Table of Contents

1. Technical Advisories

Home Top

- Technical Advisory #15 - cross site scripting CVE on Isilon
- Technical Advisory #16 - Config Sync may skip steps on Error
- Technical Advisory #17 - Isilon CSRF Authentication is not compatible with Smartconnect and API services Affects Eyeglass releases 2.5.3 and later
- Technical Advisory #18 - Ransomware Defender ECA cluster without Internet access potential for false positives
- Technical Advisory #19 - SMB Data Integrity corner case can leave Deny permission on some or all shares

Technical Advisory #1

For customers where the total number of objects (SMB Shares, NFS Exports, NFS Alias, Quotas) being managed by Superna Eyeglass exceeds 10,000, tasks being performed against the cluster for a large number of objects (such as creating quotas during a failover) may overwhelm the cluster such that not all tasks are completed. An adjustment to the Superna Eyeglass parallel task limit is required. Contact support.superna.net for assistance in updating Eyeglass.

Technical Advisory #2

In some environments, the memory allocated for the Superna Eyeglass database is not sufficient. In this case Superna Eyeglass no

longer functions and the Superna Eyeglass web page windows appear empty. If you experience this issue, contact support.superna.net for assistance in updating Eyeglass to adjust the memory allocated to the database.

Update April 6, 2016: This issue has been addressed in Eyeglass 1.5.1

Technical Advisory #3 - reissued April 20

An issue in Eyeglass Release 1.5.0 and 1.5.1 results in duplicate exports being created on the target cluster under certain conditions such as poor connectivity between Eyeglass and the Isilon cluster. This issue will be addressed in Eyeglass 1.5.2. This issue does not exist in Eyeglass 1.4.8. Eyeglass installations using exports should not upgrade to Eyeglass 1.5.0 or 1.5.1.

Update April 25, 2016: This issue has been addressed in Eyeglass 1.5.2

Technical Advisory #4 - End of Support for 1.2, 1.3, 1.4 and 1.4.x Releases

All customers running the above releases should upgrade to the latest release using upgrade guide located here. Numerous failover and performance improvements exist in the latest release with all new cases requiring an upgrade.

Technical Advisory #5 - Incomplete response from Isilon PAPI may result in deletion of Configuration Objects

Please be advised that we have observed instances where the Isilon Cluster PAPI used by Eyeglass to collect information becomes unresponsive such that Eyeglass requests for configuration objects are unanswered (for example 503 Service Unavailable). This results in empty Eyeglass inventory for objects that are not retrieved.

Should this happen during scheduled Eyeglass Configuration Replication, it may result in deletion of configuration objects (such as NFS export or SMB shares) from the target cluster. Subsequent cycle with correct response will resolve this situation by creating the configuration objects again.

Should this happen during Eyeglass assisted failover, it may result in deletion of missing configuration objects from both clusters as after the failover the target cluster with missing objects becomes the master active cluster.

The Eyeglass next release will contain defensive code to guard against deletion of configuration objects when the Isilon PAPI response is incomplete. If you are planning a controlled failover, we ask that you wait and upgrade to 1.5.4 release that blocks Isilon PAPI errors from impacting a successful failover.
Update May 13, 2016: This issue has been addressed in Eyeglass 1.5.3

Technical Advisory #6 - Set SyncIQ policies to manual schedule or longer schedule with 1.6 release or risk scheduled jobs running during failover and failing overall Eyeglass failover steps

Following EMC best practices to set SyncIQ policies to manual before any failover KB Article as reference "NOTE: A sync job and failover job cannot run simultaneously by design and will cause the failover attempt to fail. To avoid this condition, set all policies to manual."

Issue: Failover behavior in 1.6 was changed that exposes the window where scheduled policies do not have their scheduled removed in time to prevent them from running in 1.6 release.

This has been addressed in 1.6.3 by having schedules removed and cached at the beginning of the failover and reapplied at the end of the

failover.

Technical Advisory #7 - OneFS 8 BMC firmware bug API call

Please be advised that we have found new case where the BMC firmware bug API call is made under Eyeglass1.6.1 code. This issue has been observed to manifest itself after several days in operation and affects Eyeglass installations where both Isilon clusters are running OneFS 8. We have switched to a ssh call previously reviewed by EMC and confirmed to not query any BMC APIs in 1.6.x but a left over call in some cases still called this unused API in 1.6.1.

This has been addressed in the 1.6.2 patch such that the BMC firmware bug API is removed. We recommend this new patch release for all Eyeglass patch deployments managing OneFS 8 clusters.

Technical Advisory #8 - End of Support for 1.5.4 Release

Effective November 1st, 2016 release 1.5.4, All customers running the above releases should upgrade to the latest release using upgrade guide located here. Numerous failover and performance improvements exist in the latest release with all new cases with this release requiring an upgrade as first resolution step.

Technical Advisory #9 - Open files Detection on Isilon

A OneFS issue with open file detection used by Eyeglass in the DR assistant to show open files, only lists files open in system access zone. Other access zones that have open files are not returned by the ISI open files for array command. This means customers can not rely on the open file list in DR assistant to determine open files in none system access zones. No known fix available in any OneFS at this time.

As of release 1.8.1 this feature has been removed with no update or planned availability of a fixed API from Dell EMC.

Technical Advisory #10 - Uncontrolled Failover Issue when Isilon Cluster added to Eyeglass with FQDN

Applies to release < 1.8.1 For the case where Isilon clusters have been added to Eyeglass using FQDN, uncontrolled failover for case where source cluster is not reachable does not start and gives the error ""Error performing zone failover: Cannot find associated source network element for zone".

This issue is addressed in a 1.8.1 patch. Eyeglass installations using FQDN to add clusters must upgrade to this patch once available.

Workaround:
Before an uncontrolled failover where the source cluster is not available, edit the /etc/hosts file on the Eyeglass appliance following the steps below:

1. ssh to the Eyeglass appliance.
2. Assume root user - when prompted for password use the admin user password
sudo su -
3. edit the /etc/hosts file
vi /etc/hosts
4. insert a line below the last line for the FQDN of your source cluster. The syntax is:

Syntax: IP-Address Full-Qualified-Hostname Short-Hostname
Example: 172.16.89.45 sourcecluster.prod.superna.net source cluster

where
IP-Address is a node IP from the subnet pool where the source cluster FQDN is provisioned
Full-Qualified-Hostname is the FQDN that was used to add the Source cluster to Eyeglass

Technical Advisory #11 - End of Support for 1.6.x

Release Notice as of May 31, 2017

Effective July 30th, 2017 release 1.6.x, All customers running the above releases should upgrade to the latest release using upgrade guide located here. Numerous failover and performance improvements exist in the latest release with all new opened cases with this release will be asked to upgrade before issues are addressed as a first resolution step.

Technical Advisory #12 – DR Dashboard/Zone Readiness display issue for Failed Over Status – no loss of failover functionality

Applies to Release 1.9, 1.9.1. The DR Dashboard Zone Readiness status may not show the Failed Over status for the Cluster which is currently inactive. This does not affect the ability to failover from the active cluster nor is it possible to initiate a failover from the inactive cluster.

Workaround: Policy Readiness and DFS Readiness correctly display the FAILED OVER Failover Status
To determine which cluster Eyeglass considers active:
1. Login the the Eyeglass web page.
2. Open the DR Dashboard.
3. Use the Policy Readiness or DFS Readiness view to determine which cluster is active for a specific policy.
4. Then the Zone Readiness vies can be used to confirm which

Access Zone that policy falls under by opening the DR Failover Status window for an Access Zone and opening the OneFS SyncIQ Readiness folder. Here all of the SyncIQ Policies that are associated with Access Zone are listed.

This issue has been addressed in Release 1.9.2.

Technical Advisory #13 - Spectra/Meltdown Available in Appliance 2.5.x

Upgrade path, follow this guide.

Note appliance defaults to weekly automatic critical patches and security updates if Internet connection is allowed to the appliance. If you would like email notification of OS updates follow this link and register. http://lists.suse.com/mailman/listinfo/sle-security-updates.

The current Open SUSE status is explained here on this link https://www.suse.com/c/suse-addresses-meltdown-spectre-vulnerabilities/. The Open SUSE update will be posted to the mailing list once available.

CVE's below Available on appliances with 42.3 Open Suse

https://www.suse.com/security/cve/CVE-2017-5753/
https://www.suse.com/security/cve/CVE-2017-5715/

https://www.suse.com/security/cve/CVE-2017-5754/

Technical Advisory #14 - EOS 1.9.x Releases

EOS for Releases 1.9.x March 20, 2018

Technical Advisory #15 **- cross site scripting CVE on Isilon**

cross site scripting vulnerabilities in CVE-2017-8024 requires a patch from Isilon available for certain Isilon release streams. This patch also requires disabling HTTP authentication which will affect Eyeglass directly. Eyeglass will not able to login to perform any DR functions. An updated version 2.5.3 will include alternate authentication solution for Isilon to allow this complete CVE procedures to be applied. Partial implementation is possible by applying the path to Isilon without disabling the HTTP authentication on the cluster

Technical Advisory #16 **- Config Sync may skip steps on Error**

This issue is present in > 1.9.4 and can result in SMB shares and export not synced to DR if an object cannot be synced remaining objects are not attempted.

Resolution: Clear the error and all unsync changes will be synced successfully. A work around exists and requires a support case opened for instructions. This has been fixed in release 2.5.3 once it is GA. **We will also be releasing a patch to 2.5.2 that corrects this issue. The patch can be downloaded from the download page on located on the support site and will require download of the 2.5.2 offline installer and upgrading from 2.5.2 to latest build of 2.5.2 for an existing installation.**

Technical Advisory #17 - **Isilon CSRF Authentication is not compatible with Smartconnect and API services**

Affects Eyeglass releases 2.5.3 and later

NOTE: Only 2.5.3 and later supports a cluster with CSRF enabled.

Issue: Isilon does NOT support multi node cluster aware CSRF sessions for authentication and is NOT compatible with Smartconnect FQDN method #1. This is known limitation of Isilon CSRF implementation.

Impact: None. SSIP is fully supported with many deployments using this method. The load balancing of FQDN has some potential to expose issues on various nodes in the cluster and a minor performance improvement for large object customers.

Resolution: To support **CSRF** on Isilon requires settings that disable basic HTTPS authentication and uses session tokens for authentication. This requires Eyeglass to use the SSIP in the management access zone due to above **Isilon limitation**.

1. If you have added clusters to Eyeglass with FQDN (How to check: Open Inventory Icon, right click the cluster and select Edit to determine how Eyeglass was added).
2. Open Jobs icon, record all policy states in all sections of this window. You will need to re-enable these policies and enable DFS mode based on your records from this step.
3. Delete the cluster (right click menu on the cluster name, chose the delete option)
    a. Repeat the delete for each cluster listed in the inventory icon
4. Re-add the cluster with the SSIP in the system access zone, enter eyeglass service account name used before and password
    a. Repeat for each cluster Note: more than one cluster can be added before submitting the inventory job
5. Open Jobs Icon, then running jobs tab, wait for initial inventory to complete
6. Once complete click on job definition tab and enable all jobs based on the recorded configurations from the step above.
    1. You may also need to enable DFS mode (How to enable DFS mode)
    2. Use the bulk actions menu to enable the jobs (How to enable jobs)
7. Then wait 5 minutes and verify all jobs are green
8. If any errors, please open a support case.

Technical Advisory #18 - **Ransomware Defender ECA cluster without Internet access potential for false positives**

Issue: In release 2.5.3 of Ransomware Defender a threat detector will sometimes match files that should not be considered Ransomware only when the ECA cluster does not have Internet access.

Impact: False positive detection of some users depending on the IO

pattern.

Resolution: A new build of 2.5.3 with number 18257 is available for download now that addresses this issue, without any requirement to connect ECA clusters to the Internet.

1. Instructions to apply patch
2. Open a support case and request assistance to apply the patch.

Technical Advisory #19 - SMB Data Integrity corner case can leave Deny permission on some or all shares

Issue: Normal configuration sync runs every 5 minutes and under some conditions may detect the Deny everyone permission used by the Data Integrity DR Assistant failover feature and sync it to the DR cluster before the deny is removed by the failover process. This is a corner case that has rare.

Impact: After a failover some SMB shares may be left with a deny everyone permission blocking access to users.

Solution: Manually remove the Deny Everyone permission on the affected shares.

Solution to Use SMB Data Integrity Feature:

1. Disable the config Sync Job before the failover

    1. using SSH to the Eyeglass appliance run:
    2. igls admin schedules set --id Replication --enabled false
2. After the failover is complete
    1. igls admin schedules set --id Replication --enabled true

Resolution: A new build of 2.5.4 with number 18275 has been released to address this issue.