Abstract
This white paper will give you an understanding of the key features and benefits of EMC Isilon SyncIQ software. SyncIQ is an application that enables you to flexibly manage and automate data replication between two Isilon clusters. This paper outlines best practices and use cases to help you maximize the benefits of cluster-to-cluster replication.

February 2016
Table of Contents

Introduction ......................................................................................... 5  
Fast, reliable file-based replication .................................................... 5  

SyncIQ Primary Uses ......................................................................... 6  
Disaster recovery .............................................................................. 7  
Business continuance ...................................................................... 7  
Disk-to-disk backup and restore ......................................................... 8  
Remote archive ............................................................................... 8  

Architecture and functionality .......................................................... 8  
Leveraging clustered storage architecture ......................................... 8  
Asynchronous source-based replication .............................................. 9  
Continuous Replication Mode ............................................................ 10  
Snapshot Triggered Replication .......................................................... 11  
Flexible, policy-driven replication ....................................................... 12  
Efficient block-based deltas ............................................................... 13  
Source-cluster snapshot integration .................................................... 13  
Application consistent replication ...................................................... 14  
Target-cluster snapshots .................................................................. 15  
SmartConnect integration ................................................................ 15  
SyncIQ Replication and SmartDedupe ............................................... 16  
Target Aware Initial Sync (Differential Sync) ..................................... 17  
Tunable replication performance ......................................................... 17  
Real-time monitoring and historical reports ....................................... 17  
Policy assessment ........................................................................... 17  

SyncIQ Data Failover and Failback .................................................. 18  
Failover and Failback ....................................................................... 18  
Failover ......................................................................................... 19  
Failback ....................................................................................... 19  

SyncIQ Features ................................................................................. 21  
Performance .................................................................................. 21  
Snapshot integration removes need for treewalks ............................. 21  
Handling of deleted and moved files in a copy policy .......................... 22  
Source and target cluster association persistence ............................... 23  
Target protection with restricted writes – Replication Domains ........... 23  
Policy priority ................................................................................ 23  
Assess SyncIQ changes ................................................................ 24  
RPO Alert ...................................................................................... 24  
Authentication integration ................................................................. 25  
Multiple Jobs targeting a single directory tree not supported .............. 25  
Hard-link replication ...................................................................... 26  

SyncIQ Best Practices and Tips .......................................................... 26
# Best Practice for Data Replication with EMC Isilon SyncIQ

- Avoiding full dataset replications .................................................. 26
- Selecting the right source replication dataset ............................... 26
  - Including or excluding source-cluster directories ....................... 26
- Configuring SyncIQ policy file selection criteria .......................... 27
- Performance tuning ...................................................................... 28
- Guidelines ................................................................................. 28
- Scalability of SyncIQ performance .............................................. 29
- Using Isilon SnapshotIQ on the target ........................................ 31
- Using SmartConnect with SyncIQ ............................................. 32
- Monitoring SyncIQ ..................................................................... 33
  - Policy Job monitoring ............................................................. 34
  - Performance monitoring ......................................................... 34
- Roles Based Administration .......................................................... 36
- Automation via the OneFS Platform API ...................................... 36
- Troubleshooting with SyncIQ logs ............................................ 36
- Target aware initial synchronization .......................................... 37
- Failover Dry-run Testing ............................................................... 37

**Version compatibility** ................................................................ 37

**SyncIQ Licensing** ................................................................. 38

**Additional tips** ....................................................................... 38

**Conclusion** ............................................................................ 39

**About EMC** ............................................................................ 39
**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 to provide a solid foundation for disaster recovery. SyncIQ can send and receive data on every node in an Isilon cluster, taking advantage of any available network bandwidth, so replication performance increases as your data store grows. Because both the replication source and target can scale to multiple petabytes without fragmentation into multiple volumes or file systems, data replication starts and remains a simple process.

---

![SyncIQ parallel replication](image)

*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 is defined to protect the data required for each major recovery point objective (RPO) 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 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 non-current data that needs to be retained so you can reclaim valuable capacity in your production system.

SyncIQ can be tailored to use as much or as little system resource and network bandwidth as you specify, and the sync jobs can be scheduled to run at any time, in order to minimize the impact of the replication on production systems.

**SyncIQ Primary Uses**

Isilon SyncIQ offers powerful, efficient, and easy-to-manage data replication for the following business requirements:

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

Figure 2 shows the typical SyncIQ architecture – replicating data from a primary to a secondary Isilon cluster which can be local or remote. SyncIQ can also use the primary cluster as a target in order to create local replicas. In this scenario, efficient data transfer flows across the cluster’s InfiniBand back-end.
SyncIQ replication can also be configured in a hub-and-spoke topology, where a single source replicates to multiple targets (or many to one), and in a cascading topology, where each cluster replicates to the next in a chain.

SyncIQ provides the power and flexibility for the protection requirements of data-intensive, workflows and applications.

**Disaster recovery**

Disaster recovery requires quick and efficient replication of critical business data to a secondary site.

SyncIQ 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. SyncIQ 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. SyncIQ’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). SyncIQ can also be used in concert with EMC Isilon SnapshotIQ software, which allows you to store point-in-time snapshots of your data in order to support secondary activities like backup to tape.
Disk-to-disk backup and restore

Enterprise IT organizations face increasingly complex backup environments with costly operations, shrinking backup and restore windows, and stringent service-level agreement (SLA) requirements. Backups to tape are traditionally slow and hard to manage as they grow, compounded by the size and rapid growth of digital content and unstructured data. SyncIQ, as a superior disk-to-disk backup and restore solution delivers scalable 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 frequently accessed enough to justify maintaining it on production storage, replicate it with SyncIQ to a secondary site and reclaim the space on your primary system. Using a SyncIQ copy policy, data can be deleted on the source without affecting the target, leaving 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

SyncIQ leverages the full complement of resources in an Isilon cluster and the scalability and parallel architecture of the EMC Isilon OneFS® file system. SyncIQ uses a policy-driven engine to execute replication jobs across all nodes in the cluster. Multiple policies can be defined to allow for high flexibility and resource management. Each SyncIQ 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 SyncIQ job is initiated (from either a scheduled or manually applied policy), the system first takes a snapshot of the data to be replicated. SyncIQ compares this to the snapshot from the previous replication job to quickly identify the changes that need to be propagated. Those changes can be new files, changed files, metadata changes, or file deletions. SyncIQ 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 in the policy.

Replication workers on the source cluster are paired with workers on the target cluster to accrue the benefits of parallel and distributed data transfer. As more jobs run concurrently, SyncIQ 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. There are significant changes in the way workers are allocated in OneFS 8.0 compared with earlier OneFS versions. These are detailed later in this paper.

SyncIQ is configured through the OneFS WebUI, providing a simple, intuitive method to create policies, manage jobs, and view reports. In addition to the web-based interface all SyncIQ functionality is integrated into the OneFS command line interface. For a full list of all commands, run `isi sync --help`

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.

To protect distributed workflow data, SyncIQ prevents changes on target directories. 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.
Continuous Replication Mode

In addition to the manual and scheduled replication policies, OneFS 7.1 and higher offers SyncIQ continuous mode, or replicate on change. When the “Whenever the source is modified” policy configuration option is selected (or --schedule when-source-modified on the CLI), SyncIQ will continuously monitor the replication data set and automatically replicate changes to the target cluster. Continuous replication mode is applicable when you want the secondary data copy to be always consistent with the primary source, or if data changes at unpredictable intervals. Use caution when selecting this option, as it can trigger a large amount of replication traffic and snapshot traffic if the data is very volatile.

Figure 4 SyncIQ Continuous Replication Policy Configuration

Events that trigger replication include file additions, modifications and deletions, directory path, and metadata changes. SyncIQ checks the source directories every ten seconds for changes.
Before OneFS 8.0, jobs in Continuous Replication mode execute immediately a change is detected. OneFS 8.0 introduces a policy parameter to delay the replication start for a specified time after the change is detected. This allows a burst of updates to a data set to be propagated more efficiently in a single replication event rather than triggering multiple events. To enable the delay for a continuous replication policy, specify the delay period in the Change-Triggered Sync Job Delay option on the GUI as shown in Figure 4 above, or specify `--job-delay <duration>` on the CLI.

**Snapshot Triggered Replication**

In OneFS 8.0, a SyncIQ policy can be configured to trigger when the administrator takes a snapshot matching a specified pattern. If this option is specified, the administrator-taken snapshot will be used as the basis of replication, rather than generating a system snapshot. This capability can be useful for replicating data to multiple targets – these can all be simultaneously triggered when a matching snapshot is taken, and only one snapshot is required for all the replications. To enable this behavior, select the “Whenever a snapshot of the source directory is taken” policy configuration option on the GUI, or use `--snapshot-sync-pattern <string>` on the CLI.
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 which needs to be protected. 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 section SyncIQ Best Practices and Tips includes guidance on how to avoid full baseline replication when changing a policy definition.

- When a file or an entire directory at the source of a replicated dataset moves to a new location in the dataset, it is moved on the target as well. In SyncIQ before 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. Subsequent changes to the file system while the job is in progress will not be propagated; those changes will be picked up the next time the job runs. OneFS creates instantaneous snapshots before the job begins – applications remain online with full data access 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 associated ‘latest’ snapshot is deleted and the previous ‘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. Only the SyncIQ license is required.

**Note:** Deleting a SyncIQ policy also deletes all snapshots created by that policy.
Before OneFS 8.0, the snapshot is always taken for scheduled jobs, even if no data changes have occurred since the previous execution. In OneFS 8.0, you can set a policy parameter so that SyncIQ checks for changes since the last replication as the first step in the policy. If there are no changes, no further work will be done on that policy iteration, and the policy will report as “skipped”. If there are changes, the source data snapshot will be taken and the policy will proceed. This capability reduces the amount of work performed by the cluster if there is no changed data to be replicated. To enable this behavior, check “Only run if source directory contents are modified” on the WebUI, or specify `--skip-when-source-unmodified true` on the CLI.

**Application consistent replication**

To create application consistent replication, you can integrate the replication job with third-party application agents that can execute the replication job remotely by using the SyncIQ CLI.

For example, a VMware vSphere environment 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 through OneFS’ vSphere VAAI and VASA integration.

![Figure 7 SyncIQ VMware integration](image-url)
Target-cluster snapshots

In addition to the automatic OneFS snapshots created on the source cluster for point-in-time consistency, a snapshot is also generated on the target cluster at the end of each replication job, for use in the event of a failover. Only the most recent target-side snapshot is retained by default.

Optionally, additional snapshots can be taken on the target, with a user-specified retention period. These are known as target-cluster snapshots, and create multiple versions of the replicated dataset to choose from on the target cluster. A **SnapshotIQ module license is required on the target cluster in order to generate target-cluster snapshots.** These snapshots can be used for archival purposes - by using a near-line Isilon cluster (such as an Isilon NL-Series) to maintain different versions of replicated datasets archived from primary Isilon storage (S-Series or X-Series Isilon clusters).

To enable target-cluster snapshots, select “Enable capture of snapshots on the target cluster” in the GUI or use the --target-snapshot-archive options in the CLI.

![Figure 8 SyncIQ target-cluster snapshot enablement](image)

SmartConnect integration

SyncIQ uses the standard Ethernet cluster node ports to send replication data from the source to the target cluster. By selecting a predefined 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.

You can use a single SmartConnect IP address pool globally across all policies, 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.
Figure 9 Constrain SyncIQ Policies to SmartConnect Zones

**Note:** Changing the default policy global settings only affects newly created policies; existing policies will not be modified.

**SyncIQ Replication and SmartDedupe**

When deduplicated files are replicated to another Isilon cluster via SyncIQ, or backed up to a tape device, the deduplicated files are inflated (or rehydrated) back to their original size, since they no longer share blocks on the target Isilon cluster. SmartDedupe can be run on the target cluster after the replication is complete to provide the same space efficiency benefits as on the source.

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 on target clusters or tape devices, it is important to verify that the total amount of storage space saved and storage space consumed does not exceed the available space on the target cluster or tape device. 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 post-replication, via a deduplication job running on the target cluster.
Target Aware Initial Sync (Differential Sync)

The Target Aware Initial Sync feature, available only via the CLI, can 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. When enabled, a differential sync, rather than full or incremental is performed. Differential (target-aware) sync is often used when the association between the policy and target has been broken and is then re-established, since the majority of the data is likely already present on the target.

To enable target aware initial synchronization, use the following command:

```
# isi sync policies modify <policy_name> --target-compare-initial-sync=on
```

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 optimal for certain datasets or for the processing needs of the business. CPU and network use are set to ‘unlimited’ by default. However, SyncIQ allows you to control how resources are consumed and balance replication performance with other file system operations by implementing a number of cluster-wide controls. You can create rules for how much bandwidth SyncIQ uses and the rate at which it processes files for different time periods.

SyncIQ in OneFS 8.0 implements two additional rule types: CPU - to limit the CPU utilization to a percentage of the total available, and workers - to limit the number of workers available to a percentage of the maximum possible. These performance rules will apply to all policies executing during the specified time interval. An individual policy can also have a limit on the number of workers per node. As described in the section SmartConnect integration, you can limit the nodes on which a particular policy will run to a selected subnet and node pool.

Real-time monitoring and historical reports

SyncIQ 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

SyncIQ can conduct a trial run of your policy without actually transferring file data between locations. SyncIQ can scan the dataset and provide a detailed report of how many files and directories were scanned, and how many bytes of data would be transferred.
Note: From OneFS 6.5 onwards, a policy assessment can be run only before a policy has been run for the first time.

SyncIQ Data Failover and Failback

Failover and Failback

Failover is the process of directing client I/O from the primary to the secondary cluster, in the event of a planned or unplanned outage to the primary cluster. SyncIQ provides built-in recovery to the secondary cluster with minimal interruption to clients. By default, the RPO (recovery point objective) is to the last completed SyncIQ replication point. Optionally with the use of SnapshotIQ, multiple recovery points can be made available.

The administrator makes the decision to redirect client I/O to the mirror and initiates SyncIQ failover on the disaster recovery (secondary) cluster. Users continue to read and write to the secondary cluster while the primary cluster is repaired.

Once the primary cluster becomes available again, the administrator decides when to revert client I/O back to it. To achieve this, the administrator initiates a SyncIQ failback, which synchronizes any incremental changes made to the secondary cluster during failover back to the primary. When complete, the administrator redirects client I/O back to the original cluster again.

Figure 10 SyncIQ Data Failover and Failback

SyncIQ supports unplanned failover and failback, as well as controlled, proactive cluster failover and failback. A planned failover/failback is useful for:

- Disaster recovery test and validation.
- Performing planned cluster maintenance.
This section provides a summary of the failover and failback processes. A detailed set of instructions, with validation steps included, is contained in the KB “What are the CLI steps for SyncIQ failover and failback”.

Consider 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. For simplicity, we show the failover for one policy – if there are multiple policies, repeat the process for each policy.

**Failover**

The data must be prepared for failover the very first time that the policy runs. This step only needs to be performed once for a policy and can take some time - several hours or more. This step marks the data in the source directory to indicate it is part of the failover domain. It is recommended to execute this command before the first failover is required, to avoid extending the failover time.

```bash
# isi job start domainmark -root=<patm> --dm-type=synciq
```

In OneFS 8.0, the domainmark process can be run automatically in advance, rather than requiring it to be explicitly run as previously described. To enable this behavior, set the `--accelerated-failback true` option either on policy creation or subsequently by modifying the policy, or select “Prepare Policy for Accelerated Failback Performance” in the Advanced Settings for the policy in the GUI. The domainmark job will run implicitly the next time the policy syncs with the target. Note this will increase the overall execution time of the sync job.

To initiate failover, set the target cluster B ‘sync1’ replica to read-write:

```bash
# isi sync recovery allow-write --policy-name=sync1
```

The clients can now be redirected to the target cluster. Note that SyncIQ replicates data – it does not replicate configuration information such as SMB shares, NFS exports, Active Directory and authentication providers.

**Failback**

Failback may occur almost immediately, in the event of a functional test, or more likely, after some elapsed time during which the issue which prompted the failover can be resolved. Updates to the dataset while in the failover state will almost certainly
have occurred, therefore the failback process must include propagation of these back to the source.

Failback consists of three phases. Each phase should complete before proceeding.

1. Run the preparation phase (resync-prep) on the source cluster A to ready it to receive intervening changes from the target cluster. This phase creates a read-only replication domain, restores the last known good snapshot and creates a SyncIQ policy on the target policy appended with '_mirror', that is used to failback the dataset. During this phase, clients are still connected to the target:

   ```bash
   # isi sync recovery resync-prep --policy-name=sync1
   ```

2. Run the mirror policy created in the previous step to sync the most recent data to the source cluster.

   ```bash
   # isi sync jobs start -policy=sync1_mirror
   ```

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

   ```bash
   # isi sync reports list sync1_mirror
   ```
Note: SyncIQ Failover and Failback does not replicate cluster configurations such as SMB shares and NFS 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. An application like Superna EyeGlass can be used to replicate the configuration information.

Note: SyncIQ Failover and Failback is not supported for SmartLock protected directories before OneFS 8.0. In OneFS 8.0, SmartLock enterprise directories can use failover and failback using the same SyncIQ commands. This does not apply to SmartLock Compliance directories – these cannot run failover or failback.

SyncIQ Features
SyncIQ uses parallelism to optimize replication times, protects replicated data against accidental alteration and deletion, and improves source and target association persistence. This section explains some of these underlying implementation details of SyncIQ.

Performance
SyncIQ is designed and periodically enhanced to minimize its impact on cluster performance will be minimized. Some of the more significant architectural features related to performance optimization 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 (no SnapshotIQ license is required for this functionality. When a SyncIQ job starts, if a previous source-cluster snapshot is detected, 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. Comparing two snapshots to detect these changes is a much more lightweight operation than walking the entire file tree, resulting in significant gains for incremental synchronizations subsequent to the initial full replication.

If there is no previous source-cluster snapshot (for example, if a SyncIQ job is running for the first time), a full replication will be necessary.

When a SyncIQ job completes, the system deletes the previous source-cluster snapshot, retaining the most recent snapshot to be used as the basis for comparison on the next job iteration.
Handling of deleted and moved files in a copy policy

SyncIQ provides two types of replications policies: synchronization policies and copy policies. Data replicated with a synchronization policy will be maintained on the target cluster exactly as it is on the source – files deleted on the source will be deleted next time the policy runs. A copy policy produces essentially an archived version of the data – files deleted on the source cluster will not be deleted from the target cluster. However there are some specific behaviors in certain cases, shown here.

If a directory is deleted and replaced by an identically named directory, SyncIQ recognizes the re-created directory as a “new” directory, and the “old” directory and its contents will be removed.

**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. If you subsequently create a new directory named “/ifs/old/dir” in its place, the old “dir” and its contents on the target will be removed, and only the new directory’s contents will be replicated.

SyncIQ keeps track of file moves and maintains hard-link relationships at the target level. 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 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 does not remove 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's root path, 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 SyncIQ 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:**

Consider a copy policy rooted at /ifs/data/user. If /ifs/data/user1/foo is moved to /ifs/data/user2/foo, SyncIQ simply renames the file on the target on the next replication. However, if /ifs/data/user1/foo is moved to /ifs/home/foo, which is outside the SyncIQ policy root path, 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.

**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. The cookie allows the association to persist, even if the target cluster’s name or IP address is modified. If necessary, you can manually break a target association, for example, if an association is obsolete or was intended for temporary testing purposes. If the target association is broken, the target dataset will become writable and the policy must be reset before the policy can run again. A full or full differential replication will occur the next time the policy runs. During this full resynchronization, SyncIQ creates a new association between the source and its specified target.

**Target protection with restricted writes – Replication Domains**

In normal operation, SyncIQ target directories can be written to only by the SyncIQ job itself – all client writes to any target directory are disabled. This is known as a protected replication domain. In a protected replication domain, files cannot be modified, created, deleted or moved within the target path of a SyncIQ job. Hard links similarly cannot be created or modified to any files into or out of the target path.

Breaking the association between a SyncIQ source and target causes the target to become writable. For example, on failover, client writes are enabled to allow normal operation on the former SyncIQ target.

**Policy priority**

Before OneFS 8.0, policies are scheduled in order – first come, first served. OneFS 8.0 provides a mechanism to prioritize particular policies. Policies can optionally have a policy setting – policies with the priority bit set will start before unprioritized policies. If the maximum number of jobs are running, and a prioritized job is queued, the shortest running unprioritized job will be preempted (paused by the system) to allow the prioritized job to run. The preempted job will then be started next.
To set the priority bit for a job, use `--priority 1` on the `isi sync policies create` or `modify` command. The default is 0, that is unprioritized.

**Assess SyncIQ changes**

SyncIQ can conduct a trial run of a policy without actually transferring file data between locations. This provides an indication of the time and the level of resources an initial replication policy is likely to consume. This functionality is only available immediately after creating a new policy, before it has been run for the first time.

Assess SyncIQ changes

To conduct a trial run of a policy, use `isi sync policies create` or `modify` command. The default is 0, that is unprioritized.

---

**Figure 11 SyncIQ Policy Assessment Task**

**RPO Alert**

In OneFS 8.0, you can specify an RPO (recovery point objective) for a scheduled SyncIQ policy and cause an event to be sent if the RPO is exceeded. The RPO calculation is the interval between the current time and the start of the last successful sync job.

For example, consider a policy scheduled to run every 8 hours with a defined RPO of 12 hours. Suppose the policy runs at 3pm and completes successfully at 4pm. The start time of the last successful sync job is therefore 3pm. The policy should next run at 11pm, based on the 8 hour scheduled interval. If this next run completes successfully before 3am (12 hours since the last sync start), no alert will be triggered, and the RPO timer is reset to the start time of the replication job. If for any reason the policy has not run to successful completion by 3am, an alert will be triggered, since more than 12 hours elapsed between the current time (after 3am) and the start of the last successful sync (3pm).

If an alert has been triggered, it is automatically cancelled after the policy successfully completes.

The RPO alert can also be used for policies that have never been run, as the RPO timer starts at the time the policy is created. For example, consider a policy created at 4pm with a defined RPO of 24 hours. If by 4pm on the next day, the policy has not successfully completed at least one synchronization operation, the alert will be
triggered. Remember that the first run of a policy is a full synchronization and will probably require a longer elapsed time than subsequent iterations.

An RPO can only be set on a policy if the global SyncIQ setting for RPO is already set to enabled: isi sync settings modify -rpo-alerts true|false. By default, RPO alerts are enabled.

Individual policies by default have no RPO alert setting. Use --rpo-alert <duration> on the isi sync policies create or modify command to specify the duration for a particular policy. You can only define an RPO alert for a policy which is set to run on a schedule.

![Edit SyncIQ Policy Details](image)

**Figure 12 RPO Policy settings**

**Authentication integration**

UID/GID information is replicated (via SID numbers) with the metadata to the target cluster. It does not require to be separately restored on failover.

**Multiple Jobs targeting a single directory tree not supported**

You cannot create SyncIQ policies for the same directory tree on the same target location. For example, consider the source directory /ifs/data/users. Creating two separate policies on this source to the same target cluster is not supported:

- one policy excludes /ifs/data/users/ceo and replicates all other data in the source directory
- one policy includes only /ifs/data/users/ceo and excludes all other data in the source directory
Splitting the policy in this way would be possible only with different target locations, with the associated increase in complexity required in the event of a requiring to failover or otherwise restore data.

**Hard-link replication**

SyncIQ creates hard links at the source as hard links on the target.

**SyncIQ Best Practices and Tips**

**Avoiding full dataset replications**

Certain configuration changes will cause a replication job to run a full baseline replication as if it was running for the first time; that is, to copy all data in the source path(s) regardless of whether 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 unless necessary. Changing any of the following parameters will trigger a baseline sync of the policy:

- Source path(s): root path, include and exclude paths
- Source file selection criteria: type, time, and regular expressions

**Selecting the right source replication dataset**

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

**Including or excluding source-cluster directories**

A SyncIQ policy by default includes all files and folders under the specified root directory. Optionally, directories under the root directory can be explicitly included or excluded.

If any directories are explicitly included in the policy configuration, the system synchronizes only those directories and their included files to the target cluster. If any directories are explicitly excluded, those directories and any files contained in them are not synchronized to the target cluster.

Any directories explicitly included must reside within the specified root directory tree. Consider a policy with the root directory /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. However, you cannot include directory /ifs/projects, since this is not part of the /ifs/data tree.

If you explicitly exclude a directory within the specified root directory, all the contents of the root directory except for the excluded directory will be synchronized to the target cluster.

If you specify both included and excluded 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 with the root directory /ifs/data, and the following directories 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, all directories below /ifs/data/media are excluded except for those specifically included. Therefore, directories such as /ifs/data/media/pictures, /ifs/data/media/books, /ifs/data/media/games are excluded because of the exclude rule. The directory and all subdirectories of /ifs/data/media/music will be synchronized to the target cluster, except for the directory /ifs/data/media/music/working.

**Note:** Excluding a directory that contains the specified root directory has no effect. For example, consider a policy in which the specified root directory is /ifs/data. Excluding 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

A SyncIQ policy can have 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.

Policies of Copy type have more settings available than Sync policies.

In both Sync and Copy policies, 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, use `*\..jpg$`
- To select all files with either .jpg or .gif file extensions, use `*\.(jpg|gif)$`
- 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.

Copy policies also allow you to select files based on file creation time, access time, and modification time. These options are documented in the product documentation.
The following figure shows where file selection criteria are entered in the GUI.

![Figure 13 Advanced file matching policy options](image)

**Note:** With a policy of type Sync, modifying file attributes comparison options and values causes a re-sync and deletion of any non-matching files from the target the next time the job runs. This does not apply to policies of Copy type.

**Note:** 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. For this reason, it is preferable to use includes and excludes of directory paths, if possible.

**Performance tuning**

SyncIQ uses a distributed, multi-worker policy execution engine to take advantage of aggregate CPU and networking resources to address the needs of most data sets. Increased scaling has been introduced with OneFS 8.0 as described below. However, in certain cases you may want to do further tuning.

**Guidelines**

The recommended approach for measuring and optimizing performance is:

- Establish reference network performance 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 over WAN. This can help overcome network latency by having 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.

**Scalability of SyncIQ performance**

**OneFS 7.x and earlier**

A SyncIQ source cluster can have up to 100 policies configured. Up to five jobs (policies) can run at any given time, by default. Additional jobs are queued until a new job execution slot is available.

*Note:* The SyncIQ WebUI and CLI provide the ability 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 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.

**OneFS 8.0**

In OneFS 8.0, the limits have increased to provide additional scalability and capability in line with cluster sizes and higher performing nodes that are available. The
maximum number of workers and the maximum number of workers per policy both scale as the number of nodes in the cluster increases. The defaults should be changed only with the guidance of Isilon Technical Support.

- A maximum of 1000 configured policies and 50 concurrent jobs is now available.
- Maximum workers per cluster is determined by the total number of CPUs
  Default 4 * [total CPUs in the cluster]
- Maximum workers per policy is determined by the total number of nodes in the cluster
  Default 8 * [total nodes in the cluster]
- Instead of a static number of workers as in previous releases, workers are used to dynamically allocated to policies, based on the size of the cluster and the number of running policies. Workers from the pool are assigned to a policy when it starts, and the number of workers on a policy will change over time as individual policies start and stop. The idea is that each running policy always has an equal number (+/- 1) of the available workers assigned.
- Maximum number of target workers remains unchanged, at 100

As an example, consider a 3 node cluster, with 4 CPUs per node. Therefore there are 12 total CPUs in the cluster. Following the previous rules,

- Maximum workers on the cluster = 4 * 12 = 48 workers
- Maximum workers per policy = 8 * 3 = 24

When the first policy starts, it will be assigned 24 workers (out of the maximum 48). A second policy starting will also be assigned 24 workers. The maximum number of workers per policy has been determined previously as 24, and there are now a total of 48 workers – the maximum for this cluster. When a third policy starts (assuming the first two policies are still running), the maximum 48 workers are redistributed evenly, so that 16 workers are assigned to the third policy, and the first two policies have their number of workers reduced from 24 to 16. Therefore there are 3 policies running, each with 16 workers, keeping the cluster maximum number of workers at 48. Similarly, a fourth policy starting would result in all four policies having 12 workers. When one of the policies completes, the reallocation again ensures the workers are distributed evenly amongst the remaining running policies. Note that any reallocation of workers on a policy occurs gradually to reduce thrashing when policies are starting and stopping frequently.

**SyncIQ Performance rules**

SyncIQ allows multiple performance rules to be created, limiting replication jobs based on throughput (KB/sec), file count (files/sec), and in OneFS 8.0: number of workers (percentage of total workers) and CPU utilization (percentage of available CPU).
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 checks for the SnapshotIQ license on the target cluster. If it has not been licensed, the job will proceed without generating 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 available versions of the dataset. 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). SmartConnect can be used to limit and control which nodes in the cluster participate in SyncIQ jobs.

Using SmartConnect on the source cluster

On the source cluster, you can create a SmartConnect IP address pool and assign the IP address pool for the 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. 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 policies modify --policy <my_policy> --force_interface=on`

![Figure 15 Configure a Dedicated SmartConnect IP Address Pool](image-url)
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 WebUI.
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.

While you can configure SmartConnect node restriction 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.

![Figure 16 Global settings for SmartConnect integration](image)

**Monitoring SyncIQ**

In addition to including cluster-wide performance monitoring tools, such as the `isi statistics` command or the 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.

![SyncIQ Job Report Details](image)

**Figure 17 SyncIQ Job Report Details**

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 WebUI’s Cluster Overview performance reporting pages. Here, you can review network and CPU utilization rates via real-time or historical graphs. The graphs display both cluster-wide performance and per-node performance. Based on this information you can tune SyncIQ’s network and file...
processing threshold limits (to limit both CPU and bandwidth usage). These limits are cluster-wide and are shared across jobs running simultaneously.

Figure 18 Cluster Overview SyncIQ Connection Reporting

**Note:** More comprehensive resource utilization cluster statistics are available using Isilon’s InsightIQ multi-cluster reporting and trending analytics suite, as shown in the figure below.
Roles Based Administration

Roles Based Administration (RBAC) 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 be assigned full access to SyncIQ configuration and control, but only read-only access to other cluster functionality. SyncIQ administrative access is assigned via the ISI_PRIV_SYNCIQ privilege. RBAC is fully integrated with the SyncIQ CLI, 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 RBAC (described above) providing a granular authentication framework for secure, remote SyncIQ administration via scripting languages.

Troubleshooting with SyncIQ logs

SyncIQ logs provide detailed job information. To access the logs, connect to a node and view its /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. Only enable this logging level under guidance from Isilon Technical Support.

The Log Deletions on Synchronization selection specifies whether to record information on files deleted from the target cluster during SyncIQ jobs. These files are deleted from the target cluster when they are no longer present on the source cluster.

![Figure 20 SyncIQ policy log level and synchronization log settings](image)

**Target aware initial synchronization**

In situations where most of the dataset already resides on both clusters, target aware initial synchronization can reduce the initial replication time. It is 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 the policy continues as a target aware synchronization, incremental replications will occur normally; however any subsequent baseline replication (for example as the result of a policy change) will use a target aware initial synchronization instead of a normal full baseline replication. This consumes unnecessary CPU on both the source and target clusters.

**Failover Dry-run Testing**

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

```
isi sync recovery allow-write --revert [policy]
```

**Version compatibility**

The Support and Compatibility Guide shows the versions of OneFS that can be replicated with SyncIQ. Consult this for the latest information.
In general, for versions of OneFS older than 7.0, the target cluster must be at the same or higher OneFS version than the source cluster. For example, SyncIQ can replicate files if the source cluster is running OneFS 6.5 and the target cluster is running OneFS 6.5 or later.

From OneFS 7.0 onwards, a source cluster running OneFS 7.0 can synchronize with a target cluster running OneFS 6.5 or later.

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

### SyncIQ Licensing

SyncIQ is included as a core component of EMC Isilon OneFS and requires a valid product license key in order to activate it. This license key can be purchased through your EMC Isilon account team. An unlicensed cluster will show the “Activate SyncIQ” warning button as in the figure below until a valid product license has been applied to the cluster.

**Note:** Both the source and target clusters must have SyncIQ licenses.

#### Figure 21 Enable SyncIQ

#### Additional tips

Setting a target cluster password is useful if you want to verify that the source cluster is replicating to the right target cluster. The target cluster password is different from a cluster’s root password. Do not specify a target password unless you create the required password file on the 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.

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

SyncIQ implements scale-out asynchronous replication space for Isilon clusters, providing scalable replication performance, easy failover and failback and dramatically improving Recovery Objectives. SyncIQ design, combined with tight integration with OneFS, native storage tiering, point-in-time snapshots, retention, and leading backup solutions—makes SyncIQ a powerful, flexible, and easy-to-manage solution for disaster recovery, business continuance, disk-to-disk backup, and remote archive.

To learn more about SyncIQ and other EMC Isilon products please see www.emc.com/isilon.

About EMC

EMC Corporation is a global leader in enabling businesses and service providers to transform their operations and deliver IT as a service. Fundamental to this transformation is cloud computing. Through innovative products and services, EMC accelerates the journey to cloud computing, helping IT departments to store, manage, protect and analyze their most valuable asset – information – in a more agile, trusted and cost-efficient way. Additional information about EMC can be found at www.emc.com.