Best Practices Guide

FILE SYSTEM AUDITING WITH EMC ISILON AND EMC COMMON EVENT ENABLER

Abstract

This guide outlines best practices to configure a File System Audit solution in SMB and NFS environments with EMC Isilon, And EMC Common Event Enabler (CEE).

April 2015

EMC²

Part Number H12428.3

Table of Contents

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.

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)

Table 1: Regulatory requirements

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 EMC® Isilon® OneFS® 7.2 addresses these needs for SMB and NFS workflows and EMC Isilon cluster configuration changes.

EMC Isilon OneFS Audit Overview

EMC Isilon OneFS can audit system configuration events, SMB and NFS protocol access events on the EMC Isilon 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 EMC Common Event Enabler (CEE).

In OneFS 7.2, SMB and NFS protocol events can be audited. Protocol auditing must be enabled and then configured on a per-Access Zone basis. For example, you might want to audit all SMB protocol events on the system Access Zone and audit only failed attempts to delete files in a different Access Zone.

If protocol auditing is enabled on an Access Zone, file access events through the NFS and SMB protocol are recorded in the protocol audit topic. The protocol audit topic is consumable by auditing applications that support the EMC Common Event Enabler, which provides integration with auditing applications such as Varonis® DatAdvantage®, STEALTHbits StealthAUDIT®, Symantec Data Insight®, and Dell Change Auditor for EMC®.

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.

Audit Requirements

Isilon OneFS software

- OneFS 7.1 or later

Isilon OneFS Role Based Access

- Root or Admin account
- Account with built-in AuditAdmin role capabilities

EMC Common Event Enabler

- CEE 6.5.0 or later

3rd Party Software Requirements

Varonis DatAdvantage

- DatAdvantage versions 5.8.80.x and later
- Microsoft SQL Server
    - Microsoft SQL Server 2005 Standard or Enterprise, with SP2 or SP3
    - Microsoft SQL Server 2008 Standard or Enterprise, with SP1 or SP2
    - Microsoft SQL Server 2008 R2 Standard or Enterprise
    - Microsoft SQL Server 2012 Standard or Enterprise

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

- StealthAUDIT Management Platform
- FSAA 6.2.313.0
- STEALTHbits File Monitoring Service
- Microsoft SQL Server
    - Microsoft SQL Server 2008 Standard or Enterprise
    - Microsoft SQL Server 2012 Standard or Enterprise

Dell Change Auditor for EMC

- Dell Change Auditor 6.5 and later
- Microsoft .Net Framework version 4.0
- Microsoft XMLPArser (MSXML) 6.0 and SQLXML 4.0
- Microsoft SQL Server
    - Microsoft SQL Server 2008 Standard or Enterprise
    - Microsoft SQL Server 2012 Standard or Enterprise

Audit Management

Enable auditing with the OneFS WebUI

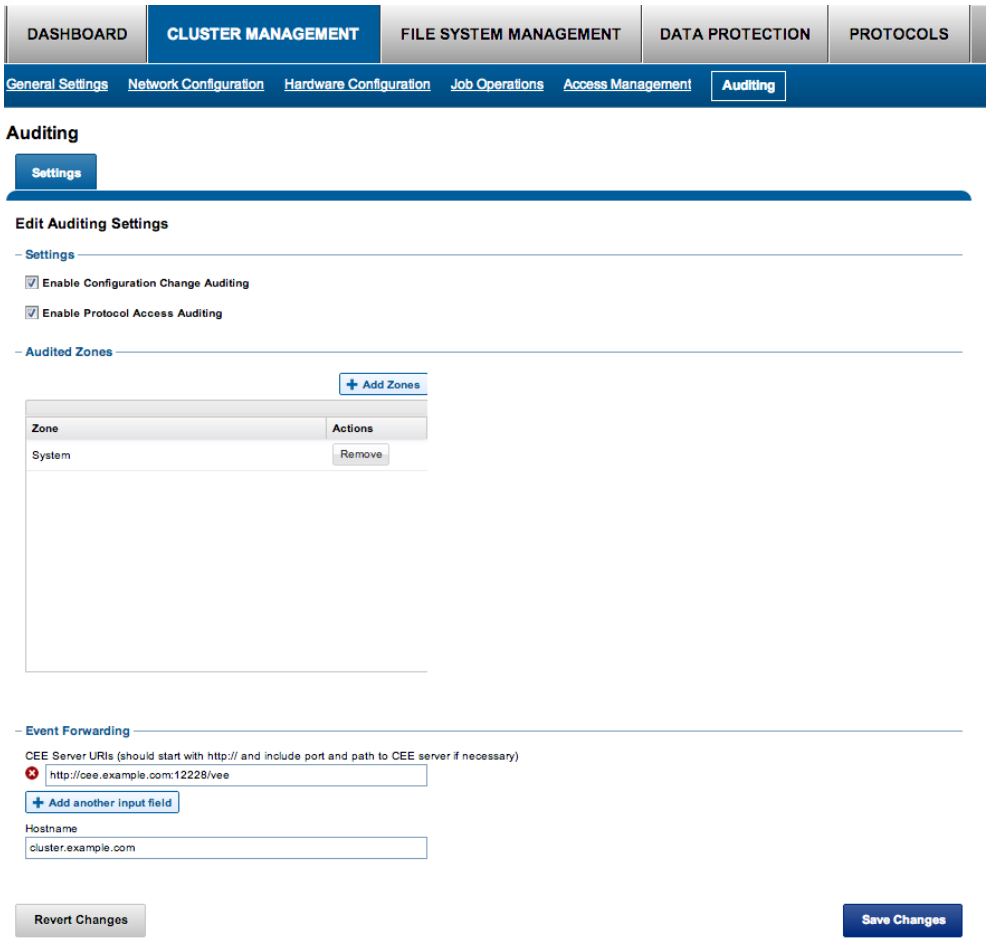

Figure 1: OneFS audit configuration

To enable protocol auditing in the OneFS WebUI

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 for the server where the Common Event Enabler is installed.

   The format for the entry will be:
   http://fullyqualifieddomain:port/cee
   For example: http://cee.example.com:12228/cee
   Port 12228 is the default CEE HTTP listen port.
6. Hostname – Entry should match the name use to defined the file server in the

Enable Auditing with CLI

OneFS 7.1 added the 'isi audit' command.

To enable auditing
cluster-1# isi audit settings modify --protocol-auditing-enabled on

To disable auditing
cluster-1# isi audit settings modify --protocol-auditing-enabled off

Add access zone to Audit
cluster-1# isi audit settings modify --audited-zones <ZONE>
cluster-1# isi audit settings modify --audited-zones System

cluster-1# isi audit settings 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

Access Zone Audit Configuration with CLI

isi zone zones modify <zone>
--audit-success {close | create | delete | get_security | logoff | logon | read | rename | set_security | tree_connect | write | all} | --clear-audit-success

--add-audit-success {close | create | delete | get_security | logoff | logon | read | rename | set_security | tree_connect | write | all}

--remove-audit-success <string>

--audit-failure {close | create | delete | get_security | logoff | logon | read | rename | set_security | tree_connect | write | all} | --clear-audit-failure

--add-audit-failure {close | create | delete | get_security | logoff | logon | read | rename

Enable specific audit events

```
isi zone zones modify System –-audit-success create,delete,get_security
cluster-1# isi zone zones list -v
                Name: System
          Cache Size: 4.77M
        Map Untrusted:
           SMB Shares: -
       Auth Providers: -
       Local Provider: Yes
         NetBIOS Name:
       All SMB Shares: Yes
   All Auth Providers: Yes
   User Mapping Rules: -
Home Directory Umask: 0077
   Skeleton Directory: /usr/share/skel
        Audit Success: create, delete, get_security
        Audit Failure: -
       HDFS Authentication: all
       HDFS Root Directory: /ifs
           WebHDFS Enabled: Yes
        HDFS Ambari Server:
      HDFS Ambari Namenode:
Syslog Forwarding Enabled: No
        Syslog Audit Events: create, delete, rename, set_security
              Zone ID: 1
```

Enable all audit events

```
isi zone zones modify System –-audit-success all
cluster-1# isi zone zones list -v
                Name: System
          Cache Size: 4.77M
        Map Untrusted:
           SMB Shares: -
       Auth Providers: -
       Local Provider: Yes
         NetBIOS Name:
       All SMB Shares: Yes
   All Auth Providers: Yes
   User Mapping Rules: -
Home Directory Umask: 0077
   Skeleton Directory: /usr/share/skel
        Audit Success: close, create, delete, get_security, logoff, logon, read, rename,
set_security, tree_connect, write
        Audit Failure: -
       HDFS Authentication: all
       HDFS Root Directory: /ifs
           WebHDFS Enabled: Yes
        HDFS Ambari Server:
      HDFS Ambari Namenode:
Syslog Forwarding Enabled: No
        Syslog Audit Events: create, delete, rename, set_security
              Zone ID: 1
```

Configure EMC Common Event Enabler 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\Celerra Event Enabler\CEPP\Audit\Configuration.
3. Edit the endpoint string value as follows:

   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

   Dell Change Auditor

   - Set Value to QuestSoftware

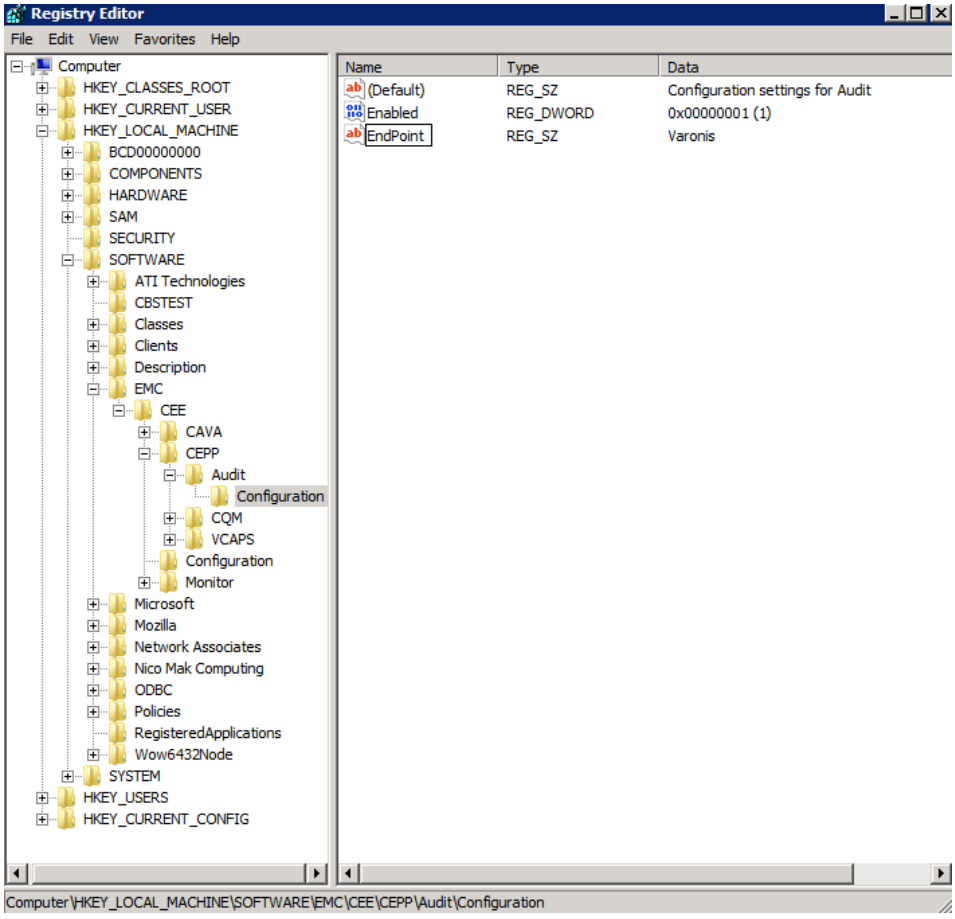

Figure 2: EMC CEE configuration

Example: Enable audit

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

Example: Single local endpoint

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

Remote endpoints are also supported and are designated as "EndPoint_Name@IP_Address".

Example: Single remote endpoint

```
[HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE\CEPP\Audit\Configuration] EndPoint = (REG_SZ) Varonis@10.7.1.2
```

Multiple endpoints may be entered and should be separated by semicolons.

Example: Multiple remote endpoints

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

Any modification requires that the EMC Celerra® Antivirus Agent (CAVA) service be restarted. The service can be restarted via the Server Manager or command line interface (CLI).

```
C:\>net stop "emc cava"
The EMC CAVA service was stopped successfully.

C:\>net start "emc cava"
The EMC CAVA service is starting.
The EMC CAVA service was started successfully.
```

Audit Syslog Forwarding

OneFS 7.1.1 added the ability to forward config and/or protocol auditing events to a syslog server.

Enable Syslog Forwarding

```
Config Audit

isi audit settings modify --config-auditing-enabled yes --config-syslog-enabled yes
cluster-1# isi audit settings view
Protocol Auditing Enabled: No
          Audited Zones: -
       CEE Server URIs: -
             Hostname:
 Config Auditing Enabled: Yes
  Config Syslog Enabled: Yes

Protocol Audit – Enabled on a Per Access Zone basis

isi zone zones modify <Access_Zone_Name> --syslog-forwarding-enabled yes
cluster-1# isi zone zones view System
                Name: System
                Path: /ifs
          Cache Size: 9.54M
        Map Untrusted:
       Auth Providers: -
         NetBIOS Name:
    All Auth Providers: Yes
    User Mapping Rules: -
  Home Directory Umask: 0077
   Skeleton Directory: /usr/share/skel
       Audit Success: create, delete, rename, set_security, close
       Audit Failure: create, delete, rename, set_security, close
   HDFS Authentication: all
   HDFS Root Directory: /ifs
      WebHDFS Enabled: Yes
    HDFS Ambari Server:
  HDFS Ambari Namenode:
Syslog Forwarding Enabled: Yes
    Syslog Audit Events: create, delete, rename, set_security
             Zone ID: 1
```

1. Update Syslog Configuration to forward events

    a. Modify Audit Entries in /etc/mcp/override/syslog.conf

    Example

    ```
    !audit_protocol
    *.*             @ip_of_syslog_server
    !audit_config
    *.*             @ip_of_syslog_server
    ```

Conclusion

OneFS 7.2 provides auditing capabilities SMB and NFS protocol events, as well as system configuration changes. Integration with the EMC CEE ecosystem allows protocol auditing events to be forwarded to 3rd party audit application.

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

References

- "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 Adminsitrator'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

  https://support.emc.com/docu45932_Isilon-Third-Party-Software-and-Hardware-Compatbility-Guide.pdf

Appendix

Configure Varonis DatAdvantage

To add an EMC Isilon cluster:

1. On the Monitored File Server page, on the Resources toolbar, click "Add".

   The File Server Wizard will open.

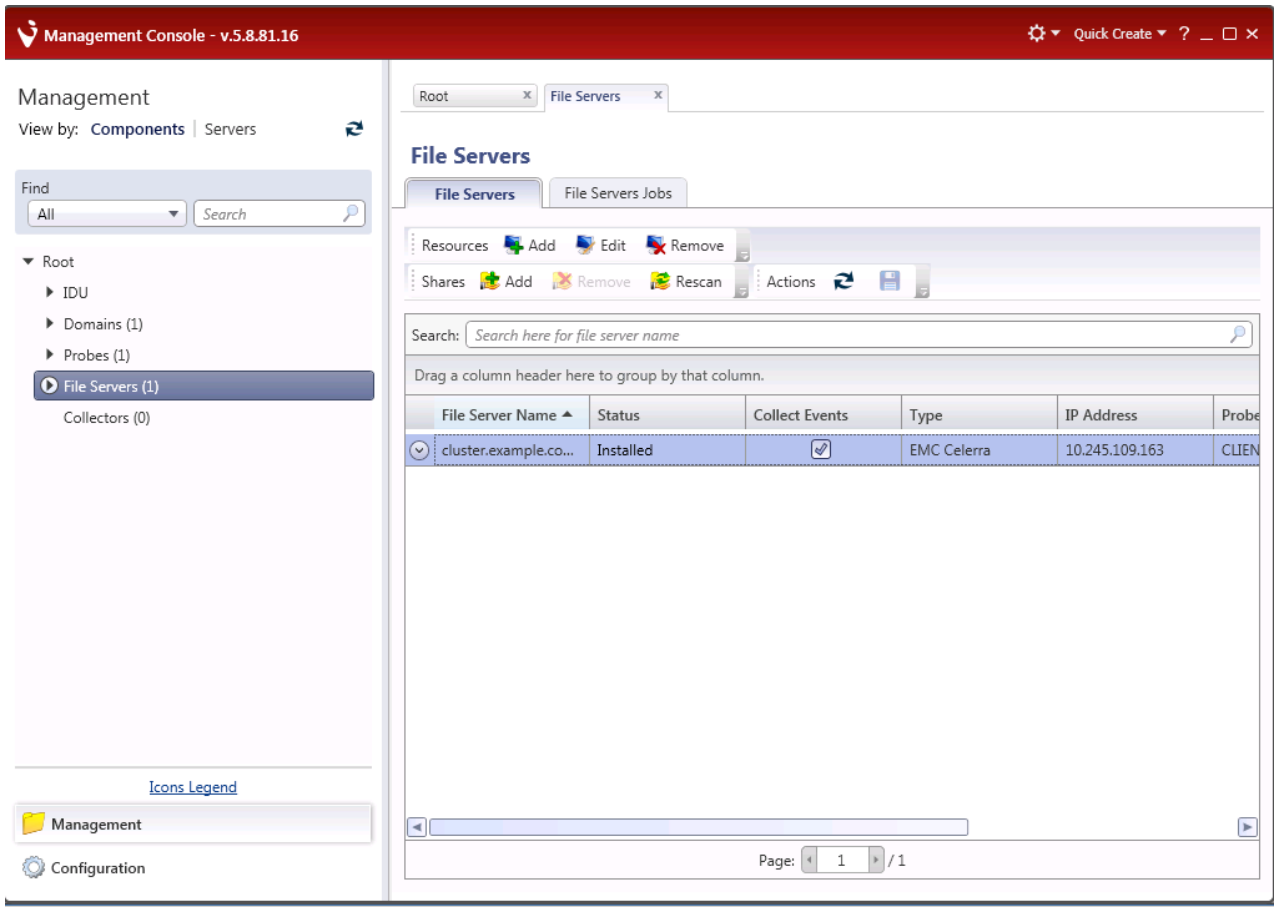

Figure 3: The Varonis Management Console

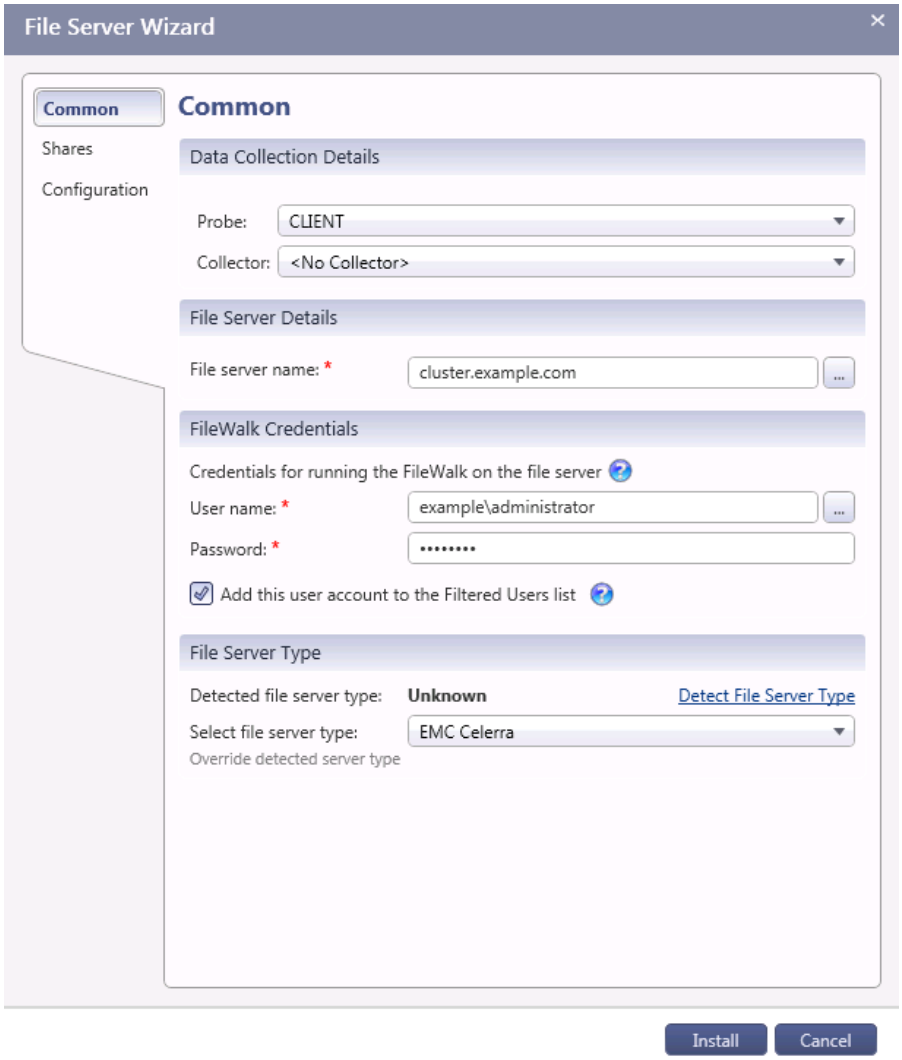

Figure 4: Varonis File System Wizard - Common

2. On the left menu, click "Common" and then set the following parameters:
   - Data Collection Details
   - Probe: From the drop-down list, select the Probe to be used with the file server.
   - File Server Details
   - File Server name: Type the resolved name or IP address of the EMC Isilon cluster to be added.
   - 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).
   - User name: Type the name of the user account to be used for event collection. The format expected is DOMAIN\username.
   - Password: Type the account's password.
   - File Server Type: Select "EMC Celerra"

Audit Log Viewer

OneFS 7.1 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.

```
Usage: isi_audit_viewer [ -n <nodeid> | -t <topic> | -s <starttime>|
        -e <endtime> | -v ]
        -n <nodeid> : Specify node id to browse (default: local node)
        -t <topic>  : Choose topic to browse.
          Topics are "config" and "protocol" (default: "config")
        -s <start>  : Browse audit logs starting at <starttime>
        -e <end>    : Browse audit logs ending at <endtime>
        -v verbose  : Prints out start / end time range before printing
           records
```

Example: View Protocol Audit Logs on a local node

cluster-1# isi_audit_viewer -t protocol

Example: 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"

Audit Events

Event	User action
create	Create a file or folder Open a file or folder Mount a share
delete	Delete a file or folder
get_security	View a file or folder's properties
logon	Map a network drive
logoff	Disconnect a mapped drive
read	View a file or folder
rename	Rename a file or folder
set_security	Modify file or folder permissions
tree_connect	Map a network drive View a file or folder's security settings
write	Modify a file

Table 2: OneFS SMB event auditing

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

From OneFS					To EMC CEE
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_ALL

Table 3 OneFS to EMC CEE Event Map

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 7.2 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 events.

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

isi audit settings modify --cee-log-time "Protocol@2014-11-19 14:00:00"

isi audit settings modify --syslog-log-time "Protocol@2014-11-19 14:00:00"