Table of Contents

1. How to Validate AD Cluster Delegation is Ready for Failover and failback of SPNs published

Home Top

Technical Note

Abstract:

This technical note provides test methodologies to AD delegation is ready for failover under four scenarios:

- **PRIMARY Cluster SELF SPN Delegation**
- **PRIMARY Cluster CROSS SPN Delegation**
- **DR Cluster SELF SPN Delegation**
- **DR Cluster CROSS SPN Delegation**

Use this procedure to validate AD delegation is done correctly. A common mistake is the computer account delegation.

Understanding how failover works

Failover process requires the target cluster to have AD permissions to manage SPN(s) on the source cluster AD machine account. The delegation guide sets this up for each cluster machine account to failover in either direction.
If not setup correctly the following issues are frequently seen:

- Ldap constraint violation
- Ldap permissions error

Locate AD PowerScale machine Account Name

Log into you cluster as 'root' and run the following CLI command to locate machine account name:

 # isi auth ads list -v

```
ishot-8-1# isi auth ads list -v
                    Name: AD2.TEST
        Machine Account: ISHOT-8$
         Authentication: No
               Groupnet: groupnet0
```

For OneFS 8.x

Section 1 - All Steps performed on PRIMARY CLUSTER [For OneFS 8.x.x.x]

1A - SELF test

- CREATE SPN for PRIMARY Cluster [oneFS 8.x]

For this test, you will need 2 OneFS 8.x.x.x clusters connected to same AD.

Step 1. Log in to your PRIMARY cluster using "eyeglass" user and issue the following command

"**whoami**"

```
ishot-8-1% whoami
eyeglass
```

Step 2. Add a SPN by using the following command

"**sudo isi_classic auth ads spn add --machinecreds --spn=HOST/superna.test.spn --domain=xxx**"

```
ishot-8-1# sudo isi_classic auth ads spn add --machinecreds --spn=HOST/superna.test.spn --domain=ad2.test
Successfully added SPN(s).
```

[--machinecred is needed to authenticate your cluster]
[--domain= Enter your Domain name]

Step 3. Check if SPN was created successfully.

"**sudo isi_classic auth ads spn list --machinecreds --domain=xxx**"

```
ishot-8-1# sudo isi_classic auth ads spn list --machinecreds --domain=ad2.test
SPNs registered for ISHOT-8$:
        HOST/superna.test.spn
```

[--machinecred is needed to authenticate your cluster]

[--domain= Enter your Domain name]

- DELETE SPN for PRIMARY Cluster [oneFS 8.x]

For this test, you will need OneFS 8.x.x.x clusters connected to same AD.

Step 1. Log in to your PRIMARY cluster using "eyeglass" user and issue the following command

"**whoami**"

```
ishot-8-1% whoami
eyeglass
```

Step 2. Delete the SPN from the same cluster by issuing the following command

"**sudo isi_classic auth ads spn delete --machinecreds --spn=HOST/superna.test.spn --domain=xxx**"

```
ishot-8-1# sudo isi_classic auth ads spn delete --machinecreds --spn=HOST/superna.test.spn --domain=ad2.test
Successfully deleted SPN(s).
```

[--machinecred is needed to authenticate your cluster]
[--domain= Enter your Domain name]

Step 3. Check if SPN was deleted successfully.

"**sudo isi_classic auth ads spn list --machinecreds --domain=xxx**"

```
ishot-8-1% sudo isi_classic auth ads spn list --machinecreds --domain=ad2.test
SPNs registered for ISHOT-8$:
```

[--machinecred is needed to authenticate your cluster]
[--domain= Enter your Domain name]

1B - CROSS test

- CREATE SPN for DR Cluster [oneFS 8.x]

For this test, you will need OneFS 8.x.x.x clusters connected to same AD.

Step 1. Log in to your PRIMARY cluster using "eyeglass" user and issue the following command

"**whoami**"

```
ishot-8-1% whoami
eyeglass
```

Step 2. Add SPN for DR cluster using PRIMARY cluster

"**sudo isi_classic auth ads spn add --machinecreds --account=xxx$ --spn=HOST/superna.test.spn --domain=xxx**"

```
ishot-8-1# sudo isi_classic auth ads spn add --machinecreds --account=ISCOLD-8$ --spn=HOST/superna.test.spn --domain=ad2.test
Successfully added SPN(s).
```

[--account= is the AD computer machine name that we are deleting SPN from. "$" sign is needed after the AD computer name.]
[--machinecred is needed to authenticate your cluster]
[--domain= Enter your Domain name]

Step 3. Check if SPN was created successfully

"sudo isi_classic auth ads spn list --machinecreds --account=xxx$ --domain=xxx"

```
ishot-8-1# sudo isi_classic auth ads spn list --machinecreds --account=ISCOLD-8$ --domain=ad2.test
SPNs registered for ISCOLD-8$:
        HOST/superna.test.spn
```

[--account= is the AD computer machine name that we are deleting SPN from. "$" sign is needed after the AD computer name.]
[--machinecred is needed to authenticate your cluster]
[--domain= Enter your Domain name]

- DELETE SPN for DR Cluster [oneFS 8.x]

For this test, you will need OneFS 8.x.x.x clusters connected to same AD.

Step 1. Log in to your PRIMARY cluster using "eyeglass" user and issue the following command

"whoami"

```
ishot-8-1% whoami
eyeglass
```

Step 2. Delete SPN for DR cluster using PRIMARY cluster

"sudo isi_classic auth ads spn delete --machinecreds --account=xxx$ --spn=HOST/superna.test.spn --domain=xxx"

```
ishot-8-1# sudo isi_classic auth ads spn delete --machinecreds --account=ISCOLD-8$ --spn=HOST/superna.test.spn --domain=ad2.test
Successfully deleted SPN(s).
```

[--account= is the AD computer machine name that we are deleting SPN from. "$" sign is needed after the AD computer name.]
[--machinecred is needed to authenticate your cluster]
[--domain= Enter your Domain name]

Step 3. Check if SPN was deleted successfully

"sudo isi_classic auth ads spn list --machinecreds --account=xxx$ --domain=xxx"

```
ishot-8-1% sudo isi_classic auth ads spn list --machinecreds --account=ISCOLD-8$ --domain=ad2.test
SPNs registered for ISCOLD-8$:
```

[--account= is the AD computer machine name that we are deleting SPN from. "$" sign is needed after the AD computer name.]
[--machinecred is needed to authenticate your cluster]
[--domain= Enter your Domain name]

Section 2 - All Steps performed on DR CLUSTER [For OneFS 8.x.x.x]

1A - SELF test

- CREATE SPN for DR Cluster [oneFS 8.x]

For this test, you will need OneFS 8.x.x.x clusters connected to same AD.

Step 1. Log in to your DR cluster using "eyeglass" user and issue the following command

"**whoami**"

```
ishot-8-1% whoami
eyeglass
```

Step 2. Add a SPN by using the following command

"**sudo isi_classic auth ads spn add --machinecreds --spn=HOST/superna.test.spn.domain.com --domain=xxx**"

```
ishot-8-1% sudo isi_classic auth ads spn add --machinecreds --spn=HOST/superna.test.spn.domain.com --domain=ad2.test
Successfully added SPN(s).
```

[--machinecred is needed to authenticate your cluster]

[--domain= Enter your Domain name]

Step 3. Check if SPN was created successfully.

"**sudo isi_classic auth ads spn list --machinecreds --domain=xxx**"

```
ishot-8-1% sudo isi_classic auth ads spn list --machinecreds --domain=ad2.test
SPNs registered for ISHOT-8$:
        HOST/superna.test.spn.domain.com
```

[--machinecred is needed to authenticate your cluster]

[--domain= Enter your Domain name]

- DELETE SPN for DR Cluster [oneFS 8.x]

For this test, you will need OneFS 8.x.x.x clusters connected to same AD.

Step 1. Log in to your DR cluster using "eyeglass" user and issue the following command

"**whoami**"

```
ishot-8-1% whoami
eyeglass
```

Step 2. Delete the SPN from the same cluster by issuing the following command

"**sudo isi_classic auth ads spn delete --machinecreds --spn=HOST/superna.test.spn --domain=xxx**"

```
iscold-8-1# sudo isi_classic auth ads spn delete --machinecreds --spn=HOST/superna.test.spn --domain=ad2.test
Successfully deleted SPN(s).
```

[--machinecred is needed to authenticate your cluster]

[--domain= Enter your Domain name]

Step 3. Check if SPN was deleted successfully.

"**sudo isi_classic auth ads spn list --machinecreds --domain=xxx**"

```
ishot-8-1% sudo isi_classic auth ads spn list --machinecreds --domain=ad2.test
SPNs registered for ISHOT-8$:
```

[--machinecred is needed to authenticate your cluster]

[--domain= Enter your Domain name]

1B - CROSS test

- CREATE SPN for PRIMARY Cluster [oneFS 8.x]

For this test, you will need OneFS 8.x.x.x clusters connected to same AD.

Step 1. Log in to your DR cluster using "eyeglass" user and issue the following command

"**whoami**"

```
ishot-8-1% whoami
eyeglass
```

Step 2. Add SPN for PRIMARY cluster using DR cluster

"**sudo isi_classic auth ads spn add --machinecreds --account=xxx$ --spn=HOST/superna.test.spn --domain=xxx**"

```
ishot-8-1% sudo isi_classic auth ads spn add --machinecreds --account=ISCOLD-8$ --spn=HOST/superna.test.spn.domain.com --domain=ad2.test
Successfully added SPN(s).
```

[--account= is the AD computer machine name that we are deleting SPN from. "$" sign is needed after the AD computer name.]
[--machinecred is needed to authenticate your cluster]
[--domain= Enter your Domain name]

Step 3. Check if SPN was created successfully

"**sudo isi_classic auth ads spn list --machinecreds --account=xxx$ --domain=xxx**"

```
ishot-8-1% sudo isi_classic auth ads spn list --machinecreds --account=ISCOLD-8$ --domain=ad2.test
SPNs registered for ISCOLD-8$:
        HOST/superna.test.spn.domain.com
```

[--account= is the AD computer machine name that we are deleting SPN from. "$" sign is needed after the AD computer name.]
[--machinecred is needed to authenticate your cluster]
[--domain= Enter your Domain name]

- DELETE SPN for PRIMARY Cluster [oneFS 8.x]

For this test, you will need OneFS 8.x.x.x clusters connected to same AD.

Step 1. Log in to your DR cluster using "eyeglass" user and issue the following command

"**whoami**"

```
ishot-8-1% whoami
eyeglass
```

Step 2. Delete SPN for PRIMARY cluster using DR cluster

"**sudo isi_classic auth ads spn delete --machinecreds --account=xxx$ --spn=HOST/superna.test.spn.domain.com --domain=xxx**"

```
ishot-8-1% sudo isi_classic auth ads spn delete --machinecreds --account=ISCOLD-8$ --spn=HOST/superna.test.spn.domain.com --domain=ad2.test
Successfully deleted SPN(s).
```

[--account= is the AD computer machine name that we are deleting SPN from. "$" sign is needed after the AD computer name.]
[--machinecred is needed to authenticate your cluster]
[--domain= Enter your Domain name]

Step 3. Check if SPN was deleted successfully

"**sudo isi_classic auth ads spn list --machinecreds --account=xxx$ --domain=xxx**"

```
ishot-8-1% sudo isi_classic auth ads spn list --machinecreds --account=ISCOLD-8$ --domain=ad2.test
SPNs registered for ISCOLD-8$:
```

[--account= is the AD computer machine name that we are deleting SPN from. "$" sign is needed after the AD computer name.]
[--machinecred is needed to authenticate your cluster]
[--domain= Enter your Domain name]

2. How To Healthcheck Eyeglass with 3rd party monitoring tools

Home Top

- Abstract:

How To Healthcheck Eyeglass with 3rd party monitoring tools

Technical Note

Abstract:

This technical note details how to setup healthcheck script for use with 3rd party monitoring applications to detect if Eyeglass process are operating normally

Overview

This solution can be used with 3rd party monitoring applications to detect if Eyeglass process are operating normally.
The key processes that should be monitored as running are

- Sca
- Scadb
- sera
- lighttpd
- iglsauth.service
- iglsservicebroker.service

Monitor these process with 3rd party monitoring tools.

The rest api can also be used to remotely collect alarms from Eyeglass, see the guide on how to retrieve alarms with an api token and curl builder tools. API Guide is here.

3. DR Manager Configuration Sync Errors and Resolutions

- Resolution:
- MESSAGE "AEC_NOT_FOUND", "message" : "Zone 'x' not found" For Eyeglass Configuration Replication Job
- Problem:
- Possible Cause for Missing Zone:
- Solution :

Message AEC_NOT_FOUND "Path 'X/Y/Z' Not Found: No Such File Or Directory" For Eyeglass Configuration Replication Job

Problem:

Eyeglass Configuration Replication Job fails with error AEC_NOT_FOUND "Path 'x/y/z' not found: No such file or directory". (Alarm code SCA0004)
This error is issued when the Eyeglass Configuration Replication job runs and attempts to replicate a share or export or quota when the associated directory does not exist on the target.

Resolution:

See below for the various reasons we see this error and their resolution (in bullets)
SyncQ Policy associated with the path has not been run and therefore the path does not exist on the target cluster

- Ensure the SyncIQ policy has recently run on the cluster.

The SMB Share or NFS Export path points to a path that does not exist on the Source cluster filesystem OR the share path does not match the path on the filesystem exactly (case-sensitive)

- Review the SMB Share or NFS Export path on the source cluster and copy it to the clipboard and then SSH to the Source cluster and run command: cd <pasted path>
- If the cd command fails then either the path does not exist or there is a mismatch in the case-sensitivity of the path

SyncIQ Policy has paths in the included or excluded list and the path that was not found is protected by the policy but is not in either list.

- Review the policy configuration and determine if the excludes or includes are configured as expected. Please note that using those options are not supported by Dell EMC for failover/failback

SMB Share path has a trailing "/" at the end of the share path - example /ifs/home/

- Remove the trailing "/" from the path of the share to resolve the error.

Once resolved the next Configuration Replication job will succeed and the alarm will be cleared.

Other possible causes for Missing Path on target cluster:

1) SyncIQ Policy associated with the path has not been run.
2) Path is on the SyncIQ Policy Excluded list.
3) SyncIQ Policy has paths in the Included or Excluded list and the path that was not found is protected by the policy but is not in either list.

Message AEC_FORBIDDEN For Eyeglass Configuration Replication Job

Problem:

Eyeglass configuration replication Job fails with error “AEC_FORBIDDEN…..”.

Possible Cause:

Isilon is provisioned in Eyeglass with a user who does not have minimum required privileges.

Troubleshooting Steps:

1. Cross reference the permissions of the Isilon OneFS user that is used in Eyeglass provisioning with Minimum Required Privileges documented here: User Minimum Privileges.
2. If the OneFS user does not have the required privileges, update the user privileges in OneFS. The next Eyeglass configuration replication job will be based on these updated privileges.
3. If the OneFS user has the minimum required privileges, double check the OneFS user privileges from the Isilon command line to ensure that they are set as required.

Message AEC_NOT_FOUND Zone <Zone Name> Not Found For Eyeglass Configuration Replication Job

Problem:

Eyeglass Configuration Replication Job fails with error “AEC_NOT_FOUND Zone <Zone Name> not found”. (Alarm code SCA0004)
This error is issued when the Eyeglass configuration replication job runs and attempts to replicate a share or export when the associated Zone does not exist on the target.

Resolution:

Review the SyncIQ policy associated to the Configuration Replication job in error and determine the following information:

- The SyncIQ policy source path on the Source cluster
- What is the name of the Access Zone where that SyncIQ policy source path is a part of on the Source cluster?
- What path is the SyncIQ policy target path replicating to on the Target cluster?
- On the Target cluster, what is the name of the Access Zone where the SyncIQ policy target path is pointing to?
- These Access Zone names need to be the same on source and target cluster otherwise you will receive the error in question.

Ensure that all Zones associated with shares and exports exist on the target.
Once the Zones exist, the next configuration replication job will succeed and the alarm will be cleared.

Message AEC_EXCEPTION Bad Hostname For Eyeglass Configuration Replication Job

Problem:

Eyeglass Configuration Replication Job fails with error “AEC_EXCEPTION message bad hostname 'host name'”. (Alarm code SCA0004)
This means that Eyeglass cannot replicate the NFS Export to the target cluster due to a hostname listed on the NFS Export "Clients" list not resolving on the target cluster.
It is best practice to allow the DR cluster to resolve host names, or data will not be mountable after a failover.

Possible Causes:

NFS Exports "Clients" field has a host name entry that cannot be resolved on replication of the Export.

Resolution:

1. Ensure that "Clients" field on the NFS Export on the source has valid host name entry.
2. Run nslookup <hostname> to determine if that name resolves correctly or not
3. Remove the host name from the clients list if not required any longer
4. If unable to remove or make the name resolve in DNS you can use the Eyeglass CLI command:
   igls admin ignoreunresolvablehosts
5. If issue still persists after running command to ignore then remove the export from the target cluster and allow Eyeglass to recreate it during Configuration Replication job

MESSAGE "AEC_NOT_FOUND", "message" : "Zone 'x' not found" For Eyeglass Configuration Replication Job

Problem:

This error will occur when Eyeglass attempts to replicate a share or export and the associated Zone does not exist on the target.

Possible Cause for Missing Zone:

1) Zone associated with share or export on the source cluster does not exist on the target cluster with the exact same name.

Solution:

Directory associated with the share or export or quota being replicated must exist on the target.
1) Run SyncIQ Policy to create the paths.
2) For SyncIQ Policy with Includes or Excludes, manually verify that the error relates to excluded paths and Job has succeeded for Included paths.
Zone associated with the share or export being replicated must exist on the target with the same name.

4. How to Use Log Parser and Doc Generator

Home Top

Overview

This feature can be used to generate detailed log parsing analysis if all Eyeglass products (Ransomware Defender, Easy Auditor and DR Manager). This is the same technology used by support to

trouble shoot issues. This allows customers to log parse their own appliance to resolve issues. It also provides reports and CSV downloads that summarize data about the environment. It will store history of all previous reports to go back in time to see previous results.

Ransomware Defender customers can use this to extract historically threat detections into a CSV file.

This tool also includes a professional services tool called Doc Generator that can build a detailed html report that summarizes the configuration of different products including building DR design documentation. This is a license key product feature for channel partners or customers that want design level documentation about their environment.

How to use Log Parser and Doc Generator

Requirements

1. Release 2.5.8.1 or later

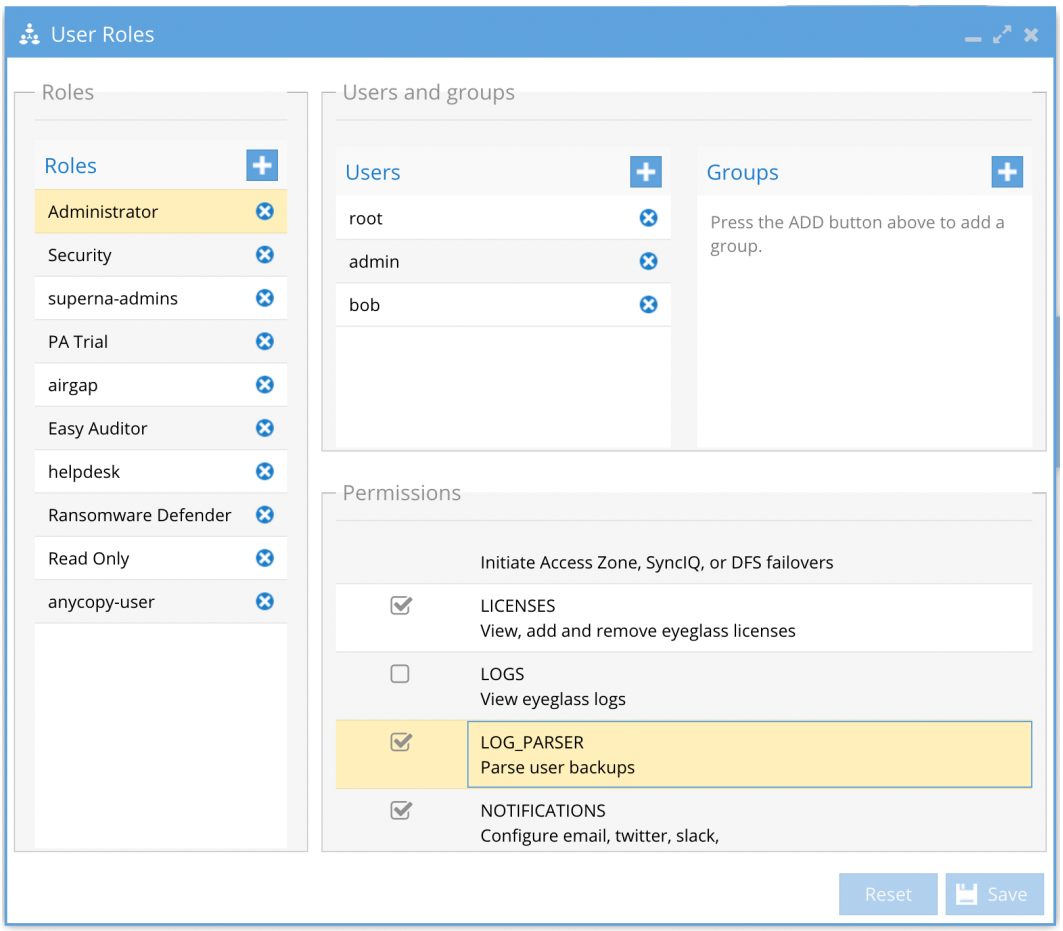
Overview

The tool can store the master zip file each time a backup is uploaded and reports. It is possible to delete the report and re-

run analysis or generate documents if licensed. The log parse tool can parse logs from any appliance even if the log was created on a different appliance.

How to Use Log parser

1. Login to Eyeglass and add the log parse role to the administrator and logout and login again.

   a. 

2. Open the Log Parse icon on the Desktop

   a. To use log parse you will need to download a backup zip file from the About Eyeglass --> Backup tab and support backup should be downloaded.

b. Click the add button.

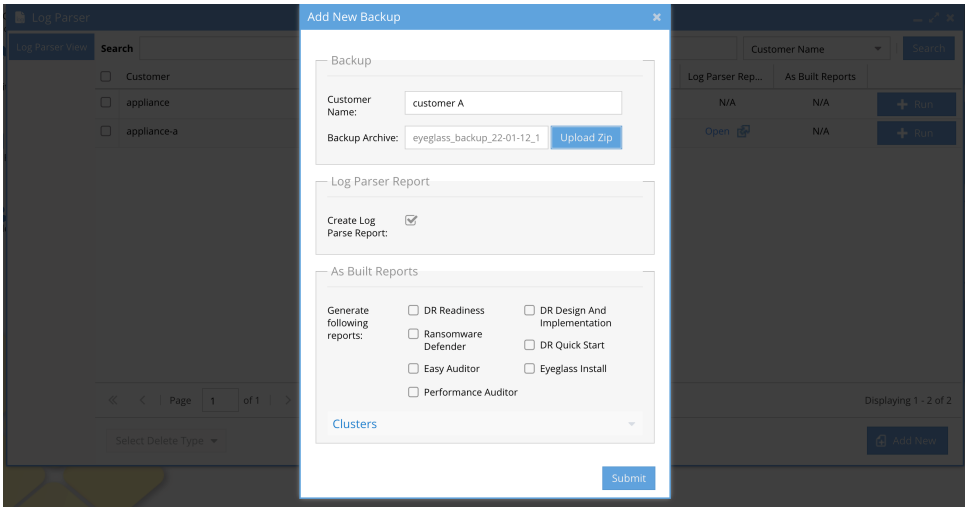
i. The default will generate a log parse

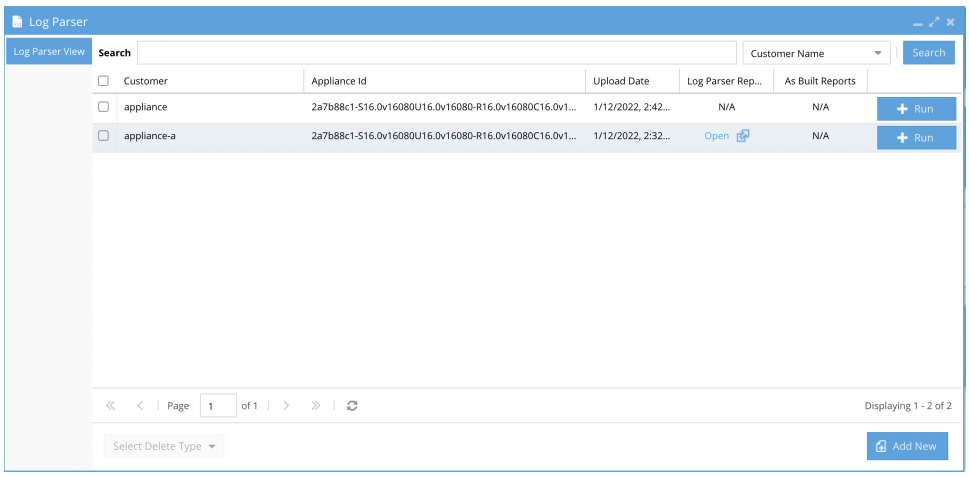
ii. Enter your site name or company name

iii. Click upload zip and locate the eyeglass support backup you downloaded to your pc.

iv. Accept the default option and click submit.

v. The zip file will take time to upload and will offer to view from the running jobs window. The final results will be displayed and stored on the appliance

vi. 

vii. 

viii. Click the open button to review the log parse results in a new browser tab.

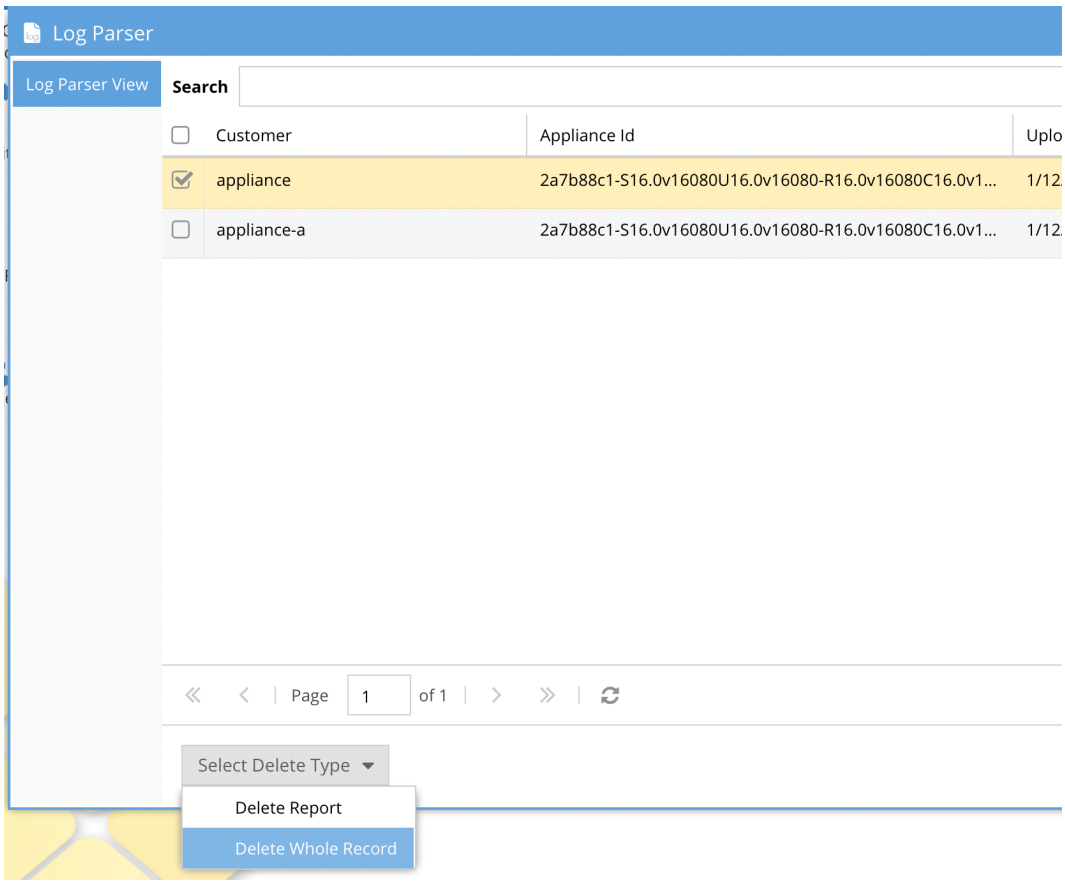
1. Use the table of contents to navigate to the section of the report to review. The Data exists means log parse found data to display. No data means nothing will be shown on this table of contents menu.

Navigation		
Search:		Clear
1	Access Zones And Policies Mapping	No data
2	Active Alarms	Data exists
3	Active Ransomware Defender Events	No data
4	Audit	No data
5	CPU Usage	No data
6	Cluster Information	No data
7	Cluster User Permissions	Data exists
8	Commands Executed To Gather OrientDB Info	Data exists
9	Consumer leaving a topic - from Kafka broker logs	Data exists
10	Continuous Operation Dashboard	Data exists
11	Cronjob count of profiler.sh	Data exists
12	DFS Readiness	No data
13	DR Testing Readiness	No data
14	ECA Disk Usage	Data exists
15	ECA Nodes: GET/POST Failures	Data exists
16	ECA Nodes: cluster up/down, HBASE up/down	Data exists
17	ECA POST requests: heartbeat	Data exists
18	ECA POST requests: notifications	Data exists
19	ECA var/log/messages: out of memory occurrences	No data
20	ECA: Error posting heartbeat to eyeglass	Data exists
21	ECA: Security Guard Events	Data exists
22	ECA: Threat Detector Overloading	Data exists
23	Event Rates	Data exists
24	Evt Archive - Event Rates	Data exists
25	Existence Of Auth Providers	No data
26	Failovers	Data exists
27	HBase Garbage Collection Errors	Data exists
28	Installed Licenses	Data exists
29	Log Parser Recent Upgrades	Data exists
30	Managed Device Alerts	No data
31	Memory Usage	No data
32	More Than 1 Access Zone Per Base Path	No data
33	NE Data	Data exists
34	Nested Base Paths	No data
35	NotServingRegionException Errors	Data exists
36	Number of objects in database tables	No data
37	Open File Limits	Data exists
38	Other Errors	Data exists
39	Policy Mirror Maps	No data
40	Policy Readiness	No data
41	Pool Readiness	No data
42	RPO Analysis - Date Gap Report	No data
43	RPO Analysis - Excluded Policies	No data
44	RPO Analysis - Policy Details	No data
45	Ransomware Defender - Learning mode	Error
46	Ransomware Defender - Paths	No data
47	Ransomware Defender - Sources	No data
48	Ransomware Defender - Thresholds	Data exists
49	Ransomware Defender - Users	No data
50	Ransomware Defender Historical Events	No data
51	Ransomware Filtered List	No data
52	Ransomware HBASE Errors	No data
53	Ransomware White List	Data exists
54	Region Server Errors	Data exists
55	Remote Services	Data exists
56	Remote Services - Running Containers	Data exists
57	Remote Services - Validation	Data exists
58	Replication Tasks	Data exists
59	Robo Audit Events	Data exists
60	SCA - Out Of Memory Occurrences	No data

c. Done

How to manage log parse records and disk space

1. A log parse record is an unzipped eyeglass backup. This consumes 1-4GB of space on the 80 GB disk on the appliance. The log parse report can be 3-12 MB in size.
2. To delete the entire record (log parse report and unzipped analysis data). Follow these steps
3. Select an appliance row (one or more) and click Select Delete type.

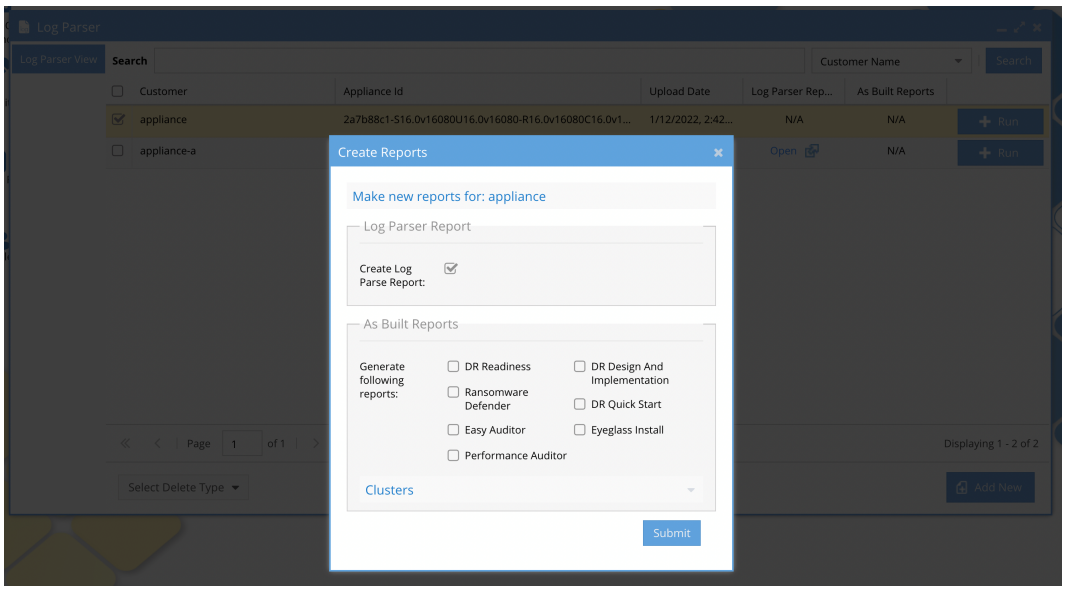
a. 

b. Select Delete whole record to delete the unzipped data from the backup and the log parse reports OR select only the log parse report.

c. If you only delete the log parse report you can re-run the log parse analysis using the run button.

How to run parse on an existing eyeglass backup record

1. Select an appliance backup row and click the + run button

a. 

b. Click submit and wait for the log parse job to complete and then view the report once it is completed. Monitor from running jobs icon, running tab.

c. Done

How Use to Doc Gen

Overview

This tool generates detailed design documents and summary if product installation. It includes details collected from the Powerscale clusters and can draw topology for replication, shares, exports, access zones , smb shares , quotas, pools, subnets for DR design documents. The other products include summary of the

design and configuration of Ransomware Defender, Easy Auditor, Performance Auditor.

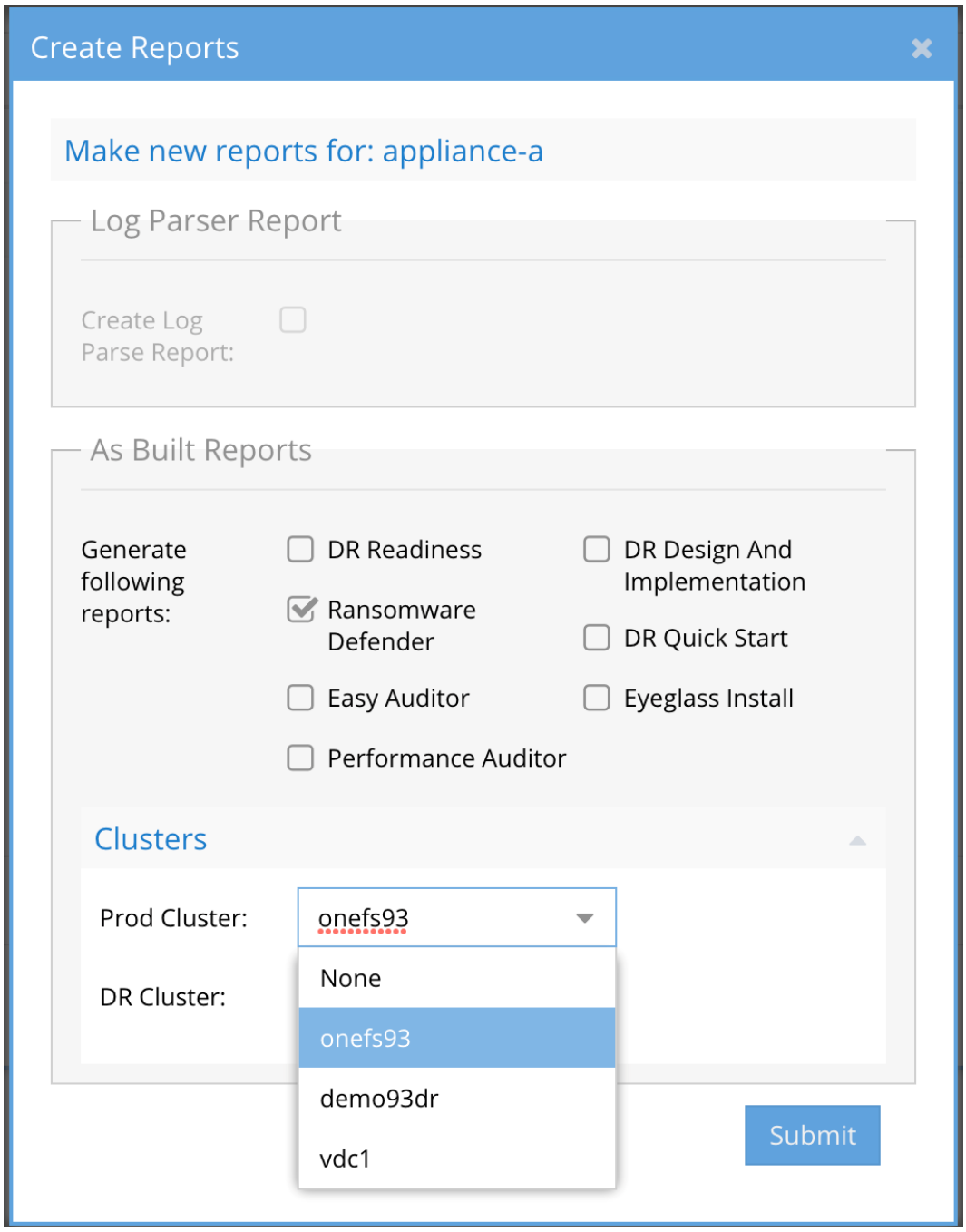
This feature is targeted at certified channel partners or customers that want automated documentation tools for the Isilon, Powerscale and Superna products.

Requirements

1. A license key for the subscription feature Eyeglass Pro Services Document Generator 1 Year Subscription

How to generate documents

1. Upload an eyeglass back or select an existing backup in the log parse icon and use the +Run button.
    a. Select check boxes for the reports that you want to generate
    b. Enter the cluster names that will be included in the report. For DR reports 2 clusters must be selected.

c. 

]

2.