Failover Best Practices Webinar

Superna Eyeglass DR Edition

superna®

Agenda

1. Failover planning
2. Failover best practices
3. Failover log review and recovery
4. Questions eyeglass@superna.net or live chat (requires youtube login)
5. Slides will be posted to https://www.supernaeyeglass.com/downloads
6. Video will be online Webinar Recording

Failover planning

1. Planning guide Review
   a. Review planning guide links for a successful failover
   b. Get a Failover Readiness Assessment
      i. Notify support 7 days prior planned event by opening a case and submit support logs and provide date and time (time zone)
      ii. Get review from support
      iii. Rectify any identified issues
      iv. Submit logs day before failover
      v. Get final assessment from support
2. Implement Runbook robot and practise failover hands on
3. Sign up for Free hands-on training failover labs

Failover best practices

1. Planning guide Review
    a. Eyeglass code level support statement
    b. Failback Domain mark?
        i. How to run a domain mark - demo
        ii. How to check domain mark has been run - demo
    c. Eyeglass timeout explanation
        i. Run policy, make writeable, Resync-prep
    d. Duplicate SyncIQ snapshots?
        i. How to check on source and target clusters - demo
    e. Dry run with Runbook robot
        i. Demo failover test
    f. SyncIQ performance estimate RPO reports
        i. Demo report

Failover log review and recovery

1. Failover Steps (table)
2. Failover Demo
   a. Before you start a Failover (DR Dashboard)
   b. Start Failover
   c. Monitor Failover
   d. Understanding Failover logs
3. When something goes wrong
   a. Recovery Guide

Common Questions DFS mode

1. What are the top issues with DFS failover?
   a. DFS folder targets are set up once and both referral paths are enabled? **yes correct, no need to enable or disable referral paths.**
   b. What If exports exist under the synciq policy protecting DFS protected SMB shares? **Access zone + DFS mode failover is needed for the exports to failover the smartconnect names used to mount the exports. DFS mode can be integrated into the access zone and failover DFS and the access zone at the same time.**

Common Questions DFS mode

1. Can one SyncIQ policy protect more than one DFS folder? **Yes many DFS folders can be protected with a single synciq policy as long as the shares created match the policy path. The DFS folders will all failover at the same time.**
2. Can single shares be failed over with DFS mode? Y**es but within limits of Eyeglass DR Design best practise of 20-25 polices for efficient failover. Isilon supports 100 policies but only 5 run at a time on onefs 7. This changes to 1000 policies with 50 run at the same time. Fewer policies fails over faster than more policies. So keep this in mind.**
3. Can I failover more than one DFS policy at the same time? **yes just select more than one to submit a single failover job**

Common Questions Access Zone Failover

1. What happens if not all policies succeed to failover? Does any rollback exist to source cluster? **Eyeglass must have at least 1 policy succeed the make write SyncIQ step, no no policies pass this step, then eyeglass will revert the smartconnect failover and the SPN failover back to the source cluster. This ensures users can access writeable data again and the failover is not aborted.**
2. Does Active Directory Service Principal Names (SPN) failover step block a failover from completing? **No , if this step fails, failover will still continue but manual SPN failover will be required with ADSI edit tool in AD using the failover log to get the list of SPN’s that need to failover from one cluster computer account to the target cluster computer account in AD.**
3. What post failover steps should be done to verify successful failover?

Common Questions Access Zone Failover

1. What post failover steps should be done to verify successful failover? **Use nslookup to check each smartconnect name involved in the failover (use failover log for the list) and test each name to make sure the target cluster responds.   Then test mount shares from a client workstation to verify authentication works as expected. NOTE: SPN's are required for kerberos authentication**

General Failover Question

1. How long does it take to failover? **speed depends on how much unsynced data exists at the time of failover and how many policies are failing over fewer is faster.**
2. In an uncontrolled failover Is DNS a concern if the source cluster is still reachable? **Yes, if the cluster still answers DNS queries the smartconnect name has not been failed over or renamed. This means the SSIP interface should be disabled to prevent DNS resolving to the cluster you failed away from.**
3. How are SPN's deleted during failover if the source cluster is down? **SPN operations for delete and create during failover use the target cluster to proxy to AD computer objects for the source and target cluster. This ensures that the source cluster is not required to automate failover of SPN's in a real DR event. This is why cross AD delegation is required in AD is required. NOTE: It is best practice to always have a domain controller at the DR site for this reason.**