Dell PowerScale SmartSync

Data Mobility Beyond the Data Center

April 2023

H19109.2

White Paper

Abstract

This document describes the data replication functions of Dell PowerScale SmartSync.

Dell Technologies

Copyright

Contents

Executive summary

Overview

This document describes the data replication functions of Dell PowerScale SmartSync. The SmartSync feature takes data mobility beyond the data center, combining data replication for file and object targets. It also provides administrators with a centralized architecture to manage replication for PowerScale clusters and cloud targets.

Note to readers

Proceed with caution if you intend to make changes on a production cluster. Ensure that you understand the concepts explained in this paper in their entirety before implementing data replication. As with any significant infrastructure update, testing changes in a lab environment is best practice. After you confirm the updates in a lab environment, you can commence with a gradual roll-out to a production cluster.

Revisions

Date	Part number/ revision	Description
April 2022	H19109	Initial release
January 2023	H19109.1	Updated for OneFS release 9.5.0.0
April 2023	H19109.2	Updated file to include object replication configuration and CPU throttling.

Note: This document may contain language that is not consistent with Dell Technologies' current guidelines. Dell plans to update the document over subsequent future releases to revise the language accordingly.

We value your feedback

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

Author: Aqib Kazi

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

SmartSync

Overview

Data mobility is one of the most critical aspects of managing data in a modern, multicloud, and co-location environment. Data replication must be viewed from a mobility perspective. Providing replication to a homogenous platform and replicating across heterogeneous platforms unlocks the value of data.

Described by the term “data capital” in the MIT Technology Review, data is an organization’s most valuable asset. Today’s organizations must be able to replicate data across platforms. Therefore, data replication cannot be confined to PowerScale clusters but must also include cloud targets.

To address the requirements of the modern enterprise, PowerScale OneFS release 9.4.0.0 introduced PowerScale SmartSync. This feature replicates file-to-file data between PowerScale clusters. SmartSync cloud copy replicates file-to-object data from PowerScale clusters to Dell ECS and cloud providers. Having multiple target destinations allows administrators to store multiple copies of a dataset across locations, providing further disaster recovery (DR) readiness.

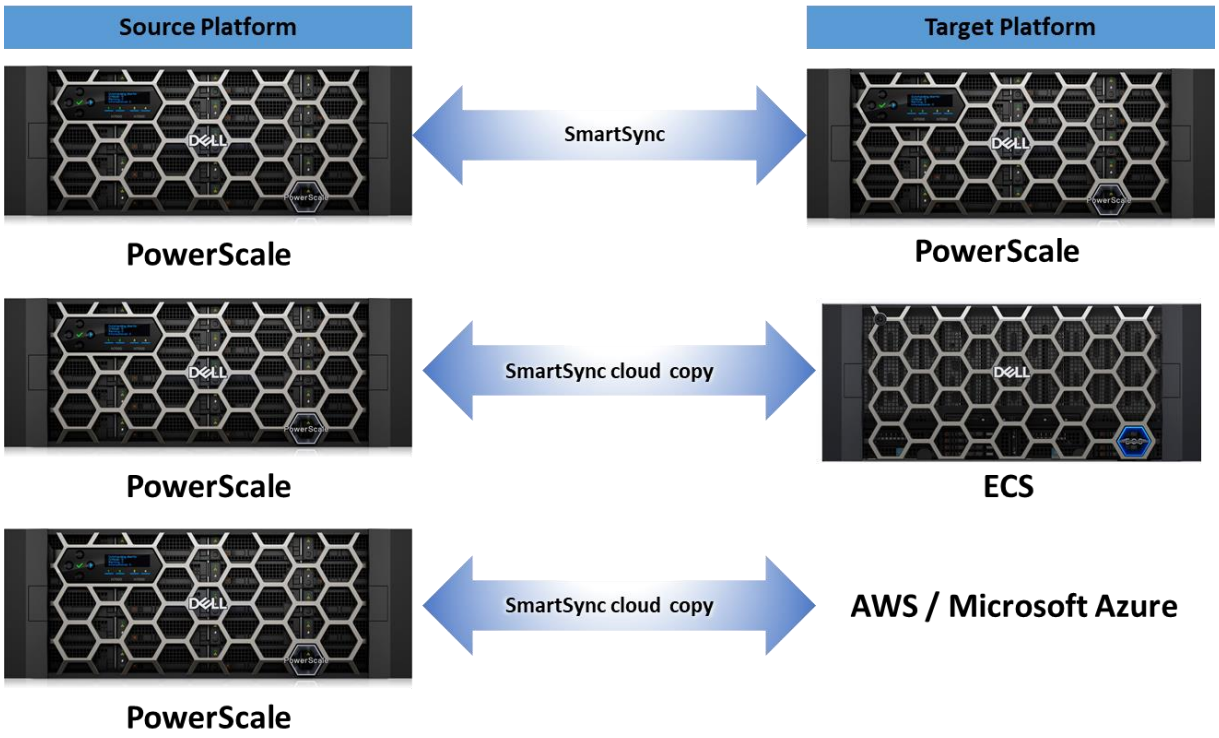

Figure 1. Cross-platform data mobility

SmartSync is designed to address the growing needs of data beyond the data center by using a powerful transport layer with robust error handling that uses a proprietary messaging system through RPC. Cloud copy uses HTTP to replicate data to cloud providers.

Eliminate re-baselining

SmartSync eliminates the lock-in of source-target relationships. Re-baselining is not required for source-target clusters containing an earlier dataset version. For example, a

typical DR topology includes three PowerScale clusters—A, B, and C in a cascade. Cluster A replicates to B, and B replicates to C. If cluster B is unavailable, the cluster A to C policy would not require a new baseline, as shown in Figure 2. The need for baselining is eliminated by introducing parent-child relationships in the dataset. A handshake compares the datasets of clusters A and C, allowing only the changed data blocks to be transferred, minimizing replication overhead. For environments with large datasets, eliminating re-baselining minimizes RPO and RTO times and further strengthens DR readiness.

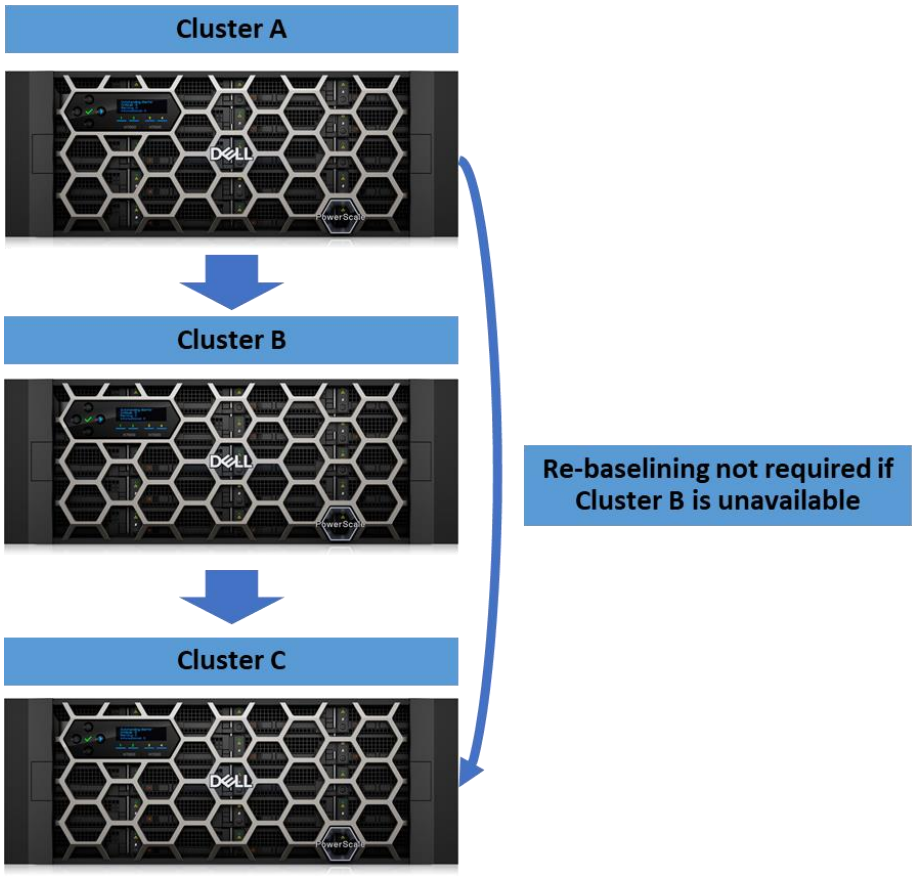

Figure 2. Re-baselining eliminated

Resource consumption

As the demands for data replication increase, the extra strain on a source cluster must be considered. Multiple targets create an immense resource strain on the source cluster, affecting client workloads as the source cluster pushes data to the target. SmartSync allows administrators to use the target cluster's resources to pull the dataset, minimizing the system resource impacts on the source cluster, as shown in the following figure. In environments with a single-source dataset and numerous targets, this is useful because the source cluster's resources can focus on client utilization.

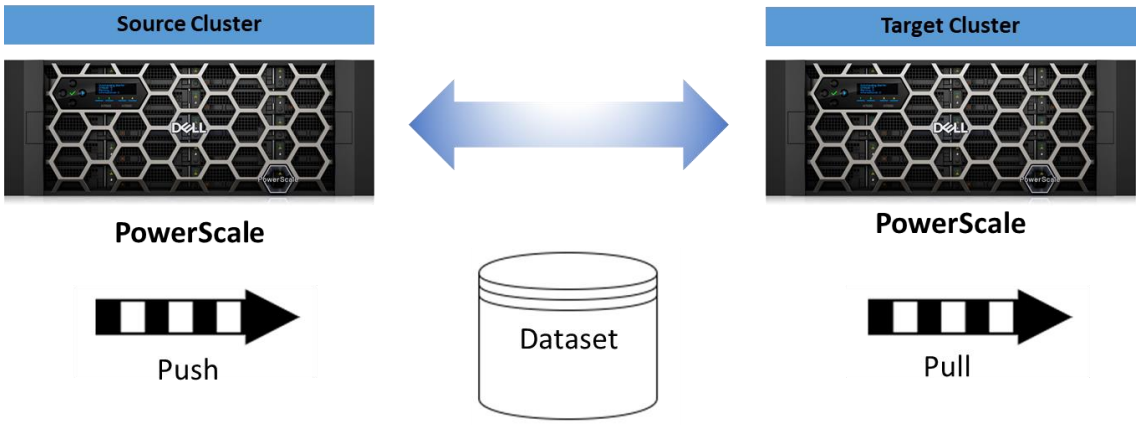

Figure 3. Dataset push and pull

Replication resiliency

Resiliency to replication failures is enhanced with SmartSync, minimizing replication times even when a job runs into an error. Traditionally, if a replication job encounters an error, the entire policy would fail, requiring an administrator to start over on the next replication attempt. With SmartSync jobs, if an error occurs, the job goes into a paused state. For each error, a log snippet containing the error is generated under `/ifs/data/Isilon_Support/datamover/transfer_failure`.

Once a job is in the pause state, an administrator has three options, as illustrated in Figure 4. The options are:

- Cancel the job
- Resolve the errors and resume the job
- Complete a partial replication, retaining the portion of the dataset already transferred to the target platform, minimizing the following job's run time

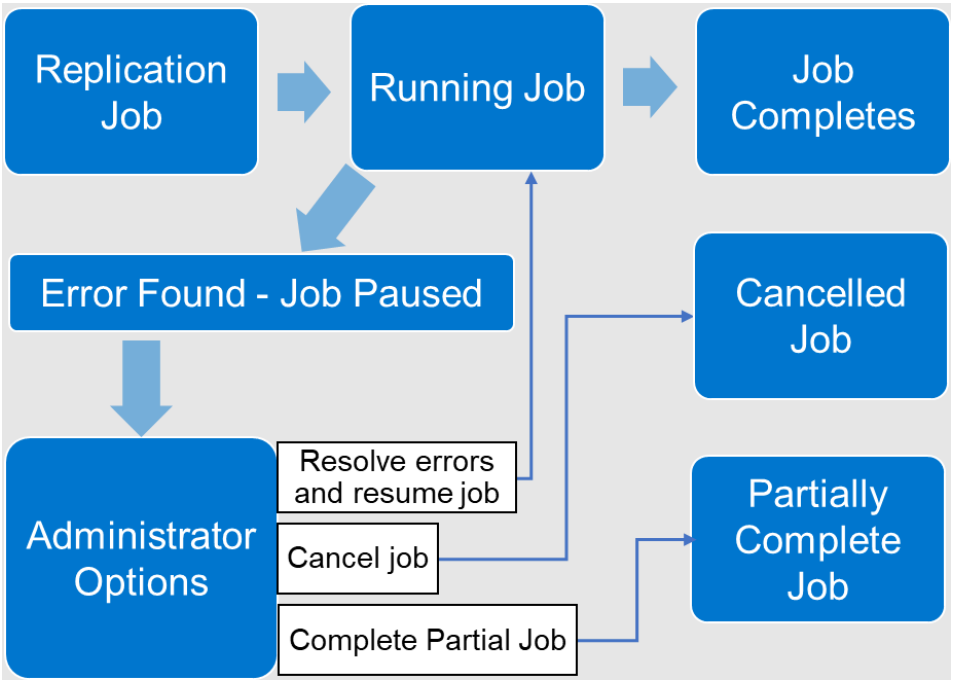

Figure 4. Replication resiliency

Decoupled snapshots

SmartSync decouples the snapshot creation process on the source cluster from the data replication to the target cluster. Separate policies are configured for snapshot creation and data replication. SmartSync refers to the snapshot creation as the dataset creation. The decoupling of snapshots and data replication allows each policy job to run independently, which further reduces the chain effect of a failure during the snapshot process early in the policy job state.

SmartSync also introduces child-parent relationships to launch a data-replication job only after the snapshot creation is complete, as described in Parent-child policies.

Base and concrete policies

In a typical environment, administrators manage several data replication policies. The number of replication policies could range from one to many on a cluster, creating an overhead of policy management. SmartSync introduces a concept of base and concrete policies. The base policy is a set of fields that applies to concrete policies. The concrete policy uses the predefined set of fields from the base policy.

File attributes

SmartSync copies file metadata to the target platform. Suppose the target platform requires read/write access. Clients and applications must have the file metadata resemble the source platform. SmartSync maintains common file attributes, including:

- POSIX attributes (stat structure)
- Create time
- NT ACLs
- POSIX ACLs
- Alternate Data Streams (applies only to PowerScale to PowerScale replication)
- Extended Attributes (applies only to PowerScale to PowerScale replication)

Configuration

Overview

A policy is required to replicate a dataset from a source PowerScale cluster to a target platform. A license is required before policy configuration, and the service must be activated. This section provides the steps to configure replication from a PowerScale source cluster.

SmartSync uses the OneFS Datamover service. Although the references in this section use SmartSync, the CLI refers to SmartSync as Datamover.

Note: This section's configuration examples and options are based on the CLI. SmartSync may also be configured using PAPI. The configuration steps may be used as a template by replacing the CLI commands with PAPI commands. For more information, see the PowerScale OneFS API Reference Guide on Dell Support.

OneFS privilege

Users must have the `ISI_PRIV_DATAMOVER` privilege to configure SmartSync.

License

SmartSync requires an active SyncIQ and SnapshotIQ license. Before you continue with the following sections, ensure that both licenses are activated.

Enable service

By default, the SmartSync service is disabled and must be enabled to start the configuration process. To enable the service, from the OneFS CLI, run the following command:

```
isi services -a isi_dm_d enable
```

Encryption

For SmartSync policies to run, trust must be established between the source and target cluster. Transport Layer Security (TLS) provides the authorization, authentication, and encryption, resulting in a mutual handshake. Each cluster requires configuration of a Certificate Authority (CA) and Certificate Identity (CI). SmartSync requires that encryption be configured for policies to run. The SmartSync daemon only runs after a CA and CI are configured.

Note: The source and target clusters establish trust by installing the CA that signed the other cluster's CI. In a scenario of replication to multiple clusters, the CA of each cluster is installed on every cluster. SmartSync establishes a mutual TLS handshake, disallowing unidirectional trust.

Further enhancing SmartSync security, PowerScale OneFS release 9.5.0.0 provides SmartSync support for the Online Certificate Status Protocol (OCSP). This section provides encryption configuration steps without an OCSP. For more information about using an OCSP, see OCSP.

As a best practice, use a local CA to sign a CI per cluster.

- If a local CA is available, go to the Local Certificate Authority section.
- If a local CA is not available, go to the Self-signed certificates section.

Note: The SmartSync daemon does not start until a CA is configured. For an example of log file output when a CA is not configured, see Unconfigured CA.

Local Certificate Authority

If a local CA is available, create the CA and CI bundles for the source and target clusters. The bundles must be X.509 public key infrastructure (PKI) certificates. The certificate formats supported are PEM, DEM, and PKCS #12 format.

If intermediates are required for the CA bundle, the order of the bundle begins with the CA certificate and ends with the root. This order includes any intermediates in between, excluding the CI. Each certificate must certify the certificate before it. For example, a certificate bundle could be in the following format:

- Intermediate certificate 3
- Intermediate certificate 2
- Intermediate certificate 1
- Root certificate

The CI bundle consists of the X.509 certificate followed by the private key. Optionally, the private key may also be encrypted and password protected in the CI bundle. If the private key is password protected, note the password for use in the steps that follow.

Once the CA and CI bundles are complete for the source and target clusters, transfer them to each cluster through any protocol, and retain the file location for use in the steps that follow. Next, go to Install Certificate Authority and Certificate Identity.

Self-signed certificates

If a local CA is not available, self-signed certificates may be used.

Note: Using a local CA is a best practice for an optimal security posture. Only use the self-signed certificate option if a local CA is unavailable.

The same CA could be used on the source and target cluster with the self-signed certificates option. However, this section provides steps to configure a CA on each cluster, and the CA signs its local CI for a more secure option.

To configure encryption with self-signed certificates, perform the following steps.

Note: In the following steps, the naming conventions and expiration of the certificates may be updated for site requirements. Customize the information as required. The output shown is a working example.

Note: This section follows a naming convention of `-s` to notate the source cluster and `-t` to notate the target cluster. Replace the notations as required.

1. Log in to the source cluster CLI. On the source cluster, generate a CA:

   ```
   source-cluster# openssl genrsa -out ca-s.key 4096
   source-cluster# openssl req -x509 -new -nodes -key ca-s.key -
   sha256 -days 1825 -out ca-s.pem
   ```

2. Copy the source cluster CA to the target cluster:

   ```
   source-cluster# scp ca-s.pem [Target Cluster IP]:/root
   ```

3. Generate the CI on the source cluster:

   ```
   source-cluster# openssl genrsa -out identity-s.key 4096
   source-cluster# openssl req -new -key identity-s.key -out
   identity-s.csr
   ```

4. Create the source cluster CI on the source cluster:

   ```
   source-cluster# cat << EOF > identity-s.ext
   authorityKeyIdentifier=keyid,issuer
   basicConstraints=CA:FALSE
   keyUsage=digitalSignature,nonRepudiation,keyEncipherment,data
   Encipherment
   EOF
   ```

5. On the source cluster, sign the source cluster's CI with the source cluster's CA:

```
source-cluster# openssl x509 -req -in identity-s.csr -CA ca-
s.pem -CAkey ca-s.key -CAcreateserial -out identity-s.crt -
days 825 -sha256 -extfile identity-s.ext
```

6. Log in to the target cluster CLI. On the target cluster, generate a CA:

```
target-cluster# openssl genrsa -out ca-t.key 4096
target-cluster# openssl req -x509 -new -nodes -key ca-t.key -
sha256 -days 1825 -out ca-t.pem
```

7. Copy the target cluster CA to the source cluster:

```
target-cluster# scp ca-t.pem [Source Cluster IP]:/root
```

8. Generate the CI on the target cluster:

```
target-cluster# openssl genrsa -out identity-t.key 4096
target-cluster# openssl req -new -key identity-t.key -out
identity-t.csr
```

9. Create the target cluster CI on the target cluster:

```
target-cluster# cat << EOF > identity-t.ext
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage=digitalSignature,nonRepudiation,keyEncipherment,data
Encipherment
EOF
```

10. On the target cluster, sign the target cluster's CI with the target cluster's CA:

```
target-cluster# openssl x509 -req -in identity-t.csr -CA ca-
t.pem -CAkey ca-t.key -CAcreateserial -out identity-t.crt -
days 825 -sha256 -extfile identity-t.ext
```

The self-signed certificates for the source and target clusters are now generated. Continue with Install Certificate Authority and Certificate Identity.

Install Certificate Authority and Certificate Identity

The CAs and CIs for each cluster are generated and copied to the appropriate cluster. Before you continue with this section, ensure that the location of all certificates is available.

The steps that follow assume a naming convention of `-s` to notate the source cluster and `-t` to notate the target cluster. If a local CA generated the bundles, replace the naming convention in the following steps with the actual name and location of the bundles. The example assumes that a unique CA is installed on each cluster. If the same CA is installed on each cluster, skip the step for a second CA.

To install the CA and CI, perform the following steps:

1. On the source cluster, install the source cluster's CA:

```
source-cluster# isi dm certificates ca create "$PWD"/ca-s.pem
--name cluster-s-ca
```

2. On the source cluster, install the target cluster's CA:

```
source-cluster# isi dm certificates ca create "$PWD"/ca-t.pem
--name cluster-t-ca
```

3. On the source cluster, install the source cluster's CI:

```
source-cluster# isi dm certificates identity create
"$PWD"/identity-s.crt --certificate-key-path "$PWD"/identity-
s.key --name cluster-s-identity
```

Note: If the identity has a password configured, use the `--certificate-key-password` option to specify the password.

4. On the target cluster, install the target cluster's CA:

```
target-cluster# isi dm certificates ca create "$PWD"/ca-t.pem
--name cluster-t-ca
```

5. On the target cluster, install the source cluster's CA:

```
target-cluster# isi dm certificates ca create "$PWD"/ca-s.pem
--name cluster-s-ca
```

6. On the target cluster, install the target cluster's CI:

```
target-cluster# isi dm certificates identity create
"$PWD"/identity-t.crt --certificate-key-path "$PWD"/identity-
t.key --name cluster-t-identity
```

Note: If the identity has a password configured, use the `--certificate-key-password` option to specify the password.

Encryption is now configured on the source and target clusters.

OCSP

OneFS release 9.5.0.0 provides SmartSync support for OCSP, as required for federal FIPS and STIG requirements. To configure OCSP, run the `isi dm certificates settings modify` command. The following options are available:

- Enable-encryption: This option enables traffic encryption. If the option is disabled, an initial successful TLS handshake is required, but SmartSync replication traffic is not encrypted.
- Strict-hostname-check: This option requires the CN/ASN found in the certificate to match the account URI; otherwise, the handshake fails.
- OCSP-URI: If the certificate does not already contain the OCSP URI, it may be provided with this option.
- Revocation-setting: This option specifies the level of OCSP checking. The following options are available:
  - Strict: Requires all handshakes to pass OCSP. All OCSP check failures are considered fatal.

- Allow revoke data unavailable: Requires the OCSP checks to pass, but if an OCSP responder is unavailable, the check is successful.
- Allow no revoke SRC: Requires the OCSP checks to pass even if a certificate does not contain a URI.
- None: Bypasses all OCSP checks.

Replication accounts

By default, a local account for the source cluster is already configured. Run the `isi dm accounts list` command, and the output displays the DM Local Account.

SmartSync account

The steps in this section assume a traditional push policy that is defined and initiated from the source cluster. After reviewing this information in this section, see Pull policy to define an account for a pull policy on the target cluster.

Note: Although the steps in this section reference specific sections for push and pull policies, you may use a single account for a push and pull policy depending on the data-replication topology. The steps in this section reference the push and pull to provide an example.

After encryption is configured, the next step is to add a replication account to the source cluster, pointing replication to a target cluster.

On the source cluster, add a replication account by running the following command:

```
source-cluster# isi dm accounts create DM dm://[Target Cluster IP]:7722 [Account name: For example 'target-acc']
```

Note: The target cluster IP address may be a hostname, IPv4, or IPv6 address. As a best practice, use a SmartConnect round-robin DNS name for the target cluster IP address.

Optionally, now you can specify the local and remote SmartConnect pools for the source and target clusters, respectively, with the `--local-network-pool` and `--remote-network-pool` fields. The fields are specified with the `isi dm accounts modify` command and the associated account `--access-id` found under `isi dm accounts list`.

Pull policy

To perform a pull policy from the target cluster, add the replication account on the target cluster and enter the source cluster's IP address.

The command is now issued on the target cluster and is updated as follows:

```
target-cluster# isi dm accounts create DM dm://[Source Cluster IP]:7722 [Account name: For example 'source-acc']
```

Cloud copy account

To replicate object data to AWS, Azure, or ECS using SmartSync cloud copy, add the bucket information with the `isi dm accounts create` command and specify the following:

- Object store type: AWS_S3, AZURE, or ECS_S3: The S3 bucket for AWS and Azure must exist in the default region.

- URI: {http,https}://hostname:port/bucketname
- Access ID, Secret Key
- Optional proxy information

As an example, to add an AWS S3 bucket as a cloud copy account:

```
isi dm account create --account-type AWS_S3 --name [Account Name]
--access-id [access-id] --uri https://s3.amazonaws.com/[bucket-
name] --auth-mode CLOUD --secret-key [secret-key]
```

When the account is added, the bucket name may be a new or existing bucket. If the bucket is new, it is created when the `isi dm account create` command is issued, otherwise, the existing bucket is used.

Confirm account creation

Run the `isi dm accounts list` command to verify that the account has been created. The new account and the local account are listed, as shown in the following figure:

```
OneFS94-S1-1# isi dm accounts list
ID                                                Name            URI                       Account Type
-------------------------------------------------------------------------------------------------------------
00000000000000010000000000000000000000000000000000 demo-acc       dm://192.168.50.120:7722 DM
000c29a3fa22e3810d62ee16339b174a89d9000000000000   DM Local Account dm://[::1]:7722          DM
-------------------------------------------------------------------------------------------------------------
Total: 2
```

Figure 5. isi dm accounts list

The output in this example lists the `DM Local Account`, which is the source cluster's account. `demo-acc` is the target cluster's account and IP address. However, the `isi dm accounts list` is run on the target cluster for a pull policy account; the `DM Local Account` would be the target cluster, while `demo-acc` would be the source cluster.

Dataset creation policy

A dataset must be available before a `copy` or `repeat-copy` data replication policy runs, as shown in Figure 6. The dataset creation step is required for SmartSync cluster replication and for cloud copy. If a dataset is unavailable, the copy or repeat-copy replication policy fails. For more information about the copy and repeat-copy policies, see Replication policies.

The steps in this section assume a traditional push dataset creation that is defined and initiated on the source cluster. After reviewing this section, see Pull dataset creation policy to define a pull dataset.

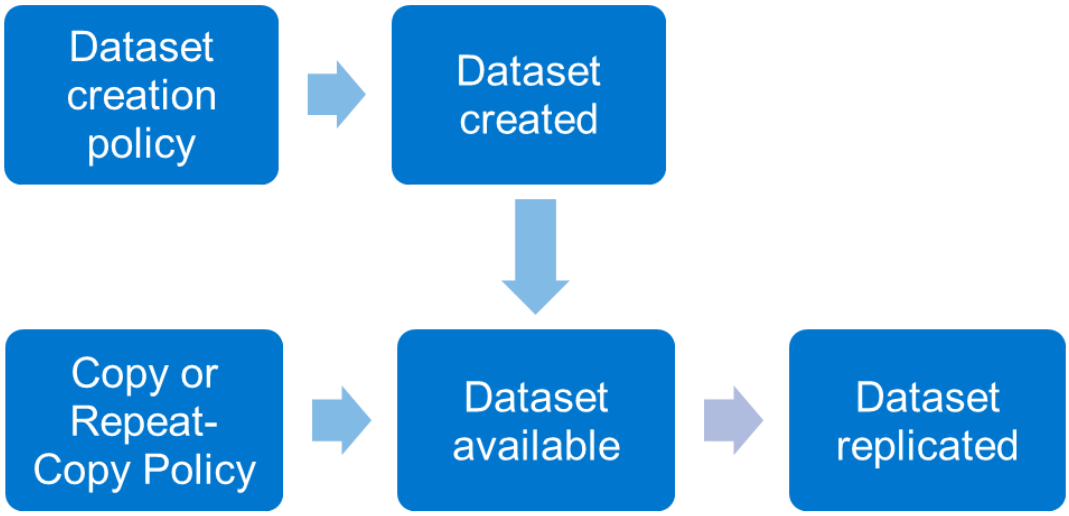

Figure 6. Datasets and replication policies

To create a dataset, run the `isi dm policies create` command with the `CREATION` policy option. For example:

```
isi dm policies create [Policy Name] NORMAL true CREATION --
creation-account-id=[DM local account] --creation-base-path= --
creation-dataset-retention-period= --creation-dataset-reserve= --
creation-dataset-expiry-action=DELETE --recurrence=”cron
expression” --start-time="YYYY-MM-DD HH:MM:SS"
```

In this example:

- The `CREATION` option specifies the policy is only to create the dataset. For data replication policies, see Replication policies.
- The `NORMAL` option assigns a normal priority to this policy. The other options are `Low` and `High`.
- The `true` field specifies that the policy is enabled.
- In the `creation-account-id` field, enter the DM local account ID specified in the `isi dm accounts list` command.
- In the `creation-base-path` field, for SmartSync specify the directory path or file for the dataset. For cloud copy, this field specifies the object store key prefix.
- In the `creation-dataset-retention-period` field, specify in seconds how long the dataset is retained before expiration.
- In the `creation-dataset-reserve field`, specify how many datasets to keep in reserve and protected from expiration, irrespective of the `creation-dataset-retention-period` specified.
- In the `creation-dataset-expiry-action`, specify what happens with the dataset after expiration. In the current release, the only expiration option is `DELETE`.
- In the `recurrence` field, optionally specify a cron expression within the quotation marks to specify how often the policy runs.

- In the `start-time` field, specify a date and time when the policy runs. If you specify a past date, the policy runs immediately after the command runs.

For more options on dataset creation, see the CLI Administration Guide on Dell Support.

Check the dataset creation policy's status by running `isi dm jobs list` and `isi dm historical-jobs list`. For more information about options for a running policy, see Troubleshooting. Once the dataset is created, it is listed under `isi dm datasets list`. The dataset creation uses a SnapshotIQ snapshot. It is displayed under `isi snapshot list`, with an `isi_dm` preceding the snapshot name.

Pull dataset creation policy

A pull dataset creation policy is defined and initiated on the target cluster. To perform a pull dataset creation on the source cluster, run the `isi dm policies create` command on the target cluster. However, the `--creation-account-id` is updated to the source cluster's account, found under `isi dm accounts list` on the target cluster. All other fields in the command remain as previously described.

Replication policies

Once the dataset is created, the next step is to replicate the dataset to the target platform. The dataset is replicated through either a `copy` or `repeat-copy` policy:

- The `copy` policy is a one-time single copy of the entire dataset to the target platform.
- The `repeat-copy` policy option is an incremental copy of a dataset that is constantly changing and is only supported for SmartSync file replication. `Repeat-copy` for file to object copy is not supported at this time. In a `repeat-copy` policy, the initial run copies the entire dataset; subsequent repeat-copy policy runs only copy the changed data blocks. The new and previous datasets are compared on the source cluster, and only changed blocks are transferred to the target cluster.

Note: Before running a `copy` or `repeat-copy` policy, ensure that a dataset creation policy is completed for the source base path. Otherwise, the `copy` or `repeat-copy` policy will remain in a paused state.

The steps in this section assume a traditional push replication that is defined and initiated on the source cluster. After reviewing this section, see Cloud copy replication policy

The `isi dm policies create` command is also used for file-to-object copy replication. However, for file-to-object copy replication, the following fields are applicable:

- The `REPEAT-COPY` option is not supported for file-to-object copy.
- The `--copy-create-dataset-on-target` field is set to true to store a copy of the dataset in the S3 bucket.
- In the `--copy-base-base-account-id` and `--copy-base-source-account-id` fields, specify the source cluster's account ID from the `isi dm accounts list` command.
- In the `--copy-base-target-account-id` field, specify the S3 bucket's account ID from the `isi dm accounts list` command.

- In the `--copy-base-target-base-path` field, specify a folder where the dataset will be copied. The folder will be created under the S3 bucket. The dataset is copied to the S3 bucket under `[s3 bucket]/.datamover/dsr/[copy-base-target-base-path folder]`. In the S3 bucket, a folder is created under `[s3 bucket]/.datamover/dsr/`. The `dsr-latest` file is metadata associated with the bucket contents.
- In the `type` field, specify `FILE_ON_OBJECT_COPY`.

Pull replication policy to define a pull replication policy.

As an example, run the following `copy` or `repeat-copy` policy command:

```
isi dm policies create [Policy Name] NORMAL true [COPY or REPEAT-COPY] --copy-source-base-path=[Source Dataset Path] --copy-create-dataset-on-target=true --copy-base-base-account-id=[Source DM Account] --copy-base-source-account-id=[Source DM Account] --copy-base-target-account-id=[Target DM Account] --copy-base-target-base-path=[Target directory path] --copy-base-target-dataset-type=FILE --copy-base-dataset-retention-period= --copy-base-dataset-reserve= --copy-base-policy-dataset-expiry-action=DELETE --start-time="YYYY-MM-DD HH:MM:SS"
```

In this example, some of the options are the same as those of the dataset creation policy. For more information about those options, see Dataset creation policy. You can specify additional options as follows:

- In the `copy-create-dataset-on-target` field, specify if a new dataset will be created on the target cluster. If this field is set to `true`, the new dataset is displayed under `isi dm datasets list` (and `isi snapshot list`, preceded by an `isi_dm_snap`) on the target cluster, and the data remains read-only. If the field is set to `false`, a dataset is not created, but the data is available for read and write.
- In the `--copy-base-base-account-id` and `--copy-base-source-account-id` fields, specify the source cluster's account ID from the `isi dm accounts list` command.
- In the `copy-base-target-account-id` field, specify the target platform account ID from the `isi dm accounts list` command.
- In the `copy-base-target-dataset-type` field, specify if the target platform is `FILE_ON_OBJECT_COPY` or `FILE`. The `FILE` option is for copying to a PowerScale cluster, while the `FILE_ON_OBJECT_COPY` option is for AWS, ECS, or Azure. Object-copy is in a copy format for a file system on object-store. For more information about file to object copy, see the section Cloud copy replication policy.
- Optionally, use the `copy-source-sub-paths` option to select only a subset of the directory structure that was specified under the `copy-source-base-path`.
- Optionally, specify a dataset ID, which is found under `isi dm datasets list`, directly for replication using the `copy-dataset-id` option. If a `copy-dataset-ID` is not specified, the most current dataset for the subpath is used for the policy by default.
- Optionally, use the `recurrence` and stagger the copy or repeat-copy policy with the dataset creation recurrence.

- Optionally, use the `reconnect` flag on a repeat-copy policy to specify that the target platform already has the baseline copy, allowing only the incremental updates to be replicated.

For more replication policy options, see the CLI Administration Guide on Dell Support.

Cloud copy replication policy

The `isi dm policies create` command is also used for file-to-object copy replication. However, for file-to-object copy replication, the following fields are applicable:

- The `REPEAT-COPY` option is not supported for file-to-object copy.
- The `--copy-create-dataset-on-target` field is set to true to store a copy of the dataset in the S3 bucket.
- In the `--copy-base-base-account-id` and `--copy-base-source-account-id` fields, specify the source cluster's account ID from the `isi dm accounts list` command.
- In the `--copy-base-target-account-id` field, specify the S3 bucket's account ID from the `isi dm accounts list` command.
- In the `--copy-base-target-base-path` field, specify a folder where the dataset will be copied. The folder will be created under the S3 bucket. The dataset is copied to the S3 bucket under `[s3 bucket]/.datamover/dsr/[copy-base-target-base-path folder]`. In the S3 bucket, a folder is created under `[s3 bucket]/.datamover/dsr/`. The `dsr-latest` file is metadata associated with the bucket contents.
- In the `type` field, specify `FILE_ON_OBJECT_COPY`.

Pull replication policy

PowerScale to PowerScale replication

A pull replication policy is defined and initiated on the target cluster. To perform a pull replication policy from the target cluster, the `isi dm policies create` command is issued on the target cluster. However, the `--copy-base-base-account-id=` and `--copy-base-source-account-id` are updated to the source cluster's account, found under `isi dm accounts list` on the target cluster. All other fields in the command remain as previously described.

Cloud copy

A pull replication policy is supported for a file-to-object copy. If a dataset is copied to an S3 bucket with a push policy, as explained in the Cloud copy replication policy section, it may be retrieved from the S3 bucket with a pull policy. From the PowerScale cluster, issue the `isi dm policies create` command but update the `--copy-base-base-account-id` and `--copy-base-source-account-id` fields with the S3 bucket account ID from the `isi dm accounts list` command. Next, update the `--copy-base-target-account-id` field with the source cluster's account ID from the `isi dm accounts list` command.

Expiration policy

An expiration policy checks for expired datasets and runs the associated expiration action. Currently, the only option is to delete.

Base and concrete policies

SmartSync uses a concept of base and concrete policies. The base policy defines a common set of options that apply to concrete policies. The predefined fields are applied from the base policy when a concrete policy is defined. To define a base policy, run the `isi dm base-policies create` command. To define an associated concrete policy, run `isi dm policies create` and use the `--base-policy-id` option.

Parent-child policies

SmartSync uses a concept of parent-child relationships for policies. As a result, policies only start after the parent job policy, using the `parent-exec-policy-id` option, is complete. The parent-child policies provide an alternative to recurrence if it is unknown how long a previous policy might take to complete.

Recurrence

Dataset creation policy and Replication policies explain that policies may be configured with recurrence. A replication policy requires a dataset to be created before starting. If recurrence is scheduled for the policies, ensure that the recurrence schedule for the dataset creation and replication policy do not conflict. Allow adequate time for the dataset creation to complete before the replication policy starts to ensure that the dataset is available when the replication policy starts. As described in Parent-child policies, an alternative to the recurrence option is to create parent-child relationships for the policies.

Snapshots

Source and target cluster snapshots use SnapshotIQ snapshots. Source cluster snapshots are enabled by default, as required by the dataset creation policy. Target cluster snapshots are created if the `copy-create-dataset-on-target` option is set to `true` for a copy or repeat-copy policy. You can view the snapshots on the source and target clusters under `isi snapshot list` and `isi dm datasets list`. Manage snapshots by using the dataset retention period and reserve options, as explained in Dataset creation policy and Replication policies. Alternatively, run an expiration policy, as described in Expiration policy.

Push and pull policies

PowerScale to PowerScale replication

A push policy is initiated and defined on the source cluster, pushing data to a target cluster and using the resources available on the source cluster. Alternately, a pull policy is initiated and defined on the target cluster, pulling data to the target cluster and using the resources available on the target cluster. Consider workflow requirements for services other than data replication for the source and target clusters. Define and initiate policies on the cluster with the most available resources. Configuring push and pull policies is based on where the policy is defined and initiated.

Cloud copy replication

File-to-object copy replication policies are initiated and defined on the source cluster for push and pull policies. The source and target account IDs are flipped in the `isi dm policies create` command. For more information, see the Cloud copy section.

Throttling

SmartSync policies may be throttled to limit system and network impacts. Depending on the workflow requirements of the source and target platforms, consider using the throttling options. For PowerScale to PowerScale replication, before you apply additional throttling, consider using a pull policy rather than the traditional push, since this policy offloads impacts to the target cluster.

Bandwidth

Bandwidth throttling is specified for a specific subnet netmask, and a bandwidth limit is specified in bytes using the following command:

```
isi dm throttling bw-rules create NETMASK -[subnet] --bw-limit=
```

CPU

SmartSync's CPU usage is controlled by two parameters, the "Allowed CPU threshold" and the "System CPU load threshold." The "Allowed CPU threshold" is the percentage of CPU that SmartSync policies can consume. The "System CPU load threshold" is the node's CPU usage. If the "System CPU load threshold" is reached and the "Allowed CPU threshold" is reached, then SmartSync throttles CPU usage to stay at or below the "Allowed CPU threshold."

By default, the "Allowed CPU threshold" is 30 percent, and the "System CPU load threshold" is 90 percent. Therefore, if the node's total CPU reaches 90 percent and if the SmartSync consumption reaches 30 percent of the total CPU, SmartSync throttles its CPU consumption.

Define CPU throttling with the `isi dm throttling settings modify` command. Use the `isi dm throttling settings view` command to view the current CPU throttling setting.

To specify the "Allowed CPU threshold," use the `--allowed-cpu-threshold` option. To specify the "System CPU load threshold," use the `--system-cpu-load-threshold` command. For each option, specify the new threshold without the percentage sign.

Troubleshooting

Overview

Once a policy is running, the status is displayed in `isi dm jobs list`. Completed jobs are shown in `isi dm historical-jobs list`.

To view more information about a specific job, use the `isi dm job view` command with the job ID from `isi dm jobs list` or `isi dm historical-jobs list`.

Further, to view more detailed information about a specific job, use the `isi_datamover_job_status` command with the job ID.

To modify the status of a running job, use the `isi dm jobs modify` command. Specify the ID from the `isi dm jobs list` command, and specify an action. The available actions for a running job are to cancel, complete it partially, pause, or resume.

Logs

Information about SmartSync jobs is in `/var/log/isi_dm.log` and `/var/log/messages`. Jobs with transfer failures create a log specific to the job ID under `/ifs/data/Isilon_Support/datamover/transfer_failures`.

Unconfigured CA

If a CA is not configured on a PowerScale cluster, the SmartSync daemon does not start. An account and policy might be configured, but none of the policies run until a CA is configured. The failed policies are not displayed under `isi dm jobs list` or `isi dm`

`historical-jobs list` because they never started. If a CA is not configured, the `/var/log/isi_dm.log` states that a CA is not installed, as shown in the following excerpt:

```
Certificates not correctly installed, Data Mover service sleeping:
At least one CA must be installed: No such file or directory
from dm_load_certs_from_store
(/b/mnt/src/isilon/lib/isi_dm/isi_dm_remote/src/rpc/dm_tls.cpp:197
)     from dm_tls_init
(/b/mnt/src/isilon/lib/isi_dm/isi_dm_remote/src/rpc/dm_tls.cpp:279
): Unable to load certificate information
```

Authentication failure

After you configure CA and identity, the SmartSync service is activated, and SmartSync attempts a handshake with the target cluster. If the CA or identity is misconfigured, the handshake process fails. In this case, the `/var/log/isi_dm.log` contains the following information:

```
2021-11-30T08:59:06.864181+00:00 <3.7> GEN-HOP-NOCL-RR-1(id1)
isi_dm_d[52758]: [0x828c0a110]:
/b/mnt/src/isilon/lib/isi_dm/isi_dm_remote/src/acct_mon.cpp:dm_acc
tmon_try_ping:459: [Fiber 4229] ping for account guid:
0000000000000000c4000000000000000000000000000000, result: dead
```

Alternatively, the full handshake error is logged if the SmartSync daemon is set to a `LOG_INFO` level using `isi_ilog`.

Dataset creation or base path mismatch

A copy or repeat-copy policy requires an available dataset for replication before running. If a dataset is not created before the copy or repeat-copy policy job is launched for the same base path, the job is paused. In the example shown in the following figure, the base path of the copy policy does not match the base path of the dataset policy. As discussed in Replication policies, a copy or repeat-copy policy requires a dataset creation in the same base path before the copy or repeat-copy policy runs.

```
OneFS94-S1-1# ll /ifs/data/Isilon_Support/datamover/transfer_failures
total 9
-rw-rw----     1 root  wheel  679 Feb 24 09:56 baseline_failures_103
OneFS94-S1-1# cat /ifs/data/Isilon_Support/datamover/transfer_failures/baseline_failu
task_id=0x00000000000000ce, task_type=root task ds base copy, task_state=failed-fatal
 path doesn't match dataset base path: '/ifs/data/test2' != '/ifs/data/repeat-copy':
    from bc_task_initialize_dsh (/b/mnt/src/isilon/lib/isi_dm/isi_dm/src/ds_base_copy
    from dmt_execute (/b/mnt/src/isilon/lib/isi_dm/isi_dm/src/ds_base_copy_root_task.
    from dm_txn_execute_internal (/b/mnt/src/isilon/lib/isi_dm/isi_dm_base/src/txn.cp
    from dm_txn_execute (/b/mnt/src/isilon/lib/isi_dm/isi_dm_base/src/txn.cpp:2247)
    from dmp_task_spark_execute (/b/mnt/src/isilon/lib/isi_dm/isi_dm/src/task_runner.
```

Figure 7. Transfer failure example

Once any errors for a policy are resolved, use the `isi dm jobs modify` command to resume the job.

Limitations

Current limitations of the SmartSync feature include:

- A failover and failback option is not available. An option to allow writes on the target cluster is also not available. However, the dataset is available for read and write on

copy policies once the replication to the target platform is complete if the `--copy-create-dataset-on-target=false` option is specified.

Note: Workflows with constantly changing data require a large dataset transfer with a copy policy. Consider using a pull policy as an alternative, offloading the resource consumption to the target cluster, assuming network bandwidth is available.

For repeat-copy policies, enabling read and write on the target platform will be available in a future release. However, SmartSync for OneFS uses SnapshotIQ for creating the dataset snapshot. If required, the files on the target platform may be copied out of the snapshot for access.

For example, run the `isi snapshot list` command on the target cluster to find the required dataset name. Next, use `ls` to list the contents of the snapshot, and copy the required file out of the snapshot, as shown in the following snippet:

```
OneFS94-S2-1# isi snapshot list
ID   Name                            Path
--------------------------------------------------------------
2    isi_dm_snap_dsr_1_1645112651  /ifs/data/test2
.
.
38   isi_dm_snap_dsr_19_1645538704 /ifs/data/repeat-copy
--------------------------------------------------------------
Total: 23
OneFS94-S2-1# ls
/ifs/.snapshot/isi_dm_snap_dsr_19_1645538704/data/repeat-copy
hello-repea1t.txt
OneFS94-S2-1# cp -c
/ifs/.snapshot/isi_dm_snap_dsr_19_1645538704/data/repeat-
copy/hello-repea1t.txt /ifs/data/test.txt
```

- PowerScale clusters in compliance mode are not supported.

OneFS features and SmartSync

Role Based Access Control

Role Based Access Control (RBAC) divides the powers of the `root` and `administrator` users into more granular privileges and allows the assignment of these privileges to specific roles. For example, data protection administrators can be assigned full access to SmartSync configuration and control but only read-only access to other cluster functionality. SmartSync administrative access is assigned through the `ISI_PRIV_DATAMOVER` privilege. RBAC is fully integrated with the CLI and platform API.

Small File Storage Efficiency

OneFS Small File Storage Efficiency (SFSE) provides a feature for small files in OneFS, packing them into larger files, resulting in increased storage efficiency. If a SmartSync policy is configured for an SFSE directory, the data is replicated to the target cluster. However, the SFSE data is unpacked on the source cluster before replication. If the target cluster has SFSE enabled, the data is packed when the next SmartPools job runs on the target cluster if the dataset is in read/write. The data remains unpacked if the target

cluster does not have SFSE enabled. For more information about SFSE, see the *PowerScale OneFS Small File Storage Efficiency for Archive* white paper.

SmartDedupe

When deduplicated files are replicated to another PowerScale cluster through SmartSync, the deduplicated files are rehydrated back to their original size because they no longer share blocks on the target PowerScale cluster. When replication is complete, SmartDedupe can run on the target cluster, providing the same space efficiency benefits as the source cluster.

Shadow stores are not transferred to target clusters. Hence, deduplicated files do not consume less space than nondeduplicated files when they are replicated. To avoid running out of space on target clusters, verify that the total amount of storage space saved and storage space consumed do not exceed the available space on the target cluster. To reduce the amount of storage space consumed on a target PowerScale cluster, configure deduplication for the target directories of the replication policies. Although this approach deduplicates data on the target directory, it does not allow SmartSync to transfer shadow stores. Deduplication is still performed post-replication through a deduplication job running on the target cluster.

Inline compression and deduplication

For source clusters that contain PowerScale and Isilon nodes that support inline compression and deduplication, during the dataset creation, the source data is rehydrated, decompressed, and transferred uncompressed to the target cluster. Suppose the target cluster consists of nodes that support inline compression and deduplication. In that case, the replication data goes through the same inline compression and deduplication as any other data that is written to these platforms.

16 TiB large file support

The large file support feature permits the maximum allowable file size in a PowerScale cluster to increase four-fold, from 4 tebibytes previously, to 16 tebibytes. For more information about the large file support feature for 16 TiB, see the *PowerScale OneFS Best Practices* white paper.

If large file support is enabled for 16 TiB on a source cluster, all new and existing SmartSync policies only connect with target clusters that also have large file support enabled, as illustrated in the following figure.

Furthermore, workflow impacts for existing SmartSync policies are possible if for any reason the target cluster does not have resources for the 16 TiB feature.

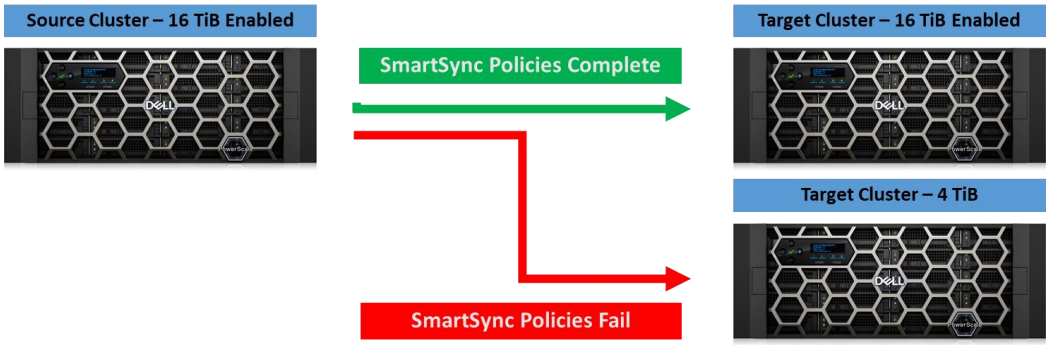

Figure 8. Large file support and SmartSync

CloudPools

PowerScale clusters that are using OneFS CloudPools to tier data to a cloud provider have a stub file, known as a SmartLink. The file is retained on the cluster with the relevant metadata to retrieve the file at a later point. Without the SmartLink, a file that is tiered to the cloud cannot be retrieved. If a SmartLink is replicated to a target cluster, the target cluster must have CloudPools active with the same configuration as the source cluster to be able to retrieve files tiered to the cloud.

SmartSync performs a deep copy for dataset creation of data tiered with CloudPools. Deep copy is a process that retrieves all data that is tiered to a cloud provider on the source cluster, allowing all the data to be replicated to the target cluster.

Hadoop Transparent Data Encryption

Apache Hadoop Distributed File System (HDFS) Transparent Data Encryption (TDE) provides end-to-end encryption between HDFS clients and a PowerScale cluster. HDFS TDE is configured in OneFS through encryption zones, where data is transparently encrypted and decrypted as data is read and written. For more information about HDFS TDE for OneFS, see the *Using Transparent Data Encryption with Isilon HDFS* white paper.

SmartSync does not support the replication of the TDE domain and keys. On the source cluster, if a SmartSync policy is configured to include an HDFS TDE directory, the encrypted data is replicated to the target cluster. However, on the target cluster, the encrypted data is not accessible because the target cluster is missing the metadata that is stored in the IFS domain for clients to decrypt the data. TDE ensures that the data is encrypted before it is stored on the source cluster. Also, TDE stores the mapping to the keys required to decrypt the data, but not the actual keys, making the encrypted data on the target cluster inaccessible.

Conclusion

Meeting modern data replication requirements means replicating data beyond the traditional data center and multiple cloud targets. SmartSync provides a unified approach to data replication, including cloud targets and PowerScale clusters, and allows administrators to design effective RPO and RTO solutions.

References

Dell Technologies documentation

The following Dell Technologies resources provide additional information related to this document. Access to some documents depends on your login credentials. If you do not have access to a document, contact your Dell Technologies representative.

- PowerScale Info Hub
- Using Transparent Data Encryption with Isilon HDFS
- Dell PowerScale OneFS Best Practices
- PowerScale OneFS Documentation – Dell Support
- PowerScale Network Design Considerations
- High Availability and Data Protection with Dell PowerScale Scale-Out NAS
- PowerScale OneFS CloudPools Administration Guide
- PowerScale: CloudPools and ECS

Other documentation

- MIT Technology Review: The Rise of Data Capital