Version: 4.0.0

Failover Recovery

Introduction

Failover Log Analysis

Steps to Reading a Failover Log

1. The Failover Logs can be found by clicking on the DR Assistant icon on the desktop of the Eyeglass Web UI.
2. Click on the Failover History tab, you'll see the various jobs that have been run, run date and results. (By clicking on an individual job, the details of that job will appear in the lower half of the window).
3. Identify the section in the log with an error message by expanding folders to locate the red "X".
4. Determine which step failed and refer to the appropriate table (from this guide) for the next steps.
5. Match the scenario in the failover log to the corresponding scenario in the table to identify the issue and resolution steps.

Additional Reporting for SyncIQ Job Errors

As of version 1.8 and later, SyncIQ job reports are collected in a separate log to simplify troubleshooting. This log includes:

- **Run Report**: Provides details of the executed jobs.
- **Resync Prep Report**: Tracks preparation steps for synchronization.
- **Resync Prep Domain Mark Report**: Captures domain-specific preparations.

> **INFO**
> If the root cause of a failure is identified as a SyncIQ policy error that cannot be recovered or retried, this log can be provided to Support for faster resolution and escalation with EMC.

Replication Policy Failover Preparation

Below are several more failover steps that can fail or time out, along with concise, step-by-step fixes.

Wait for Other Failover Jobs to Complete

Impact on Failover

- Eyeglass allows only one failover job at a time.
- If another job is already running, your new failover won't start.

Recovery Steps

1. **Check Running Jobs**
   - Go to the Eyeglass "running jobs" window. Confirm any existing failover jobs are completed or canceled.
2. **Wait or Cancel**
   - If a job is still in progress, allow it to finish or manually stop it if appropriate.
3. **Restart Failover**
   - Once no failover jobs are running, launch the new failover job again.

> **WARNING**
> - **Time-Out**: This step can remain in the "running" state for up to two hours before timing out.
> - **Data Loss Impact**: Not typically applicable here since failover hasn't started; however, no progress will be made until other jobs finish.

SOURCE get POLICY Info

Impact on Failover

- Eyeglass can't communicate with the source cluster, causing an immediate failover failure.

Recovery Steps

1. **Check Connectivity**
   - Verify the network path between Eyeglass and the source cluster. Ensure DNS, IP addresses, and firewalls are correctly configured.
2. **Fix Communication Errors**
   - If there are permission or authentication issues, update credentials or correct them in Eyeglass.
3. **Restart Failover**
   - Once Eyeglass can reach the source cluster, rerun the failover job.

> **WARNING**
> - **Uncontrolled Failover**: This step does not run during an emergency failover scenario.
> - **Data Loss Impact**: Failover cannot begin; any delay could risk data currency until this is resolved.

Wait for Existing Policy Jobs to Complete

Impact on Failover

- If Eyeglass detects other active policy jobs, it waits for them to finish.
- Default timeout is often 180 minutes (3 hours), but this can vary by release or be modified via `isi_gs` CLI commands.

Recovery Steps

1. **Confirm No Overlapping Jobs**
   - Check Eyeglass to ensure no other SyncIQ or replication jobs are running.
2. **Address Stuck Policies**
   - If a policy is stuck or returning errors from the cluster, you may need EMC support to resolve the underlying issue before failover can proceed.
3. **Restart Failover**
   - Once no conflicting jobs remain, retry the failover.

> ⚠ **WARNING**
> - **Timeout**: If the wait exceeds the configured failover timeout, the failover will fail.
> - **Data Loss Impact**: Failover remains blocked, leaving you in a potential data loss scenario until resolved.

SOURCE Remove Schedule POLICY

Impact on Failover

- Eyeglass is unable to remove or adjust the schedule on the source cluster.
- Communication failure prevents the failover from proceeding.

Recovery Steps

1. **Verify Eyeglass–Source Connectivity**
   - Confirm network or permission settings allow Eyeglass to manage schedules on the source.
2. **Manually Remove/Update Schedule**
   - If needed, log into OneFS on the source cluster and remove or modify the relevant SyncIQ schedule.
3. **Restart Failover**
   - Retry the failover job once the schedule is successfully removed or updated.

> ⚠ **WARNING**
> - **Uncontrolled Failover**: This step does not run during an emergency failover.
> - **Data Loss Impact**: Failover is halted until the schedule is addressed, so data is not actively protected.

Replication Policy Failover (Run All Policies with "SyncIQ Data Sync")

Impact on Failover

- The final incremental sync of data failed, causing the failover to abort.
- Source and target remain in the initial state (target cluster read-only).

Recovery Steps

1. **Identify Which Policies Failed**
   - Check the Eyeglass Job Details to see which policies ran successfully and which timed out or failed.
2. **Troubleshoot or Cancel Ongoing Sync**
   - If a policy job is still running on OneFS, wait for it to finish or cancel it if it's stuck.
   - Manually run the policy again to see if it can succeed.
3. **Open a Support Case & Retry Failover**
   - If the policy repeatedly fails, open a case with EMC (or relevant vendor).
   - Once resolved, restart the failover job.

> ⚠ **WARNING**
> - **Timeout**: Eyeglass will wait for each policy over a set timeout. If incremental sync takes longer than that, it fails.
> - **Optional "Data Sync"**: If unsynced data is not critical, you can uncheck the "Data Sync" box. This moves forward with failover but any unreplicated data will be lost.
> - **Uncontrolled Failover**: Not run during an emergency failover.

Run Configuration Replication Now (Config Sync)

Impact on Failover

- The final sync of configuration items (e.g., shares, exports, aliases) has failed.
- Failover continues, but the target cluster remains read-only until config replication succeeds.

Recovery Steps

1. **Review the Eyeglass Jobs**
   - In the Eyeglass interface, switch to the running jobs tab and find the recent config replication job.
2. **Identify & Fix the Failure Reason**
   - Use the Job Details to see if there's a permissions, network, or file conflict issue.
   - Correct the problem (re-auth, DNS, etc.).
3. **Restart Failover**
   - If config data remains unsynced but is nonessential, you can uncheck "Config Sync" to speed up failover.
   - Otherwise, once the issue is fixed, rerun the replication and then proceed with failover.

> ⚠ **WARNING**
> - **Skipping Config Sync**: You can uncheck "Config Sync" if source/target configs are already aligned or you accept losing any changes

changes.

- **Uncontrolled Failover**: Not applicable in an emergency scenario.
- **Data Loss Impact**: Typically minimal for config items, but the target remains in a partial failover state until replication is resolved.

Notes

- **Eyeglass Timeout Values**: Many failover steps rely on timeouts (e.g., 180 minutes). Adjust these if you have large datasets or slower networks.
- **Support Calls**: Frequent communication or schedule failures may require a vendor (EMC) support case.
- **Documentation**: Always consult "Best Practices for Failover with Eyeglass" and official OneFS guides for deeper command-level instructions.

DFS Mode

If DFS Share(s) rename fails on target or source, DFS clients will not switch clusters.

Recovery Steps

1. Remove `igls-dfs` prefix manually from the target cluster shares that weren't renamed (check the failover log). This will complete failover, and clients will switch automatically.
2. Add `igls-dfs` prefix manually to the source cluster shares that weren't renamed (check the failover log). This will block client access to the source and switch them to the target.
3. Allow writes manually from OneFS for selected failover policies. This applies to release 1.9 and below.
4. Run quota jobs related to the failover manually from Eyeglass.
5. Run re-sync prep manually from OneFS for selected failover policies.
6. Apply SyncIQ policy schedule to target cluster policies that failed over.

> **INFO**
> Releases after 2.0 will run these steps automatically if a share rename fails.

Networking Operations

The following subtitles will explore the possibility of each of the mentioned steps *not* finishing, the effects this may have on failover, and how you can react.

Rename Source SC (SmartConnect) Zone Names & Aliases

Impact on Failover

- Failover fails during the networking step.
- Auto-rollback reverts Source/Target clusters to initial states.
- The source file system remains read/write, returning SmartConnect zones to original settings.

Recovery Steps

1. **Check the Job Details**: Determine the cause of the networking failure (e.g., DNS or network misconfiguration).
2. **Fix & Retry**: Correct the error, then rerun failover. If networking is still unstable, only select the SyncIQ portion until you're sure network issues are resolved.
3. **Start Fresh**: Once networking is stable, choose the required policies and rerun the failover.

Warnings

- Not performed during *uncontrolled* (emergency) failovers.

Modify Source SPNs

Impact on Failover

- SPN failure does *not* stop the failover; errors go into the log.
- Failover continues, but SPNs may be incorrect.

Recovery Steps

1. **Review the Failover Log**: Identify failing SPNs.
2. **Manually Fix SPNs**: Use ADSIEdit (with domain admin rights) to create/delete SPNs on the source cluster.
3. **Validate**: Ensure the corrected SPNs match what's required for each SmartConnect zone.

Warnings

- SPN changes on the source are *proxied* through target cluster ISI commands, so source cluster availability is not impacted by these corrections.

Rename Target SC (SmartConnect) Zone Names & Aliases

Impact on Failover

- Failover fails during the networking step.
- Rollback restores both clusters to pre-failover state.
- SmartConnect zones revert to original configuration.

Recovery Steps

1. **Identify Failure Reason**: Check job details to see what caused the networking step to fail.

2. **Attempt Partial Failover**: If networking remains unstable, try just the SyncIQ portion while you troubleshoot the network or DNS.
3. **Rerun Full Failover**: After fixing issues, rerun failover with the necessary policies.

Warnings

- Not performed during *uncontrolled* failover.

Modify Target SPNs

Impact on Failover

- SPN failure does *not* stop the failover; it continues.
- Errors are logged, and SPNs may be incorrect afterward.

Recovery Steps

1. **Review the Failover Log**: Locate SPN failures.
2. **Fix SPNs**: Use ADSIEdit on the domain to create/delete SPNs for the *target* cluster.
3. **Confirm Changes**: Ensure the new SPNs match each SmartConnect zone that failed over.

Warnings

- SPN operations on the target are also proxied through ISI commands, so the cluster's availability is not affected.

Replication Policy Failover

Below are the most common issues that can occur when failing over SyncIQ policies, along with quick step-by-step fixes. For more advanced scenarios or troubleshooting, refer back to the full documentation or contact Support.

Replication Policy Failover (All Policies)

Impact on Failover

- One or more SyncIQ policies did not successfully complete their failover operation.
- This is the *parent task* that contains all sub-policies.

Recovery Steps

1. **Determine Failure Reason**
   - Check the job details (policy failover logs) to see which policies failed and why.
   - Look for a step called "`CLUSTERNAME allow writes POLICY PATH`" to confirm if at least one policy succeeded.
2. **Create a New Failover Job (If Needed)**
   - If some policies never started or failed partway, create a new SyncIQ failover job with the incomplete policies selected.
   - Retry only those policies that did not finish.
3. **Review Data Loss Impact**
   - Some failing sub-steps can lead to partial or inconsistent data states. Consult the next sections (or vendor docs) for safe remediation steps.

> ⚠ **WARNING**
> - **Parent Step**: Because this is a top-level failover task, a failure here can have cascading effects on sub-policies.
> - **Data Loss**: Review each policy's logs to see if data was at risk when failover halted.

Target "Allow Writes" Policy Path

Impact on Failover

- The target cluster cannot be put into a writeable state (i.e., "writes allowed").
- By default (as of 1.6.1), the failover attempts a "make writeable" command before running the Resync Prep step.
- On releases prior to 2.0, failover halts if the "make writeable" command fails.

Recovery Steps

1. **Check Job Details**
   - Investigate error messages about "allow writes" on the target cluster.
   - If needed, manually run the "allow writes" command for the failing policy or fix the underlying cause (e.g., permission issues).
2. **Restart Failover or Run Prep**
   - For controlled failovers, manually run Resync Prep on the *source* cluster after "allow writes" succeeds on the target.
   - Re-initiate failover if the policy is still in a failed state.
3. **Open EMC Support Case (If Required)**
   - If the cluster returns repeated errors, you may need EMC assistance to resolve the underlying problem.
   - After the error is fixed, re-attempt the policy failover or proceed with post-failover tasks (e.g., Quota sync jobs).

> ⚠ **WARNING**
> - **Data Access Impact**: Until "allow writes" succeeds, users only have *read-only* access to the affected policy data.
> - **Failover Stops (Pre-2.0)**: Releases before 2.0 will halt entirely if "make writeable" fails.

Replication Policy Failover – Recovery

Impact on Failover

- One or more SyncIQ policies in the Failover job did not successfully complete their multi-step failover.
- **Important**: No automatic rollback occurs in this failover section. Previously completed steps (networking, allow-writes) remain in place, and the cluster is treated as "failed over" for those parts.

Recovery Steps

1. **Diagnose the Specific Policy Error**
   - Check the failover logs for each policy that returned an error.
   - Identify if "resync prep," "schedule," or "run" actions are failing.
2. **Manually Complete or Retry Failing Steps**
   - If "resync prep" or "allow writes" steps had an error, fix the problem and re-run them manually.
   - If scheduling or running the policy fails, correct the issue (quota error, DNS, permission) and retry.
3. **Open EMC Support Case (If Needed)**
   - Policies that persistently return errors might require EMC assistance to resolve.
   - Completing these steps is critical to fully protect the filesystem after failover.

> ⚠ **WARNING**
> - **Data Loss Impact**: Typically *none*, because earlier failover steps have completed. However, any policy that remains unfinished is *not* actively protecting data.
> - **Parent Step**: This step is a container for multiple sub-steps; partial completion could leave some policies in a limbo state.

Source "Resync Prep" Policy

Impact on Failover

- The *mirror policy* cannot be created or prepared.
- The target cluster is active, but the overall failback readiness status is failed.
- As of 1.6.1, the "make writeable" command is attempted before Resync Prep; on 2.0 or newer, the failover tries to run Resync Prep against all included policies in sequence.

Recovery Steps

1. **Log In to OneFS on the Source**
   - Manually execute "resync prep" for the failing policy.
   - Address any errors that appear (permissions, path issues, etc.).
2. **Set the Schedule** (If Needed)
   - Confirm that the *target* policy has a proper schedule.
   - If it's missing or broken, configure it to ensure ongoing replication.
3. **Re-Run Quota or Cleanup Tasks**
   - If the policy completes Resync Prep successfully, you may also need to run Quota Jobs from Eyeglass or contact support for post-failover quota sync.

> ⚠ **WARNING**
> - **Uncontrolled Failover**: This step does not run in an emergency failover scenario.
> - **Data Loss Impact**: Typically *none*, but any policy not prepped for resync is left unprotected until this is fixed.

Target "Run" Policy Mirror

Impact on Failover

- The mirror policy cannot run on the target.
- Target cluster is active, but overall failover status is marked as failure.

Recovery Steps

1. **Log In to OneFS on the Target**
   - Identify the error preventing the policy from running (permissions, connectivity, etc.).
2. **Fix & Retry**
   - Correct the issue (e.g., reconfigure the policy, address any DNS or network errors).
   - Re-attempt running the mirror policy.
3. **Contact Support (If Needed)**
   - If the policy repeatedly fails, open a support case (EMC or vendor-specific) to resolve deeper issues.

> ⚠ **WARNING**
> - **Uncontrolled Failover**: This step does not run during an emergency failover.
> - **Data Loss Impact**: Typically *none*, but full protection is blocked until the mirror policy runs successfully.

Target "Set Schedule"

Impact on Failover

- The mirror policy's schedule cannot be set on the target cluster.
- The policy is considered failed over, but the overall failover status shows failure until scheduling is resolved.

Recovery Steps

1. **Log In to OneFS on the Target**
   - Attempt to set or edit the schedule for the mirror policy.
   - Verify that any required fields (e.g., replication frequency) are correct.
2. **Confirm Policy State**
   - Ensure the policy is recognized by the target cluster and not in an error state.
   - If the policy is incomplete, address that first (e.g., "allow writes," "resync prep").
3. **Check Quotas & Post-Failover Tools**
   - If the policy schedule still cannot be set, you may need to run or fix Quota Jobs.
   - Contact Superna support if scheduling remains blocked.

> ⚠ **WARNING**
> - **Uncontrolled Failover**: Not applicable in an emergency failover.
> - **Data Loss Impact**: Typically *none*, but the filesystem is not fully protected until the mirror policy has a valid schedule and runs successfully.

> **NOTE**
>
> - **Recovery Logic**: Many of these failures rely on manual intervention to fix or retry steps like "allow writes," "resync prep," or scheduling.
> - **Support Cases**: Persistent SyncIQ policy errors often require EMC (or vendor) support involvement.
> - **Documentation**: Refer to your solution's official Failover Design Guide and logs for deeper troubleshooting steps.

Replication Policy Failover Finalize

> **INFO**
>
> This step runs one child step per policy, listed as "Finalize quota for path `<policy source path>`". The table below describes failures on those steps, and the following should be done for any failed steps, or steps that did not run.

Step That Failed	Impact on Failover	Recovery Steps	Notes or Data Loss Impact
Finalize quota for path: Delete Quotas on Source	- Could not delete quotas from the source. - Policy is failed over. - Target cluster is now active. - Failover status: *Failure*.	1. On the *SOURCE OneFS*, locate all quotas for data protected by the SyncIQ policy. 2. Verify these quotas exist on the *TARGET cluster*. 3. Delete these quotas from the *SOURCE*.	- This step isn't required during uncontrolled failover. - No data loss impact: Policies can failover even without completing this step. - Note: Not completing this step may affect re-protecting due to leftover quotas on the source cluster.
Enable configuration replication for policies	- Unable to enable Eyeglass Configuration Replication Jobs. - Policy is failed over. - Target cluster is now active. - Failover status: *Failure*.	1. Open the *Eyeglass Jobs* window. 2. Select the configuration replication job and enable it. 3. Use logs to find the reason for failure.	- This step activates the newly configured mirror policies after failover (if they weren't already active). - No data loss impact: Eyeglass will detect and enable the new policy even after failure. - Note: If this step fails, configuration syncing from the source cluster may be blocked, but it can be enabled manually in the jobs window.

Post Failover Script Execution

Step That Failed	Impact on Failover	Recovery Steps	Warnings or Data Loss Impact
Eyeglass Script Engine	- A user-provided post-failover script failed. - Failover status: *Failure*.	1. Use the script engine to correct errors in the failing scripts and re-run the scripts that failed. 2. Use the test script function to validate output and error codes returned to failover jobs.	- This step relies on user-supplied implementations. - Review the script output to ensure proper execution. - If the script fails, it should halt the failover job if set up correctly. - *Data Loss Impact*: This step mainly affects remounting or starting applications after failover. Logs should be reviewed to confirm all steps completed and correct any script failures manually if needed.

> **NOTE**
>
> See Pre Post Failover Scripting Guide on proper script exit code values to indicate failure vs successful execution.

Post Failover

> **INFO**
>
> This step is completed once all critical tasks have been successfully executed. If all steps have been completed up to this point, no failures can result in data loss. This section applies to rolling back SmartConnect to the source cluster. If dual delegation is configured, no DNS steps are required.

Check Network Health

Impact on Failover

- The Networking Rollback job could not be initiated.
- This only matters if the failover didn't reach the "make writeable" step of a policy.

Recovery Steps

1. **Review the Failover Log**
   - Identify which networking operations were attempted (DNS updates, interface changes, etc.).
2. **Manually Revert on OneFS**
   - Log into OneFS (on both SOURCE and TARGET if needed) to undo or fix any partial networking changes.
3. **Plan Next Steps**
   - If additional help is required (e.g., the source data was marked unusable), contact EMC and consult Best Practices for Failover with Eyeglass.

> **WARNING**
>
> - **Rollback Logic**: Only executes if failover failed *before* the make writeable step on a policy.
> - **Data Loss Impact**: If failover never completed, the source cluster might still be the production copy, risking data loss if that data was deemed unusable.
> - **Uncontrolled Failover**: Not applicable in an emergency scenario.

Post Failover Inventory

Impact on Failover

- The post failover Inventory job failed.
- Failover itself is successful, but the Eyeglass UI may not reflect the latest status.

Recovery Steps

1. **Check Cluster Connectivity**
   - Validate that Eyeglass can communicate with both the source and target clusters.
2. **Review Alarms**
   - Open the Eyeglass alarms window to see if there are issues related to configuration replication.
3. **Run or Wait**
   - Manually start the configuration replication job, or wait for the next automatic cycle to update the UI.

> **WARNING**
> - **Uncontrolled Failover**: This step does not run during an emergency failover.
> - **Data Loss Impact**: **None**. This job simply updates Eyeglass UI data.

Post Failover Readiness Task

Impact on Failover

- The post failover Readiness job failed.
- The failover succeeded, but Eyeglass UI may be outdated.

Recovery Steps

1. **Validate Cluster Connectivity**
   - Ensure Eyeglass can still reach both source and target clusters without errors.
2. **Manually Run "Access Zone Readiness"**
   - If necessary, go into Eyeglass and trigger the readiness job.
3. **Wait for Automatic Cycle**
   - If you don't start it manually, Eyeglass will attempt to run this job again on its normal schedule.

> **WARNING**
> - **Uncontrolled Failover**: Not run during an emergency failover.
> - **Data Loss Impact**: **None**. This step only updates the Eyeglass interface.

Final Notes

- **Data Loss Considerations**: Most post-failover jobs primarily update the UI and cluster states. If your failover never reached the "make writeable" step, investigate potential data consistency issues.
- **Support Resources**: When network or rollback logic fails, consult Eyeglass Best Practices and EMC support for more advanced recovery methods.

Check Client Access (Manual Step)

If this isn't done	Impact to Failover	Recovery Steps	Notes or Warnings
DNS SmartConnect zone validation	Note: Dual delegation switches DNS automatically after failover, requiring validation.	1. Use `nslookup` to check the SmartConnect zone name. 2. Confirm the DNS delegation status.	
Refresh session to pick up DNS change	SMB Client is unable to access data on failover due to session issues.	1. Check SPNs using the ADSI Edit tool. 2. Confirm the DNS refresh and reinitialize sessions.	You cannot create a missing SPN on the Active Directory.
SMB Direct Mount Shares	Dual delegation updates DNS but requires clients to reconnect for the changes to apply.	1. Run `net use //sharename /delete`. 2. Run `net use //sharename` to reinitialize the connection.	
NFS mounts	Dual delegation updates DNS but requires clients to remount for changes to apply.	1. Run `umount -fl /path of mount`. 2. Run `mount -a` (reads from the `fstab` file) to remount.	
DFS clients	DNS auto-switches without additional intervention.	No action needed.	

> **INFO**
> This step is completed once all critical tasks have been successfully executed. If all steps have been completed up to this point, no failures can result in data loss. This section applies to rolling back SmartConnect to the source cluster. If dual delegation is configured, no DNS steps are required.

Edit this page

Previous
« Post Failover (Policy)

Next
Troubleshooting Failover »