WHITE PAPER

FILE SYSTEM AUDITING WITH DELL EMC POWERSCALE AND DELL EMC COMMON EVENT ENABLER

Abstract

This white paper outlines best practices to configure a File System Audit solution in an SMB or NFS environment with Dell EMC PowerScale & Common Event
Enabler (CEE).

May 2020

Document ID

Revisions

Date	Description
March 2019	Initial release
Dec 2019	Update the detailed audit event
May 2020	Update OneFS 9.0.0
Sept 2020	Update OneFS 9.1.0.0

Acknowledgements

This paper was produced by the following:

Author: Vincent.Shen@dell.com

Support:

Other:

Acknowledgements

Table of contents

Executive summary

1.1 Overview

Information technology auditors are faced with rapidly growing unstructured data in their data centers, including sensitive information such as intellectual property, confidential customer or employee data, and proprietary company records. The need to audit unstructured data to keep company proprietary information secure, as well as the need to comply with governmental regulations, drives the need for business-critical audit capabilities.

Auditing can detect many potential sources of data loss, including fraudulent activities, inappropriate entitlements, unauthorized access attempts, and a range of other anomalies that are indicators of risk. Customers in industries such as financial services, health care, life sciences, and media and entertainment, as well as in governmental agencies, must meet stringent regulatory requirements developed to protect against these sources of data loss.

Table 1 Regulatory requirements

Segment	Key business drivers
Financial services	Compliance requirements for the Sarbanes-Oxley Act (SOX)
Health care	Compliance requirements for the Health Insurance Portability and Accountability Act (HIPAA) 21 CFR (Part 11)
Life sciences	Compliance requirements for the Genetic Information Non-Discrimination Act (GINA)
Media and entertainment	Security requirements for Motion Picture Association of America (MPAA) content movement
Federal agencies	Security requirements for Security Technical Information Guide (STIG)/Federal Information Security Management Act (FISMA)

Depending on the regulation requirements, auditing file system operations, such as file creation or deletion, is required to demonstrate compliance with chain of custody. In other scenarios, the goal of auditing is to track configuration changes to the storage system. Lastly, auditing needs to track activities such as logon/logoff events, which may not involve file data or configuration changes. The audit enhancements included in Dell EMC® PowerScale® OneFS® 8.0 addresses these needs for SMB, NFS and HDFS workflows and PowerScale cluster configuration changes

1.2 Document purpose

This white paper provides configuration considerations and best practices of PowerScale OneFS Audit including:

- Audit architecture
- Audit requirement
- Audit management configuration and considerations including
  - Configure audit settings through OneFS WebUI and CLI
  - Configure audit Dell EMC Common Event Enabler (CEE) event forwarding
  - Audit syslog forwarding

- Audit log progress check
- Audit log time adjustment
- Audit event delivery rate statistics

1.3 Audience

This guide is intended for experienced system and storage administrators who are familiar with file services and network storage administration.

This guide assumes you have a working knowledge of the following:

- Network-attached Storage (NAS) systems
- Audit 3rd party applications
- Dell EMC Common Event Enabler
- The PowerScale scale-out storage architecture and the PowerScale OneFS operating system

You should also be familiar with PowerScale documentation resources, including:

- EMC Community Network (ECN) info hubs
- DELL EMC OneFS release notes, which are available on the Dell EMC support network and contain important information about resolved and known issues.
- Dell EMC PowerScale OneFS Best Practices

1.4 We value your feedback

Dell EMC and the authors of this document welcome your feedback on the whitepaper.

Authors: Vincent Shen (Vincent.shen@dell.com)

2 Audit configuration consideration

2.1 PowerScale OneFS audit overview

PowerScale OneFS can audit system configuration events, SMB, NFS, and HDFS protocol access events on the PowerScale cluster. All audit data is stored in files called audit topics, which collect log information that can be further processed by auditing tools. System configuration auditing is either enabled or disabled; no additional configuration is required. If configuration auditing is enabled, all configuration events that are handled by the application programming interface (API) are tracked and recorded in the configuration audit topic. Configuration events will not be forwarded to the Dell EMC Common Event Enabler (CEE). SMB, NFS and HDFS protocol events can be audited. If protocol auditing is enabled, file access events through the SMB, NFS, and HDFS are recorded in the protocol audit topic. The protocol audit topic is consumable by auditing applications that support the Common Event Enabler, which provides integration with auditing applications such as Varonis® DatAdvantage®, STEALTHbits StealthAUDIT®, Symantec Data Insight®, and Dell Change Auditor for Dell EMC®.

2.2 Audit architecture

Starting with OneFS 7.1, a likewise input/output (LWIO) filter manager was created. The filter manager provides a plug-in framework for pre- and post-input/output request packet (IRP). The IRP provides the mechanism to encode a protocol request handled by LWIO and encodes the request handled by the file system drivers.

Audit events are processed after the kernel has serviced the IRP. If the IRP involves a configured audit event for an Access Zone where auditing is enabled, an audit payload is created.

The audit events are logged on the individual nodes where the SMB/NFS client initiated the activity. The events are then stored in a binary file under /ifs/.ifsvar/audit/logs. The logs automatically roll over to a new file once the size reaches 1 GB. The default protection for the audit log files is +3. Given various regulatory requirements, such as HIPAA, which require two years of audit logs, the audit log files are not deleted from the cluster.

Starting in OneFS 7.1.1, audit logs are automatically compressed. Audit logs are compressed on file roll over. As part of the audit log roll over, a new audit log file is actively written to, while the previous log file is compressed. The estimated space savings for the audit logs is 90%.

Once the auditing event has been logged, a CEE forwarder service handles forwarding the event to CEE. The event is forwarded via an HTTP PUT operation.

At this point, CEE will forward the audit event to a defined endpoint, such as Varonis DatAdvantage. The audit events are coalesced by the 3rd Party audit application.

OneFS 7.1.1 added the ability to forward config and protocol auditing events to a syslog server. By default, syslog forwarding will write the events to /var/log/audit_protocol.log for protocol auditing events and /var/log/audit_config for configuration auditing events.

OneFS 8.0.1 adds the support for concurrent delivery to multiple CEE servers. Each node initiates 20 HTTP 1.1 connections across a subset of CEE servers. Each node can choose up to 5 CEE servers for delivery. The HTTP connections are evenly balanced across the CEE servers from each node. The change results in increased audit performance.

Starting from OneFS 8.2.0, OneFS protocol audit events have been improved to allow for more control of what protocol activity should be audited. It provides a granular way to select protocol audit events to stop collecting unneeded audit events that 3rd party applications do not register for. The changes allow for increased performance and efficiency by allowing customers to configure OneFS to no longer collect audit events their auditing application does not register for.

2.3 Audit requirements

Refer to Table 2 for the details on PowerScale and CEE requirements:

Table 2 PowerScale and CEE requirements

Audit requirement	Audit requirement details
PowerScale OneFS software	• OneFS 7.1 or later
PowerScale OneFS role-based access	• Root or Admin account • Account with ISI_PRIV_AUDIT privilege
Dell EMC CEE	• CEE 6.6.0 or later

Refer to Table 3 for the 3rd party software requirements:

Table 3 3rd party software requirements

3rd party software	3rd party software requirements
Varonis DatAdvantage	• DatAdvantage versions 5.8.80.x and later • Microsoft SQL Server
Symantec Data Insight	• Symantec Data Insight 4.5 and later • Microsoft .Net Framework version 3 or 3.5 on Collector Node • DataInsightCelerra service is installed on Data Insight Collector
STEALTHbits StealthAUDIT	• STEALTHbits StealthAUDIT • StealthAUDIT Management Platform • FSAA 6.2.313.0 • STEALTHbits File Monitoring Service • Microsoft SQL Server

2.4 Audit management

2.4.1 Manage audit setting with OneFS WebUI

To enable protocol auditing in the OneFS WebUI, refer to the steps below:

1. Select “Cluster Management”
2. Select “Auditing”
3. Click “Enable Protocol Access Auditing”
4. Add Access Zone(s) that need to be audited
5. In the Event Forwarding Section, enter the uniform resource identifier (URI) for the server where the CEE stays. The format for the entry will be: http://FQDN:port/cee and 12228 is the default CEE HTTP listen port.
   For example http://cee.example.com:12228/cee
6. Hostname – Storage cluster name

Note: Hostname is required only if needed by 3rd party audit application and it should match the name used to define the file server in the auditing application.

2.4.2 Manage audit setting with CLI

To enable protocol auditing, refer the following CLI command:

```
isi audit settings global modify --protocol-auditing-enabled on
```

To disable protocol auditing, refer the following CLI command:

```
isi audit settings global modify --protocol-auditing-enabled off
```

To add access zone to Audit, use the following CLI command:

```
isi audit settings global modify --audited-zones <ZONE>
```

To view the audit settings:

```
#isi audit settings global view
Protocol Auditing Enabled: No
Audited Zones: System
CEE Server URIs: http://cee.example.com:12228/cee
Hostname: cluster.example.com
Config Auditing Enabled: Yes
Config Syslog Enabled: Yes
Config Syslog Servers: -
Protocol Syslog Servers: -
```

2.4.3 Granular audit selection

Before 8.2.0 auditing could be configured to collect only a subset of events but not directly to match the events the auditing application needed. This resulted in collecting unneeded audit events.

The new audit events in OneFS 8.2.0 allow for collecting just the events needed. It is still required for the customer to correctly enable the events they need for their auditing application. If the customer enables everything the same number of events will be collected and sent off the cluster. This will bring the following benefits:

1. Lower storage footprint
2. Better performance

Audit collects events are re-designed and implemented at a more granular level in OneFS 8.2. The new events in OneFS 8.2.0 and their mapping relationship with the ones in the previous OneFS version are listed in Table 4.

Table 4 Audit events in OneFS 8.2.0 and the previous version

Audit events prior to OneFS 8.2.0	**Audit events in OneFS 8.2.0**
open	• open_directory, • open_file, • open_file_noaccess, • open_file_read, • open_file_write • create_directory, • create_file
close	• close_directory, • close_file, • close_file_modified, • close_file_unmodified
delete	• delete_directory, • delete_file
read	• read_file
write	• write_file
rename	• rename_directory, • rename_file
get_security	• get_security_directory, • get_security_file
set_security	• set_security_directory, • set_security_file
logon	• logon
logoff	• logoff
tree_connect	• tree_connect

Protocol audit events are configurable at CEE granularity with each OneFS event mapping to a CEE event. This 1:1 mapping relationship is shown in Table 5.

Table 5 Map between CEE events and OneFS events in 8.2.0

Audit events in OneFS 8.2.0	CEE events	Description
create_file	CEPP_CREATE_FILE	Send a notification when a file is created.
create_directory	CEPP_CREATE_DIRECTORY	Send a notification when a directory is created.
open_file_write	CEPP_OPEN_FILE_WRITE	Send a notification when a file is opened for write access.
open_file_read	CEPP_OPEN_FILE_READ	Send a notification when a file is opened for read access.
open_file_noaccess	CEPP_OPEN_FILE_NOACCESS	Send a notification when a file is opened for a change other than read or write access (for example, read or write attributes on the file)
open_directory	CEPP_OPEN_DIRECTORY	Send a notification when a directory is opened.
close_file_modified	CEPP_CLOSE_MODIFIED	Send a notification when a file is changed before closing.
close_file_unmodified	CEPP_CLOSE_UNMODIFIED	Send a notification when a file is not changed before closing.
close_directory	CEPP_CLOSE_DIRECTORY	Send a notification when a directory is closed
delete_file	CEPP_DELETE_FILE	Send a notification when a file is deleted.
delete_directory	CEPP_DELETE_DIRECTORY	Send a notification when a directory is deleted.
rename_file	CEPP_RENAME_FILE	Send a notification when a file is renamed.
rename_directory	CEPP_RENAME_DIRECTORY	Send a notification when a directory is renamed.
write_file	CEPP_WRITE_FILE	Send a notification when a file write is received.
read_file	CEPP_FILE_READ	Send a notification when a file read is received.
set_security_file	CEPP_SETACL_FILE	Send a notification when a file security change is received.
set_security_directory	CEPP_SETACL_DIRECTORY	Send a notification when a directory security change is received.

logon	N/A	Send a notification when an SMB session is established.
Logoff	N/A	Send a notification when there is an SMB session logoff.
tree_connect	N/A	Send a notification when there is a first attempt to access an SMB share.

For the OneFS version prior to OneFS 8.2.0, refer to OneFS to Dell EMC CEE event map in Appendix B.

The new audit events in OneFS 8.2.0 are referred as `detailType` within the event payload. The following is an example to compare the payload for the same audit event in different OneFS versions. The payload for OneFS 8.2.0 audit feature contains everything the previous version has, which means auditing is backward compatible with previous audit events.

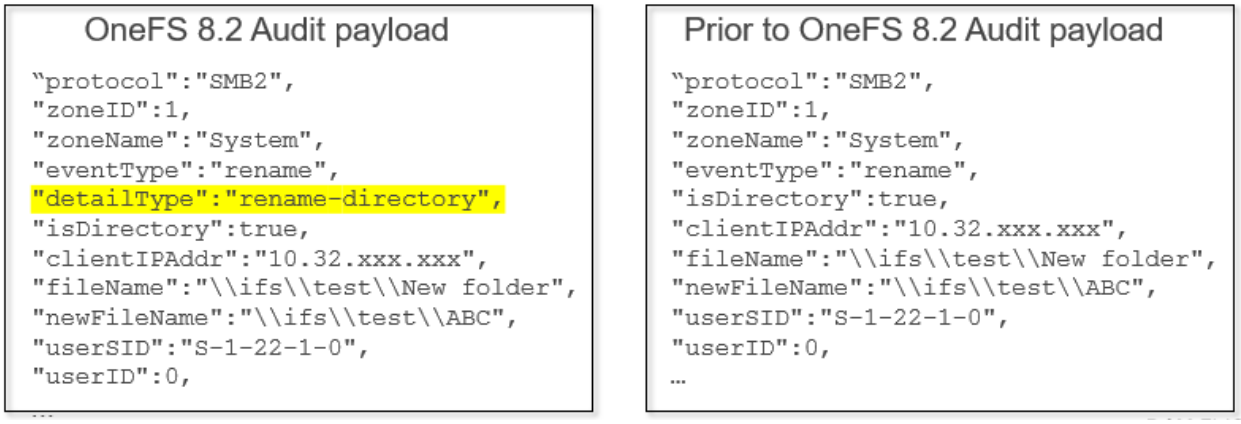

Figure 1 Audit payload

The CLI for audit fully supports these granular event type as the parameter.

2.4.4 Configure Dell EMC CEE event forwarding

The CEE needs to be configured with an audit endpoint to forward events. The CEE configuration changes are performed using Windows Registry Editor (regedit):

1. Open the registry (select "`Start > Run > regedit`").
2. Locate the following key: `HKLM\Software\EMC\CEE\CEPP\Audit\Configuration`.
3. Enable audit by setting the registry key – `Enabled` to 1 (REG_DWORD)

```
[HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE\CEPP\Audit\Configuration] Enabled =
(REG_DWORD) 0x00000001
```

4. Edit the endpoint string value as shown in Table 6:

Table 6 Configuration on CEE event forwarding

3rd audit application	**Configuration on CEE event forwarding**

Varonis DatAdvantage	• If the Varonis Probe is installed on the same machine, set the value to `Varonis`. • If the Varonis Probe is installed on another machine, set the value to `Varonis@<ProbeIP>`, where `<ProbeIP>` is the IP address of the Varonis Probe server.
STEALTHbits StealhAUDIT	• Set Value to SteathAUDIT
Symantec Data Insight	• Set Value to SymantecDataConnector

5. Restart Dell EMC Celerra® Antivirus Agent (CAVA) service by the following command:

```
net stop "emc cava"
net start "emc cava"
```

The followings show an example of adding a local endpoint for Varonis DatAdvantage:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE\CEPP\Audit\Configuration] EndPoint = (REG_SZ)
Varonis
```

The followings show an example of adding a remote endpoint for Varonis DatAdvantage:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE\CEPP\Audit\Configuration] EndPoint = (REG_SZ)
Varonis@10.aaa.xxx.yyy
```

The followings show an example of adding multiple remote endpoints for Varonis DatAdvantage:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE\CEPP\Audit\Configuration] EndPoint = (REG_SZ)
Varonis@192.168.22.3;Varonis@192.168.33.2
```

2.4.5 Configuration of audit syslog forwarding

To configure the audit syslog forwarding, use the following steps:

1. Enable forwarding of system configuration changes to syslog by running the following command:

```
isi audit settings global modify –config-syslog-enabled=true
```

2. Run the following command to back up the `/etc/mcp/templates/syslog.conf` file:

```
cp /etc/mcp/templates/syslog.conf /etc/mcp/templates/syslog.conf.bku1
```

3. Open the `/etc/mcp/templates/syslog.conf` file in a text editor. Add a line to identify which syslog events to forward. Add the line between the `cevents.*` line and the `# ARRAY_MACHINES` line. The line you add should be in the following format:

```
<list of events to forward> @<hostname/IP address>
```

The following line is an example. The syslog events that are listed here are the default events that you would get if you used Method 1 above. You can add additional filter options.

```
*.warn;*.notice;kern.*;ifs.info;istat.none @172.16.0.1
```

Note: A filter of *.* will generate a lot of traffic.

An example of the syslog.conf file showing where to add the line is as follows:

```
...
ifsidi.*                                          /var/log/idi.log
ifssnap.*                                         /var/log/isi_snapshot_d.log
ifssstore.*                                       /var/log/isi_sstore.log
cevents.*                                         /var/log/isi_celog_events.log
*.warn;*.notice;kern.*;ifs.info;istat.none @172.16.0.1
# ARRAY_MACHINES
security.*                                        /var/log/security
mail.info                                         /var/log/maillog
...
```

4. To enable remote syslog for configuration or protocol auditing, find the following sections of the `/etc/mcp/templates/syslog.conf` file:

```
!audit_config
*.*                                               /var/log/audit_config.log
!audit_protocol
*.*                                               /var/log/audit_protocol.log
```

5. Add a line for remote syslog servers so that the resulting sections of the file will now look similar to the following. In this example, the IP address we are forwarding to is 172.16.0.1. You need to substitute your remote server IP address.

```
!audit_config
*.*                                               /var/log/audit_config.log
*.*                                               @172.16.0.1
!audit_protocol
*.*                                               /var/log/audit_protocol.log
*.*                                               @172.16.0.1
```

   In OneFS 8.2.0, there are new PAPI and CLI commands for configuring remote syslog servers:

   - Using “isi audit settings global modify --config-syslog-servers=<servers>” for configuring a remote syslog server for config audit
   - Using “isi audit settings global modify –protocol-syslog-servers=<servers>” for protocol audit.

6. Save the file and exit the text editor. MCP will push out your changes from the template file into `/etc/syslog.conf` a short time later.

For more details on how to configure audit syslog forwarding on PowerScale, refer to the KB article: OneFS: How to configure remote logging from a cluster to a remote server (syslog forwarding)

2.4.6 Audit log viewer

OneFS provides a tool to view the binary audit logs stored on the cluster. The command “isi_audit_viewer” can provide a view of either the protocol or configuration logs.

The following is an example to view protocol audit logs on a local PowerScale node

```
isi_audit_viewer -t protocol
```

The following is an example to view protocol audit logs between two dates

```
isi_audit_viewer -t protocol -s "2013-08-18 12:00:00" -e "2013-08-19 12:00:00"
```

2.4.7 Audit log progress

To check the last captured audit event and the event time of the last event that was sent to the CEE server, run the `isi audit progress view` command to view the forwarder log position of the CEE server.

The command shows the times for the node the command is run on.

A sample output of the isi audit progress view is shown:

```
Protocol Audit Log Time: Tue Mar 29 13:32:38 2016
Protocol Audit Cee Time: Tue Mar 29 13:32:38 2016
Protocol Audit Syslog Time: Fri Mar 25 17:00:28 2016
```

The command can be called using `isi_for_array` to gather the time for all the nodes in the cluster. In addition, the command can be called with `--lnn` to specify a different node than the command is run from.

The following command displays the progress of delivery of the audit events on a node with logical node number 2:

```
isi audit progress view --lnn=2
```

The output appears as shown:

```
Protocol Audit Log Time: Wed Mar 30 16:32:31 2016
Protocol Audit Cee Time: Wed Mar 30 16:32:31 2016
Protocol Audit Syslog Time: Mon Mar 28 19:05:18 2016
```

Starting in OneFS 8.0.1, the following command allows one to see the oldest unsent protocol audit event for the cluster.

```
#isi audit progress global view
Protocol Audit Latest Log Time: Fri Sep 2 10:06:36 2016
Protocol Audit Oldest Cee Time: Fri Sep 2 10:02:28 2016
Protocol Audit Oldest Syslog Time: Fri Sep 2 10:02:28 2016
```

2.4.8 Audit log time adjustment

In a scenario where auditing on the cluster has been configured and enabled prior to setting up CEE and/or Syslog, the cluster will attempt to forward all events from the time auditing was configured.

OneFS provides a configuration setting to manually update the time to begin forwarding events from. By setting the `--cee-log-time` or `--syslog-log-time`, you can advance the point of time from where to start to forward

Example: The following will update the pointer to forward events after Nov 19, 2014 at 2pm

```
isi audit settings global modify --cee-log-time "Protocol@2014-11-19 14:00:00"
isi audit settings global modify --syslog-log-time "Protocol@2014-11-19 14:00:00" events.
```

2.4.9 Audit event delivery rate statistics

OneFS provides statistics to monitor the delivery rate and total events delivered to CEE.

The following is an example to view the current rate of the CEE forwarder:

```
isi statistics query current list --keys=node.audit.cee.export.rate
Node node.audit.cee.export.rate
---------------------------------
1 3904.600000
---------------------------------
Total: 1
```

The following is an example to view the total amount of events delivered since isi_audit_cee last started

```
isi statistics query current list --keys=node.audit.cee.export.total
Node node.audit.cee.export.total
----------------------------------
1 221844
----------------------------------
Total: 1
```

2.4.10 Audit purging

OneFS starts to support audit purging from the release of 9.1.0.0. This feature supports the following two types if deletion:

1. Auto deletion
2. Manual deletion

Both deletions allow to delete both protocol and configuration audit. For the details, refer to the following sections.

2.4.10.1 Auto deletion

Auto deletion takes the retention period as the parameter to control which audits can be deleted. An internal timer job will be triggered every hour to delete all the audits outside the retention period as shown in the figure below:

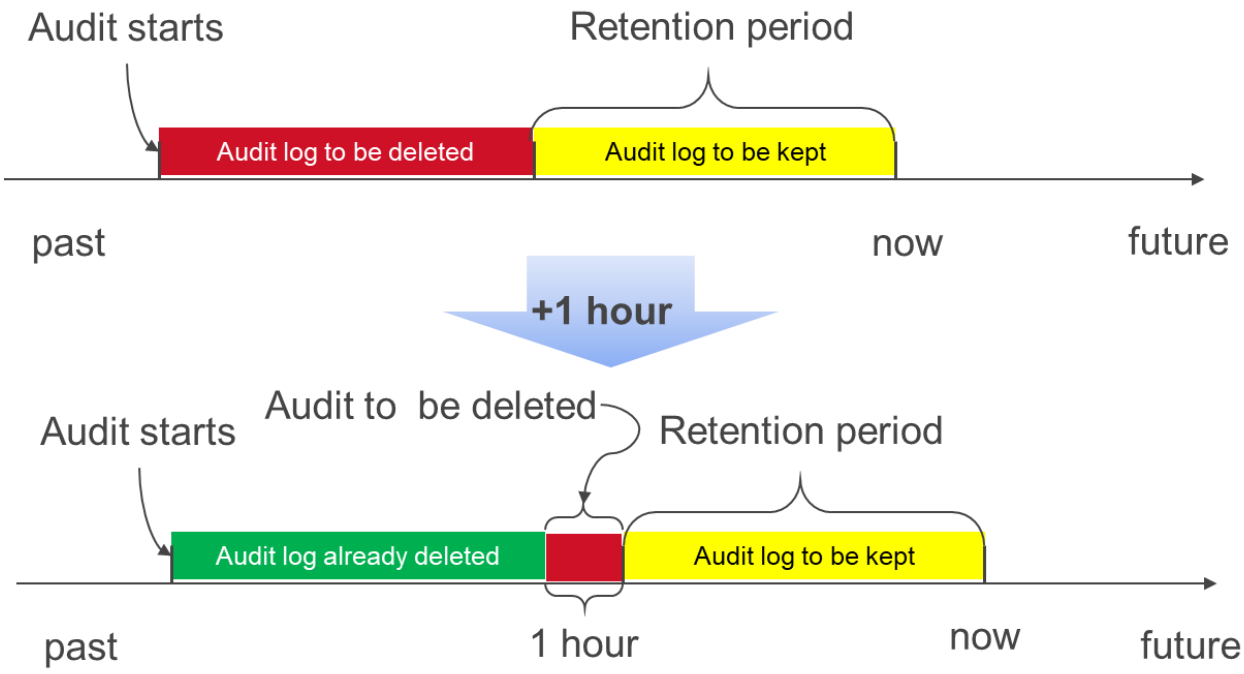

Figure 2 Auto deletion

Deletion will only happen when the following two conditions are met at the same time

- Audit falls out of the retention window
- Audit has been forwarded

To enable the auto deletion, use the following CLI:

```
Deccan-1# isi audit settings global modify --auto-purging-enabled=yes
You are enabling the automatic log purging.
Automatic log purging will run in background to delete audit log files.
Please check the retention period before enabling automatic log purging.
Are you sure you want to do this?? (yes/[no]): yes
```

To set the retention period, use the following CLI:

```
Deccan-1# isi audit settings global modify --retention-period=250
```

To view the configurations, use the following CLI:

```
Deccan-1# isi audit settings global view
Protocol Auditing Enabled: Yes
           Audited Zones: System, testZone
         CEE Server URIs: -
                Hostname:
  Config Auditing Enabled: Yes
    Config Syslog Enabled: No
    Config Syslog Servers: -
  Protocol Syslog Servers: -
     Auto Purging Enabled: Yes
         Retention Period: 250
```

2.4.10.2 Manual deletion

Manual deletion shares the same underlying mechanism with auto deletion. The only difference is that it is triggered manually. To delete the audit log use the following CLI:

```
Deccan-1# isi audit logs delete --before=2020-09-09
You are going to delete the audit logs before 2020-09-09.
Are you sure you want to do this?? (yes/[no]): yes
The purging request has been triggered.
`isi audit logs check` can be used to monitor the process.
```

To monitor the deletion process, use the following CLI:

```
Deccan-1# isi audit logs check
Purging Status:
             Using Before Value: 2020-09-08
Currently Manual Purging Status: COMPLETED
```

3 Conclusion

OneFS 8.0 provides auditing capabilities for SMB, NFS and HDFS protocol events, as well as system configuration changes. OneFS 8.0.1 builds upon the enhancements in OneFS and provides concurrent delivery to multiple CEE servers, which results in increased delivery of audit events to CEE. Integration with the CEE ecosystem allows protocol auditing events to be forwarded to 3rd party audit application. OneFS 8.2.0 provides granular audit selection to improve storage efficiency and performance.

The logs and reports available within the various audit applications provide information technology auditors with the data needed to meet regulatory and compliance requirements.

A Configure Varonis DatAdvantage

To add an PowerScale cluster in Varonis DatAdvantage:

1. On the Monitored File Server page, on the Resources toolbar, click “Add”. The File Server Wizard will open.

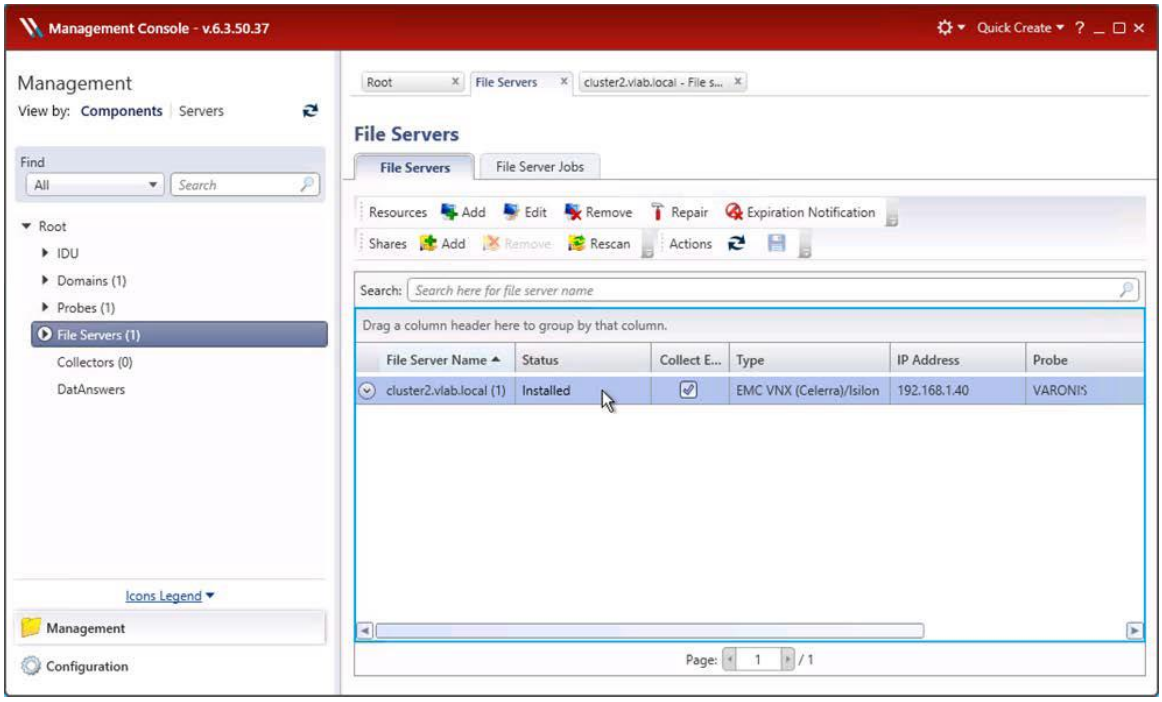

Figure 3 The Varonis Management Console

2. On the left menu, click “Common” and then set the following parameters:

   a. Data Collection Details
   b. Probe: From the drop-down list, select the Probe to be used with the file server.
   c. File Server Details
   d. File Server name: Type the resolved name or IP address of the PowerScale cluster to be added.
   e. FileWalk Credentials: File System operations include the directory crawl (FileWalk), event collection (if it is set), and user crawl (ADwalk) on local accounts (if it is set).
   f. User name: Type the name of the user account to be used for event collection. The format expected is DOMAIN\username.
   g. Password: Type the account's password.
   h. File Server Type: Select “EMC VNX (Celerra)/Isilon”

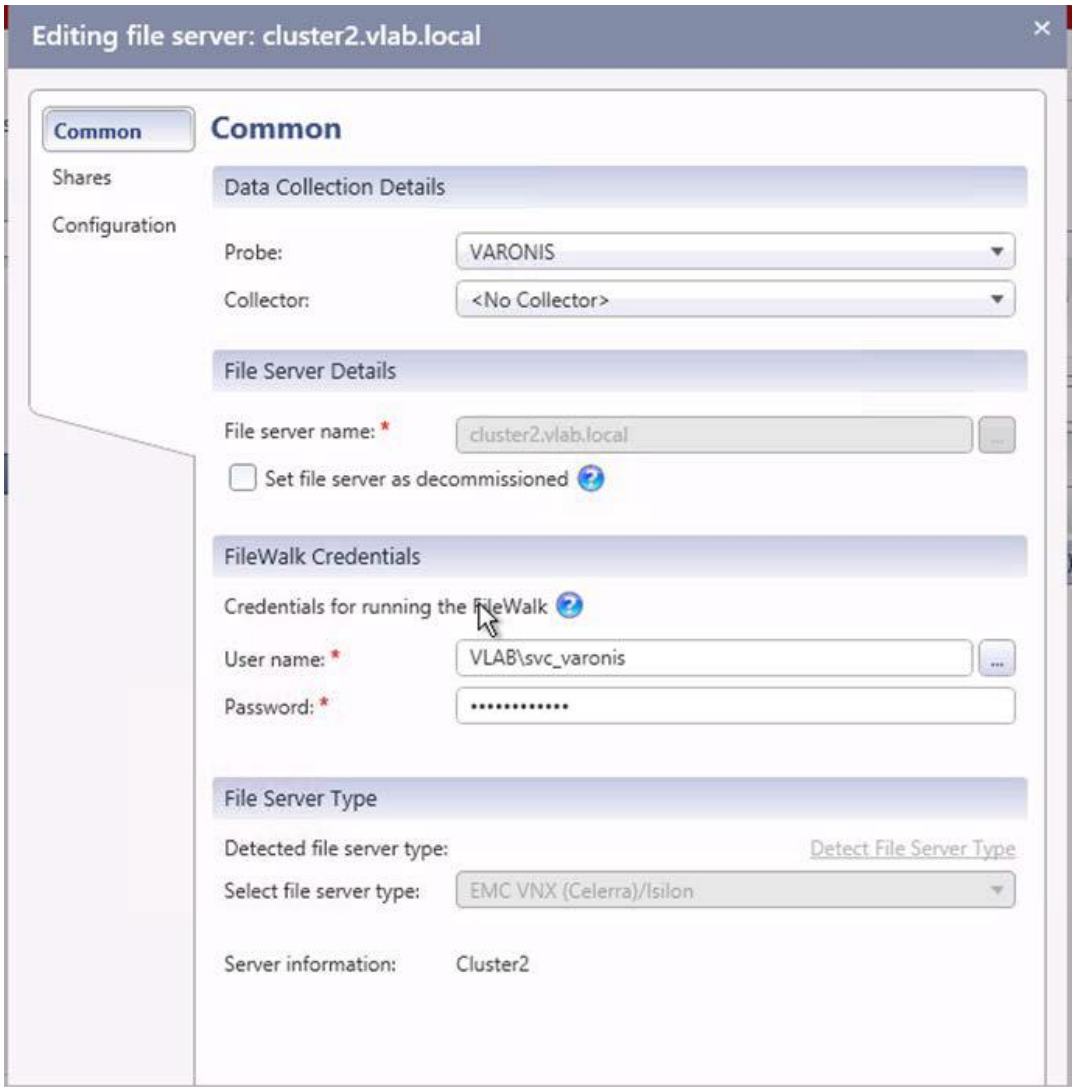

Figure 4 Varonis File System Wizard - Common

B OneFS to Dell EMC CEE event map

The following table details the translation of the OneFS IO Request Packets (IRPs) to the CEE event types prior to OneFS 8.2.0.

Table 7 OneFS to Dell EMC CEE Event Map

eventType	File|dir	CreateResult	DesiredAccess	Other	CEPP_EventType
Create	File	Created			CEPP_CREATE_FILE
Create	Dir	Created			CEPP_CREATE_DIRECTORY
Close	Dir				CEPP_CLOSE_DIRECTORY
Close	File			bytesWritten!=0	CEPP_CLOSE_MODIFIED
Close	File			bytesWritten=0	CEPP_CLOSE_UNMODIFIED
Read	-				CEPP_FILE_READ
Write	-				CEPP_FILE_WRITE
Rename	File				CEPP_RENAME_FILE
Rename	Dir				CEPP_RENAME_DIRECTORY
Delete	File				CEPP_DELETE_FILE
Delete	Dir				CEPP_DELETE_DIRECTORY
setSecurity	File				CEPP_SETACL_FILE
setSecurity	Dir				CEPP_SETACL_DIRECTORY
getSecurity					N/A
Create	File	Opened	Read, write, append bits clear		CEPP_OPEN_FILE_NOACCESS
Create	File	Opened	Read bit set		CEPP_OPEN_FILE_READ
Create	File	Opened	Write bit set		CEPP_OPEN_FILE_WRITE
Create	File	Opened	Append bit set		CEPP_OPEN_FILE_WRITE
Create	Dir	Opened			CEPP_OPEN_DIRECTORY
					CEPP_SETSEC_FILE
					CEPP_SETSEC_DIRECTORY
n/a					CEPP_UNKNOWN
n/a					CEPP_ALLL

C Technical support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.

C.1 Related resources

- “EMC CEE Release 6.5 Using the Common Event Enabler for Windows” (P/N 302-000-085 Rev 05)
- “Configuring DatAdvantage for EMC Celerra VNX Isilon CEPA Event Collection” available from Varonis
- “StealthAUDIT Management Platform User Guide” available from STEALTHbits
- “Symantec Data Insight Administrator’s Guide” available from Symantec
- “Dell Change Auditor Installation Guide” from Dell
- The up-to-date list of compatible Auditing Software solutions is maintained in the Isilon Third-Party Software and Hardware Compatibility Guide