Table of Contents

1. Eyeglass Failover Design Guide

Home Top

1.1. Introduction to this Guide

Home Top

Introduction to this Guide

Overview

Eyeglass offers single button assisted failover by; Access Zone, IP pool , Microsoft DFS enabled SyncIQ policies, or SyncIQ policy(s). This document provides:

- An overview of each failover mode
- High level steps for each failover mode
- How to assess readiness for failover
- Planning and operational steps for each failover mode

For guidance on which failover mode is appropriate for your environment, please consult the document Eyeglass Start here First. The Eyeglass Start Here First document provides the information you will need for each failover option to assist you in making the decision of which option is appropriate for your own environment:

- When to use it?
- Why use it?
- What you need to know?
- Estimated knowledge to configure

What's New with Eyeglass Failover

Release	Description	Failover Mode
1.6	New error handling for OneFS PAPI errors that occur during	All Failover

	failover. Should PAPI return an error such as 503 Service Unavailable on any of the steps for: allow writes, run policy/mirror policy, resync prep, Superna Eyeglass will now retry this action 3 times as an error such as 503 Service Unavailable may be transient.	Modes
1.6	New timeout count down added to each step that is being processed so timeout is visible during a failover. URL to long running steps to recovery guide included in log, along with login https url to cluster management to allow simple "One" click from a failover to PowerScale UI console access to check on cluster operations.	All Failover Modes
1.6	Key steps are now grouped: 1. Make writable all policies are processed together (in series) making the filesystem writable faster for all policies involved in the failover. 2. Resync prep step now run in batch for all policies after the make writable step for all policies.	All Failover Modes
1.6.1	New release notes on failover acknowledge in DR assistant is required reading, before allowed to continue with a failover.	All Failover Modes
1.7	As of release 1.7 and beyond all Failover modes will restrict number of parallel Job requests to the PowerScale cluster for the Run SyncIQ Policy data sync step based on cluster version: OneFS 7.2 - 5 parallel job requests (OneFS 7.x cluster have a limit of 5 concurrent policies). Eyeglass will monitor the progress for each Job and submit a new request as previously submitted requests are completed. OneFS 8 - parallel job requests limit based on Eyeglass appliance configuration (default 10). Based on extensive testing for safe failovers, make writable and resync prep are serialized steps.	All Failover Modes
1.8	This release introduces parallel failover mode disabled by default. **High Speed Failover - Parallel Failover Flag :** 1. Allows make write step and resync prep to run in parallel with up to 10 threads, ensures that 10	All Failover Modes

	policies are submitted to be processed at all times. 2. NOTE: Risk of a policy failure increases, and new flag will NOT stop the failover in progress, and will continue to issue api calls to submit all SyncIQ policies in the failover job until all have been submitted. This runs the risk of more complex recovery if more than one policy fails to complete its step (Allow Writes OR resync Prep) 3. Testing has shown these steps for large quantity policy failover can improve failover times 3x to 4x. **Access Zone Failover Enhancement**: 1. **New validation detects time skew** between cluster nodes and between Eyeglass and the cluster's. 2. Validation warning raised if detected 3. Time skew can cause failed steps if the time on different nodes is not within an acceptable range to detect the steps or running status on a policy during failover. **SyncIQ Job Reports appended to Eyeglass failover log :** 1. Now policy run, and resync prep reports are appended to the end of the Eyeglass failover log to allow simplified triage of failed steps, and escalation to EMC support based on cluster policies failing. 2. All information and time stamps are now in a single file.	
1.9	**Failover Enhancements** 1. Open files validation removed from DR Assistant until PowerScale API support per Access Zone open files. 2. New Access Zone readiness validation verifies all IP pools have a SmartConnect zone defined. 3. DR Assistant SyncIQ reports from a failover are now separated from Eyeglass logs in the failover history, making debugging simpler. 4. **Restrict at source validation updated to show info only in the DR Dashboard** 5. To simplify validation of Access Zones readiness for failover. Restrict at source is a best practice and	

shows green if implemented or info if not implemented on each policy

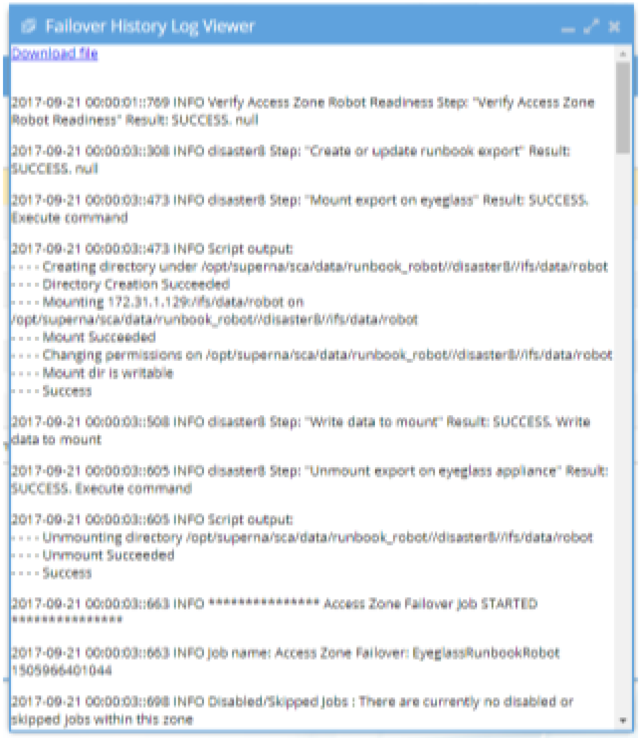
5. SPN Management Enhancements

6. SPN failover enhancement for Access Zone failover now restricts the delete and add SPN API calls to a single cluster node in the target cluster.

7. This change will insure a single domain controller is used for the failover operations.

8. Short SPN's are now synced to AD computer objects (not used for Kerberos) during config sync, if any are missing they are inserted. NOTE: This is not related to failover of SPN’s only maintaining newly detected SmartConnect names, and ensure they are synced to AD computer object.

6. **Failover log real-time** view in DR assistant allows a live failover log to be monitored with auto refresh or stop and pause option.



```
2017-09-21 00:00:01::769 INFO Verify Access Zone Robot Readiness Step: "Verify Access Zone
Robot Readiness" Result: SUCCESS. null

2017-09-21 00:00:03::308 INFO disaster8 Step: "Create or update runbook export" Result:
SUCCESS. null

2017-09-21 00:00:03::473 INFO disaster8 Step: "Mount export on eyeglass" Result: SUCCESS.
Execute command

2017-09-21 00:00:03::473 INFO Script output:
- - - - Creating directory under /opt/superna/sca/data/runbook_robot//disaster8//ifs/data/robot
- - - - Directory Creation Succeeded
- - - - Mounting 172.31.1.129:/ifs/data/robot on
/opt/superna/sca/data/runbook_robot//disaster8//ifs/data/robot
- - - - Mount Succeeded
- - - - Changing permissions on /opt/superna/sca/data/runbook_robot//disaster8//ifs/data/robot
- - - - Mount dir is writable
- - - - Success

2017-09-21 00:00:03::508 INFO disaster8 Step: "Write data to mount" Result: SUCCESS. Write
data to mount

2017-09-21 00:00:03::605 INFO disaster8 Step: "Unmount export on eyeglass appliance" Result:
SUCCESS. Execute command

2017-09-21 00:00:03::605 INFO Script output:
- - - - Unmounting directory /opt/superna/sca/data/runbook_robot//disaster8//ifs/data/robot
- - - - Unmount Succeeded
- - - - Success

2017-09-21 00:00:03::663 INFO *************** Access Zone Failover job STARTED
***************

2017-09-21 00:00:03::663 INFO Job name: Access Zone Failover: EyeglassRunbookRobot
1505966401044

2017-09-21 00:00:03::698 INFO Disabled/Skipped Jobs : There are currently no disabled or
skipped jobs within this zone
```

7. Quota Failover Enhancement

11. Linked quotas that are unlinked to the parent quota creates a quota that be can be managed with a different limit applied from the parent quota.

12. Eyeglass will now correctly failover unlinked quotas. Now the unlinked quotas failover as a normal quota, and then the parent all users quota is failed over next to ensure no conflict occurs on the target

	cluster. 13. Syncing Shares with variable expansion in the path name now sync correctly between clusters 8. Ransomware Defender Failover	
2.0	New Failover Mode 1. **IP Pool failover** allowing hot hot data within an Access Zone and more granular failover options. See Access Zone guide for configuration requirements. Failover Logic Major Enhancements 1. Parallel Failover Jobs: 2. This feature will allow multiple failovers to execute in parallel. All Failover types are supported. 3. NOTE: parallel threads is set to 10 which is shared across all failover jobs. 4. LOGGING: Failover log will be split into Failed over data and client redirect. This will indicate the failover of data and clients and post failover scripts. The second half of the log will be for post failover steps including failback steps and quota failover. 5. **Continue on failed Step**: After analyzing many failovers the new logic will continue to execute steps as outlined below. This will ensure SyncIQ policies are attempted even if one SyncIQ policy encounters an error. 6. Make Write Step on each SyncIQ policy - If any policy fails to run, all other policies are run and failover continues. The steps that are not yet run for the failed policy will be skipped. 7. Run Resync Prep SyncIQ - If any policy fails to run, all other policies are run and failover continues. 8. NOTE: Any policy that fails a step will have its following steps skipped. 9. Cancel a running failover: This option appears in the running failover tab of DR Assistant and allows a running failover to be canceled. **NOTE: No Rollback will occur and failover stops at what ever step was being executed. All steps to recover from this will be manual. Use with caution.**	

10. Cancel Failover option on running failovers UI.
NOTE: Only used if directed by support.

New Failover Options in DR Assistant

1. Data Integrity Failover.
2. Access Zones or DFS and Per SyncIQ policy failover will now insert deny everyone permissions to shares that will be failed over as a pre-Failover step. This will disconnect open files, disconnect users from all shares involved in the failover. This will ensure data integrity of the failed over data set when SyncIQ is run by Superna Eyeglass® after users are disconnected.
3. Post failover step to correct share permissions to original security settings.
4. Option to disable this feature on per failover with DR Assistant.
5. Supports SMB shares in this release.
6. See New DR Assistant option below. Mouse over help text on options for failover.
7. Failover option added to skip Quota Failover: This new DR Assistant check box allows skipping quota failover step for situations when a failback is planned within a short period of time. This also can help avoid failed failovers due to quota scan failing SyncIQ steps.

Skip quota failover step option DR Assistant

2. In some customer environments the quota scan job interferes with failover and failback performance. The requirement to wait until quota scan completes adds hours to a failover or interrupts a failover with a failed SyncIQ step.
3. This feature allows skipping failover of quotas and leave them on the source cluster.
4. Eyeglass has a special quota sync command line tool that allows quotas to be synced AFTER a failover has been completed.
5. Customers can now choose to skip quota failover in DR Assistant. Another feature detects if quotas already exist that will fail SyncIQ steps.

3. DR Assistant Block Failover Failover on Warnings

Overview: This will validate failover jobs and prevent a failover from starting under certain conditions that will result in a failure. This applies to newly created quotas that have not been scanned by quota scan job.

3. Quota scans are triggered on Onefs 8 when quotas are created or quota scan jobs are scheduled to run to calculate quotas.
4. This can interfere with the make writable step and resync prep during failover.
5. It is best practice to ensure no quotas are created before failover to avoid this conflict.
6. Quota scan locks the file system blocking SyncIQ from completing steps.
7. DR Assistant will have new option (enabled by default) to detect if any quotas exist on the target cluster at the time of failover matching SyncIQ policies selected for a failover, and will abort the failover:
8. If any quotas have the ready for Quota scan attribute set (this flag indicates quota scan needs to run).
9. Note: disabling or canceling a running quota scan job on the cluster does not avoid the conflict with SyncIQ. The attribute on the quota determines of SyncIQ step will fail.
10. DR Assistant will offer the ability to uncheck this detection function at the users risk of SyncIQ steps failing.

Failover log Enhancements

1. Color coded Success and Failure per step. To quickly identify any step that was failed
2. **Failover Summary:** Each step is summarized at the end of the failover for all keys steps Example below:
3. Overall Failover Job status: Completed, total elapsed time: 0 hours, 11 minutes, 40.50 seconds.
4. Final SyncIQ Jobs status: Completed, elapsed time: 0 hours, 1 minutes, 34.02 seconds.
5. Client Redirect status: Completed, elapsed time: 0 hours, 0 minutes, 26.17 seconds.
6. Make Target Writable status: Completed, elapsed time: 0 hours, 0 minutes, 40.75 seconds.

	7. Quota Jobs status: Completed, elapsed time: 0 hours, 0 minutes, 2.21 seconds. 8. Preparation for Failback status: Completed, elapsed time: 0 hours, 0 minutes, 56.89 seconds.	
2.5.3	Quota Failover Options 1. Large quota count environments now have new options to collect inventory of quotas and pre sync quotas before failover, and allow skipping of quota failover option. a. Admin Guide 2. Data Integrity failover option will continue on errors to restore permissions after the failover completes, and log any failures to the failover log.	
2.5.6	See feature list here 1. New copy to clipboard feature on the failover log, also option to open support site with a simple click to to open. 2. Updated Failover log format clearly documents each step in sections, and indicates sections with a warning with yellow text. Much simpler to understand the steps success. 3. Pop up Window indicates when data access testing is possible for each policy in the failover. Direct link to supporting documentation on how to test SMB and NFS access to data. This accelerates data access testing without needing to send the failover log to support to provide this feedback. 4. DR Rehearsal mode allows a new failover work flow to test and throw away changes during a DR test. 5. DFS mode auto SMB share auto rollback feature. 6. New validations for Access Zone and IP pool failover mode checks Dual DNS delegation configuration for all SmartConnect names and aliases along with diagnostics on what is mis-configured. 7. SPN AD Delegation test will validate of AD	

	delegation is completed correctly by testing SPN adds, deletes and indicates mis-configured AD Delegation for each cluster. 8. SyncIQ domain mark validation will warn if the domain mark step for accelerated failback is not been completed or enabled on the SyncIQ policy. 9. Concurrent failover mode is now enabled by default after upgrade.	

1.2. Failover Planning

Home Top

Failover Planning

- Are you Planning a failover?
- Do I need to remount shares with Access Zone Failover or Pool failover?
- How to determine best approach for Quota for failover?
- Quota failover options:
- Access Zone Failover
- IP Pool Failover
- SyncIQ DFS Mode with Eyeglass
- SyncIQ Mode with Eyeglass
- DR Rehearsal Mode
- Failover Readiness

Are you Planning a failover?

We recommend you review our planning checklist for proven process to successfully failover:

Failover Planning Guide and checklist

For a summary of Best Practices for Eyeglass and PowerScale Refer to Eyeglass and PowerScale DR Best Practices.

Do I need to remount shares with Access Zone Failover or Pool failover?

This is a common question the data integrity failover option helps improve and reduce the impact on the client machine with Access Zone and IP pool failover. The data integrity failover feature disconnects the netbios session for all shares involved in a failover. This also removes the cached IP session to the source cluster. After the DNS redirect step is completed Windows machines can mount the DR cluster correctly with some exceptions identified below.

Windows machines can re-establish the netbios session and query DNS to get an IP from the DR cluster. This avoids a remount requirement on the Windows machine.

Limitations

1. A machine with an open file will continue to cache the source cluster netbios session.
2. Machines with no active open file can switch clusters without a remount requirement.
3. A user active using explorer on the share that was failed over will still cache the netbios session of the source cluster, and will require a remount of the share.

How to determine best approach for Quota for failover?

Quota have some challenges for failover with Onefs 8.x.   The quota scan job runs as soon as new quotas are created. The quota scan job sets a flag on newly created quotas to indicate when the quota domain has been created.   SyncIQ operations that conflict when Quotas are marked with a flag indicating the quota domain has not been created yet. This can fail SyncIQ operations for make writable or resync prep step in a failover.

Quota failover options:

1. Failover quotas before a planned failover and leave quotas on both clusters after failover.
    a. During Failover use the new skip failover option by unchecking the quota check box and the quota step of the failover will be skipped leaving quotas on the source cluster. This should be used if failing over and back within a weekend to avoid interference from quota scan and SyncIQ. The quotas will not be required for the failover testing, and it is safer to leave them on source cluster.
        i. NOTE: On failback make sure to uncheck the quota failover option.
    b. New option in 2.5.3 or later see the CLI guide to enable quota inventory job to collect quotas on a new job on a default twice per day schedule. Pre-sync quotas is also available as well using a new quota sync schedule job. CLI guide. This will ensure quota's are not failed over and are pre-staged on the target DR cluster at all times.
        i. **NOTE: Use the skip quota option in DR Assistant if pre-syncing quotas.**

Access Zone Failover

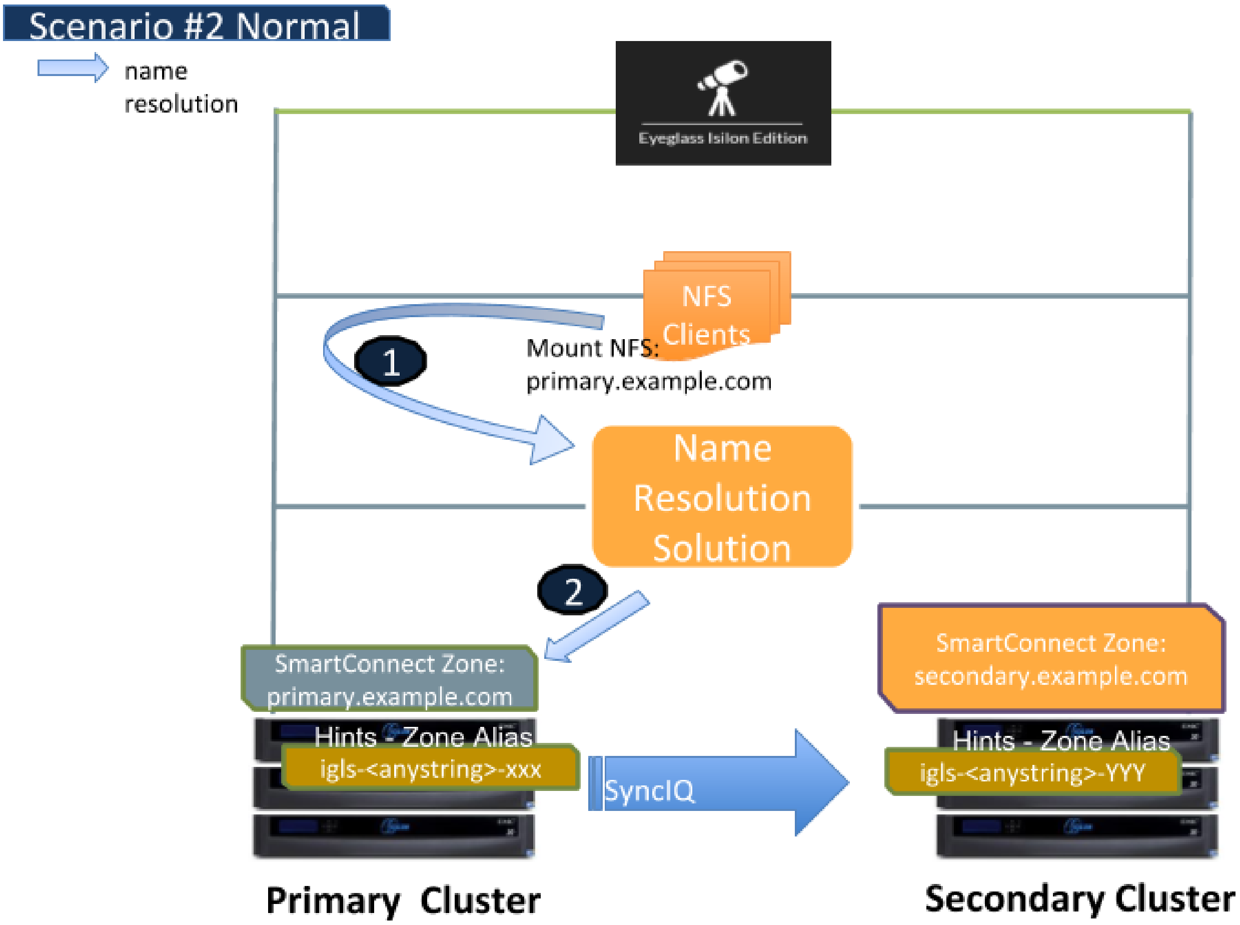
Eyeglass uses the Access Zone as the basis for grouping data for failover when customers choose not to use DFS mode or per SyncIQ. This Access Zone is selected as the unit of failover to simplify the DR readiness to the Access Zone level planning and failover operations. Shares, exports and quotas can be failed over with this mode of failover.

Access Zone failover includes networking failover of SmartConnect Zones and any SmartConnect Zone aliases that exist as well. Eyeglass must failover **ALL** IP pools that are members of the Access Zone and all aliases, which means all SyncIQ policies and **ALL** shares, exports and quotas must failover at the same time. The SmartConnect failover process requires the source cluster zone names to be renamed (not deleted) during failover to avoid SPN collisions in Active Directory, and to prevent clients from mounting the source cluster after failover.

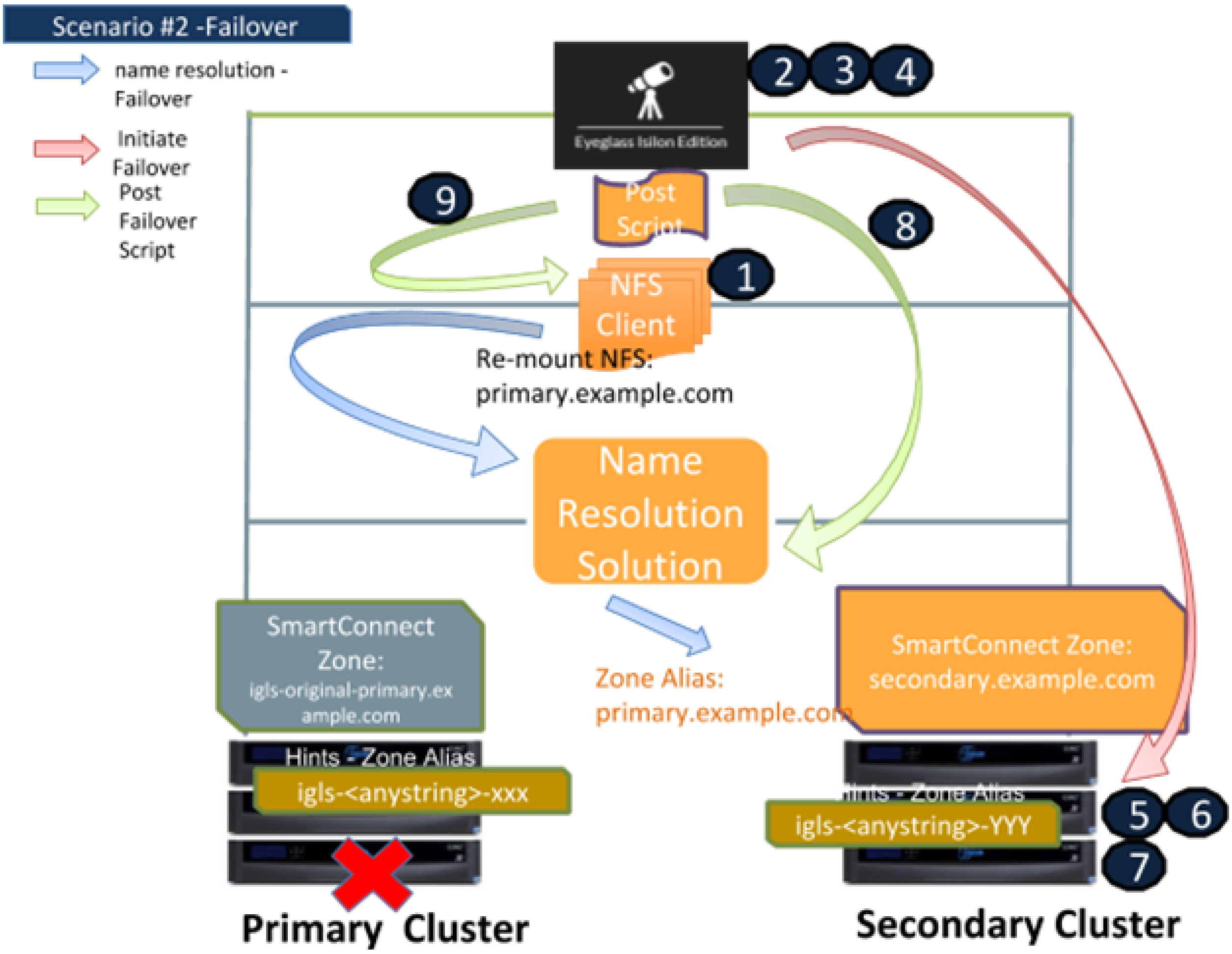
This requires planning and mapping of IP pools from source to target clusters before readiness for the Access Zone is marked as ready for failover.

In addition, SMB authentication depends on the AD machine account to have the correct and SPN values for SmartConnect Zones, failover and authentication depend on SPN’s being registered with the cluster that is writable . Eyeglass Access Zone failover automates SPN management. Eyeglass Access Zone failover also creates SmartConnect Zone aliases required to access data with a simple DNS update that that will delegate the SmartConnect Zone to the PowerScale cluster. (**NOTE: DFS mode does not require DNS, SPN and SmartConnect Zone changes during failover**)

The following figure shows Cluster Configuration Before Access Zone Failover. This is the normal state with primary and secondary clusters available. Preparation for Failover is the creation of mapping hints before failover.



The following second figure shows the Cluster Configuration Access Zone Failover Steps with the Primary Cluster not accessible (e.g. Real DR example)



Eyeglass DR Assistant - Access Zone Failover - Summary

1. Ensure that there is no live access to data, OR enable the Data Integrity failover option to disable access to SMB Shares before failover.
2. Begin Failover **(Eyeglass automated).**
3. Validation **(Eyeglass automated).**
4. Set configuration replication for policies to USERDISABLED **(Eyeglass automated).**
5. Provide write access to data on target **(Eyeglass automated).**
6. Move SmartConnect Zone to Target **(Eyeglass automated).**
7. Update SPN to allow for authentication against target **(Eyeglass automated).**

8. Repoint DNS to the Target cluster IP address (use post failover script) **(Eyeglass automated with scripting).**
9. Refresh session to pick up DNS change (use post failover script) **(Eyeglass automated with scripting).**

For details on this failover mode consult the Access Zone Failover Guide link.

IP Pool Failover

Eyeglass now offers IP pools as new failover unit within an Access Zone. The IP pool is selected as the unit of failover to simplify the DR readiness to the IP pool now has its own DR Readiness calculation and failover operations. Shares, exports and quotas can be failed over with this mode of failover.

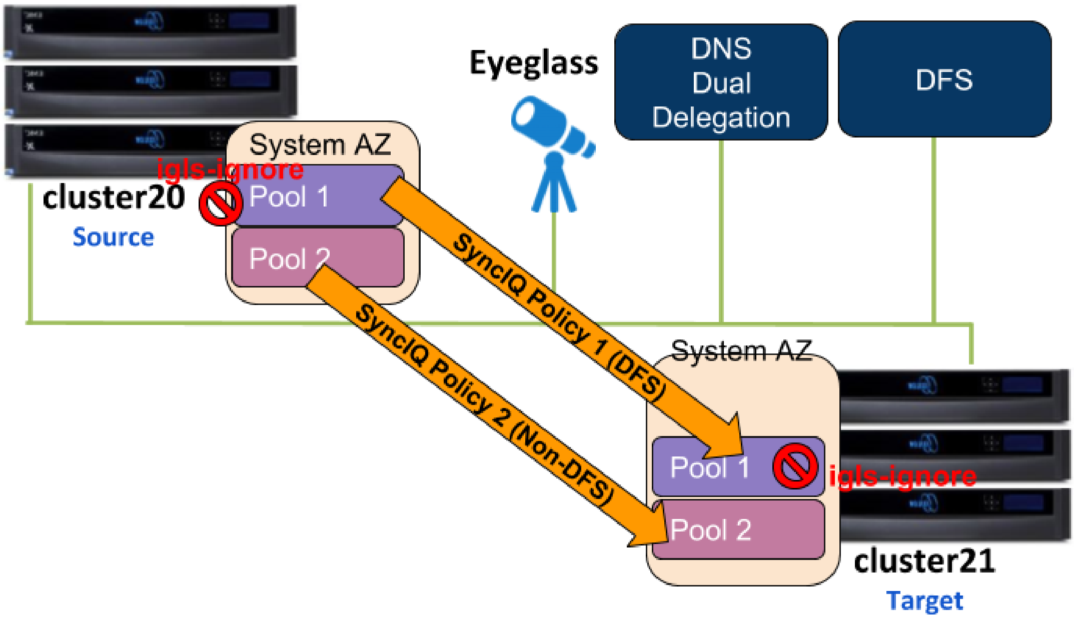
IP pool failover includes networking failover of SmartConnect Zones and any SmartConnect Zone aliases that exist as well. Eyeglass must failover **ALL** policies mapped to the Pool using IP pool policy mapping UI in the DR Dashboard. All SmartConnect names and aliases configured on the pool, and all mapped SyncIQ policies plus **ALL** shares, exports and quotas associated to the SyncIQ policies will failover at the same time.   The SmartConnect failover process requires the source cluster zone names to be renamed (not deleted) during failover to avoid SPN collisions in Active Directory and to prevent clients from mounting the source cluster after failover.

This requires planning and mapping of IP pools from source to target clusters before readiness for the pools is marked as ready for failover.

It also requires converting an Access Zone to IP pool failover, which means all pools within an Access Zone must have a policy mapped to a pool before ANY pool in the zone can be failed over.

In addition, SMB authentication depends on the AD machine account to have the correct and SPN values for SmartConnect Zones. Failover and authentication depend on SPN's being registered with the cluster that is writable . Eyeglass IP pool failover automates SPN management, along with SmartConnect Zone aliases creation needed to access data with a simple DNS update that delegates the SmartConnect Zone to the PowerScale cluster. (**NOTE: DFS mode does not require DNS, SPN and SmartConnect zone changes during failover**). DFS IP pools can be failed with Pool failover feature.

The following figure shows IP Pool Failover with the Primary Cluster is not accessible (e.g. Real DR example):



Eyeglass DR Assistant - IP pool Failover - Summary

1. Ensure that there is no live access to data, OR enable Data Integrity failover option to disable access to SMB Shares before failover.
2. Begin Failover **(Eyeglass automated).**
3. Validation **(Eyeglass automated).**
4. Set configuration replication for policies to USERDISABLED **(Eyeglass automated).**
5. Provide write access to data on target **(Eyeglass automated).**
6. Move SmartConnect zone to Target **(Eyeglass automated).**
7. Update SPN to allow for authentication against target **(Eyeglass automated).**
8. Repoint DNS to the Target cluster IP address (use post failover script) **(Eyeglass automated with scripting).**
9. Refresh session to pick up DNS change (use post failover script) **(Eyeglass automated with scripting).**

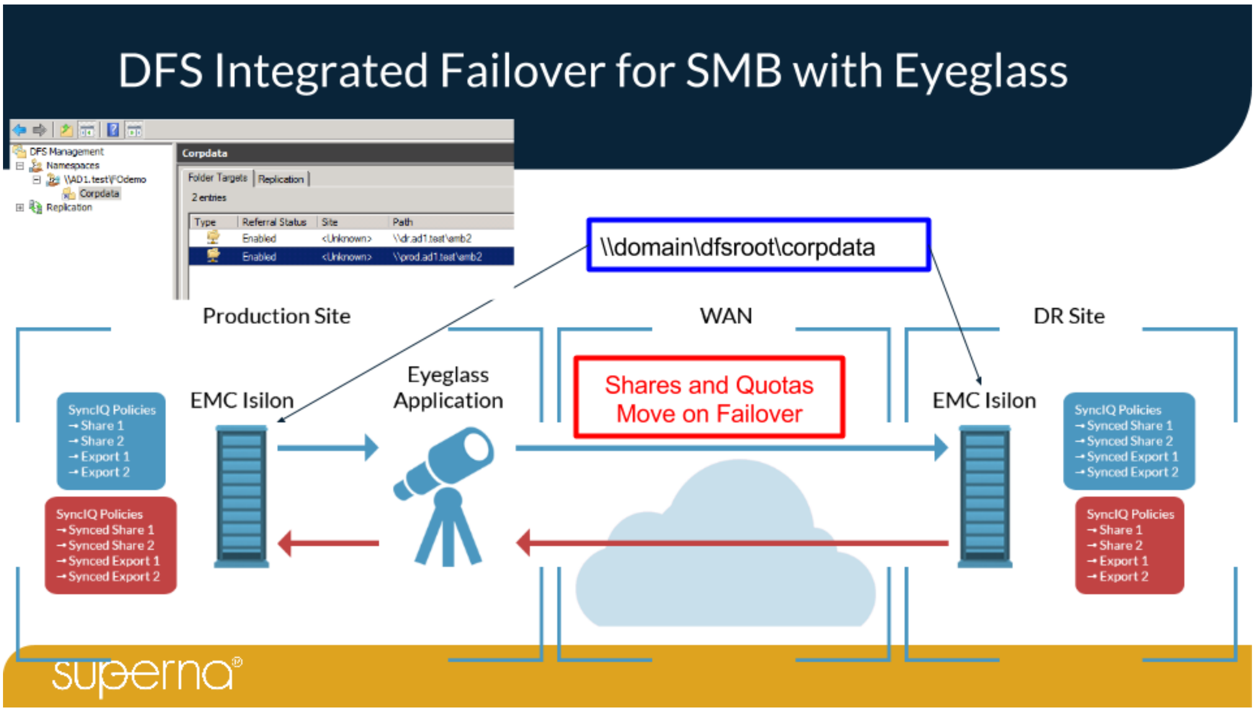
For details on this failover mode consult the Access Zone Failover Guide link.   Look for the IP pool failover section.

SyncIQ DFS Mode with Eyeglass

This mode enables the most seamless failover and failback operations with full Quota failover/failback integration (excluding exports). The solution enables zero touch client failover to always mount the writable copy of the SyncIQ data with quotas active, and requires no DNS updates, no remount, no re-authentication.

This is achieved using DFS folder UNC targets (with the same share name), a SmartConnect Zone for each cluster setup with DFS to use both clusters, and Eyeglass ensures shares only existing on **one** cluster at a time and **moves** them during failover events. The DFS Target folder - path to the Secondary cluster will automatically be activated once the shares are created by Eyeglass.

NOTE: It's possible to use 2 different SmartConnect Zones on source and destination cluster so that nothing needs to change during failover on either cluster. The following figure shows typical DFS folder setup:



Type	Referral Status	Site	Path
	Enabled	<Unknown>	\\dr.ad1.test\amb2
	Enabled	<Unknown>	\\prod.ad1.test\amb2

Eyeglass DR Assistant - DFS Mode Failover - Summary

1. Ensure that there is no live access to data, OR enable Data Integrity failover option to disable access to SMB Shares before failover.
2. Begin Failover **(Eyeglass automated).**
3. Validation **(Eyeglass automated)**.
4. Set configuration replication for policies to USERDISABLED **(Eyeglass automated).**

5. Provide write access to data on target **(Eyeglass automated).**
6. (Not performed and not required) Move SmartConnect zone to Target **(Eyeglass automated).**
7. (Not performed and not required) Update SPN to allow for authentication against target **(Eyeglass automated).**
8. (Not performed and not required) Repoint DNS to the Target cluster IP address (use post failover script) **(Eyeglass automated with scripting).**
9. Fail over Shares and Quotas - shares and quotas are created on target and deleted from the source cluster **(Eyeglass automated).**
10. DFS Clients automatically switch to DR cluster with DFS 2nd Folder UNC target path.

For Details on this failover mode consult the Microsoft DFS Mode Failover Guide link.

SyncIQ Mode with Eyeglass

This mode of failure allows targeted failover with some manual steps that allows selected policies to failover without entire Access Zone of policies. Since no SPN management is performed with this failover type, it is better suited to NFS export failover + quotas. Shares and exports are pre-synced with Eyeglass so both protocols are supported with this mode.

This failover mode does not automate SmartConnect Zone failover as is done with Access Zone failover. This means selective SmartConnect Zones can be failed over requiring manual SmartConnect Zone aliases and DNS update to complete the failover.

This mode of failover is also useful with post failover script engine that can execute host side unmount and remount commands using scripts and leveraging the samples provided with Eyeglass. Superna Professional Services can also be engaged to build host side scripts for customer requirements.

Review the Script Engine Overview section in the Eyeglass Administration Guide

These scripts allow simple SSH based remote host unmount and remount automation but can also be done without needing to update DNS since the target cluster SmartConnect Zone can be mounted directly once the SyncIQ policy is marked writable on the target cluster.

We recommend this option for automation when the host count is <30. If the host count is higher we recommend Access Zone failover and DNS updates.

The following diagrams show the flow of failover and steps with sample commands that would be run during the Eyeglass policy failover. The SPN commands are shown if SMB manual failover is being executed.

For Details on this failover mode consult the SyncIQ Policy Failover Guide.

DR Rehearsal Mode

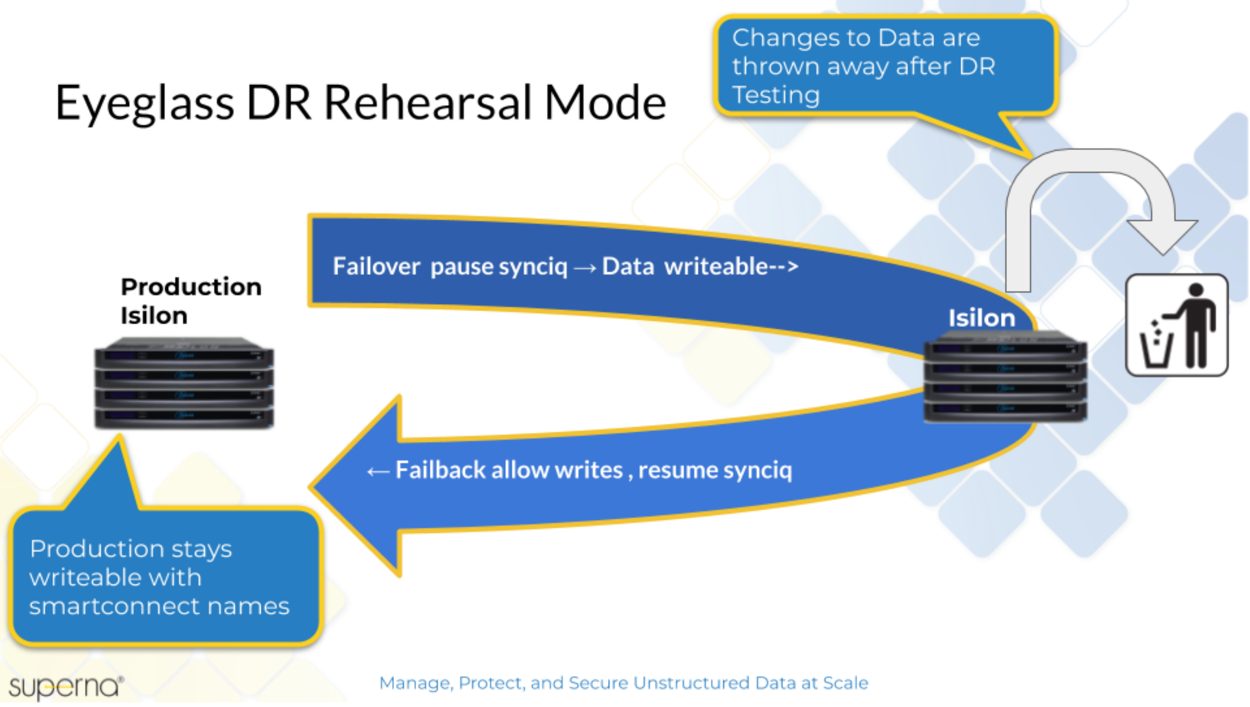
This is a new failover mode that allows the target cluster to have its file system writable while production cluster stays in production. During this time only 1 copy of data exists, when DR Rehearsal mode is disabled the changes to the target cluster are discarded and re-synced from the production cluster. A different DNS name is required to mount the data.

Pros:

1. Faster failover and testing is possible.
2. Production stays operational .
3. AD and network cloning is possible to mirror production .

Cons:

1. Data is not synced during the testing.



Eyeglass DR Rehearsal Mode

Changes to Data are thrown away after DR Testing

Failover pause synciq → Data writeable-->

← Failback allow writes , resume synciq

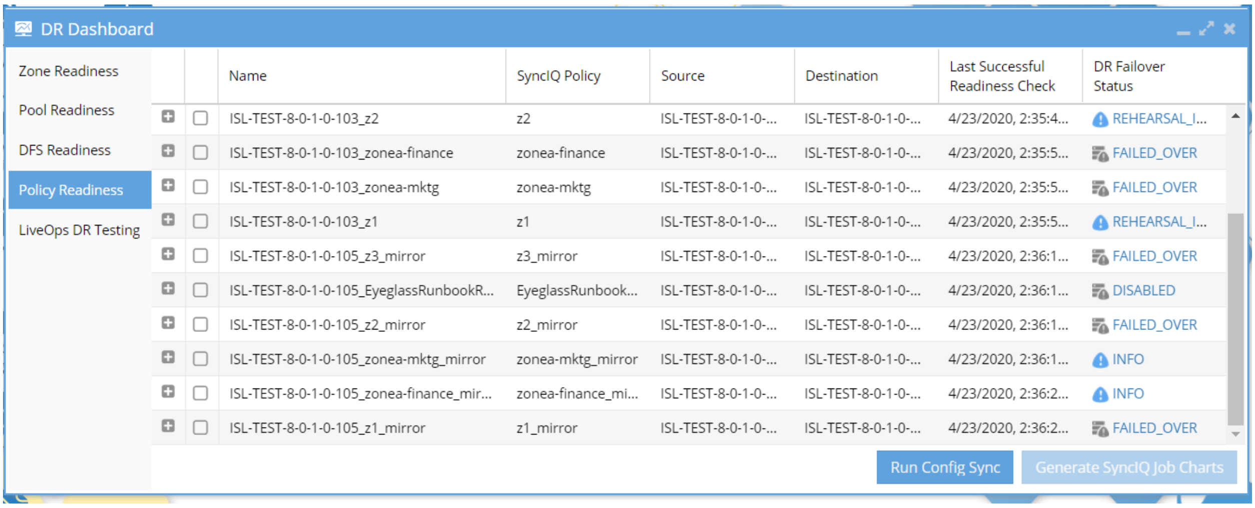
Production stays writeable with smartconnect names

superna

Manage, Protect, and Secure Unstructured Data at Scale

Failover Readiness

The Eyeglass assisted failover has diagnostics to detect when failover is not possible or recommended, and updates a simple DR Dashboard to indicate your current state.



		Name	SyncIQ Policy	Source	Destination	Last Successful Readiness Check	DR Failover Status
⊞	□	ISL-TEST-8-0-1-0-103_z2	z2	ISL-TEST-8-0-1-0-...	ISL-TEST-8-0-1-0-...	4/23/2020, 2:35:4...	REHEARSAL_I...
⊞	□	ISL-TEST-8-0-1-0-103_zonea-finance	zonea-finance	ISL-TEST-8-0-1-0-...	ISL-TEST-8-0-1-0-...	4/23/2020, 2:35:5...	FAILED_OVER
⊞	□	ISL-TEST-8-0-1-0-103_zonea-mktg	zonea-mktg	ISL-TEST-8-0-1-0-...	ISL-TEST-8-0-1-0-...	4/23/2020, 2:35:5...	FAILED_OVER
⊞	□	ISL-TEST-8-0-1-0-103_z1	z1	ISL-TEST-8-0-1-0-...	ISL-TEST-8-0-1-0-...	4/23/2020, 2:35:5...	REHEARSAL_I...
⊞	□	ISL-TEST-8-0-1-0-105_z3_mirror	z3_mirror	ISL-TEST-8-0-1-0-...	ISL-TEST-8-0-1-0-...	4/23/2020, 2:36:1...	FAILED_OVER
⊞	□	ISL-TEST-8-0-1-0-105_EyeglassRunbookR...	EyeglassRunbook...	ISL-TEST-8-0-1-0-...	ISL-TEST-8-0-1-0-...	4/23/2020, 2:36:1...	DISABLED
⊞	□	ISL-TEST-8-0-1-0-105_z2_mirror	z2_mirror	ISL-TEST-8-0-1-0-...	ISL-TEST-8-0-1-0-...	4/23/2020, 2:36:1...	FAILED_OVER
⊞	□	ISL-TEST-8-0-1-0-105_zonea-mktg_mirror	zonea-mktg_mirror	ISL-TEST-8-0-1-0-...	ISL-TEST-8-0-1-0-...	4/23/2020, 2:36:1...	INFO
⊞	□	ISL-TEST-8-0-1-0-105_zonea-finance_mir...	zonea-finance_mi...	ISL-TEST-8-0-1-0-...	ISL-TEST-8-0-1-0-...	4/23/2020, 2:36:2...	INFO
⊞	□	ISL-TEST-8-0-1-0-105_z1_mirror	z1_mirror	ISL-TEST-8-0-1-0-...	ISL-TEST-8-0-1-0-...	4/23/2020, 2:36:2...	FAILED_OVER

For Access Zones or IP pools, the DR Dashboard indicates when any of the following need attention: Data sync issues, configuration sync issues, SPN out of sync conditions and invalid IP pool mapping for IP pool or Access Zone failover.

The DR Dashboard also provides a per SyncIQ readiness and DFS mode policy dashboard for SyncIQ + configuration sync readiness. This allows sub Access failover readiness to be assessed versus the entire Access Zone. Eyeglass validates your DR readiness at regular intervals and will notify you via Eyeglass external alarming (if configured) if a problem is detected.

The Eyeglass Runbook Robot feature is another way to validate your readiness by automating a failover on a specific, non-production “EyeglassRunbootRobot” Access Zone or SyncIQ Policy every night at midnight. This exercises the actual failover steps in your environment daily and will also notify you via Eyeglass external alarming (if configured) when a problem is detected.

This feature operates as cluster witness and mounts the cluster over NFS and writes and reads back test data to verify failover from the client view of the cluster.   It can be configured in basic or advanced modes. See Runbook Robot admin guide.

The basic mode only uses a SyncIQ policy for failover with no other logic running. Easy to setup and provides quick test of failover and failback.

The advanced mode tests all logic and operates with the Access Zone failover mode and provides the same NFS write and re-read logic in addition to SPN management and SmartConnect Zone mapping and failover logic.

1.3. Storage Failover with Eyeglass Failover Modes

Home Top

Storage Failover with Eyeglass Failover Modes

The following section outlines the storage layer failover steps. The full end to end DR plan should also include application shutdown and bring up procedures to complete a true end to end failover. The storage layer is the foundation upon which all higher layer failover depends, and Eyeglass ensures this step is simple to execute and detect errors during failover.

Superna Professional Services can be engaged on end to end POC, or recommendations and assessments for complex or application layer orchestrated failover scenarios. Examples include:

1. VMware SRM + externally mounted storage by VM’s.
2. Oracle RAC Data Guard + File System dependencies for applications.
3. Please see Eyeglass Solutions page.

Once you have determined which Failover Mode is appropriate for your environment, the table below provides the high level steps for each mode:

Column 1 - Ordered Steps: Ordered steps and purpose of step.

Column 2 - Description: Description of action taken by step.

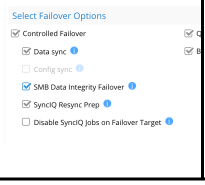
Column 3 - How Action is Initiated: How each step is executed with Eyeglass depending on whether a SyncIQ Policy Failover, or Microsoft DFS Mode failover is being done.

Column 5 - Ordered Steps for Access Zone OR IP Pool Failover: - Ordered steps and purpose of step.

Column 6 - Description: Description of action taken by step.

Column 7 - How Action is Initiated: for Access Zone or IP Zone Failover.

Target of operation is shown in brackets as source, target or Eyeglass in the table below.

Ordered Steps for - Non DFS and DFS Mode	Description	How Action is Initiated DFS Mode		Ordered Steps for - Access Zone OR IP Pool Failover	Description	How Action is Initiated Access Zone
		SyncIQ Mode	DFS Mode			
1 - Ensure that there is no live access to data (source) (**See new feature in 1A in 2.0 or later**)	Manual check for open files. If Open files found, decide whether to failover or wait to be closed. NOTE: DR Assistant Data Integrity failover option for 2.0 or later releases blocks IO to SMB shares before failover.  Select Failover Options ☑ Controlled Failover ☑ Data sync □ Config sync ☑ SMB Data Integrity Failover ☑ SyncIQ Resync Prep □ Disable SyncIQ Jobs on Failover Target ☑ Q ☑ B	Manual	Manual	1 - Ensure that there is no live access to data (source)	Manual check for open files. If Open files found, decide whether to failover or wait to be closed. **It is recommended to always disable SMB**	Manual

	It is recommended to always disable SMB and NFS protocols on the SOURCE cluster prior to failover WHICH IS A CLUSTER WIDE OPERATION to eliminate data loss.				**and NFS protocols on the SOURCE cluster prior to failover WHICH IS A CLUSTER WIDE OPERATION to eliminate data loss.**	
1a - Enable Data Integrity Failover (SMB only)	Applies Deny Everyone to SMB shares before failover starts	Automated by Eyeglass	Automated by Eyeglass	1a - Enable Data Integrity Failover (SMB only)	Applies Deny Everyone to SMB shares before failover starts	Automated by Eyeglass
1b - Cache schedule for SyncIQ policies being failed over and prevent SyncIQ policies being failed over from running (source)	Get schedule associated with the SyncIQ policies being failed over on OneFS, set policies to manual so they don't run again during failover	Automated by Eyeglass	Automated by Eyeglass	1a - Cache schedule for SyncIQ policies being failed over and prevent SyncIQ policies being failed over from running (source)	Get schedule associated with the SyncIQ policies being failed over on OneFS, set policies to manual so they don't run again during failover	Automated by Eyeglass
2 - Begin Failover with DR Assistant (Eyeglass)	Initiate Failover from Eyeglass	Manual or Eyeglass REST API	Manual Eyeglass REST API	2 - Begin Failover with DR Assistant (Eyeglass)	Initiate Failover from Eyeglass	Manual or Eyeglass REST API
3 - Validation of failover job (Eyeglass)	Verify all warnings before submitting the failover job	Automated by Eyeglass	Automated by Eyeglass	3 - Validation of failover job (Eyeglass)	Verify all warnings before submitting the failover job	Automated by Eyeglass
3a - Validation - Block on Warning	Will prevent continuing a	Automated by	Automated by	3a - Validation - Block on	Automated by	Automated by Eyeglass

enabled	failover on warnings (quota scan required detection)	Eyeglass	Eyeglass	Warning enabled	Eyeglass	
3b - Set Eyeglass config Jobs to **userdisabled**	This sets config jobs to user disabled state to prevent failed steps from allowing these jobs to run unless a user enables them post failover	Automated by Eyeglass	Automated by Eyeglass	3b - Set Eyeglass config Jobs to **userdisabled**	Automated by Eyeglass	Automated by Eyeglass
4 - Synchronize data (Run SyncIQ policies) (source) **(parallelized step)3**	Run all OneFS SyncIQ policy jobs related to the Access Zone being failed over	Automated by Eyeglass	Automated by Eyeglass	4 - Synchronize data (run SyncIQ policies) (source) **(parallelized step)3**	Run all OneFS SyncIQ policy jobs related to the Access Zone being failed over	**Automated by Eyeglass** (all policies in the Access Zone)
5 - Synchronize configuration (shares/export/alias, snapshot schedules, dedupe paths) (Eyeglass)(**parallelized step)3**	Run Eyeglass configuration replication	**Automated by Eyeglass** (configuration exists on source and target)	**Automated by Eyeglass**	5 - Synchronize configuration (shares/export/alias, snapshot schedules, dedupe paths) (Eyeglass) **(parallelized step)3**	Run Eyeglass configuration replication	**Automated by Eyeglass** (based on matching Access Zone base path)
6 - Renaming shares DFS mode to redirect DFS clients (multi threaded) **(parallelized step)3**	For DFS Failover, shares renamed on source and target cluster so clients are redirected with dual DFS target paths to target cluster	Not Applicable	**Automated by Eyeglass** (special handling renames Shares on source and target so that only one DFS target UNC is reachable and active for DFS clients to switch	NOTE: It is possible to integrate DFS protected data inside an Access Zone failover to protect Shares , exports and DFS data with Access Zone failover.	If DFS configured redirect rename steps would executed at this point	**Automated by Eyeglass** (based on matching Access Zone base path)
				6 - Change SmartConnect Zone on Source so not to resolve by Clients (source) (dual delegation eliminates DNS updates)	Rename SmartConnect Zones and Aliases (Source)	**Automated by Eyeglass** (based on matching Access Zone base path)

			over)	7 - Avoid SPN Collision (source)	Sync SPNs in all AD providers to current SmartConnect Zone names and aliases (proxy through target cluster (Source)	**Automated by Eyeglass** (AD delegation must be completed as per install docs)
9 - Provide write access to data on target (target) (single threaded for safe failover) **(parallelized step)3**	Allow writes to SyncIQ policy(s) related to failover2	Automated by Eyeglass	Automated by Eyeglass	8 - Move SmartConnect Zone to Target (target)	Add source SmartConnect Zone(s) and Alias(s) on (Target)	Automated by Eyeglass
10 - Resync prep Step SyncIQ - Disable SyncIQ on source and make active on target (source) **(parallelized step)3**	Resync prep SyncIQ policy step to failover (Creates Mirror Policy on target and disables source cluster policy and enables target cluster policy OneFS	Automated by Eyeglass	Automated by Eyeglass	9 - Update SPN to allow for authentication against target (target)	Sync SPNs in all AD providers to current SmartConnect Zone names and aliases (proxied through target cluster) (Target)	**Automated by Eyeglass**
11- Re-Set SyncIQ schedule on target mirror policy (target)	Set schedule on Mirror Policy(Target) using schedule from step 1 from OneFS for policy(s) related to the Failover job	Automated by Eyeglass	Automated by Eyeglass	10 - Repoint DNS to the Target cluster IP address	DNS Dual delegation for all SmartConnect Zones that are members of the Access Zone	**Automated by Eyeglass** (See "Geographic Highly Available Storage solution with Eyeglass Access Zone Failover and Dual Delegation")
12 - Failover quota(s) (Eyeglass) (option	Eyeglass DR Assistant automatically	**Automated by Eyeglass** (	**Automated by Eyeglass** (	12 - Failover quota(s) (Eyeglass) (o	Eyeglass DR Assistant	**Automated by Eyeglass** (

al can be skipped) **(parallelized step)3**	fails over quotas by running the Quota Jobs related to the SyncIQ Policy(s) being failed over	deleted on source cluster and created on target cluster)	deleted on source cluster and created on the target cluster so that post failover quotas are applied)	ptional can be skipped) **(parallelized step)3**	automatically fails over quotas by running the Quota Jobs related to the SyncIQ Policy(s) being failed over	deleted on source cluster and created on target cluster)
13 - Remove quotas on directories that are target of SyncIQ (PowerScale best practice) (source) **(parallelized step)3**	Eyeglass deletes all quotas on the source for all the policies	Automated by Eyeglass	Automated by Eyeglass			
13a - Run Mirror policy **(parallelized step)3**	Run policy to resync data in reference direction	Automated by Eyeglass	Automated by Eyeglass	13a - Run Mirror policy **(parallelized step)3**	Run policy to resync data in reference direction	Automated by Eyeglass
13b - Set Eyeglass config Jobs to **enabled**	Enables configuration sync ONLY if Resync prep completes successful for the policy	Automated by Eyeglass	Automated by Eyeglass	13b - Set Eyeglass config Jobs to **enabled**	Enables configuration sync ONLY if Resync prep completes successful for the policy	Automated by Eyeglass
14 - Change SmartConnect Zone on Source so that names are not resolved by Clients (source)	Rename SmartConnect Zones and Aliases (Source)	Manual	**Not Required** (source and destination clusters can use existing SmartConnect Zones)	14 - Disable SyncIQ on source and make active on target (source)	Resync prep SyncIQ policy step to failover (Creates Mirror Policy on target and disables source cluster policy and enables	Automated by Eyeglass

					target cluster policy OneFS **(parallelized step)3**	
15 - Avoid SPN Collision (source)	Sync SPNs in all AD providers to current SmartConnect Zone names and aliases (Source)	**Manual** (deletes SmartConnect SPN from source cluster machine account)	**Not Applicable** (DFS SPN's are not changed during failover)	15 - Set proper SyncIQ schedule on target (target)	Set schedule on Mirror Policy(Target) using schedule from step 6 from OneFS for policy(s) related to the Failover	**Automated by Eyeglass**
16 - Move SmartConnect Zone to Target (target)	Add source SmartConnect Zone(s) as Alias(s) on (Target)	Manual	**Not Required** (source and destination clusters can use existing SmartConnect Zones)	16 - Synchronize quota(s) (Eyeglass) **(parallelized step)3**	Run Eyeglass Quota Jobs related to the SyncIQ Policy or Access Zone being failed over	Automated by Eyeglass
17 - Create SPN's to allow for kerberos authentication against target for SMB shares (target)	Sync SPNs in all AD providers to current SmartConnect Zone names and aliases (Target)	**Manual** (adds new SmartConnect alias SPN's to target cluster machine account)	**Not Applicable** (DFS SPN's are not changed or registered to Cluster machine accounts)	17 - Remove quotas on directories that are target of SyncIQ (PowerScale best practice) (source) **(parallelized step)3**	Delete all quotas on the source for all the policies	**Automated by Eyeglass** (Requires IP pool hints are configured See docs)
18 - Repoint DNS to the Target cluster IP address	Update DNS delegations for all SmartConnect Zones that are members of the Access Zone	Manual	**Not Applicable** (no updates are needed as DFS resolution has not changed in DNS, only the target UNC with	18 - Repoint DNS to the Target cluster IP address	Dual Delegation feature with Eyeglass avoids any DNS steps during failover for all SmartConnect Zones	**Automated by Eyeglass** (see dual delegation one time configuration here)

			an active share		that are failed over	
19 - Refresh session to pick up DNS change	Remount the SMB/NFS share(s) **(if data integrity issued remount is not required for SMB)**	**Manual** on clients	**Automatic** (Windows 7 or later with DFS support)	19 - Refresh session to pick up DNS change	Remount the SMB/NFS share(s) or remount exports **(if data integrity issued remount is not required for SMB)** See IP pool Interface Removal procedure for SMB.	**Automated by Eyeglass** using Dual SmartConnect Zone Delegation (How to Configure Here)

1. Initiates Eyeglass Configuration Replication task for all Eyeglass jobs.
2. SyncIQ does NOT modify the ACL (Access control settings on the file system), it locks the file system.   ls -l   will be identically on both source and target
3. System.xml change required to enable parallel step mode. NOTE: all policy steps are attempted. On failure, the failover job will continue to attempt all steps and skip downstream steps per policy if the previous SyncIQ step failed.

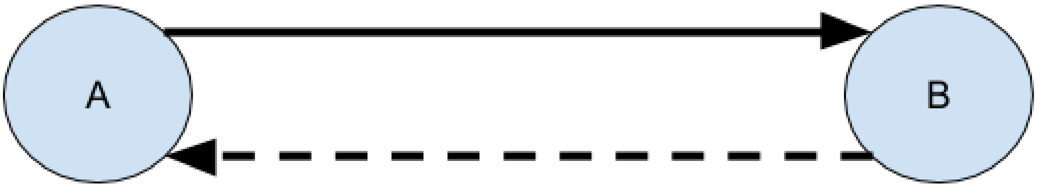
1.4. Supported DR Site and Failover Topologies

Home Top

Supported DR Site and Failover Topologies

This replication topology covers the scenario commonly used to remote sites. This allows for 1 or 2 DR copies of data to be available at different geographic distances. The option to automate failover end to end is possible with Access Zone and DFS mode failover.

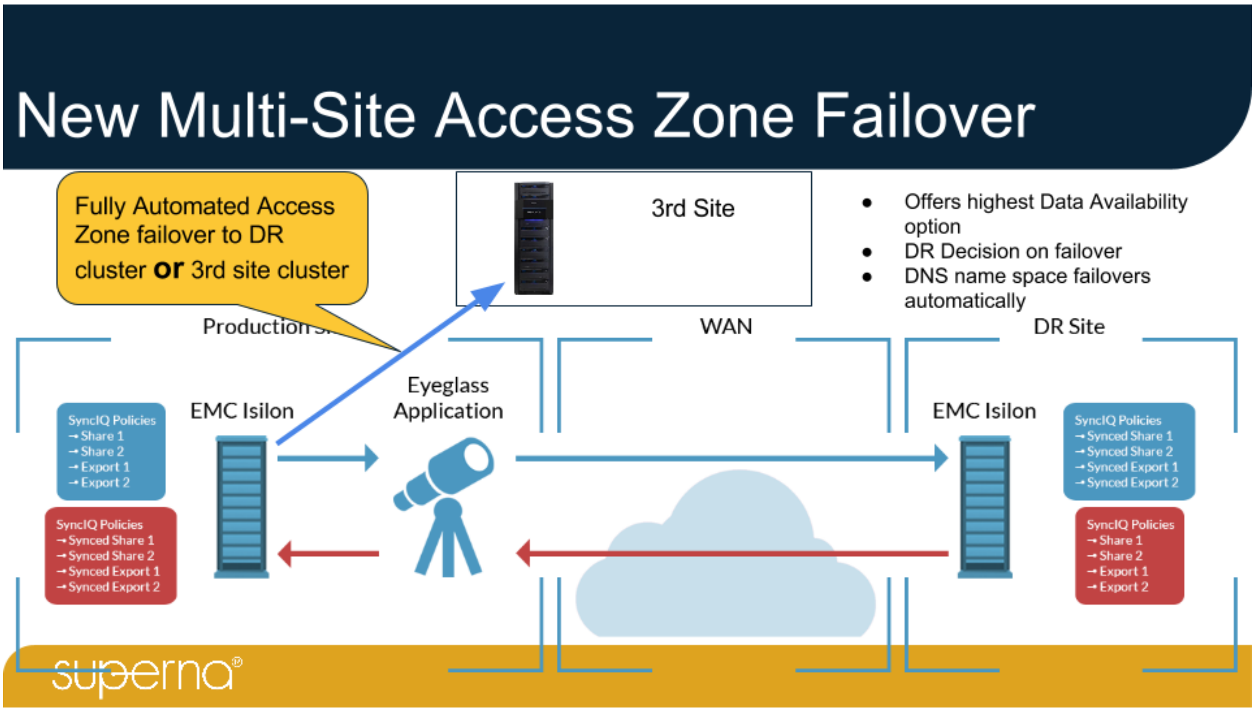
Data Center to Data Center



Supported Failover Modes

1. Access Zone - Fully automated any site failover.
2. DFS mode - Fully automated any site failover.
3. Per SyncIQ - partially automated any site failover.

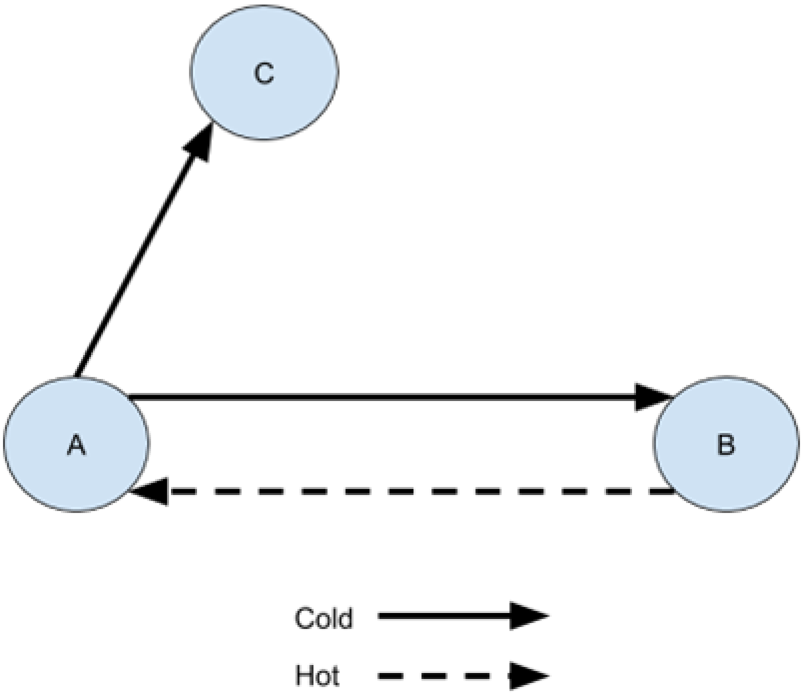
Multi Site Failover



New Multi-Site Access Zone Failover

Fully Automated Access Zone failover to DR cluster **or** 3rd site cluster

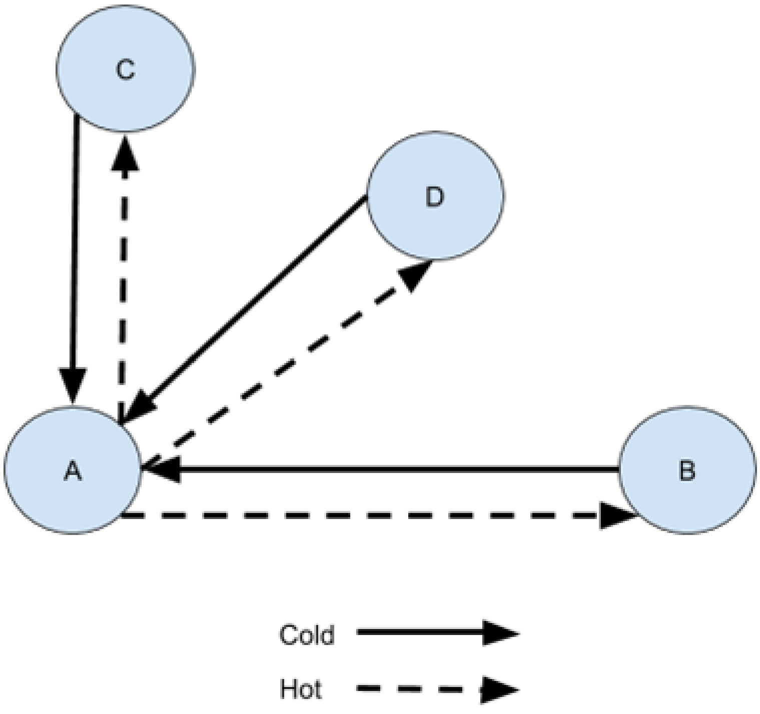
- Offers highest Data Availability option
- DR Decision on failover
- DNS name space failovers automatically



Supported Failover Modes (See Multi Site Failover Guide)

1. Access Zone - Fully automated any site failover.
2. DFS mode - Fully automated any site failover.
3. **Per SyncIQ - partially automated any site failover**

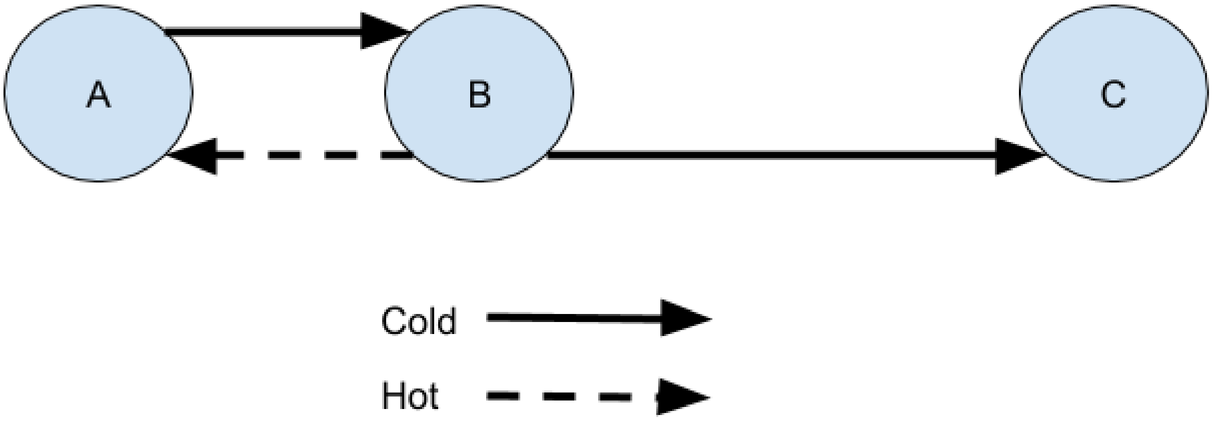
Data Center DR Fan-IN Topology



Supported Failover Modes

1. Per SyncIQ.
2. Access Zone.
3. DFS mode.

2 Site DR - Stretch 3rd site Configuration Sync



Supported Failover Modes

1. Access Zone (A to B) Config synced to C manual failover.

2. Per SyncIQ (A to B) Config synced to C manual failover.
3. DFS mode (A to B) Config synced to C manual failover.

1.5. How to Manage Custom None Default SPN's for Failover

Home Top

Overview

The default SPN used for Kerberos Windows client failover is HOST\ and this is managed for failover by Eyeglass in all releases. New in 2.5.6 or later releases is a the ability to add custom SPN's to be inserted into AD, based on SmartConnect names and alias and managed through failover process. In addition the igls- prefix alias SPN will also be auto inserted to suppress PowerScale alarms about missing SPN's. These SPN's will also be failed over to avoid creating new alarms after a failover.

Unsupported Use of this Feature

This feature is only supported for customers that use HDFS hadoop for failover. A known bug in OneFS raises an alarm for missing SPN's for HDFS, NFS and HTTP. These are used with hadoop deployments and are not required for NFS or SMB failover.   This feature is not supported to suppress these alarms on Isilon. Dell support should be contacted for procedure to suppress the alarms in Onefs that are incorrectly alarmed, when HDFS protocol is not enabled or licensed on a cluster.

SPN Handling in Eyeglass

This table shows each Eyeglass job type or function and how SPN's are managed.

Readiness Job (check for SPN errors, no create/delete) - database			**Inventory** / **Configuration Replication** (creates missing SPNs, no delete) - OneFS/*isi auth ads spn check*			**Access Zone/Pool Failover** (deletes and creates SPNs)		
Full SPN	**Short SPN**	**Igls-hint-, igls-original-**	**Full**	**Short**	**Igls-hint-, igls-original-**	**Full**	**Short**	**igls-original-**
Yes, checks for Full SPN version like **HOST/a.b.net.**	**No**, does not check for Short SPN version like **HOST/a**	**No,** does not check for missing *igls-hint* and *igls-orignal-* in GUI. But raises alarms (can't find them in Alarm GUI) about them in debug.log.	**Yes**, creates for Full SPN version like **HOST/a.b.net**	**No**, does not create Short SPN version example **HOST/a**	**Yes**, creates all missing *igls-hints-* example **igls-clusterABnet-PROD** and *igls-original-* like **/igls-original-a.b.net**.	**Yes**, creates for Full SPN version like **HOST/a.b.net** for Target cluster. Also deletes on other Cluster before creating the above	**Yes**, creates for short SPN version example **HOST/a** for Target cluster. Also deleted on other cluster before creating	**Yes**, creates Full and Short SPN version for Source cluster example **HOST/igls-original-a.b.net** and **HOST/igls-a**. Also deletes on other

							above	Cluster before creating the above.

Use Cases:

1. Kerberos NFS.
2. HADOOP deployments (HDFS\xxxx, WEB\xxxx).
3. SMB load balancers that use CIFS\xxxx spn.
4. Any other custom requirement .

How to add support for custom SPN's for auto insertion to AD and Failover

1. To add support for additional none standard SPN's follow these steps:
   a. Login to eyeglass as admin user .
   b. nano /opt/superna/sca/data/system.xml .
   c. Locate the tag <process> .
   d. locate the <spnserviceclass> tag and edit it as per below:
      i. include upper case HOST and then add other spn prefix that are required. NOTE: 8.2 and later Onefs will add nfs,hdfs, http (NOTE Lower case), 2.5.6 can be configured to manage these SPN's as well. Use example below.
   e. <spnserviceclass>HOST,nfs,hdfs,http</spnserviceclass>

f. control + x to save and exit

g. sudo -s (enter admin password) .

h. systemctl restart sca .

i. The above tag will insert nfs hdfs and web spn (with exact case) into AD spn property for ALL SmartConnect names and aliases.

j. The new AD validation will validate the new SPN service classes are in AD and raise a warning if they are not present. If AD delegation is done correctly Eyeglass will repair and insert any missing service class SPN's.

k. Failover will automatically manage all service class spn's in this tag for failover between clusters.

l. Done.

1.6. How to use the DR Dashboard to Assess Failover Readiness

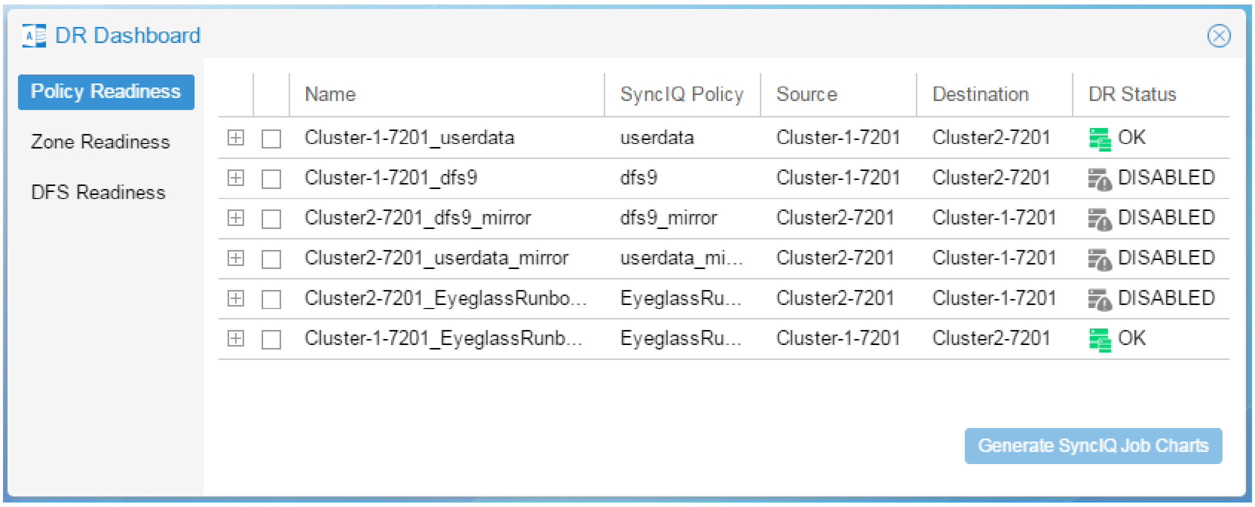
Home Top

How to use the DR Dashboard to Assess Failover Readiness

The DR Dashboard is the main status screen for overall cluster readiness for a DR event. The status column is sent as a critical alarm when a validation function is in Error state (SyncIQ, Config replication, SPN checks, Network IP Pool mapping readiness audit). This way you can address any issues that would affect your ability to failover when they are detected instead of discovering these issues at failover time.

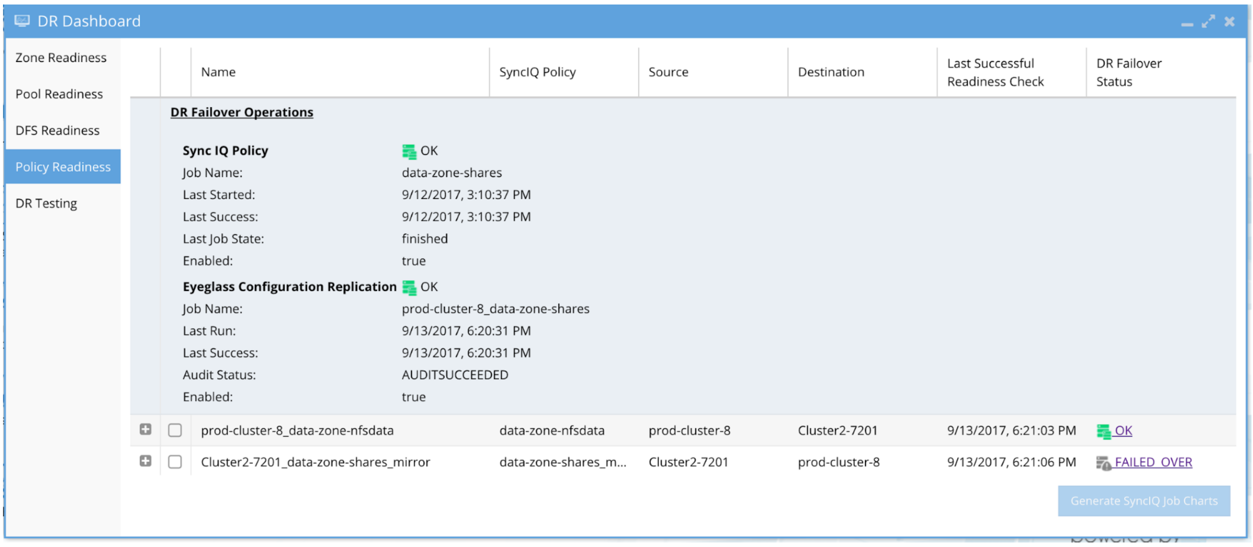
Policy Readiness / DFS Readiness

SyncIQ Policy Failover Readiness and SyncIQ DFS Mode Failover Readiness are based upon the status of the SyncIQ Policy Job (Data replication) in OneFS and the Eyeglass Configuration Replication Job (Configuration Replication) for that SyncIQ Policies related configuration data (shares, exports, and aliases). The status of these two are combined to provide an overall DR Status. The Policy Readiness and DFS Readiness are updated each time Eyeglass Configuration Replication is run.



DR Dashboard

		Name	SyncIQ Policy	Source	Destination	DR Status
⊞	□	Cluster-1-7201_userdata	userdata	Cluster-1-7201	Cluster2-7201	🟩 OK
⊞	□	Cluster-1-7201_dfs9	dfs9	Cluster-1-7201	Cluster2-7201	DISABLED
⊞	□	Cluster2-7201_dfs9_mirror	dfs9_mirror	Cluster2-7201	Cluster-1-7201	DISABLED
⊞	□	Cluster2-7201_userdata_mirror	userdata_mi…	Cluster2-7201	Cluster-1-7201	DISABLED
⊞	□	Cluster2-7201_EyeglassRunbo…	EyeglassRu…	Cluster2-7201	Cluster-1-7201	DISABLED
⊞	□	Cluster-1-7201_EyeglassRunb…	EyeglassRu…	Cluster-1-7201	Cluster2-7201	🟩 OK



DR Dashboard

		Name	SyncIQ Policy	Source	Destination	Last Successful Readiness Check	DR Failover Status

DR Failover Operations

Sync IQ Policy 🟩 OK
Job Name: data-zone-shares
Last Started: 9/12/2017, 3:10:37 PM
Last Success: 9/12/2017, 3:10:37 PM
Last Job State: finished
Enabled: true

Eyeglass Configuration Replication 🟩 OK
Job Name: prod-cluster-8_data-zone-shares
Last Run: 9/13/2017, 6:20:31 PM
Last Success: 9/13/2017, 6:20:31 PM
Audit Status: AUDITSUCCEEDED
Enabled: true

		Name	SyncIQ Policy	Source	Destination	Last Successful Readiness Check	DR Failover Status
⊞	□	prod-cluster-8_data-zone-nfsdata	data-zone-nfsdata	prod-cluster-8	Cluster2-7201	9/13/2017, 6:21:03 PM	🟩 OK
⊞	□	Cluster2-7201_data-zone-shares_mirror	data-zone-shares_m…	Cluster2-7201	prod-cluster-8	9/13/2017, 6:21:06 PM	FAILED_OVER

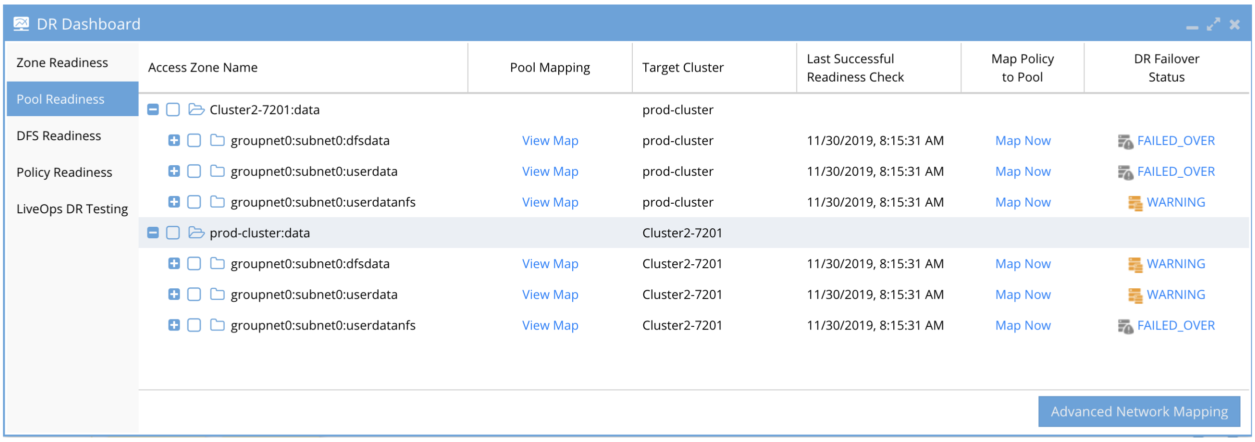
For more detailed information on these status, please refer to the Eyeglass Admin Guide here.

Zone/Pool Readiness

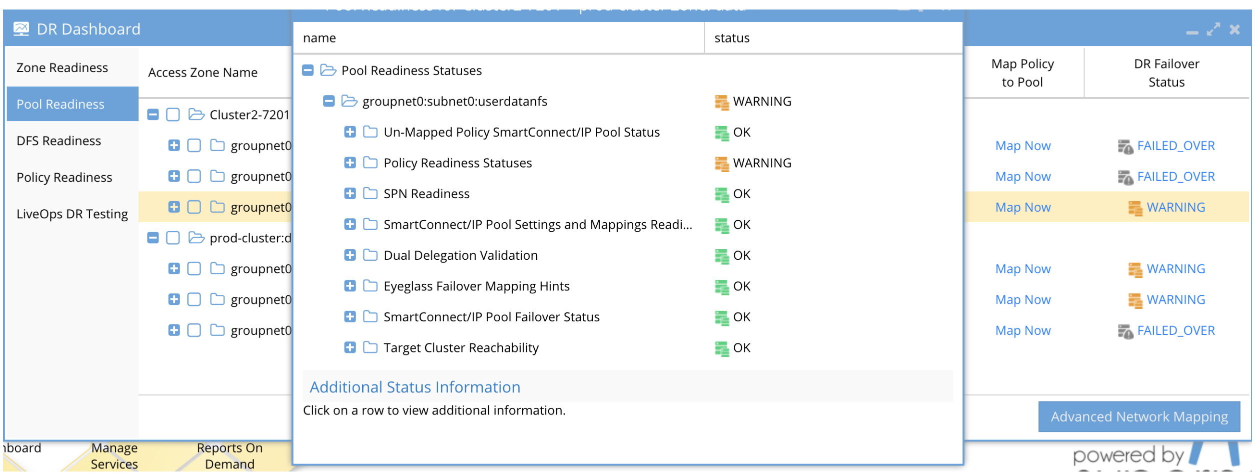
The Zone/Pool Readiness tabs provides a per Access Zone or per Pool summary of all the key networking, Kerberos SPN, SmartConnect connect subnet\pool information along with SyncIQ status and Configuration replication validations done for assessing readiness for failover by Access Zone or IP Pool. The status for each are combined to provide an overall DR Status. The Zone/Pool Failover Readiness is updated every 15 minutes by default.

This information provides the best indicator of DR readiness for failover. Also it allows administrators to check status on each component of failover, identify status, errors, and correct them to get each Access Zone/IP Pool configured and ready for failover.

By default the Failover Readiness job which populates this information is disabled. Instructions to enable this Job can be found in the Eyeglass Administration Guide.



Access Zone Name	Pool Mapping	Target Cluster	Last Successful Readiness Check	Map Policy to Pool	DR Failover Status
Cluster2-7201:data		prod-cluster			
groupnet0:subnet0:dfsdata	View Map	prod-cluster	11/30/2019, 8:15:31 AM	Map Now	FAILED_OVER
groupnet0:subnet0:userdata	View Map	prod-cluster	11/30/2019, 8:15:31 AM	Map Now	FAILED_OVER
groupnet0:subnet0:userdatanfs	View Map	prod-cluster	11/30/2019, 8:15:31 AM	Map Now	WARNING
prod-cluster:data		Cluster2-7201			
groupnet0:subnet0:dfsdata	View Map	Cluster2-7201	11/30/2019, 8:15:31 AM	Map Now	WARNING
groupnet0:subnet0:userdata	View Map	Cluster2-7201	11/30/2019, 8:15:31 AM	Map Now	WARNING
groupnet0:subnet0:userdatanfs	View Map	Cluster2-7201	11/30/2019, 8:15:31 AM	Map Now	FAILED_OVER



name	status
Pool Readiness Statuses	
groupnet0:subnet0:userdatanfs	WARNING
Un-Mapped Policy SmartConnect/IP Pool Status	OK
Policy Readiness Statuses	WARNING
SPN Readiness	OK
SmartConnect/IP Pool Settings and Mappings Readi...	OK
Dual Delegation Validation	OK
Eyeglass Failover Mapping Hints	OK
SmartConnect/IP Pool Failover Status	OK
Target Cluster Reachability	OK

Additional Status Information

Click on a row to view additional information.

For more detailed information on these status, please refer to the Eyeglass Admin Guide here.

1.7. How to enable Automated DR Testing the Eyeglass Runbook Robot Feature

Home Top

How to enable Automated DR Testing the Eyeglass Runbook Robot Feature

Many organizations schedule DR tests during maintenance windows and weekends, only to find out that the DR procedures did not work or documentation needed to be updated. Eyeglass Runbook Robot feature automates DR runbook procedures that would normally be scheduled in off peak hours, and avoids down time to validate DR procedures, providing Failover and Failback automation tests with reporting.

This level of automation provides high confidence that your PowerScale storage is ready for failover with all of the key functions executed on a daily basis.   In addition to automating failover and failback, Eyeglass operates as a cluster witness and mounts storage on both source and destination clusters the same way the cluster users and machines mount storage externally using Access Zone mount paths.

The feature exercises maximum automation used in Access Zone Failover (Advanced mode) or a basic Quick start more that only uses SyncIQ policy failover mode.

For more detailed information on planning and operation for Eyeglass Runbook Robot, please refer to the RunBookRobot Admin Guide

1.8. Planning and Procedures for Eyeglass SyncIQ DFS Mode Failover

Home Top

DFS Mode Preparation Checklist

DFS mode requires the following prerequisites:

1. Windows 2008 or 2012 Domain Controller.
2. DNS role installed.
3. DFS files services role.
2. 2 x PowerScale clusters with SyncIQ.
3. Eyeglass appliance.
4. DFS enabled clients Windows 7, 8, 10, Server 2008, 2012, 2016.

DFS Mode Compatibility

1. Not compatible with RunBook Robot feature, since NFS is used for data access.

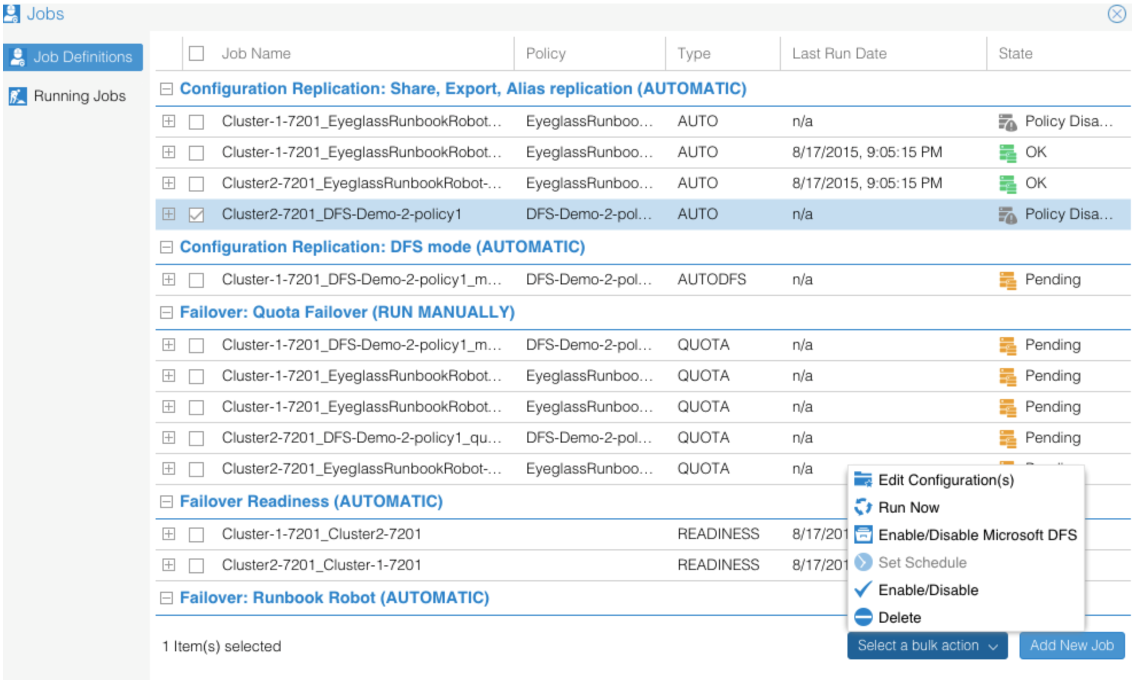
2. Hot\Hot and Hot\Cold compatible.
3. Compatible with Access Zones and Access Zone and IP pool Failover mode but requires dedicated subnet:pool with Eyeglass igls-ignore hint applied to retain SmartConnect zones on source and target clusters. DFS mode does not require SmartConnect Zone names to failover.

Considerations for Eyeglass SyncIQ DFS mode vs Default Configuration Sync job mode in Eyeglass

1. Default Eyeglass Job mode is Configuration Sync job mode which places configuration data on both source and target cluster treating the configuration data the same as SyncIQ, meaning it's maintained in full sync on both clusters.
2. Eyeglass SyncIQ DFS mode can be enabled and will rename share objects from the target cluster referenced in the policy, and fails over shares. Quotas are also failed over during share failover.

Procedure to Enable Eyeglass SyncIQ DFS mode

1. Select policy with shares to be protected and then **Select a bulk action** option **Enable/Disable Microsoft DFS**.

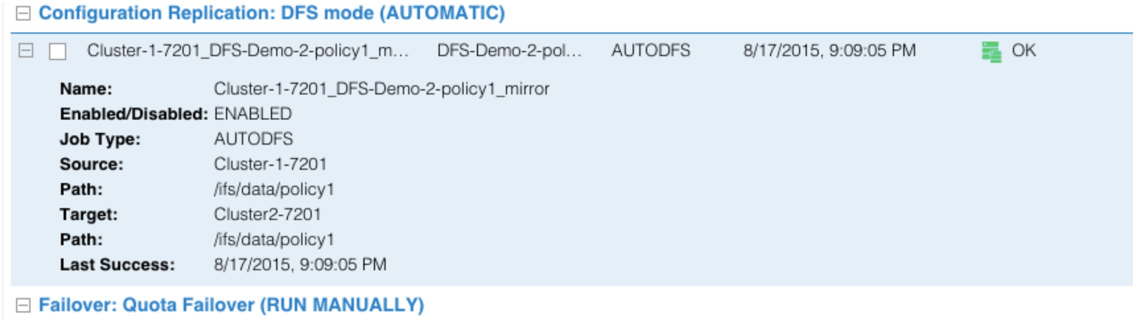


	Job Name	Policy	Type	Last Run Date	State
⊟	**Configuration Replication: Share, Export, Alias replication (AUTOMATIC)**				
⊞ □	Cluster-1-7201_EyeglassRunbookRobot...	EyeglassRunboo...	AUTO	n/a	Policy Disa...
⊞ □	Cluster-1-7201_EyeglassRunbookRobot...	EyeglassRunboo...	AUTO	8/17/2015, 9:05:15 PM	OK
⊞ □	Cluster2-7201_EyeglassRunbookRobot-...	EyeglassRunboo...	AUTO	8/17/2015, 9:05:15 PM	OK
⊞ ☑	Cluster2-7201_DFS-Demo-2-policy1	DFS-Demo-2-pol...	AUTO	n/a	Policy Disa...
⊟	**Configuration Replication: DFS mode (AUTOMATIC)**				
⊞ □	Cluster-1-7201_DFS-Demo-2-policy1_m...	DFS-Demo-2-pol...	AUTODFS	n/a	Pending
⊟	**Failover: Quota Failover (RUN MANUALLY)**				
⊞ □	Cluster-1-7201_DFS-Demo-2-policy1_m...	DFS-Demo-2-pol...	QUOTA	n/a	Pending
⊞ □	Cluster-1-7201_EyeglassRunbookRobot...	EyeglassRunboo...	QUOTA	n/a	Pending
⊞ □	Cluster-1-7201_EyeglassRunbookRobot...	EyeglassRunboo...	QUOTA	n/a	Pending
⊞ □	Cluster2-7201_DFS-Demo-2-policy1_qu...	DFS-Demo-2-pol...	QUOTA	n/a	Pending
⊞ □	Cluster2-7201_EyeglassRunbookRobot-...	EyeglassRunboo...	QUOTA	n/a	
⊟	**Failover Readiness (AUTOMATIC)**				
⊞ □	Cluster-1-7201_Cluster2-7201		READINESS	8/17/201	
⊞ □	Cluster2-7201_Cluster-1-7201		READINESS	8/17/201	
⊟	**Failover: Runbook Robot (AUTOMATIC)**				

1 Item(s) selected

2. Run the DFS Enabled job.

3. Verify its green before configuring DFS in Active Directory.



Configuration Replication: DFS mode (AUTOMATIC)

	Job Name	Policy	Type	Last Run Date	State
⊟ □	Cluster-1-7201_DFS-Demo-2-policy1_m...	DFS-Demo-2-pol...	AUTODFS	8/17/2015, 9:09:05 PM	OK

Name: Cluster-1-7201_DFS-Demo-2-policy1_mirror
Enabled/Disabled: ENABLED
Job Type: AUTODFS
Source: Cluster-1-7201
Path: /ifs/data/policy1
Target: Cluster2-7201
Path: /ifs/data/policy1
Last Success: 8/17/2015, 9:09:05 PM

Failover: Quota Failover (RUN MANUALLY)

Failover Rules for DFS when errors occur during failover

This section covers scenario's when failures occur and how Eyeglass will behave.

1. It is expected that if **SOME** of the share renames for a SyncIQ policy succeed (meaning SOME failed as well), failover steps will continue.
    a. Client Redirection phase marked as Warning in the failover log .
2. It is expected that if **ALL** of the share renames for a SyncIQ policy fail, the failover is aborted in **FAILED** state
    a. **Note: in this case**
        i. cluster is not failed over
        ii. **< 2.5.6 release the share renaming is not rolled back - must be done manually by customer**
        iii. **In > 2.5.6 release the shares will automatically be rolled back to the original state on the source cluster. This ensures users can access data again without any manual steps. This step will be logged in the failover log.**
3. How is share rename step declared a failure status:
    a. A share rename failure is considered to be:
        i. Failure to rename ALL shares on the SOURCE cluster
        ii. OR
        iii. Failure to rename ALL shares on the TARGET cluster.
4. For a multi-policy DFS failover (selecting multiple policies to failover at the same time), if a share rename failure occurs for any 1 of the policies then failover is aborted for that policy and continues for other policies.

a. **Note: in this case:**

    i. cluster is not failed over for the policy where all share renaming failed.

    ii. **< 2.5.6 release the share renaming is not rolled back - must be done manually by customer.**

    iii. **In > 2.5.6 release the shares will automatically be rolled back to the original state on the source cluster. This ensures users can access data again without any manual steps. This step will be logged in the failover log.**

Detailed DFS Mode Configuration, Operating procedures and Design guidelines

See Microsoft DFS Mode Failover Guide

1.9. Planning and Procedures for Eyeglass SyncIQ Mode Failover

Home Top

Planning and Procedures for Eyeglass SyncIQ Mode Failover

Recommended for NFS or application failover that requires post failover scripting for DNS, unmount/mount host side automation.

Not recommended for SMB failover. DFS mode or Access Zone failover handles SPN management and SmartConnect Zone operations during failover.

SyncIQ mode Failover mode Guide

1.10. Planning and Procedures for Eyeglass Access Zone Failover

Home Top

Planning and Procedures for Eyeglass Access Zone Failover

For requirements on setting up Access Zone planning guide see here.

1.11. How to Execute A Failover with DR Assistant

Home Top

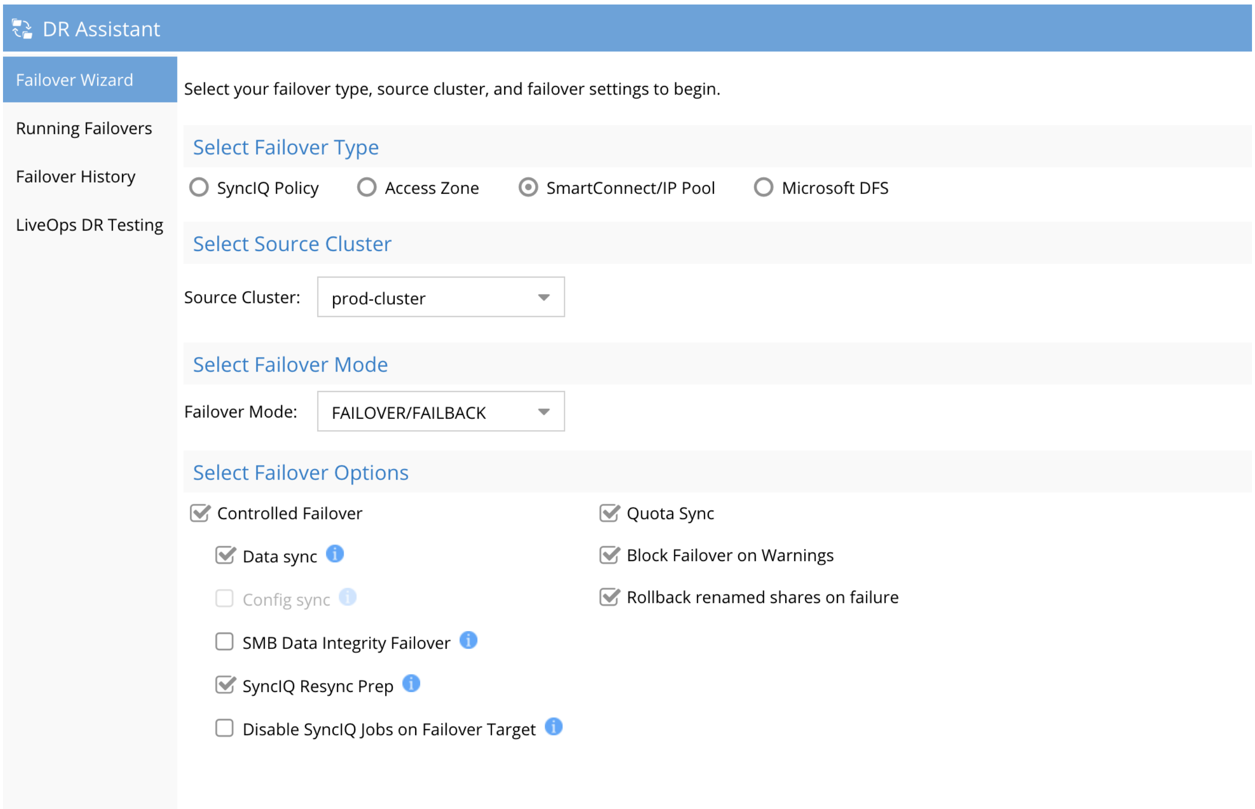
How to Execute A Failover with DR Assistant

Follow these steps to execute a failover.

Note: The planning guide is expected to be the referenced document for all planned failovers. **Support expects this document has been used for planning**.

How to know when Uncontrolled failover should be used?

This option in Eyeglass DR assistant should be used while understanding the data protection implications.



DR Assistant

Failover Wizard
Running Failovers
Failover History
LiveOps DR Testing

Select your failover type, source cluster, and failover settings to begin.

Select Failover Type

○ SyncIQ Policy ○ Access Zone ● SmartConnect/IP Pool ○ Microsoft DFS

Select Source Cluster

Source Cluster: prod-cluster

Select Failover Mode

Failover Mode: FAILOVER/FAILBACK

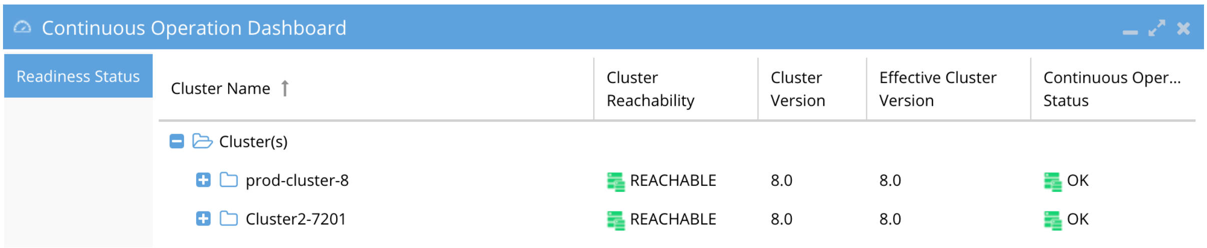
Select Failover Options

☑ Controlled Failover
- ☑ Data sync
- □ Config sync
- □ SMB Data Integrity Failover
- ☑ SyncIQ Resync Prep
- □ Disable SyncIQ Jobs on Failover Target

☑ Quota Sync
☑ Block Failover on Warnings
☑ Rollback renamed shares on failure

READ THIS FIRST: Using this option means you are failing away from the data and losing **ALL** changes at the moment the failover is started in Eyeglass.

NOTE: Uncontrolled failover should only be used when the Eyeglass VM DOES NOT have reachability to both Clusters that replicate. Even if data access is an issue to PowerScale BUT Eyeglass reachability is green on the liveops icon. DO NOT USE UNCONTROLLED FAILOVER, USE CONTROLLED FAILOVER.



Continuous Operation Dashboard

Readiness Status

Cluster Name	Cluster Reachability	Cluster Version	Effective Cluster Version	Continuous Oper... Status
Cluster(s)				
prod-cluster-8	REACHABLE	8.0	8.0	OK
Cluster2-7201	REACHABLE	8.0	8.0	OK

NOTE: All steps to recover from this failover mode, WILL require manual steps to recover DR sync status and failback from the DR cluster back to the Production cluster.

- Recovery from uncontrolled failover is customer responsibility and is NOT covered by Superna support contract.
- This will require involvement with all vendors related to the equipment in customer data center and receiving the green light from all vendors that the data center is ready to resume operations. This will include PowerScale and all dependent components such as AD, DNS, other application using PowerScale services, physical infrastructure (power, networking WAN links).

DO NOT BRING THE CLUSTER ONLINE WITHOUT PLANNING. RESYNC PREP DOES NOT RUN, WHICH MEANS BOTH CLUSTERS WILL BE WRITEABLE. YOU SHOULD DISCONNECT THE SOURCE CLUSTER AND PLAN A CONTROLLED RECOVERY FROM AN UNCONTROLLED FAILOVER.

Reasons you may choose to execute an uncontrolled failover include the following:

1. WAN link is cut to the data center with a **very long repair time** to restore service.
2. Loss of power for extended periods of time to the production data center.
3. Damaged cluster or serious cluster issue (upgrade).

4. Equipment failover blocking access to the cluster, or application server failures with long recovery times.
5. Networking failure that prevents users from accessing storage and PowerScale management network has ALSO Failed.

Eyeglass Pre-Failover Check Important - Read me

IMPORTANT:

Making any changes to the SyncIQ Policies or related Eyeglass Configuration Replication Jobs during failover may result in unexpected results.

IMPORTANT:

Eyeglass Assisted Failover has a 45 minute timeout on each failover step. Any step which is not completed within this timeout period will cause the failover to fail. This can occur if SyncIQ policies are already running when failover job is started or SyncIQ steps take longer than expected to complete. This timeout can be changed but does not accelerate failover if lowered.

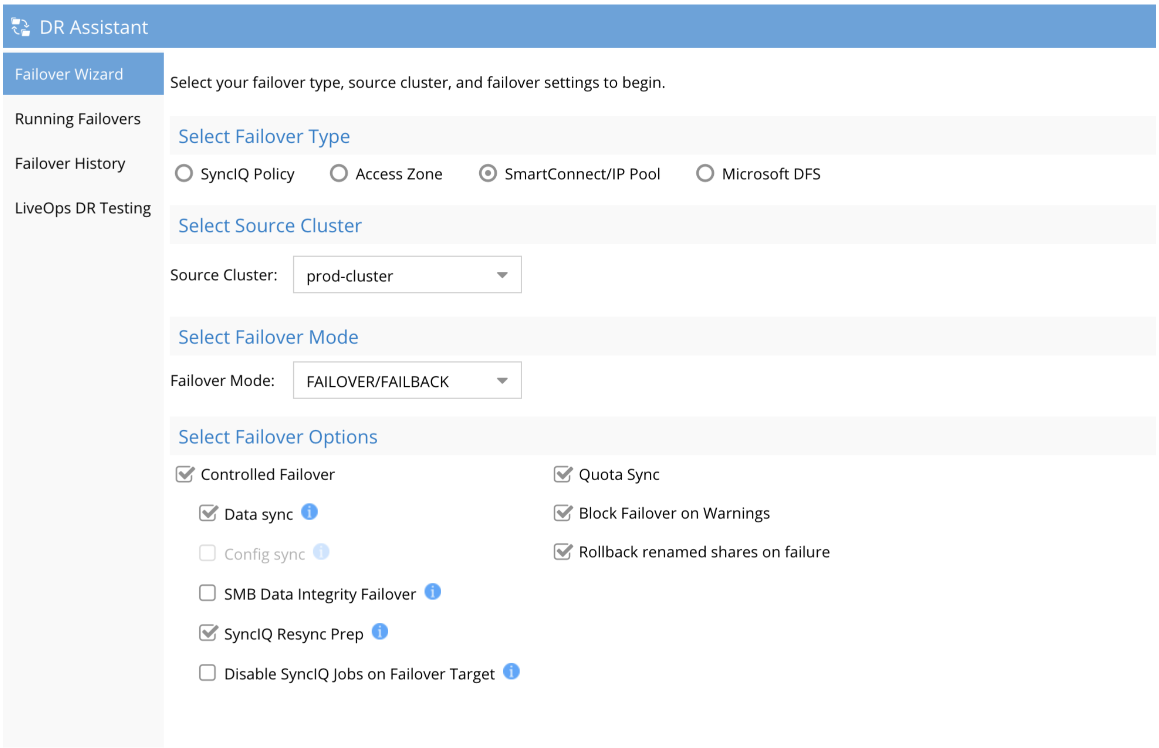
IMPORTANT:

Deleting configuration data (shares, exports, quotas) or modifying Share name or NFS Alias name or NFS Export path on the target cluster before failing over without running Eyeglass Configuration Replication will incorrectly result in the object being deleted on the source cluster after failover. You must run Eyeglass configuration replication before the failover OR select the Config Sync checkbox on failover to prevent this from happening.

How to failover Data With DR Assistant

This covers **Access Zone/ IP Pool mode, DFS policy mode or SyncIQ mode.**

To failover Data with DR Assistant:

1. Consult the [Failover Design Guide]() for monitoring failover progress.
2. There should be no client access to the Failover Source cluster during failover as this data will not be replicated. **Use SMB Data Integrity option to disconnect user sessions on shares that will failover (NFS clients should unmount).**
3. **Open DR Assistant Icon**
4. 

DR Assistant

Failover Wizard
Running Failovers
Failover History
LiveOps DR Testing

Select your failover type, source cluster, and failover settings to begin.

Select Failover Type

○ SyncIQ Policy ○ Access Zone ● SmartConnect/IP Pool ○ Microsoft DFS

Select Source Cluster

Source Cluster: prod-cluster

Select Failover Mode

Failover Mode: FAILOVER/FAILBACK

Select Failover Options

☑ Controlled Failover
☑ Data sync
□ Config sync
□ SMB Data Integrity Failover
☑ SyncIQ Resync Prep
□ Disable SyncIQ Jobs on Failover Target

☑ Quota Sync
☑ Block Failover on Warnings
☑ Rollback renamed shares on failure

5. Select Failover Type that is configured in your environment.
6. Select Source Cluster that has the writable data to failover.
7. **Leave the Failover Mode set to "Failover / Failback".**

8. Leave all default check boxes for a planned controlled failover (**or read the options below to make changes**) .

9. FAILOVER OPTIONS ARE DEFINED BELOW:

1. **Controlled failover**

    a. Check if the source cluster is healthy and reachable. Review the **LiveOPS Dashboard Icon** and verify the clusters show reachable true.

    b. Uncheck this option ONLY IF THIS IS A REAL DR EVENT. **This option is a REAL DR event. NOTE: Do not use this option unless lab testing OR you are prepared for manual steps to recover from the resulting end state.** In this case, source cluster API calls are skipped and cached knowledge of shares, quotas are used to failover (**Real DR Event**).

    c. **MUST READ: Uncheck Controlled Failover ONLY if this is a REAL DR event (NOTE: If this is unchecked Eyeglass assumes the source cluster is destroyed, NO steps that provide failback are executed. Customer is responsible for recovery from uncontrolled failover - it is not covered by Superna support. NO automated recovery is possible from using this option. It is expected customers make decisions to protect data at all times and only use this option if data is deemed not usable for business reasons.**

        i. **Recovery from uncontrolled failover is customer responsibility and is NOT covered by Superna support contract.**

        ii. **This will require involvement with all vendors related to the equipment in customer data center and receiving the green light from all vendors that the data center is**

ready to resume operations. This will include PowerScale and all dependent components such as AD, DNS, other application using PowerScale services, physical infrastructure (power, networking WAN links).

d. **All recovery is manual if this option is used. Ensure the cluster you fail away from is no longer accessible to users and take steps to ensure it cannot be accessed.**

1. **IMPORTANT:**

   a. Eyeglass Configuration Replication Jobs will be in USERDISABLED state on source and target cluster after an uncontrolled failover.

2. Data Sync

   b. Check to run a final SyncIQ data sync Job as part of the failover (**RECOMMENDED**)

   a. Uncheck to skip the SyncIQ data sync step

5. Config Sync **(DISABLED > 2.5.6)**

   b. Check to run a final Eyeglass Configuration Replication Job as part of the failover to sync shares, exports, nfs aliases.

   c. Uncheck to skip the Eyeglass Configuration Replication step (**RECOMMENDED**)

6. SMB Data Integrity Failover **(Optional)**

   b. Check to enable SMB Data Integrity Failover . This mode disconnects any active SMB sessions prior to failover and ensures that no new sessions can be established on the failover source. It applies a deny read permission to the Everyone user to each share.

    c. NOTE: if shares use root with full control, you are no longer using Active Directory user, this is a Linux user on PowerScale only and not an Active Directory user. Any share with run as root by passes all security and cannot be locked out from a share. Any shares with this permission will not be locked out.

    d. Uncheck to skip SMB Data Integrity Failover step. **(Default)**

7. Quota Sync **(Default enabled)**

    b. This option allows skipping of quota failover and will leave the quotas on the source cluster. This would be selected if 1000’s of quotas exist which affects failover performance of SyncIQ operations. It will also remove the risk of a quota scan job impacting SyncIQ operations on quotas that are flagged with needs a scan on the destination cluster.

    c. Checked means quotas will failover will create quotas on the target cluster and then delete them on the source cluster.

    d. Unchecked means quotas will not be failed over but will remain on the source cluster.

    e. **Best Practice: If you plan to failover and failback in the same day, uncheck this option to ensure quota scan job does not impact failover operations.**

8. Block Failover on Warning **(Default Enabled)**

b. This option will block failover from starting if a validation shows warning in DR Dashboard. All Warnings in DR Dashboard will block a failover and must be reviewed before unchecking this option to continue.

c. Preceding with a failover with warnings, proceed at your own risk to data.

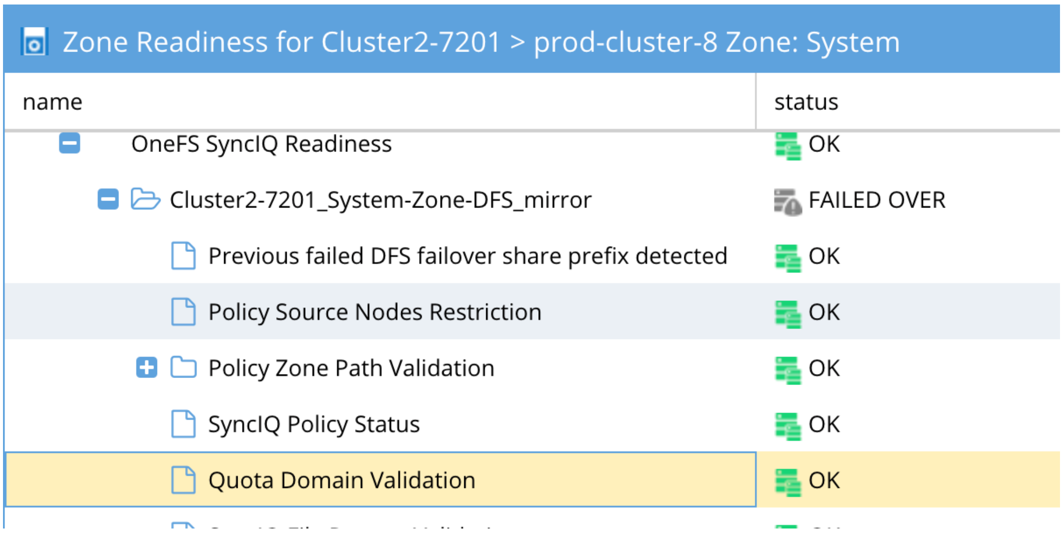
d. **Best Practice: Open a case and get input from support.**

9. **Quota Domain conflict with SyncIQ Validation**

b. Allows override of default validation that will detect target cluster quotas with a quota scan pending flag set. This flag blocks running policies, resync prep and make writable steps from completing on policies that have newly created quotas and no quota domain created.

c. See image below on policy quota domain validation check.

d.



Zone Readiness for Cluster2-7201 > prod-cluster-8 Zone: System

name	status
⊟ OneFS SyncIQ Readiness	OK
⊟ Cluster2-7201_System-Zone-DFS_mirror	FAILED OVER
Previous failed DFS failover share prefix detected	OK
Policy Source Nodes Restriction	OK
⊞ Policy Zone Path Validation	OK
SyncIQ Policy Status	OK
Quota Domain Validation	OK

e. This validation will block a failover attempt when checked and a warning validation is detected on the Access zone, SyncIQ policy or ip pool mode.

f. To continue uncheck this option and restart the failover, **If unchecked you are taking the risk of SyncIQ policies failing either Make Writable step or Re-sync prep.**

g. **Solution**: Run quota scan job from cluster jobs menu and allow quota scan to complete the quota domain creation on all quotas with the flag set. Then start the failover again once the validation shows Green OK.

h. **NOTE: If multiple policies are defined some policies may fail make writable step OR resync prep step. In this release Eyeglass will continue to the next policy if a step fails.**

7. SyncIQ Resync Prep **(Default Enabled)**

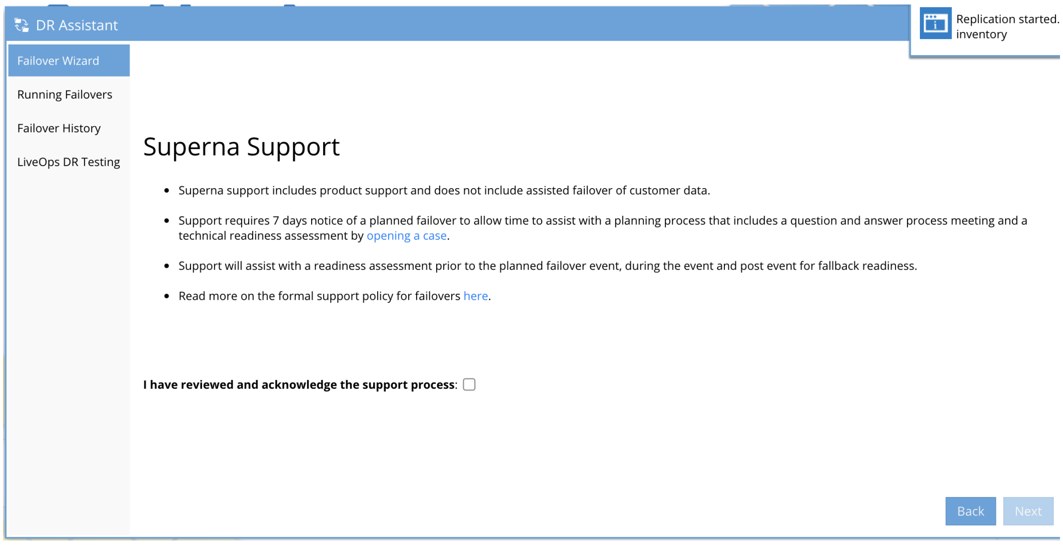
   b. Check to execute the SyncIQ Resync Prep failover step (leave this default advanced setting) **(Recommended)**

   c. Uncheck to skip SyncIQ Resync Prep failover step. **This is not recommended as it will leave the system in state where you will not be able to use Eyeglass to failback. This is used ONLY when customers want to failover in one direction and then recreate a new policy or they know how to manually recover and create mirror policy.**

5. Disable SyncIQ Jobs on Failover Target **(Default Enabled, advanced setting leave at default)**

   b. **Recommendation to leave enabled**

   c. Disable on failover is optional if you don't want to configure failback and execute sync job in the return direction. This is used when you want to verify systems before replicating data back to the source. **Warning: Using this option WILL require manual steps to failback to enable the policy and set the schedule on the policy.**

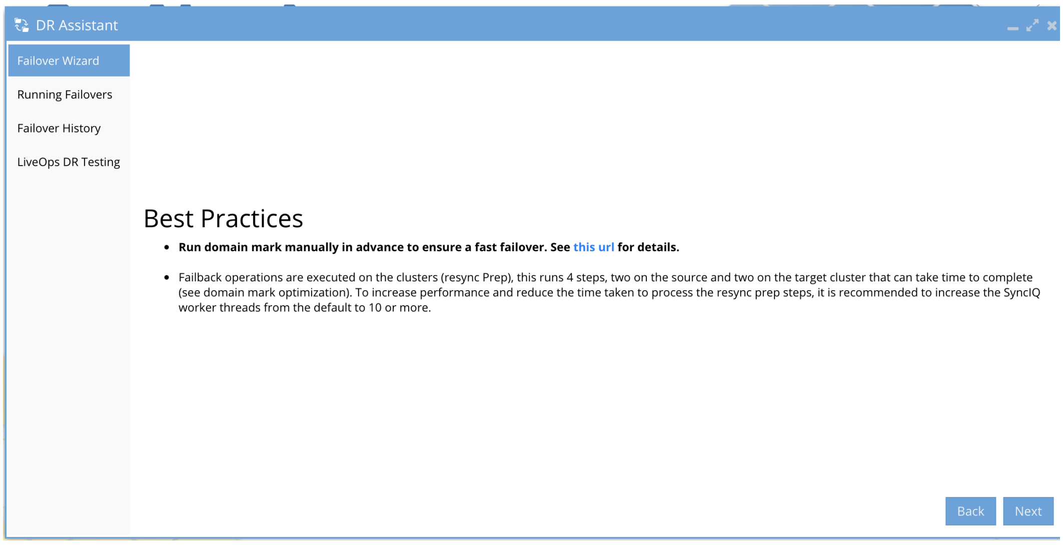
6. **Rollback SMB Shares on Failure (default enabled)**
    - This only applies to DFS mode failover and should be left enabled to automatically rollback SMB share rename step if a share rename step fails the the failover needs to rollback.
    - Recommendation: Enabled.
7. Click Next after making selecting all DR Assistant Failover Options
    - Review and accept that you have read all preparation material regarding support process and customer responsibilities.
    - 

Superna Support

- Superna support includes product support and does not include assisted failover of customer data.
- Support requires 7 days notice of a planned failover to allow time to assist with a planning process that includes a question and answer process meeting and a technical readiness assessment by opening a case.
- Support will assist with a readiness assessment prior to the planned failover event, during the event and post event for fallback readiness.
- Read more on the formal support policy for failovers here.

I have reviewed and acknowledge the support process: □

8. Verify domain mark steps have been completed **(> 2.5.6 has new validation warning if Domain mark has not be completed)**

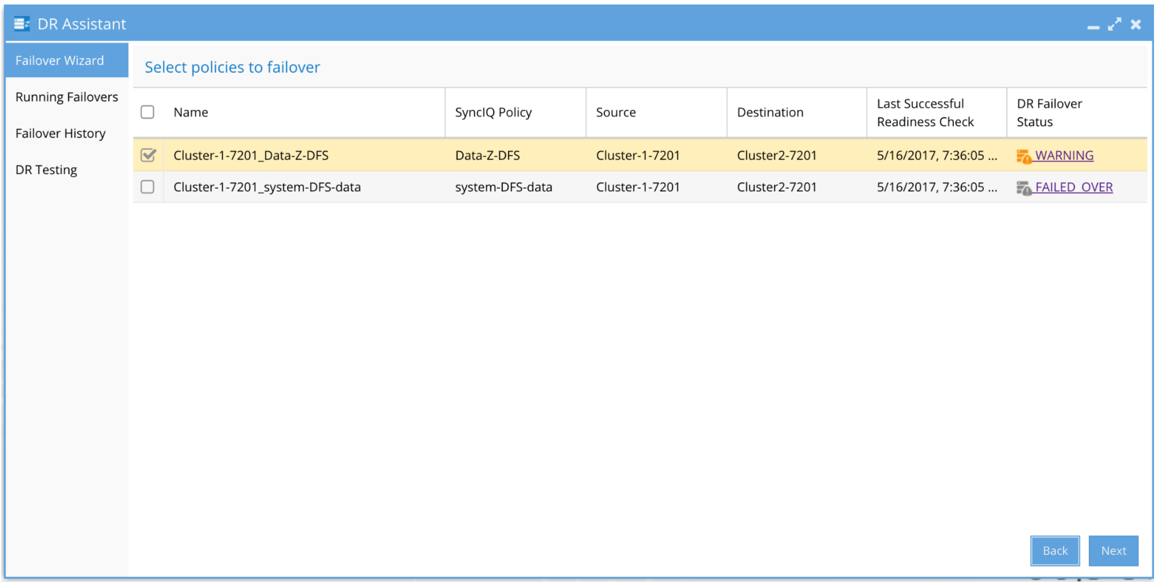
- 

Best Practices

- **Run domain mark manually in advance to ensure a fast failover. See this url for details.**
- Failback operations are executed on the clusters (resync Prep), this runs 4 steps, two on the source and two on the target cluster that can take time to complete (see domain mark optimization). To increase performance and reduce the time taken to process the resync prep steps, it is recommended to increase the SyncIQ worker threads from the default to 10 or more.

9. Select the policy or policies (multi select) or Access Zone (no multi select) or IP pool (multi select) for the failover type selected.

10. Check readiness again before continuing to ensure you understand the warnings and if they will affect your failover. In general warnings do not block failover. Errors block failover. **Consult with support to get clarification.**

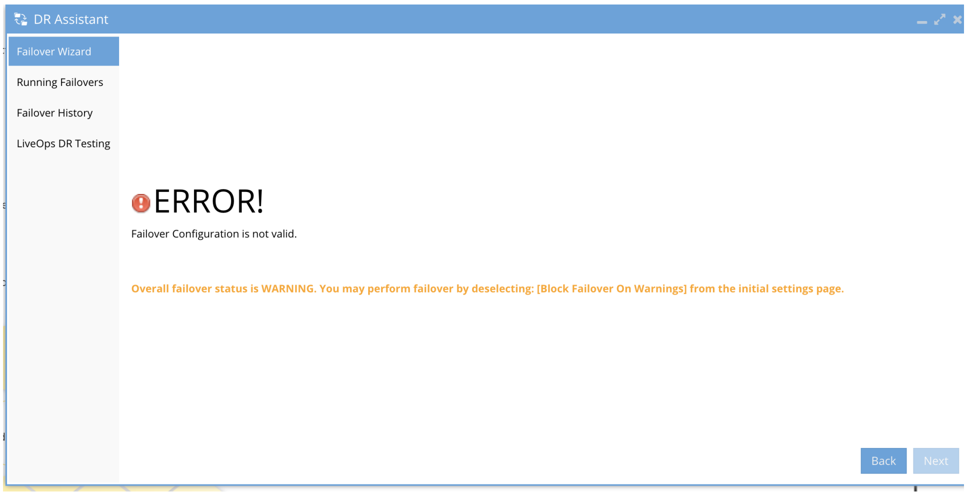
11. 

Select policies to failover

□	Name	SyncIQ Policy	Source	Destination	Last Successful Readiness Check	DR Failover Status
☑	Cluster-1-7201_Data-Z-DFS	Data-Z-DFS	Cluster-1-7201	Cluster2-7201	5/16/2017, 7:36:05 ...	WARNING
□	Cluster-1-7201_system-DFS-data	system-DFS-data	Cluster-1-7201	Cluster2-7201	5/16/2017, 7:36:05 ...	FAILED_OVER

12. Click Next for Failover Configuration Validation

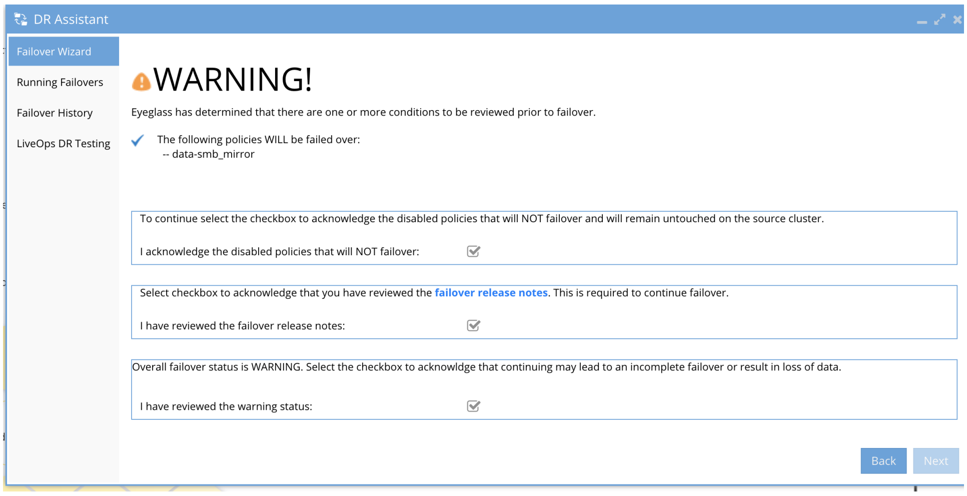
- If you see a failover validation error (example below), review the error and determine if you need to uncheck block failover with warnings on the first DR assistant options screen. **You will need to click back to the start to make this change. See image below. If unsure consult with support on the warning to understand the impact.**

- **If you do not receive a validation you will see the next screen to review.**
- **Each Failover mode has a validation screen.**
- **SyncIQ or DFS mode failover Validation example**
  - 

    ERROR!

    Failover Configuration is not valid.

    Overall failover status is WARNING. You may perform failover by deselecting: [Block Failover On Warnings] from the initial settings page.
  - Access Zone or IP pool Failover Validation Example
  - Access Zone and IP Pool Failover Mode validation Screen (below). NOTE: This screen will show all policies within the Access Zone that are eligible for failover. If any policy is USER DISABLED or policy disabled it will be shown as “will NOT be failed over”. NOTE: Do not failover with a disabled policy unless you know the data protected by this policy does not need to be failed over.

- 

WARNING!

Eyeglass has determined that there are one or more conditions to be reviewed prior to failover.

✓ The following policies WILL be failed over:
-- data-smb_mirror

To continue select the checkbox to acknowledge the disabled policies that will NOT failover and will remain untouched on the source cluster.

I acknowledge the disabled policies that will NOT failover: ☑

Select checkbox to acknowledge that you have reviewed the failover release notes. This is required to continue failover.

I have reviewed the failover release notes: ☑

Overall failover status is WARNING. Select the checkbox to acknowldge that continuing may lead to an incomplete failover or result in loss of data.

I have reviewed the warning status: ☑

13. **Review each validation**

    - This screen requires acknowledgment before continuing.
    - Failing to read this document can result in data loss.
    - Customer's are expected to read all supporting documents prior to planning a failover event.

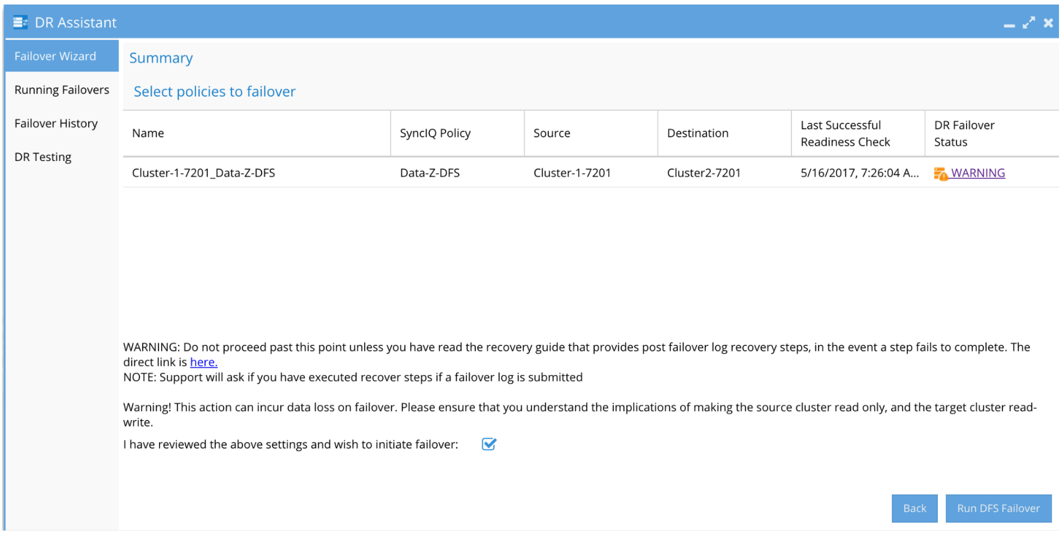
14. **Final acceptance and point of no return.**

15. **NOTE: The failover job can be canceled once started but recovery steps will be manual.**

16. **Final summary page before starting the failover. New in 2.5.7 or later is a summary of all options selected.**

    b. **Release < 2.5.6 Summary page**

c.



Summary

Select policies to failover

Name	SyncIQ Policy	Source	Destination	Last Successful Readiness Check	DR Failover Status
Cluster-1-7201_Data-Z-DFS	Data-Z-DFS	Cluster-1-7201	Cluster2-7201	5/16/2017, 7:26:04 A...	WARNING

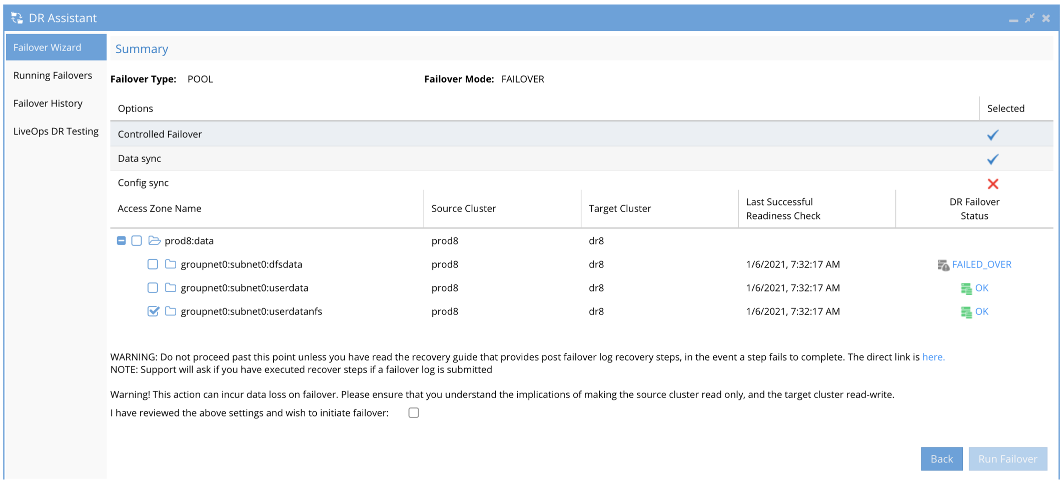
WARNING: Do not proceed past this point unless you have read the recovery guide that provides post failover log recovery steps, in the event a step fails to complete. The direct link is here.
NOTE: Support will ask if you have executed recover steps if a failover log is submitted

Warning! This action can incur data loss on failover. Please ensure that you understand the implications of making the source cluster read only, and the target cluster read-write.

I have reviewed the above settings and wish to initiate failover: ☑

d. Release > 2.5.7 Summary Page allows a review of all options selected for the failover before starting the failover.

e.



Summary

Failover Type: POOL **Failover Mode:** FAILOVER

Options	Selected
Controlled Failover	✓
Data sync	✓
Config sync	✗

Access Zone Name	Source Cluster	Target Cluster	Last Successful Readiness Check	DR Failover Status
□ prod8:data	prod8	dr8		
□ groupnet0:subnet0:dfsdata	prod8	dr8	1/6/2021, 7:32:17 AM	FAILED_OVER
□ groupnet0:subnet0:userdata	prod8	dr8	1/6/2021, 7:32:17 AM	OK
☑ groupnet0:subnet0:userdatanfs	prod8	dr8	1/6/2021, 7:32:17 AM	OK

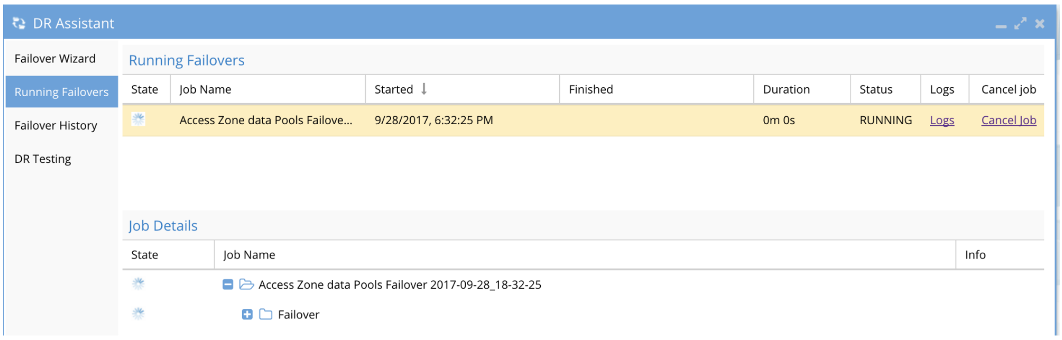
WARNING: Do not proceed past this point unless you have read the recovery guide that provides post failover log recovery steps, in the event a step fails to complete. The direct link is here.
NOTE: Support will ask if you have executed recover steps if a failover log is submitted

Warning! This action can incur data loss on failover. Please ensure that you understand the implications of making the source cluster read only, and the target cluster read-write.

I have reviewed the above settings and wish to initiate failover: □

17. Start the failover with Run button.

- Click Watch to follow the failover real-time or click fetch to update log window with current progress.

- 

DR Assistant

Running Failovers

State	Job Name	Started	Finished	Duration	Status	Logs	Cancel job
	Access Zone data Pools Failove...	9/28/2017, 6:32:25 PM		0m 0s	RUNNING	Logs	Cancel Job

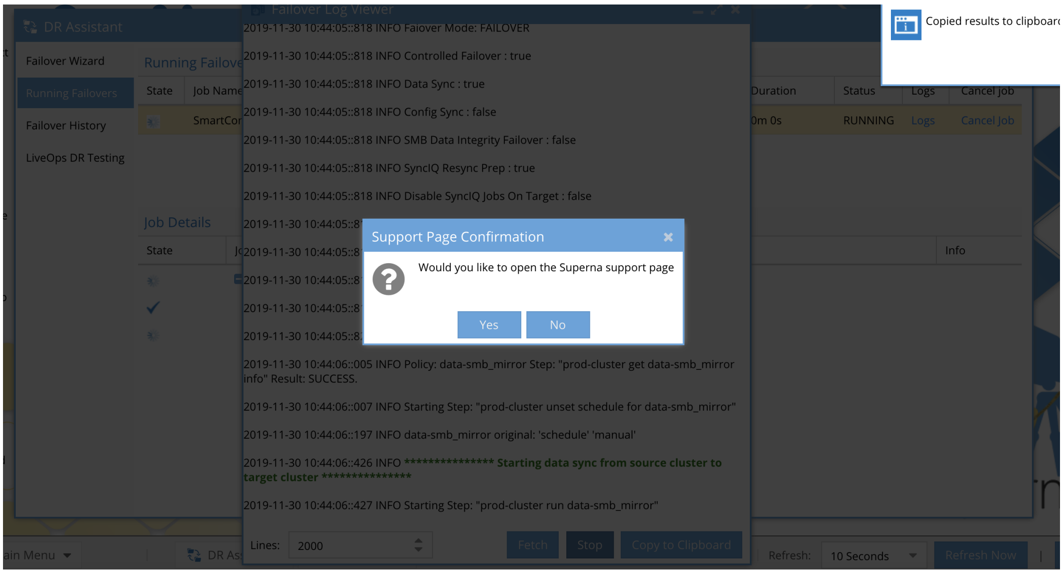
Job Details

State	Job Name	Info
	Access Zone data Pools Failover 2017-09-28_18-32-25	
	Failover	

18. NOTE: Failover jobs can be canceled cancel job link.

- ONLY USE IF DIRECTED BY SUPPORT
- WARNING: IF YOU CANCEL A FAILOVER, MANUAL RECOVERY OF NETWORKING POLICY STATE, SHARES, SPN, SMARTCONNECT IS REQUIRED. SUPPORT IS UNABLE TO ASSIST WITH RECOVERY FROM INTENTIONALLY CANCELING A FAILOVER.

19. Monitor the Failover job Progress

- (2.5.6 or later Release) Use the Copy to Clipboard button to update support case for partial Failover Review.
  - Clicking the button will prompt to open a browser tab to the support web site to paste the support log. Answer no to skip opening the support site.
- 

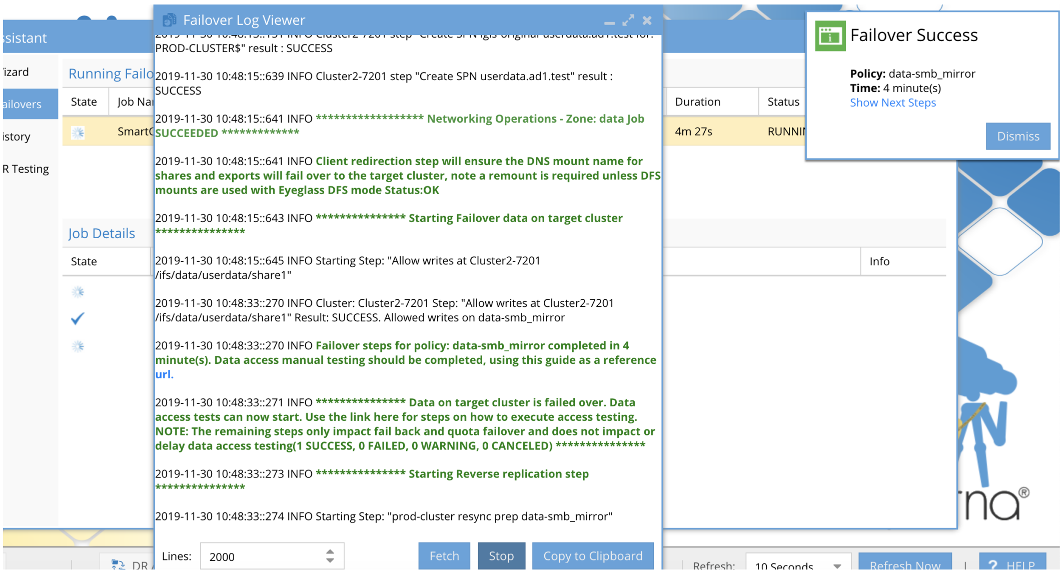
Copied results to clipboar

```
2019-11-30 10:44:05::818 INFO Faiover Mode: FAILOVER
2019-11-30 10:44:05::818 INFO Controlled Failover : true
2019-11-30 10:44:05::818 INFO Data Sync : true
2019-11-30 10:44:05::818 INFO Config Sync : false
2019-11-30 10:44:05::818 INFO SMB Data Integrity Failover : false
2019-11-30 10:44:05::818 INFO SyncIQ Resync Prep : true
2019-11-30 10:44:05::818 INFO Disable SyncIQ Jobs On Target : false
2019-11-30 10:44:05::8
2019-11-30 10:44:05::8
2019-11-30 10:44:05::8
2019-11-30 10:44:05::8
2019-11-30 10:44:05::8
2019-11-30 10:44:06::005 INFO Policy: data-smb_mirror Step: "prod-cluster get data-smb_mirror
info" Result: SUCCESS.
2019-11-30 10:44:06::007 INFO Starting Step: "prod-cluster unset schedule for data-smb_mirror"
2019-11-30 10:44:06::197 INFO data-smb_mirror original: 'schedule' 'manual'
2019-11-30 10:44:06::426 INFO *************** Starting data sync from source cluster to
target cluster ***************
2019-11-30 10:44:06::427 INFO Starting Step: "prod-cluster run data-smb_mirror"
```

Support Page Confirmation

Would you like to open the Superna support page

- **(2.5.6 or later release)** Notification Popup Indicates each Policy that Completes Steps to Allow Data Access Testing
  - Click to open instructions or Dismiss button to close the Window.



```
PROD-CLUSTER$" result : SUCCESS

2019-11-30 10:48:15::639 INFO Cluster2-7201 step "Create SPN userdata.ad1.test" result :
SUCCESS

2019-11-30 10:48:15::641 INFO ***************** Networking Operations - Zone: data Job
SUCCEEDED *************

2019-11-30 10:48:15::641 INFO Client redirection step will ensure the DNS mount name for
shares and exports will fail over to the target cluster, note a remount is required unless DFS
mounts are used with Eyeglass DFS mode Status:OK

2019-11-30 10:48:15::643 INFO *************** Starting Failover data on target cluster
***************

2019-11-30 10:48:15::645 INFO Starting Step: "Allow writes at Cluster2-7201
/ifs/data/userdata/share1"

2019-11-30 10:48:33::270 INFO Cluster: Cluster2-7201 Step: "Allow writes at Cluster2-7201
/ifs/data/userdata/share1" Result: SUCCESS. Allowed writes on data-smb_mirror

2019-11-30 10:48:33::270 INFO Failover steps for policy: data-smb_mirror completed in 4
minute(s). Data access manual testing should be completed, using this guide as a reference
url.

2019-11-30 10:48:33::271 INFO *************** Data on target cluster is failed over. Data
access tests can now start. Use the link here for steps on how to execute access testing.
NOTE: The remaining steps only impact fail back and quota failover and does not impact or
delay data access testing(1 SUCCESS, 0 FAILED, 0 WARNING, 0 CANCELED) ***************

2019-11-30 10:48:33::273 INFO *************** Starting Reverse replication step
***************

2019-11-30 10:48:33::274 INFO Starting Step: "prod-cluster resync prep data-smb_mirror"
```

Failover Success

Policy: data-smb_mirror
Time: 4 minute(s)
Show Next Steps

Dismiss

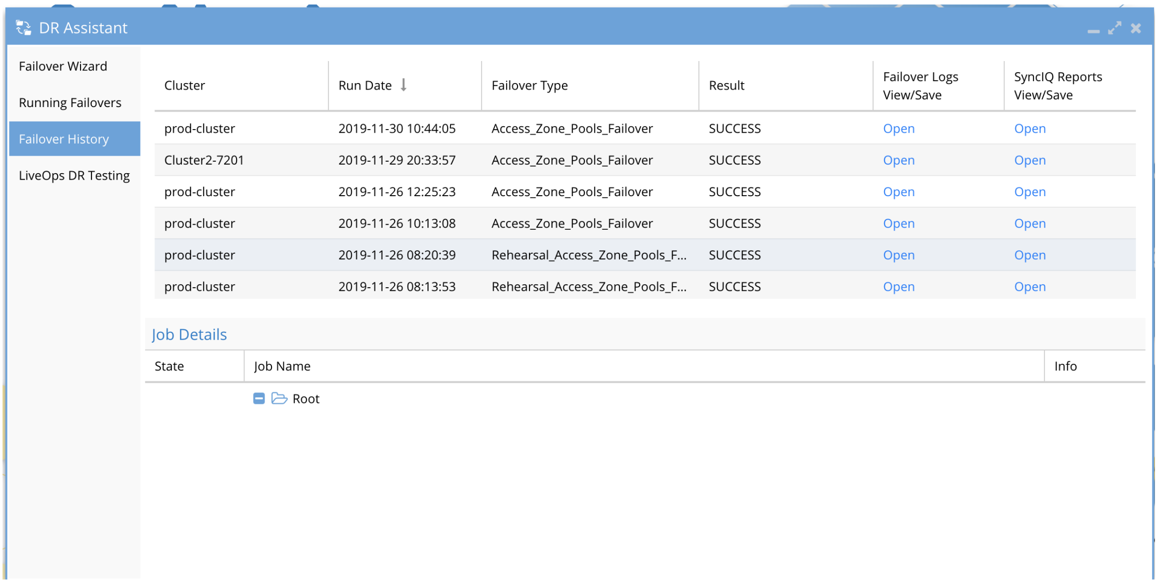
20. All other Releases Follow Data Access Testing Documentation once the failover log indicates the Allow writes step has completed.
    - IMPORTANT: Always test data access for any failover success or failure. Detailed steps are posted **How to Validate and troubleshoot A Successful Failover WHEN Data is NOT Accessible on the Target Cluster**

21. The failover will continue to complete Resync Prep, Run mirror and quota failover steps
    - Auto enabling of Eyeglass jobs to prepare for failback (Requires 2.5.6 or later)

22. Download Completed Failover logs or review failover log history by Clicking on the Failover History Tab.

23. **NOTE: SyncIQ steps are logged to a separate log that can be downloaded and provided to support to provide details on why a syncIQ step failed and can be used when opening a Dell SR with PowerScale support.**

24. Example below



Cluster	Run Date ↓	Failover Type	Result	Failover Logs View/Save	SyncIQ Reports View/Save
prod-cluster	2019-11-30 10:44:05	Access_Zone_Pools_Failover	SUCCESS	Open	Open
Cluster2-7201	2019-11-29 20:33:57	Access_Zone_Pools_Failover	SUCCESS	Open	Open
prod-cluster	2019-11-26 12:25:23	Access_Zone_Pools_Failover	SUCCESS	Open	Open
prod-cluster	2019-11-26 10:13:08	Access_Zone_Pools_Failover	SUCCESS	Open	Open
prod-cluster	2019-11-26 08:20:39	Rehearsal_Access_Zone_Pools_F...	SUCCESS	Open	Open
prod-cluster	2019-11-26 08:13:53	Rehearsal_Access_Zone_Pools_F...	SUCCESS	Open	Open

Job Details

State	Job Name	Info
	Root	

25.

26. **Failover Complete**

© Superna LLC

1.12. How to Execute a DR Rehearsal Failover with DR Assistant

Home Top

Overview

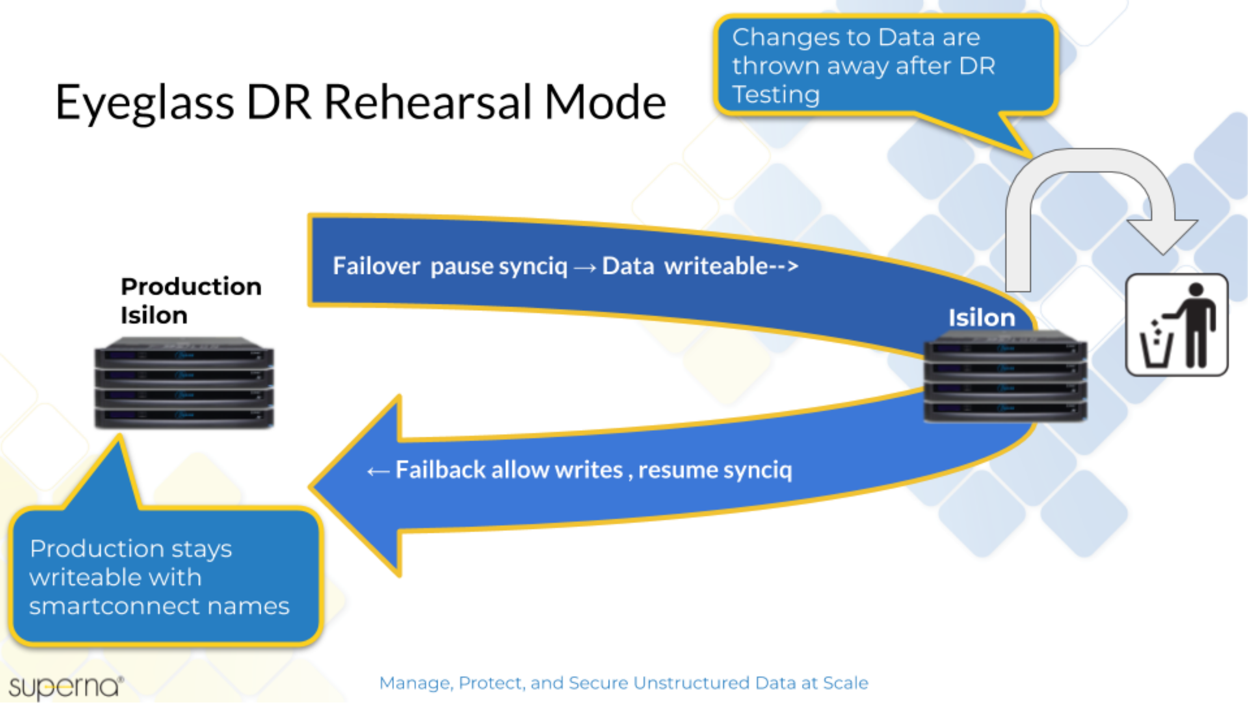
This option is not a failover , it is a test that does not complete all the steps needed to failover users and applications. It does allow testing of write access to data at a DR location.   It can be used in combination with network and host isolation documented here.

Considerations Before Using DR Rehearsal Mode

1. Not Recommended for for production Data. Recommended for Dev Test data sets or use Live OPS DR Test mode feature see guide here.

2. Data is not protected on the source cluster while DR Rehearsal mode is enabled.
3. Eyeglass blocks Uncontrolled Failover Attempt while DR Rehearsal mode is enabled, which means exposure to a real DR event during the DR Rehearsal test.
4. **Mandatory Configuration Change**: The longer you are in active DR Rehearsal and the more data modified during the testing, the longer it will take to exit DR Rehearsal mode to revert the file system on the DR target to the pre-test state. This is normal and expected.
    a. **It is Mandatory to increase the failover timeout value to 3 hours minimum, to ensure this step does not timeout with the default of 45 minutes.**
    b. **Login to Eyeglass as admin user over ssh and then run this command:**
        i. **igls adv failovertimeout set --minutes 180**
5. Access Zone, IP pool and SyncIQ mode will NOT redirect DNS or SPN and will not require production maintenance window.
6. WARNING: DFS Mode will redirect users DFS mounts and will require an outage and maintenance window to use this failover mode.

DR Rehearsal Mode Diagram



Eyeglass DR Rehearsal Mode

Changes to Data are thrown away after DR Testing

Production Isilon

Failover pause synciq → Data writeable-->

Isilon

← Failback allow writes , resume synciq

Production stays writeable with smartconnect names

superna

Manage, Protect, and Secure Unstructured Data at Scale

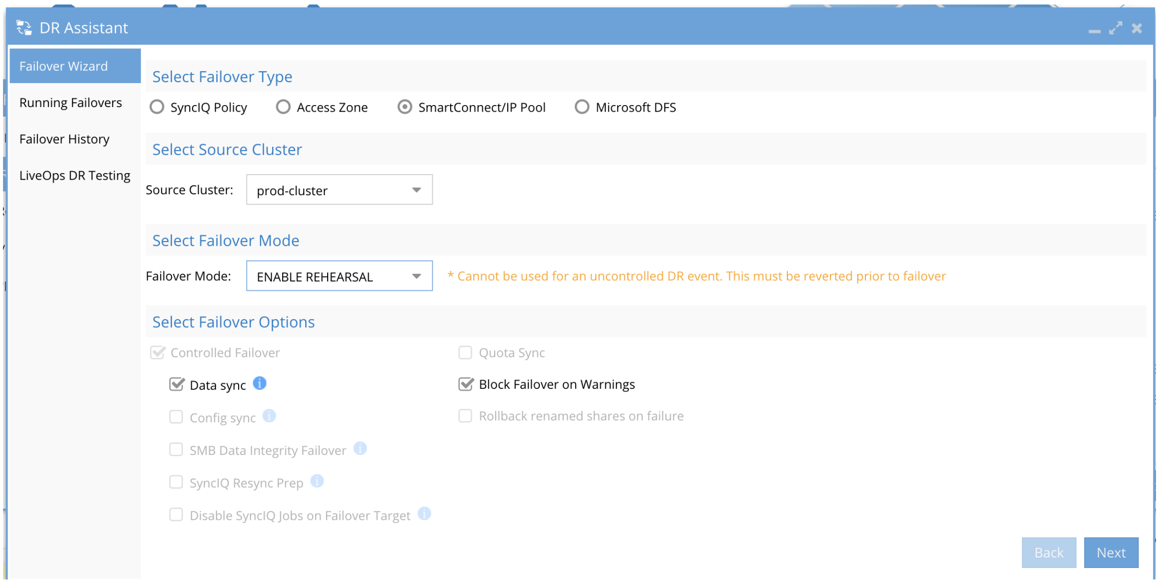
What Steps Execute During DR Rehearsal Mode Enable

1. The run SyncIQ step runs to sync data .
2. **DFS Mode :**
    a. SMB Shares will be renamed to failover DFS folders during DR Rehearsal for write access testing.
3. **Access Zone, IP Pool, SyncIQ Mode:**
    a. No client redirection - SmartConnect names will NOT be redirected to DR cluster.
4. Allow writes step is completed for policies that are selected.
5. The source cluster SyncIQ policies are disabled so that will not run while in DR Rehearsal mode.
6. DR Dashboard will display Active for DR Rehearsal mode.

What Steps Execute During DR Rehearsal Revert

1. The target cluster will have the disallow writes step execute blocking writes on the target cluster.
2. **DFS Mode:**
    a. SMB Shares will be renamed and redirect users connections back to the source cluster.
3. **Access zone, IP Pool, SyncIQ Mode:**
    a. No redirection is done, SmartConnect names and spn's were not redirected when entering DR Rehearsal mode.
4. The source cluster will have the policy enabled.
5. **NOTE: The source cluster policy will not be run and will run on it's previous schedule.**
6. **To force sync the source cluster changes to the DR cluster is a manual step by the administrator to run the Source cluster policy, which will cause all changes to the target cluster to be lost.**
7. **To monitor progress of disallow writes, login to the DR cluster --> SyncIQ menu --> local targets --> find policy path and verify status is running. A job report will only appear once this step completes.**
8. **done.**

How to Enable DR Rehearsal Mode

1. 

DR Assistant

Failover Wizard
Running Failovers
Failover History
LiveOps DR Testing

Select Failover Type

○ SyncIQ Policy ○ Access Zone ● SmartConnect/IP Pool ○ Microsoft DFS

Select Source Cluster

Source Cluster: prod-cluster

Select Failover Mode

Failover Mode: ENABLE REHEARSAL * Cannot be used for an uncontrolled DR event. This must be reverted prior to failover

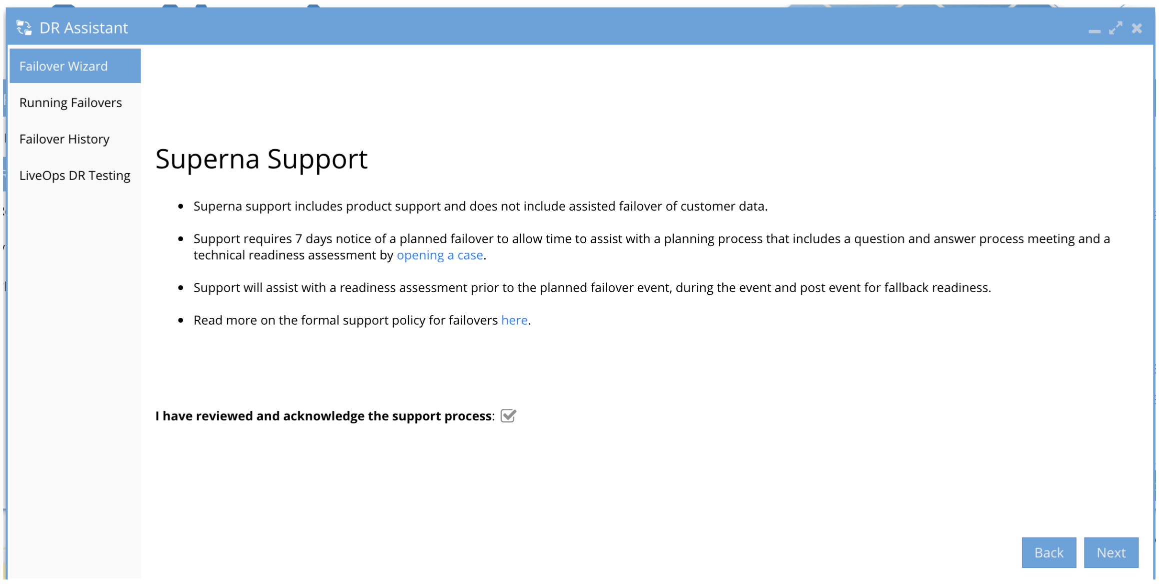
Select Failover Options

☑ Controlled Failover
☑ Data sync
☐ Config sync
☐ SMB Data Integrity Failover
☐ SyncIQ Resync Prep
☐ Disable SyncIQ Jobs on Failover Target
☐ Quota Sync
☑ Block Failover on Warnings
☐ Rollback renamed shares on failure

Back Next

2. Configure as per screenshot above and Click Next.

3. Acknowledge Support Process has been reviewed.

4. 

DR Assistant

Failover Wizard
Running Failovers
Failover History
LiveOps DR Testing

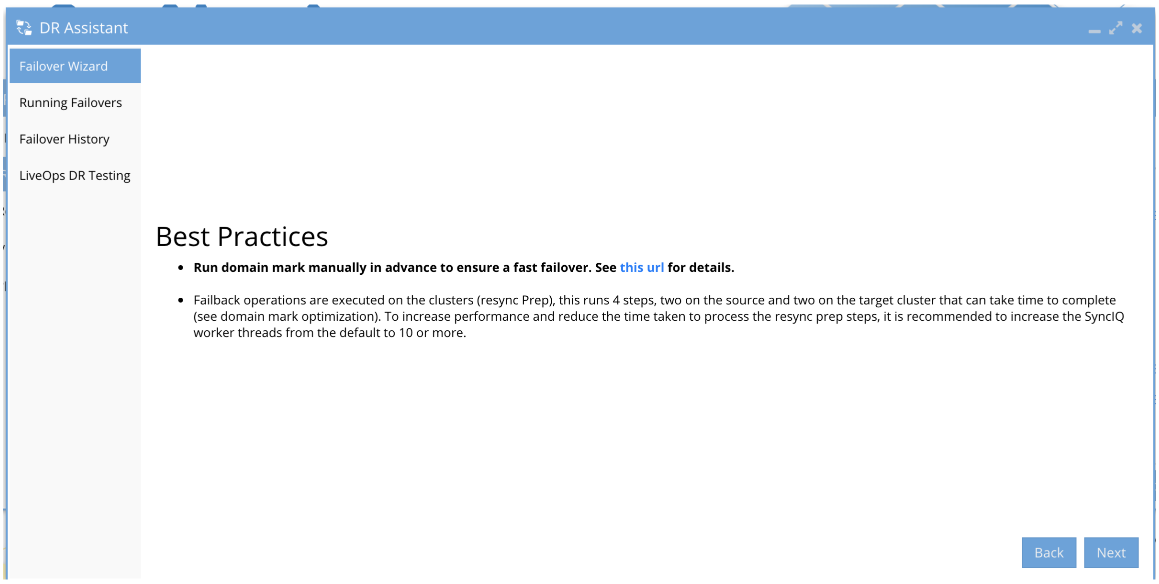
Superna Support

- Superna support includes product support and does not include assisted failover of customer data.
- Support requires 7 days notice of a planned failover to allow time to assist with a planning process that includes a question and answer process meeting and a technical readiness assessment by opening a case.
- Support will assist with a readiness assessment prior to the planned failover event, during the event and post event for fallback readiness.
- Read more on the formal support policy for failovers here.

I have reviewed and acknowledge the support process: ☑

Back Next

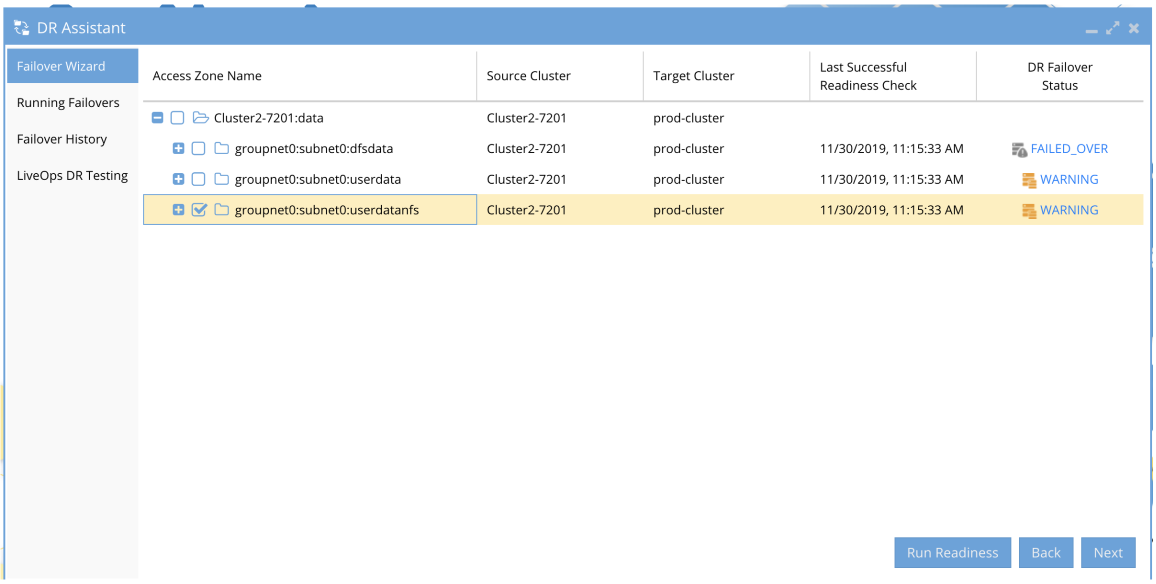
5. Review Best practices example below.

6. 

Best Practices

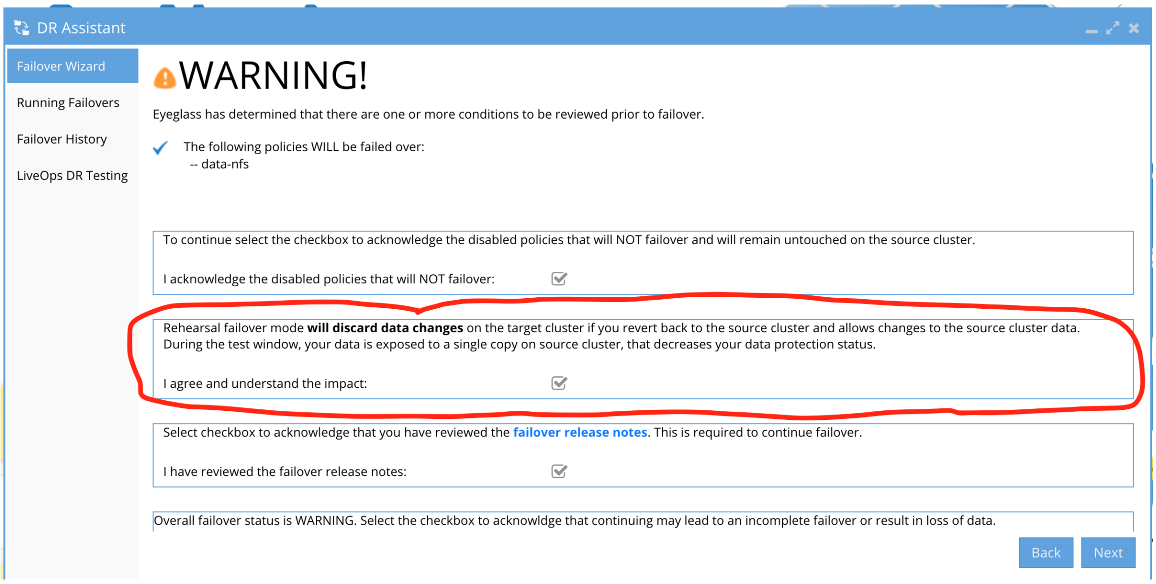
- **Run domain mark manually in advance to ensure a fast failover. See this url for details.**
- Failback operations are executed on the clusters (resync Prep), this runs 4 steps, two on the source and two on the target cluster that can take time to complete (see domain mark optimization). To increase performance and reduce the time taken to process the resync prep steps, it is recommended to increase the SyncIQ worker threads from the default to 10 or more.

7. Select the Access Zone, IP pool or SyncIQ policies depending on the failover type configured for your environment, then click Next.

8. 

Access Zone Name	Source Cluster	Target Cluster	Last Successful Readiness Check	DR Failover Status
□ Cluster2-7201:data	Cluster2-7201	prod-cluster		
□ groupnet0:subnet0:dfsdata	Cluster2-7201	prod-cluster	11/30/2019, 11:15:33 AM	FAILED_OVER
□ groupnet0:subnet0:userdata	Cluster2-7201	prod-cluster	11/30/2019, 11:15:33 AM	WARNING
☑ groupnet0:subnet0:userdatanfs	Cluster2-7201	prod-cluster	11/30/2019, 11:15:33 AM	WARNING

9. Validation Summary Screen is presented and special acknowledgment required for DR Rehearsal Mode that confirms understanding this will stop Data sync between the clusters. Acknowledge and Click Next.

10. 

WARNING!

Eyeglass has determined that there are one or more conditions to be reviewed prior to failover.

✓ The following policies WILL be failed over:
-- data-nfs

To continue select the checkbox to acknowledge the disabled policies that will NOT failover and will remain untouched on the source cluster.

I acknowledge the disabled policies that will NOT failover: ☑

Rehearsal failover mode **will discard data changes** on the target cluster if you revert back to the source cluster and allows changes to the source cluster data. During the test window, your data is exposed to a single copy on source cluster, that decreases your data protection status.

I agree and understand the impact: ☑

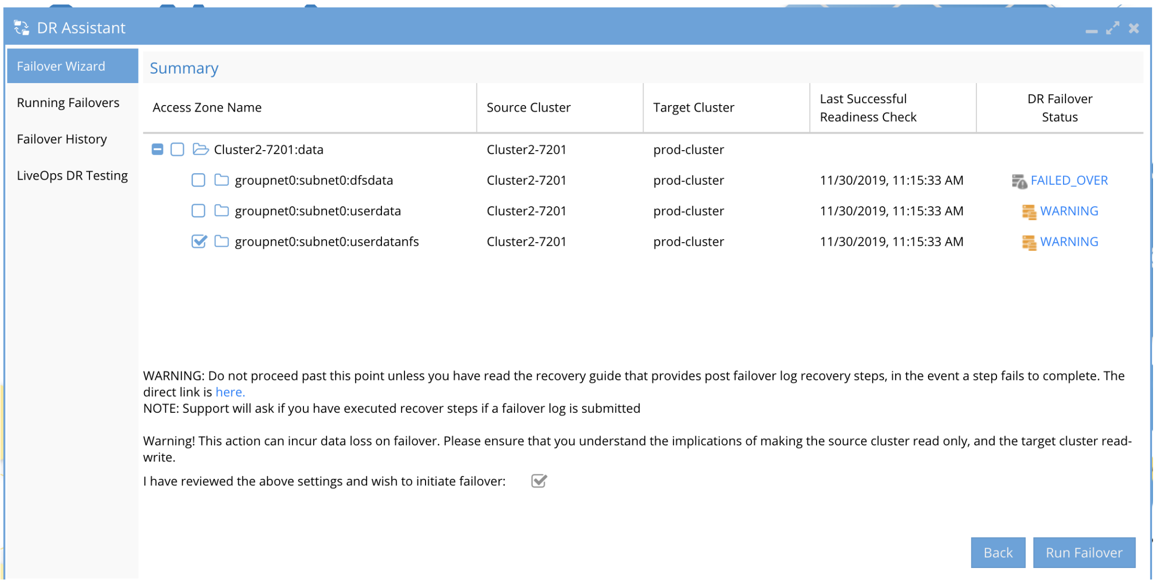
Select checkbox to acknowledge that you have reviewed the **failover release notes**. This is required to continue failover.

I have reviewed the failover release notes: ☑

Overall failover status is WARNING. Select the checkbox to acknowldge that continuing may lead to an incomplete failover or result in loss of data.

11. Final Screen is displayed with final acknowledgment required to Enter DR Rehearsal mode.

12. Start the DR Rehearsal mode by clicking the start Failover button.

13. 

Summary

Access Zone Name	Source Cluster	Target Cluster	Last Successful Readiness Check	DR Failover Status
□ Cluster2-7201:data	Cluster2-7201	prod-cluster		
□ groupnet0:subnet0:dfsdata	Cluster2-7201	prod-cluster	11/30/2019, 11:15:33 AM	FAILED_OVER
□ groupnet0:subnet0:userdata	Cluster2-7201	prod-cluster	11/30/2019, 11:15:33 AM	WARNING
☑ groupnet0:subnet0:userdatanfs	Cluster2-7201	prod-cluster	11/30/2019, 11:15:33 AM	WARNING

WARNING: Do not proceed past this point unless you have read the recovery guide that provides post failover log recovery steps, in the event a step fails to complete. The direct link is here.
NOTE: Support will ask if you have executed recover steps if a failover log is submitted

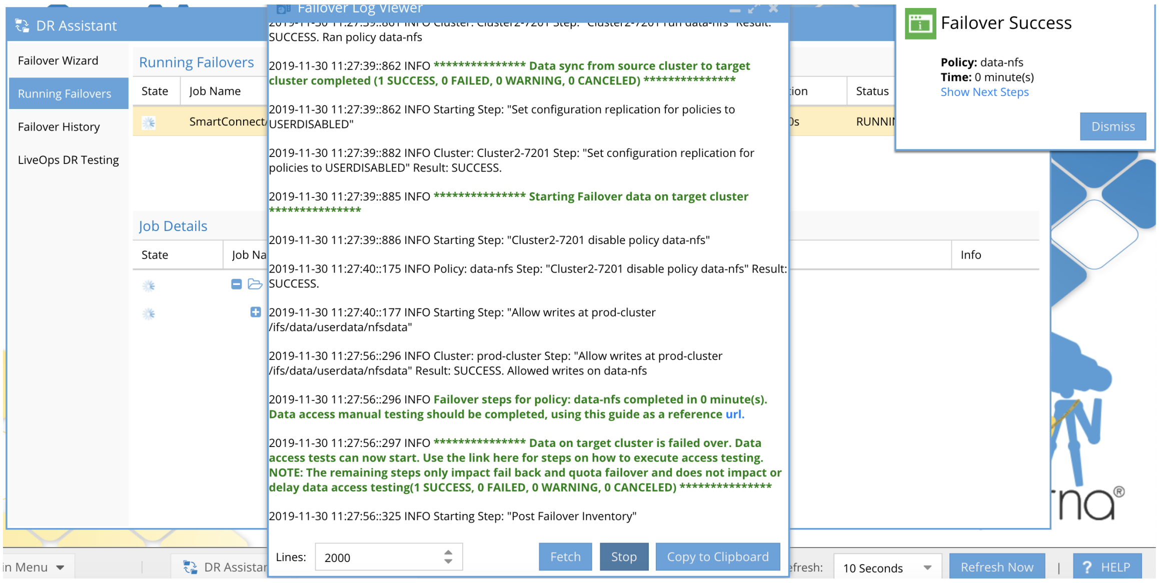
Warning! This action can incur data loss on failover. Please ensure that you understand the implications of making the source cluster read only, and the target cluster read-write.

I have reviewed the above settings and wish to initiate failover: ☑

14. The failover can be monitored with the watch button and use the copy to clipboard option to provide support with the log.

15. When DR Rehearsal Mode is active a pop up window will appear with a link to next steps. See example below.

16.



```
2019-11-30 11:27:39::861 INFO Cluster: Cluster2-7201 Step: "Cluster2-7201 run data-nfs" Result:
SUCCESS. Ran policy data-nfs

2019-11-30 11:27:39::862 INFO *************** Data sync from source cluster to target
cluster completed (1 SUCCESS, 0 FAILED, 0 WARNING, 0 CANCELED) ***************

2019-11-30 11:27:39::862 INFO Starting Step: "Set configuration replication for policies to
USERDISABLED"

2019-11-30 11:27:39::882 INFO Cluster: Cluster2-7201 Step: "Set configuration replication for
policies to USERDISABLED" Result: SUCCESS.

2019-11-30 11:27:39::885 INFO *************** Starting Failover data on target cluster
***************

2019-11-30 11:27:39::886 INFO Starting Step: "Cluster2-7201 disable policy data-nfs"

2019-11-30 11:27:40::175 INFO Policy: data-nfs Step: "Cluster2-7201 disable policy data-nfs" Result:
SUCCESS.

2019-11-30 11:27:40::177 INFO Starting Step: "Allow writes at prod-cluster
/ifs/data/userdata/nfsdata"

2019-11-30 11:27:56::296 INFO Cluster: prod-cluster Step: "Allow writes at prod-cluster
/ifs/data/userdata/nfsdata" Result: SUCCESS. Allowed writes on data-nfs

2019-11-30 11:27:56::296 INFO Failover steps for policy: data-nfs completed in 0 minute(s).
Data access manual testing should be completed, using this guide as a reference url.

2019-11-30 11:27:56::297 INFO *************** Data on target cluster is failed over. Data
access tests can now start. Use the link here for steps on how to execute access testing.
NOTE: The remaining steps only impact fail back and quota failover and does not impact or
delay data access testing(1 SUCCESS, 0 FAILED, 0 WARNING, 0 CANCELED) ***************

2019-11-30 11:27:56::325 INFO Starting Step: "Post Failover Inventory"
```

Failover Success

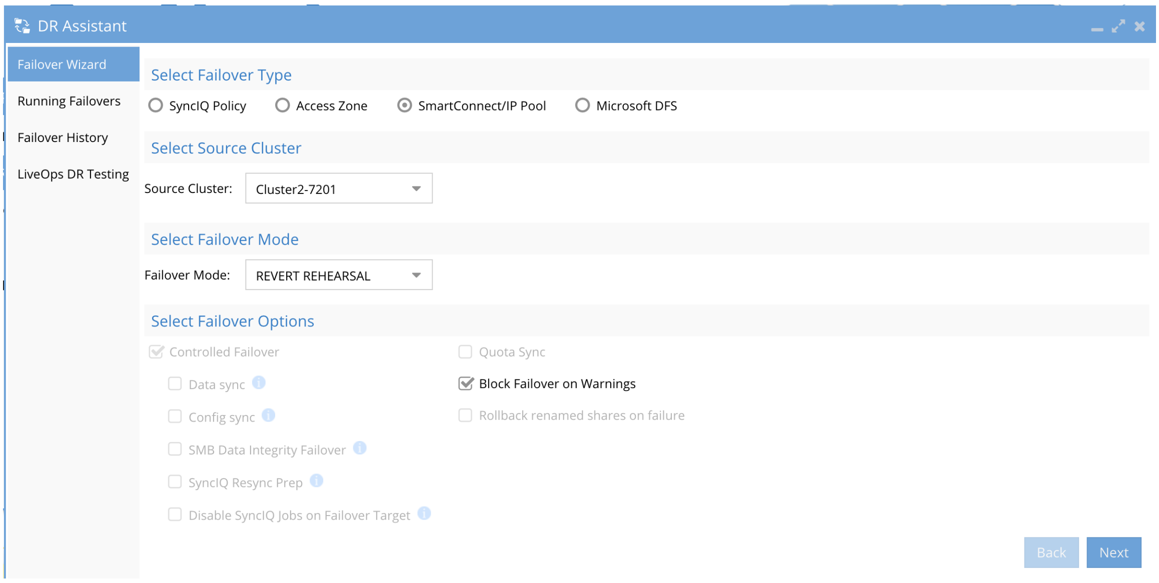
Policy: data-nfs
Time: 0 minute(s)
Show Next Steps

Dismiss

17. Done

How to Revert DR Rehearsal Mode

1. Open DR Assistant.
2. Select the same Source Cluster that was selected when you enabled Rehearsal Mode.
3. Change Failover Mode to Revert DR Rehearsal mode.

4. 

Select Failover Type

○ SyncIQ Policy ○ Access Zone ● SmartConnect/IP Pool ○ Microsoft DFS

Select Source Cluster

Source Cluster: Cluster2-7201

Select Failover Mode

Failover Mode: REVERT REHEARSAL

Select Failover Options

☑ Controlled Failover

□ Data sync

□ Config sync

□ SMB Data Integrity Failover

□ SyncIQ Resync Prep

□ Disable SyncIQ Jobs on Failover Target

□ Quota Sync

☑ Block Failover on Warnings

□ Rollback renamed shares on failure

5. Complete the steps to validate and review acknowledgments.
6. Start the Revert Failover job.
7. Review the Failover log with Watch and Copy to Clipboard button.
8. Once complete source to target cluster policies will be enabled to sync data on the previous schedule.
9. Done.

1.13. Post Failover Procedures

Home Top

Post Failover Procedures

Use this procedures that apply to your failover mode.

Post Access Zone Failover Steps

1. Test Dual Delegation .
2. Check SPN for SPN Errors .
3. Automated SMB connection switch to target cluster after Failover :
    a. OR use Manual SMB connection switch to target cluster after Failover.
4. Refreshing NFS connection after Failover completed .
5. Test Data Access and debug.

Post Access Zone Failover Health Check Steps

1. Post Access Zone Failover Checklist.

POST DFS Mode Failover Steps

1. Post Eyeglass Microsoft DFS Mode Failover Manual Steps for NFS Exports .
2. Post Eyeglass Microsoft DFS Mode Failover Checklist .
3. Procedure for Checking your SMB Clients Post DFS Failover .

1.14. How to Validate and troubleshoot A Successful Failover WHEN Data is NOT Accessible on the Target Cluster

Home Top

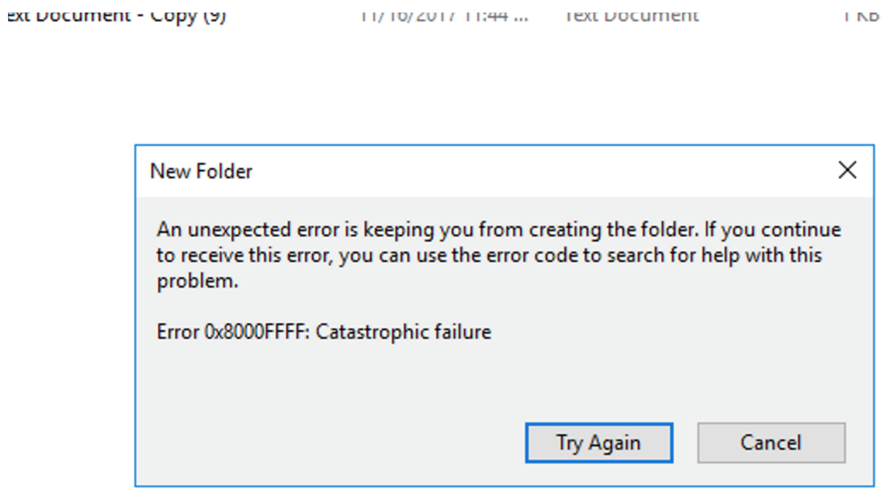
- Quick and Simple Debug Data Access Steps for Access Zone or IP Pool Failover Modes:
- Detailed Steps to Debug SmartConnect and DNS Resolution failures for Access Zone or IP Pool modes:
- Detailed Steps to test Mounting a DFS protected Share with DFS failover mode:
- Detailed steps to test NFS export remount for Access Zone, IP pool or SyncIQ mode

Quick and Simple Debug Data Access Steps for Access Zone or IP Pool Failover Modes:

NOTE: follow the order below to find root cause quickly.

1. **READ ME FIRST: Have you rebooted the PC you are testing SMB share access? Do not proceed if you have not already done this! Number issue when testing data access.**

2. Did you get this error message below? This means your PC is connected to the source cluster that is read only and locked by SyncIQ. Reboot PC test again.



ext Document - Copy (9)   11/16/2017 11:44 ...   Text Document   1 KB

New Folder

An unexpected error is keeping you from creating the folder. If you continue to receive this error, you can use the error code to search for help with this problem.

Error 0x8000FFFF: Catastrophic failure

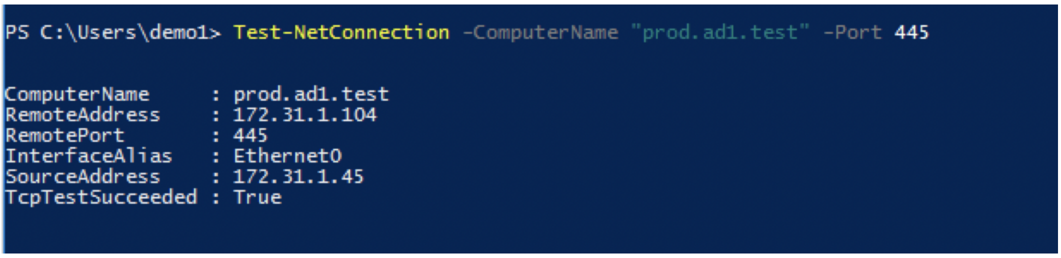
   a.

3. Check your firewall/network is not blocking the SMB protocol from your test PC and the Target Cluster SMB share

   a. Open a powershell prompt on the pc you are using to test data access. Replace yellow with the FQDN smartconnect name used to mount the SMB share.

   b. **Test-NetConnection -ComputerName "example.smartconnect.test" -Port 445**

   c. A successful test should return the output below.

   d. 

```
PS C:\Users\demo1> Test-NetConnection -ComputerName "prod.ad1.test" -Port 445


ComputerName     : prod.ad1.test
RemoteAddress    : 172.31.1.104
RemotePort       : 445
InterfaceAlias   : Ethernet0
SourceAddress    : 172.31.1.45
TcpTestSucceeded : True
```

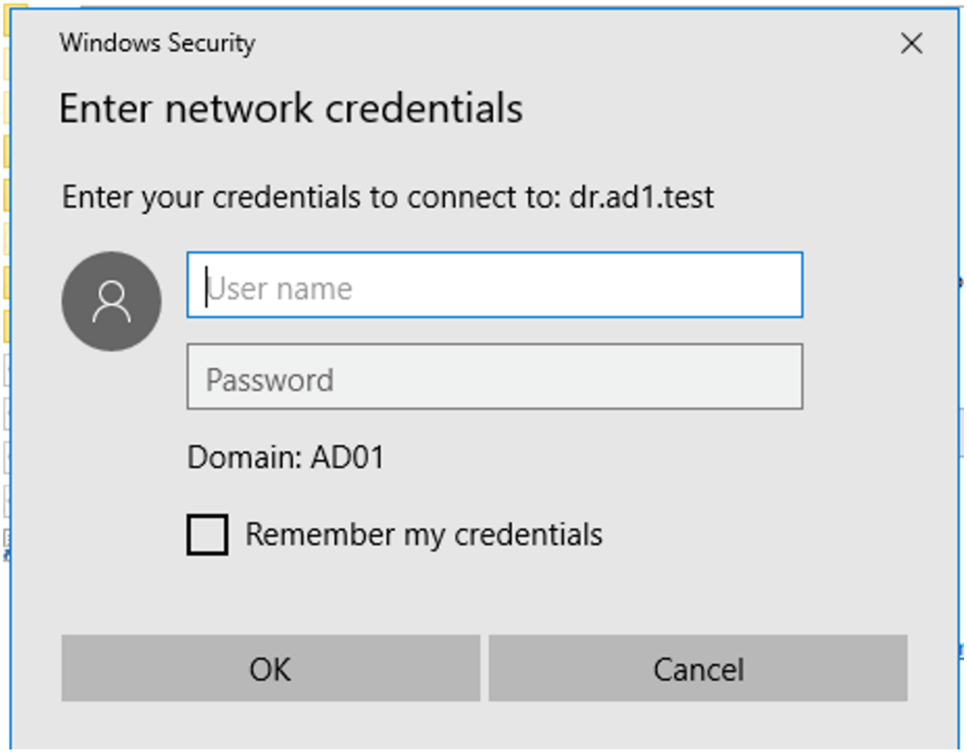
e. **IMPORTANT: If the test fails, escalate to your firewall team to resolve the blocked SMB port to the target cluster. Do not proceed until this test passes.**

4. Check DNS and SmartConnect by pinging the FQDN SmartConnect name (**NEVER USE SHORT NAME TO PING**) and verify the IP address returned is from the target cluster.

   a. If you get DNS failed to resolve error message continue with detailed nslookup steps below to check DNS resolution of SmartConnect names. If IP is correct check next steps below.

5. **Mount share from client (DFS or non DFS) with password login popup Error**

   a. Did you get this popup message to login with a user name and password? This is mostly likely an Active Directory SPN missing on the target cluster AD computer object. Use ADSI Edit to verify the HOST\<FQDN SmartConnect name> is present on the SPN property of the target cluster. See animated GIF example of how to check.

i. 

Windows Security

Enter network credentials

Enter your credentials to connect to: dr.ad1.test

Domain: AD01

☐ Remember my credentials

b. Enter an administrator account to authenticate and test data access before fixing the SPN to verify this the only issue

6. Done. If none of these steps resolve data access. Then proceed into the detailed debugging steps below.

Detailed Steps to Debug SmartConnect and DNS Resolution failures for Access Zone or IP Pool modes:

Test DNS response on the clusters: This test verifies that SmartConnect names were failed over successfully and also can verify if dual delegation in your DNS environment is setup correctly. This test also eliminates any issues with your internal DNS and verifies PowerScale SmartConnect zones failed over successfully.

1. If you get failed Ping or name does not resolve name to correct IP address of the TARGET cluster. **Continue with steps below to debug DNS.**
    a. From any Windows client machine type "**nslookup**" **<press enter key> .**
    b. **Source Cluster DNS Test:**
        i. Then type "**server x.x.x.x**" <**enter key>** (where x.x.x.x is the Subnet service ip of the **source** cluster).
        ii. Type "**FQDN of SmartConnect Zone used in failover**" **<press enter key> . Hint: Refer to the failover log from DR Assistant for the full list of SmartConnect names that were failed over.**
        iii. The **expected response is a failed resolution** since failover disables the SOURCE cluster DNS response. **It is important clients do not receive an IP from the source cluster.**
        iv. **Example** of a failed nslookup on the cluster you failed away from "** server can't find userdata.ad1.test: REFUSED"
        v. NOTE: if lookup does NOT return REFUSED response, then SmartConnect name did not failover correctly AND consult recovery guide Networking section**. To fix SmartConnect names.**
2. **Target Cluster DNS Test:**
    a. Test **TARGET** cluster SSIP (subnet service IP) with DNS.
    b. Type "**server y.y.y.y**" <**enter key>** (where y.y.y.y is the subnet service ip of the **target** cluster).

c. Type "**FQDN of SmartConnect Zone used in failover**". Refer to the failover log for list of SmartConnect names that were failed over

d. Expected response **SUCCESSFUL NAME RESOLUTION RETURNING IP OF THE TARGET CLUSTER**. This means SmartConnect was failed over **correctly** to the **target** cluster.

e. If DNS test fails this step OR IP fails to resolve OR is the wrong IP address. **Consult recovery guide Networking section to fix SmartConnect names.**

f. **Double check dual delegation is configured correctly.**

   i. **On a Windows PC type "nslookup" at the command prompt.**

   ii. **Type "set type=ns" <enter key> .**

   iii. **Type "FQDN of smartconnect name" .**

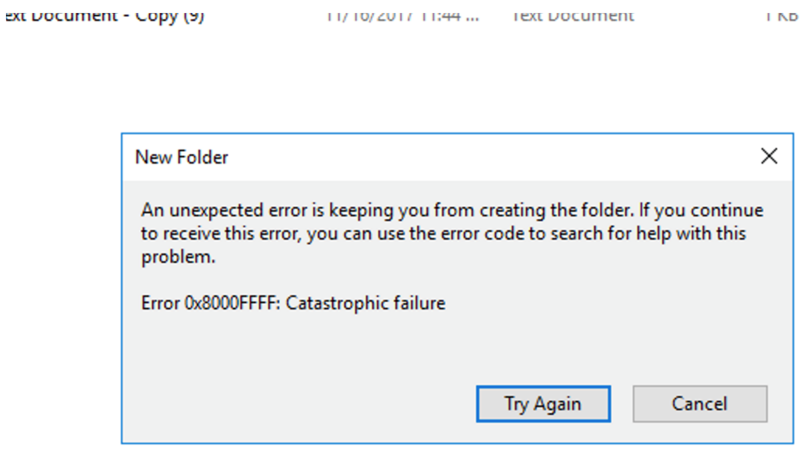
   iv. **You should receive two name server IP in the response, and each should be the SSIP on source and target cluster.** If you do not receive 2 name server records in the response, Dual DNS delegation is not configured correctly. **Escalate to your DNS administrator.**

   v. **Root Cause: Your internal DNS is not setup correctly for dual delegation is not configured correctly, since SSIP on the cluster correctly answers DNS queries. Stop here and correct using guide and video below.**

   vi.

Detailed Steps to test Mounting a DFS protected Share with DFS failover mode:

1. From a Windows client machine connected to Active Directory mount a dfs folder. Example: \\<domain name>\<dfs root name>\<DFS folder name>
2. Verify file write access by creating a file.
    a. If successful - **done.**
3. If write test fails OR mount fails or mount error:
    a. Login to the source cluster and verify the SMB share used for the DFS referral UNC has been **renamed igls-dfs-xxx,** where xxx is the name of the share used for the referral UNC on the DFS folder. If the share name does not have the igls-dfs prefix, add the prefix and save the share.
        i. Common error when DFS client is still connected to the source cluster.



ext Document - Copy (9)   11/10/2017 11:44 ...   Text Document   1 KB

New Folder

An unexpected error is keeping you from creating the folder. If you continue to receive this error, you can use the error code to search for help with this problem.

Error 0x8000FFFF: Catastrophic failure

        ii.
    b. Retest data access.

    c. If data write still fails, login to the target cluster and verify the SMB share name **DOES NOT have igls-DFS prefix.** If it does remove the prefix and save the SMB share.

    d. Retest data access.

    e. **Ask support for a list of SMB Shares that failed to rename during failover to get a complete list of shares that need to repeat the above steps to remediate failed rename steps.**

4. Double Check DFS Folder is setup correctly.

1. If the above steps did not show a rename step failed on source or target cluster, continue below to double check DFS folder configuration.

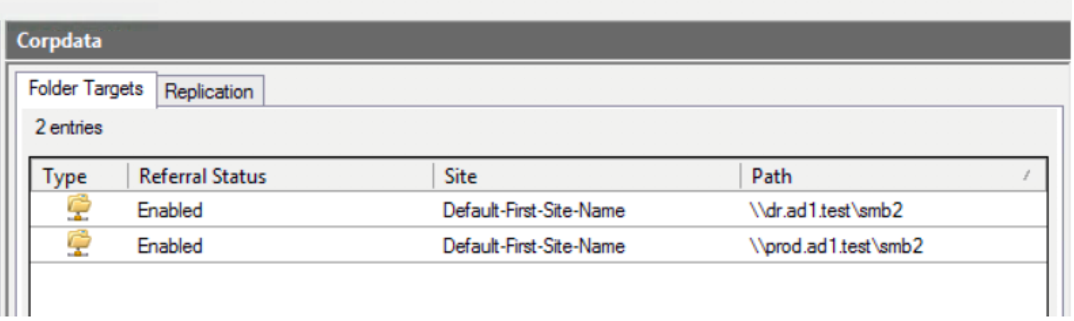
2. DFS Folder Configuration Validation:

    a. Verify DFS referrals are correctly configured in Microsoft DFS Management snapin.

    b. Check each item below to verify configuration:

    c. Open DFS manager snapin, right click the DFS folder you are validating

    d. See example



2 entries

Type	Referral Status	Site	Path
	Enabled	Default-First-Site-Name	\\dr.ad1.test\smb2
	Enabled	Default-First-Site-Name	\\prod.ad1.test\smb2

    e. Verify if both DFS referrals exist and are pointing at source and target cluster SmartConnect names and the share name is the same name as the screenshot example shows.

Continue to next step. MAKE SURE DFS REFERRALS USE FQDN SMARTCONNECT NAME, NEVER USE SHORT DNS NAMES.

f. **Test each referral mount UNC path DIRECTLY** :

  i. Example from above tested from a Windows client \\dr.ad1.test\smb2 (failover target cluster SmartConnect name used in this test).

  ii. If the share mounts and data is visible, verify you can write data.

  iii. This test verifies DNS and SmartConnect is configured correctly and AD authentication to the SMB share is correctly configured.

  iv. **If this step fails continue below.**

3. Follow steps above in this section How to Validate and troubleshoot A Successful Failover WHEN Data is NOT Accessible on the Target Cluster.

   a. If the above steps find a DNS resolution issue, fix the issue and retest direct share referral UNC mount to DR target cluster or mount the DFS folder again.

Detailed steps to test NFS export remount for Access Zone, IP pool or SyncIQ mode

1. NFS exports must be remounted to allow the Linux host to resolve the name to ip and connect to the export.
2. Command to unmount an export if a file is open is "umount -fl **<export-path-here>"** (the flags are force and lazy to un mount if an open file exists).
3. Command to re-read /etc/fstab and mount any export that is not already mounted "sudo mount -a" (Run as root user).
4. If a mount error occurs review the error message for reason.
5. Type "mount".
6. Find the export in the output and verify the ip address showing in the output is from the target cluster, if not follow SmartConnect debugging steps.
7. To test data write access:
    1. Change directory to the mount point created in /etc/fstab .
    2. **example only if mount point was /mnt/appdata:**
        1. **cd /mnt/appdata**
        2. **touch test.txt**
        3. The above command should complete without error. If a read- only filesystem error is returned, it means DNS returned the source cluster ip address, follow SmartConnect steps here.
        4. Verify the file was created "**ls test.txt**"
        5. **If the file is present data access is confirmed.**
        6. Clean up test file:
            1. **rm test.txt**

8. NOTE: IF YOU CHANGED THE TARGET PATH TO REPLICATE AN EXPORT THE REMOUNT PATH WILL NEED TO BE UPDATED. EXAMPLE: source path /ifs/data/export is replicated to /ifs/data/dr/export will require the host to change the mount path to /ifs/data/dr/export.
    a. To avoid this issue do not change the target cluster path when creating the SyncIQ policy

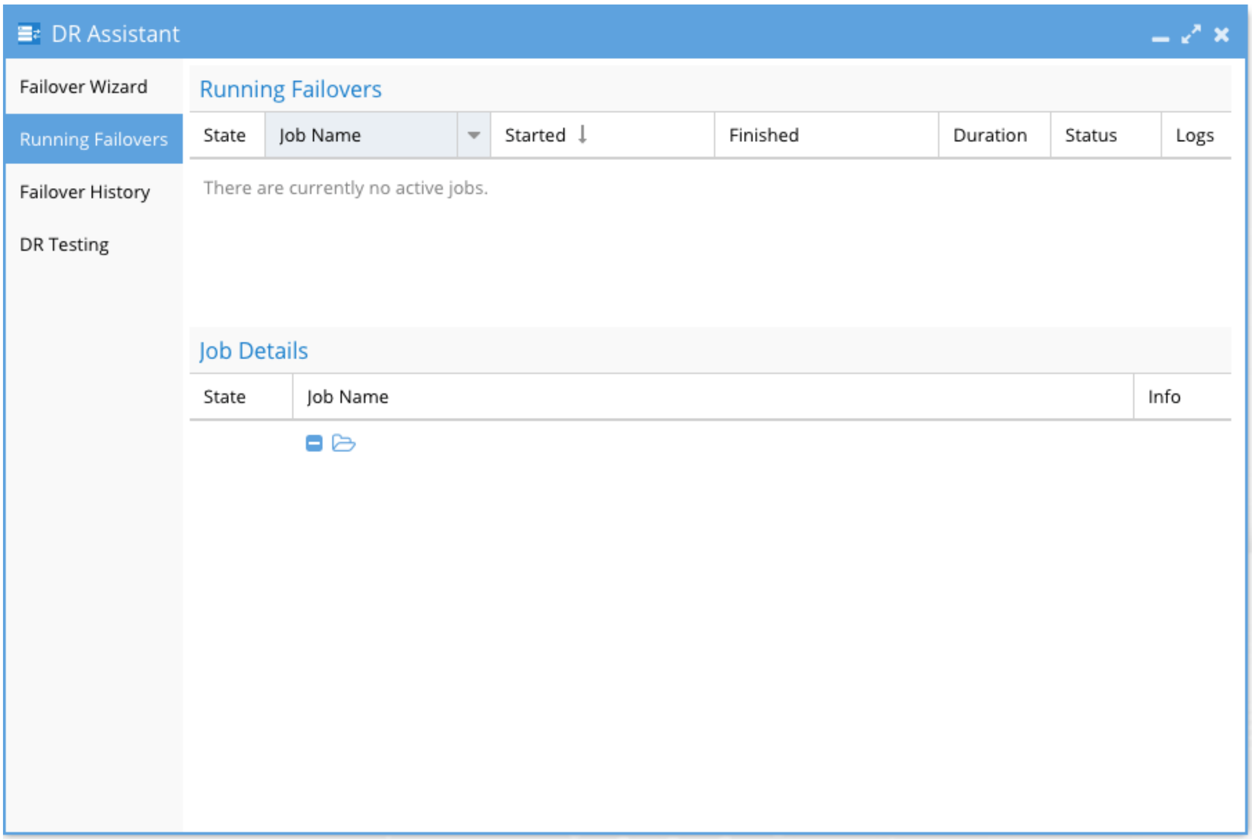
1.15. How to Monitor the Eyeglass Assisted Failover

Home Top

How to Monitor the Eyeglass Assisted Failover

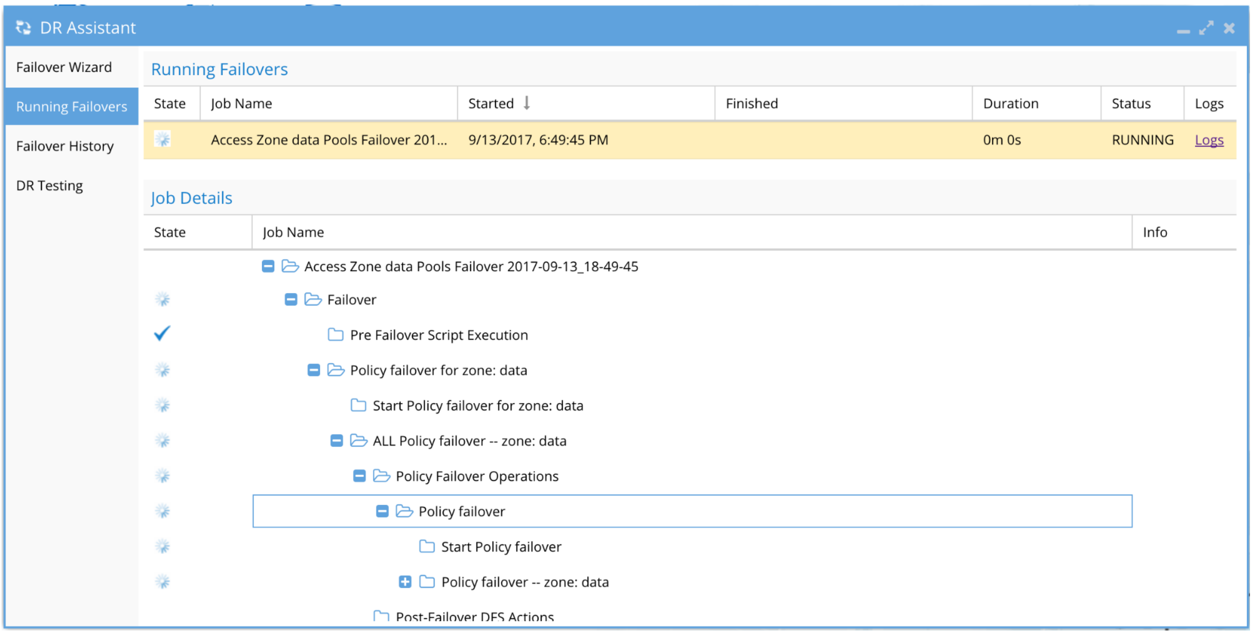
In-Progress Failover

Once a failover has been started, you can monitor its progress from the Eyeglass **DR Assistant / Running Failovers** tab.



There are currently no active jobs.

From this window you can expand the **Job Details** tree to see the progress and status for each failover step.



Running Failovers

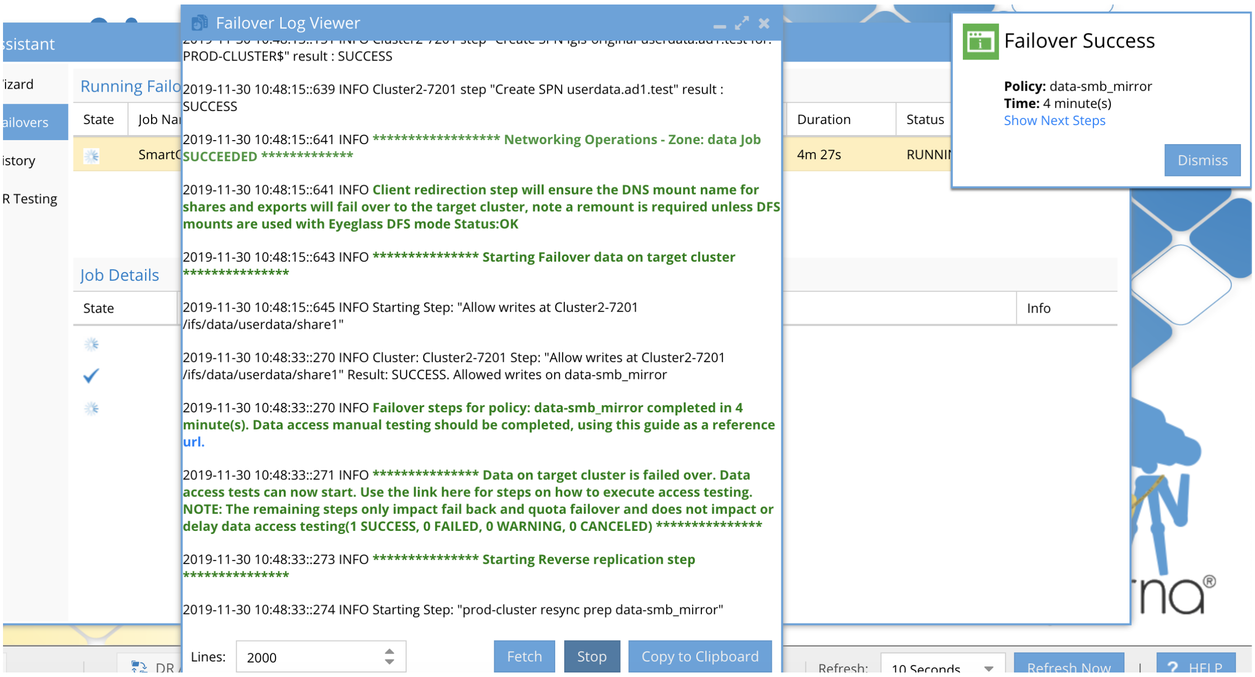
State	Job Name	Started ↓	Finished	Duration	Status	Logs
	Access Zone data Pools Failover 201...	9/13/2017, 6:49:45 PM		0m 0s	RUNNING	Logs

Job Details

```
State   Job Name                                                        Info
          Access Zone data Pools Failover 2017-09-13_18-49-45
            Failover
✓             Pre Failover Script Execution
              Policy failover for zone: data
                Start Policy failover for zone: data
                ALL Policy failover -- zone: data
                  Policy Failover Operations
                    Policy failover
                      Start Policy failover
                      Policy failover -- zone: data
                  Post-Failover DFS Actions
```

You can also open the failover log from this window to see the details for each step by selecting the **Logs** link.

- As of release 2.5.6 or later a copy to clipboard option is available and link to support site.
- The failover complete popup window is also new in 2.5.6 or later to prompt Data Access Testing as soon as all required steps are completed.



```
PROD-CLUSTER$" result : SUCCESS

2019-11-30 10:48:15::639 INFO Cluster2-7201 step "Create SPN userdata.ad1.test" result :
SUCCESS

2019-11-30 10:48:15::641 INFO ****************** Networking Operations - Zone: data Job
SUCCEEDED *************

2019-11-30 10:48:15::641 INFO Client redirection step will ensure the DNS mount name for
shares and exports will fail over to the target cluster, note a remount is required unless DFS
mounts are used with Eyeglass DFS mode Status:OK

2019-11-30 10:48:15::643 INFO *************** Starting Failover data on target cluster
***************

2019-11-30 10:48:15::645 INFO Starting Step: "Allow writes at Cluster2-7201
/ifs/data/userdata/share1"

2019-11-30 10:48:33::270 INFO Cluster: Cluster2-7201 Step: "Allow writes at Cluster2-7201
/ifs/data/userdata/share1" Result: SUCCESS. Allowed writes on data-smb_mirror

2019-11-30 10:48:33::270 INFO Failover steps for policy: data-smb_mirror completed in 4
minute(s). Data access manual testing should be completed, using this guide as a reference
url.

2019-11-30 10:48:33::271 INFO *************** Data on target cluster is failed over. Data
access tests can now start. Use the link here for steps on how to execute access testing.
NOTE: The remaining steps only impact fail back and quota failover and does not impact or
delay data access testing(1 SUCCESS, 0 FAILED, 0 WARNING, 0 CANCELED) ***************

2019-11-30 10:48:33::273 INFO *************** Starting Reverse replication step
***************

2019-11-30 10:48:33::274 INFO Starting Step: "prod-cluster resync prep data-smb_mirror"
```

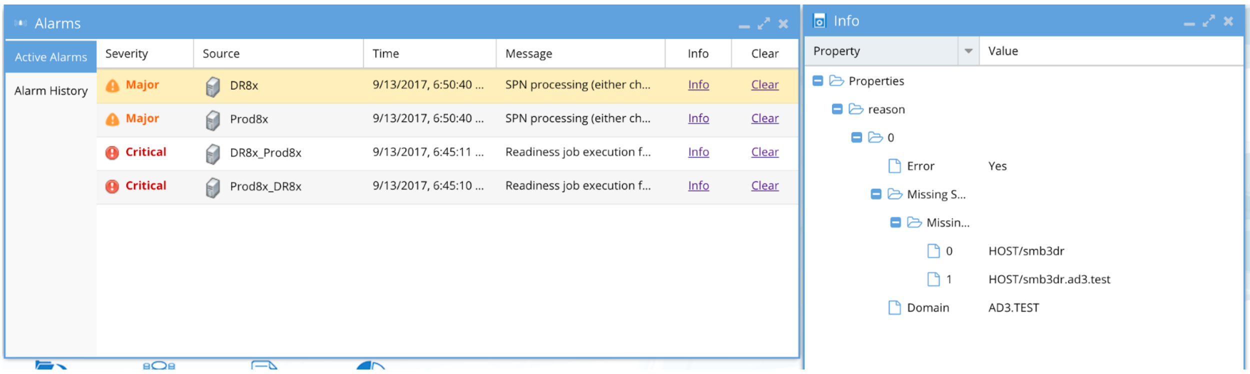
Lines: 2000

Failover Success

Policy: data-smb_mirror
Time: 4 minute(s)
Show Next Steps

Each entry in the log is timestamped. The log is updated as the failover proceeds and you can see log updates by closing and opening the log file again.

Should an error occur during failover, an Eyeglass system alarm will be issued. If you have configured external notification by email or Twitter you will receive these alarms this way. The alarms are also visible from the Eyeglass **Alarms** window.

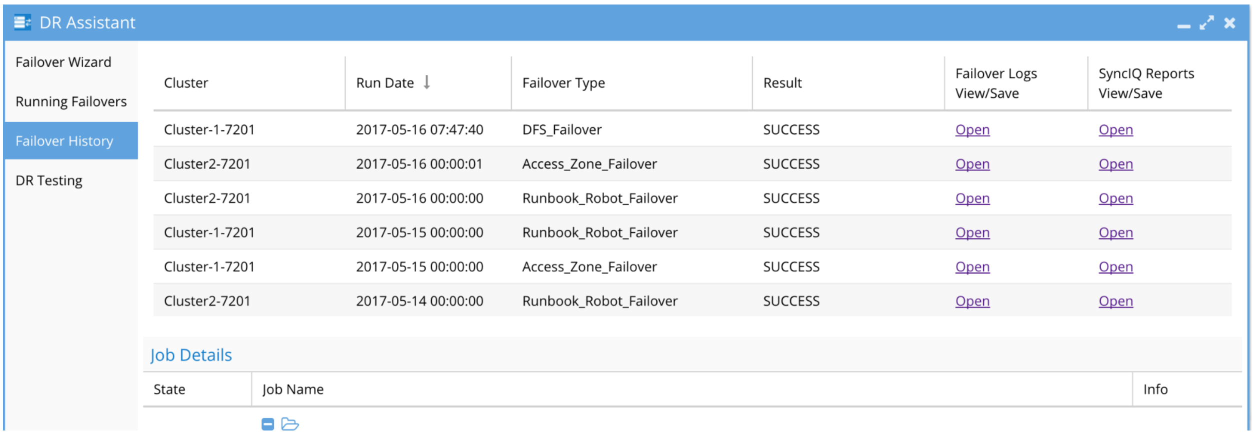


Severity	Source	Time	Message	Info	Clear
Major	DR8x	9/13/2017, 6:50:40 ...	SPN processing (either ch...	Info	Clear
Major	Prod8x	9/13/2017, 6:50:40 ...	SPN processing (either ch...	Info	Clear
Critical	DR8x_Prod8x	9/13/2017, 6:45:11 ...	Readiness job execution f...	Info	Clear
Critical	Prod8x_DR8x	9/13/2017, 6:45:10 ...	Readiness job execution f...	Info	Clear

Property	Value
Properties	
reason	
0	
Error	Yes
Missing S...	
Missin...	
0	HOST/smb3dr
1	HOST/smb3dr.ad3.test
Domain	AD3.TEST

Completed Failover

Once the failover is completed, it will appear in the **DR Assistant / Failover History** tab.



Cluster	Run Date ↓	Failover Type	Result	Failover Logs View/Save	SyncIQ Reports View/Save
Cluster-1-7201	2017-05-16 07:47:40	DFS_Failover	SUCCESS	Open	Open
Cluster2-7201	2017-05-16 00:00:01	Access_Zone_Failover	SUCCESS	Open	Open
Cluster2-7201	2017-05-16 00:00:00	Runbook_Robot_Failover	SUCCESS	Open	Open
Cluster-1-7201	2017-05-15 00:00:00	Runbook_Robot_Failover	SUCCESS	Open	Open
Cluster-1-7201	2017-05-15 00:00:00	Access_Zone_Failover	SUCCESS	Open	Open
Cluster2-7201	2017-05-14 00:00:00	Runbook_Robot_Failover	SUCCESS	Open	Open

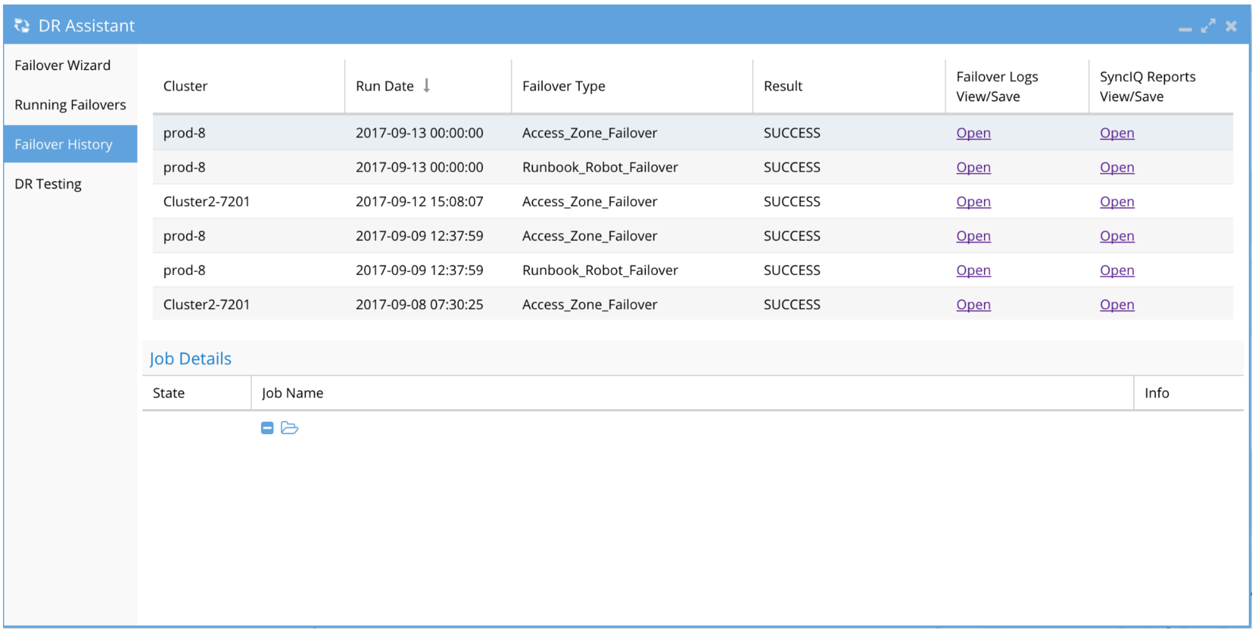
Job Details

State	Job Name	Info

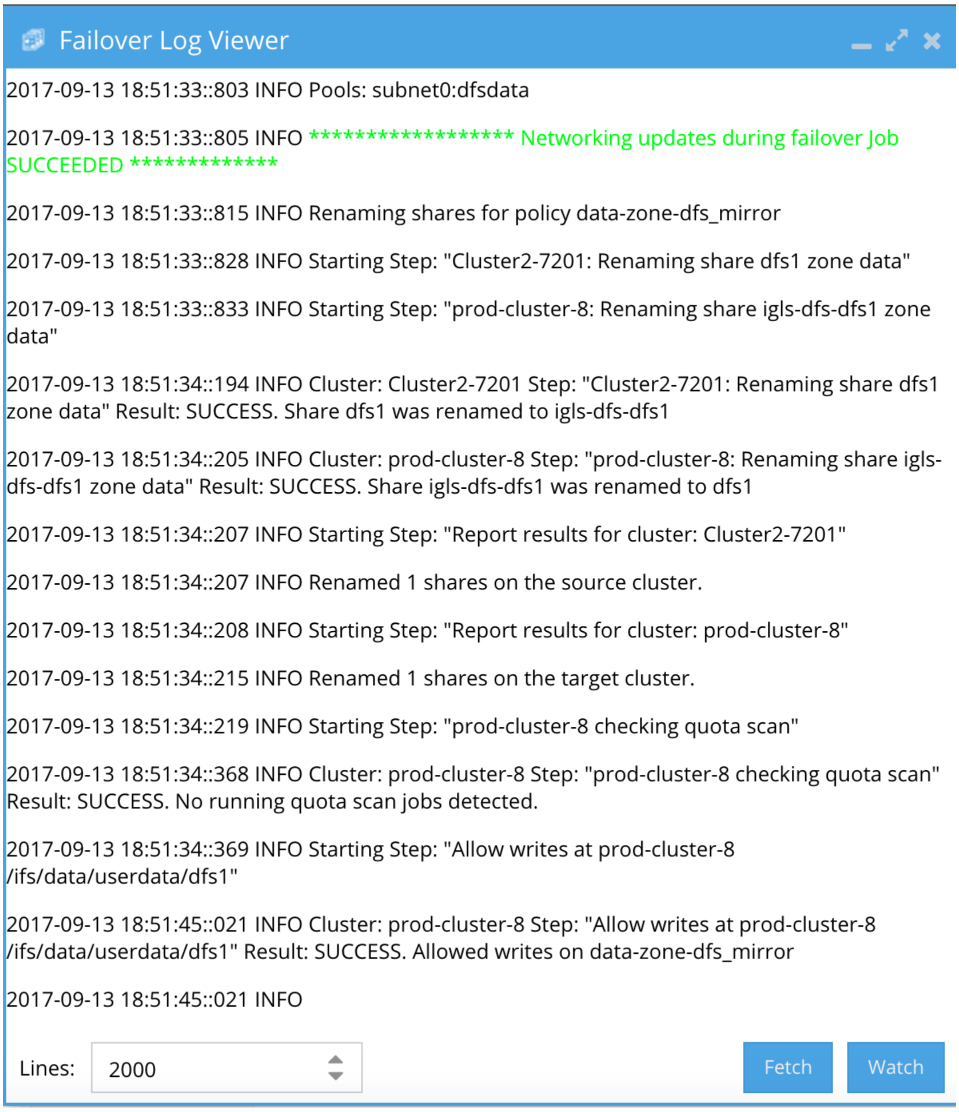
The **Result** column displays the **SUCCESS** if the Failover completed successfully and **FAIL** if there were errors encountered in the Failover steps. The SyncIQ reports are available separately to review cluster logs for each step of the failover.

Note: An Access Zone Failover with Result of SUCCESS may have had SPN errors. Please refer to the Access Zone Failover Guide for details on checking for SPN errors and resolution.

From the **Failover History** window, click on the row corresponding to the Failover that you would like to review. The **Job Details** tree will appear below and the Failover Log can be retrieved for viewing or download by selecting the **Open** link.



Cluster	Run Date ↓	Failover Type	Result	Failover Logs View/Save	SyncIQ Reports View/Save
prod-8	2017-09-13 00:00:00	Access_Zone_Failover	SUCCESS	Open	Open
prod-8	2017-09-13 00:00:00	Runbook_Robot_Failover	SUCCESS	Open	Open
Cluster2-7201	2017-09-12 15:08:07	Access_Zone_Failover	SUCCESS	Open	Open
prod-8	2017-09-09 12:37:59	Access_Zone_Failover	SUCCESS	Open	Open
prod-8	2017-09-09 12:37:59	Runbook_Robot_Failover	SUCCESS	Open	Open
Cluster2-7201	2017-09-08 07:30:25	Access_Zone_Failover	SUCCESS	Open	Open



```
2017-09-13 18:51:33::803 INFO Pools: subnet0:dfsdata

2017-09-13 18:51:33::805 INFO ****************** Networking updates during failover Job SUCCEEDED *************

2017-09-13 18:51:33::815 INFO Renaming shares for policy data-zone-dfs_mirror

2017-09-13 18:51:33::828 INFO Starting Step: "Cluster2-7201: Renaming share dfs1 zone data"

2017-09-13 18:51:33::833 INFO Starting Step: "prod-cluster-8: Renaming share igls-dfs-dfs1 zone data"

2017-09-13 18:51:34::194 INFO Cluster: Cluster2-7201 Step: "Cluster2-7201: Renaming share dfs1 zone data" Result: SUCCESS. Share dfs1 was renamed to igls-dfs-dfs1

2017-09-13 18:51:34::205 INFO Cluster: prod-cluster-8 Step: "prod-cluster-8: Renaming share igls-dfs-dfs1 zone data" Result: SUCCESS. Share igls-dfs-dfs1 was renamed to dfs1

2017-09-13 18:51:34::207 INFO Starting Step: "Report results for cluster: Cluster2-7201"

2017-09-13 18:51:34::207 INFO Renamed 1 shares on the source cluster.

2017-09-13 18:51:34::208 INFO Starting Step: "Report results for cluster: prod-cluster-8"

2017-09-13 18:51:34::215 INFO Renamed 1 shares on the target cluster.

2017-09-13 18:51:34::219 INFO Starting Step: "prod-cluster-8 checking quota scan"

2017-09-13 18:51:34::368 INFO Cluster: prod-cluster-8 Step: "prod-cluster-8 checking quota scan" Result: SUCCESS. No running quota scan jobs detected.

2017-09-13 18:51:34::369 INFO Starting Step: "Allow writes at prod-cluster-8 /ifs/data/userdata/dfs1"

2017-09-13 18:51:45::021 INFO Cluster: prod-cluster-8 Step: "Allow writes at prod-cluster-8 /ifs/data/userdata/dfs1" Result: SUCCESS. Allowed writes on data-zone-dfs_mirror

2017-09-13 18:51:45::021 INFO
```

Lines: 2000

1.16. Troubleshooting Failover

Home Top

Troubleshooting Failover

Failover Recovery Procedures

In the event that a Failover does not complete all steps successfully, please refer to the Eyeglass Failover Recovery Procedures to assess the state of your environment and for recovery steps.

Collecting Logs for Failover Troubleshooting

To collect the logs for Failover Troubleshooting, following the instructions for collecting support information found in the Eyeglass FAQ document here. The Failover logs will be included with other Eyeglass logs contained in the Logs Backup file.

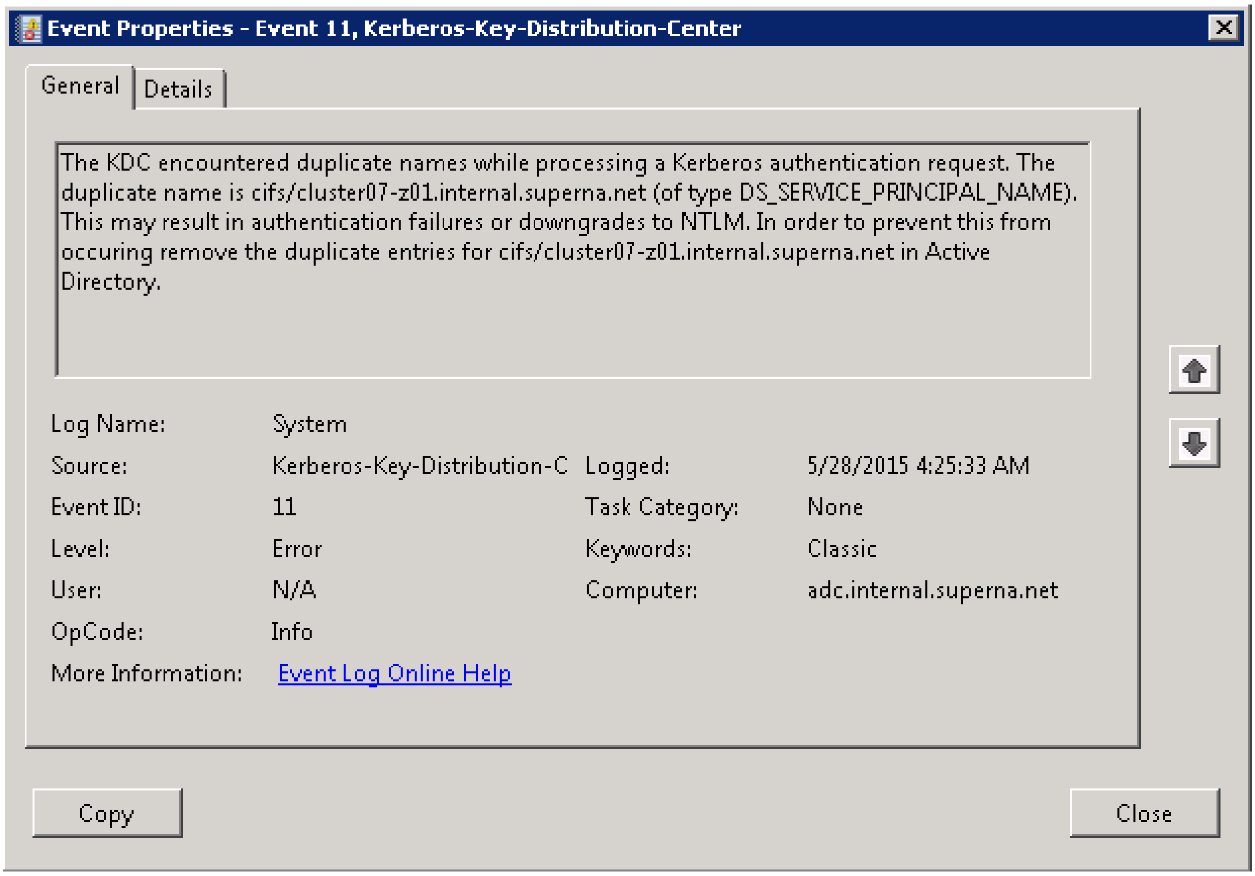
Authentication with Service Principal Name Considerations with Active Directory and SMB Shares in Access Zones

Active Directory only allows a single computer account to register a Service Principal Name against a computer account. This property can be seen with ADSI Edit tool. The SPN is in the form of HOST/service name and typically has 2 entries one for Netbios naming (15 characters), and one for DNS URL format for each SmartConnect zone or zone alias created on a cluster.

The service principal name is required to exist on the machine account handling authentication requests from clients to send to a domain controller for authentication using kerberos session tickets.

Active Directory **does** prevent duplicate SPN from being registered, if this occurs Kerberos authentication fails for clients and they will be unable to mount data if NTLM fall back authentication does not succeed. Eyeglass failover deletes the SPN's of the subnet pool and it’s aliases on the selected source cluster Access Zone from the AD computer account, or ALL AD providers assigned to the Access Zone during failover.

Eyeglass also scans cluster machine accounts during configuration replication jobs and fixes missing SPN’s if detected.


Event Properties - Event 11, Kerberos-Key-Distribution-Center
General
Details
Copy
Close

The KDC encountered duplicate names while processing a Kerberos authentication request. The duplicate name is cifs/cluster07-z01.internal.superna.net (of type DS_SERVICE_PRINCIPAL_NAME). This may result in authentication failures or downgrades to NTLM. In order to prevent this from occuring remove the duplicate entries for cifs/cluster07-z01.internal.superna.net in Active Directory.

Log Name: System
Source: Kerberos-Key-Distribution-C Logged: 5/28/2015 4:25:33 AM
Event ID: 11 Task Category: None
Level: Error Keywords: Classic
User: N/A Computer: adc.internal.superna.net
OpCode: Info
More Information: Event Log Online Help

Example: Error seen after duplicate SPN’s were created. This is seen on the domain controller attempting to authenticate a mount request. This error only appears once and not for each failed authentication.

For information this event see KB article

https://support.microsoft.com/en-us/kb/321044

1.17. Appendix A - Advanced Failover Modes

Home Top

Appendix A - Advanced Failover Modes

Cached config advanced mode

In some cases customers can not pre-sync configuration data from one cluster to the DR site, as this exposes data at the DR location. This requirement means, all configuration data must be cached on the Eyeglass appliance versus pre-synced to the DR cluster.

Eyeglass always has a database of changes but it’s not used for failover operations as this information can be stale in planned failovers.   As of release 1.6 and later a failover mode switches Eyeglass to sync configuration data to files that are used in all failover modes controlled and uncontrolled.

The process now looks like this:

1. Sync every 5 minutes, get configuration information difference changes and update local files on Eyeglass appliance.
2. Controlled AND uncontrolled failover reads from cache files only, and never communicates with the source cluster to create shares, exports, quotas during the failover process on the target DR cluster.
3. For controlled failover this means that potential stale data is used to failover in this scenario.

How to enable cached config advanced mode

1. Ssh to Eyeglass as admin.

2. igls adv failovermode set --readfromfile=true.
3. Done.

1.18. IPv6 Requirements and Considerations

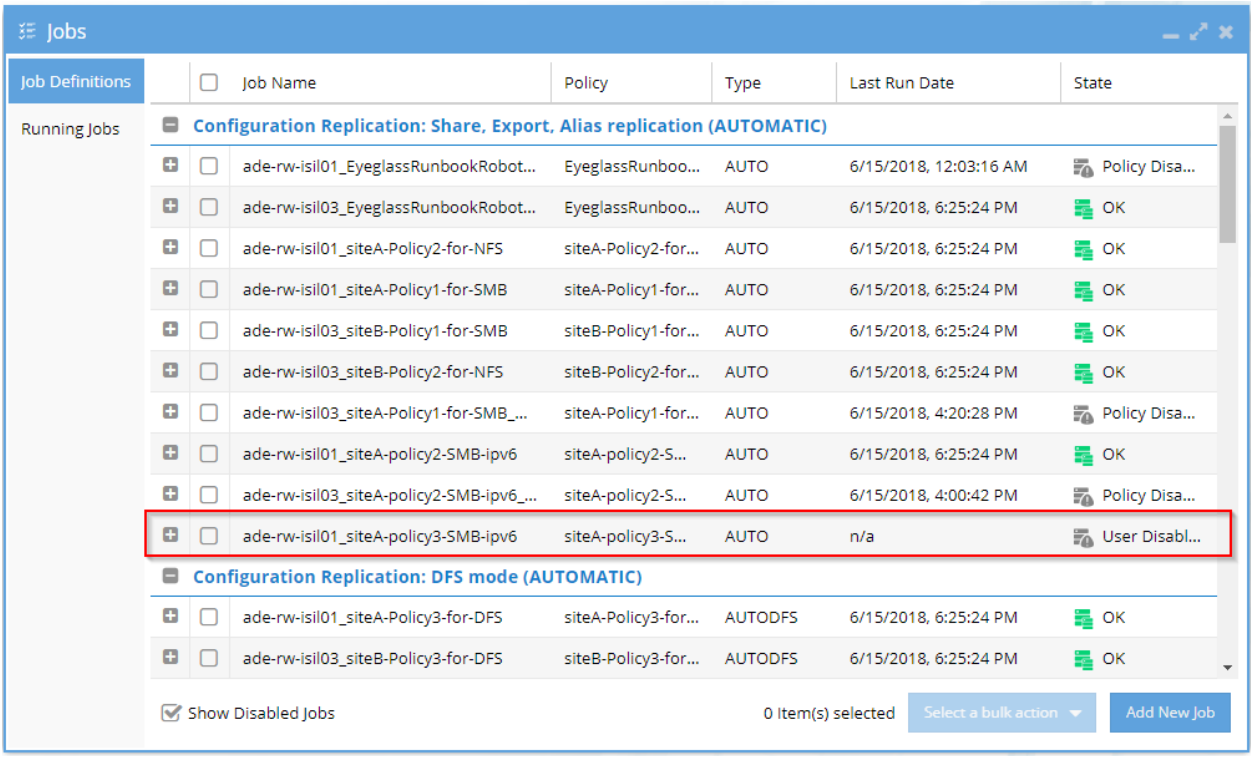
Home Top

This section covers requirements for a supported IPv6 configuration with Eyeglass DR edition.

Requirements

1. Dedicated management pool using ipv4 to add clusters to Eyeglass.
2. Dedicated SyncIQ replication pool using ipv4 for all policies to be failed over.
    a. Target host property must be either SSIP of remote cluster or SmartConnect FQDN that MUST resolve to IPv4 ip address.
3. SyncIQ policies using target host property of SSIP of remote cluster or FQDN SmartConnect that resolves to an ipv4 address used to validate cluster replication.

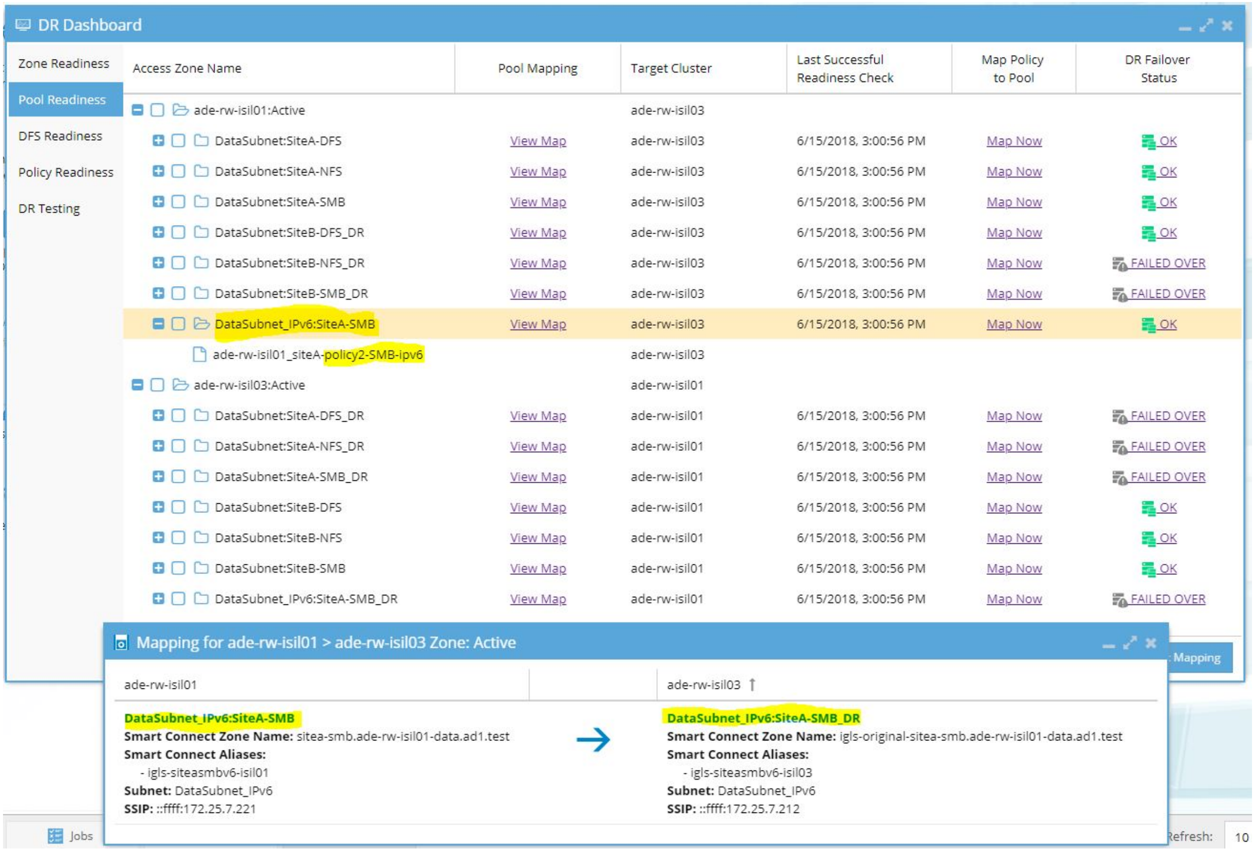
Examples of UI screens once configured as a reference:



	Job Name	Policy	Type	Last Run Date	State
Configuration Replication: Share, Export, Alias replication (AUTOMATIC)					
□	ade-rw-isil01_EyeglassRunbookRobot...	EyeglassRunboo...	AUTO	6/15/2018, 12:03:16 AM	Policy Disa...
□	ade-rw-isil03_EyeglassRunbookRobot...	EyeglassRunboo...	AUTO	6/15/2018, 6:25:24 PM	OK
□	ade-rw-isil01_siteA-Policy2-for-NFS	siteA-Policy2-for...	AUTO	6/15/2018, 6:25:24 PM	OK
□	ade-rw-isil01_siteA-Policy1-for-SMB	siteA-Policy1-for...	AUTO	6/15/2018, 6:25:24 PM	OK
□	ade-rw-isil03_siteB-Policy1-for-SMB	siteB-Policy1-for...	AUTO	6/15/2018, 6:25:24 PM	OK
□	ade-rw-isil03_siteB-Policy2-for-NFS	siteB-Policy2-for...	AUTO	6/15/2018, 6:25:24 PM	OK
□	ade-rw-isil03_siteA-Policy1-for-SMB_...	siteA-Policy1-for...	AUTO	6/15/2018, 4:20:28 PM	Policy Disa...
□	ade-rw-isil01_siteA-policy2-SMB-ipv6	siteA-policy2-S...	AUTO	6/15/2018, 6:25:24 PM	OK
□	ade-rw-isil03_siteA-policy2-SMB-ipv6_...	siteA-policy2-S...	AUTO	6/15/2018, 4:00:42 PM	Policy Disa...
□	ade-rw-isil01_siteA-policy3-SMB-ipv6	siteA-policy3-S...	AUTO	n/a	User Disabl...
Configuration Replication: DFS mode (AUTOMATIC)					
□	ade-rw-isil01_siteA-Policy3-DFS	siteA-Policy3-for...	AUTODFS	6/15/2018, 6:25:24 PM	OK
□	ade-rw-isil03_siteB-Policy3-for-DFS	siteB-Policy3-for...	AUTODFS	6/15/2018, 6:25:24 PM	OK

☑ Show Disabled Jobs

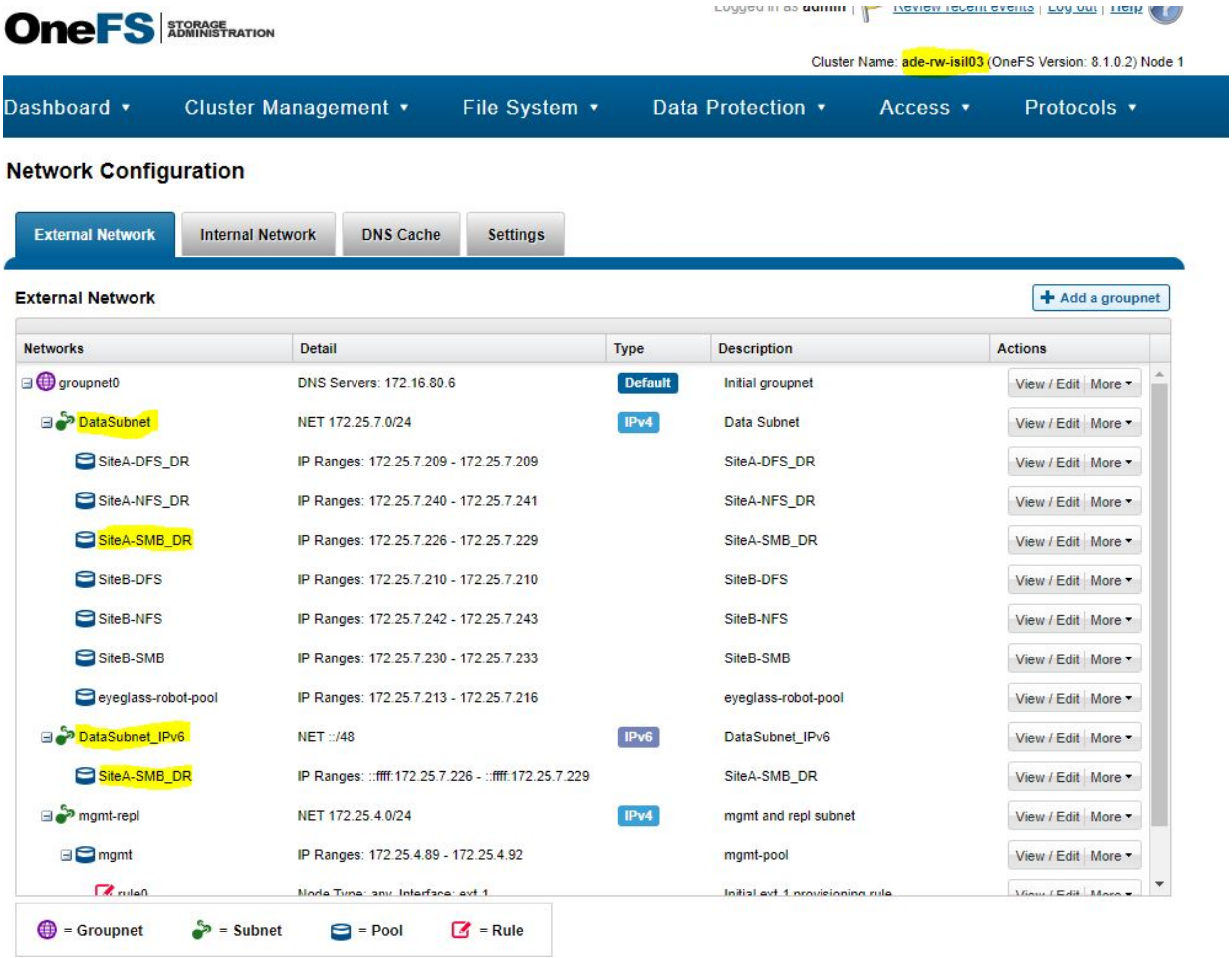
0 Item(s) selected



Access Zone Name	Pool Mapping	Target Cluster	Last Successful Readiness Check	Map Policy to Pool	DR Failover Status
ade-rw-isil01:Active		ade-rw-isil03			
DataSubnet:SiteA-DFS	View Map	ade-rw-isil03	6/15/2018, 3:00:56 PM	Map Now	OK
DataSubnet:SiteA-NFS	View Map	ade-rw-isil03	6/15/2018, 3:00:56 PM	Map Now	OK
DataSubnet:SiteA-SMB	View Map	ade-rw-isil03	6/15/2018, 3:00:56 PM	Map Now	OK
DataSubnet:SiteB-DFS_DR	View Map	ade-rw-isil03	6/15/2018, 3:00:56 PM	Map Now	OK
DataSubnet:SiteB-NFS_DR	View Map	ade-rw-isil03	6/15/2018, 3:00:56 PM	Map Now	FAILED OVER
DataSubnet:SiteB-SMB_DR	View Map	ade-rw-isil03	6/15/2018, 3:00:56 PM	Map Now	FAILED OVER
DataSubnet_IPv6:SiteA-SMB	View Map	ade-rw-isil03	6/15/2018, 3:00:56 PM	Map Now	OK
ade-rw-isil01_siteA-policy2-SMB-ipv6		ade-rw-isil03			
ade-rw-isil03:Active		ade-rw-isil01			
DataSubnet:SiteA-DFS_DR	View Map	ade-rw-isil01	6/15/2018, 3:00:56 PM	Map Now	FAILED OVER
DataSubnet:SiteA-NFS_DR	View Map	ade-rw-isil01	6/15/2018, 3:00:56 PM	Map Now	FAILED OVER
DataSubnet:SiteA-SMB_DR	View Map	ade-rw-isil01	6/15/2018, 3:00:56 PM	Map Now	FAILED OVER
DataSubnet:SiteB-DFS	View Map	ade-rw-isil01	6/15/2018, 3:00:56 PM	Map Now	OK
DataSubnet:SiteB-NFS	View Map	ade-rw-isil01	6/15/2018, 3:00:56 PM	Map Now	OK
DataSubnet:SiteB-SMB	View Map	ade-rw-isil01	6/15/2018, 3:00:56 PM	Map Now	OK
DataSubnet_IPv6:SiteA-SMB_DR	View Map	ade-rw-isil01	6/15/2018, 3:00:56 PM	Map Now	FAILED OVER

Mapping for ade-rw-isil01 > ade-rw-isil03 Zone: Active

ade-rw-isil01		ade-rw-isil03
DataSubnet_IPv6:SiteA-SMB **Smart Connect Zone Name:** sitea-smb.ade-rw-isil01-data.ad1.test **Smart Connect Aliases:** - igls-siteasmbv6-isil01 **Subnet:** DataSubnet_IPv6 **SSIP:** ::ffff:172.25.7.221	→	**DataSubnet_IPv6:SiteA-SMB_DR** **Smart Connect Zone Name:** igls-original-sitea-smb.ade-rw-isil01-data.ad1.test **Smart Connect Aliases:** - igls-siteasmbv6-isil03 **Subnet:** DataSubnet_IPv6 **SSIP:** ::ffff:172.25.7.212



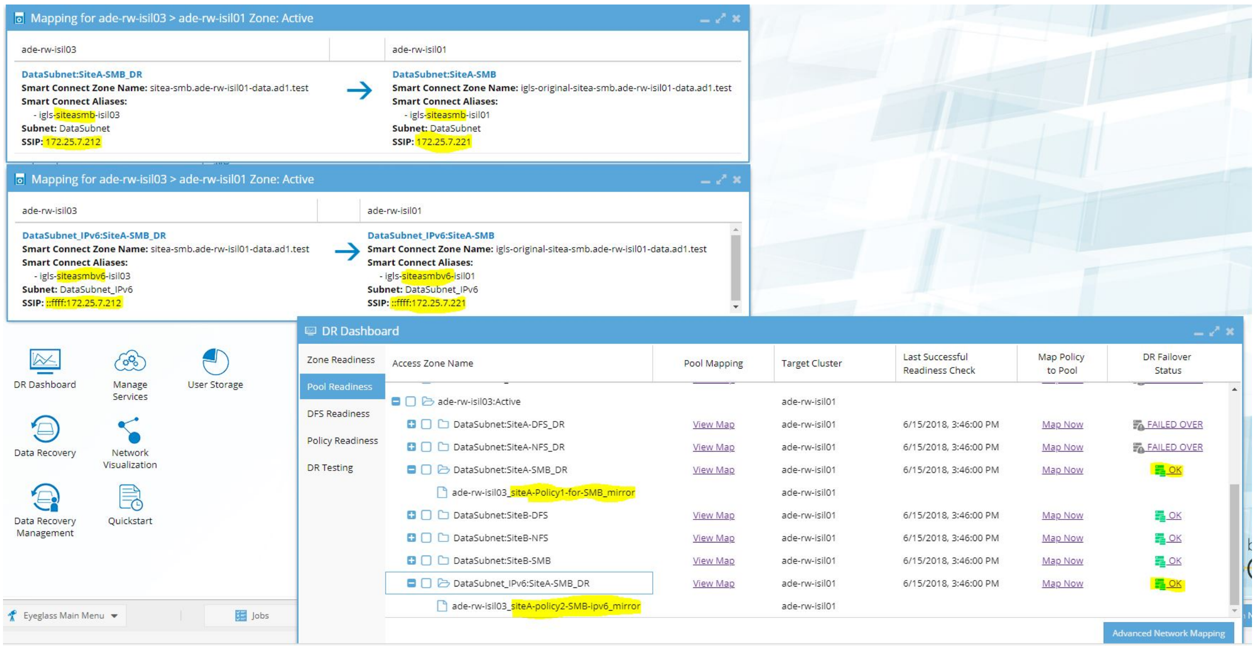
Cluster Name: ade-rw-isil03 (OneFS Version: 8.1.0.2) Node 1

Network Configuration

External Network

Networks	Detail	Type	Description	Actions
⊟ groupnet0	DNS Servers: 172.16.80.6	Default	Initial groupnet	View / Edit More ▾
⊟ DataSubnet	NET 172.25.7.0/24	IPv4	Data Subnet	View / Edit More ▾
SiteA-DFS_DR	IP Ranges: 172.25.7.209 - 172.25.7.209		SiteA-DFS_DR	View / Edit More ▾
SiteA-NFS_DR	IP Ranges: 172.25.7.240 - 172.25.7.241		SiteA-NFS_DR	View / Edit More ▾
SiteA-SMB_DR	IP Ranges: 172.25.7.226 - 172.25.7.229		SiteA-SMB_DR	View / Edit More ▾
SiteB-DFS	IP Ranges: 172.25.7.210 - 172.25.7.210		SiteB-DFS	View / Edit More ▾
SiteB-NFS	IP Ranges: 172.25.7.242 - 172.25.7.243		SiteB-NFS	View / Edit More ▾
SiteB-SMB	IP Ranges: 172.25.7.230 - 172.25.7.233		SiteB-SMB	View / Edit More ▾
eyeglass-robot-pool	IP Ranges: 172.25.7.213 - 172.25.7.216		eyeglass-robot-pool	View / Edit More ▾
⊟ DataSubnet_IPv6	NET ::/48	IPv6	DataSubnet_IPv6	View / Edit More ▾
SiteA-SMB_DR	IP Ranges: ::ffff:172.25.7.226 - ::ffff:172.25.7.229		SiteA-SMB_DR	View / Edit More ▾
⊟ mgmt-repl	NET 172.25.4.0/24	IPv4	mgmt and repl subnet	View / Edit More ▾
⊟ mgmt	IP Ranges: 172.25.4.89 - 172.25.4.92		mgmt-pool	View / Edit More ▾
rule0	Node Type: any, Interface: ext-1		Initial ext-1 provisioning rule	View / Edit More ▾

= Groupnet = Subnet = Pool = Rule



Mapping for ade-rw-isil03 > ade-rw-isil01 Zone: Active

ade-rw-isil03

DataSubnet:SiteA-SMB_DR
Smart Connect Zone Name: sitea-smb.ade-rw-isil01-data.ad1.test
Smart Connect Aliases:
- igls-siteasmb-isil03
Subnet: DataSubnet
SSIP: 172.25.7.212

→

ade-rw-isil01

DataSubnet:SiteA-SMB
Smart Connect Zone Name: igls-original-sitea-smb.ade-rw-isil01-data.ad1.test
Smart Connect Aliases:
- igls-siteasmb-isil01
Subnet: DataSubnet
SSIP: 172.25.7.221

Mapping for ade-rw-isil03 > ade-rw-isil01 Zone: Active

ade-rw-isil03

DataSubnet_IPv6:SiteA-SMB_DR
Smart Connect Zone Name: sitea-smb.ade-rw-isil01-data.ad1.test
Smart Connect Aliases:
- igls-siteasmbv6-isil03
Subnet: DataSubnet_IPv6
SSIP: ::ffff:172.25.7.212

→

ade-rw-isil01

DataSubnet_IPv6:SiteA-SMB
Smart Connect Zone Name: igls-original-sitea-smb.ade-rw-isil01-data.ad1.test
Smart Connect Aliases:
- igls-siteasmbv6-isil01
Subnet: DataSubnet_IPv6
SSIP: ::ffff:172.25.7.221

DR Dashboard

Access Zone Name	Pool Mapping	Target Cluster	Last Successful Readiness Check	Map Policy to Pool	DR Failover Status
⊟ □ ade-rw-isil03:Active		ade-rw-isil01			
⊞ □ DataSubnet:SiteA-DFS_DR	View Map	ade-rw-isil01	6/15/2018, 3:46:00 PM	Map Now	FAILED OVER
⊞ □ DataSubnet:SiteA-NFS_DR	View Map	ade-rw-isil01	6/15/2018, 3:46:00 PM	Map Now	FAILED OVER
⊟ □ DataSubnet:SiteA-SMB_DR	View Map	ade-rw-isil01	6/15/2018, 3:46:00 PM	Map Now	OK
ade-rw-isil03_siteA-Policy1-for-SMB_mirror		ade-rw-isil01			
⊞ □ DataSubnet:SiteB-DFS	View Map	ade-rw-isil01	6/15/2018, 3:46:00 PM	Map Now	OK
⊞ □ DataSubnet:SiteB-NFS	View Map	ade-rw-isil01	6/15/2018, 3:46:00 PM	Map Now	OK
⊞ □ DataSubnet:SiteB-SMB	View Map	ade-rw-isil01	6/15/2018, 3:46:00 PM	Map Now	OK
⊟ □ DataSubnet_IPv6:SiteA-SMB_DR	View Map	ade-rw-isil01	6/15/2018, 3:46:00 PM	Map Now	OK
ade-rw-isil03_siteA-policy2-SMB-ipv6_mirror		ade-rw-isil01			

1.19. Failover Advanced mode Configuration - Parallel thread and failover jobs

Home Top

Failover Advanced mode Configuration - Parallel thread , failover jobs & Concurrent Failovers Overview

These configurations are aimed at customers that have greater than 50 policies for business reasons and require faster failover option to maintain SLA on data recovery.

3 features exist:

1. **Parallel threads** - allows make writable and resync prep to operate in parallel up to thread limit of 10. This means 10 policies will be executed at a time for all SyncIQ steps, and Eyeglass will ensure that at least 10 policies are executing at a time throughout the failover process across all failover jobs.

2. **Parallel Jobs -** used to allow more active jobs to share threads for failover. This value and the threads value should be set to the same values. It defaults to 10 jobs.
3. **Concurrent Failovers** - A default of 5 is configured but can be increased with the parameters above to increase the number of active failover jobs. In a multi tenant scenario this my be required when users are able to submit failover jobs.

Parallel Failover Job and Concurrent Failover Configuration

This feature allows multiple failover jobs of any type to be failed over in parallel . This means multiple failovers can be running at the same time. This feature still has a 10 thread limit for all failover jobs that are shared across all jobs. This can be combined with the parallel threads feature to increase each failover jobs parallelization. **Testing this in advance of a failover is mandatory step. 3 different values must be changed to increase the parallel jobs, threads and concurrent failover limits.**   NOTE: Do NOT start more than 4 concurrent failovers with releases < 2.5.6. A failover job can be any type of failover with any number of policies in each failover job.

How to increase Fast Failover parallel threads, increase Failover jobs and concurrent failover limit

These options default to 10 failover jobs and 10 threads in a pool. This can be increased in release 2.5.6 which has been tested to 50 failover jobs and 50 threads. It is NOT recommended to increase beyond these limits.   The default for concurrent failovers is 5 but can be increased. See steps below.

1. Login via ssh as admin to Eyeglass.
2. sudo -s
3. Enter admin password to become root user.
4. Type: **nano /opt/superna/sca/data/parallelTaskLimits.json**
    a. To increase to 20 failover jobs and 20 threads change the values below to 20 and 20. **NOTE: increasing the job count requires increasing the thread count to the same number.**
    b. {"parallelJobs":20,"totalParallelTasks":20}
    c. Use the arrow keys to move, and delete key to change the values.
    d. Then to save and exit press CTRL+x, answer Y to save the changes .
5. To change the default concurrent failover limit. This is required if the parallel jobs count is increased or if 5 concurrent fail overs is not enough.
    a. Type: **nano /opt/superna/sca/data/system.xml .**
    b. Add a tag inside the <process> tag .
    c. Add a new line and paste this tag into the file and change the yellow value. This has been tested to 50 concurrent failovers and it is NOT recommended to change to a higher value. **NOTE: Do not increase the value above the parallel jobs value.**

d. <max_concurrent_failovers>5</max_concurrent_failovers>
.

e. Then to save and exit press CTRL+x answer Y to save the changes .

5. After making changes above the SCA process must be restarted:

f. systemctl restart sca

6. The feature is now enabled after the restart command above.
7. To submit parallel Access Zone, policy, DFS or IP Pool jobs use the DR Assistant to start a failover job.
8. Close DR Assistant, re-open it and start another failover.
9. Repeat, the above step to submit more parallel failover jobs.
10. Monitor all failovers from DR Assistant running failover tab.
11. **NOTE: Cluster resources may be exhausted and testing is mandatory prior to attempting a very large number of failovers.**

Parallel threads for Failover Mode Configuration (Legacy Mode)

This mode switches to parallel policy with up to 10 threads for make all steps. **This defaults to enabled in all current releases. No need to change unless directed by support.**

Key differences between default sequential and parallel mode:

1. For 8.x clusters, 50 policies can run at a time and Eyeglass will use a maximum of 10 threads allow 10 policy make writable or resync prep commands to be sent in at once. For 7.2 clusters

only 5 will execute and 5 are queued. If one policy completes, another policy is started with the goal of keeping maximum number queued at all times.

2. Testing has shown 3x to 4x improvements in overall time to complete make writable. Results in production may vary.

How to enable Fast Failover parallel threads

This runs steps with multi threads, and runs steps in parallel . NOTE: 2.5.4 and later is enabled by default.

8. igls adv failovermode set --parallel=true .
9. Done. The change affects all failover jobs.
10. Disable with:
    h. igls adv failovermode set --parallel=false .