White Paper

BEST PRACTICES FOR DATA REPLICATION WITH EMC ISILON SYNCIQ

Abstract

This white paper provides a detailed overview of the key features and benefits of EMC Isilon SyncIQ software and describes how SyncIQ enables enterprises to flexibly manage and automate data replication between two Isilon clusters. This paper also describes best practices and use cases to maximize the benefits of cluster-to-cluster replication.

November 2012

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided "as is." EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Part Number h8224.1

Table of Contents

Introduction 5
Fast, reliable file-based replication 5
Use cases 6
Disaster recovery 7
Business continuance 7
Disk-to-disk backup and restore 7
Remote archive 8
Architecture and functionality 8
Leveraging clustered storage architecture 8
Asynchronous source-based replication 9
Flexible, policy-driven replication 9
Efficient block-based deltas 10
Source-cluster snapshot integration 10
Target-cluster snapshots 12
SmartConnect integration 12
Target Aware Initial Sync 13
Tunable replication performance 13
Real-time monitoring and historical reports 14
Policy assessment 14
SyncIQ automated data failover and failback 14
Failover and failback 14
SyncIQ features 17
Performance 17
Snapshot integration removes need for treewalks 17
Copy jobs 17
Source and target cluster association persistence 19
Target protection with restricted writes—replication domains 19
Assess SynclQ changes 19
Improved authentication integration 20
Multiple jobs targeting a single directory tree no longer supported 20
Hard-link replication now supported 20
Report changes 20
SynclQ best practices and tips 20
Avoiding full dataset replications 20
Selecting the right source replication dataset 21
Including or excluding source-cluster directories 21
Configuring SynclQ policy file selection criteria 22
Disaster recovery from a target Isilon cluster 23
Performance tuning 24
Guidelines 25

Limitations and restrictions 25
Using Isilon SnapshotIQ on the target 26
Using SmartConnect with SyncIQ 26
Using SmartConnect on the source cluster 26
Using SmartConnect zones on the target cluster 27
Monitoring SyncIQ 28
Policy job monitoring 29
Performance monitoring 29
Roles Based Administration 30
Automation via the OneFS Platform API 30
Troubleshooting with SyncIQ logs 30
Target aware initial synchronization 31
Failover dry-run testing 32
Version compatibility 32
Additional tips 32
Conclusion 33
About EMC Isilon 33
Contact EMC Isilon 33

Introduction

Simple, efficient, and scalable, EMC® Isilon® SyncIQ® data replication software provides data-intensive businesses with a multi-threaded, multi-site solution for reliable disaster protection.

Fast, reliable file-based replication

All businesses want to protect themselves against unplanned outages and data loss. The best practice is typically to create and keep copies of important data so it can always be recovered. There are many approaches to creating and maintaining data copies. The right approach depends on the criticality of the data to the business and its timeliness. In essence, how long the business can afford to be without it.

As the sheer amount of data requiring management grows, it puts considerable strain on a company's ability to protect its data. Backup windows shrink, bottlenecks emerge, and logical and physical divisions of data fragment data protection processes. The result is increasing risk to your data and growing complexity in managing it.

Isilon SyncIQ offers powerful, flexible, and easy-to-manage asynchronous replication for collaboration, disaster recovery, business continuance, disk-to-disk backup, and remote disk archiving.

Designed for big data, SyncIQ delivers unique, highly parallel replication performance that scales with the dataset. Every node in an Isilon cluster can send and receive data, so replication performance increases as your data store grows, since SyncIQ can take advantage of any available network bandwidth. Because both the source and the target can scale to multiple petabytes without fragmentation into multiple ivolumes or file systems, data replication starts simple and stays that way as the system scales to provide a solid foundation for disaster recovery.

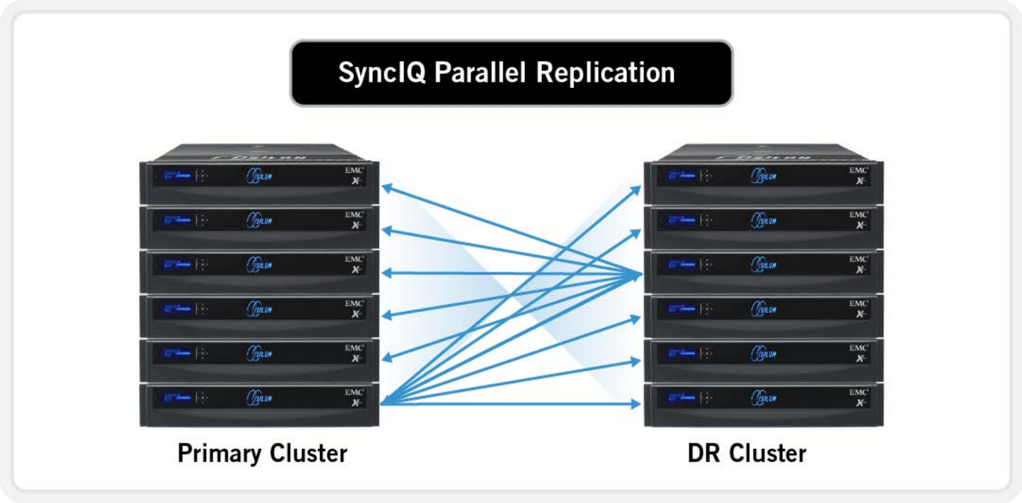


Figure 1. SyncIQ parallel replication

A simple and intuitive web-based user interface allows you to easily organize SyncIQ replication job rates and priorities to match business continuance priorities. Typically, a SyncIQ recurring job would be put in place to protect the data required for each major recovery point objective in your disaster recovery plan. For example, you may choose to sync every 6 hours for customer data, every 2 days for HR data, and so on. You can also configure a directory, file system or even specific files for more or less frequent replication based on their business criticality. In addition, you can create remote archive copies of out-of-use data that needs to be retained so you can reclaim valuable capacity in your production system.

In addition to being easy-to-use and non-disruptive, SyncIQ uses as much or as little system resource and network bandwidth as you specify. With Isilon, you may also schedule sync jobs for off-peak hours.

Use cases

Isilon SyncIQ offers powerful, efficient, and easy-to-manage data replication supporting the following solutions:

- Disaster recovery
- Business continuance
- Remote collaboration
- Disk-to-disk backup
- Remote disk archive

As shown in Figure 2, SyncIQ typically replicates data from a primary site to a secondary, local or remote site, creating a copy for disaster recovery, business continuance, disk-to- disk backup, or remote archiving purposes.

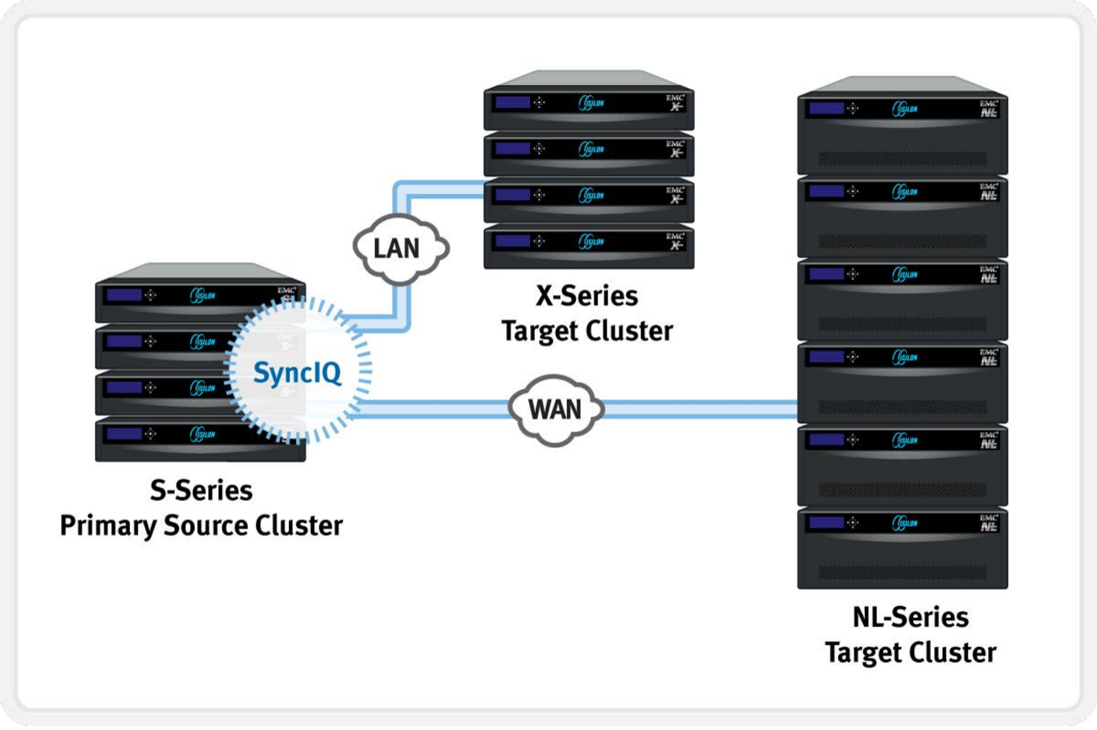


Figure 2. SyncIQ over LAN or WAN

SyncIQ is also able to use the same cluster as a target in order to create local replicas. In this scenario, efficient data transfer occurs across the cluster's Infiniband back-end network.

Additionally, SyncIQ replication can be configured in a hub-and-spoke topology, where a single source replicates to multiple targets (or many to one), and also cascading topology, where each cluster replicates to the next in a chain.

As we can see, SyncIQ is both powerful and flexible, and can deliver the data protection requirements of data-intensive, core, revenue workflows across multiple industries.

Disaster recovery

Disaster recovery requires quick and efficient replication of critical business data to a secondary site, either local or remote.

SynclQ delivers high performance, asynchronous replication of data over short (LAN) or long distances (WAN), providing protection from both local site and regional disasters, to satisfy a range of recovery objectives. SynclQ has a very robust policy-driven engine that allows you to customize your replication datasets to minimize system impact while still meeting your data protection requirements.

Additionally, SyncIQ's automated data failover and failback reduces the time, complexity and risks involved with transferring operations between a primary and secondary site, in order to meet an organization's recovery objectives. This functionality can be crucial to the success of a disaster recovery plan.

Business continuance

By definition, a business continuance solution needs to meet your most aggressive recovery objectives for your most timely, critical data. SynclQ's highly efficient architecture - performance that scales to maximize usage of any available network bandwidth - gives you the best-case replication time for tight recovery point objectives (RPO). You can also use SynclQ in concert with Isilon SnapshotIQ® software which allows you to store as many point-in-time snapshots of your data as needed to support secondary activities like backup to tape.

Disk-to-disk backup and restore

SynclQ increases the performance of large-scale backups and restores.

Enterprise IT organizations face increasingly complex backup environments with costly operations, shrinking backup and restore windows, and increasing service-level agreement (SLA) requirements. Backups to tape are traditionally slow and hard to manage as they grow, and are compounded by the size and rapid growth of digital content and unstructured data. SynclQ is a superior disk-to-disk backup and restore solution that delivers unmatched performance and simplicity, enabling IT organizations to reduce backup and restore times and costs, eliminate complexity, and minimize risk. With Isilon scale-out network-attached storage (NAS), petabytes of backup storage can be managed within a single system-as one volume and one file system-and can be the disk backup target for multiple Isilon clusters.

Remote archive

For data that is too valuable to throw away, but not time-critical enough to justify maintaining it on production storage, replicate it with SyncIQ to a secondary local or remote site and reclaim the space on your primary system. Deletion of data on the source does not affect the target, leaving you with a remote archive for disk-based tertiary storage applications or for staging data before it moves to offline storage. Remote archiving is ideal for intellectual property preservation, long-term records retention, or project archiving.

Architecture and functionality

Leveraging clustered storage architecture

SynclQ leverages the full complement of resources in an Isilon cluster and the scalability and parallel architecture of the EMC Isilon OneFS® operating system. SynclQ uses a policy-driven engine to execute replication jobs across all nodes in the cluster. To allow for high flexibility and resource management, you can create any number of SynclQ policies. Each SynclQ policy defines a job profile with a source directory and a target location (cluster and directory) that can either be executed on a user-defined schedule or started manually. This flexibility allows you to replicate datasets based on predicted cluster usage, network capabilities, and requirements for data availability.

When a SynclQ job is initiated (from either a scheduled or manual policy), the system first takes a snapshot of the data to be replicated. SynclQ compares this to the snapshot from the previous replication job, which enables it to quickly identify the changes that need to be addressed. SynclQ then pools the aggregate resources from the cluster, splitting the replication job into smaller work items and distributing these amongst multiple workers across all nodes in the cluster. Each worker scans a part of the snapshot differential for changes and transfers those changes to the target cluster. While the cluster resources are managed to maximize replication performance, You can decrease impact on other workflows using configurable SyncIQ resource limits.

Replication workers on the source cluster are paired with workers on the target cluster so the benefits of parallel and distributed data transfer are carried over to the target cluster. As more jobs run concurrently, SynclQ will employ more workers to utilize more cluster resources. As more nodes are added to the cluster, file system processing on the source cluster and file transfer to the remote cluster are accelerated, a benefit of the Isilon scale-out NAS architecture.

SynclQ provides a simple, intuitive, web-based UI to create policies, manage jobs, and view reports. In addition to the web-based interface all SynclQ functionality is available through a command line interface that can be launched remotely over SSH connections. A full list of all commands is available by running the following CLI command on an Isilon node: `isi sync --help`

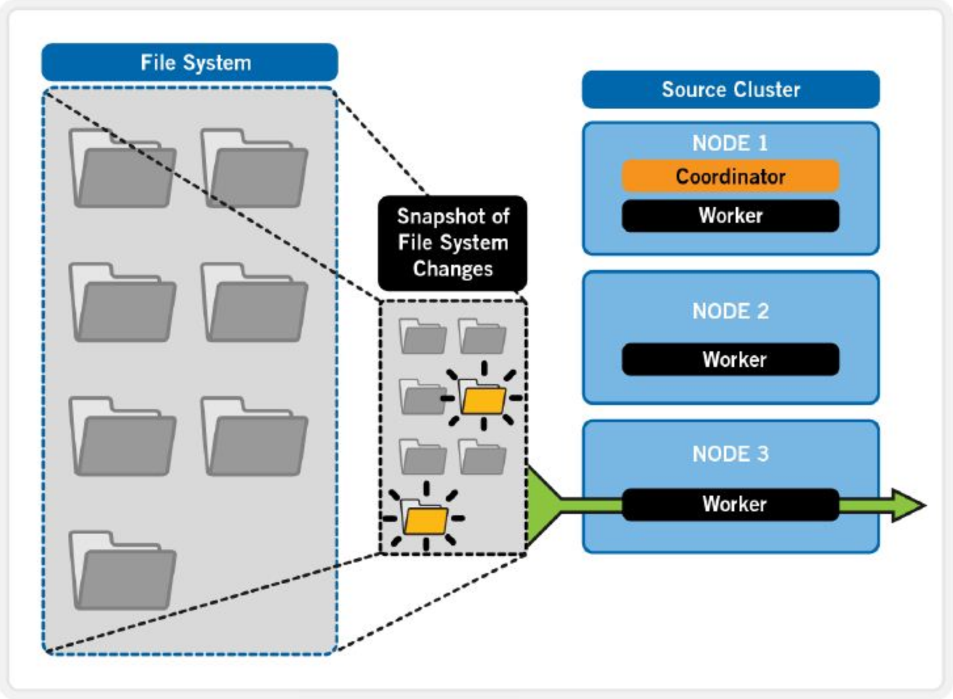


Figure 3. SyncIQ work distribution across the cluster

Asynchronous source-based replication

SyncIQ is an asynchronous remote replication tool. It differs from synchronous remote replication tools where writes to the local storage system are not acknowledged back to the client until those writes are committed to the remote storage system. SyncIQ asynchronous replication allows the cluster to respond quickly to client file system requests while replication jobs run in the background, per policy settings.

SyncIQ is source-based, which means it is aware only of changes that have occurred on the source cluster. Those changes can be new files, changed files, metadata changes, or file deletions.

Notes:

- To better protect distributed workflow data, SyncIQ prevents changes on target directories that are associated with a SyncIQ job. In previous versions, SyncIQ was not aware of changes made on the target cluster, so it was necessary that replication destination paths on the target cluster were protected from manual changes. If your workflow requires writeable targets, you must break the SyncIQ source/target association before writing data to a target directory, and any subsequent re-activation of the synchronize association will require a full synchronization.
- SyncIQ does not support bi-directional replication.

Flexible, policy-driven replication

SyncIQ policies allow you to replicate only directories and files that meet specified criteria. File selection criteria are comprehensive, yet easy to use and can be used to build flexible policies that support varied workflows. Selection criteria include:

- filename
- include/exclude directories
- file size
- file accessed
- created and modified times
- file type
- regular expression (file and path names)

With policy-driven replication, you can reduce the amount of time, processing resources, and network resources by replicating only the data you need. For example, in VMware environments you can select individual virtual machines (VMs) based on the directory of each VM (unlike other replication tools that require you to choose entire volumes with multiple VMs). In the case of user home directories, you can exclude large media files that are not critical to the business operations.

Efficient block-based deltas

The initial replication of a new policy or a changed policy will perform a full baseline replication of the entire dataset based on the directory and file selection policy criteria. This baseline replication is necessary to ensure all original data is replicated to the remote location. However, every incremental job execution of that policy will transfer only the bytes which have changed since the previous run (on a per-file basis). SyncIQ uses internal file system structures to identify changed blocks and, along with parallel data transfer across the cluster, minimizes the replication time window and network use. This is critical in cases where only a small fraction of the dataset has changed, as in the case of virtual machine VMDK files, in which only a block may have changed in a multi-gigabyte virtual disk file. Another example is where an application changed only the file metadata (ACLs, Windows ADS). In these cases, only a fraction of the dataset is scanned and subsequently transferred to update the target cluster dataset.

Notes:

- Certain policy definition changes cause incremental jobs to conduct a full baseline dataset replication. The next section describes how to avoid full baseline replication when changing a policy definition.
- In SyncIQ, when a file or an entire directory at the source of a replicated dataset is moved to a new location within the dataset, it is simply moved on the target as well. With SyncIQ versions prior to OneFS 6.5, the entire file, or files within a moved directory, will be replicated.

Source-cluster snapshot integration

To provide point-in-time data protection, when a SyncIQ job starts, it automatically generates a snapshot of the dataset on the source cluster. Once it takes a snapshot, it bases all replication activities (scanning, data transfer, etc.) on the snapshot view; any changes that occur to the file system during the replication job execution do not affect the replicated dataset (those changes are picked up the next time the job runs). OneFS creates instantaneous snapshots before the job begins so you do not have to block application activity during the replication operation.

Source-cluster snapshots are named SIQ-<policy-id>-[new, latest], where <policy-id> is the unique system-generated policy identifier. SyncIQ compares the newly created snapshot with the one taken during the previous run and determines the changed files and blocks to transfer. Each time a SyncIQ job completes, the 'latest' snapshot is deleted and the 'new' snapshot is renamed to 'latest'.

Regardless of the existence of other inclusion or exclusion directory paths, only one snapshot is created on the source cluster at the beginning of the job based on the policy root directory path.

Note: This source-cluster snapshot does not require a SnapshotIQ module license.

Note: When a SyncIQ policy is deleted, SyncIQ also deletes any snapshots that the policy created.

When application consistency is important, you can integrate the replication job with third-party application agents that can execute the replication job remotely by using the SyncIQ command line over an SSH session.

For example, in a VMware vSphere environment, you can take application or OS consistent VMware backups via the Isilon vCenter plug-in, before manually running a SyncIQ job. Once the SyncIQ job completes, you can safely remove the VMware snapshot. This process can also be automated via scripts that call the VMware commands from a local host, and which leverage OneFS' vSphere VAAI and VASA integration.

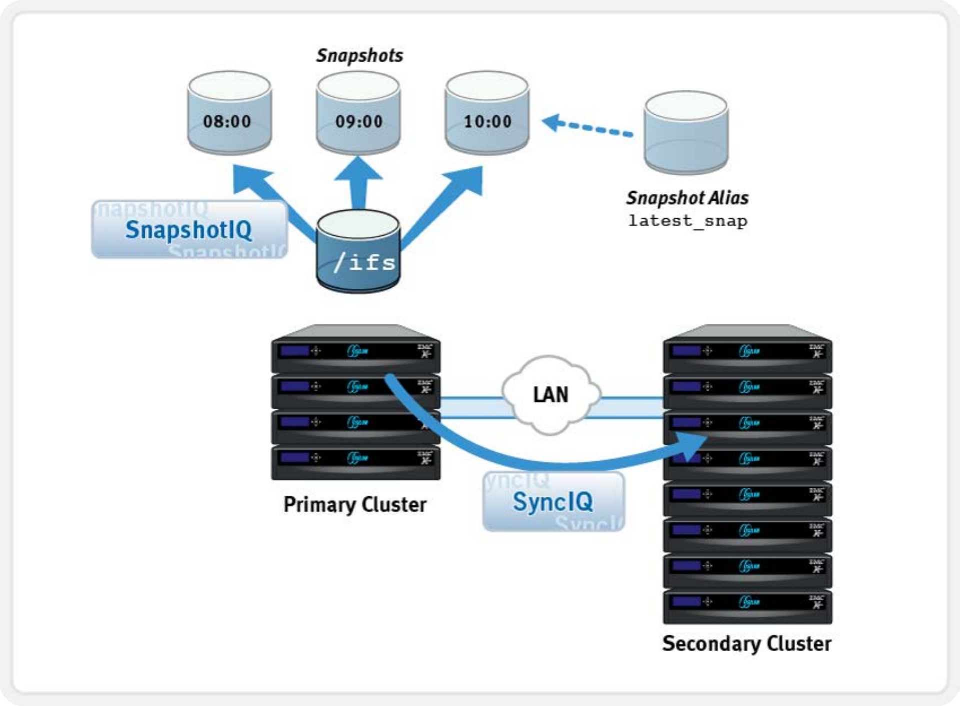


Figure 4. SyncIQ point-in-time consistent replication

Target-cluster snapshots

In addition to integrating OneFS snapshots on the source cluster for point-in-time consistency, snapshots of the directory can be generated on the target cluster. For an initial sync, a snapshot is taken on the target cluster at the beginning of the replication job (before data is transferred) to prevent unintentionally overwriting the existing data. A snapshot is taken at the end of each replication job, both initial and incremental. This creates multiple, space-efficient versions of the replicated dataset to choose from on the target cluster.

This is very useful for archiving purposes when you want to use a near-line Isilon cluster (typically an NL-Series) to maintain different versions of replicated datasets archived from primary Isilon storage (typically S-Series or X-Series Isilon clusters).

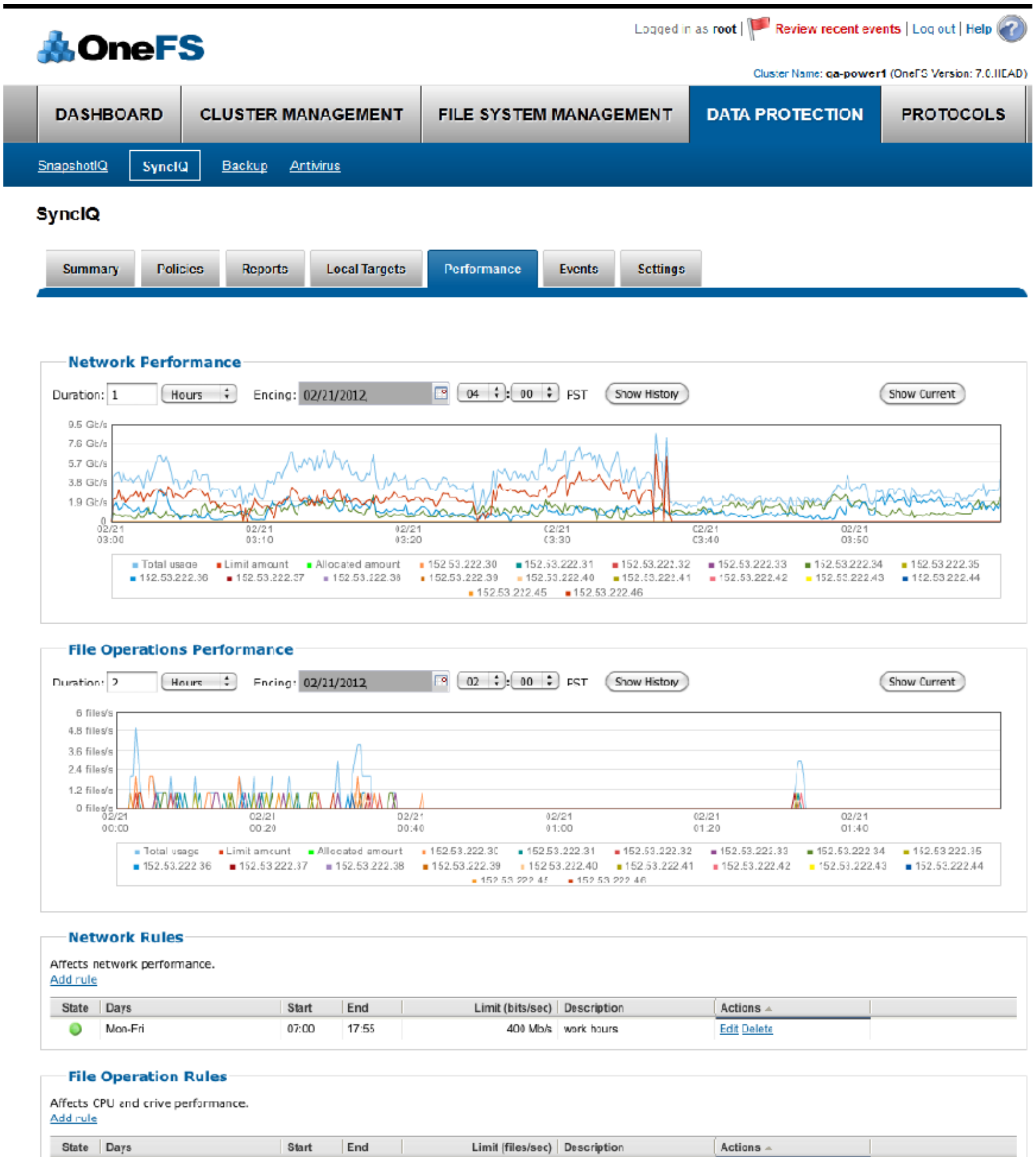
Note: SnapshotIQ is a licensed software module that delivers a powerful snapshot management tool to create, schedule, and expire an unlimited number of OneFS snapshots anywhere in the OneFS file system. To enable target-cluster snapshots you must have a SnapshotIQ module license and enable the Isilon SnapshotIQ module on the target cluster. For more details please see http://www.isilon.com/snapshotiq.

SmartConnect integration

SyncIQ uses the standard Gigabit and 10 Gigabit Ethernet ports available on cluster nodes to send replication data from the source to the destination cluster. However, by selecting a predefined EMC Isilon SmartConnect™ IP address pool, you can restrict replication processing to specific nodes both on the source and target clusters. This is useful when you want to guarantee that replication jobs are not competing with other applications for specific node resources. By selecting particular nodes, you can also define which networks are used for replication data transfer.

Once you define a SmartConnect IP address pool on the source cluster via the Isilon web administration interface, you can use that IP address pool globally across all policies on the source cluster, or you can select different IP address pools for use on a per-policy basis. To restrict sending replication traffic to specific nodes on the target cluster you can associate (globally or per policy) a SmartConnect zone name with the target cluster.

Note: If you change the Default Policy global settings, the default policy will not update existing policies but will be used when creating new policies.



Network Performance

Duration: 1 Hours Ending: 02/21/2012 04 : 00 EST

File Operations Performance

Duration: 2 Hours Ending: 02/21/2012 02 : 00 EST

Network Rules

Affects network performance.

State	Days	Start	End	Limit (bits/sec)	Description	Actions
●	Mon-Fri	07:00	17:55	400 Mb/s	work hours	Edit Delete

File Operation Rules

Affects CPU and drive performance.

State	Days	Start	End	Limit (files/sec)	Description	Actions

Figure 5. SyncIQ web-based management interface

Target Aware Initial Sync

The Target Aware Initial Sync advanced feature, available only through the command line interface, allows you to reduce network traffic during initial baseline replication. In cases where most of the dataset already resides on both the source and target cluster, this feature can accelerate the initial baseline replication job by using file hashes to limit replication to only those files that differ between source and target.

Tunable replication performance

SyncIQ uses aggregate resources across the cluster to maximize replication performance, thus potentially affecting other cluster operations and client response. The default performance configurations (number of workers, network use, CPU use) may not be optimized for certain datasets. CPU and network use are set to ‘unlimited’ by default. However, SynclQ allows you to control how resources are consumed and balance replication performance with other file system operations. You can control how much bandwidth SynclQ uses and the rate at which it processes files on a cluster-wide level, as well as which nodes and how many workers it should use on each node, on a per-SyncIQ-policy basis.

Real-time monitoring and historical reports

SynclQ allows you to monitor the status of policies and replication jobs with real-time performance indicators and resource utilization. This allows you to determine how different policy settings affect job execution and impact performance on the cluster. In addition, every job execution produces a comprehensive report that can be reviewed for troubleshooting and performance analysis. This real-time report provides you with information about the amount of data replicated and the effectiveness of those jobs, enabling you to tune resources accordingly.

Policy assessment

SynclQ can conduct a trial run of your policy without actually transferring file data between locations. SynclQ can scan the dataset and provide a detailed report of how many files and directories were scanned. Running a policy assessment is also useful for performance tuning, allowing you to understand how changing worker loads affects the file scanning process so you can reduce latency or control CPU resource consumption.

Note: Beginning with OneFS 6.5, this functionality is available only after you create a new policy and before you attempt a normal synchronization for the first time.

SyncIQ automated data failover and failback

Failover and failback

OneFS 7.0 introduces automated data failover and failback, bringing high availability to SyncIQ. Utilizing SnapshotIQ technology for simple, Point in Time, differential tracking - and combined with highly parallel replication - SyncIQ is able to deliver granular, efficient recovery points. In the event that a primary cluster becomes unavailable, SyncIQ provides the ability to failover to a mirrored, DR cluster with minimal interruption.

During such a scenario, the administrator makes the decision to redirect client I/O to the mirror and initiates SyncIQ failover on the DR cluster. Users continue to read and write to the DR cluster while the primary cluster is repaired.

Once the primary cluster becomes available again, the administrator may decide to revert client I/O back to it. To achieve this, the administrator initiates a SyncIQ failback process which synchronizes any incremental changes made to the DR cluster back to the primary. When complete, the administrator redirects client I/O back to the original cluster again.

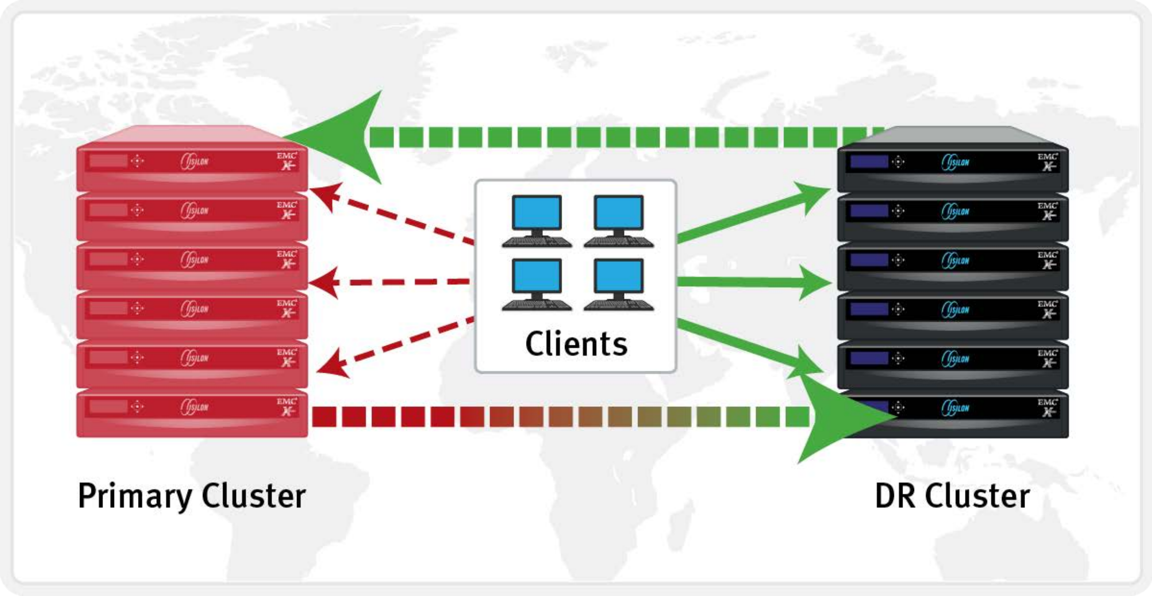


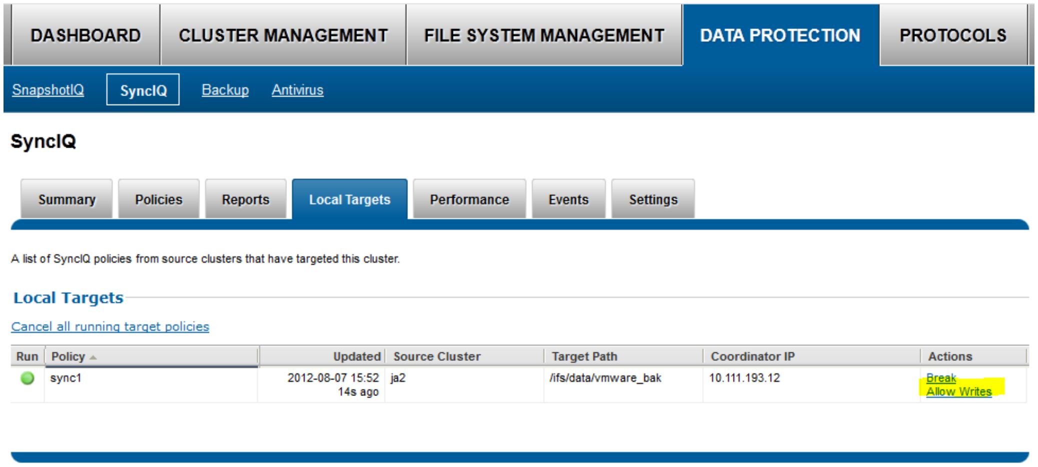
Figure 6. SyncIQ Automated Data Failover and Failback

To illustrate this process in more detail, imagine there's a replication job 'sync1' running between the source cluster A and target cluster B. Cluster A experiences an issue and the administrator decides to failover to cluster B.

To initiate failover:

- The administrator sets the target cluster B 'sync1' replica to read-write:

  ```
  # isi sync target allow_write sync1
  ```



A list of SyncIQ policies from source clusters that have targeted this cluster.

Local Targets

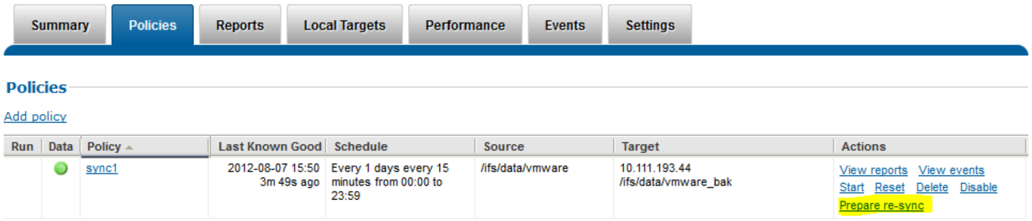
Cancel all running target policies

Run	Policy	Updated	Source Cluster	Target Path	Coordinator IP	Actions
●	sync1	2012-08-07 15:52 14s ago	ja2	/ifs/data/vmware_bak	10.111.193.12	Break Allow Writes

Failback is split into three distinct phases:

- First, the failback prep phase readies the source cluster A to receive changes from the target cluster by setting up a read-only replication domain and then restoring the last known good snapshot:

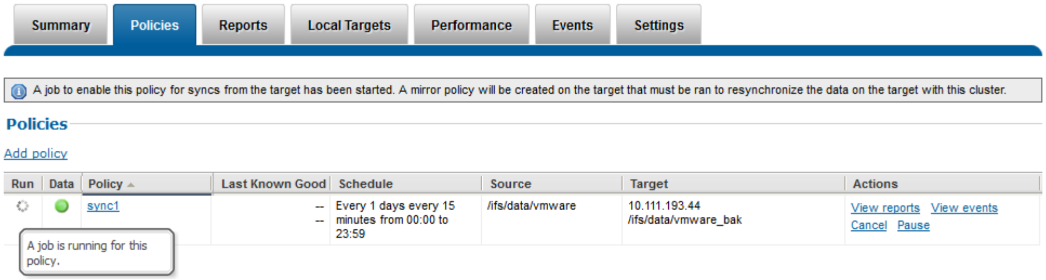
  ```
  # isi sync resync prep sync1
  ```



Policies

Add policy

Run	Data	Policy	Last Known Good	Schedule	Source	Target	Actions
	●	sync1	2012-08-07 15:50 3m 49s ago	Every 1 days every 15 minutes from 00:00 to 23:59	/ifs/data/vmware	10.111.193.44 /ifs/data/vmware_bak	View reports View events Start Reset Delete Disable Prepare re-sync



A job to enable this policy for syncs from the target has been started. A mirror policy will be created on the target that must be ran to resynchronize the data on the target with this cluster.

Policies

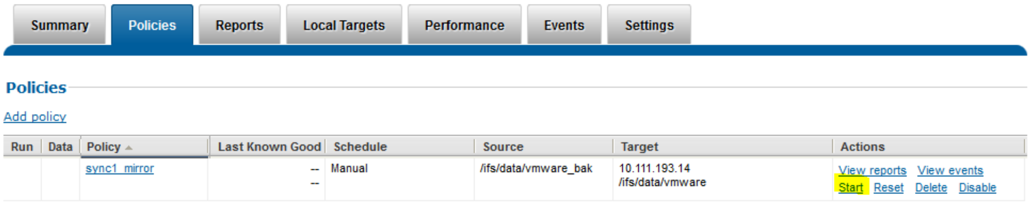
Add policy

Run	Data	Policy	Last Known Good	Schedule	Source	Target	Actions
	●	sync1	-- --	Every 1 days every 15 minutes from 00:00 to 23:59	/ifs/data/vmware	10.111.193.44 /ifs/data/vmware_bak	View reports View events Cancel Pause

A job is running for this policy.

- Next, upon successful completion of failback prep, a final failback differential sync is performed:

  ```
  # isi sync policy run sync1_mirror
  ```



Policies

Add policy

Run	Data	Policy	Last Known Good	Schedule	Source	Target	Actions
		sync1_mirror	-- --	Manual	/ifs/data/vmware_bak	10.111.193.14 /ifs/data/vmware	View reports View events Start Reset Delete Disable

- Lastly, the administrator verifies that the failback has completed, via the replication policy report, and redirects clients back to the primary cluster A again. At this time, cluster B is automatically relegated back to its role a target.

  ```
  # isi sync policy report sync1_mirror –N=0

  sync1_mirror:
      Start              Stop               Act                         Status
      08/19/12 14:58:43  08/19/12 14:58:46 sync                        Success
      08/19/12 15:18:40  08/19/12 15:18:48 resync_prep                 Success
      08/19/12 15:18:49  08/19/12 15:18:52 resync_prep_domain_mark Success
      08/19/12 15:18:52  08/19/12 15:19:01 resync_prep_restore         Success
      08/19/12 15:19:01  08/19/12 15:19:02 resync_prep_finalize        Success
  ```

In addition to the obvious unplanned failover and failback, SyncIQ also supports controlled, proactive cluster failover and failback. This provides two major benefits:

- The ability to validate and test DR procedures and requirements.
- Performing planned cluster maintenance.

Note: SynclQ Failover and Failback does not replicate cluster configurations such as shares and exports, quotas, snapshots, and networking settings, from the source cluster. Isilon does copy over UIO/GID ID mapping during replication. In the case of failover to the remote cluster, other cluster configurations must be configured manually. Please consult Isilon Technical Support for more information.

SyncIQ features

SyncIQ's highly parallel architecture dramatically improves replication times, protecting replicated data against accidental alteration and deletion, and improving source and target association persistence.

Performance

SyncIQ has significant, positive performance impacts for most customer workflows. Some of the most significant architectural enhancements include:

- Incremental synchronizations do not require a treewalk of the replication set and only the changed data is replicated.
- Rename operations are treated as a move not a delete.

Snapshot integration removes need for treewalks

SyncIQ automatically takes a snapshot of the dataset on the source cluster before starting each SyncIQ data-synchronization or copy job; this source-cluster snapshot does not require a SnapshotIQ module license. When a SyncIQ job starts, if the system detects a previous source-cluster snapshot, SyncIQ sends to the target only those files that are not present in the previous snapshot, as well as changes to files since the last source-cluster snapshot was taken. Because comparing two snapshots is typically miniscule compared with walking the entire tree, the performance gain for incremental synchronizations can be significant.

When a SyncIQ job starts, if the system does not find a previous source-cluster snapshot (for example, if a SyncIQ job is running for the first time), SyncIQ takes an initial snapshot of the specified root path on the source cluster. When a SyncIQ job completes, the system deletes the previous source-cluster snapshot and retains the most recent snapshot.

During a SyncIQ job, SyncIQ identifies any changes on the source cluster and then replicates those changes to the target cluster.

Copy jobs

- In previous OneFS versions, copy jobs did not remove files from the target that were deleted on the source. Also, SyncIQ treated a renamed file operation as a delete and a re-create operation, so the target left a copy of the file at the old location. SyncIQ now keeps track of file moves and no longer leaves links to old file locations where the file simply moved within the synchronization job or where hard-linked files still contain at least one link in the replication set. Additionally, SyncIQ previously considered the deletion of a directory and its replacement by an identically named directory as a reuse of a directory. SyncIQ recognizes the re-created directory as a "new" directory, causing the "old" directory to be removed (along with its contents).

  Example: If you delete "/ifs/old/dir" and all of its contents on the source with a copy policy, "/ifs/old/dir" still exists on the target. On the other hand, if you delete

"/ifs/old/dir" and create a new directory named "/ifs/old/dir" in its place, the old "dir" and its contents on the target will be removed.

- SyncIQ keeps track of file moves and maintains hard-link relationships at the target level. Because of this change, the behavior of SyncIQ copy jobs is slightly different from that in earlier releases. In earlier releases, SyncIQ did not perform delete operations on the target unless it used the target path for another file. SyncIQ also removes links during repeated replication operations if it points to the file or directory in the current replication pass.

  Example:

  If a single linked file is moved within the replication set, SyncIQ removes the old link and adds a new link. Assume the following:

  - The SyncIQ policy root directory is set to /ifs/data.
  - /ifs/data/user1/foo is hard-linked to /ifs/data/user2/bar.
  - /ifs/data/user2/bar is moved to /ifs/data/user3/bar.

  With copy replication, on the target cluster, /ifs/data/user1/foo will remain, and ifs/data/user2/bar will be moved to /ifs/data/user3/bar.

- If a single hard link to a multiply linked file is removed. SyncIQ now removes the destination link.

  Example:

  Using the example above, if /ifs/data/user2/bar is deleted from the source, copy replication also removes /ifs/data/user2/bar from the target.

- If the last remaining link to a file is removed on the source, SyncIQ no longer removes the file on the target unless another source file or directory with the same filename is created in the same directory (or unless a deleted ancestor is replaced with a conflicting file or directory name).

  Example:

  Continuing with the same example, assume that /ifs/data/user2/bar has been removed, which makes /ifs/data/user1/foo the last remaining link. If /ifs/data/user1/foo is deleted on the source cluster, with a copy replication, SyncIQ does not delete /ifs/data/user1/foo from the target cluster unless a new file or directory was created on the source cluster that was named /ifs/data/user1/foo. Once SyncIQ creates the new file or directory with this name, the old file on the target cluster is removed and re-created upon copy replication.

- If a file or directory is renamed or moved on the source cluster and still falls within the SyncIQ policy' root path, then, when copied, SyncIQ will rename that file on the target; it does not delete and re-create the file. However. if the file is moved outside of the SyncIQ policy root path, then with copy replication, SyncIQ will leave that file on the target but will no longer associate it with the file on the source. If that file is moved back to the original source location or even to another directory within the Sync IQ policy root path, with copy replication, SyncIQ creates a new file on the target since it no longer associates it with the original target file.

  Example:

  If the policy is rooted at /ifs/data/user and /ifs/data/user1/foo is moved to /ifs/data/user2/foo with an incremental copy replication, SyncIQ simply renames the file on the target. This prevents deletion and re-creation, as was the case in earlier versions. However, if /ifs/data/user1/foo is moved to /ifs/home/foo, which is outside the SyncIQ policy root path. Then with copy replication, SyncIQ does not delete /ifs/data/user1/foo on the target, but it does disassociate (or orphan) it from the source file, that now resides at /ifs/home/foo. If, on the source cluster, the file is moved back to /ifs/data/user1/foo, an incremental copy writes that entire file to the target cluster because the association with the original file has been broken.[1]

Source and target cluster association persistence

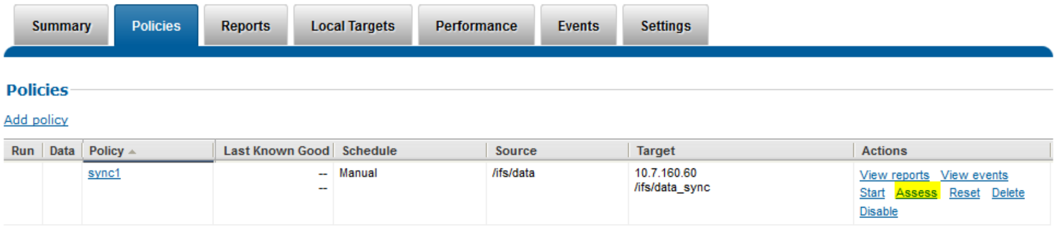
OneFS associates a policy with its specified target directory by placing a cookie on the source cluster when the job runs for the first time. Even if you modify the name or IP address of the target cluster, the cookie causes the association to persist. If necessary, you can manually break a target association, for example, if an association is obsolete or was intended for temporary testing purposes. Breaking a target association causes the source to fully resynchronize the next time the job runs, and also causes the target dataset to become writable again. During this full resynchronization, SyncIQ creates a new association between the source and its specified target.

Target protection with restricted writes—replication domains

Previous versions of SyncIQ strongly recommended that you restrict write permissions on target directories. This is now enforced by SyncIQ via protected replication domains. As such, all writes outside of a SyncIQ process are disabled on any directory that is a target for a SyncIQ job. However, if you break the association between a target and a source, the target then returns to a writeable state. Resolving a broken association will force a full resynchronization to occur at the next job run. Every SyncIQ policy has a direct 1:1 association with its target directory, and all sub-directories. Restricted writes prevent modification, creation, deletion, or movement of any files within the target path of a SyncIQ job, and prevent movement or creation of hard links to any files into orout of the target path of a SyncIQ job.

Assess SyncIQ changes

SyncIQ can conduct a trial run of your policy without actually transferring file data between locations. This provides an indication as to how much time and the level of resources an initial replication policy is likely to consume. This functionality is only available after you create a new policy and before you attempt a normal synchronization for the first time.



Policies

Add policy

Run	Data	Policy ▲	Last Known Good	Schedule	Source	Target	Actions
		sync1	-- --	Manual	/ifs/data	10.7.160.60 /ifs/data_sync	View reports View events Start Assess Reset Delete Disable

[1] In the policy-configuration content, specifying file criteria in a SyncIQ policy will slow down a copy or synchronization job. Using includes or excludes for directory paths does not affect performance, but specifying file criteria does.

Improved authentication integration

In prior OneFS versions, the UID/GID information was backed up and replicated to the target cluster. If you needed the target cluster to become the primary cluster, you had to restore the UID/GID information on the target cluster. SynclQ no longer requires this, since the UID/GID information has been replaced with SID numbers and is replicated with the metadata. The result is much easier transition and management.

Multiple jobs targeting a single directory tree no longer supported

In previous versions of OneFS, it was possible to create multiple SyncIQ jobs that pointed to the same target directory on the same target cluster.

Example:

If you wanted to replicate the source directory /ifs/data/users from the source cluster, except for one particularly large user folder like /ifs/data/users/ceo, you could set up two SynclQ policies that were essentially the same except the first job excluded the /ifs/data/users/ceo folder, and the second policy included only /ifs/data/users/ceo. This essentially split one policy into two separate policies, with the target at the same location.

This is not possible in prior OneFS versions due to a change in how the policy associations work. A valid configuration requires changing the target location, but this can create complications if you need to do a restore or failover.

Hard-link replication now supported

SynclQ creates hard links at the source as hard links on the target, including recombining any files that were split during prior SyncIQ version synchronizations.

Report changes

Reports are customized based on the type of job that is run. Reports generated for incremental synchronization are different from these reports:

- Initial synchronization
- Jobs that occurred during a pre-OneFS 6.5 run
- Jobs that occurred during the first run after a OneFS upgrade

SynclQ best practices and tips

Avoiding full dataset replications

Certain configuration changes will cause a replication job to run an initial full baseline replication as if it was running for the first time; that is, it will copy all data in the source path(s) whether or not the data has changed since the last run. Full baseline replication typically takes much longer than incremental synchronizations, so to optimize performance, avoid triggering full synchronizations when they are not necessary. Changes to the following parameters will cause this behavior:

- Source path(s): root path , include and exclude paths

- Source file selection criteria: type, time, and regular expressions

To prevent full dataset replications from occurring, avoid changing the file selection criteria on the source dataset.

Selecting the right source replication dataset

SyncIQ policies provide fine-grain control of the dataset you want to replicate, from determining what directories to include, or exclude, to creating file filtering regular expressions.

Including or excluding source-cluster directories

When you configure source-cluster settings in a SyncIQ policy, in addition to specifying a root directory on the source cluster, you can optionally include, or exclude, specific source-cluster directories.

By default, all files and folders under the specified root directory are synchronized to the target cluster. However, if you explicitly included any directories in the policy configuration, the system synchronizes only the files that are contained in that included directory to the target cluster. In addition, if you explicitly excluded any directories, those directories and any files contained in them, are not synchronized to the target cluster.

Any directories that you explicitly include must reside in, or under, the specified root directory. Consider a policy in which the specified root directory is /ifs/data. In this example, you could explicitly include the /ifs/data/media directory because it is under /ifs/data. When the associated policy runs, only the contents of the /ifs/data/media directory would be synchronized to the target cluster.

If you were to explicitly exclude a directory that is contained in the specified root directory, and you did not explicitly include any directories, only the contents of the excluded directory would not be synchronized to the target cluster.

If you were to both explicitly include directories and exclude directories, every explicitly included directory will be replicated and every other file, or directory, under the exclude directory will be excluded from the replication dataset.

For example, consider a policy in which the specified root directory is /ifs/data, and the following directories are explicitly included and excluded:

Explicitly included directories:

- /ifs/data/media/music
- /ifs/data/media/movies

Explicitly excluded directories:

- /ifs/data/media/music/working
- /ifs/data/media

In this example, excluding /ifs/data/media would exclude all directories below /ifs/data/media except those specifically included. Directories /ifs/data/media/pictures, /ifs/data/media/books, /ifs/data/media/games would be excluded because the directory /ifs/data/media was explicitly excluded. In other words, /ifs/data/media excludes all files under /ifs/data/media, except music and movies that are explicitly included.

Note: If you exclude a directory that contains the specified root directory, the exclude directory setting has no effect. For example, consider a policy in which the specified root directory is /ifs/data. Configuring a policy setting that excludes the /ifs directory would have no effect, and all contents of the specified root directory (In this example, /ifs/data) would be replicated to the target cluster.

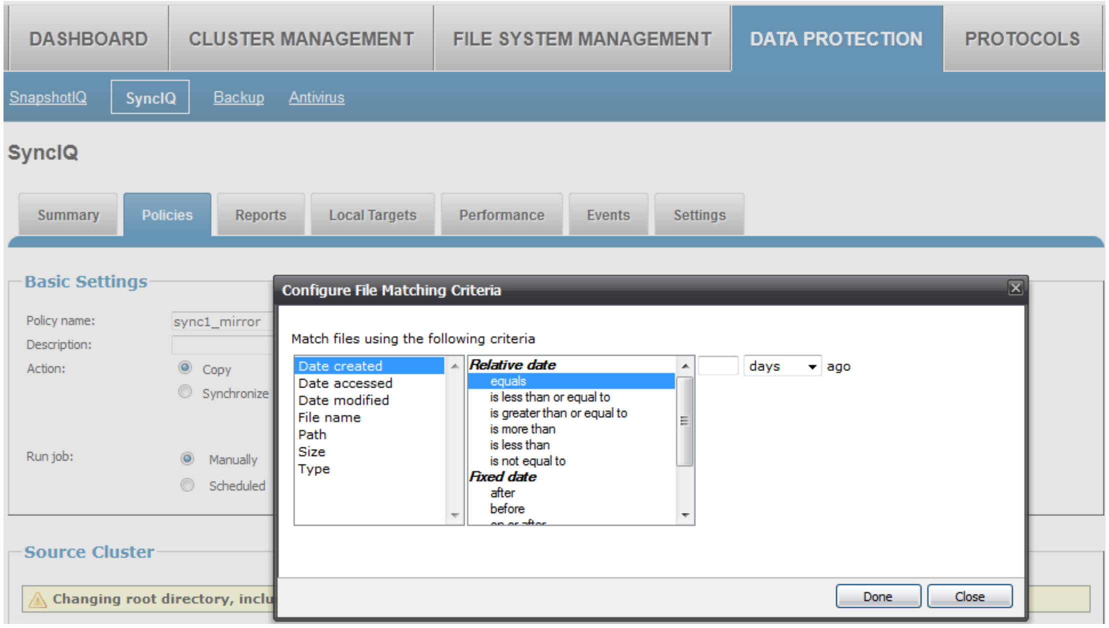
Configuring SyncIQ policy file selection criteria

For each SyncIQ policy, you can define file-criteria statements that explicitly include or exclude files from the policy action. A file-criteria statement can include one or more elements and each file-criteria element contains a file attribute, a comparison operator, and a comparison value. To combine multiple criteria elements into a criteria statement, use the Boolean 'AND' and 'OR' operators. You can configure any number of 'AND' and 'OR' file-criteria definitions.

You can include or exclude files based on the following predicates depending on whether the policy is defined as a Sync or Copy type.

Sync policies are more restrictive in the file selection criteria and include the following:

- You can use the wildcard characters *, ?, and [] or advanced POSIX regular expressions (regex). Regular expressions are sets of symbols and syntactic elements that match patterns of text. These expressions can be more powerful and flexible than simple wildcard characters. Isilon clusters support IEE E Std 1003.2 (POSIX.2) regular expressions. For more information about POSIX regular expressions, see the BSD man pages. For example:
- To select all files ending in .jpg, you could type *\.jpg$.
- To select all files with either .jpg or .gif file extensions, you could type *\.(jpglgif)$.
- You can also include or exclude files based on file size by specifying the file size in bytes, KB, MB, GB, TB, or PB. file sizes are represented in multiples of 1.024, not 1,000.
- You can include or exclude files based on the following type options: regular file, directory, or soft link. A soft link is a special type of POSIX file that contains a reference to another file or directory.



Policy name: sync1_mirror

Description:

Action: ● Copy ○ Synchronize

Run job: ● Manually ○ Scheduled

Changing root directory, inclu

Match files using the following criteria

Date created equals [ ] days ago

Figure 7. Policy advanced file selection options

Note: When managing a Sync type of policy, use care when modifying a file attributes comparison option and comparison values. With a Sync type of policy (not Copy type), modifying these settings will cause a re-sync and any non-matching files will be deleted from the target the next time the job runs.

Copy policies also allow you to select files based on file creation time, access time, and modification time.

Note: In the policy-configuration content, specifying file criteria in a SyncIQ policy will slow down a copy or synchronize job. Using includes or excludes for directory paths does not affect performance, but specifying file criteria does.

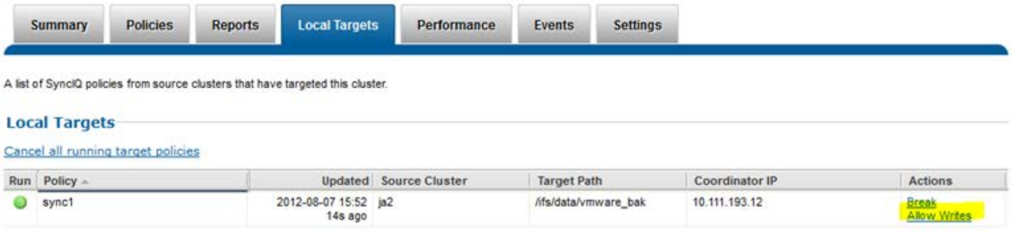
Disaster recovery from a target Isilon cluster

As described above, a common use for data replication using SyncIQ is for recovery from disasters at a local site. This can be achieved by either redirecting users to the target cluster or by re-creating the dataset on a local cluster with data replication from the target cluster.

Note: Isilon recommends using target cluster snapshots for disaster recovery.

You can meet specific recovery point objectives (RPO) and reduce recovery time objectives (RTO) by setting the right policy schedule interval and using target cluster snapshots. It is possible to accomplish RTO by either failing over to the target cluster, or replicating the necessary dataset from the remote cluster back to a local cluster.

To recover from a disaster and fail over to the target cluster, simply run the ‘Allow Writes” action on the appropriate Local Targets policy. Once complete, redirect clients to the target cluster.



A list of SyncIQ policies from source clusters that have targeted this cluster.

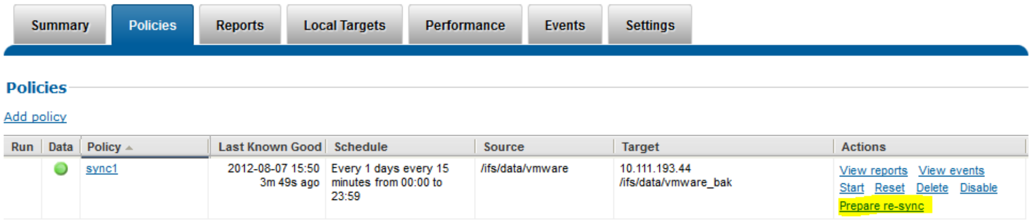
Local Targets

Cancel all running target policies

Run	Policy	Updated	Source Cluster	Target Path	Coordinator IP	Actions
●	sync1	2012-08-07 15:52 14s ago	ja2	/ifs/data/vmware_bak	10.111.193.12	Break Allow Writes

To recover from a disaster by failing back to the original source cluster take the following steps:

1. Prepare the source cluster for failback by running ‘prepare re-sync’ action on the appropriate SyncIQ policy.

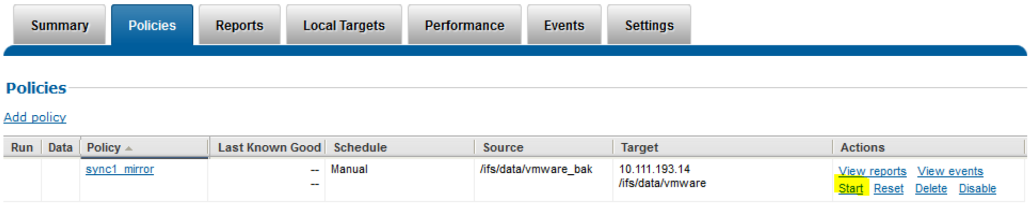


Policies

Add policy

Run	Data	Policy	Last Known Good	Schedule	Source	Target	Actions
	●	sync1	2012-08-07 15:50 3m 49s ago	Every 1 days every 15 minutes from 00:00 to 23:59	/ifs/data/vmware	10.111.193.44 /ifs/data/vmware_bak	View reports View events Start Reset Delete Disable Prepare re-sync

2. On successful completion of the failback prep, run a final failback differential sync on the appropriate mirror policy on target cluster.



Policies

Add policy

Run	Data	Policy	Last Known Good	Schedule	Source	Target	Actions
		sync1_mirror	-- --	Manual	/ifs/data/vmware_bak	10.111.193.14 /ifs/data/vmware	View reports View events Start Reset Delete Disable

3. Verify that the failback has completed, via the replication policy report, and redirect clients back to the source cluster A again. At this time, target cluster is automatically relegated back to its role a DR target.

Note: SyncIQ does not replicate cluster configurations such as shares and exports, quotas, snapshots, and networking settings, from the source cluster. Isilon does copy over UIO/GID ID mapping during replication. In the case of failover to the remote cluster, other cluster configuration must be configured manually. Please consult Isilon Technical Support for more information.

Performance tuning

SyncIQ uses a multi-worker intelligent job execution engine to take advantage of aggregate CPU and networking resources to address the needs of most data sets. However, in certain cases you may want to do further tuning.

Guidelines

Although no overarching formula exists for making changes to specific performance settings, a good methodology for optimizing performance is to use the following guidelines:

- Establish reference network performance by using common tools such as Secure Copy (scp) or NFS copy from cluster to cluster. This will provide a baseline for a single thread data transfer over the existing network.
- After creating a policy and before running the policy for the first time, use the policy assessment option to see how long it takes to scan the source cluster dataset with default settings.
- Increase workers per node in cases where network utilization is low, for example oyer WAN. This can help overcome network latency by haying more workers generate I/O on the wire. If adding more workers per node does not improve network utilization, avoid adding more workers because of diminishing returns and worker scheduling overhead.
- Increase workers per node in datasets with many small files to process more files in parallel. Be aware that as more workers are employed, more CPU is consumed, due to other cluster operations.
- Use file rate throttling to roughly control how much CPU and disk I/O SyncIQ consumes while jobs are running through the day.
- Remember that “target aware synchronizations” are much more CPU-intensive than regular baseline replication but they potentially yield much less network traffic if both source and cluster datasets are already seeded with similar data.
- Use SmartConnect IP address pools to control which nodes participate in a replication job and to avoid contention with other workflows accessing the cluster through those nodes.
- Use network throttling to control how much network bandwidth SyncIQ can consume through the day.

Limitations and restrictions

A SyncIQ source cluster can run up to five jobs at any given time, by default. Additional jobs are queued until a new job execution slot is available.

Note: SyncIQ can be used to cancel already queued jobs.

- The maximum number of workers per node per policy is eight and the default number of workers per node is three.
- The number of workers per job is a product of the number of workers per node setting multiplied by the number of nodes of the smallest cluster participating in a job (which defaults to all nodes unless a SmartConnect IP address pool is used to restrict the number of participating nodes to a job). For example, if the source cluster has 6 nodes, the target has 4 nodes and the number of workers per node is 3, the total worker count will be 12.
- The maximum number of workers per job is 40. At any given time, 200 workers could potentially be running on the cluster (5 jobs with 40 workers each).

- If a user sets a limit of 1 file per second, each worker gets a ration rounded up to the minimum allowed (1 file per second). If the limit is ‘unlimited’, all workers are unlimited, and if the limit is zero (stop), all workers get zero.
- On the target cluster, there is a limit of configurable workers per node (sworkers) to avoid overwhelming the target cluster if multiple source clusters are replicating to the same target cluster. This is set to 100 workers by default, and is controlled via the ‘max-sworkers-per-node’ parameter. Contact Isilon Technical Support if load on the target cluster, generated by incoming SyncIQ jobs, needs to be adjusted.

Using Isilon SnapshotIQ on the target

By default, taking snapshots on the target cluster is not enabled. To enable snapshots on the target cluster, you must acquire a SnapshotIQ license and activate it on the target cluster.

When SyncIQ policies are set with snapshots on the target cluster, on the initial sync a snapshot will be taken at the beginning and the end. For incremental syncs, a snapshot will only be taken at the completion of the job.

Note: Prior to initializing a job, SyncIQ will first confirm SnapshotIQ is licensed on the target cluster. If SnapshotIQ is not licensed on the target cluster, the job will proceed, but it will not generate a snapshot on the target cluster and SyncIQ will issue an alert to that effect.

You can control how many snapshots of the target replication path are maintained over time by defining an expiration period on each of the target-cluster snapshot. For example, if you execute a replication job every day for a week (with target snapshots enabled), you will have seven snapshots of the dataset on the target cluster, representing seven versions of the dataset from which to choose.

In this example, if you choose to make the target-cluster snapshot expire after seven days on a replication policy that is executed once per day, only seven snapshots will be available on the target cluster dataset.

Using SmartConnect with SyncIQ

In most cases, SyncIQ replication uses the full set of resources on the cluster (that is, all nodes in the cluster participate in the job). In cases where you want to limit (and control) which nodes in the cluster should participate in SyncIQ jobs, use SmartConnect to achieve this.

Using SmartConnect on the source cluster

On the source cluster, you can create a SmartConnectIP address pool and assign the IP address pool forthe source cluster:

1. Create or use an existing SmartConnect IP address pool in the desired subnet.
2. If the SmartConnect IP address pool was created exclusively to integrate with SyncIQ, you do not need to allocate an IP range for this pool. Simply leave the IP range fields empty.

3. After a node appears in the SmartConnect IP address pool, SyncIQ will use network interfaces based on the standard routing on that node to connect with the target cluster.

Note: By default, SyncIQ uses all interfaces in the nodes that belong to the IP address pool disregarding any interface membership settings in the pool. If you want to restrict SyncIQ to use only the interfaces in the IP address pool, use the following command line interface commands to modify the SyncIQ policy: isi sync policy modify --policy <my_policy> --force_interface=on

---

Using SmartConnect zones on the target cluster

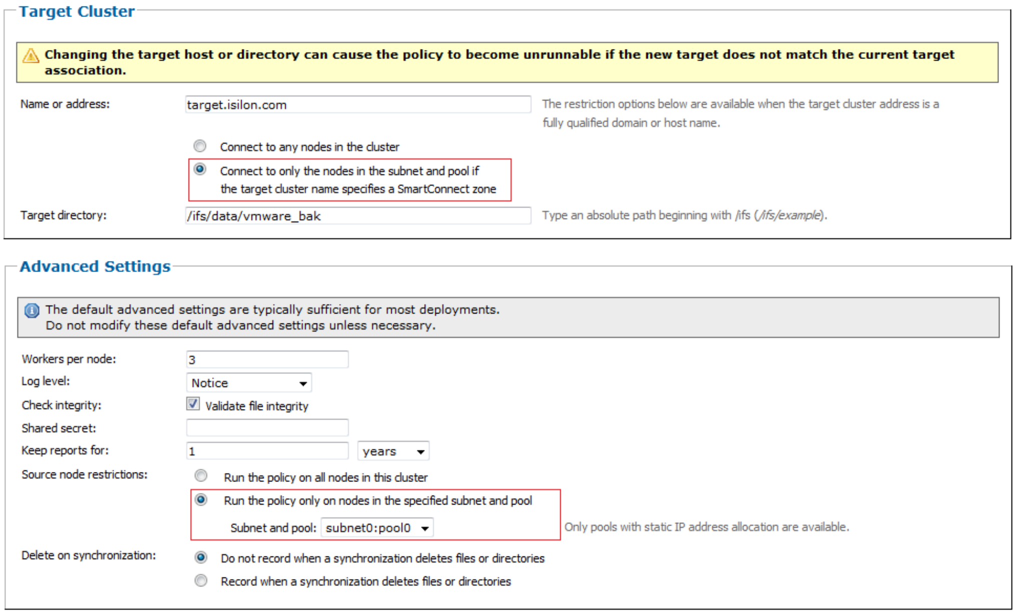
When you set a policy target cluster name or address, you can use a SmartConnect DNS zone name instead of an IP address or a DNS name of a specific node. If you choose to restrict the connection to nodes in the SmartConnect zone, the replication job will only connect with the target cluster nodes assigned to that zone. During the initial part of a replication job, SyncIQ on the source cluster will establish an initial connection with the target cluster using SmartConnect. Once connection with the target cluster is established, the target cluster will reply with a set of target IP addresses assigned to nodes restricted to that SmartConnect zone. SyncIQ on the source cluster will use this list of target cluster IP addresses to connect local replication workers with remote workers on the target cluster.

The basic steps are:

1. On the target cluster, create a SmartConnect zone using the cluster networking UI.
2. Add only those nodes that will be used for SyncIQ to the newly created zone.
3. On the source cluster, SyncIQ replication jobs (or global settings) specify the SmartConnect zone name as the target server name.

Note: SyncIQ does not support dynamic IPs in SmartConnect IP address pools. If dynamic IPs are specified, the replication job will fail with an error message in the log file and an alert.

You can find more information on how to configure SmartConnect zones in the Isilon Administration web interface.



Target Cluster

⚠ Changing the target host or directory can cause the policy to become unrunnable if the new target does not match the current target association.

Name or address: target.isilon.com

The restriction options below are available when the target cluster address is a fully qualified domain or host name.

○ Connect to any nodes in the cluster

● Connect to only the nodes in the subnet and pool if the target cluster name specifies a SmartConnect zone

Target directory: /ifs/data/vmware_bak

Type an absolute path beginning with /ifs (/ifs/example).

Advanced Settings

The default advanced settings are typically sufficient for most deployments.
Do not modify these default advanced settings unless necessary.

Workers per node: 3

Log level: Notice

Check integrity: ☑ Validate file integrity

Shared secret:

Keep reports for: 1 years

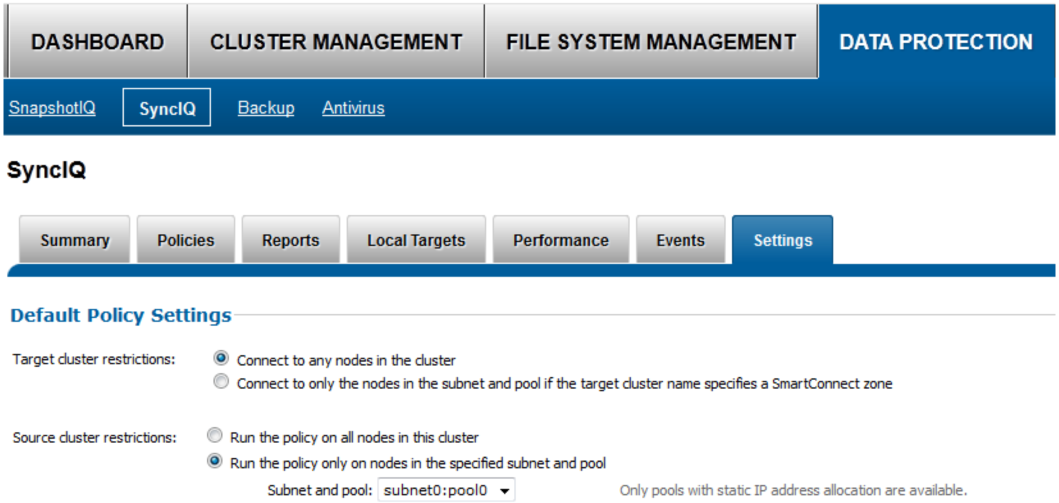
Source node restrictions:
○ Run the policy on all nodes in this cluster
● Run the policy only on nodes in the specified subnet and pool
Subnet and pool: subnet0:pool0

Only pools with static IP address allocation are available.

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

Figure 8. SyncIQ policy-specific SmartConnect integration

While you can set these settings per SyncIQ policy, often it is more useful to set them globally in the SyncIQ Settings page as shown below. Those settings will be applied by default to new policies unless you override them on a per-policy basis. However, changing these global settings will not affect existing policies.



SyncIQ

Default Policy Settings

Target cluster restrictions:
● Connect to any nodes in the cluster
○ Connect to only the nodes in the subnet and pool if the target cluster name specifies a SmartConnect zone

Source cluster restrictions:
○ Run the policy on all nodes in this cluster
● Run the policy only on nodes in the specified subnet and pool
Subnet and pool: subnet0:pool0

Only pools with static IP address allocation are available.

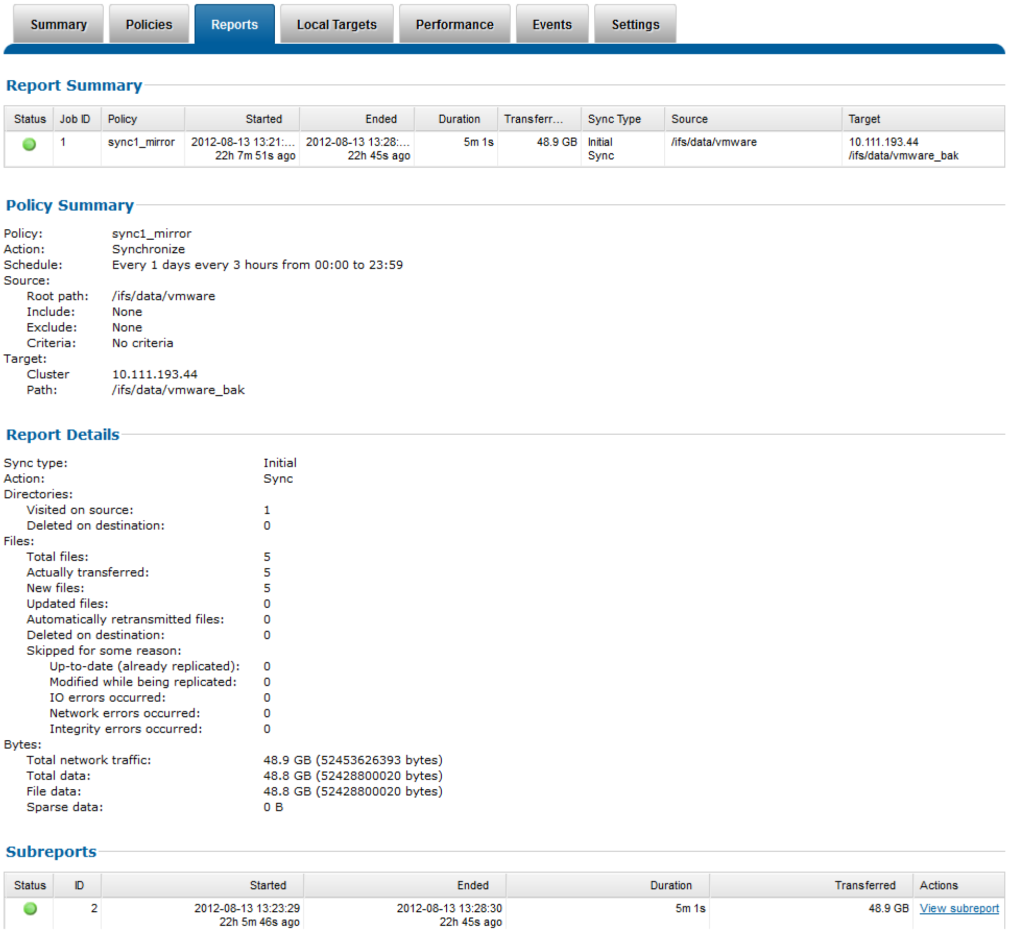
Figure 9. SyncIQ global settings for SmartConnect integration

Monitoring SyncIQ

In addition to including cluster-wide performance monitoring tools, such as the “isi statistics" command line interface or the new Isilon InsightIQ software module, SyncIQ includes module-specific performance monitoring tools. For information on "isi statistics" and InsightIQ, please refer to the product documentation and Isilon knowledge base.

Policy job monitoring

For high-level job monitoring, use the SyncIQ Summary page where job duration and total dataset statistics are available. The Summary page includes currently running jobs, as well as reports on completed jobs. For more information on a particular job, click the “View Details” link to review job-specific data sets and performance statistics. You can use the Reports page to select a specific policy that was run within a specific period and completed with a specific job status.



Report Summary

Status	Job ID	Policy	Started	Ended	Duration	Transferr...	Sync Type	Source	Target
●	1	sync1_mirror	2012-08-13 13:21:... 22h 7m 51s ago	2012-08-13 13:28:... 22h 45s ago	5m 1s	48.9 GB	Initial Sync	/ifs/data/vmware	10.111.193.44 /ifs/data/vmware_bak

Policy Summary

```
Policy:         sync1_mirror
Action:         Synchronize
Schedule:       Every 1 days every 3 hours from 00:00 to 23:59
Source:
    Root path:  /ifs/data/vmware
    Include:    None
    Exclude:    None
    Criteria:   No criteria
Target:
    Cluster     10.111.193.44
    Path:       /ifs/data/vmware_bak
```

Report Details

```
Sync type:                                   Initial
Action:                                      Sync
Directories:
    Visited on source:                       1
    Deleted on destination:                  0
Files:
    Total files:                             5
    Actually transferred:                    5
    New files:                               5
    Updated files:                           0
    Automatically retransmitted files:       0
    Deleted on destination:                  0
    Skipped for some reason:
        Up-to-date (already replicated):     0
        Modified while being replicated:     0
        IO errors occurred:                  0
        Network errors occurred:             0
        Integrity errors occurred:           0
Bytes:
    Total network traffic:                   48.9 GB (52453626393 bytes)
    Total data:                              48.8 GB (52428800020 bytes)
    File data:                               48.8 GB (52428800020 bytes)
    Sparse data:                             0 B
```

Subreports

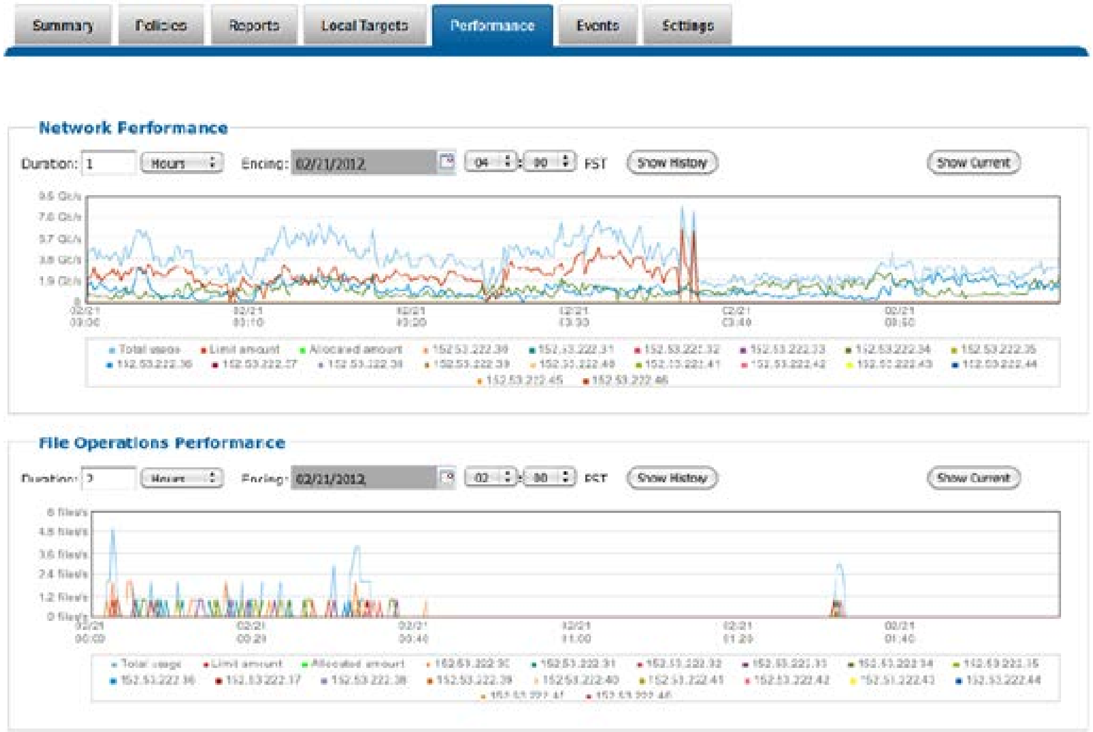
Status	ID	Started	Ended	Duration	Transferred	Actions
●	2	2012-08-13 13:23:29 22h 5m 46s ago	2012-08-13 13:28:30 22h 45s ago	5m 1s	48.9 GB	View subreport

Figure 10. SyncIQ policy Job report

In addition to the Summary and Reports pages, the Alerts page displays SyncIQ specific alerts extracted from the general-purpose cluster Alerts system.

Performance monitoring

For performance tuning purposes, use the SyncIQ Performance page. On this page, you can review network utilization and files processing rate and you can control the network and CPU usage. When reviewing real-time or historical graphs you can control the starting time and time interval to provide the level of detail you need. The graphs display both cluster-wide performance and per-node performance. Based on this information you can set network and file processing threshold limits (to limit CPU usage). These limits are cluster-wide and are shared across jobs running simultaneously.



Network Performance: Duration: 1 Hours Ending: 02/21/2012 04 : 00 PST

File Operations Performance: Duration: 2 Hours Ending: 02/21/2012 02 : 00 PST

Figure 11. Performance monitoring

Roles Based Administration

Roles Based Administration is a cluster management access control system (RBAC) that divides up the powers of the “root” and “administrator” users into more granular privileges, and allows assignment of these to specific roles. For example, data protection administrators can easily be assigned full access to SyncIQ configuration and control, but only read-only access to the remaining functionality of the cluster. Roles Based Administration is integrated with the SyncIQ command line interface, WebUI and Platform API.

Automation via the OneFS Platform API

The OneFS Platform API provides a RESTful programmatic interface to SyncIQ, allowing automated control of cluster replication. The Platform API is integrated with Roles Based Administration (described above) providing a granular authentication framework for secure, remote SyncIQ administration via the scripting language of your choice.

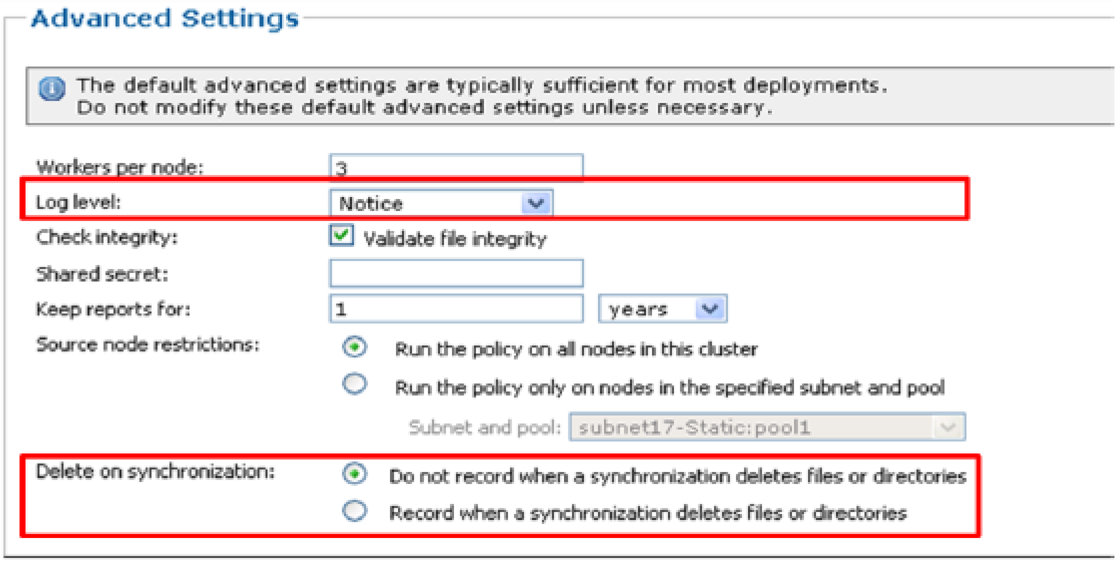
Troubleshooting with SyncIQ logs

To get more detailed job information for troubleshooting purposes, please review the SynclQ log files. If necessary, you can log into the appropriate node through the command line interface and view the node's /var/log/isi_migrate.log file. The output detail depends on the log level, configured under a policy’s “advanced settings”:

- Error: Logs only events related to specific types of failures.

- Notice: Logs job-level and process-level activity, including job starts and stops, as well as worker coordination information. This is the default log level and is recommended for most SyncIQ deployments.
- Network Activity: Logs expanded job-activity and work-item information, including specific paths and snapshot names.
- File Activity: Logs a separate event for each action taken on a file. Please do not enable this logging level without assistance from Isilon Technical Support.

You can also choose to record log information on files deleted from the target cluster during synchronization jobs (these files are deleted from the target cluster when they are no longer present on the source cluster).



Advanced Settings

The default advanced settings are typically sufficient for most deployments.
Do not modify these default advanced settings unless necessary.

Workers per node: 3

Log level: Notice

Check integrity: ☑ Validate file integrity

Shared secret:

Keep reports for: 1 years

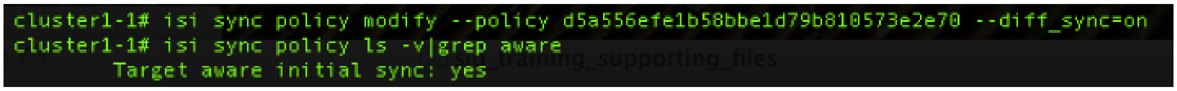
Source node restrictions:
● Run the policy on all nodes in this cluster
○ Run the policy only on nodes in the specified subnet and pool
Subnet and pool: subnet17-Static:pool1

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

Figure 12. SyncIQ policy log level and synchronization log settings

Target aware initial synchronization

In situations where most of the dataset already resides on both clusters, target aware initial synchronizations are designed as a one-time manual replication job. Once run, you should disable the target aware initial synchronization so that normal replication can proceed. If you do not disable it, incremental replications will continue with normal replication; however, if any changes occur to the policy definition (triggering a baseline replication), the system will use a target aware initial synchronization instead of a normal full baseline replication.



```
cluster1-1# isi sync policy modify --policy d5a556efe1b58bbe1d79b810573e2e70 --diff_sync=on
cluster1-1# isi sync policy ls -v|grep aware
        Target aware initial sync: yes
```

Figure 13. Enabling target aware initial synchronization via the CLI

Note: Target aware initial synchronization consumes CPU on both source and target clusters (comparing hashes of file blocks). It is an advanced feature only available through the command line and should be used only in specific cases as described in this paper. Please contact Isilon Technical Support for more information.

Failover dry-run testing

To easily test SyncIQ's failover functionality (described in a previous chapter), the allow_write command features a 'revert' option. This makes it easy to switch the target cluster back to its previous state:

```
isi sync target allow_write –-revert [policy]
```

Version compatibility

The target cluster must be running the same or higher OneFS version as the source(s) so that it can accept replication from a source cluster with earlier OneFS versions. To enable SyncIQ Automated Failover and Failback functionality, both clusters must be running OneFS 7.0.

Note: Upgrade the target cluster before upgrading the source cluster to ensure no interruptions to replication jobs occur as part of the upgrade process.

Additional tips

- Do not specify a target password unless you create the required password file on the target cluster. (This is not the same password as either cluster's root password.) Setting a target cluster password is useful if you want to verify that the source cluster is replicating to the right target cluster.

  Note: There can be only one password per target cluster. All replication policies to the same target cluster must be set with the same target cluster password.

- Do not use hyphens or other special characters in bandwidth or throttle rules.
- When administering or executing SyncIQ jobs remotely over SSH, install SSH client certificates on the Isilon cluster to avoid having to enter the user password for every policy job.

Conclusion

SynclQ continues to define the parallel asynchronous replication space for modern data architectures. With snapshot integration, SynclQ performance allows customers to protect data faster, failover and failback easier, and dramatically improve their Recovery Objectives. This performance enhancement - combined with SynclQ's integration with OneFS, native storage tiering, point-in-time snapshots, retention, and leading backup solutions—makes SynclQ a powerful, flexible, and easy-to-manage solution for disaster recovery, business continuance, disk-to-disk backup, and remote disk archive.

About EMC Isilon

Isilon, a division of EMC, is the global leader in scale-out NAS. We deliver powerful yet simple solutions for enterprises that want to manage their data, not their storage. Isilon products are simple to install, manage and scale, at any size and, unlike traditional enterprise storage, Isilon stays simple no matter how much storage is added, how much performance is required, or how business needs change in the future. We're challenging enterprises to think differently about their storage, because when they do, they'll recognize there’s a better, simpler way. Learn what we mean at www.isilon.com.

Contact EMC Isilon

http://www.isilon.com

505 1st Avenue South, Seattle, WA 98104

Toll-Free: 877-2-ISILON • Phone: +1-206-315-7602

Fax: +1-206-315-7501 • Email: sales@isilon.com