## CONTENTS

<table>
<thead>
<tr>
<th>Chapter 1</th>
<th>Introduction to this guide</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>About this guide:</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>Isilon scale-out NAS overview</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>Where to go for support:</td>
<td>8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 2</th>
<th>OneFS backup and recovery</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>OneFS backup and recovery overview</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>SyncIQ backup and recovery overview</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>NDMP backup and recovery overview</td>
<td>10</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 3</th>
<th>Data replication with SyncIQ</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Replication policies and jobs:</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>Automated replication policies:</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>Source and target cluster association:</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>Full and differential replication:</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>Controlling replication job resource consumption:</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>Replication policy priority:</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>Replication reports:</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>Replication snapshots:</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>Source cluster snapshots:</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>Target cluster snapshots:</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>Data failover and failback with SyncIQ:</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>Data failover:</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>Data failback:</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Replication and backup with SmartLock:</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>SmartLock replication and backup limitations:</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>Data replication and backup with deduplication:</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>Recovery times and objectives for SyncIQ:</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>SyncIQ license functionality:</td>
<td>23</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 4</th>
<th>Backing up data with SyncIQ</th>
<th>25</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Creating replication policies:</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>Excluding directories in replication:</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>Excluding files in replication:</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>File criteria options:</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>Configure default replication policy settings:</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>Create a replication policy:</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>Create a SyncIQ domain:</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>Assess a replication policy:</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>Managing replication to remote clusters:</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>Start a replication job:</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>Pause a replication job:</td>
<td>37</td>
</tr>
<tr>
<td></td>
<td>Resume a replication job:</td>
<td>37</td>
</tr>
<tr>
<td></td>
<td>Cancel a replication job:</td>
<td>37</td>
</tr>
<tr>
<td></td>
<td>View active replication jobs:</td>
<td>37</td>
</tr>
<tr>
<td></td>
<td>Replication job information:</td>
<td>37</td>
</tr>
<tr>
<td></td>
<td>Managing replication policies:</td>
<td>38</td>
</tr>
</tbody>
</table>
Modify a replication policy ............................................................... 38
Delete a replication policy ............................................................... 38
Enable or disable a replication policy ............................................. 39
View replication policies ............................................................... 39
Replication policy information ....................................................... 39
Replication policy settings ............................................................. 40
Managing replication to the local cluster ........................................... 43
  Cancel replication to the local cluster ........................................... 43
  Break local target association ..................................................... 44
  View replication policies targeting the local cluster......................... 44
  Remote replication policy information ......................................... 44
Managing replication performance rules ......................................... 45
  Create a network traffic rule ..................................................... 45
  Create a file operations rule ..................................................... 45
  Modify a performance rule ..................................................... 45
  Delete a performance rule ..................................................... 46
  Enable or disable a performance rule ......................................... 46
  View performance rules ..................................................... 46
Managing replication reports ....................................................... 46
  Configure default replication report settings ............................. 46
  Delete replication reports ..................................................... 47
  View replication reports ..................................................... 47
  Replication report information .................................................. 47
Managing failed replication jobs ................................................... 48
  Resolve a replication policy ..................................................... 48
  Reset a replication policy ..................................................... 48
  Perform a full or differential replication ..................................... 49
Managing changelists ............................................................... 49
  Create a changelist .......................................................... 50
  View a changelist .......................................................... 50
  Changelist information .......................................................... 50
Chapter 5  Recovering data with SyncIQ ................................. 53
Initiating data failover and failback with SyncIQ ............................. 54
  Fail over data to a secondary cluster ..................................... 54
  Revert a failover operation ..................................................... 54
  Fail back data to a primary cluster ......................................... 55
Performing disaster recovery for SmartLock directories .................. 56
  Recover SmartLock compliance directories on a target cluster .... 56
  Migrate SmartLock compliance directories ................................. 56
Chapter 6  NDMP backup ......................................................... 59
NDMP two-way backup ............................................................. 60
NDMP three-way backup ............................................................. 60
  Setting preferred IPs for NDMP three-way operations ................. 60
  Configure preferred IP settings for NDMP three-way operations .... 61
Snapshot-based incremental backups .......................................... 61
NDMP protocol support ............................................................. 62
Supported DMAs ........................................................................... 63
NDMP hardware support ............................................................. 63
NDMP backup limitations ............................................................. 63
NDMP performance recommendations ......................................... 64
Excluding files and directories from NDMP backups ..................... 65
Configure a library.................................................................87
Create a data media pool..........................................................87
Label tape devices.................................................................88
Create a metadata media pool...............................................88
Create a client........................................................................89

Configuring NDMP backup with Symantec NetBackup...............90
Add an NDMP host..................................................................91
Configure storage devices.....................................................91
Create a volume pool...........................................................92
Inventory a robot.....................................................................92
Create a NetBackup policy.....................................................93

Configuring NDMP backup with CommVault Simpana...............94
Add a NAS client..................................................................94
Add an NDMP library...........................................................95
Create a storage policy........................................................95
Assign a storage policy and schedule to a client....................96

Configuring NDMP backup with IBM Tivoli Storage Manager.....97
Initialize an IBM Tivoli Storage Manager server for an Isilon cluster
..........................................................................................97

Configure an IBM Tivoli Storage Manager server for an Isilon cluster
..........................................................................................97
CHAPTER 1

Introduction to this guide

This section contains the following topics:

- About this guide ................................................................. 8
- Isilon scale-out NAS overview .............................................. 8
- Where to go for support ........................................................ 8
About this guide

This guide describes how to back up and recover data on Isilon clusters through either the SyncIQ software module or the Network Data Management Protocol (NDMP).

We value your feedback. Please let us know how we can improve this document.

- Take the survey at https://www.research.net/s/isi-docfeedback.
- Send your comments or suggestions to docfeedback@isilon.com.

Isilon scale-out NAS overview

The EMC Isilon scale-out NAS storage platform combines modular hardware with unified software to harness unstructured data. Powered by the OneFS operating system, an EMC Isilon cluster delivers a scalable pool of storage with a global namespace.

The platform's unified software provides centralized web-based and command-line administration to manage the following features:

- A cluster that runs a distributed file system
- Scale-out nodes that add capacity and performance
- Storage options that manage files and tiering
- Flexible data protection and high availability
- Software modules that control costs and optimize resources

Where to go for support

You can contact EMC Isilon Technical Support for any questions about EMC Isilon products.

<table>
<thead>
<tr>
<th>Online Support</th>
<th>Live Chat</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Create a Service Request</td>
</tr>
<tr>
<td>Telephone Support</td>
<td>United States: 1-800-SVC-4EMC (800-782-4362)</td>
</tr>
<tr>
<td></td>
<td>Canada: 800-543-4782</td>
</tr>
<tr>
<td></td>
<td>Worldwide: +1-508-497-7901</td>
</tr>
<tr>
<td></td>
<td>For local phone numbers in your country, see</td>
</tr>
<tr>
<td></td>
<td>EMC Customer Support Centers.</td>
</tr>
<tr>
<td>Help with online</td>
<td>For questions specific to EMC Online Support</td>
</tr>
<tr>
<td>support</td>
<td>registration or access, email <a href="mailto:support@emc.com">support@emc.com</a></td>
</tr>
</tbody>
</table>
CHAPTER 2

OneFS backup and recovery

This section contains the following topics:

- OneFS backup and recovery overview ................................................................. 10
- SyncIQ backup and recovery overview ................................................................. 10
- NDMP backup and recovery overview ................................................................. 10
OneFS backup and recovery overview

You can back up data stored on Isilon clusters to another Isilon cluster or a tape device. You can back up data to an Isilon cluster with the SyncIQ software module. SyncIQ enables you to recover backed up data through failover and failback. Failover enables you to access data on the cluster it was backed up to. After you fail over, you can fail back to resume accessing your data on the cluster it was backed up from.

You can back up data to a tape device over NDMP. After you back up data to a tape device, you can restore the data to any Isilon cluster.

SyncIQ backup and recovery overview

OneFS enables you to replicate data from one Isilon cluster to another through the SyncIQ software module. You must activate a SyncIQ license on both Isilon clusters before you can replicate data between them.

You can replicate data at the directory level while optionally excluding specific files and sub-directories from being replicated. SyncIQ creates and references snapshots to replicate a consistent point-in-time image of a root directory. Metadata such as access control lists (ACLs) and alternate data streams (ADS) are replicated along with data.

SyncIQ enables you to maintain a consistent backup copy of your data on another Isilon cluster. SyncIQ offers automated failover and failback capabilities that enable you to continue operations on another Isilon cluster if a primary cluster becomes unavailable.

NDMP backup and recovery overview

In OneFS, you can back up and restore file-system data through the Network Data Management Protocol (NDMP). From a backup server, you can direct backup and recovery processes between an Isilon cluster and backup devices such as tape devices, media servers, and virtual tape libraries (VTLs).

OneFS supports both three-way and two-way NDMP backup models. Three-way NDMP backup is also known as the remote NDMP backup and the two-way NDMP backup is known as the local or direct NDMP backup. During a three-way NDMP backup operation, a data management application (DMA) on a backup server instructs the cluster to start backing up data to a tape media server that is either attached to the LAN or directly attached to the DMA.

During a two-way NDMP backup operation, a DMA on a backup server instructs a Backup Accelerator node on the cluster to start backing up data to a tape media server that is attached to the Backup Accelerator node.

Two-way NDMP backup is significantly faster than the three-way NDMP backup. It is also the most efficient method in terms of cluster resource consumption. However, a two-way NDMP backup requires that you attach one or more Backup Accelerator nodes to the cluster.

In both the two-way and three-way NDMP backup models, file history data is transferred from the cluster to the backup server. Before a backup begins, OneFS creates a snapshot of the targeted directory, then backs up the snapshot, which ensures that the backup image represents a specific point in time.

You do not need to activate a SnapshotIQ license on the cluster to perform NDMP backups. If you have activated a SnapshotIQ license on the cluster, you can generate a snapshot through the SnapshotIQ tool, and then back up the same snapshot to multiple
tape devices. If you back up a SnapshotIQ snapshot, OneFS does not create another snapshot for the backup.

Note

If you are backing up SmartLock directories for compliance purposes, it is recommended that you do not specify autocommit time periods for the SmartLock directories. This is because, depending on the autocommit period, files in the SmartLock directories may still be subject to change.
CHAPTER 3

Data replication with SyncIQ

This section contains the following topics:

- Replication policies and jobs ................................................................. 14
- Replication snapshots .............................................................................. 18
- Data failover and failback with SyncIQ .................................................. 19
- Replication and backup with SmartLock .................................................. 20
- Data replication and backup with deduplication ...................................... 21
- Recovery times and objectives for SyncIQ ................................................. 22
- SyncIQ license functionality ..................................................................... 23
Replication policies and jobs

Data replication is coordinated according to replication policies and replication jobs. Replication policies specify what data is replicated, where the data is replicated to, and how often the data is replicated. Replication jobs are the operations that replicate data from one Isilon cluster to another. SyncIQ generates replication jobs according to replication policies.

A replication policy specifies two clusters: the source and the target. The cluster on which the replication policy exists is the source cluster. The cluster that data is being replicated to is the target cluster. When a replication policy starts, SyncIQ generates a replication job for the policy. When a replication job runs, files from a directory tree on the source cluster are replicated to a directory tree on the target cluster; these directory trees are known as source and target directories.

After the first replication job created by a replication policy finishes, the target directory and all files contained in the target directory are set to a read-only state, and can be modified only by other replication jobs belonging to the same replication policy. We recommend that you do not create more than 1,000 policies on a cluster.

Note

To prevent permissions errors, make sure that ACL policy settings are the same across source and target clusters.

You can create two types of replication policies: synchronization policies and copy policies. A synchronization policy maintains an exact replica of the source directory on the target cluster. If a file or sub-directory is deleted from the source directory, the file or directory is deleted from the target cluster when the policy is run again.

You can use synchronization policies to fail over and fail back data between source and target clusters. When a source cluster becomes unavailable, you can fail over data on a target cluster and make the data available to clients. When the source cluster becomes available again, you can fail back the data to the source cluster.

A copy policy maintains recent versions of the files that are stored on the source cluster. However, files that are deleted on the source cluster are not deleted from the target cluster. Failback is not supported for copy policies. Copy policies are most commonly used for archival purposes.

Copy policies enable you to remove files from the source cluster without losing those files on the target cluster. Deleting files on the source cluster improves performance on the source cluster while maintaining the deleted files on the target cluster. This can be useful if, for example, your source cluster is being used for production purposes and your target cluster is being used only for archiving.

After creating a job for a replication policy, SyncIQ must wait until the job completes before it can create another job for the policy. Any number of replication jobs can exist on a cluster at a given time; however, no more than 50 replication jobs can run on a source cluster at the same time. If more than 50 replication jobs exist on a cluster, the first 50 jobs run while the others are queued to run.

There is no limit to the number of replication jobs that a target cluster can support concurrently. However, because more replication jobs require more cluster resources, replication will slow down as more concurrent jobs are added.

When a replication job runs, OneFS generates workers on the source and target cluster. Workers on the source cluster send data while workers on the target cluster write data.
OneFS generates no more than 8 workers per node per replication job. For example, in a five node cluster, OneFS would create no more than 40 workers for a replication job.

You can replicate any number of files and directories with a single replication job. You can prevent a large replication job from overwhelming the system by limiting the amount of cluster resources and network bandwidth that data synchronization is allowed to consume. Because each node in a cluster is able to send and receive data, the speed at which data is replicated increases for larger clusters.

**Automated replication policies**

You can manually start a replication policy at any time, but you can also configure replication policies to start automatically based on source directory modifications or schedules.

You can configure a replication policy to run according to a schedule, so that you can control when replication is performed. You can also configure policies to replicate the data captured in snapshots of a directory. You can also configure a replication policy to start when SyncIQ detects a modification to the source directory, so that SyncIQ maintains a more current version of your data on the target cluster.

Scheduling a policy can be useful under the following conditions:

- You want to replicate data when user activity is minimal
- You can accurately predict when modifications will be made to the data

If a policy is configured to run according to a schedule, you can configure the policy not to run if no changes have been made to the contents of the source directory since the job was last run. However, if changes are made to the parent directory of the source directory or a sibling directory of the source directory, and then a snapshot of the parent directory is taken, SyncIQ will create a job for the policy, even if no changes have been made to the source directory. Also, if you monitor the cluster through the File System Analytics (FSA) feature of InsightIQ, the FSA job will create snapshots of /ifs, which will most likely cause a replication job to start whenever the FSA job is run.

Replicating data contained in snapshots of a directory can be useful under the following conditions:

- You want to replicate data according to a schedule, and you are already generating snapshots of the source directory through a snapshot schedule
- You want to maintain identical snapshots on both the source and target cluster
- You want to replicate existing snapshots to the target cluster
  To do this, you must enable archival snapshots on the target cluster. This setting can only been enabled when the policy is created.

If a policy is configured to replicate snapshots, you can configure SyncIQ to replicate only snapshots that match a specified naming pattern.

Configuring a policy to start when changes are made to the source directory can be useful under the following conditions:

- You want to retain a up-to-date copy of your data at all times
- You are expecting a large number of changes at unpredictable intervals

For policies that are configured to start whenever changes are made to the source directory, SyncIQ checks the source directories every ten seconds. SyncIQ checks all files and directories underneath the source directory, regardless of whether those files or directories are excluded from replication, so SyncIQ might occasionally run a replication job unnecessarily. For example, assume that newPolicy replicates /ifs/data/media but excludes /ifs/data/media/temp. If a modification is made to /ifs/data/
media/temp/file.txt, SyncIQ will run newPolicy, even though /ifs/data/
media/temp/file.txt will not be replicated.

If a policy is configured to start whenever changes are made to the source directory, and
a replication job fails, SyncIQ waits one minute before attempting to run the policy again.
SyncIQ increases this delay exponentially for each failure up to a maximum of eight
hours. You can override the delay by running the policy manually at any time. After a job
for the policy completes successfully, SyncIQ will resume checking the source directory
every ten seconds.

If a policy is configured to start whenever changes are made to the source directory, you
can configure SyncIQ to wait a specified period of time after the source directory is
modified before starting a job.

---

**Note**

To avoid frequent synchronization of minimal sets of changes, and overtaxing system
resources, we strongly advise against configuring continuous replication when the source
directory is highly active. In such cases, it is often better to configure continuous
replication with a change-triggered delay of several hours to consolidate groups of
changes.

---

**Source and target cluster association**

SyncIQ associates a replication policy with a target cluster by marking the target cluster
when the job runs for the first time. Even if you modify the name or IP address of the
target cluster, the mark persists on the target cluster. When a replication policy is run,
SyncIQ checks the mark to ensure that data is being replicated to the correct location.

On the target cluster, you can manually break an association between a replication policy
and target directory. Breaking the association between a source and target cluster causes
the mark on the target cluster to be deleted. You might want to manually break a target
association if an association is obsolete. If you break the association of a policy, the
policy is disabled on the source cluster and you cannot run the policy. If you want to run
the disabled policy again, you must reset the replication policy.

Breaking a policy association causes either a full replication or differential replication to
occur the next time you run the replication policy. During a full or differential replication,
SyncIQ creates a new association between the source and target clusters. Depending on
the amount of data being replicated, a full or differential replication can take a very long
time to complete.

**CAUTION**

Changes to the configuration of the target cluster outside of SyncIQ can introduce an
error condition that effectively breaks the association between the source and target
cluster. For example, changing the DNS record of the target cluster could cause this
problem. If you need to make significant configuration changes to the target cluster
outside of SyncIQ, make sure that your SyncIQ policies can still connect to the target
cluster.

---

**Full and differential replication**

If a replication policy encounters an issue that cannot be fixed (for example, if the
association was broken on the target cluster), you might need to reset the replication
policy. If you reset a replication policy, SyncIQ performs either a full replication or a
differential replication the next time the policy is run. You can specify the type of replication that SyncIQ performs.

During a full replication, SyncIQ transfers all data from the source cluster regardless of what data exists on the target cluster. A full replication consumes large amounts of network bandwidth and can take a very long time to complete. However, a full replication is less strenuous on CPU usage than a differential replication.

During a differential replication, SyncIQ first checks whether a file already exists on the target cluster and then transfers only data that does not already exist on the target cluster. A differential replication consumes less network bandwidth than a full replication; however, differential replications consume more CPU. Differential replication can be much faster than a full replication if there is an adequate amount of available CPU for the replication job to consume.

**Controlling replication job resource consumption**

You can create rules that limit the network traffic created by replication jobs, the rate at which files are sent by replication jobs, the percent of CPU used by replication jobs, and the number of workers created for replication jobs.

If you limit the percentage of total workers that SyncIQ can create, the limit is applied to the total amount of workers that SyncIQ could create, which is determined by cluster hardware.

**Note**

File-operation rules might not work accurately for files that can take more than a second to transfer and for files that are not predictably similar in size.

**Replication policy priority**

When creating a replication policy, you can configure a policy to have priority over other jobs.

If multiple replication jobs are queued to be run because the maximum number of jobs are already running, jobs created by policies with priority will be run before jobs without priorities. For example, assume that 50 jobs are currently running. A job without priority is the created and queued to run; next, a job with priority is created and queued to run. The job with priority will run next, even though the job without priority has been queued for a longer period of time.

SyncIQ will also pause replication jobs without priority to allow jobs with priority to run. For example, assume that 50 jobs are already running, and one of them does not have priority. If a replication job with priority is created, SyncIQ will pause the replication job without priority and run the job with priority.

**Replication reports**

After a replication job completes, SyncIQ generates a replication report that contains detailed information about the job, including how long the job ran, how much data was transferred, and what errors occurred.

If a replication report is interrupted, SyncIQ might create a subreport about the progress of the job so far. If the job is then restarted, SyncIQ creates another subreport about the progress of the job until the job either completes or is interrupted again. SyncIQ creates a subreport each time the job is interrupted until the job completes successfully. If multiple subreports are created for a job, SyncIQ combines the information from the subreports into a single report.
SyncIQ routinely deletes replication reports. You can specify the maximum number of replication reports that SyncIQ retains and the length of time that SyncIQ retains replication reports. If the maximum number of replication reports is exceeded on a cluster, SyncIQ deletes the oldest report each time a new report is created.

You cannot customize the content of a replication report.

**Note**

If you delete a replication policy, SyncIQ automatically deletes any reports that were generated for that policy.

## Replication snapshots

SyncIQ generates snapshots to facilitate replication, failover, and failback between Isilon clusters. Snapshots generated by SyncIQ can also be used for archival purposes on the target cluster.

### Source cluster snapshots

SyncIQ generates snapshots on the source cluster to ensure that a consistent point-in-time image is replicated and that unaltered data is not sent to the target cluster.

Before running a replication job, SyncIQ creates a snapshot of the source directory. SyncIQ then replicates data according to the snapshot rather than the current state of the cluster, allowing users to modify source directory files while ensuring that an exact point-in-time image of the source directory is replicated.

For example, if a replication job of `/ifs/data/dir/` starts at 1:00 PM and finishes at 1:20 PM, and `/ifs/data/dir/file` is modified at 1:10 PM, the modifications are not reflected on the target cluster, even if `/ifs/data/dir/file` is not replicated until 1:15 PM.

You can replicate data according to a snapshot generated with the SnapshotIQ software module. If you replicate data according to a SnapshotIQ snapshot, SyncIQ does not generate another snapshot of the source directory. This method can be useful if you want to replicate identical copies of data to multiple Isilon clusters.

SyncIQ generates source snapshots to ensure that replication jobs do not transfer unmodified data. When a job is created for a replication policy, SyncIQ checks whether it is the first job created for the policy. If it is not the first job created for the policy, SyncIQ compares the snapshot generated for the earlier job with the snapshot generated for the new job.

SyncIQ replicates only data that has changed since the last time a snapshot was generated for the replication policy. When a replication job is completed, SyncIQ deletes the previous source-cluster snapshot and retains the most recent snapshot until the next job is run.

### Target cluster snapshots

When a replication job is run, SyncIQ generates a snapshot on the target cluster to facilitate failover operations. When the next replication job is created for the replication policy, the job creates a new snapshot and deletes the old one.

If a SnapshotIQ license has been activated on the target cluster, you can configure a replication policy to generate additional snapshots that remain on the target cluster even as subsequent replication jobs run.
SyncIQ generates target snapshots to facilitate failover on the target cluster regardless of whether a SnapshotIQ license has been configured on the target cluster. Failover snapshots are generated when a replication job completes. SyncIQ retains only one failover snapshot per replication policy, and deletes the old snapshot after the new snapshot is created.

If a SnapshotIQ license has been activated on the target cluster, you can configure SyncIQ to generate archival snapshots on the target cluster that are not automatically deleted when subsequent replication jobs run. Archival snapshots contain the same data as the snapshots that are generated for failover purposes. However, you can configure how long archival snapshots are retained on the target cluster. You can access archival snapshots the same way that you access other snapshots generated on a cluster.

Data failover and failback with SyncIQ

SyncIQ enables you to perform automated data failover and failback operations between Isilon clusters. If a cluster is rendered unusable, you can fail over to another Isilon cluster, enabling clients to access their data on the other cluster. If the unusable cluster becomes accessible again, you can fail back to the original Isilon cluster.

For the purposes of explaining failover and failback procedures, the cluster originally accessed by clients is referred to as the primary cluster, and the cluster that client data is originally replicated to is referred to as the secondary cluster. Failover is the process that allows clients to modify data on a secondary cluster. Failback is the process that allows clients to access data on the primary cluster again and begins to replicate data back to the secondary cluster.

Failover and failback can be useful in disaster recovery procedures. For example, if a primary cluster is damaged by a natural disaster, you can migrate clients to a secondary cluster until the primary cluster is repaired and then migrate the clients back to the primary cluster.

You can fail over and fail back to facilitate scheduled cluster maintenance. For example, if you are upgrading the primary cluster, you might want to migrate clients to a secondary cluster until the upgrade is complete and then migrate clients back to the primary cluster.

Note

Data failover is not supported for compliance SmartLock directories. However, data failover is supported for enterprise SmartLock directories. Data failback is unsupported for all SmartLock directories.

Data failover

Data failover is the process of preparing data on a secondary cluster to be modified by clients. After you fail over to a secondary cluster, you can redirect clients to modify their data on the secondary cluster.

Before failover is performed, you must create and run a replication policy on the primary cluster. You initiate the failover process on the secondary cluster. Failover is performed per replication policy; to migrate data that is spread across multiple replication policies, you must initiate failover for each replication policy.

You can use any replication policy to fail over. However, if the action of the replication policy is set to copy, any file that was deleted on the primary cluster will be present on the secondary cluster. When the client connects to the secondary cluster, all files that were deleted on the primary cluster will be available to the client.
If you initiate failover for a replication policy while an associated replication job is running, the failover operation completes but the replication job fails. Because data might be in an inconsistent state, SyncIQ uses the snapshot generated by the last successful replication job to revert data on the secondary cluster to the last recovery point.

If a disaster occurs on the primary cluster, any modifications to data that were made after the last successful replication job started are not reflected on the secondary cluster. When a client connects to the secondary cluster, their data appears as it was when the last successful replication job was started.

Data failback

Data failback is the process of restoring clusters to the roles they occupied before a failover operation. After data failback is complete, the primary cluster hosts clients and replicates data to the secondary cluster for backup.

The first step in the failback process is updating the primary cluster with all of the modifications that were made to the data on the secondary cluster. The next step in the failback process is preparing the primary cluster to be accessed by clients. The final step in the failback process is resuming data replication from the primary to the secondary cluster. At the end of the failback process, you can redirect users to resume accessing their data on the primary cluster.

To update the primary cluster with the modifications that were made on the secondary cluster, SyncIQ must create a SyncIQ domain for the source directory.

You can fail back data with any replication policy that meets all of the following criteria:

- The source directory is not a SmartLock directory.
- The policy has been failed over.
- The policy is a synchronization policy.
- The policy does not exclude any files or directories from replication.

Replication and backup with SmartLock

You must ensure that SmartLock directories on the EMC Isilon cluster remain protected during replication and backup operations.

If you are replicating SmartLock directories with SyncIQ, it is recommended that you configure all nodes on the source and target clusters into Network Time Protocol (NTP) peer mode to ensure that the node clocks are synchronized. For compliance clusters, it is recommended that you configure all nodes on the source and target clusters into NTP peer mode before you set the compliance clock to ensure that the compliance clocks are initially set to the same time.

**Note**

If you replicate data to a SmartLock directory, do not configure SmartLock settings for that directory until you are no longer replicating data to the directory. Configuring an autocommit time period for a SmartLock directory that you are replicating to can cause replication jobs to fail. If the target directory commits a file to a WORM state, and the file is modified on the source cluster, the next replication job will fail because it cannot update the file.
SmartLock replication and backup limitations

Be aware of the limitations of replicating and backing up SmartLock directories with SyncIQ and NDMP.

If the source directory or target directory of a SyncIQ policy is a SmartLock directory, replication might not be allowed. For more information, see the following table:

<table>
<thead>
<tr>
<th>Source directory type</th>
<th>Target directory type</th>
<th>Allowed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-SmartLock</td>
<td>Non-SmartLock</td>
<td>Yes</td>
</tr>
<tr>
<td>Non-SmartLock</td>
<td>SmartLock enterprise</td>
<td>Yes</td>
</tr>
<tr>
<td>Non-SmartLock</td>
<td>SmartLock compliance</td>
<td>No</td>
</tr>
<tr>
<td>SmartLock enterprise</td>
<td>Non-SmartLock</td>
<td>Yes; however, retention dates and commit status of files will be lost.</td>
</tr>
<tr>
<td>SmartLock enterprise</td>
<td>SmartLock enterprise</td>
<td>Yes</td>
</tr>
<tr>
<td>SmartLock enterprise</td>
<td>SmartLock compliance</td>
<td>No</td>
</tr>
<tr>
<td>SmartLock compliance</td>
<td>Non-SmartLock</td>
<td>No</td>
</tr>
<tr>
<td>SmartLock compliance</td>
<td>SmartLock enterprise</td>
<td>No</td>
</tr>
<tr>
<td>SmartLock compliance</td>
<td>SmartLock compliance</td>
<td>Yes</td>
</tr>
</tbody>
</table>

If you are replicating a SmartLock directory to another SmartLock directory, you must create the target SmartLock directory prior to running the replication policy. Although OneFS will create a target directory automatically if a target directory does not already exist, OneFS will not create a target SmartLock directory automatically. If you attempt to replicate an enterprise directory before the target directory has been created, OneFS will create a non-SmartLock target directory and the replication job will succeed. If you replicate a compliance directory before the target directory has been created, the replication job will fail.

If you replicate SmartLock directories to another EMC Isilon cluster with SyncIQ, the WORM state of files is replicated. However, SmartLock directory configuration settings are not transferred to the target directory.

For example, if you replicate a directory that contains a committed file that is set to expire on March 4th, the file is still set to expire on March 4th on the target cluster. However, if the directory on the source cluster is set to prevent files from being committed for more than a year, the target directory is not automatically set to the same restriction.

If you back up data to an NDMP device, all SmartLock metadata relating to the retention date and commit status is transferred to the NDMP device. If you restore data to a SmartLock directory on the cluster, the metadata persists on the cluster. However, if the directory that you restore to is not a SmartLock directory, the metadata is lost. You can restore to a SmartLock directory only if the directory is empty.

Data replication and backup with deduplication

When deduplicated files are replicated to another Isilon cluster or backed up to a tape device, the deduplicated files no longer share blocks on the target Isilon cluster or
backup device. However, although you can deduplicate data on a target Isilon cluster, you cannot deduplicate data on an NDMP backup device.

Shadows stores are not transferred to target clusters or backup devices. Because of this, deduplicated files do not consume less space than non-deduplicated files when they are replicated or backed up. To avoid running out of space, you must ensure that target clusters and tape devices have enough free space to store deduplicated data as if the data had not been deduplicated. To reduce the amount of storage space consumed on a target Isilon cluster, you can configure deduplication for the target directories of your replication policies. Although this will deduplicate data on the target directory, it will not allow SyncIQ to transfer shadow stores. Deduplication is still performed by deduplication jobs running on the target cluster.

The amount of cluster resources required to backup and replicate deduplicated data is the same as for non-deduplicated data. You can deduplicate data while the data is being replicated or backed up.

Recovery times and objectives for SyncIQ

The Recovery Point Objective (RPO) and the Recovery Time Objective (RTO) are measurements of the impacts that a disaster can have on business operations. You can calculate your RPO and RTO for a disaster recovery with replication policies.

RPO is the maximum amount of time for which data is lost if a cluster suddenly becomes unavailable. For an Isilon cluster, the RPO is the amount of time that has passed since the last completed replication job started. The RPO is never greater than the time it takes for two consecutive replication jobs to run and complete.

If a disaster occurs while a replication job is running, the data on the secondary cluster is reverted to the state it was in when the last replication job completed. For example, consider an environment in which a replication policy is scheduled to run every three hours, and replication jobs take two hours to complete. If a disaster occurs an hour after a replication job begins, the RPO is four hours, because it has been four hours since a completed job began replicating data.

RTO is the maximum amount of time required to make backup data available to clients after a disaster. The RTO is always less than or approximately equal to the RPO, depending on the rate at which replication jobs are created for a given policy.

If replication jobs run continuously, meaning that another replication job is created for the policy before the previous replication job completes, the RTO is approximately equal to the RPO. When the secondary cluster is failed over, the data on the cluster is reset to the state it was in when the last job completed; resetting the data takes an amount of time proportional to the time it took users to modify the data.

If replication jobs run on an interval, meaning that there is a period of time after a replication job completes before the next replication job for the policy starts, the relationship between RTO and RPO depends on whether a replication job is running when the disaster occurs. If a job is in progress when a disaster occurs, the RTO is roughly equal to the RPO. However, if a job is not running when a disaster occurs, the RTO is negligible because the secondary cluster was not modified since the last replication job ran, and the failover process is almost instantaneous.
SyncIQ license functionality

You can replicate data to another Isilon cluster only if you activate a SyncIQ license on both the local cluster and the target cluster.

If a SyncIQ license becomes inactive, you cannot create, run, or manage replication policies. Also, all previously created replication policies are disabled. Replication policies that target the local cluster are also disabled. However, data that was previously replicated to the local cluster is still available.
Data replication with SyncIQ
CHAPTER 4

Backing up data with SyncIQ

This section contains the following topics:

- Creating replication policies ................................................................. 26
- Managing replication to remote clusters .............................................. 36
- Managing replication policies ................................................................. 38
- Managing replication to the local cluster ............................................ 43
- Managing replication performance rules ............................................. 45
- Managing replication reports ............................................................... 46
- Managing failed replication jobs ......................................................... 48
- Managing changelists ........................................................................... 49
Creating replication policies

You can create replication policies that determine when data is replicated with SyncIQ.

Excluding directories in replication

You can exclude directories from being replicated by replication policies even if the directories exist under the specified source directory.

Note

Failback is not supported for replication policies that exclude directories.

By default, all files and directories under the source directory of a replication policy are replicated to the target cluster. However, you can prevent directories under the source directory from being replicated.

If you specify a directory to exclude, files and directories under the excluded directory are not replicated to the target cluster. If you specify a directory to include, only the files and directories under the included directory are replicated to the target cluster; any directories that are not contained in an included directory are excluded.

If you both include and exclude directories, any excluded directories must be contained in one of the included directories; otherwise, the excluded-directory setting has no effect. For example, consider a policy with the following settings:

- The root directory is /ifs/data
- The included directories are /ifs/data/media/music and /ifs/data/media/movies
- The excluded directories are /ifs/data/archive and /ifs/data/media/music/working

In this example, the setting that excludes the /ifs/data/archive directory has no effect because the /ifs/data/archive directory is not under either of the included directories. The /ifs/data/archive directory is not replicated regardless of whether the directory is explicitly excluded. However, the setting that excludes the /ifs/data/media/music/working directory does have an effect, because the directory would be replicated if the setting was not specified.

In addition, if you exclude a directory that contains the source directory, the exclude-directory setting has no effect. For example, if the root directory of a policy is /ifs/data, explicitly excluding the /ifs directory does not prevent /ifs/data from being replicated.

Any directories that you explicitly include or exclude must be contained in or under the specified root directory. For example, consider a policy in which the specified root directory is /ifs/data. In this example, you could include both the /ifs/data/media and the /ifs/data/users/directories because they are under /ifs/data.

Excluding directories from a synchronization policy does not cause the directories to be deleted on the target cluster. For example, consider a replication policy that synchronizes /ifs/data on the source cluster to /ifs/data on the target cluster. If the policy excludes /ifs/data/media from replication, and /ifs/data/media/file exists on the target cluster, running the policy does not cause /ifs/data/media/file to be deleted from the target cluster.
Excluding files in replication

If you do not want specific files to be replicated by a replication policy, you can exclude them from the replication process through file-matching criteria statements. You can configure file-matching criteria statements during the replication-policy creation process.

**Note**
You cannot fail back replication policies that exclude files.

A file-criteria statement can include one or more elements. Each file-criteria element contains a file attribute, a comparison operator, and a comparison value. You can combine multiple criteria elements in a criteria statement with Boolean "AND" and "OR" operators. You can configure any number of file-criteria definitions.

Configuring file-criteria statements can cause the associated jobs to run slowly. It is recommended that you specify file-criteria statements in a replication policy only if necessary.

Modifying a file-criteria statement will cause a full replication to occur the next time that a replication policy is started. Depending on the amount of data being replicated, a full replication can take a very long time to complete.

For synchronization policies, if you modify the comparison operators or comparison values of a file attribute, and a file no longer matches the specified file-matching criteria, the file is deleted from the target the next time the job is run. This rule does not apply to copy policies.

**File criteria options**

You can configure a replication policy to exclude files that meet or do not meet specific criteria.

You can specify file criteria based on the following file attributes:

**Date created**
Includes or excludes files based on when the file was created. This option is available for copy policies only.
You can specify a relative date and time, such as "two weeks ago", or specific date and time, such as "January 1, 2012." Time settings are based on a 24-hour clock.

**Date accessed**
Includes or excludes files based on when the file was last accessed. This option is available for copy policies only, and only if the global access-time-tracking option of the cluster is enabled.
You can specify a relative date and time, such as "two weeks ago", or specific date and time, such as "January 1, 2012." Time settings are based on a 24-hour clock.

**Date modified**
Includes or excludes files based on when the file was last modified. This option is available for copy policies only.
You can specify a relative date and time, such as "two weeks ago", or specific date and time, such as "January 1, 2012." Time settings are based on a 24-hour clock.

**File name**
Includes or excludes files based on the file name. You can specify to include or exclude full or partial names that contain specific text.
The following wildcard characters are accepted:

### Note
Alternatively, you can filter file names by using POSIX regular-expression (regex) text. Isilon clusters support IEEE Std 1003.2 (POSIX.2) regular expressions. For more information about POSIX regular expressions, see the BSD man pages.

<table>
<thead>
<tr>
<th>Wildcard character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Matches any string in place of the asterisk. For example, m* matches movies and m123.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Matches any characters contained in the brackets, or a range of characters separated by a dash. For example, b[aei]t matches bat, bet, and bit. You can exclude characters within brackets by following the first bracket with an exclamation mark. For example, b[!ie] matches bat but not bit or bet. You can match a bracket within a bracket if it is either the first or last character. For example, [[c]at matches cat and [at. You can match a dash within a bracket if it is either the first or last character. For example, car[-s] matches cars and car-.</td>
</tr>
<tr>
<td>?</td>
<td>Matches any character in place of the question mark. For example, t?p matches tap, tip, and top.</td>
</tr>
</tbody>
</table>

**Path**
Includes or excludes files based on the file path. This option is available for copy policies only. You can specify to include or exclude full or partial paths that contain specified text. You can also include the wildcard characters *, ?, and [ ].

**Size**
Includes or excludes files based on their size.

### Note
File sizes are represented in multiples of 1024, not 1000.

**Type**
Includes or excludes files based on one of the following file-system object types:
- Soft link
- Regular file
Configure default replication policy settings

You can configure default settings for replication policies. If you do not modify these settings when creating a replication policy, the specified default settings are applied.

Procedure

1. Click **Data Protection > SyncIQ > Settings.**

2. In the **Default Policy Settings** section, if you want policies to connect only to nodes in a specified SmartConnect zone, select **Connect only to the nodes within the target cluster SmartConnect zone.**

   **Note**

   This option will affect only policies that specify the target cluster as a SmartConnect zone.

3. Specify which nodes you want replication policies to connect to when a policy is run.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect policies to all nodes on a source cluster.</td>
<td>Click <strong>Run the policy on all nodes in this cluster.</strong></td>
</tr>
</tbody>
</table>
   | Connect policies only to nodes contained in a specified subnet and pool. | a. Click **Run the policy only on nodes in the specified subnet and pool.**
   |                                             | b. From the **Subnet and pool** list, select the subnet and pool.           |

   **Note**

   SyncIQ does not support dynamically allocated IP address pools. If a replication job connects to a dynamically allocated IP address, SmartConnect might reassign the address while a replication job is running, which would disconnect the job and cause it to fail.

4. Click **Submit.**

Create a replication policy

You can create a replication policy with SyncIQ that defines how and when data is replicated to another Isilon cluster. Configuring a replication policy is a five-step process.

Configure replication policies carefully. If you modify any of the following policy settings after the policy is run, OneFS performs either a full or differential replication the next time the policy is run:

- Source directory
- Included or excluded directories
- File-criteria statement
- Target cluster name or address
This applies only if you target a different cluster. If you modify the IP or domain name of a target cluster, and then modify the replication policy on the source cluster to match the new IP or domain name, a full replication is not performed.

- Target directory

Configure basic policy settings

You must configure basic settings for a replication policy.

Procedure

1. Click Data Protection > SyncIQ > Policies.
2. Click Create a SyncIQ policy.
3. In the Settings area, in the Policy name field, type a name for the replication policy.
4. (Optional) In the Description field, type a description for the replication policy.
5. In the Action area, specify the type of replication policy.
   - To copy all files from the source directory to the target directory, click Copy.
     
     **Note**
     
     Failback is not supported for copy policies.
     
   - To copy all files from the source directory to the target directory and delete any files on the target directory that are not in the source directory, click Synchronize.

6. In the Run job area, specify whether replication jobs will be run.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run jobs only when manually initiated by a user.</td>
<td>Click Only manually.</td>
</tr>
<tr>
<td>Run jobs automatically according to a schedule.</td>
<td>a. Click On a schedule.</td>
</tr>
<tr>
<td></td>
<td>b. Specify a schedule.</td>
</tr>
<tr>
<td></td>
<td>If you configure a replication policy to run more than once a day, you cannot configure the interval to span across two calendar days. For example, you cannot configure a replication policy to run every hour starting at 7:00 PM and ending at 1:00 AM.</td>
</tr>
<tr>
<td></td>
<td>c. To prevent the policy from being run when the contents of the source directory have not been modified, click Only run if source directory contents are modified.</td>
</tr>
<tr>
<td></td>
<td>d. To create OneFS events if a specified RPO is exceeded, click Send RPO alerts after... and then specify an RPO. For example, assume you set an RPO of 5 hours; a job starts at 1:00 PM and completes at 3:00 PM; a second job starts at 3:30 PM; if the second job does not complete by 6:00 PM, SyncIQ will create a OneFS event.</td>
</tr>
</tbody>
</table>

**Note**

This option is valid only if RPO alerts have been globally enabled through SyncIQ settings. The events have an event ID of 400040020.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Run jobs automatically every time that a change is made to the source directory. | a. Click Whenever the source is modified.  
b. To configure SyncIQ to wait a specified amount of time after the source directory is modified before starting a replication job, click Change-Triggered Sync Job Delay and then specify a delay. |
| Runs jobs automatically every time that a snapshot is taken of the source directory. | a. Click Whenever a snapshot of the source directory is taken.  
b. To only replicate only data contained in snapshots that match a specific naming pattern, type a snapshot naming pattern into the Run job if snapshot name matches the following pattern box.  
c. To replicate data contained in all snapshots that were taken of the source directory before the policy was created, click Sync existing snapshots before policy creation time. |

**After you finish**

The next step in the process of creating a replication policy is specifying source directories and files.

Specify source directories and files

You must specify the directories and files you want to replicate.

**Procedure**

1. In the Source Cluster area, in the Source Root Directory field, type the full path of the source directory that you want to replicate to the target cluster.
   
   You must specify a directory contained in /ifs. You cannot specify the /ifs/.snapshot directory or subdirectory of it.

2. (Optional) Prevent specific subdirectories of the source directory from being replicated.
   - To include a directory, in the Included Directories area, click Add a directory path.
   - To exclude a directory, in the Excluded Directories area, click Add a directory path.

3. (Optional) Prevent specific files from being replicated by specifying file matching criteria.
   a. In the File Matching Criteria area, select a filter type.
   b. Select an operator.
   c. Type a value.
   
   Files that do not meet the specified criteria will not be replicated to the target cluster. For example, if you specify File Type doesn't match .txt, SyncIQ will not replicate any files with the .txt file extension. If you specify Created after 08/14/2013, SyncIQ will not replicate any files created before August 14th, 2013. If you want to specify more than one file matching criterion, you can control how the criteria relate to each other by clicking either Add an "Or" condition or Add an "And" condition.
4. Specify which nodes you want the replication policy to connect to when the policy is run.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect the policy to all nodes in the source cluster.</td>
<td>Click Run the policy on all nodes in this cluster.</td>
</tr>
<tr>
<td>Connect the policy only to nodes contained in a specified subnet and pool.</td>
<td>a. Click Run the policy only on nodes in the specified subnet and pool.</td>
</tr>
<tr>
<td></td>
<td>b. From the Subnet and pool list, select the subnet and pool.</td>
</tr>
</tbody>
</table>

**Note**

SyncIQ does not support dynamically allocated IP address pools. If a replication job connects to a dynamically allocated IP address, SmartConnect might reassign the address while a replication job is running, which would disconnect the job and cause it to fail.

**After you finish**

The next step in the process of creating a replication policy is specifying the target directory.

**Specify the policy target directory**

You must specify a target cluster and directory to replicate data to.

**Procedure**

1. In the **Target Cluster** area, in the **Target Host** field, type one of the following:
   - The fully qualified domain name (FQDN) of any node in the target cluster.
   - The host name of any node in the target cluster.
   - The name of a SmartConnect zone in the target cluster.
   - The IPv4 or IPv6 address of any node in the target cluster.
   - localhost
     This will replicate data to another directory on the local cluster.

**Note**

SyncIQ does not support dynamically allocated IP address pools. If a replication job connects to a dynamically allocated IP address, SmartConnect might reassign the address while a replication job is running, which would disconnect the job and cause it to fail.

2. In the **Target Directory** field, type the absolute path of the directory on the target cluster that you want to replicate data to.
CAUTION

If you specify an existing directory on the target cluster, make sure that the directory is not the target of another replication policy. If this is a synchronization policy, make sure that the directory is empty. All files are deleted from the target of a synchronization policy the first time that the policy is run.

If the specified target directory does not already exist on the target cluster, the directory is created the first time that the job is run. We recommend that you do not specify the /ifs directory. If you specify the /ifs directory, the entire target cluster is set to a read-only state, which prevents you from storing any other data on the cluster.

If this is a copy policy, and files in the target directory share the same name as files in the source directory, the target directory files are overwritten when the job is run.

3. If you want replication jobs to connect only to the nodes included in the SmartConnect zone specified by the target cluster, click Connect only to the nodes within the target cluster SmartConnect Zone.

After you finish

The next step in the process of creating a replication policy is to specify policy target snapshot settings.

Configure policy target snapshot settings

You can optionally specify how archival snapshots are generated on the target cluster. You can access archival snapshots the same way that you access SnapshotIQ snapshots.

SyncIQ always retains one snapshot on the target cluster to facilitate failover, regardless of these settings.

Procedure

1. To create archival snapshots on the target cluster, in the Target Snapshots area, click Capture snapshots on the target cluster.

2. (Optional) To modify the default alias of the last snapshot created according to the replication policy, in the Snapshot Alias Name field, type a new alias.

   You can specify the alias name as a snapshot naming pattern. For example, the following naming pattern is valid:

   \%(PolicyName)\-on-\%(SrcCluster)\-latest

   The previous example produces names similar to the following:

   newPolicy-on-Cluster1-latest

3. (Optional) To modify the snapshot naming pattern for snapshots created according to the replication policy, in the Snapshot Naming Pattern field, type a naming pattern. Each snapshot generated for this replication policy is assigned a name based on this pattern.

   For example, the following naming pattern is valid:

   \%(PolicyName)\-from-\%(SrcCluster)\-at-%H: %M-on-%m-%d-%Y

   The example produces names similar to the following:

   newPolicy-from-Cluster1-at-10:30-on-7-12-2012
4. Select one of the following options:
   - Click **Snapshots do not expire**.
   - Click **Snapshots expire after**... and specify an expiration period.

**After you finish**

The next step in the process of creating a replication policy is configuring advanced policy settings.

**Configure advanced policy settings**

You can optionally configure advanced settings for a replication policy.

**Procedure**

1. (Optional) In the **Priority** field, specify whether the policy has priority.
   
   Selecting **Normal** will cause jobs created by the policy not to have priority. Selecting **High** will give priority to jobs created by the replication policy.

2. (Optional) From the **Log Level** list, select the level of logging you want SyncIQ to perform for replication jobs.
   
   The following log levels are valid, listed from least to most verbose:
   
   - Fatal
   - Error
   - Notice
   - Info
   - Copy
   - Debug
   - Trace

   Replication logs are typically used for debugging purposes. If necessary, you can log in to a node through the command-line interface and view the contents of the `/var/log/isi_migrate.log` file on the node.

   **Note**

   The recommended log level is **Notice**.

3. (Optional) If you want SyncIQ to perform a checksum on each file data packet that is affected by the replication policy, select the **Validate File Integrity** check box.
   
   If you enable this option, and the checksum values for a file data packet do not match, SyncIQ retransmits the affected packet.

4. (Optional) To increase the speed of failback for the policy, click **Prepare policy for accelerated failback performance**.
   
   Selecting this option causes SyncIQ to perform failback configuration tasks the next time that a job is run, rather than waiting to perform those tasks during the failback process. This will reduce the amount of time needed to perform failback operations when failback is initiated.

5. (Optional) To modify the length of time SyncIQ retains replication reports for the policy, in the **Keep Reports For** area, specify a length of time.
   
   After the specified expiration period has passed for a report, SyncIQ automatically deletes the report.
Some units of time are displayed differently when you view a report than how they were originally entered. Entering a number of days that is equal to a corresponding value in weeks, months, or years results in the larger unit of time being displayed. For example, if you enter a value of 7 days, 1 week appears for that report after it is created. This change occurs because SyncIQ internally records report retention times in seconds and then converts them into days, weeks, months, or years.

6. (Optional) Specify whether to record information about files that are deleted by replication jobs by selecting one of the following options:
   - Click Record when a synchronization deletes files or directories.
   - Click Do not record when a synchronization deletes files or directories.
   This option is applicable for synchronization policies only.

7. Specify how the policy replicates CloudPools SmartLink files.
   - If set to Deny, SyncIQ replicates all CloudPools SmartLink files to the target cluster as SmartLink files; if the target cluster does not support CloudPools, the job will fail. If set to Force, SyncIQ replicates all SmartLink files to the target cluster as regular files. If set to Allow, SyncIQ will attempt to replicate SmartLink files to the target cluster as SmartLink files; if the target cluster does not support CloudPools, SyncIQ will replicate the SmartLink files as regular files.

After you finish
The next step in the process of creating a replication policy is saving the replication policy settings.

Save replication policy settings
SyncIQ does not create replication jobs for a replication policy until you save the policy.

Before you begin
Review the current settings of the replication policy. If necessary, modify the policy settings.

Procedure
1. In the Create SyncIQ Policy dialog box, after all policy settings are as intended, click Create Policy.

Create a SyncIQ domain
You can create a SyncIQ domain to increase the speed at which failback is performed for a replication policy. Because you can fail back only synchronization policies, it is not necessary to create SyncIQ domains for copy policies.

Failing back a replication policy requires that a SyncIQ domain be created for the source directory. OneFS automatically creates a SyncIQ domain during the failback process. However, if you intend on failing back a replication policy, it is recommended that you create a SyncIQ domain for the source directory of the replication policy while the directory is empty. Creating a domain for a directory that contains less data takes less time.

Procedure
1. Click Cluster Management > Job Operations > Job Types.
2. In the Job Types area, in the DomainMark row, from the Actions column, select Start Job.
3. In the **Domain Root Path** field, type the path of a source directory of a replication policy.

4. From the **Type of domain** list, select **SyncIQ**.

5. Ensure that the **Delete domain** check box is cleared.

6. Click **Start Job**.

**Assess a replication policy**

Before running a replication policy for the first time, you can view statistics on the files that would be affected by the replication without transferring any files. This can be useful if you want to preview the size of the data set that will be transferred if you run the policy.

---

**Note**

You can assess only replication policies that have never been run before.

**Procedure**

1. Click **Data Protection** > **SyncIQ** > **Policies**.

2. In the **SyncIQ Policies** table, in the row of a replication policy, from the **Actions** column, select **Assess Sync**.

3. Click **Data Protection** > **SyncIQ** > **Summary**.

4. After the job completes, in the **SyncIQ Recent Reports** table, in the row of the replication job, click **View Details**.

   The report displays the total amount of data that would have been transferred in the **Total Data** field.

**Managing replication to remote clusters**

You can manually run, view, assess, pause, resume, cancel, resolve, and reset replication jobs that target other clusters.

After a policy job starts, you can pause the job to suspend replication activities. Afterwards, you can resume the job, continuing replication from the point where the job was interrupted. You can also cancel a running or paused replication job if you want to free the cluster resources allocated for the job. A paused job reserves cluster resources whether or not the resources are in use. A cancelled job releases its cluster resources and allows another replication job to consume those resources. No more than five running and paused replication jobs can exist on a cluster at a time. However, an unlimited number of canceled replication jobs can exist on a cluster. If a replication job remains paused for more than a week, SyncIQ automatically cancels the job.

**Start a replication job**

You can manually start a replication job for a replication policy at any time.

If you want to replicate data according to an existing snapshot, at the OneFS command prompt, run the `isi sync jobs start` command with the `--source-snapshot` option. You cannot replicate data according to snapshots generated by SyncIQ.

**Procedure**

1. Click **Data Protection** > **SyncIQ** > **Policies**.

2. In the **SyncIQ Policies** table, in the **Actions** column for a job, select **Start Job**.
Pause a replication job

You can pause a running replication job and then resume the job later. Pausing a replication job temporarily stops data from being replicated, but does not free the cluster resources replicating the data.

Procedure
1. Click Data Protection > SyncIQ > Summary.
2. In the Active Jobs table, in the Actions column for a job, click Pause Running Job.

Resume a replication job

You can resume a paused replication job.

Procedure
1. Click Data Protection > SyncIQ > Summary.
2. In the Currently Running table, in the Actions column for a job, click Resume Running Job.

Cancel a replication job

You can cancel a running or paused replication job. Cancelling a replication job stops data from being replicated and frees the cluster resources that were replicating data. You cannot resume a cancelled replication job. To restart replication, you must start the replication policy again.

Procedure
1. Click Data Protection > SyncIQ > Summary.
2. In the Active Jobs table, in the Actions column for a job, click Cancel Running Job.

View active replication jobs

You can view information about replication jobs that are currently running or paused.

Procedure
1. Click Data Protection > SyncIQ > Policies.
2. In the Active Jobs table, review information about active replication jobs.

Replication job information

You can view information about replication jobs through the Active Jobs table.

Status
The status of the job. The following job statuses are possible:

- Running
  The job is currently running without error.

- Paused
  The job has been temporarily paused.

Policy Name
The name of the associated replication policy.
Back up data with SyncIQ

**Started**
The time the job started.

**Elapsed**
How much time has elapsed since the job started.

**Transferred**
The number of files that have been transferred, and the total size of all transferred files.

**Source Directory**
The path of the source directory on the source cluster.

**Target Host**
The target directory on the target cluster.

**Actions**
Displays any job-related actions that you can perform.

### Managing replication policies
You can modify, view, enable, and disable replication policies.

#### Modify a replication policy
You can modify the settings of a replication policy.
If you modify any of the following policy settings after a policy runs, OneFS performs either a full or differential replication the next time the policy runs:
- Source directory
- Included or excluded directories
- File-criteria statement
- Target cluster
  - This applies only if you target a different cluster. If you modify the IP or domain name of a target cluster, and then modify the replication policy on the source cluster to match the new IP or domain name, a full replication is not performed.
- Target directory

**Procedure**
1. Click Data Protection > SyncIQ > Policies.
2. In the SyncIQ Policies table, in the row for a policy, click View/Edit.
3. In the View SyncIQ Policy Details dialog box, click Edit Policy.
4. Modify the settings of the replication policy, and then click Save Changes.

#### Delete a replication policy
You can delete a replication policy. After a policy is deleted, SyncIQ no longer creates replication jobs for the policy. Deleting a replication policy breaks the target association on the target cluster, and allows writes to the target directory.
If you want to temporarily suspend a replication policy from creating replication jobs, you can disable the policy, and then enable the policy again later.
Procedure

1. Click Data Protection > SyncIQ > Policies.
2. In the SyncIQ Policies table, in the row for a policy, select Delete Policy.
3. In the confirmation dialog box, click Delete.

Note

The operation will not succeed until SyncIQ can communicate with the target cluster; until then, the policy will not be removed from the SyncIQ Policies table. After the connection between the source cluster and target cluster is reestablished, SyncIQ will delete the policy the next time that the job is scheduled to run; if the policy is configured to run only manually, you must manually run the policy again. If SyncIQ is permanently unable to communicate with the target cluster, run the `isi sync policies delete` command with the `--local-only` option. This will delete the policy from the local cluster only and not break the target association on the target cluster. For more information, see the OneFS CLI Administration Guide.

Enable or disable a replication policy

You can temporarily suspend a replication policy from creating replication jobs, and then enable it again later.

Note

If you disable a replication policy while an associated replication job is running, the running job is not interrupted. However, the policy will not create another job until the policy is enabled.

Procedure

1. Click Data Protection > SyncIQ > Policies.
2. In the SyncIQ Policies table, in the row for a replication policy, select either Enable Policy or Disable Policy.

   If neither Enable Policy nor Disable Policy appears, verify that a replication job is not running for the policy. If an associated replication job is not running, ensure that the SyncIQ license is active on the cluster.

View replication policies

You can view information about replication policies.

Procedure

1. Click Data Protection > SyncIQ > Policies.
2. In the SyncIQ Policies table, review information about replication policies.

Replication policy information

You can view information about replication policies through the SyncIQ Policies table.

Policy Name
  The name of the policy.

State
  Whether the policy is enabled or disabled.
Last Known Good
When the last successful job ran.

Schedule
When the next job is scheduled to run. A value of Manual indicates that the job can be run only manually. A value of When source is modified indicates that the job will be run whenever changes are made to the source directory.

Source Directory
The path of the source directory on the source cluster.

Target Host : Directory
The IP address or fully qualified domain name of the target cluster and the full path of the target directory.

Actions
Any policy-related actions that you can perform.

Replication policy settings
You configure replication policies to run according to replication policy settings.

Policy name
The name of the policy.

Description
Describes the policy. For example, the description might explain the purpose or function of the policy.

Enabled
Determines whether the policy is enabled.

Action
Determines the how the policy replicates data. All policies copy files from the source directory to the target directory and update files in the target directory to match files on the source directory. The action determines how deleting a file on the source directory affects the target. The following values are valid:

Copy
If a file is deleted in the source directory, the file is not deleted in the target directory.

Synchronize
Deletes files in the target directory if they are no longer present on the source. This ensures that an exact replica of the source directory is maintained on the target cluster.

Run job
Determines whether jobs are run automatically according to a schedule or only when manually specified by a user.

Last Successful Run
Displays the last time that a replication job for the policy completed successfully.

Last Started
Displays the last time that the policy was run.
Source Root Directory
The full path of the source directory. Data is replicated from the source directory to the target directory.

Included Directories
Determines which directories are included in replication. If one or more directories are specified by this setting, any directories that are not specified are not replicated.

Excluded Directories
Determines which directories are excluded from replication. Any directories specified by this setting are not replicated.

File Matching Criteria
Determines which files are excluded from replication. Any files that do not meet the specified criteria are not replicated.

Restrict Source Nodes
Determines whether the policy can run on all nodes on the source cluster or run only on specific nodes.

Target Host
The IP address or fully qualified domain name of the target cluster.

Target Directory
The full path of the target directory. Data is replicated to the target directory from the source directory.

Restrict Target Nodes
Determines whether the policy can connect to all nodes on the target cluster or can connect only to specific nodes.

Capture Snapshots
Determines whether archival snapshots are generated on the target cluster.

Snapshot Alias Name
Specifies a snapshot alias for the latest archival snapshot taken on the target cluster.

Snapshot Naming Pattern
Specifies how archival snapshots are named on the target cluster.

Snapshot Expiration
Specifies how long archival snapshots are retained on the target cluster before they are automatically deleted by the system.

Workers Threads Per Node
Specifies the number of workers per node that are generated by OneFS to perform each replication job for the policy.

Log Level
Specifies the amount of information that is recorded for replication jobs. More verbose options include all information from less verbose options. The following list describes the log levels from least to most verbose:
- Fatal
- Error
Replication logs are typically used for debugging purposes. If necessary, you can log in to a node through the command-line interface and view the contents of the `/var/log/isi_migrate.log` file on the node.

**Note**

Notice is the recommended log level.

**Validate File Integrity**

Determines whether OneFS performs a checksum on each file data packet that is affected by a replication job. If a checksum value does not match, OneFS retransmits the affected file data packet.

**Keep Reports For**

Specifies how long replication reports are kept before they are automatically deleted by OneFS.

**Log Deletions on Synchronization**

Determines whether OneFS records when a synchronization job deletes files or directories on the target cluster.

The following replication policy fields are available only through the OneFS command-line interface.

**Source Subnet**

Specifies whether replication jobs connect to any nodes in the cluster or if jobs can connect only to nodes in a specified subnet.

**Source Pool**

Specifies whether replication jobs connect to any nodes in the cluster or if jobs can connect only to nodes in a specified pool.

**Password Set**

Specifies a password to access the target cluster.

**Report Max Count**

Specifies the maximum number of replication reports that are retained for this policy.

**Target Compare Initial Sync**

Determines whether full or differential replications are performed for this policy. Full or differential replications are performed the first time a policy is run and after a policy is reset.

**Source Snapshot Archive**

Determines whether snapshots generated for the replication policy on the source cluster are deleted when the next replication policy is run. Enabling archival source snapshots does not require you to activate the SnapshotIQ license on the cluster.
Source Snapshot Pattern
If snapshots generated for the replication policy on the source cluster are retained, renames snapshots according to the specified rename pattern.

Source Snapshot Expiration
If snapshots generated for the replication policy on the source cluster are retained, specifies an expiration period for the snapshots.

Restrict Target Network
Determines whether replication jobs connect only to nodes in a given SmartConnect zone. This setting applies only if the Target Host is specified as a SmartConnect zone.

Target Detect Modifications
Determines whether SyncIQ checks the target directory for modifications before replicating files. By default, SyncIQ always checks for modifications.

Note
Disabling this option could result in data loss. It is recommended that you consult Isilon Technical Support before disabling this option.

Resolve
Determines whether you can manually resolve the policy if a replication job encounters an error.

Managing replication to the local cluster
You can interrupt replication jobs that target the local cluster.
You can cancel a currently running job that targets the local cluster, or you can break the association between a policy and its specified target. Breaking a source and target cluster association causes SyncIQ to perform a full replication the next time the policy is run.

Cancel replication to the local cluster
You can cancel a replication job that is targeting the local clusters.

Procedure
1. Click Data Protection > SyncIQ > Local Targets.
2. In the SyncIQ Local Targets table, specify whether to cancel a specific replication job or all replication jobs targeting the local cluster.
   • To cancel a specific job, in the row for a replication job, select Cancel Running Job.
   • To cancel all jobs targeting the local cluster, select the check box to the left of Policy Name and then select Cancel Selection from the Select a bulk action list.
Break local target association

You can break the association between a replication policy and the local cluster. Breaking the target association allows writes to the target directory but also requires you to reset the replication policy before you can run the policy again.

**CAUTION**

After a replication policy is reset, SyncIQ performs a full or differential replication the next time the policy is run. Depending on the amount of data being replicated, a full or differential replication can take a very long time to complete.

**Procedure**

1. Click **Data Protection > SyncIQ > Local Targets**.
2. In the **SyncIQ Local Targets** table, in the row for a replication policy, select **Break Association**.
3. In the **Confirm** dialog box, click **Yes**.

View replication policies targeting the local cluster

You can view information about replication policies that are currently replicating data to the local cluster.

**Procedure**

1. Click **Data Protection > SyncIQ > Local Targets**.
2. In the **SyncIQ Local Targets** table, view information about replication policies.

Remote replication policy information

You can view information about replication policies that are currently targeting the local cluster.

The following information is displayed in the **SyncIQ Local Targets** table:

- **ID**
  - The ID of the replication policy.

- **Policy Name**
  - The name of the replication policy.

- **Source Host**
  - The name of the source cluster.

- **Source Cluster GUID**
  - The GUID of the source cluster.

- **Coordinator IP**
  - The IP address of the node on the source cluster that is acting as the job coordinator.

- **Updated**
  - The time when data about the policy or job was last collected from the source cluster.

- **Target Path**
  - The path of the target directory on the target cluster.
Managing replication performance rules

You can manage the impact of replication on cluster performance by creating rules that limit the network traffic created and the rate at which files are sent by replication jobs.

Create a network traffic rule

You can create a network traffic rule that limits the amount of network traffic that replication policies are allowed to generate during a specified time period.

Procedure

1. Click Data Protection > SyncIQ > Performance Rules.
2. Click Create a SyncIQ Performance Rule.
3. From the Rule Type list, select Bandwidth.
4. In the Limit field, specify the maximum number of kilobits per second that replication policies are allowed to send.
5. In the Schedule area, specify the time and days of the week that you want to apply the rule.
6. Click Create Performance Rule.

Create a file operations rule

You can create a file-operations rule that limits the number of files that replication jobs can send per second.

Procedure

1. Click Data Protection > SyncIQ > Performance Rules.
2. Click Create a SyncIQ Performance Rule.
3. From the Rule Type list, select Bandwidth.
4. In the Limit field, specify the maximum number of files per second that replication policies are allowed to send.
5. In the Schedule area, specify the time and days of the week that you want to apply the rule.
6. Click Create Performance Rule.

Modify a performance rule

You can modify a performance rule.

Procedure

1. Click Data Protection > SyncIQ > Performance Rules.
2. In the SyncIQ Performance Rules, in the row for the rule you want to modify, click View/Edit.
3. Click **Edit Performance Rule**.
4. Modify rule settings, and then click **Save Changes**.

**Delete a performance rule**

You can delete a performance rule.

**Procedure**
1. Click **Data Protection > SyncIQ > Performance Rules**.
2. In the **SyncIQ Performance Rules** table, in the row for the rule you want to delete, select **Delete Rule**.
3. In the **Confirm Delete** dialog box, click **Delete**.

**Enable or disable a performance rule**

You can disable a performance rule to temporarily prevent the rule from being enforced. You can also enable a performance rule after it has been disabled.

**Procedure**
1. Click **Data Protection > SyncIQ > Performance Rules**.
2. In the **SyncIQ Performance Rules** table, in the row for a rule you want to enable or disable, select either **Enable Rule** or **Disable Rule**.

**View performance rules**

You can view information about replication performance rules.

**Procedure**
1. Click **Data Protection > SyncIQ > Performance Rules**.
2. In the **SyncIQ Performance Rules** table, view information about performance rules.

**Managing replication reports**

In addition to viewing replication reports, you can configure how long reports are retained on the cluster. You can also delete any reports that have passed their expiration period.

**Configure default replication report settings**

You can configure the default amount of time that SyncIQ retains replication reports for. You can also configure the maximum number of reports that SyncIQ retains for each replication policy.

**Procedure**
1. Click **Data Protection > SyncIQ > Settings**.
2. In the **Report Settings** area, in the **Keep Reports For** area, specify how long you want to retain replication reports for.

   After the specified expiration period has passed for a report, SyncIQ automatically deletes the report.

   Some units of time are displayed differently when you view a report than how you originally enter them. Entering a number of days that is equal to a corresponding value in weeks, months, or years results in the larger unit of time being displayed. For example, if you enter a value of 7 days, 1 week appears for that report after it is...
created. This change occurs because SyncIQ internally records report retention times in seconds and then converts them into days, weeks, months, or years for display.

3. In the **Number of Reports to Keep Per Policy** field, type the maximum number of reports you want to retain at a time for a replication policy.

4. Click **Submit**.

## Delete replication reports

Replication reports are routinely deleted by SyncIQ after the expiration date for the reports has passed. SyncIQ also deletes reports after the number of reports exceeds the specified limit. Excess reports are periodically deleted by SyncIQ; however, you can manually delete all excess replication reports at any time. This procedure is available only through the command-line interface (CLI).

**Procedure**

1. Open a secure shell (SSH) connection to any node in the cluster, and log in.
2. Delete excess replication reports by running the following command:

   ```
   isi sync reports rotate
   ```

## View replication reports

You can view replication reports and subreports.

**Procedure**

1. Click **Data Protection** > **SyncIQ** > **Reports**.
2. In the **SyncIQ Reports** table, in the row for a report, click **View Details**.

   If a report is composed of subreports, the report is displayed as a folder. Subreports are displayed as files within report folders.

## Replication report information

You can view information about replication jobs through the **Reports** table.

**Policy Name**

The name of the associated policy for the job. You can view or edit settings for the policy by clicking the policy name.

**Status**

Displays the status of the job. The following job statuses are possible:

- **Running**
  
  The job is currently running without error.

- **Paused**
  
  The job has been temporarily paused.

- **Finished**
  
  The job completed successfully.

- **Failed**
  
  The job failed to complete.

- **Started**
  
  Indicates when the job started.
Ended
Indicates when the job ended.

Duration
Indicates how long the job took to complete.

Transferred
The total number of files that were transferred during the job run, and the total size of all transferred files. For assessed policies, Assessment appears.

Source Directory
The path of the source directory on the source cluster.

Target Host
The IP address or fully qualified domain name of the target cluster.

Action
Displays any report-related actions that you can perform.

Managing failed replication jobs
If a replication job fails due to an error, SyncIQ might disable the corresponding replication policy. For example, SyncIQ might disable a replication policy if the IP or hostname of the target cluster is modified. If a replication policy is disabled, the policy cannot be run.

To resume replication for a disabled policy, you must either fix the error that caused the policy to be disabled, or reset the replication policy. It is recommended that you attempt to fix the issue rather than reset the policy. If you believe you have fixed the error, you can return the replication policy to an enabled state by resolving the policy. You can then run the policy again to test whether the issue was fixed. If you are unable to fix the issue, you can reset the replication policy. However, resetting the policy causes a full or differential replication to be performed the next time the policy is run.

Note
Depending on the amount of data being synchronized or copied, full and differential replications can take a very long time to complete.

Resolve a replication policy
If SyncIQ disables a replication policy due to a replication error, and you fix the issue that caused the error, you can resolve the replication policy. Resolving a replication policy enables you to run the policy again. If you cannot resolve the issue that caused the error, you can reset the replication policy.

Procedure
1. Click Data Protection > SyncIQ > Policies.
2. In the Policies table, in the row for a policy, select Resolve.

Reset a replication policy
If a replication job encounters an error that you cannot resolve, you can reset the corresponding replication policy. Resetting a policy causes OneFS to perform a full or
Perform a full or differential replication

After you reset a replication policy, you must perform either a full or differential replication. You can do this only from the CLI.

Before you begin
Reset a replication policy.

Procedure
1. Open a secure shell (SSH) connection to any node in the cluster and log in through the root or compliance administrator account.
2. Specify the type of replication you want to perform by running the `isi sync policies modify` command.
   - To perform a full replication, disable the `--target-compare-initial-sync` option.
     For example, the following command disables differential synchronization for `newPolicy`:
     ```
     isi sync policies modify newPolicy --target-compare-initial-sync false
     ```
   - To perform a differential replication, enable the `--target-compare-initial-sync` option.
     For example, the following command enables differential synchronization for `newPolicy`:
     ```
     isi sync policies modify newPolicy --target-compare-initial-sync true
     ```
3. Run the policy by running the `isi sync jobs start` command.
   For example, the following command runs `newPolicy`:
   ```
   isi sync jobs start newPolicy
   ```

Managing changelists

You can create and view changelists that describe the differences between two snapshots. You can create a changelist for any two snapshots that have a common root directory.

Changelists are most commonly accessed by applications through the OneFS Platform API. For example, a custom application could regularly compare the two most recent
snapshots of a critical directory path to determine whether to back up the directory, or to trigger other actions.

Create a changelist

You can create a changelist to view the differences between two snapshots.

Procedure

1. (Optional) Record the IDs of the snapshots.
   a. Click Data Protection > SnapshotIQ > Snapshots.
   b. In the row of each snapshot that you want to create a changelist for, click View Details, and record the ID of the snapshot.
2. Click Cluster Management > Job Operations > Job Types.
3. In the Job Types area, in the ChangelistCreate row, from the Actions column, select Start Job.
4. In the Older Snapshot ID field, type the ID of the older snapshot.
5. In the Newer Snapshot ID field, type the ID of the newer snapshot.
6. Click Start Job.

View a changelist

You can view a changelist that describes the differences between two snapshots. This procedure is available only through the command-line interface (CLI).

Procedure

1. View the IDs of changelists by running the following command:

   `isi_changelist_mod -l`

   Changelist IDs include the IDs of both snapshots used to create the changelist. If OneFS is still in the process of creating a changelist, inprog is appended to the changelist ID.

2. (Optional) View all contents of a changelist by running the `isi_changelist_mod` command with the -a option.

   The following command displays the contents of a changelist named 2_6:

   `isi_changelist_mod -a 2_6`

Changelist information

You can view the information contained in changelists.

Note

The information contained in changelists is meant to be consumed by applications through the OneFS Platform API.

The following information is displayed for each item in the changelist when you run the `isi_changelist_mod` command:

- **st_ino**
  Displays the inode number of the specified item.
**st_mode**
Displays the file type and permissions for the specified item.

**st_size**
Displays the total size of the item in bytes.

**st_atime**
Displays the POSIX timestamp of when the item was last accessed.

**st_mtime**
Displays the POSIX timestamp of when the item was last modified.

**st_ctime**
Displays the POSIX timestamp of when the item was last changed.

**cl_flags**
Displays information about the item and what kinds of changes were made to the item.

01
The item was added or moved under the root directory of the snapshots.

02
The item was removed or moved out of the root directory of the snapshots.

04
The path of the item was changed without being removed from the root directory of the snapshot.

10
The item either currently contains or at one time contained Alternate Data Streams (ADS).

20
The item is an ADS.

40
The item has hardlinks.

---

**Note**
These values are added together in the output. For example, if an ADS was added, the code would be `cl_flags=021`.

**path**
The absolute path of the specified file or directory.
CHAPTER 5

Recovering data with SyncIQ

This section contains the following topics:

- Initiating data failover and failback with SyncIQ .................................................. 54
- Performing disaster recovery for SmartLock directories ............................................. 56
Initiating data failover and failback with SyncIQ

You can fail over from one Isilon cluster to another if, for example, a cluster becomes unavailable. You can then fail back to a primary cluster if the primary cluster becomes available again. You can revert failover if you decide that the failover was unnecessary, or if you failed over for testing purposes.

---

**Note**

Data failover and failback is not supported for compliance SmartLock directories. However, failover and failback are supported for enterprise SmartLock directories. Although you cannot fail over compliance SmartLock directories, you can recover compliance directories on a target cluster. Also, although you cannot fail back SmartLock compliance directories, you can migrate them back to the source cluster.

---

Fail over data to a secondary cluster

You can fail over to a secondary Isilon cluster if, for example, a cluster becomes unavailable.

**Before you begin**

Create and successfully run a replication policy.

---

**Note**

Data failover is not supported for compliance SmartLock directories. However, data failover is supported for enterprise SmartLock directories.

---

Complete the following procedure for each replication policy that you want to fail over.

**Procedure**

1. On the secondary Isilon cluster, click **Data Protection > SyncIQ > Local Targets**.
2. In the **SyncIQ Local Targets** table, in the row for a replication policy, from the **Actions** column, select **Allow Writes**.
3. On the primary cluster, modify the replication policy so that it is set to run only manually.

   This step will prevent the policy on the primary cluster from automatically running a replication job. If the policy on the primary cluster runs a replication job while writes are allowed to the target directory, the job will fail and the policy will be set to an unrunnable state. If this happens, modify the replication policy so that it is set to run only manually, resolve the policy, and complete the failback process. After you complete the failback process, you can modify the policy to run according to a schedule again.

**After you finish**

Direct clients to begin accessing the secondary cluster.

Revert a failover operation

Failover reversion undoes a failover operation on a secondary cluster, enabling you to replicate data from the primary cluster to the secondary cluster again. Failover reversion
is useful if the primary cluster becomes available before data is modified on the secondary cluster or if you failed over to a secondary cluster for testing purposes.

**Before you begin**

Fail over a replication policy.

Reverting a failover operation does not migrate modified data back to the primary cluster. To migrate data that clients have modified on the secondary cluster, you must fail back to the primary cluster.

---

**Note**

Failover reversion is not supported for SmartLock directories.

Complete the following procedure for each replication policy that you want to fail over.

**Procedure**

1. Run the `isi sync recovery allow-write` command with the `--revert` option.
   
   For example, the following command reverts a failover operation for `newPolicy`:
   
   ```
   isi sync recovery allow-write newPolicy --revert
   ```

---

### Fail back data to a primary cluster

After you fail over to a secondary cluster, you can fail back to the primary cluster.

**Before you begin**

Fail over by executing a replication policy.

---

**Note**

Data failback is not supported for compliance SmartLock directories. However, data failback is supported for enterprise SmartLock directories.

**Procedure**

1. On the primary cluster, click **Data Protection > SyncIQ > Policies**.

2. In the **SyncIQ Policies** table, in the row for a replication policy, from the **Actions** column, select **Resync-prep**.

   SyncIQ creates a mirror policy for each replication policy on the secondary cluster.

   SyncIQ names mirror policies according to the following pattern:

   ```
   <replication-policy-name>_mirror
   ```

3. On the secondary cluster, replicate data to the primary cluster by using the mirror policies.

   You can replicate data either by manually starting the mirror policies or by modifying the mirror policies and specifying a schedule.

4. Prevent clients from accessing the secondary cluster and then run each mirror policy again.

   To minimize impact to clients, it is recommended that you wait until client access is low before preventing client access to the cluster.
5. On the primary cluster, click Data Protection > SyncIQ > Local Targets.
6. In the SyncIQ Local Targets table, from the Actions column, select Allow Writes for each mirror policy.
7. On the secondary cluster, click Data Protection > SyncIQ > Policies.
8. In the SyncIQ Policies table, from the Actions column, select Resync-prep for each mirror policy.

After you finish
Redirect clients to begin accessing the primary cluster.

Performing disaster recovery for SmartLock directories
Although you cannot fail over or fail back compliance SmartLock directories, you can recover compliance directories on a target cluster and migrate them back to the source cluster.

Note
Data failover and failback is supported for SmartLock enterprise directories.

Recover SmartLock compliance directories on a target cluster
You can recover compliance SmartLock directories that you have replicated to a target cluster.

Before you begin
Create and successfully run a replication policy.
Complete the following procedure for each compliance SmartLock directory that you want to recover.

Procedure
1. On the target cluster, click Data Protection > SyncIQ > Local Targets.
2. In the SyncIQ Local Targets table, in the row of the replication policy, enable writes to the target directory of the policy.
   - If the last replication job completed successfully and a replication job is not currently running, select Allow Writes.
   - If a replication job is currently running, wait until the replication job completes, and then select Allow Writes.
   - If the primary cluster became unavailable while a replication job was running, select Break Association.
3. If you clicked Break Association, restore any files that are left in an inconsistent state.
   a. Delete all files that are not committed to a WORM state from the target directory.
   b. Copy all files from the failover snapshot to the target directory.
   Failover snapshots are named according to the following naming pattern:
   
   SIQ-Failover-<policy-name>-<year>-<month>-<day>_<hour>-<minute>-<second>

   Snapshots are stored in the /ifs/.snapshot directory.
4. If any SmartLock directory configuration settings, such as an autocommit time period, were specified for the source directory of the replication policy, apply those settings to the target directory.

Because autocommit information is not transferred to the target cluster, files that were scheduled to be committed to a WORM state on the source cluster will not be scheduled to be committed at the same time on the target cluster. To ensure that all files are retained for the appropriate time period, you can commit all files in target SmartLock directories to a WORM state.

For example, the following command automatically commits all files in /ifs/data/smartlock to a WORM state after one minute:

```
isi worm domains modify /ifs/data/smartlock --autocommit-offset 1m
```

**After you finish**

Redirect clients to begin accessing the target cluster.

---

**Migrate SmartLock compliance directories**

You might want to migrate compliance SmartLock directories if you restored the compliance directories on a target cluster and want to transfer those directories either back to the source cluster or to a new cluster.

**Procedure**

1. On a cluster, create a replication policy for each directory that you want to migrate.
   
   The policies must meet the following requirements:
   
   • The source directory is the SmartLock directory that you are migrating.
   
   • The target directory is an empty SmartLock directory. The source and target directories must be of the same SmartLock type. For example, if the target directory is a compliance directory, the source must also be a compliance directory.
   
   2. Replicate data to the target cluster by running the policies you created.
   
   You can replicate data either by manually starting the policies or by specifying a policy schedule.
   
   3. (Optional) To ensure that SmartLock protection is enforced for all files, commit all files in the SmartLock source directory to a WORM state.
   
   Because autocommit information is not transferred to the target cluster, files that were scheduled to be committed to a WORM state on the source cluster will not be scheduled to be committed at the same time on the target cluster. To ensure that all files are retained for the appropriate time period, you can commit all files in target SmartLock directories to a WORM state.
   
   For example, the following command automatically commits all files in /ifs/data/smartlock to a WORM state after one minute:
   
   ```
   isi worm domains modify /ifs/data/smartlock --autocommit-offset 1m
   ```
   
   This step is unnecessary if you have not configured an autocommit time period for the SmartLock directory being replicated.
   
   4. Prevent clients from accessing the source cluster and run the policy that you created.
To minimize impact to clients, it is recommended that you wait until client access is low before preventing client access to the cluster.

5. On the target cluster, click Data Protection > SyncIQ > Local Targets.

6. In the SyncIQ Local Targets table, in the row of each replication policy, from the Actions column, select Allow Writes.

7. (Optional) If any SmartLock directory configuration settings, such as an autocommit time period, were specified for the source directories of the replication policies, apply those settings to the target directories.

8. (Optional) Delete the copy of your SmartLock data on the source cluster.

   If the SmartLock directories are compliance directories or enterprise directories with the privileged delete functionality permanently disabled, you cannot recover the space consumed by the source SmartLock directories until all files are released from a WORM state. If you want to free the space before files are released from a WORM state, contact Isilon Technical Support for information about reformatting your cluster.
CHAPTER 6

NDMP backup

This section contains the following topics:

- NDMP two-way backup ................................................................. 60
- NDMP three-way backup ............................................................... 60
- Snapshot-based incremental backups .......................................... 61
- NDMP protocol support ................................................................. 62
- Supported DMAs ........................................................................... 63
- NDMP hardware support ............................................................... 63
- NDMP backup limitations ............................................................. 63
- NDMP performance recommendations ......................................... 64
- Excluding files and directories from NDMP backups .................. 65
NDMP two-way backup

The NDMP two-way backup is also known as the local or direct NDMP backup. To perform NDMP two-way backups, you must attach a Backup Accelerator node to your Isilon cluster and attach a tape device to the Backup Accelerator node. You must then use OneFS to detect the tape device before you can back up to that device.

You can connect supported tape devices directly to the Fibre Channel ports of a Backup Accelerator node. Alternatively, you can connect Fibre Channel switches to the Fibre Channel ports on the Backup Accelerator node, and connect tape and media changer devices to the Fibre Channel switches. For more information, see your Fibre Channel switch documentation about zoning the switch to allow communication between the Backup Accelerator node and the connected tape and media changer devices.

If you attach tape devices to a Backup Accelerator node, the cluster detects the devices when you start or restart the node or when you re-scan the Fibre Channel ports to discover devices. If a cluster detects tape devices, the cluster creates an entry for the path to each detected device.

If you connect a device through a Fibre Channel switch, multiple paths can exist for a single device. For example, if you connect a tape device to a Fibre Channel switch, and then connect the Fibre Channel switch to two Fibre Channel ports, OneFS creates two entries for the device, one for each path.

Note

If you perform an NDMP two-way backup operation, you must assign static IP addresses to the Backup Accelerator node. If you connect to the cluster through a data management application (DMA), you must connect to the IP address of a Backup Accelerator node. If you perform an NDMP three-way backup, you can connect to any node in the cluster.

NDMP three-way backup

The NDMP three-way backup is also known as the remote NDMP backup.

During a three-way NDMP backup operation, a data management application (DMA) on a backup server instructs the cluster to start backing up data to a tape media server that is either attached to the LAN or directly attached to the DMA. The NDMP service runs on one NDMP Server and the NDMP tape service runs on a separate server. Both the servers are connected to each other across the network boundary.

Setting preferred IPs for NDMP three-way operations

For performing NDMP three-way backup and restore operations in an environment with multiple network interfaces, you can configure preferred IP settings within a network interface and apply the settings to all the nodes in a cluster.

You can run the `isi ndmp settings variables` command with the appropriate options to set up the preferred IPs.
Configure preferred IP settings for NDMP three-way operations

You can configure preferred IP settings for NDMP three-way operations and apply the settings to all the nodes in a cluster.

Procedure

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Run the following command to specify a cluster-wide preferred IP setting:

   ```
   isi ndmp settings variables create --path=/CLUSTER --name=DATA_TX_IFS --value=<value>
   ```

   You must set `path` to `/CLUSTER` and `name` to `DATA_TX_IFS`. You can set `value` to a network interface name.

   For example, run the following command to configure all the nodes in a cluster to use the IPs within the network interface em1 as the preferred IPs:

   ```
   isi ndmp settings variables create --path=/CLUSTER --name=DATA_TX_IFS --value=em1
   ```

Snapshot-based incremental backups

You can implement snapshot-based incremental backups to increase the speed at which these backups are performed.

During a snapshot-based incremental backup, OneFS checks the snapshot taken for the previous NDMP backup operation and compares it to a new snapshot. OneFS then backs up all data that was modified since the last snapshot was made.

If the incremental backup does not involve snapshots, OneFS must scan the directory to discover which files were modified. OneFS can perform incremental backups significantly faster if snapshots are referenced.

You can perform incremental backups without activating a SnapshotIQ license on the cluster. Although SnapshotIQ offers a number of useful features, it does not enhance snapshot capabilities in NDMP backup and recovery.

**Note**

If you run an NDMP backup on a cluster with a SnapshotIQ license, the snapshot visibility must be turned on for SMB, NFS, and local clients for a successful completion of the operation.

Set the `BACKUP_MODE` environment variable to `SNAPSHOT` to enable snapshot-based incremental backups. If you enable snapshot-based incremental backups, OneFS retains each snapshot taken for NDMP backups until a new backup of the same or lower level is performed. However, if you do not enable snapshot-based incremental backups, OneFS automatically deletes each snapshot generated after the corresponding backup is completed or canceled.

After setting the `BACKUP_MODE` environment variable, snapshot-based incremental backup works with certain data management applications (DMAs) as listed in the next table.
Table 2 DMA support for snapshot-based incremental backups

<table>
<thead>
<tr>
<th>DMA</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec NetBackup</td>
<td>Yes</td>
</tr>
<tr>
<td>EMC Networker</td>
<td>Yes</td>
</tr>
<tr>
<td>EMC Avamar</td>
<td>Yes</td>
</tr>
<tr>
<td>Commvault Simpana</td>
<td>No</td>
</tr>
<tr>
<td>IBM Tivoli Storage Manager</td>
<td>No</td>
</tr>
<tr>
<td>Symantec Backup Exec</td>
<td>Yes</td>
</tr>
<tr>
<td>Dell NetVault</td>
<td>No</td>
</tr>
<tr>
<td>ASG-Time Navigator</td>
<td>No</td>
</tr>
</tbody>
</table>

**NDMP protocol support**

You can back up the EMC Isilon cluster data through version 3 or 4 of the NDMP protocol. OneFS supports the following features of NDMP versions 3 and 4:

- Full (level 0) NDMP backups
- Incremental (levels 1-9) NDMP backups and Incremental Forever (level 10)

**Note**

In a level 10 NDMP backup, only data changed since the most recent incremental (level 1-9) backup or the last level 10 backup is copied. By repeating level 10 backups, you can be assured that the latest versions of files in your data set are backed up without having to run a full backup.

- Token-based NDMP backups
- NDMP TAR backup type
- Dump backup type
- Path-based and dir/node file history format
- Direct Access Restore (DAR)
- Directory DAR (DDAR)
- Including and excluding specific files and directories from backup
- Backup of file attributes
- Backup of Access Control Lists (ACLs)
- Backup of Alternate Data Streams (ADSs)
- Backup Restartable Extension (BRE)

OneFS supports connecting to clusters through IPv4 or IPv6.
Supported DMAs

NDMP backups are coordinated by a data management application (DMA) that runs on a backup server. OneFS supports all the DMAs that are listed in the Isilon Third-Party Software and Hardware Compatibility Guide.

Note
All supported DMAs can connect to an EMC Isilon cluster through the IPv4 protocol. However, only some of the DMAs support the IPv6 protocol for connecting to an EMC Isilon cluster.

NDMP hardware support

OneFS can back up data to and recover data from tape devices and virtual tape libraries (VTLs).

Supported tape devices
See the OneFS and NDMP hardware compatibility section in the Isilon Third-Party Software and Hardware Compatibility Guide for a list of supported tape devices for two-way NDMP backups. For NDMP three-way backups, the data management application (DMA) determines the tape devices that are supported.

Supported tape libraries
For both the two-way and three-way NDMP backups, OneFS supports all of the tape libraries that are supported by the DMA.

Supported virtual tape libraries
See the OneFS and NDMP hardware compatibility section in the Isilon Third-Party Software and Hardware Compatibility Guide for a list of supported virtual tape libraries. For three-way NDMP backups, the DMA determines the virtual tape libraries that will be supported.

NDMP backup limitations

NDMP backups have the following limitations.

- Does not support more than 4 KB path length.
- Does not back up file system configuration data, such as file protection level policies and quotas.
- Does not back up tape blocks larger than 256 KB.
- Does not support recovering data from a file system other than OneFS. However, you can migrate data through the NDMP protocol from a NetApp or EMC VNX storage system to OneFS through the isi_vol_copy tools. For more information on these tools, see the OneFS Migration Tools Guide.
- Backup accelerator nodes cannot interact with more than 4096 tape paths.
NDMP performance recommendations

Consider the following recommendations to optimize OneFS NDMP backups.

General performance recommendations

- Install the latest patches for OneFS and your data management application (DMA).
- Run a maximum of eight NDMP concurrent sessions per A100 Backup Accelerator node and four NDMP concurrent sessions per Isilon IQ Backup Accelerator node to obtain optimal throughput per session.
- NDMP backups result in very high Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs). You can reduce your RPO and RTO by attaching one or more Backup Accelerator nodes to the cluster and then running two-way NDMP backups.
- The throughput for an Isilon cluster during the backup and recovery operations is dependent on the dataset and is considerably reduced for small files.
- If you are backing up large numbers of small files, set up a separate schedule for each directory.
- If you are performing NDMP three-way backups, run multiple NDMP sessions on multiple nodes in your Isilon cluster.
- Recover files through Direct Access Restore (DAR), especially if you recover files frequently. However, it is recommended that you do not use DAR to recover a full backup or a large number of files, as DAR is better suited to restoring smaller numbers of files.
- Recover files through Directory DAR (DDAR) if you recover large numbers of files frequently.
- Use the largest tape record size available for your version of OneFS to increase throughput.
- If possible, do not include or exclude files from backup. Including or excluding files can affect backup performance, due to filtering overhead.
- Limit the depth of nested subdirectories in your file system.
- Limit the number of files in a directory. Distribute files across multiple directories instead of including a large number of files in a single directory.

SmartConnect recommendations

- A two-way NDMP backup session with SmartConnect requires backup accelerators for backup and recovery operations. However, a three-way NDMP session with SmartConnect does not require backup accelerators for these operations.
- For a NDMP two-way backup session with SmartConnect, connect to the NDMP session through a dedicated SmartConnect zone consisting of a pool of Network Interface Cards (NICs) on the backup accelerator nodes.
- For a two-way NDMP backup session without SmartConnect, initiate the backup session through a static IP address or fully qualified domain name of the backup accelerator node.
- For a three-way NDMP backup operation, the front-end Ethernet network or the interfaces of the nodes are used to serve the backup traffic. Therefore, it is recommended that you configure a DMA to initiate an NDMP session only using the nodes that are not already overburdened serving other workloads or connections.
For a three-way NDMP backup operation with or without SmartConnect, initiate the backup session using the IP addresses of the nodes that are identified for running the NDMP sessions.

**Backup Accelerator recommendations**
- Assign static IP addresses to Backup Accelerator nodes.
- Attach more Backup Accelerator nodes to larger clusters. The recommended number of Backup Accelerator nodes is listed in the following table.

<table>
<thead>
<tr>
<th>Node type</th>
<th>Recommended number of nodes per Backup Accelerator node</th>
</tr>
</thead>
<tbody>
<tr>
<td>X-Series</td>
<td>3</td>
</tr>
<tr>
<td>NL-Series</td>
<td>3</td>
</tr>
<tr>
<td>S-Series</td>
<td>3</td>
</tr>
<tr>
<td>HD-Series</td>
<td>3</td>
</tr>
</tbody>
</table>

- Attach more Backup Accelerator nodes if you are backing up to more tape devices.

**DMA-specific recommendations**
- Enable parallelism for the DMA if the DMA supports this option. This allows OneFS to back up data to multiple tape devices at the same time.

### Excluding files and directories from NDMP backups

You can exclude files and directories from NDMP backup operations by specifying NDMP environment variables through a data management application (DMA). If you include a file or directory, all other files and directories are automatically excluded from backup operations. If you exclude a file or directory, all files and directories except the excluded one are backed up.

You can include or exclude files and directories by specifying the following character patterns. The examples given in the table are valid only if the backup path is `/ifs/data`.

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
<th>Example</th>
<th>Includes or excludes the following directories</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Takes the place of any character or characters</td>
<td>archive*</td>
<td>/ifs/archive1 src/archive42_a/media</td>
</tr>
<tr>
<td>[]</td>
<td>Takes the place of a range of letters or numbers</td>
<td>data_store_[a-f] data_store_[0-9]</td>
<td>/ifs/data/data_store_a /ifs/data/data_store_c /ifs/data/data_store_8</td>
</tr>
<tr>
<td>?</td>
<td>Takes the place of any single character</td>
<td>user_?</td>
<td>/ifs/data/user_1 /ifs/data/user_2</td>
</tr>
</tbody>
</table>
### Table 4 NDMP file and directory matching wildcards (continued)

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
<th>Example</th>
<th>Includes or excludes the following directories</th>
</tr>
</thead>
<tbody>
<tr>
<td>\</td>
<td>Includes a blank space</td>
<td>user\ 1</td>
<td>/ifs/data/user 1</td>
</tr>
<tr>
<td>//</td>
<td>Takes the place of a single slash (/)</td>
<td>ifs//data//archive</td>
<td>/ifs/data/archive</td>
</tr>
<tr>
<td>***</td>
<td>Takes the place of a single asterisk (*)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>..</td>
<td>Ignores the pattern if it is at the beginning of a path</td>
<td>../home/john</td>
<td>home/john</td>
</tr>
</tbody>
</table>

**Note**

" " are required for Symantec NetBackup when multiple patterns are specified. The patterns are not limited to directories.

Unanchored patterns such as `home` or `user1` target a string of text that might belong to many files or directories. If a pattern contains `/`, it is an anchored pattern. An anchored pattern is always matched from the beginning of a path. A pattern in the middle of a path is not matched. Anchored patterns target specific file pathnames, such as `ifs/data/home`. You can include or exclude either types of patterns.

If you specify both the include and exclude patterns, the include pattern is first processed followed by the exclude pattern.

If you specify both the include and exclude patterns, any excluded files or directories under the included directories would not be backed up. If the excluded directories are not found in any of the included directories, the exclude specification would have no effect.

**Note**

Specifying unanchored patterns can degrade the performance of backups. It is recommended that you avoid unanchored patterns whenever possible.
CHAPTER 7

Backing up and recovering data with NDMP

This section contains the following topics:

- **NDMP backup and recovery tasks** ............................................................. 68
- Configuring basic NDMP backup settings ..................................................... 68
- Managing NDMP user accounts ................................................................. 69
- Managing NDMP backup devices ............................................................... 70
- Managing NDMP backup ports ................................................................. 72
- Managing NDMP backup sessions .............................................................. 73
- Managing restartable backups .................................................................. 75
- Managing file list backups ....................................................................... 77
- NDMP restore operations ......................................................................... 79
- Sharing tape drives between clusters ......................................................... 80
- Managing default NDMP settings ............................................................. 81
- Managing snapshot based incremental backups ....................................... 85
- View NDMP backup logs ......................................................................... 86
- Configuring NDMP backups with EMC NetWorker ................................. 86
- Configuring NDMP backup with Symantec NetBackup ............................ 90
- Configuring NDMP backup with CommVault Simpana ............................ 94
- Configuring NDMP backup with IBM Tivoli Storage Manager ............... 97
NDMP backup and recovery tasks

Before you can back up data with NDMP, you must configure and enable NDMP backup on the cluster. After this, you can configure settings for NDMP backup ports and backup devices. After you start backing up data with NDMP, you can monitor backup sessions.

Configuring basic NDMP backup settings

You can configure NDMP backup settings to control how these backups are performed for the cluster. You can also configure OneFS to interact with a specific data management application (DMA) for NDMP backups.

NDMP backup settings

You can configure the following settings to control how NDMP backups are performed on the cluster.

- **Port number**
  The number of the port through which the data management application (DMA) can connect to the cluster.

- **DMA vendor**
  The DMA vendor that the cluster is configured to interact with.

View NDMP backup settings

You can view current NDMP backup settings. These settings define whether NDMP backup is enabled, the port through which your data management application (DMA) connects to the cluster, and the DMA vendor that OneFS is configured to interact with.

Procedure

1. Click **Data Protection > Backup > NDMP Settings** and view NDMP backup settings.
2. In the **Settings** area, review NDMP backup settings.

Configure and enable NDMP backup

OneFS prevents NDMP backups by default. Before you can perform NDMP backups, you must enable NDMP backups and configure NDMP settings.

Procedure

1. Click **Data Protection > Backup > NDMP Settings**.
2. In the **Service** area, click **Enable**.
3. (Optional) To specify a port through which data management applications (DMAs) access the cluster, or the DMA vendor that OneFS is to interact with, in the **Settings** area, click **Edit settings**.
   - In the **Port number** field, type a port number.
   - From the **DMA vendor** list, select the name of the DMA vendor to manage backup operations.
     If your DMA vendor is not included in the list, select **generic**. However, note that any vendors not included on the list are not officially supported and might not function as expected.
4. Add an NDMP user account through which your DMA can access the cluster.

Disable NDMP backup

You can disable NDMP backup if you no longer want to use this backup method.

Procedure
1. Click Data Protection > Backup > NDMP Settings.
2. In the Service area, click Disable.

Managing NDMP user accounts

You can create, delete, and modify the passwords of NDMP user accounts.

Create an NDMP user account

Before you can perform NDMP backups, you must create an NDMP user account through which your data management application (DMA) can access the Isilon cluster.

Procedure
1. Click Data Protection > Backup > NDMP Settings.
2. In the NDMP Administrators area, click Add administrator.
3. In the Add Administrator dialog box, in the Name field, type a name for the account.
4. In the Password and Confirm password fields, type a password for the account.
5. Click Submit.

View NDMP user accounts

You can view information about NDMP user accounts.

Procedure
1. Click Data Protection > Backup > NDMP Settings.
2. In the NDMP administrators area, review information about NDMP user accounts.

Modify the password of an NDMP user account

You can modify the password for an NDMP user account.

Procedure
1. Click Data Protection > Backup > NDMP Settings.
2. In the NDMP Administrator table, in the row for an NDMP user account, click Change password.
3. In the Password and Confirm password fields, type a new password for the account.
4. Click Submit.

Delete an NDMP user account

You can delete an NDMP user account.

Procedure
1. Click Data Protection > Backup > NDMP Settings.
2. In the NDMP Administrators table, in the row for an NDMP user account, click Delete.
3. In the Confirm dialog box, click Yes.

Managing NDMP backup devices

After you attach a tape or media changer device to a Backup Accelerator node, you must configure OneFS to detect and establish a connection to the device. After the connection between the cluster and the backup device is established, you can modify the name that the cluster has assigned to the device, or disconnect the device from the cluster.

NDMP backup device settings

OneFS creates a device entry for each device you attach to the cluster through a Backup Accelerator node.

The following table describes the settings available in the Tape Devices and Media Changers tables:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A device name assigned by OneFS.</td>
</tr>
<tr>
<td>State</td>
<td>Indicates whether the device is in use. If data is currently being backed up to or restored from the device, Read/Write appears. If the device is not in use, Closed appears.</td>
</tr>
<tr>
<td>WWN</td>
<td>The world wide node name (WWNN) of the device.</td>
</tr>
<tr>
<td>Product</td>
<td>The name of the device vendor and the model name or number of the device.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number of the device.</td>
</tr>
<tr>
<td>Paths</td>
<td>The name of the Backup Accelerator node that the device is attached to and the port number or numbers to which the device is connected.</td>
</tr>
<tr>
<td>LUN</td>
<td>The logical unit number (LUN) of the device.</td>
</tr>
<tr>
<td>Port ID</td>
<td>The port ID of the device that binds the logical device to the physical device.</td>
</tr>
<tr>
<td>WWPN</td>
<td>The world wide port name (WWPN) of the port on the tape or media changer device.</td>
</tr>
</tbody>
</table>

Detect NDMP backup devices

If you connect a tape device or media changer to a Backup Accelerator node, you must configure OneFS to detect the device. Only then can OneFS back up data to and restore data from the device. In OneFS, you can scan a specific node, a specific port, or all ports on all nodes.

Procedure

1. Click Data Protection ‹ Backup › Devices.
2. Click Discover devices.
3. (Optional) To scan only a specific node for NDMP devices, from the Nodes list, select a node.
4. (Optional) To scan only a specific port for NDMP devices, from the Ports list, select a port.
   If you specify a port and a node, only the specified port on the node is scanned. However, if you specify only a port, the specified port will be scanned on all nodes.

5. (Optional) To remove entries for devices or paths that have become inaccessible, select the Delete inaccessible paths or devices check box.

6. Click Submit.

Results
For each device that is detected, an entry is added to either the Tape Devices or Media Changers tables.

View NDMP backup devices
You can view information about tape and media changer devices that are currently attached to your Isilon cluster.

Procedure
1. Click Data Protection > Backup > Devices.
2. In the Tape Devices and Media Changers tables, review information about NDMP backup devices.

Modify the name of an NDMP backup device
You can modify the name of an NDMP backup device in OneFS.

Procedure
1. Click Data Protection > Backup > Devices.
2. In the Tape Devices table, click the name of a backup device entry.
3. In the Rename Device dialog box, in the Device Name field, type a new name for the backup device.
4. Click Submit.

Delete an entry for an NDMP backup device
If you physically remove an NDMP device from a cluster, OneFS retains the entry for the device. You can delete a device entry for a removed device. You can also remove the device entry for a device that is still physically attached to the cluster; this causes OneFS to disconnect from the device.

If you remove a device entry for a device that is connected to the cluster, and you do not physically disconnect the device, OneFS will detect the device the next time it scans the ports. You cannot remove a device entry for a device that is currently in use.

Procedure
1. Click Data Protection > Backup > Devices.
2. In the Tape Devices table, in the row for the target device, click Delete device.
3. In the Confirm dialog box, click Yes.
Managing NDMP backup ports

You can manage the Fibre Channel ports that connect tape and media changer devices to a Backup Accelerator node. You can also enable, disable, or modify the settings of an NDMP backup port.

NDMP backup port settings

OneFS assigns default settings to each port on each Backup Accelerator node attached to the cluster. These settings identify each port and specify how the port interacts with NDMP backup devices.

The settings that appear in the Ports table are as follows:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The name of the Backup Accelerator node, and the number of the port.</td>
</tr>
<tr>
<td>Topology</td>
<td>The type of Fibre Channel topology that the port is configured to support. Options are:</td>
</tr>
<tr>
<td></td>
<td>Point to Point</td>
</tr>
<tr>
<td></td>
<td>A single backup device or Fibre Channel switch directly connected to the port.</td>
</tr>
<tr>
<td></td>
<td>Loop</td>
</tr>
<tr>
<td></td>
<td>Multiple backup devices connected to a single port in a circular formation.</td>
</tr>
<tr>
<td></td>
<td>Auto</td>
</tr>
<tr>
<td></td>
<td>Automatically detects the topology of the connected device. This is the recommended setting, and is required if you are using a switched-fabric topology.</td>
</tr>
<tr>
<td>WWNN</td>
<td>The world wide node name (WWNN) of the port. This name is the same for each port on a given node.</td>
</tr>
<tr>
<td>WWPN</td>
<td>The world wide port name (WWPN) of the port. This name is unique to the port.</td>
</tr>
<tr>
<td>Rate</td>
<td>The rate at which data is sent through the port. The rate can be set to 1 Gb/s, 2 Gb/s, 4 Gb/s, 8 Gb/s, and Auto. 8 Gb/s is available for A100 nodes only. If set to Auto, OneFS automatically negotiates with the DMA to determine the rate. Auto is the recommended setting.</td>
</tr>
</tbody>
</table>

View NDMP backup ports

You can view information about Fibre Channel ports of Backup Accelerator nodes attached to a cluster.

Procedure

1. Click Data Protection > Backup > Ports.
2. In the **Ports** table, review information about NDMP backup ports.

### Modify NDMP backup port settings

You can modify the settings of an NDMP backup port.

**Procedure**
1. Click **Data Protection > Backup > Ports**.
2. In the **Sessions** table, click the name of a port.
3. In the **Edit Port** dialog box, modify port settings as needed, and then click **Submit**.

### Enable or disable an NDMP backup port

You can enable or disable an NDMP backup port.

**Procedure**
1. Click **Data Protection > Backup > Ports**.
2. In the **Ports** table, in the row of a port, click **Enable** or **Disable**.

### Managing NDMP backup sessions

You can view the status of NDMP backup sessions or terminate a session that is in progress.

### NDMP session information

You can view information about active NDMP sessions.

The following information is included in the **Sessions** table, as follows:

<table>
<thead>
<tr>
<th><strong>Table 7 NDMP session information</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Item</strong></td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>Session</td>
</tr>
<tr>
<td>Elapsed</td>
</tr>
<tr>
<td>Transferred</td>
</tr>
<tr>
<td>Throughput</td>
</tr>
<tr>
<td>Client/Remote</td>
</tr>
<tr>
<td>Mover/Data</td>
</tr>
</tbody>
</table>
Table 7 NDMP session information (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>is a component of OneFS that sends data during backups and receives information during restore operations. The following states might appear: <strong>Active</strong>  The data mover or data server is currently sending or receiving data. <strong>Paused</strong>  The data mover is temporarily unable to receive data. While the data mover is paused, the data server cannot send data to the data mover. The data server cannot be paused. <strong>Idle</strong>  The data mover or data server is not sending or receiving data. <strong>Listen</strong>  The data mover or data server is waiting to connect to the data server or data mover. <strong>Operation</strong>  The type of operation (backup or restore) that is currently in progress. If no operation is in progress, this field is blank. <strong>Backup (0-10)</strong>  Indicates that data is currently being backed up to a media server. The number indicates the level of NDMP backup. <strong>Restore</strong>  Indicates that data is currently being restored from a media server. <strong>Source/Destination</strong>  If an operation is currently in progress, specifies the /ifs directories that are affected by the operation. If a backup is in progress, displays the path of the source directory that is being backed up. If a restore operation is in progress, displays the path of the directory that is being restored along with the destination directory to which the tape media server is restoring data. If you are restoring data to the same location that you backed up your data from, the same path appears twice. <strong>Device</strong>  The name of the tape or media changer device that is communicating with the cluster. <strong>Mode</strong>  How OneFS is interacting with data on the backup media server, as follows: <strong>Read/Write</strong>  OneFS is reading and writing data during a backup operation. <strong>Read</strong>  OneFS is reading data during a restore operation.</td>
</tr>
</tbody>
</table>
### Table 7 NDMP session information (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Raw</td>
<td>The DMA has access to tape drives, but the drives do not contain writable tape media.</td>
</tr>
</tbody>
</table>

### View NDMP sessions

You can view information about active NDMP sessions.

**Procedure**

1. Click **Data Protection > Backup > Sessions**.
2. In the **Sessions** table, review information about NDMP sessions.

### End an NDMP session

You can end an NDMP backup or restore session at any time.

**Procedure**

1. Click **Data Protection > Backup > Sessions**.
2. In the **Sessions** table, in the row of the NDMP session that you want to end, click **Kill**.
3. In the **Confirm** dialog box, click **Yes**.

### Managing restartable backups

A restartable backup is a type of NDMP backup that you can enable in your data management application (DMA). If a restartable backup fails, for example, because of a power outage, you can restart the backup from a checkpoint close to the point of failure. In contrast, when a non-restartable backup fails, you must back up all data from the beginning, regardless of what was transferred during the initial backup process.

After you enable restartable backups from your DMA, you can manage restartable backup contexts from OneFS. These contexts are the data that OneFS stores to facilitate restartable backups. Each context represents a checkpoint that the restartable backup process can return to if a backup fails.

Restartable backups are supported only for EMC NetWorker 8.1 and later.

### Configure restartable backups for EMC NetWorker

You must configure EMC NetWorker to enable restartable backups and, optionally, define the checkpoint interval.

If you do not specify a checkpoint interval, NetWorker uses the default interval of 5 GB.

**Procedure**

1. Configure the client and the directory path that you want to back up as you would normally.
2. In the **Client Properties** dialog box, enable restartable backups.
   a. On the **General** page, click the **Checkpoint enabled** checkbox.
b. In the **Checkpoint granularity** drop-down list, select **File**.

3. In the **Application information** field, type any NDMP variables that you want to specify.

   The following variable setting specifies a checkpoint interval of 1 GB:
   
   ```
   CHECKPOINT_INTERVAL_IN_BYTES=1GB
   ```

4. Finish configuration and click **OK** in the **Client Properties** dialog box.

5. Start the backup.

6. If the backup is interrupted—for example, because of a power failure—restart it.

   a. On the **Monitoring** page, locate the backup process in the **Groups** list.

   b. Right-click the backup process and then, in the context menu, click **Restart**.

   NetWorker automatically restarts the backup from the last checkpoint.

---

**View restartable backup contexts**

You can view restartable backup contexts that have been configured.

**Procedure**

1. View all backup contexts by running the following command:

   ```
   isi ndmp extensions contexts list
   ```

2. To view detailed information about a specific backup context, run the **isi ndmp extensions contexts view** command.

   The following command displays detailed information about a backup context with an ID of 792eeb8a-8784-11e2-aa70-0025904e91a4:

   ```
   isi ndmp extensions contexts view 792eeb8a-8784-11e2-aa70-0025904e91a4
   ```

---

**Delete a restartable backup context**

After a restartable backup context is no longer needed, your data management application (DMA) automatically requests that OneFS delete the context. You can manually delete a restartable backup context before the DMA requests it.

**Note**

It is recommended that you do not manually delete restartable backup contexts. Manually deleting a restartable backup context requires you to restart the corresponding NDMP backup from the beginning.

**Procedure**

1. Run the **isi ndmp extensions contexts delete** command.

   The following command deletes a restartable backup context with an ID of 792eeb8a-8784-11e2-aa70-0025904e91a4:

   ```
   isi ndmp extensions contexts delete 792eeb8a-8784-11e2-aa70-0025904e91a4
   ```
Configure restartable backup settings

You can specify the number of restartable backup contexts that OneFS retains at a time, up to a maximum of 1024 contexts.

Procedure

1. Run the `isi ndmp extensions settings modify` command.

The following command sets the maximum number of restartable backup contexts to 128:

```bash
isi ndmp extensions settings modify --bre_max_contexts 128
```

View restartable backup settings

You can view the current limit of restartable backup contexts that OneFS retains at one time.

Procedure

1. Run the following command:

```bash
isi ndmp extensions settings view
```

Managing file list backups

If your data management application (DMA) can pass environment variables to OneFS, you can control backups by specifying a file list.

Currently, EMC Networker and Symantec NetBackup can pass environment variables to OneFS.

With a normal NDMP level 0 (full) backup, your DMA backs up an entire source directory. With an NDMP incremental (level 1-10) backup, your DMA backs up only those files that have been created or changed since the previous incremental backup of the same level.

When you specify a file list backup, only the listed files and subdirectories in the source directory are backed up. With a level 0 file list backup, all listed files and directories in the source directory are backed up.

A backup level other than 0 triggers an incremental file list backup. In an incremental file list backup, only the listed files that were created or changed in the source directory since the last incremental backup of the same level are backed up.

To configure a file list backup, you must complete the following tasks:

- Create the file list and place it in OneFS
- Specify the path of the source directory
- Specify the file list location

The file list is an ASCII text file that lists the pathnames of files to be backed up. The pathnames must be relative to the path specified in the `FILESYSTEM` environment variable. Absolute file paths in the file list are not supported. The pathnames of all files must be included, or they are not backed up. For example, if you include the pathname of a subdirectory, only the subdirectory, not the files it contains, is backed up.
To specify the full path of the source directory to be backed up, you must specify the FILESYSTEM environment variable in your DMA. For example:

```bash
FILESYSTEM=/ifs/data/projects
```

To specify the pathname of the file list, you must specify the environment variable, BACKUP_FILE_LIST in your DMA. The file list must be accessible from the node performing the backup. For example:

```bash
BACKUP_FILE_LIST=/ifs/data/proj_list.txt
```

## Format of a backup file list

You must create a file list to enable a file list backup. A file list backup requires an ASCII text file in a particular format to identify the pathnames of files to be backed up. Following is an example of a file list with pathnames relative to `/ifs/data/projects`:

```plaintext
proj001/plan/\001File
proj001/plan/\002File
proj001/plan/\003File
proj001/plan/\004File
proj001/plan/\005File
proj001/plan/\006File
proj001/plan/\007File
proj001/plan/\008File
proj001/plan/\009File
proj001/plan/\010File
proj001/plan/\011File
proj001/plan/\012File
proj001/plan/\013File
proj001/plan/\014File
proj001/plan/\015File
proj002/plan/\016File
proj002/plan/\017File
proj002/plan/\018File
proj002/plan/\019File
proj002/plan/\020File
proj002/plan/\021File
proj002/plan/\022File
proj002/plan/\023File
proj002/plan/\024File
proj005/plan/\036File
proj005/plan/\037File
proj005/plan/ File
proj005/plan/!File
proj005/plan/"File
proj005/plan/#File
proj005/plan/$File
proj005/plan/%File
proj005/plan/&File
proj005/plan/'File
```

As shown in the example, the pathnames are relative to the full path of the source directory, which you specify in the FILESYSTEM environment variable. Absolute file paths are not supported in the file list.

Also as shown, the directories and files must be in sorted order for the backup to be successful. A # at the beginning of a line in the file list indicates to skip the line.

The pathnames of all files must be included in the file list, or they are not backed up. For example, if you only include the pathname of a subdirectory, the subdirectory is backed up, but not the files the subdirectory contains. The exception is ADS (alternate data streams). All ADS associated with a file to be backed up are automatically backed up.
Placement of the file list

Before you can perform a file list backup, you must place the file list in OneFS. For example, suppose the FILESYSTEM environment variable specifies the full path of the directory to be backed up as /ifs/data/projects. You can place the text file containing the file list anywhere within the /ifs path.

Start a file list backup

You can configure and start a file list backup from your data management application (DMA).

Before you begin

You should have already specified and saved the list of files to be backed up in an ASCII text file.

Configure a file list backup from your DMA as you would any backup, but with a few additional steps as described in the following procedure.

Procedure

1. Copy the file list to the OneFS file system on the EMC Isilon cluster containing the files to be backed up.
   For example, if the directory that you specify in the FILESYSTEM environment variable is /ifs/data/projects, you could place your file list at /ifs/data.

2. In your DMA, specify the BACKUP_FILE_LIST environment variable to be the full pathname of the file list that resides on the EMC Isilon cluster.
   For example, if the file list was named proj_backup.txt, and you placed it at /ifs/data, specify /ifs/data/proj_backup.txt as the full pathname of the file list.

3. Start your backup as you normally would.

Results

The files in your file list are backed up as specified.

NDMP restore operations

NDMP supports the following types of restore operations:

- Parallel restore (multi-threaded process)
- Serial restore (single-threaded process)

NDMP parallel restore operation

Parallel (multi-threaded) restore enables faster full or partial restore operations by writing data to the cluster as fast as the data can be read from the tape. Parallel restore is the default restore mechanism in OneFS.

You can restore multiple files concurrently through the parallel restore mechanism.
NDMP serial restore operation

For troubleshooting or for other purposes, you can run a serial restore operation which uses fewer system resources. The serial restore operation runs as a single-threaded process and restores one file at a time to the specified path.

Specify a serial restore operation

You can use the RESTORE_OPTIONS environment variable to specify a serial (single-threaded) restore operation.

Procedure

1. In your data management application, configure a restore operation as you normally would.
2. Make sure that the RESTORE_OPTIONS environment variable is set to 1 on your data management application.

   If the RESTORE_OPTIONS environment variable is not already set to 1, specify the isi ndmp settings variables modify command from the OneFS command line. The following command specifies serial restore for the /ifs/data/projects directory:

   ```bash
   isi ndmp settings variables modify --path /ifs/data/projects --name restore_options --value 1
   ```

   The value of the path option is the FILESYSTEM environment variable set during the backup operation. The value that you specify for the name option is case sensitive.
3. Start the restore operation.

Sharing tape drives between clusters

Multiple Isilon clusters, or an Isilon cluster and a third-party NAS system, can be configured to share a single tape drive. This helps to maximize the use of the tape infrastructure in your data center.

In your data management application (DMA), you must configure NDMP to control the tape drive and ensure that it is shared properly. The following configurations are supported.

<table>
<thead>
<tr>
<th>OneFS Versions</th>
<th>Supported DMAs</th>
<th>Tested configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 7.1.1</td>
<td>• EMC NetWorker 8.0 and later</td>
<td>• Isilon Backup Accelerator with a second Backup Accelerator</td>
</tr>
<tr>
<td>• 7.1.0.1 (and later)*</td>
<td>• Symantec NetBackup 7.5 and later</td>
<td>• Isilon Backup Accelerator with a NetApp storage system</td>
</tr>
<tr>
<td>• 7.0.2.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 6.6.5.26</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* The tape drive sharing function is not supported in the OneFS 7.0.1 release.

EMC NetWorker refers to the tape drive sharing capability as DDS (dynamic drive sharing). Symantec NetBackup uses the term SSO (shared storage option). Consult your DMA vendor documentation for configuration instructions.
Managing default NDMP settings

In OneFS, you can manage NDMP backup and restore operations by specifying default NDMP environment variables. You can also override default NDMP environment variables through your data management application (DMA). For more information about specifying NDMP environment variables through your DMA, see your DMA documentation.

Set default NDMP settings for a directory

You can set default NDMP settings for a directory.

Procedure

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Set default NDMP settings by running the `isi ndmp settings variables create` command.

   For example, the following command enables snapshot-based incremental backups for `/ifs/data/media`:

   ```bash
   isi ndmp settings variables create /ifs/data/media BACKUP_MODE SNAPSHOT
   ```

Modify default NDMP settings for a directory

You can modify the default NDMP settings for a directory.

Procedure

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Modify default NDMP settings by running the `isi ndmp settings variables modify` command.

   For example, the following command sets the default file history format to path-based format for `/ifs/data/media`:

   ```bash
   isi ndmp settings variables modify /ifs/data/media HIST F
   ```
3. (Optional) To remove a default NDMP setting for a directory, run the `isi ndmp settings variables delete` command:

   For example, the following command removes the default file history format for `/ifs/data/media`:

   ```bash
   isi ndmp settings variables delete /ifs/data/media --name HIST
   ```

View default NDMP settings for directories

You can view the default NDMP settings for directories.

Procedure

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. View default NDMP settings by running the following command:

   ```bash
   isi ndmp settings variables list
   ```
## NDMP environment variables

You can specify default settings of NDMP backup and restore operations through NDMP environment variables. You can also specify NDMP environment variables through your data management application (DMA).

### Table 8 NDMP environment variables

<table>
<thead>
<tr>
<th>Environment variable</th>
<th>Valid values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BACKUP_MODE=</td>
<td>TIMESTAMP, SNAPSHOT</td>
<td>TIMESTAMP</td>
<td>Enables or disables snapshot-based incremental backups. To enable snapshot-based incremental backups, specify SNAPSHOT. To disable snapshot-based incremental backups, specify TIMESTAMP.</td>
</tr>
<tr>
<td>FILESYSTEM=</td>
<td>&lt;file-path&gt;</td>
<td>None</td>
<td>Specifies the full path of the directory you want to back up. Must be specified by the DMA before starting the backup, or an error is generated.</td>
</tr>
<tr>
<td>LEVEL=</td>
<td>&lt;integer&gt;</td>
<td>0</td>
<td>Specifies the level of NDMP backup to perform. The following values are valid:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - 9</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>UPDATE=</td>
<td>Y, N</td>
<td>Y</td>
<td>Determines whether OneFS updates the dump dates file.</td>
</tr>
<tr>
<td></td>
<td>Y</td>
<td>OneFS updates the dump dates file.</td>
<td></td>
</tr>
<tr>
<td>Environment variable</td>
<td>Valid values</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>N</td>
<td>OneFS does not update the dump dates file.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIST=</td>
<td>&lt;file-history-format&gt;</td>
<td>Y</td>
<td>Specifies the file history format. The following values are valid:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>D</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specifies dir/node file history.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>F</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specifies path-based file history.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specifies the default file history format determined by your NDMP backup settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>N</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Disables file history.</td>
</tr>
<tr>
<td>DIRECT=</td>
<td>Y</td>
<td>N</td>
<td>Enables or disables Direct Access Restore (DAR) and Directory DAR (DDAR). The following values are valid:</td>
</tr>
<tr>
<td></td>
<td>N</td>
<td></td>
<td>Enables DAR and DDAR.</td>
</tr>
<tr>
<td></td>
<td>N</td>
<td></td>
<td>Disables DAR and DDAR.</td>
</tr>
<tr>
<td>FILES=</td>
<td>&lt;file-matching-pattern&gt;</td>
<td>None</td>
<td>If you specify this option, OneFS backs up only files and directories that meet the specified pattern. Separate multiple patterns with a space.</td>
</tr>
<tr>
<td>EXCLUDE=</td>
<td>&lt;file-matching-pattern&gt;</td>
<td>None</td>
<td>If you specify this option, OneFS does not back up files and directories that</td>
</tr>
</tbody>
</table>
Table 8 NDMP environment variables (continued)

<table>
<thead>
<tr>
<th>Environment variable</th>
<th>Valid values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>
| RESTORE_HARDLINK_BY_TABLE                  | Y, N         | N       | Determines whether OneFS recovers hard links by building a hard-link table during restore operations. Specify this option if hard links were incorrectly backed up, and restore operations are failing. If a restore operation fails because hard links were incorrectly backed up, the following message appears in the NDMP backup logs: 

Bad hardlink path for <path> |

| BACKUP_FILE_LIST=                          | <file-path>  | None    | Specifies the pathname in OneFS of the file list to control the backup. This variable must be passed from the DMA initiating the backup. Currently, only EMC Networker and Symantec NetBackup can pass environment variables to OneFS. |
| RESTORE_OPTIONS=                           | 0, 1         | 0       | The restore operation, by default, is multi-threaded to improve performance. To change the restore operation to single-threaded, specify RESTORE_OPTIONS=1 |
Managing snapshot based incremental backups

After you enable snapshot-based incremental backups, you can view and delete the snapshots created for these backups.

Enable snapshot-based incremental backups for a directory

You can configure OneFS to perform snapshot-based incremental backups for a directory by default. You can also override the default setting in your data management application (DMA).

Procedure

1. Run the `isi ndmp settings variable create` command.

   The following command enables snapshot-based incremental backups for `/ifs/data/media`:

   ```
   isi ndmp settings variables create /ifs/data/media BACKUP_MODE SNAPSHOT
   ```

View snapshots for snapshot-based incremental backups

You can view snapshots generated for snapshot-based incremental backups.

Procedure

1. Run the following command:

   ```
   isi ndmp dumpdates list
   ```

Delete snapshots for snapshot-based incremental backups

You can delete snapshots created for snapshot-based incremental backups.

Note

It is recommended that you do not delete snapshots created for snapshot-based incremental backups. If all snapshots are deleted for a path, the next backup performed for the path is a full backup.

Procedure

1. Run the `isi ndmp dumpdates delete` command.

   The following command deletes all snapshots created for backing up `/ifs/data/media`:

   ```
   isi ndmp dumpdates delete /ifs/data/media
   ```
View NDMP backup logs

You can view information about NDMP backup and restore operations through NDMP backup logs.

Procedure

1. Click Data Protection > Backup > Logs.
2. In the Log Location area, from the Node list, select a node.
3. In the Log Contents area, review information about NDMP backup and restore operations.

Configuring NDMP backups with EMC NetWorker

You can configure OneFS and EMC NetWorker to backup data stored on an Isilon cluster. The following procedures explain how to configure NDMP backup with EMC NetWorker.

Note

The steps described in the procedures are general guidelines only. They might change for different versions of EMC NetWorker. Consult your DMA vendor documentation for the configuration information for a specific version of EMC NetWorker.

Create a group

With EMC NetWorker, you must configure a group to manage backups from an Isilon cluster.

Procedure

1. Connect to the NetWorker server from the NetWorker Management Console Server.
2. Click Configuration.
3. Right-click Groups and then click New.
4. In the Name field, type a name for the group.
5. Click OK.

Scan for tape devices

With EMC NetWorker, you must detect tape devices for backup and restore operations.

Procedure

1. Connect to the NetWorker server from the NetWorker Management Console Server.
2. Click Devices.
3. Right-click Libraries, and then click Scan for Devices.
4. Ensure that no existing storage nodes are selected.
5. Click Create a new Storage Node.
6. Configure the following settings:
Configure a library

With EMC NetWorker, you must configure the tape library that contains the tape devices for backup and recovery operations.

Procedure
1. Connect to the NetWorker server from the NetWorker Management Console Server.
2. Click Devices.
3. Right-click Libraries and then click Refresh.
   - The system displays a list of tape libraries that are currently attached to the Isilon cluster.
4. Right-click the name of the tape library you want to configure and then click Configure Library.
5. In the Configure Library window, click Check All.
6. Click Start Configuration.

Create a data media pool

With EMC NetWorker, you must create a media pool that specifies the type of backups you want to perform and the tape devices you want to use.

Procedure
1. Connect to the NetWorker server from the NetWorker Management Console Server.
2. Click Media.
3. Click Media Pools.
4. In the Media Pools area, right-click and then click New.
5. Configure the following settings:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Setting name</th>
<th>Setting value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic</td>
<td>Name</td>
<td>A name for the media pool</td>
</tr>
<tr>
<td></td>
<td>Enabled</td>
<td>Selected</td>
</tr>
<tr>
<td></td>
<td>Groups</td>
<td>The group that you created for the Isilon cluster</td>
</tr>
<tr>
<td>Selection Criteria</td>
<td>Levels</td>
<td>Select 1-9, full, and incremental</td>
</tr>
<tr>
<td></td>
<td>Devices</td>
<td>Each tape device that you want to use</td>
</tr>
</tbody>
</table>
Label tape devices

With EMC NetWorker, you must label tape devices attached to an Isilon cluster before you can back up data to these devices.

**Procedure**

1. Connect to the NetWorker server from the NetWorker Management Console Server.
2. Click **Devices**.
3. Click the name of the library that you configured.
4. In the device list, highlight all tape drives you want to label.
5. Right-click on the highlighted list, and then click **Label**.
6. In the **Label Library Media** window, from the **Target Media Pool** list, select the name of the media pool you created.
7. Ensure that the **Prompt to Overwrite Existing Label** box is cleared.
8. Click OK.

Create a metadata media pool

With EMC NetWorker, you must create a media pool for the metadata you want to back up from an Isilon cluster.

**Procedure**

1. On your local machine, create a directory to contain your metadata.
2. Connect to the NetWorker server from the NetWorker Management Console Server.
3. Configure a new media pool device.
   a. Click **Devices**.
   b. Right-click **Devices** and then click **New**.
   c. Configure the following settings:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Setting Name</th>
<th>Setting Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Name</td>
<td>A name for the metadata device</td>
</tr>
<tr>
<td></td>
<td>Media Type</td>
<td>file</td>
</tr>
</tbody>
</table>

   d. Click OK.
4. Right-click the name of the device and then click **Label**.
5. In the **Label** window, click OK.
6. Configure a new media pool.
   a. Click **Media**.
b. Right-click Media Pools and then click New.

c. Configure the following settings:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Setting name</th>
<th>Setting value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic</td>
<td>Name</td>
<td>A name for the metadata media pool</td>
</tr>
<tr>
<td></td>
<td>Enabled</td>
<td>Selected</td>
</tr>
<tr>
<td></td>
<td>Groups</td>
<td>The group that you created for the Isilon cluster</td>
</tr>
<tr>
<td></td>
<td>Label template</td>
<td>Default</td>
</tr>
<tr>
<td>Selection Criteria</td>
<td>Save sets</td>
<td>Type the following text:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>bootstrap</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Index:</td>
</tr>
<tr>
<td></td>
<td>Devices</td>
<td>The name of the metadata device</td>
</tr>
</tbody>
</table>

d. Click OK.

Create a client

With EMC NetWorker, you must create a client that specifies the data to be backed up from an Isilon cluster.

Procedure

1. Connect to the NetWorker server from the NetWorker Management Console Server.
2. Configure the new client.
   a. Click Configuration.
   b. Click the name of the group you created.
   c. In the right pane, right-click and then click New.
   d. In the Create Client window, in the Name field, type a name for the client.
3. In the Save set field, type the full path of the directory that you want to back up.
4. From the Pool list, select the name of the data media pool you created.
5. Configure the remote user.
   a. Click Apps & Modules.
   b. In the Remote user field, type the name of an NDMP user you configured on the cluster.
   c. In the Password field, type the password of the NDMP user.
6. Select NDMP, and in the Backup command field, type the backup command.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>With DSA</td>
<td>nsrcdmp_save -T -M tar</td>
</tr>
<tr>
<td>Without DSA</td>
<td>nsrcdmp_save -T tar</td>
</tr>
</tbody>
</table>
7. In the **Application information** field, type any NDMP environment variables that you want to specify.

The following text enables directory-based file history and direct access restores (DAR):

```
DIRECT=Y
HIST=F
```

For a complete list of available options, see NDMP environment variables.

8. Click **Globals (1 of 2)**.

9. In the **Parallelism** field, specify the client parallelism value.
   - If you are not using the Data Service Agent (DSA) feature, specify 1.
   - If you are using the Data Service Agent (DSA) feature, specify a value based on your cluster configuration. For more information about client parallelism values, see the *EMC NetWorker Administration Guide*.

10. In the **Aliases** field, specify the short and fully qualified domain name of the Isilon node that you want to backup data from.

11. Click **Globals (2 of 2)**

12. In the **Storage nodes** field, specify the storage node.
   - If you are using the DSA feature, type `nsrserverhost` and then press ENTER.
   - If you are not using the DSA feature and performing a two-way NDMP backup, type the hostname of the Isilon node you want to backup data from.
   - If you are not using the DSA feature and performing a three-way NDMP backup, type the hostname of the tape server. You can specify multiple tape servers by specifying each tape server on a separate line.

13. In the **Remote access** field, type the name of a user on the Isilon cluster.
   - If the cluster has not been upgraded to SmartLock compliance mode, type `root@<cluster-host-name>`.
   - If the cluster has been upgraded to SmartLock compliance mode, type `compadmin@<cluster-host-name>`.

---

### Configuring NDMP backup with Symantec NetBackup

You can configure OneFS and Symantec NetBackup to backup data stored on an Isilon cluster. The following procedures explain how to configure NDMP backup with Symantec NetBackup.

**Note**

The steps described in the procedures are general guidelines only. They might change for different versions of Symantec NetBackup. Consult your DMA vendor documentation for the configuration information for a specific version of Symantec NetBackup.
Add an NDMP host

You must add an Isilon cluster as an NDMP host before you can back up data with Symantec NetBackup.

Before you begin

Create an NDMP user account.

Procedure

1. In the NetBackup Administration Console, expand Media and Device Management.
2. Under Media and Device Management, expand Credentials, and then click NDMP Hosts.
3. Click Actions > New > NDMP Host.
4. In the NDMP Host Name dialog box, specify the cluster that you want to back up data from.
   - If you have a single Backup Accelerator node in the cluster, type the fully qualified domain name, host name, and the IPv4 or IPv6 address of the Backup Accelerator node.
   - If you have multiple Backup Accelerator nodes in the cluster, type the name of a SmartConnect zone that contains only the Backup Accelerator nodes.
   - If you are performing a three-way NDMP backup, type the fully qualified domain name (FQDN), host name, SmartConnect zone, and the IPv4 or IPv6 address of any node in the cluster.
5. Click OK.
6. In the Add NDMP Host box, click Use the following credentials for this NDMP host on all media servers.
7. In the Username and Password fields, type the user name and password of an NDMP user on the cluster.
8. Click OK.

Configure storage devices

If you are backing up data to tape devices connected to one or more Backup Accelerator nodes, you must configure Symantec NetBackup to recognize those storage devices. This procedure is required only if you are performing a two-way NDMP backup.

Procedure

1. In the NetBackup Administration Console, click Media and Device Management.
2. Click Configure Storage Devices.
   - The Device Configuration Wizard appears.
3. Click Next.
4. Scan the cluster for attached NDMP devices.
   b. Select NDMP Host, and then click OK.
   c. Click Next.
   d. Select the NDMP host you created earlier, and then click Next.
e. After the wizard completes the scan for devices on the cluster, click **Next**.

5. On the **SAN Clients** page, click **Next**.

6. Specify backup devices that NetBackup should use.
   a. On the **Backup Devices** page, verify that all attached tape devices are displayed in the table, and then click **Next**.
   b. On the **Drag and Drop Configuration** page, select the tape devices that you want NetBackup to backup data to and then click **Next**.
   c. In the confirmation dialog box, click **Yes**.
   d. On the **Updating Device Configuration** page, click **Next**.
   e. On the **Configure Storage Units** page, view the name of your storage unit and then click **Next**.
   f. Click **Finish**.

7. Specify the storage unit to associate with the backup devices.
   a. Expand **NetBackup Management**.
   b. Expand **Storage**.
   c. Click **Storage Units**.
   d. Double-click the name of the storage unit you created previously.
   e. In the **Change Storage Unit** window, ensure that **Maximum concurrent write drives** is equal to the number of tape drives connected to your cluster.

**Results**
A storage unit is created for your cluster and tape devices. You can view all storage units by clicking **Storage Units**.

### Create a volume pool

Before you can inventory a robot in NetBackup, you must create a volume pool.

**Procedure**

1. In the **NetBackup Administration Console**, expand **Media and Device Management**.
2. Expand **Media**.
3. Expand **Volume Pools**.
4. Click **Actions** > **New** > **Volume Pool**.
5. In the **Pool name** field, type a name for the volume pool.
6. (Optional) In the **Description** field, type a description for the volume pool.
7. Click **OK**.

### Inventory a robot

Before you create a NetBackup policy, you must inventory a robot with NetBackup and associate it with a volume pool.

**Procedure**

1. In the **NetBackup Administration Console**, expand **Media and Device Management**.
2. Inventory a robot.
4. (Optional) To verify that the robot has been inventoried successfully, click the name of the media pool you created, and ensure that all media are displayed in the table.

Create a NetBackup policy

You must create a NetBackup policy that specifies how you want to back up data from an Isilon cluster.

Procedure

1. In the NetBackup Administration Console, expand Media and Device Management.
2. Expand Policies.
3. Right-click Summary of all Policies, and then click New Policy.
4. In the Policy name field, type a name for the policy and then click OK.
5. Configure the following settings:

<table>
<thead>
<tr>
<th>Setting name</th>
<th>Setting value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Type</td>
<td>NDMP</td>
<td>Required</td>
</tr>
<tr>
<td>Policy volume pool</td>
<td>The name of the volume pool you created</td>
<td>Required</td>
</tr>
<tr>
<td>Allow multiple data streams</td>
<td>Selected</td>
<td>Optional. Enables multistreaming. It is recommended that you enable multistreaming whenever possible to increase the speed of backups.</td>
</tr>
<tr>
<td>Clients</td>
<td>The Isilon cluster you want to backup data from</td>
<td>Required</td>
</tr>
<tr>
<td>Backup Selections</td>
<td>The full path of a directory on the cluster that you want to backup</td>
<td>Required</td>
</tr>
<tr>
<td>set DIRECT=Y</td>
<td></td>
<td>Optional. Enables direct access restore (DAR) for the directory. It is recommended that you enable DAR for all backups.</td>
</tr>
<tr>
<td>set HIST=F</td>
<td></td>
<td>Optional. Specifies path-based file history. It is recommended that you specify path-</td>
</tr>
</tbody>
</table>
### Configuring NDMP backup with CommVault Simpana

You can configure OneFS and CommVault Simpana to backup data stored on an Isilon cluster. The following procedures explain how to configure NDMP backup with CommVault Simpana.

**Note**

The steps described in the procedures are general guidelines only. They might change for different versions of CommVault Simpana. Consult your DMA vendor documentation for the configuration information for a specific version of CommVault Simpana.

### Add a NAS client

With CommVault Simpana, you must add a NAS client for an Isilon cluster before you can back up data from the cluster.

**Procedure**

1. In the **CommCell Browser**, right-click **Client Computers**, and then click **New Client > File System > NAS**.
2. In the **Add NDMP Server** window, configure the following settings:

<table>
<thead>
<tr>
<th>Setting name</th>
<th>Setting value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NDMP Server Hostname</td>
<td>The cluster that you want to back up data from.</td>
</tr>
<tr>
<td></td>
<td>• If you have a single Backup Accelerator node in the cluster, type the fully</td>
</tr>
<tr>
<td></td>
<td>qualified domain name, host name, and the IPv4 or IPv6 address of the</td>
</tr>
<tr>
<td></td>
<td>Backup Accelerator node.</td>
</tr>
<tr>
<td></td>
<td>• If you have multiple Backup Accelerator nodes in the cluster, type the name</td>
</tr>
<tr>
<td></td>
<td>of a SmartConnect zone that contains only the Backup Accelerator nodes.</td>
</tr>
<tr>
<td></td>
<td>• If you are performing a three-way NDMP backup, type the fully qualified</td>
</tr>
<tr>
<td></td>
<td>domain name, host name, SmartConnect zone, and the IPv4 or IPv6 address of</td>
</tr>
<tr>
<td></td>
<td>any node in the cluster.</td>
</tr>
<tr>
<td>NDMP Login</td>
<td>The name of the NDMP user account that you configured on the Isilon cluster.</td>
</tr>
<tr>
<td>NDMP Password</td>
<td>The password of the NDMP user account that you configured on the Isilon</td>
</tr>
<tr>
<td></td>
<td>cluster.</td>
</tr>
<tr>
<td>Listen port</td>
<td>The number of the port through which data management applications (DMAs) can</td>
</tr>
<tr>
<td></td>
<td>connect to the cluster. This field must match the Port number setting on the</td>
</tr>
<tr>
<td></td>
<td>Isilon cluster. The default Port number on the Isilon cluster is 10000.</td>
</tr>
</tbody>
</table>
3. Click Detect.
   The system populates the Vendor and Firmware Revision fields.
4. Click OK.

Add an NDMP library

With CommVault Simpana, you must add an NDMP library to detect tape devices attached to an Isilon cluster before you can backup data to those devices.

Procedure
1. Add the CommVault Simpana server to the configuration.
   a. In the CommCell Browser, click Storage > Library and Drive.
   b. In the Select MediaAgents window, add the Simpana server you are currently using, and then click OK.
2. Detect NDMP devices attached to the cluster.
   a. In the Library and Drive Configuration window, click Start > Detect/Configure Devices.
   b. Click NDMP Devices.
   c. Click OK.
   d. In the Select NDMP Servers to Detect window, add the Isilon cluster you want to backup data from, and then click OK. The system informs you that library services will be stopped during the detection process.
   e. Click Yes.
3. After the detection process is complete, close the Log window.
4. In the Library and Drive Configuration window, select the media changer that controls the tape drives that you want to back up data to.
   You can view the name of the media changer by right-clicking the media changer and then clicking Properties.
5. Right-click the media changer you selected, and then click Configure.
6. Click Library and all drives, and then click OK.
7. In the Confirm dialog box, specify whether the library has a barcode reader.
8. In the Discover Media Options window, specify the default media type.

Create a storage policy

With Commvault Simpana, you must configure a storage policy that specifies the Isilon cluster with the data you want to back up.

Procedure
1. Add and name a new storage policy.
   a. In the CommCell Browser, expand Policy.
   b. Right-click Storage Policies, and then click New Storage Policy.
   c. In the Create Storage Policy Wizard window, click Data Protection and Archiving, and then click OK.
   d. In the Storage Policy Name field, type a name for the storage policy, and then click Next.
2. Specify the Isilon cluster containing the data you want to back up.
   a. From the Library list, select the name of the NDMP library you configured previously.
   b. From the MediaAgent list, select the Isilon cluster you want to back up data from.
   c. Click Next.
3. From the Scratch Pool list, select Default Scratch.
4. (Optional) To enable multistreaming, specify the Number of Device Streams setting as a number greater than one.
   It is recommended that you enable multistreaming to increase the speed of backup operations.
5. Click Next.
6. Select Hardware Compression, and then click Next.
7. Click Finish.

Assign a storage policy and schedule to a client

With Commvault Simpana, you must assign a policy and schedule to a client before you can back up data from an Isilon cluster that is associated with the client.

Procedure
1. In the CommCell Browser, expand Client Computers, expand `{isilon-cluster-name}`, expand NAS, and then select the name of a backup set.
2. In the right panel, right-click the name of a subclient, and then click Properties.
3. Ensure that the following settings are configured:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Setting name</th>
<th>Setting value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Device</td>
<td>Storage Policy</td>
<td>The name of the storage policy you created</td>
<td>Required</td>
</tr>
<tr>
<td>Content</td>
<td>Backup Content Path</td>
<td>The full path of the directory that you want to back up</td>
<td></td>
</tr>
</tbody>
</table>

4. Right-click the subclient you configured, and then click Backup.
5. In the Select Backup Type area, select the type of backup.
6. Click Schedule, and then click Configure.
7. In the Schedule Details window, specify the times that you want to back up data, and then click OK.
8. Click OK.
Configuring NDMP backup with IBM Tivoli Storage Manager

You can configure OneFS and IBM Tivoli Storage Manager (TSM) to backup data stored on an Isilon cluster. The following procedures explain how to configure NDMP backup with IBM Tivoli Storage Manager.

**Note**

The steps described in the procedures are general guidelines only. They might change for different versions of IBM TSM. Consult your DMA vendor documentation for the configuration information for a specific version of IBM TSM.

**Initialize an IBM Tivoli Storage Manager server for an Isilon cluster**

You must initialize an IBM Tivoli Storage Manager server to manage NDMP backups on an Isilon cluster.

**Procedure**

1. Open the Tivoli Storage Manager Management Console.
2. Expand the Tivoli Storage Manager folder.
3. Right-click the host name of your local machine and then select Add a New Tivoli Storage Manager Server.
4. In the Initial Configuration Task List window, click Minimal configuration.
5. Click Start.
6. Follow the prompts to configure a Tivoli Storage Manager server.

**Configure an IBM Tivoli Storage Manager server for an Isilon cluster**

You can configure an IBM Tivoli Storage Manager (TSM) server to manage NDMP backups on an Isilon cluster.

Configure the TSM server by following these steps:

1. Configure the tape library.
2. Configure your system for the backup and restore operations.
3. Define a virtual filespace mapping and perform the backup operation.
4. Define a virtual filespace mapping if you are restoring data to a location other than the location from where you backed up the data, and then perform the restore operation. Otherwise, perform the restore operation without defining a virtual filespace mapping.

**Configure a tape library**

With IBM Tivoli Storage Manager (TSM), you must configure a tape library that contains the tape devices for backup and restore operations.

**Procedure**

1. Create a TSM node by running the following command:

```
register node <node-name> <admin-password> userid=admin
domain=STANDARD type=NAS
```
The following command creates a TSM node called node001:

```
register node node001 password123 userid=admin domain=STANDARD
type=NAS
```

2. Define a data mover for the node you want to back up data from by running the following command:

```
define datamover <datamover_name> type=NAS
hladdress=<backup_accelerator_ip_address> lladdress=<ndmp_port>
userid=<ndmp_username> password=<ndmp_password> dataformat=ndmpdump
```

The following command defines a data mover for node001:

```
define datamover node001 type=NAS hladdress=10.13.17.117
lladdress=10000 userid=ndmp password=ndmppw dataformat=ndmpdump
```

3. Define a tape library by running the following command:

```
def lib <library-name> libtype=scsi
```

The following command defines a tape library called ISILIB:

```
def libr ISILIB libtype=scsi autolabel=overwrite shared=no
serial=autodetect
```

4. Define the path for the data mover by running the following command:

```
define path <data_mover_name> <tape_library> srctype=datamover
desttype=library device=<backup_accelerator_library_name>
```

Specify `device` as the name of the device entry for the tape library on the Isilon cluster.

The following command defines a path for the data mover created in step 2.

```
define path node001 ISILIB srctype=datamover desttype=library
device=mc005
```

5. Define drives for the tape library by running the following command:

```
define drive <tape_library> <backup_accelerator_tape_drive>
serial=autodetect online=yes element=<tape_element_address>
```

The following commands defines four tape drives and configures TSM to automatically detect the addresses of the tape drives.

```
define drive ISILIB tape015 serial=autodetect online=yes
element=256
define drive ISILIB tape016 serial=autodetect online=yes
element=257
define drive ISILIB tape017 serial=autodetect online=yes
element=258
define drive ISILIB tape018 serial=autodetect online=yes
element=259
```

6. Define paths for tape drives by running the following command:

```
define path <data_mover_name> <path_name> srctype=datamover
desttype=drive libr=<tape_library>
device=<backup_accelerator_tape_drive>
```
The following commands define paths for the tape drives defined in the previous step:

```plaintext
define path node001 tape015 srctype=datamover desttype=drive
  libr=ISILIB device=tape015
define path node001 tape016 srctype=datamover desttype=drive
  libr=ISILIB device=tape016
define path node001 tape017 srctype=datamover desttype=drive
  libr=ISILIB device=tape017
define path node001 tape018 srctype=datamover desttype=drive
  libr=ISILIB device=tape018
```

7. Label the tape media by running the following command:

```plaintext
label libvol <tape_library> voll=<tape_media_label>
```

The following commands create labels for the tape media in the tape library:

```plaintext
label libvol ISILIB voll=C90000LA search=yes overwrite=yes
  labelsource=barcode checkin=scratch
label libvol ISILIB voll=C90001LA search=yes overwrite=yes
  labelsource=barcode checkin=scratch
label libvol ISILIB voll=C90002LA search=yes overwrite=yes
  labelsource=barcode checkin=scratch
label libvol ISILIB voll=C90003LA search=yes overwrite=yes
  labelsource=barcode checkin=scratch
```

8. Verify that the tape library has been configured accurately by performing the following steps:

   a. Verify that the tapes are online by running the following command:

```plaintext
query tape libr=<tape_library>
```

   b. Query the tape media by running the following command:

```plaintext
query libvol libr=<tape_library>
```

   c. Query the path configured to ensure that it is accurate:

```plaintext
query path <data_mover_name>
```

   d. Audit the tape library by running the following command:

```plaintext
audit library <lib_name>
```

Configure your system for backup and restore operations

With IBM Tivoli Storage Manager (TSM), you must configure your system for performing backup and restore operations.

Procedure

1. Define a device class by running the following command:

```plaintext
define devclass <class-name> devtype=<dev-type> library=<library-name> mountretention=0 estcapacity=120g
```
The following command defines a device class called ISICLASS:

```bash
define devclass ISICLASS devtype=NAS library=ISILIB
mountretention=0 estcapacity=120g
```

2. Define an NDMP storage pool by running the following command:

```bash
define stgpool <ndmp-pool-name> <class-name> maxscratch=10
dataformat=ndmpdump
```

The following command defines an NDMP storage pool called NDMPPOOL:

```bash
define stgpool NDMPPOOL ISICLASS maxscratch=10 dataformat=ndmpdump
```

3. Define a device class for the table of contents (TOC) of the files to be backed up by running the following command:

```bash
def devclass TOC devtype=<dev-type>
```

The following command defines a device class for the TOC for a device type called file:

```bash
def devclass TOC devtype=file
```

4. Define a storage TOC by running the following command:

```bash
define stgpool <TOC_POOL_NAME> DISK
```

The following command defines a storage TOC called TOC:

```bash
define stgpool TOC DISK
```

5. Define a volume for the storage pool by running the following command:

```bash
define volume <TOC_NAME> <PATH> formatsize=<SIZE_IN_MB> wait=no
```

The following command defines a storage pool volume:

```bash
define volume TOC'e:\Program Files\Tivoli\TSM\server1\tsm_6.toc.dsm' formatsize=1024 wait=no
```

6. Define a domain by running the following command:

```bash
def domain domain_name
```

The following command defines a domain called NASDOMAIN:

```bash
def domain NASDOMAIN
```

7. Define a policy by running the following command:

```bash
def pol domain_name policy_name
```

The following command defines a policy called NASPOLICY:

```bash
def pol NASDOMAIN NASPOLICY
```

8. Define a management class by running the following command:

```bash
define mgmtclass <domain_name> <policy_set_name> <mgmt_class_name>
```
The following command defines a management class called NASMGMT:

```bash
define mgmtclass STANDARD STANDARD NASMGMT
```

9. Define a copy group by running the following command:

```bash
define copygroup <domain_name> <policy_set_name> <mgmt_class_name>
type=backup destination=<ndmp_pool_name> [serialization=static]
tocdestination=<toc_pool_name>
```

The following command defines a copy group:

```bash
define copygroup STANDARD STANDARD ISIMC type=backup
destination=NDMPPOOL serialization=static tocdestination=TOCPool
```

10. Assign a default management class by running the following command:

```bash
assign defmgmtclass <domain_name> <policy_set_name> <mgmt_class_name>
```

In order to allow a TOC to be backed up to disk, a specific management class must be defined because the standard management class cannot be modified. The following command assigns the ISIMC management class as the default for the standard policy set and the standard domain:

```bash
assign defmgmtclass STANDARD STANDARD ISIMC
```

11. Validate the policy set by running the following command:

```bash
validate policyset <domain_name> <policy_set_name>
```

The following command validates the standard policy set:

```bash
validate policyset STANDARD STANDARD
```

12. Activate the policy set by running the following command:

```bash
activate policyset <domain_name> <policy_set_name>
```

The following command activates the standard policy set:

```bash
activate policyset STANDARD STANDARD
```

13. Update the TSM node to the domain that you created in step 6 by running the following command:

```bash
update node <ip_addr_or_node_name> <domain_name>
```

The following command updates the node to the domain that you created in step 6:

```bash
activate policyset 10.27.49.39 NASDOMAIN
```

14. Update the path to the NAS library by running the following command:

```bash
update path <ip_addr_or_node_name> <tape_library>
srctype=datamover desttype=libr
```
The following command updates the path to the NAS library for node001:

```
update path node001 ISILIB srctype=datamover desttype=libr
        online=yes
```

**Define a virtual filespace mapping for the backup operation**

As a part of configuring IBM Tivoli Storage Manager for managing NDMP backups on an Isilon cluster, you must define a virtual filespace mapping before performing the backup operation.

**Procedure**

1. Define virtual filespace mapping by running the following command:

   ```
def virtualfs <ip_addr_or_node_name> <virtual_filespace_name>
            <file_system_name> <path>
```

   The following example creates a virtual filespace mapping for `/ifs/data`.

   ```
def virtualfs node001 /data-backup /ifs /data
```

2. Perform the backup operation by running the following command:

   ```
backup node <ip_addr_or_node_name> <virtual_filespace_name>
        mode=backup_mode
```

   The following example performs a backup operation on node001.

   ```
backup node node001 /data-backup mode=full toc=yes wait=yes
```

**Define a virtual filespace mapping for the restore operation**

If you are restoring data to a location that is different from the location that you backed up the data from, define a virtual filespace mapping for the restore operation. You must perform this process as a part of configuring IBM Tivoli Storage Manager for managing NDMP backups on an Isilon cluster.

**Procedure**

1. Define a virtual filespace mapping by running the following command:

   ```
def virtualfs <ip_addr_or_node_name> <virtual_filespace_name>
            <file_system_name> <path>
```

   The following example creates a filespace mapping for `/ifs/data`.

   ```
def virtualfs node001 /data-restore /ifs /data
```

2. Restore data by running the following command:

   ```
restore node <ip_addr_or_node_name> <virtual_fs_backup_location>
        <restore_file_system_name>
```

**Note**

If you are restoring data to the same location that you backed up the data from, you do not need to define a virtual filespace mapping.
The following example restores data on node001:

```bash
restore node node001 /data-backup /data-restore wait=yes
```