

Table of Contents

1. Alarm Codes..... 2

1. Alarm Codes

[Home](#) [Top](#)

Abbreviation	Project
SCA	Eyeglass
AG	AIRGAP
RSW	Ransomware Defender
EAU	Easy Auditor
ECA	Eyeglass
ES	Eyeglass Search
DRSDEdge	Eyeglass for virtual clusters
SETUP	Setup issues
LM	License Manager

- [SCA0001 GENERIC_ALARM](#)
- [SCA0002 INVALID_SRC_DST_CONFIGURATION](#)
- [SCA0003 INVENTORY_FAILED](#)
- [SCA0004 REPLICATION_JOB_FAILED](#)
- [SCA0005 FAILED_TO_CONNECT](#)
- [SCA0006 BACKUP_JOB_FAILED](#)
- [SCA0007 JOB_AUDIT_FAILURE](#)
- [SCA0008 QUOTA_FAILOVER_JOB_FAILED](#)
- [SCA0009 BASE_LICENSE_TO_EXPIRE](#)
- [SCA0010 BASE_LICENSE_HAS_EXPIRED](#)
- [SCA0011 DISCOVERY_LICENSE_TO_EXPIRE](#)
- [SCA0012 DISCOVERY_LICENSE_HAS_EXPIRED](#)

- SCA0013 FEATURE_LICENSE_TO_EXPIRE
- SCA0014 FEATURE_LICENSE_HAS_EXPIRED
- SCA0015 MANAGEDOBJECT_LICENSE_TO_EXPIRE
- SCA0016 MANAGEDOBJECT_LICENSE_HAS_EXPIRED
- SCA0017 SUPPORT_LICENSE_TO_EXPIRE
- SCA0018 SUPPORT_LICENSE_HAS_EXPIRED
- SCA0019 TRIAL_KEY_LIMITS_REACHED
- SCA0020 AUDITTRUSTEE_ISSUE
- SCA0021 SINGLE_SHARE_MIGRATION_FAILURE
- SCA0022 NO_SUPPORT_LICENSE_INSTALLED
- SCA0023 REPLICATION_SOURCE_MATCHES_DESTINATION
- SCA0024 PREVIOUS_JOB_STILL_RUNNING
- SCA0025 NETWORK_ELEMENT_TOO_BUSY
- SCA0026 DR_DASHBOARD_STATUS_CHANGE_ALARM
- SCA0027 DR_DASHBOARD_STATUS_CHANGE_WARNING
- SCA0028 RUNBOOK_ROBOT_JOB_FAILED
- SCA0029 POLICY_FAILOVER_FAILURE
- SCA0030 ACCESS_ZONE_FAILOVER_FAILURE
- SCA0031 DFS_FAILOVER_FAILURE
- SCA0032 READINESS_JOB_FAILED
- SCA0033 READINESS_CHECK_ERRORS
- SCA0034 SPN_PROCESSING_FAILED
- SCA0035 NODE_COUNT_VIOLATION
- SCA0036 RUNBOOK_ROBOT_COUNT_EXCEEDED
- SCA0037 ACCESS_ZONE_FAILOVER_SPN_FAILURE
- SCA0038 POLICY_CONTAINS_EXCLUDES
- SCA0039 DISASTER_RECOVERY_TESTING_FAILED
- SCA0040 FAILOVER_SUCCEEDED
- SCA0041 DISASTER_RECOVERY_TEMPLATE_FAILED

- SCA0042 DISASTER_RECOVERY_EDGE_REPLICATION_FAILED
- SCA0043 DISASTER_RECOVERY_EDGE_DEPLOYMENT_FAILED
- SCA0044 PROBE_UNDER_LICENSED
- SCA0045 INVENTORY_DEGRADED
- SCA0046 CREATE_SD_EDGE_DEPLOYMENT_JOB
- SCA0047 NE_REMOVAL_ERROR
- SCA0049 JOB_AUDIT_WARNING
- SCA0050 QUOTA_INVENTORY_FAILED
- SCA0051 DEDUPE_REPLICATION_FAILED
- SCA0052 DUPLICATE_INVENTORY_ITEM
- SCA0053 CONTINUOUS_OPERATION_STATUS_ERROR
- SCA0054 MIGRATION_JOB_SUCCEEDED
- SCA0055 ARCHIVE_UPLOAD_FAILED
- SCA0056 DEDUPE_AUDIT_FAILED
- SCA0057 QUOTA_SYNCHRONIZATION_FAILED
- SCA0058 ERROR_RETRIEVING_CLUSTER_VERSION
- SCA0060 ERROR_GENERATING_DATASET
- SCA0061 DISCOVERY_RETRIEVAL_ERROR
- SCA0062 REST_API_ERROR
- SCA0063 POLICY_FAILOVER_CANCEL
- SCA0064 ACCESS_ZONE_FAILOVER_CANCEL
- SCA0065 DFS_FAILOVER_CANCEL
- SCA0066 RUNBOOK_ROBOT_JOB_CANCELED
- SCA0067 REHEARSAL_FAILOVER_CANCEL
- SCA0068 REHEARSAL_FAILOVER_FAILURE
- SCA0069 POLICY_POOL_MAPPING_ERROR
- SCA0070 DISK_SPACE_FULL_WARNING
- SCA0071 DISK_SPACE_FULL_ERROR
- SCA0073 CSM_GROUP_QUOTAS_MANAGER_FAILURE

- SCA0074 REHEARSAL_FAILOVER_SUCCEEDED
- SCA0075 ISK_SIZE_MONITOR_ALARM
- SCA0076 DISK_SIZE_MONITOR_INACTIVE
- SCA0077 DISK_SIZE_MONITOR_ERROR
- SCA0078 REST_API_CALL_FAILURE
- SCA0079 NEW_POLICY_DISCOVERED
- SCA0080 UNCONFIGURED_JOB_PRESENT
- SCA0081 READINESS_CHECK_WARNINGS
- SCA0087 SYNCIQ_MONITOR_ERRORS
- SCA0088 ONFIG_BACKUP_JOB_FAILURE
- SCA0094 RAM_UNDERSIZED
- AG0001 AIRGAP_JOB_FAILED
- AG0002 AIRGAP_JOB_SUCCEEDED
- AG0003 AIRGAP_ROUTE_CLOSED
- AG0004 AIRGAP_ROUTE_OPEN
- AG0005 AIRGAP_JOB_DISABLED_FOR_ACTIVE_EVENT
- AG0006 VAULT_AIRGAP_JOB_FAILED
- AG0007 VAULT_AIRGAP_JOB_SUCCEEDED
- AG0008 VAULT_OPENED
- AG0009 AIRGAP_EVENT_RETRIEVE_JOB_FAILED
- AG0010 AIRGAP_EVENT_RETRIEVE_JOB_SUCCEEDED
- AG0011 AIRGAP_SCHEDULES_QUERY
- AG0012 AIRGAP_JOB_NOT_STARTED
- AG0013 AIRGAP_JOB_STARTED
- AG0014 AIRGAP_POLICY_CHANGED
- RSW0001 RANSOMWARE_DEFENDER_EVENT
- RSW0002 RANSOMWARE_USER_LOCKED
- RSW0003 RANSOMWARE_USER_LOCK_FAILED
- RSW0004 RANSOMWARE_ECA_IGLS_SERVICE_FAILURE

- RSW0005 RANSOMWARE_ECA_HBASE_FAILURE
- RSW0006 RANSOMWARE_ECA_COMM_FAILURE
- RSW0008 RANSOMWARE_ENTER_MONITOR_MODE
- RSW0009 RANSOMWARE_LEAVE_MONITOR_MODE
- RSW0010 RANSOMWARE_ECA_VERSION
- RSW0011 RSW_RESTORE_ACCESS_SUCCESS
- RSW0012 RSW_RESTORE_ACCESS_FAILED
- RSW0013 RSW_SNAPSHOT_WARNING
- RSW0014 RSW_SNAPSHOT_FAILED
- RSW0015 RSW_SNAPSHOT_DELETE_WARNING
- RSW0016 RSW_SNAPSHOT_DELETE_FAILED
- RSW0017 HBASE_UPGRADE_FAILURE
- RSW0018 RANSOMWARE_DEFENDER_UNDER_LICENSED
- RSW0021 SECURITY_EVENT_FAILED
- RSW0022 SECURITY_EVENT_RETURNED_ZERO
- RSW0025 RANSOMWARE_WARNING_ERROR
- RSW0026 TURBOAUDIT_EVENTRATE_BELOW_THRESHOLD_WARNING
- RSW0027 EVTARCHIVE_EVENTRATE_BELOW_THRESHOLD_WARNING
- RSW0028 SECURITY_GUARD_SUCCESS
- RSW0029 CYBER_RECOVERY_MANAGER_JOB_ERROR
- EAU0002 AUDITOR_REPORT_FAILURE
- EAU0003 EVENT_AUDIT_TIME_SKEW_ERROR
- EAU0004 TIME_SKEW_ERROR
- EAU0005 NO_SMART_QUOTA_FOR_DLP_PATH
- EAU0006 AUDITOR_REPORT_SUCCESS
- EAU0007 ACTIVE_AUDITOR_EVENT
- EAU0008 ROBO_AUDIT_FAILURE
- EAU0009 ROBO_AUDIT_SUCCESS
- ECA0001 ECA_SERVICE_INFO

- ECA0002 ECA_CRITICAL_ERROR
- ECA0003 ECA_SERVICE_WARNING
- ECA0004 ECA_MINOR_ERROR
- ECA0005 ECA_MAJOR_ERROR
- ECA0006 ECA_FATAL_ERROR
- ECA0007 ECA_NODE_FAILURE
- ES0001 ES_NODE_COUNT_VIOLATION
- ES001
- ES002
- ES003
- ES004
- ES005
- ES006
- ES007
- ES008
- ES009
- ES010
- ES011
- ES012
- ES013
- ES014
- ES015
- ES016
- ES017
- ES018
- ES019
- ES020
- ES021
- ES022

- [ES023](#)
- [ES024](#)
- [ES025](#)
- [DRSDEDGE0001 DRSDEDGE_NODE_COUNT_VIOLATION](#)
- [SETUP0001 SETUP_REDISCOVER_REQUEST](#)
- [SETUP0002 SETUP_INVENTORY_DUPLICATES_CRITICAL](#)
- [SETUP0003 SETUP_INVENTORY_DUPLICATES_WARNING](#)
- [LM0001 LM_LICENSE_TO_EXPIRE](#)
- [LM0002 LM_LICENSE_HAS_EXPIRED](#)

SCA0001 GENERIC_ALARM

Description: Error within the SCA service

Severity: CRITICAL

Help on this Alarm:

This covers all unknown errors that have no more specific errors.

SCA0002 INVALID_SRC_DST_CONFIGURATION

Description: Found a replication job where either the source or destination is not a managed network element

Severity: CRITICAL

Help on this Alarm:

- **Problem:** This alarm will occur when an Eyeglass configuration replication Job fails to run because it is associated with a PowerScale cluster not being provisioned in Eyeglass. The Eyeglass configuration replication Jobs are created based on the SynclQ policies discovered during the Eyeglass Inventory task. It is

possible that a PowerScale cluster provisioned in Eyeglass could have SyncIQ policies that have PowerScale cluster targets that are not provisioned in Eyeglass.

- Resolution:
 - Provision Eyeglass with all PowerScale clusters related to Eyeglass configuration replication Jobs
 - If not all PowerScale clusters associated with Eyeglass configuration replication Jobs can be managed by Eyeglass, disable Eyeglass configuration replication Jobs associated with PowerScale clusters not managed by Eyeglass to avoid the error

SCA0003 INVENTORY_FAILED

Description: Failed to retrieve inventory

Severity: CRITICAL

Help on this Alarm:

- Problem: This alarm will occur when the Eyeglass Inventory task which discovers the configuration information on an PowerScale cluster has failed to run.
- Resolution:
 - Ensure that PowerScale clusters are reachable from Eyeglass server
 - This problem can also occur if the Inventory task attempts to start while another instance of the Inventory task is still running. In this case the problem will be transient and will clear on it's own. If this problem persists, contact support.superna.net for assistance.
 - If the Info for the alarm shows "Error fetching data from ssh. Inventory may be incomplete" there is an issue with retrieving the Inventory information that requires ssh access.
 - Ensure that the PowerScale cluster user role in Eyeglass has Network Read/Write permissions
 - Ensure that the PowerScale cluster user roled in Eyeglass does not contain a - or other special characters. This can cause an issue with the sudo command that is used. To troubleshoot this condition:
 1. Login to PowerScale cluster CLI as PowerScale Cluster user that has been provisioned in Eyeglass

2. Execute the command below - it needs to be able to execute without error

```
sudo isi networks list pools
```

Example of successful command execution

```
% sudo isi networks list pools
```

Subnet	Pool	SmartConnect Zone	Ranges Alloc

int-a-subnet	int-a-pool	192.168.4.145-192.1...	Static

Example of failed command execution

```
sudo isi networks list pools
```

```
sudo: >>> /usr/local/etc/sudoers: syntax error near line 168 <<<
```

```
sudo: parse error in /usr/local/etc/sudoers near line 168
```

```
sudo: no valid sudoers sources found, quitting
```

```
sudo: unable to initialize policy plugin
```

SCA0004 REPLICATION_JOB_FAILED

Description: Replication job failed to run

Severity: CRITICAL

Help on this Alarm:

Following reasons are commonly seen to cause a replication job failure. The Info related to the alarm should be verified to confirm the cause:

- AEC_NOT_FOUND Zone <Zone Name> not found.
 - Problem: 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: Ensure 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.
- AEC_NOT_FOUND "Path 'x/y/z' not found: No such file or directory".
 - Problem: 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.
 - Possible Cause for Missing Path (Group 1):
 - SyncQ Policy associated with the path has not been run.
 - Path is on the SyncIQ Policy Excluded list.
 - 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.
 - Resolution (Group 1): Ensure that all directories associated with shares and exports and quotas exist on the target. Once the Zones exist, the next configuration replication job will succeed and the alarm will be cleared
 - Possible Cause for Missing Path (Group 2):
 - share path has a trailing "/" at the end of the share path - example /ifs/home/
 - Resolution (Group 2): We recommend to remove the trailing "/" from the path of the share to resolve the error.
- AEC_EXCEPTION bad hostname <host name>
 - NFS Export Clients field has a host name entry that cannot be resolved on replication of the Export
- AEC_EXCEPTION Cannot set security descriptor on <share path> Read only file system
 - You will receive the above error when Eyeglass is not able to sync share properties such as ABE (Access based Enumeration).
 - In this case we recommend you to compare all properties of the active cluster share with the target cluster share and make it identical with the source.

NOTE: failure for any property of a share, export or quota to replicate will stop all replication for that share/export/quota

SCA0005 FAILED_TO_CONNECT

Description: Failed to connect to the designated target

Severity: CRITICAL

Help on this Alarm:

- **Problem:** This alarm will occur when Eyeglass cannot establish a connection with the PowerScale cluster it is managing.
- **Resolution:**
 - Verify that there have been no changes in PowerScale credentials, which would cause Eyeglass provisioning to be outdated.
 - Verify that there have been no networking or firewall changes that would result in network connectivity loss between the Eyeglass server and the PowerScale clusters.

SCA0006 BACKUP_JOB_FAILED

Description: Failed to create a backup archive

Severity: MAJOR

SCA0007 JOB_AUDIT_FAILURE

Description: Replication job audit failed

Severity: MAJOR

Help on this Alarm:

- **Problem:** The Eyeglass audit task compares source and destination configuration items post-replication to confirm that the replication task has done its Job and that the configuration items on the source and target are indeed identical. Replication job audit failed alarm will occur when:
 - audit job fails to run
 - audit job finds configuration items where the source and target are different

- Resolution: Use the Info related to the alarm aid to resolve the issue
 - audit job failure to run
 - Info: Audit of shares for current job is inconclusive because source and target network element are identical.
 - Resolution: Eyeglass configuration replication Job has same PowerScale cluster configured as source and target. Eyeglass cannot perform replication configuration or the associated audit with this configuration. Disable this Job to avoid this alarm.
- Info: Audit of job 'xxx' has failed: Source and/or target network element were not found in provided list of network elements
- Resolution: Source and target PowerScale Clusters in Job xxx must be managed by Eyeglass for audit to run.
- audit job finds configuration item where source and target are different
 - Info: Audit failed: Values for key 'xxx' do not match: source: share or export ; target: share or export
 - key 'xxx' refers to a property of share or export where mismatch was found
 - Info: Auditable source (type: 'xxx', zone: 'yyy', name: 'zzz') and target (type: 'xxx', zone: 'yyy', name: 'zzz') objects not found on source or target cluster, hence audit fails.
 - Auditable source refers to configuration item
 - Resolution:
 - Check that associated Replication Job was successfully run. If not, the source and destination may be different, and the Replication Job issue must be resolved.
 - It is possible that a change to configuration item was made via OneFS after the replication Job was completed and before audit task ran. The next replication task will resolve this mismatch.

SCA0008 QUOTA_FAILOVER_JOB_FAILED

Description: Quota failover job failed

Severity: CRITICAL

SCA0009 BASE_LICENSE_TO_EXPIRE

Description: Base license to expire

Severity: WARNING

Help on this Alarm:

A base license is about to expire; it can be renewed on the support.superna.net site by opening a case with your appliance id.

SCA0010 BASE_LICENSE_HAS_EXPIRED

Description: Base license has expired

Severity: MAJOR

Help on this Alarm:

A base license has expired; can be renewed on the support.superna.net site by opening a case with your appliance id.

SCA0011 DISCOVERY_LICENSE_TO_EXPIRE

Description: Discovery license to expire

Severity: WARNING

Help on this Alarm:

A base license is about to expire; can be renewed on the support.superna.net site by opening a case with your appliance id.

SCA0012 DISCOVERY_LICENSE_HAS_EXPIRED

Description: Discovery license has expired

Severity: MAJOR

Help on this Alarm:

A base license is about to expire; can be renewed on the support.superna.net site by opening a case with your appliance id.

SCA0013 FEATURE_LICENSE_TO_EXPIRE

Description: Feature license to expire

Severity: WARNING

Help on this Alarm:

A feature license is about to expire; can be renewed on the support.superna.net site by opening a case with your appliance id.

SCA0014 FEATURE_LICENSE_HAS_EXPIRED

Description: Feature license has expired

Severity: MAJOR

Help on this Alarm:

A feature license has expired; it can be renewed on the support.superna.net site by opening a case with your appliance id.

SCA0015 MANAGEDOBJECT_LICENSE_TO_EXPIRE

Description: Managed object license to expire

Severity: WARNING

Help on this Alarm:

A managed object license is about to expire; it can be renewed on the support.superna.net site by opening a case with your appliance id.

SCA0016 MANAGEDOBJECT_LICENSE_HAS_EXPIRED

Description: Managed object license has expired

Severity: MAJOR

Help on this Alarm:

A managed object license has expired; can be renewed on the support.superna.net site by opening a case with your appliance id.

SCA0017 SUPPORT_LICENSE_TO_EXPIRE

Description: Support license to expire

Severity: WARNING

Help on this Alarm:

A support license is about to expire; can be renewed on the support.superna.net site by opening a case with your appliance id.

SCA0018 SUPPORT_LICENSE_HAS_EXPIRED

Description: Support license has expired

Severity: MAJOR

Help on this Alarm:

A support license has expired; can be renewed on the support.superna.net site by opening a case with your appliance id.

SCA0019 TRIAL_KEY_LIMITS_REACHED

Description: Replication functionality limited by trial

Severity: WARNING

Help on this Alarm:

The trial key has limits applied. Open a case on support.superna.net to request higher limits.

SCA0020 AUDITTRUSTEE_ISSUE

Description: Replication audit issue with the trustee(s)

Severity: CRITICAL

SCA0021 SINGLE_SHARE_MIGRATION_FAILURE

Description: Single Share Migration Job failed

Severity: MAJOR

Help on this Alarm:

The migration job has encountered an error, this error code relates to folder migration feature. The SyncIQ policy and migration job from running jobs window should be checked for the failed step and find the info button for the error to raise a case with support.

SCA0022 NO_SUPPORT_LICENSE_INSTALLED

Description: No support license has been installed. Patches cannot be applied

Severity: MAJOR

Help on this Alarm:

This indicates no support license key is installed, which is required to raise a case for a production appliance. If your support keys have expired, a new order is required to purchase a new support contract.

SCA0023 REPLICATION_SOURCE_MATCHES_DESTINATION

Description: Found a replication job where the source is. Destinations are the same, and that replicates shares

Severity: CRITICAL

Help on this Alarm:

This alarm is expected if a SynclQ Job is discovered where the source and target refer to the same cluster.

SCA0024 PREVIOUS_JOB_STILL_RUNNING

Description: A scheduled task could not run as another instance was already running

Severity: WARNING

Help on this Alarm:

This alarm will occur when a replication task is in progress when a new replication task is scheduled to begin. Eyeglass attempts to begin a new replication task every 5 minutes by default. In the event that configuration replication takes longer than 5 minutes on your Eyeglass system, you will see this alarm for each attempt to start replication that was blocked.

No action is required. When the in-progress configuration replication Job is completed, the next scheduled configuration replication task will begin.

SCA0025 NETWORK_ELEMENT_TOO_BUSY

Description: The target is too busy to respond to all requests. Consider reducing the number of parallel operations

Severity: MAJOR

Help on this Alarm:

This alarm will occur when the API call to the cluster returns this error. It indicates the cluster node is busy and is refusing to answer API calls. This can happen if too many parallel operations are issued to the cluster using PAPI. No arm will occur in this condition, but Eyeglass can not complete the operation and will generate other errors. This can also occur on a heavily used cluster or a node in the cluster that has resource issues i.e. CPU utilization.

To correct this operation, raise a support request to get instructions to reduce the number of parallel API calls used to connect to a cluster.

SCA0026

DR_DASHBOARD_STATUS_CHANGE_ALARM

Description: The job status for the job changed to error.

Severity: CRITICAL

Help on this Alarm:

This alarm will occur when there is an error state either on a Configuration Replication Job or on a SyncIQ Policy Job, resulting in an overall DR Dashboard status related to that policy to be in Error.

To troubleshoot this error, login to the Eyeglass web page and open the DR Dashboard window. Find the Job which was reporting an error and expand it to determine whether the issue is with the SyncIQ policy Job or the Eyeglass Configuration Replication Job. If the problem lies with the SyncIQ Job, further troubleshooting should be done from OneFS. If the problem lies with Eyeglass Configuration Replication Job, open the Alarms window and look for an alarm which has this Configuration Replication Job as the source. The Info of this alarm will provide additional details regarding the cause of the issue.

SCA0027

DR_DASHBOARD_STATUS_CHANGE_WARNING

Description: The job status for the job changed to either 'pending' or 'disabled'

Severity: WARNING

Help on this Alarm:

This alarm will occur when there is a DR Dashboard status change for a Job to either Pending or Disabled.

For a status of Pending, no action is required. This is an indication that the Job has not yet been run.

For the status of Disabled, this status may occur if the SyncIQ Policy has been disabled in OneFS or if the Configuration Replication Job has been User Disabled in Eyeglass. If Disabled is not the correct status for this Job, login to the Eyeglass web page and open the DR Dashboard window. Expand the Job related to the alarm to determine whether the SyncIQ Policy has been disabled or the Eyeglass Configuration Replication Job. If this Job should not be disabled for the SyncIQ policy, you must enable using the OneFS interface. For Eyeglass Configuration Replication, open the Jobs window and then select the Job in the list. Open the Select a bulk action menu and select Enable/Disable.

SCA0028 RUNBOOK_ROBOT_JOB_FAILED

Description: The Runbook Robot job failed for the job

Severity: MAJOR

Help on this Alarm:

This alarm will occur when the run book robot job fails and indicates you have misconfigured the robot or the robot failed and your cluster is not ready for a real DR event. The robot is the best indication of readiness for failover.

SCA0029 POLICY_FAILOVER_FAILURE

Description: Policy Failover Job failed

Severity: MAJOR

Help on this Alarm:

This alarm will occur when a DR Assistant failover job has been created and submitted to failover a policy. To recover from this alarm. Open the DR Assistant icon on the Eyeglass desktop and select the failover history. Review the failover log for the failover job to find which step in the failover did not complete so you know where to begin manual step recovery. Use the [Failover Recovery Procedures](#) for guidance on manual recovery.

SCA0030

ACCESS_ZONE_FAILOVER_FAILURE

Description: Access Zone Failover Job failed

Severity: MAJOR

Help on this Alarm:

This alarm will occur when a DR Assistant failover job has been created and submitted to failover an Access zone. To recover from this alarm. Open the DR Assistant icon on the Eyeglass desktop and select the failover history. Review the failover log for the failover job to find which step in the failover did not complete, so you know where to begin manual step recovery. Use the [Failover Recovery Procedures](#) for guidance on manual recovery.

SCA0031 DFS_FAILOVER_FAILURE

Description: DFS Failover Job failed

Severity: MAJOR

Help on this Alarm:

This alarm will occur when a DR Assistant failover of a DFS job has failed. The DR Assistant history window has a log that should be reviewed for which step failed and take corrective action from when the failure occurred to recover the failed steps manually. Use the [Failover Recovery Procedures](#) for guidance on manual recovery.

SCA0032 READINESS_JOB_FAILED

Description: Readiness job failed to run

Severity: MAJOR

Help on this Alarm:

The Failover Readiness job encountered unexpected errors when running. Run Failover Readiness manually from the Eyeglass Jobs window. Ensure the Access Zone Prerequisites have been [Planning and Procedures for Eyeglass Access Zone Failover](#).

SCA0033 READINESS_CHECK_ERRORS

Description: Readiness job execution found errors - not ready for failover

Severity: CRITICAL

Help on this Alarm:

This alarm will occur when a Zone readiness job that check various parameters, settings, mappings for Smartconnect Zones, SPN values on cluster machine accounts are not registered with the AD. This requires delegation steps to SPN property on the machine account and should be check first in documentation the procedures. Network mapping not completed is another reason the readiness job can fail.

It will also be failed if SynclQ job associated with the Zone has failed (based on its path and access zone root path), if configuration replication also fails for any policy in an Access zone this will also trigger a zone readiness failure.

Go to the Eyeglass DR Dashboard Zone Readiness tab and select the zone name to check the status. Click mapping to verify all hints are in place, then click status make sure its green if not look for the failed item in the list and take action to resolve either SynclQ failures, configuration replication job failures and policies and SPN failures.

SCA0034 SPN_PROCESSING_FAILED

Description: SPN processing (either checking or repairing) has failed

Severity: MAJOR

Help on this Alarm:

This alarm will occur when Eyeglass was unable to create or delete SPNs during the regular Inventory task. Manually inspect existing SPNs using the ADSI Edit tool and ensure that there is an SPN for each Smartconnect Zone and Smartconnect Zone alias used for SMB share access. [Failover Readiness Validations DR Dashboard - SPN Delegation Example](#)

SCA0035 NODE_COUNT_VIOLATION

Description: The node count limitation has been exceeded

Severity: CRITICAL

Help on this Alarm:

This alarm will occur when you have an Eyeglass Node based license (License Type SEL EYEGGLASS DR MANAGER ADVANCED OR Ent VAPP in the Eyeglass Managed Licenses window) and the number of nodes in the PowerScale clusters being managed by Eyeglass exceeds the number of nodes that you have licensed. Additional node licenses must be purchased to match the total number of managed nodes. No product support is provided for under licensed clusters.

SCA0036

RUNBOOK_ROBOT_COUNT_EXCEEDED

Description: The runbook robot job count has been exceeded

Severity: WARNING

Help on this Alarm:

This alarm will inform you that you have configured more than one Eyeglass Runbook Robot job on the PowerScale clusters being managed by Eyeglass. Eyeglass will only execute one Runbook Robot job.

Remove extra Runbook Robot jobs by deleting the SyncIQ policies with the special name and ensuring only 1 exists.

SCA0037

ACCESS_ZONE_FAILOVER_SPN_FAILURE

Description: Failed to delete or repair SPNs during failover

Severity: CRITICAL

Help on this Alarm:

This alarm will occur when Eyeglass was unable to create or delete SPNs related to Smartconnect Zone changes that were made during an Access Zone failover. Manually inspect existing SPNs using the ADSI Edit tool:

1. Failover Source Cluster - SPN for SmartConnect Zone that is prefixed with "igls-original" SHOULD exist, if not then add it.
2. Failover Target Cluster - SPN for SmartConnect Zone name or Alias added during failover SHOULD exist, if not then add it

Where the above conditions are not met, using ADSI Edit to update SPN to be on correct cluster. You cannot create a missing SPN on the Active Cluster if it still exists for

the Failed Over cluster. You need to remove from Failover Over cluster first and then add to active cluster. [How to Configure Delegation of Cluster Machine Accounts with Active Directory Users and Computers Snapin](#)

SCA0038 POLICY_CONTAINS_EXCLUDES

Description: Found a policy with excluded directories. This is not a supported SyncIQ configuration for failback

Severity: WARNING

Help on this Alarm:

This alarm will inform you that Eyeglass has detected a SyncIQ Policy with excludes (or includes) configured. This is not a supported SyncIQ configuration for failback.

SCA0039 DISASTER_RECOVERY_TESTING_FAILED

Description: The disaster recovery testing has failed

Severity: MAJOR

Help on this Alarm:

This alarm will occur when Eyeglass has executed DR test mode job and it resulted in an error, retry the enable or disable or check the running jobs window for details on the failover.

SCA0040 FAILOVER_SUCCEEDED

Description: Failover Succeeded

Severity: INFORMATIONAL

Help on this Alarm:

This alarm will occur when Eyeglass has successfully executed any failover mode without error and is sent to log that a failover has occurred.

SCA0041

DISASTER_RECOVERY_TEMPLATE_FAILED

Description: The disaster recovery Template Replication has failed

Severity: MAJOR

Help on this Alarm:

This alarm will occur when Eyeglass PowerScaleSD product has deployed an access zone template to an edge cluster and the job has failed. Check the running job for specific error or step that failed before retrying again.

SCA0042 DISASTER_RECOVERY_EDGE_REPLICATION_FAILED

Description: The disaster recovery Replication to SD Edge has failed

Severity: MAJOR

Help on this Alarm:

This alarm will occur when Eyeglass PowerScaleSD edition has executed failover from the core to the edge cluster and resulted in failure to setup the edge site after configuring failover. Consult the running jobs window for specific error and step before attempting to retry the job.

SCA0043

DISASTER_RECOVERY_EDGE_DEPLOYMENT_FAILED

Description: The disaster recovery Deployment to SD Edge has failed

Severity: MAJOR

Help on this Alarm:

This alarm will occur when Eyeglass PowerScaleSD edition product deploys the core access zone template and syncs shares and exports to the edge cluster. This setup requires policies to sync folder structure before shares and exports can be created.

Check policy run status on the PowerScale and running jobs window to verify the step and error code that blocked the job from completing before retrying the job.

SCA0044 PROBE_UNDER_LICENSED

Description: The Probe is under-licensed

Severity: MAJOR

Help on this Alarm:

This alarm indicates more clusters are managed by eyeglass DR than eyeglass CA UIM Probe license keys installed. Eyeglass will randomly select which clusters are managed for the CA UIM alarm monitoring. contact sales@superna.net to get a quote on additional probe license keys to remove the alarm and get a fully supported installation.

SCA0045 INVENTORY_DEGRADED

Description: Inventory is degraded/incomplete

Severity: MINOR

Help on this Alarm:

This alarm indicates the inventory process that runs when cluster configuration replication job runs (default 5 minute intervals), encountered API failure responses from the cluster node the API request was sent too. This condition can clear on its own if the cluster node resumes processing API REST calls. If the configuration replication job fails completely then the cluster has stopped answering API calls. It is best to monitor how often this alarm is seen, and IF persistent open a case with support and upload the logs to the case. The logs will be requested if not attached to the case. If the condition persists EMC support case should be opened, as the node is overloaded and unable to respond to API queries.

NOTE: The OneFS UI also uses the REST API and ignoring this event can affect OneFS UI on the node that is returning the API failures.

SCA0046 CREATE_SD_EDGE_DEPLOYMENT_JOB

Description: Creation of SD Edge deployment Job failed

Severity: MINOR

Help on this Alarm:

This alarm only applies to the Branch office config and data protection licensed solution. When building a new edge site the deployment job failed.

1. This can be caused by un-reachable cluster
2. SyncIQ command failed to return with a status code from the cluster
3. Timeout waiting on a cluster command to complete. Check syncIQ reports for the temporary deployment policy that Eyeglass creates to look for errors on the source cluster where the template access zone was created.

SCA0047 NE_REMOVAL_ERROR

Description: Network element removal failed

Severity: CRITICAL

Help on this Alarm:

This alarm is raised and logged when a cluster previously under management has been deleted which is a user action. This alarm will never be generated without manual delete from the Inventory Icon on the eyeglass desktop. If this alarm is unexpected, it indicates someone deleted the cluster and re-added it. This is not a recommended procedure for any errors encountered with eyeglass. Unless you know what procedure you are doing, check with support before deleting a cluster from inventory when active DR monitoring in production is the current state for this cluster. Test clusters can be deleted if needed using this procedure.

1. Open Inventory Window
2. Select Cluster
3. Right-click and select Delete NE

SCA0049 JOB_AUDIT_WARNING

Description: Replication job audit resulted in a warning

Severity: WARNING

Help on this Alarm:

This alarm is raised when the cluster sync audit step runs as per the configuration replication job. This step gets inventory from both clusters and does a share, export, quota, snapshot schedule, dedupe setting, nfs aliases object and Attribute comparison.

This generally indicates the source cluster policy and target cluster policy configuration data is not 100% in sync. The error in the alarms window includes an info text describing the field or objects that are not an exact match.

The resolution will require checking with support on the error to determine the resolution.

It is possible that target cluster defaults for shares exports are set in a way that means synced shares or exports by Eyeglass get modified by the target cluster to apply cluster defaults that are different from the source cluster. This can cause an attribute to change that the audit will detect.

The first place to check is default settings on both clusters match for shares and exports.

It is also possible someone manually changed a setting on a share or export on the target cluster, causing the audit to fail.

In general, we recommend that both source and target clusters are exact matches.

SCA0050 QUOTA_INVENTORY_FAILED

Description: Failed to retrieve quotas

Severity: CRITICAL

Help on this Alarm:

The quotas are retrieved with REST api calls pages at a time. On clusters with 1000's or 10 000's of thousands of quotas, this process requires many api calls to complete to collect each quota and any notifications setup for each quota (retrieved with separate API calls). If an API call fails while retrieving quotas through this long running multi query part of the Configuration Sync job, this error can be returned.

This could also happen if eyeglass minimum permissions where not set correctly and should be checked.

SCA0051 DEDUPE_REPLICATION_FAILED

Description: Deduplication replication job failed to run

Severity: MAJOR

Help on this Alarm:

As of Eyeglass 1.6.3 and later dedupe paths are synced between clusters, configuration replication jobs are responsible for syncing dedupe paths and if an API failure to set all the paths on the target cluster occurs this alarm is raised. This could be minimum permissions issue with the eyeglass service account or API failure and configuration replication in running jobs should be expanded to find the info text that identifies the API error that triggered the failure. Search documentation site on how to find and identify sync errors.

SCA0052 DUPLICATE_INVENTORY_ITEM

Description: Found duplicate inventory items

Severity: MAJOR

Help on this Alarm:

This error is raised when the inventory function that runs as part of the configuration job identifies two entries that are duplicates and cannot be saved to the database. If this error is seen on instructions on resetting the database to remove duplicate items, raise a support case. The database in 1.7.0 and later can be rediscovered safely with all job settings being discovered.

SCA0053 CONTINUOUS_OPERATION_STATU S_ERROR

Description: Continuous operation status is ERROR

Severity: MAJOR

Help on this Alarm:

The new continuous operations dashboard shows the overall status of Snapshot sync and dedupe sync status, if this dashboard and status can not be updated from the configuration sync jobs or if sync status failed on SyncIQ policies paths with snapshot schedules or dedupe path settings related to SyncIQ jobs are not in Sync on source and target cluster, this alarm is raised indicate Readiness for operations on the target cluster is impacted.

Review the dashboard to identify the policy that is affected, which will help identify which area snapshots or dedupe are in sync error state. This can be done using the running jobs window and expanding the last errored job to find the policy and section for snapshot schedule and dedupe sync to identify the API error that is the root cause of

the dashboard state change to error state. Search documentation site on how to find and identify sync errors.

SCA0054 MIGRATION_JOB_SUCCEEDED

Description: Migration job succeeded

Severity: INFORMATIONAL

Help on this Alarm:

This indicates an Access Zone Migration job has completed successfully.

SCA0055 ARCHIVE_UPLOAD_FAILED

Description: Archive upload failed

Severity: CRITICAL

Help on this Alarm:

The new about Eyeglass --> backup tab now has upload directly to support option for logs, this error indicates the upload failed. Which is likely caused by firewall blocking the Eyeglass appliance from directly reaching the support portal to upload the log.

If you see this error it means support did not get the log file and you should login to the support site download the backup archive and upload manually to the support site. The direct upload requires port 443 HTTPS directly to the Internet from the Eyeglass appliance.

SCA0056 DEDUPE_AUDIT_FAILED

Description: Deduplication audit job failed to run

Severity: MAJOR

Help on this Alarm:

This indicates the audit of both clusters dedupe settings (run automatically for the configuration sync jobs), was not able to complete the comparison between the cluster. Run manually again and see if the error persists. If the error is still present then open a case with support.

SCA0057 QUOTA_SYNCHRONIZATION_FAILURE

Description: Quota Synchronization Job Failed

Severity: MAJOR

Help on this Alarm:

When a quota job run during failover or manual (should not be run manually), an error can occur if the cluster returns a create or delete quota error. This is most common when a domain lock from a quota scan blocks quota create API's. Unlinked Everyone quotas can also cause quota create or delete to fail. Use the info text in the running jobs screen to collect the error code and submit a case to Support.

SCA0058 ERROR_RETRIEVING_CLUSTER_VERSION

Description: Error retrieving cluster version.

Severity: MAJOR

Help on this Alarm:

This error occurs when a heartbeat task checks the cluster Onefs version and the api fails. This is commonly seen when a cluster was upgraded to Onefs 8 but the SCA process was not restarted afterwards. This document explains steps needed when a cluster major version from 7 to 8 is completed and how to have Eyeglass detect the new cluster version. [Guide here](#).

SCA0060 ERROR_GENERATING_DATASET

Description: Error generating data sets

Severity: MINOR

Help on this Alarm:

This alarm is raised when the servicenow integration api tries to build a data set that is exposed via an xml url `https://eyeglass ip address/servicenow/servicenow.xml`. This error would occur if not all API data is available to generate the dataset and expose through the xml interface. This does not affect DR functionality and can be ignored if you are not using this feature.

SCA0061 DISCOVERY_RETRIEVAL_ERROR

Description: Failed to retrieve NE data

Severity: MAJOR

Help on this Alarm:

This applies to Unity REST API retrieval failure.

SCA0062 REST_API_ERROR

Description: Failed API REST request

Severity: MAJOR

Help on this Alarm:

This applies to Unity REST API retrieval failure.

SCA0063 POLICY_FAILOVER_CANCEL

Description: Policy Failover Job cancelled

Severity: MAJOR

Help on this Alarm:

In release 2.0 and later, a failover job can be cancelled. This alarm indicates someone cancelled a running failover. The failover log also indicates the failover was cancelled.

NOTE: all recover steps from a failed failover are manual.

SCA0064 ACCESS_ZONE_FAILOVER_CANCEL

Description: Access Zone Failover Job cancelled.

Severity: MAJOR

Help on this Alarm:

In release 2.0 and later a failover job can be canceled. This alarm indicates someone canceled a running failover. The failover log also indicates the failover was canceled.

NOTE: all recover steps from a failed failover are manual.

SCA0065 DFS_FAILOVER_CANCEL

Description: DFS Failover Job cancelled.

Severity: MAJOR

Help on this Alarm:

In release 2.0 and later a failover job can be canceled. This alarm indicates someone canceled a running failover. The failover log also indicates the failover was canceled.

NOTE: all recover steps from a failed failover are manual.

SCA0066 RUNBOOK_ROBOT_JOB_CANCELED

Description: The Runbook Robot job cancelled for job

Severity: MAJOR

Help on this Alarm:

In release 2.0 and later, a failover job can be cancelled. This alarm indicates someone cancelled a running failover. The failover log also indicates the failover was cancelled.

NOTE: All recovery steps from a failed failover are manual.

SCA0067 REHEARSAL_FAILOVER_CANCEL

Description: Rehearsal Failover Job canceled

Severity: MAJOR

Help on this Alarm:

The user has cancelled a DR assistant failover using rehearsal mode. User decision to cancel a running failover can leave the system in an inconsistent state and should never be done without consulting support. Open DR Assistant Running failover and open the failover log to download the failover log. Open a support case for assistance and provide the failover log. DR Rehearsal mode allows a rollback to the previous state on

some failed steps. Start consulting the recovery guide for the state where you left the system. [Guide here](#). Impact: Data Access failure can occur from this alarm.

SCA0068 REHEARSAL_FAILOVER_FAILURE

Description: Rehearsal Failover Job failed

Severity: MAJOR

Help on this Alarm:

The DR rehearsal failover job failed. Open DR Assistant --> running failovers and, download the failover log, find the failed step. Open a support case and attach the failover log and the failed step from the log. Create a support backup archive, upload it to the support site, and update the case that logs have been uploaded. Manual recover steps may be required, and consult the failover recovery guide [here](#). Impact: data access failure can occur from this alarm

SCA0069 POLICY_POOL_MAPPING_ERROR

Description: Error mapping policy to a pool

Severity: MAJOR

Help on this Alarm:

This validation alarm is raised by the DR Readiness process that verifies that each policy in an Access zone has been mapped to an IP pool. This alarm will be raised if the IP pool configuration has been started on an access zone and not completed OR if a new policy is created for an access zone and not yet mapped to a pool. Consult the Access Zone Design guide on IP pool-supported configurations.

SCA0070 DISK_SPACE_FULL_WARNING

Description: Disk usage has reached 75%

Severity: WARNING

Help on this Alarm:

This alarm is raised when disk space on Eyeglass or ECA nodes exceeds 75%, indicating the logs consume more space than required. The logs are configured for circular logging and should not fill the hard disk space. > 75% may indicate another

process consuming space or memory dump files. Open a case with support if you get this alarm.

SCA0071 DISK_SPACE_FULL_ERROR

Description: Disk usage has reached 90%

Severity: CRITICAL

Help on this Alarm:

This alarm is raised when disk space on Eyeglass or ECA nodes exceeds 90%. The VM will likely fail soon if not corrected and will be unable to log or perform normal operations. Open a case immediately with support.

SCA0073 CSM_GROUP_QUOTAS_MANAGER_FAILURE

Description: Saving AD trustees to the database failed

Severity: WARNING

Help on this Alarm:

This error indicates that AD user and membership have failed to be stored in the database. This function is used for Quota creation automation as part of the Cluster Storage Monitor product. Open a support case and upload a support backup.

SCA0074 REHEARSAL_FAILOVER_SUCCEEDED

Description: Rehearsal Failover Job succeeded

Severity: INFORMATIONAL

Help on this Alarm:

A DR rehearsal mode failover has been completed successfully. This alarm indicates that all steps were completed successfully, and data access should be tested. Testing data access guide [here](#). No impact on data access.

SCA0075 ISK_SIZE_MONITOR_ALARM

Description: The Disk Size Monitor has detected that a folder or file(s) exceeded a threshold

Severity: MAJOR

Help on this Alarm:

This indicates the disk space has crossed the threshold, and a support case should be opened to remove unnecessary files. There is no immediate impact unless the disk reaches 100% usage.

SCA0076 DISK_SIZE_MONITOR_INACTIVE

Description: The Disk Size Monitor is inactive

Severity: MAJOR

Help on this Alarm:

This alarm indicates that the monitoring process for disk space is no longer active. Open a support case to get this process restarted. No functional impact other than monitoring is not active.

SCA0077 DISK_SIZE_MONITOR_ERROR

Description: The Disk Size Monitor identified an error

Severity: MAJOR

Help on this Alarm:

The disk monitor process has failed. Open a support case to get this proactive monitoring process fixed. Impact: No functional impact to product functionality other than monitoring of disk usage is not active.

SCA0078 REST_API_CALL_FAILURE

Description: Rest API call failed

Severity: MINOR

Help on this Alarm:

The rest API is used to automate failover tasks; when a rest API call is issued from an external application, a return code of http 200 is sent on a successful API request. This alarm will be raised if an internal error occurs while processing an API request. Open a support case, provide the API call that the application was using, create a support archive and upload to the support site. All of this information will be requested by support to assist with the root cause of the failure.

SCA0079 NEW_POLICY_DISCOVERED

Description: Create a new job for the discovered policy

Severity: INFORMATIONAL

Help on this Alarm:

This alarm means a new synciq policy was discovered and requires the administrator to set the mode and enable the policy to bring this policy into production service within Eyeglass.

SCA0080 UNCONFIGURED_JOB_PRESENT

Description: Unconfigured job present

Severity: MAJOR

Help on this Alarm:

This alarm means a Job in the job icon has a synciq policy in an unconfigured state that requires the administrator to set the mode (auto or DFS or skip config) and then enable the job before this policy is enabled for DR protection.

SCA0081 READINESS_CHECK_WARNINGS

Description: Readiness job execution found warnings

Severity: WARNING

Help on this Alarm:

The failover readiness job detected and a validation warning that affects your failover readiness. Please login to Eyeglass, open the DR Dashboard, review the validation tree

for the failover mode you have configured and expand the tree to find the failed validation. The warning description is available in the DR Dashboard by selecting the validation in the tree and reading the description at the bottom of the window.

SCA0087 SYNCIQ_MONITOR_ERRORS

Description: SyncIQ Monitor Job errors

Severity: MAJOR

Help on this Alarm:

This alarm is raised when the synciq data integrity monitor feature is enabled. This feature creates a test file on the source policy path; each time synciq runs, this file is audited on the target cluster to verify the file was synced correctly to the target cluster. If the file audit fails, this alarm will be raised to warn the administrator that a data sync failed to sync correctly.

SCA0088 ONFIG_BACKUP_JOB_FAILURE

Description: Configuration backup job failed

Severity: WARNING

Help on this Alarm:

The appliance backup zip creation process failed. Please open the jobs icon running jobs to click on the job and review the reason for the failure.

SCA0094 RAM_UNDERSIZED

Description: The RAM Size exceeded the published limits.

Severity: CRITICAL

Help on this Alarm:

The cluster count, object count (smb, nfs, quota), policy count, access zone count or a combination of these requirements additional RAM on the eyeglass vm to maintain support as per the product documentation [here](#). Any use of the product that is below product specifications voids support.

AG0001 AIRGAP_JOB_FAILED

Description: Ransomware Defender AirGap job <JOB_NAME> failed - needs attention

Severity: CRITICAL

Help on this Alarm:

Open a case with support if you get this alarm.

AG0002 AIRGAP_JOB_SUCCEEDED

Description: Ransomware Defender AirGap job <JOB_NAME> succeeded

Severity: INFORMATIONAL

Help on this Alarm:

Each time the Airgap synciq policies run, the Airgap is opened to run the policie. This alarm confirms that the airgap was opened, the sync jobs ran successfully, and the Airgap was closed after the sync jobs finished.

AG0003 AIRGAP_ROUTE_CLOSED

Description: AirGap network is now DISCONNECTED for policy <POLICY_NAME>

Severity: INFORMATIONAL

Help on this Alarm:

This alarm is raised after an Airgap sync job is completed and confirms the Airgap was closed at the end of the sync to the vault.

AG0004 AIRGAP_ROUTE_OPEN

Description: AirGap network is now CONNECTED for policy <POLICY_NAME>

Severity: INFORMATIONAL

Help on this Alarm:

Each time the Airgap jobs execute, the Airgap network is opened. This alarm indicates the network is open before the sync job starts.

AG0005

AIRGAP_JOB_DISABLED_FOR_ACTIVE_EVENT

Description: AirGap job on policy <POLICY_NAME> - cancelled for active RSW event

Severity: WARNING

Help on this Alarm:

Each time a scheduled Airgap sync is scheduled, Ransomware Defender active alarms are checked for any active threat to the production data. The sync and airgap should remain closed to protect the Vault data integrity. This alarm indicates an active threat alarm is raised, and the scheduled data sync will be skipped. The action required when this alarm is raised is for the Ransomware Defender administrator to validate the alarm and clear the alarm. Until active alarms are cleared, no data sync will occur, and each scheduled data sync will generate a new alarm to warn the airgap administrator that no data sync will occur.

AG0006 VAULT_AIRGAP_JOB_FAILED

Description: Vault AirGap job <JOB_NAME> failed - needs attention

Severity: MAJOR

Help on this Alarm:

Open a case with support if you get this alarm.

AG0007 VAULT_AIRGAP_JOB_SUCCEEDED

Description: Vault AirGap job <JOB_NAME> succeeded

Severity: INFORMATIONAL

AG0008 VAULT_OPENED

Description: Vault is opened

Severity: CRITICAL

Help on this Alarm:

This alarm indicates the secure airgap vault is currently open

AG0009

AIRGAP_EVENT_RETRIEVE_JOB_FAILED

Description: Ransomware Defender Event Retriever AirGap job <JOB_NAME> failed - needs attention

Severity: CRITICAL

Help on this Alarm:

Open a case with support if you get this alarm.

AG0010

AIRGAP_EVENT_RETRIEVE_JOB_SUCCEEDED

Description: Ransomware Defender AirGap Event Retriever job <JOB_NAME> succeeded

Severity: INFORMATIONAL

Help on this Alarm:

The alarms were successfully retrieved from the vault cluster.

AG0011 AIRGAP_SCHEDULES_QUERY

Description: Ransomware Defender AirGap Schedules query

Severity: INFORMATIONAL

Help on this Alarm:

This means the Enterprise vault opened the vault and queried Eyeglass for new policies or schedule changes.

AG0012 AIRGAP_JOB_NOT_STARTED

Description: Ransomware Defender AirGap Job did not run according to schedule

Severity: CRITICAL

Help on this Alarm:

Open a case with support if you get this alarm.

AG0013 AIRGAP_JOB_STARTED

Description: Ransomware Defender AirGap Job Started.

Severity: INFORMATIONAL

Help on this Alarm:

This informs you that the airgap job has started execution.

AG0014 AIRGAP_POLICY_CHANGED

Description: AirGap policy changed

Severity: CRITICAL

Help on this Alarm:

This indicates an administrator has modified an airgap policy. This event should be investigated, that this is not a security breach and that the change was approved. The information on this event lists the change that was detected.

RSW0001 RANSOMWARE_DEFENDER_EVENT

Description: Ransomware signal received

Severity: CRITICAL

Help on this Alarm:

This alarm is raised for each security event raised for a user. This should be reviewed in the active events tab of the ransomware defender icon to determine the shares affected or lock-out status for this event. Actions possible are lockout, recover, and initiate self-recovery options.

RSW0002 RANSOMWARE_USER_LOCKED

Description: Locked user access

Severity: CRITICAL

Help on this Alarm:

A user was locked out with a Major or Critical detection security event. Consult the Ransomware defender GUI to identify the user ID, IP address of the machine where the user was logged in. Files affected can be exported to a CSV to inspect and remediate comprised files. The data recovery initiated option can be used to recover files from DR and snapshots. The user can be restored using the restore user access option.

RSW0003 RANSOMWARE_USER_LOCK_FAILURE

Description: Failed to lock user access after ransomware events received

Severity: CRITICAL

Help on this Alarm:

A lock of a user account was not successful, consult the log for the action menu to see which shares or clusters the lockout job failed. This indicates these shares are not locked out for this user and manual lockout of the share for the affected user should be done. The lockout is not retried. It can be retried from the actions menu.

RSW0004 RANSOMWARE_ECA_IGLS_SERVICE_FAILURE

Description: ECA Service not forwarding all security events

Severity: MAJOR

Help on this Alarm:

One or more nodes on an ECA cluster are not successfully communicating with the Eyeglass appliance. Click on the Manage Services icon on the Eyeglass desktop, and use the status of each ECA node and its subcomponents to determine which ECA node is unhealthy.

RSW0005 RANSOMWARE_ECA_HBASE_FAILURE

Description: ECA Service not scanning Hbase for events

Severity: MAJOR

Help on this Alarm:

If the alarm in SCA0064 is raised, Eyeglass will attempt to scan the ransomware signals database for new signals periodically. If this scanning cannot happen, this alarm will be raised. To resolve: restore Eyeglass to Hbase connectivity.

RSW0006 RANSOMWARE_ECA_COMM_FAILURE

Description: ECA Service is unreachable to scan for events

Severity: MAJOR

Help on this Alarm:

The Eyeglass VM cannot reach the ECA cluster to scan the analytics database. This impacts the detection of Ransomware events. This should be fixed, and look at networking and ecactl CLI commands in the ransomware admin guide for troubleshooting.

RSW0008 RANSOMWARE_ENTER_MONITOR_MODE

Description: Ransomware: Entered monitor-only mode

Severity: MAJOR

Help on this Alarm:

When the Eyeglass Ransomware settings have monitor mode enabled no lockout will occur. This alarm is a reminder that no data protection is enabled with monitor mode.

RSW0009 RANSOMWARE_LEAVE_MONITOR_MODE

Description: Ransomware: Left monitor-only mode

Severity: MAJOR

Help on this Alarm:

When the Eyeglass Ransomware Defender setting disables monitor mode, this alarm indicates that data protection monitoring is now active.

RSW0010 RANSOMWARE_ECA_VERSION

Description: Ransomware: ECA node version does not match the Eyeglass version

Severity: MAJOR

Help on this Alarm:

If the ECA cluster version does not match the Eyeglass version this alarm is raised. The versions should match and upgrades should be completed to match ECA and Eyeglass versions.

RSW0011 RSW_RESTORE_ACCESS_SUCCESS

Description: User access restored

Severity: INFORMATIONAL

Help on this Alarm:

The user's permissions on the security event were restored for all shares with a lockout. Check the security event history to verify the list of shares.

RSW0012 RSW_RESTORE_ACCESS_FAILED

Description: Failed to restore user access

Severity: CRITICAL

Help on this Alarm:

The user's permissions on the security event were not all restored. Open the security event history to review the list of shares that were not successfully restored and manually edit the share permissions to remove the deny read permission for the user named in the security event.

RSW0013 RSW_SNAPSHOT_WARNING

Description: Not all snapshots were created

Severity: CRITICAL

Help on this Alarm:

This alarm is raised by the Ransomware defender when a snapshot creation failed on one or more shares detected as part of a security event for a user. The Active security event tab should be checked, and review the list of shares for the security event and compare to the snapshot list column to see which cluster or path does not have a snapshot created. Also open job icon, running jobs tab and find the snapshot created job and find the cluster and path that failed to create the snapshot.

Alternative open is select security action menu and run Create Snapshot to retry the snapshot created again.

Possible reasons for failure: licensing on PowerScale, eyeglass service account snapshot create permission is missing (fix by adding snapshot create permission to the eyeglass service account).

RSW0014 RSW_SNAPSHOT_FAILED

Description: Failed to create snapshots

Severity: CRITICAL

Help on this Alarm:

See the explanation on alarm SCA0075 for details and steps to attempt another snapshot creation or debug the issue.

RSW0015

RSW_SNAPSHOT_DELETE_WARNING

Description: Not all snapshots were deleted

Severity: MAJOR

Help on this Alarm:

It indicates a security event snapshot was attempted to be deleted from the GUI but failed.

Snapshots are applied on a security event and have an expiry of 48 hours. If you want to delete the snapshot from the Ransomware Defender security event action menu sooner, it fails with this error code. Check eyeglass role permissions are set correctly.

RSW0016 RSW_SNAPSHOT_DELETE_FAILED

Description: Failed to delete snapshots

Severity: MAJOR

Help on this Alarm:

See the explanation for SCA0077.

RSW0017 HBASE_UPGRADE_FAILURE

Description: HBASE upgrade failed.

Severity: INFORMATIONAL

Help on this Alarm:

The Database stored on the PowerScale upgrade failed to complete. Contact support.

RSW0018 RANSOMWARE_DEFENDER_UNDER_LICENSED

Description: The Ransomware Defender is under-licensed

Severity: MAJOR

Help on this Alarm:

This alarm will be raised when Eyeglass has more licenses and clusters added than the Ransomware agent license installed. Each monitored cluster requires an agent license. Contact sales@superna.net to get a quote for agent licenses.

RSW0020 BACKUP_INGESTION_FAILURE

Description: Turboaudit backup ingestion failed.

Severity: WARNING

Help on this Alarm:

This error means the historical event ingestion did not process all files. Please open a support case for instructions to resolve this.

RSW0021 SECURITY_EVENT_FAILED

Description: Security Event Received but Failed to Process

Severity: CRITICAL

Help on this Alarm:

The Ransomware Defender or Easy Auditor products use the ECA cluster to process audit events. When a security event is detected, a REST message is sent to Eyeglass to process the event. This error indicates Eyeglass received a security event but could not connect to the ECA cluster to retrieve specifics about the event. This is a critical event indicated networking or reachability between Eyeglass and ECA cluster. This should be debugged immediately as it is possible that now security events will be reported in Eyeglass UI or process with automated response actions until corrected.

RSW0022 SECURITY_EVENT_RETURNED_ZERO

Description: Security event received but failed to return affected file list

Severity: MAJOR

Help on this Alarm:

This alarm indicates a high rate of false positive detections and requires a support case to adjust settings.

RSW0024 SECURITY_GUARD_FAILURE

Description: Ransomware: Security Guard Failure

Severity: MAJOR

Help on this Alarm:

The security if configured, runs on a schedule and failure should be checked from the logs on the Ransomware defender icon, Security guard tab and open the last log to check which step failed. This feature tests your defenses are active and functioning as expected. This should be corrected and using service manager icon to verify the ECA is reachable and healthy. Check the cluster igls-honey pot share exists. Check other alarms in the alarms icon to verify the cluster(s) managed by the security guard feature can be reached.

NOTE: SMB open port is required from Eyeglass to the PowerScale clusters under management.

RSW0025 RANSOMWARE_WARNING_ERROR

Description: Warning or Error

Severity: CRITICAL

Help on this Alarm:

Please contact support.

RSW0026

TURBOAUDIT_EVENTRATE_BELOW_THRESHOLD_WARNING

Description: String.format: Event rate for all TurboAudit nodes over the last %d minute(s) is below %d

Severity: WARNING

Help on this Alarm:

Check the NFS mount for audit data ingestion.

RSW0027

EVTARCHIVE_EVENTRATE_BELOW_THRESH OLD_WARNING

Description: String.format: Event rate for all EvtArchive nodes over the last %d minute(s) is below %d

Severity: WARNING

RSW0028 SECURITY_GUARD_SUCCESS

Description: Ransomware: Security Guard Success

Severity: INFORMATIONAL

Help on this Alarm:

The security, if configured, runs on a schedule and simulates a Ransomware attack on a daily basis to validate that all components, including alerting and lockout of user sessions are functioning. This alarm confirms that the security guard job was completed successfully and your defences are active and functioning as expected.

RSW0029

CYBER_RECOVERY_MANAGER_JOB_ERROR

Description: There was an error recovering files for Cyber Recovery Manager

Severity: WARNING

Help on this Alarm:

Check Cyber Recovery Job details in the Job Window to see which files failed and why.

EAU0002 AUDITOR_REPORT_FAILURE

Description: Auditor report failed

Severity: CRITICAL

Help on this Alarm:

A running report job failed. Open the Easy Auditor icon, click on running reports and expand to locate the error. Restart the report, and if it fails again, open a support case.

EAU0003 EVENT_AUDIT_TIME_SKEW_ERROR

Description: Time skew between the last consumed and the last logged audit event is too great

Severity: MAJOR

Help on this Alarm:

This alarm condition monitors the PowerScale nodes last logged audit events versus the last event processed by the ECA cluster. To ensure real-time monitoring and searching current audit data, this gap in time should be as low as possible. This alarm is raised when the gap is widening between auditing and consuming audit events and is an indication that cluster resources CPU should be increased to allow audit event processing to increase. Audit event ingestion is also limited on ECA clusters and this value can be configured to allow higher event rates to be processed. Contact support if you receive this alarm.

EAU0004 TIME_SKEW_ERROR

Description: Time skew between the Eyeglass Clustered Agent and the Eyeglass Appliance is too great

Severity: WARNING

Help on this Alarm:

This alarm indicates the time has drifted between the ECA cluster nodes and Eyeglass. Accurate time is required between all the nodes and between the Eyeglass and the ECA nodes.

EAU0005 NO_SMART_QUOTA_FOR_DLP_PATH

Description: There is no smart quota for a path limited by a Data Loss Prevention threat detector

Severity: MAJOR

Help on this Alarm:

The data loss prevention feature in Easy Auditor uses a quota to detect space used on a monitored path. This is required to compute a data copy by users greater than the threshold set on the path. No quota means the DLP trigger is disabled until the quota can be created. The quota is created automatically and this alarm indicates the API call failed to create the quota. Impact the DLP trigger is not active.

EAU0006 AUDITOR_REPORT_SUCCESS

Description: Easy Auditor Report job succeeded

Severity: INFORMATIONAL

Help on this Alarm:

This indicates an audit report has been completed by and audit administrator action in the Easy Auditor GUI or a scheduled search has been completed.

EAU0007 ACTIVE_AUDITOR_EVENT

Description: Active Auditor event received.

Severity: CRITICAL

Help on this Alarm:

This alarm indicates an automated security policy in Easy Auditor has crossed a defined policy limit and raised a security event too be reviewed by a security administrator.

EAU0008 ROBO_AUDIT_FAILURE

Description: Robo Audit Failed

Severity: CRITICAL

Help on this Alarm:

The RoboAudit schedule health check failed to find all the events created by the RoboAudit service account. Login to Eyeglass, open Easy Auditor, select RobotAudit on

the menu and open the last log that indicates failed. Download the log, open a support case and attach the log and A full support backup to have support review your environment.

EAU0009 ROBO_AUDIT_SUCCESS

Description: Robo Audit Succeeded

Severity: INFORMATIONAL

Help on this Alarm:

This Alarm confirms that the RoboAudit schedule health check completed successfully and the audit data is being processed and stored.

ECA0001 ECA_SERVICE_INFO

Description: Eyeglass Clustered Agent information

Severity: INFORMATIONAL

ECA0002 ECA_CRITICAL_ERROR

Description: Eyeglass Clustered Agent unexpected error

Severity: CRITICAL

Help on this Alarm:

The clustered Agent has an error that requires support logs to investigate. Please open a support case.

ECA0003 ECA_SERVICE_WARNING

Description: Eyeglass Clustered Agent warning

Severity: WARNING

Help on this Alarm:

The Eyeglass clustered agent has a warning state component, which can impact the operational state. Open the managed service icon to identify the warning and the

component name. Open a support case and identify the component name and error in managed services for procedures to resolve.

ECA0004 ECA_MINOR_ERROR

Description: Eyeglass Clustered Agent unexpected minor error

Severity: MINOR

Help on this Alarm:

The Eyeglass clustered agent has a component in a minor errored state; this will not negatively affect operations. Open the managed service icon to identify the warning and the component name. Open a support case and identify the component name and error in managed services for procedures to resolve.

ECA0005 ECA_MAJOR_ERROR

Description: Eyeglass Clustered Agent unexpected major error

Severity: MAJOR

Help on this Alarm:

The Eyeglass clustered agent has a component in major errored state, this will negatively affect operations. Open the managed service icon to identify the warning and the component name. Open a support case and identify the component name and error in managed services for procedures to resolve.

NOTE: You have this alarm text that states "Eyeglass Clustered Agent unexpected major error". and the information text says

```
{"info":"Turboaudit is lagging behind 1396 seconds processing events.", "service":"Turboaudit Lag Monitor", "severity":"MAJOR", "source":"ecapdcl2_2"}
```

This means ingestion of audit data is slowing down due to the build up or archive gz audit files on the cluster. This can be address with 1 of two options

1. Using 9.2 or later Onefs enable the prune old GZ archived files to save space on the cluster and set prune settings to the number of days to retain gz files. **NOTE:** gz files contain historicaly audit data that can be deleted, if you require long term storage of audit data you most follow Dell procedure to move GZ files to alternate location from the default location under /ifs/.ifsvar Open a Dell SR for the procedure to move old GZ files to long term storage location.

- a. **NOTE:** Easy Auditor customers have a long term copy of the GZ data in the Archive database already and can purge old GZ files. Recommended to keep 6 months of GZ files
 2. To keep GZ files in place on the cluster you can enable REST API NFSv4 audit data ingestion. **NOTE:** keeping gz files in place has no value, the isi_audit_viewer command cannot read through any useful number of GZ files and there is no reason to keep GZ files and they should be archived using option 1 above.
 - a. Install Guide on how to configure REST API mode that removes the requirement to remove the GZ files. See point above, there is no reason or purpose to keep them, they are not usable for any purpose. [See Guide](#).
-

ECA0006 ECA_FATAL_ERROR

Description: Eyeglass Clustered Agent unexpected fatal error

Severity: FATAL

Help on this Alarm:

The Eyeglass clustered agent has a component in crashed state, this will negatively affect operations. Open the managed service icon to identify the warning and the component name. Open a support case and identify the component name and error in managed services for procedures to resolve.

NOTE: You have this alarm text that states "Eyeglass Clustered Agent unexpected major error. and the information text says

```
{"info":"Turboaudit is lagging behind 1396 seconds processing events.", "service":"Turboaudit Lag Monitor", "severity":"MAJOR", "source":"ecapdcl2_2"}
```

This means ingestion of audit data is slowing down due to the build up or archive gz audit files on the cluster. This can be address with 1 of two options

1. Using 9.2 or later Onefs enable the prune old GZ archived files to save space on the cluster and set prune settings to the number of days to retain gz files. **NOTE:** gz files contain historicaly audit data that can be deleted, if you require long term storage of audit data you most follow Dell procedure to move GZ files to alternate location from the default location under /ifs/.ifsvvar Open a Dell SR for the procedure to move old GZ files to long term storage location.
 - a. **NOTE:** Easy Auditor customers have a long term copy of the GZ data in the Archive database already and can purge old GZ files. Recommended to keep 6 months of GZ files

2. To keep GZ files in place on the cluster you can enable REST API NFSv4 audit data ingestion. **NOTE:** keeping gz files in place has no value, the `isi_audit_viewer` command cannot read through any useful number of GZ files and there is no reason to keep GZ files and they should be archived using option 1 above.
 - a. Install Guide on how to configure REST API mode that removes the requirement to remove the GZ files. See point above, there is no reason or purpose to keep them, they are not usable for any purpose. [See Guide](#).

ECA0007 ECA_NODE_FAILURE

Description: ECA Node inactive or in error state

Severity: MAJOR

Help on this Alarm:

An ECA cluster node has stopped sending alive heartbeats to the eyeglass VM. The ECA cluster is now in a degraded state until the node is fixed. See the admin guide on steps to login to the node and check services and container health.

ES0001 ES_NODE_COUNT_VIOLATION

Description: Node count limitation has been exceeded for the application Eyeglass Search

Severity: CRITICAL

Help on this Alarm:

This alarm indicates a license violation based on the PowerScale node count and the installed license keys for the Eyeglass Search product. This affects your appliance access to support in this state. Please open a case with support for the next steps.

ES001

Description: Eyeglass Search - Trace Notification

Help on this Alarm:

Debug level messages.

ES002

Description: Eyeglass Search - Informational Notification

Help on this Alarm:

Not an error, indicates a task completed.

ES003

Description: Eyeglass Search - Warning Notification

Help on this Alarm:

Warning condition on a task.

ES004

Description: Eyeglass Search - Minor Notification

Help on this Alarm:

An alarm that has a minor functional impact.

ES005

Description: Eyeglass Search - Major Notification

Help on this Alarm:

Functional impact.

ES006

Description: Critical error in the Eyeglass Search subsystem

Help on this Alarm:

Product functionality impacted alarm.

ES007

Description: Successfully initialized module

Help on this Alarm:

Low-impact state change.

ES008

Description: Failed to initialize module

Help on this Alarm:

The module could not start a task.

ES009

Description: Consecutive service failure

Help on this Alarm:

A repeating failure condition.

ES010

Description: Retrieved subsystem successfully

ES011

Description: Created subsystem successfully

ES012

Description: Deleted subsystem successfully

ES013

Description: Modified subsystem successfully

ES014

Description: Failed to retrieve subsystem

ES015

Description: Failed to create a subsystem

ES016

Description: Failed to delete subsystem

ES017

Description: Failed to modify subsystem

ES018

Description: Added configuration successfully

ES019

Description: Deleted configuration successfully

ES020

Description: Modified configuration successfully

ES021

Description: Job started successfully

ES022

Description: Job completed successfully

ES023

Description: Job failed to run

ES024

Description: Login successful

ES025

Description: Login failed. Case

DRSDEGE0001

DRSDEGE_NODE_COUNT_VIOLATION

Description: The node count limitation has been exceeded for the application DRSDEdge

Severity: CRITICAL

Help on this Alarm:

The PowerScaleSD clusters added to Eyeglass exceed the license key count for PowerScaleSD clusters. Please open a support case to determine the next steps and impact on your environment.

SETUP0001 SETUP_REDISCOVER_REQUEST

Description: Database is in a corrupt, unrepairable state. Please schedule a time to execute a rediscover operation (igls appliance rediscover)

Severity: CRITICAL

Help on this Alarm:

The alarm is issued during inventory updates in the database if this process fails. Eyeglass will attempt to correct any failure in the process, but at times, this is impossible; for example, if eyeglass is shut down incorrectly or hard powered off - both operations can result in database content becoming corrupt. The database can be rebuilt with the cli command `igls appliance rediscover`. This command will delete the database and rebuild from API calls to the cluster. This operation is safe to run to rebuild the database. If this error occurs more than once, open a support case with the error code and upload support logs.

Impact: blocking saves to the database impacts failover readiness validations from completing and will not allow an accurate view of DR readiness until addressed.

SETUP0002 SETUP_INVENTORY_DUPLICATE S_CRITICAL

Description: Duplicate inventory found (please see alarm info); inventory not saved to the database as requested in file system.xml (tag manageinventoryduplicates). Please correct this manually on your cluster or set the tag to 'DELETE' to allow the system to ignore those entries

Severity: CRITICAL

Help on this Alarm:

This alarm indicates duplicate cluster object detected which blocks saving to the database. This is normally an issue with cluster configuration that should be fixed on the cluster. Open a support case to identify the corrupt cluster configuration data. A workaround option that allows duplicates to be removed before saving is available in the system.xml file. Consult with support to apply this setting. Impact: blocking saves to the database impacts failover readiness validations from completing and will not allow an accurate view of DR readiness until addressed.

SETUP0003 SETUP_INVENTORY_DUPLICATE S_WARNING

Description: Duplicate inventory found (please see alarm info); duplicate inventory has been ignored, and data is saved to the database. Please correct this manually on your cluster

Severity: WARNING

Help on this Alarm:

This alarm indicates duplicated data was detected by removing it before saving it to the database. This means the duplicate skip flag is set in system.xml to continue to save to the database after removing duplicate inventory data. Duplicate inventory indicates an issue with the cluster configuration data that should be fixed on the cluster. Duplicates can be synciq policy objects, share permissions and other configuration data; this should be fixed on the cluster. Impact: no functional impact to eyeglass functions; this alarm indicates an issue was found on the cluster configuration data.

LM0001 LM_LICENSE_TO_EXPIRE

Description: License(s) to expire

Severity: WARNING

Help on this Alarm:

This means the support license will expire soon, and a renewal order is required.

LM0002 LM_LICENSE_HAS_EXPIRED

Description: License(s) expired

Severity: MAJOR

Help on this Alarm:

This alarm indicates that maintenance has expired, and access to support and software will not be possible until the new key is replaced.

© Superna Inc