID> is the GUID shown from the previous list command.

Copy the CloudPools GUID that shows the correct file pool policy and cloud storage account.

Figure 47 Identify GUID for CloudPools Account and File Pool Policy

Since write access to the ECS system is currently given to the secondary Isilon cluster you first need to disable this write access. From the ssh session on the secondary Isilon cluster run the command isi cloud access remove <GUID> where <GUID> is the GUID shown from the previous list command.

Figure 48 Remove Write Access on the Secondary Isilon Cluster to the ECS system

Since write access to the ECS system is currently given to the secondary Isilon cluster you first need to disable this write access. From the ssh session on the secondary Isilon cluster run the command isi cloud access remove <GUID> where <GUID> is the GUID shown from the previous list command.

Are you sure?? (yes/[no]): yes
Step 2: Enable Write Access to the ECS System on the Primary Isilon Cluster

Now you can add write access to the CloudPools to the primary Isilon cluster. This will enable the file pool policy, CloudPools and Cloud Storage Account on the primary Isilon system and allow it to run the file pool policy that archives data to the ECS system. To do this ssh into the primary Isilon cluster and run `isi cloud access add <GUID>` with the GUID identified in the previous list command.

Figure 49) Give the Primary Isilon Cluster Write Access to the ECS System

```
Cluster1-1# isi cloud access add 000e1e83f0e0d2abf956771ee7all31ca682
Giving access to 000e1e83f0e0d2abf956771ee7all31ca682 will enable the following CloudPool accounts and FilePool policies:
  CP1 (CloudPool Account)
  CPPolicy1 (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 all 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 accept the default expiration date:

```
<date>/[default]/cancel);
Cluster1-1#
```

Failback is now complete.

**FAILOVER TO SECONDARY ECS SITE**

If the primary ECS system becomes unavailable the Isilon cluster can still access data from the cloud if:

- multiple virtual data centers (VDC) were configured and federated together
- the replication group that your CloudPools buckets are using includes two or more federated virtual data centers
- the other sites in your replication group are online and available
- Access During Outage (ADO) is enabled on the buckets or the site has completed a permanent site failover.

Note: Object updates that have not completed replication to the secondary ECS site maybe lost.

By default all sites in an ECS replication group have read/write access to the buckets. This means that if the primary ECS site is unavailable the buckets and data are still available to the Isilon cluster. To direct the CloudPools to a secondary ECS system either:

- **Option 1:**  If you have a load balancer it should be configured to recognize that the primary site is unavailable and have a secondary site configured. If so, this will automatically direct requests to the secondary ECS site.

**HAProxy HTTP connections example:**

```
option httpchk GET /?ping HTTP/1.1\n Host: haproxy\n X-Emc-Namespace: foo
option allbackups
server node1S1 <Node 1 S1 IP address>:9020 check inter 10000 rise 2 fall 5
server node1S2 <Node 1 S2 IP address>: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 ECS node who’s IP is listed in `Node 1 S1 IP address`:9020. It performs this health check using the command stated in the option httpchk
line. If the health checks fail, meaning the service is unavailable on the primary site then the option allbackups line tells HAProxy to direct traffic to the nodes configured with the backup option such as server node1S2.

- Option 2: As the Isilon cluster admin edit the Cloud Storage Account to point the URI of the second ECS system, either directly or to its local load balancer.

If the primary site will be permanently unavailable follow the instructions in the ECS Administrator's Guide to permanently remove a VDC and initiate fail over processing.

SUMMARY

CloudPools with ECS provide a massively scalable storage solution that enables IT administrators to optimize storage resources. It uses custom policies that allow flexibility and control over where data physically resides while maintaining the same Isilon namespace and file system access. CloudPools is easy to configure and manage and includes built-in options to extend the enterprise availability across sites. With the option to co-locate both systems you get a private cloud solution with low data residency risks as well as lower latency. Because both products are developed and supported by Dell EMC you gain all the benefits of a solution has been fully tested together as well as single vendor support.

REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Author</th>
<th>Change Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 2016</td>
<td>1.0</td>
<td>Kshitij Tambe</td>
<td>Initial Document</td>
</tr>
<tr>
<td>March 2017</td>
<td>2.0</td>
<td>Sandra Moulton</td>
<td>Updated OneFS and ECS versions. Added additional details and step-by-step example.</td>
</tr>
</tbody>
</table>