TROUBLESHOOT PROTOCOL AUDITING ISSUES ON YOUR ISILON CLUSTER

OneFS 7.2 – 8.2

Abstract

This troubleshooting guide helps you identify and troubleshoot issues with auditing protocol activity on an Isilon cluster.

June 9, 2020
Contents and overview

Note
Follow all of these steps, in order, until you reach a resolution.

1. Follow these steps.
   - Page 3: Before you begin
   - Page 4: OneFS protocol auditing overview

2. Perform troubleshooting steps in order.
   - Page 5: Start troubleshooting
   - Page 6: Check for valid URI and hostnames
   - Page 7: Confirm which events are configured for auditing
   - Page 8: Check for delays in sending events
   - Page 10: Check the timestamp of recent events
   - Page 11: Confirm that nodes are forwarding events to the CEE server
   - Page 12: Confirm that your third-party auditing application is receiving events
   - Page 13: Increase the logging level for the audit driver
   - Page 14: Check the lwiod.log file
   - Page 15: STATUS_TIMEOUT errors
   - Page 16: Configure events for auditing
   - Page 17: Audit performance and servers

3. Appendixes
   - Appendix A: If you need further assistance
   - Appendix B: How to use this flowchart
   - Appendix C: Example output
   - Appendix D: Example output
   - Appendix E: Example output
   - Appendix F: Example output
Before you begin

**CAUTION!**
If the node, subnet, or pool that you are working on goes down during the course of troubleshooting and you do not have any other way to connect to the cluster, you could experience data unavailability.

Therefore, make sure that you have more than one way to connect to the cluster before you start this troubleshooting process. The best method is to have a serial console connection available. This way, if you are unable to connect through the network, you will still be able to connect to the cluster physically.

For specific requirements and instructions for making a physical connection to the cluster, see [article 304071](http://www.dell.com/support/article/us/en/04/SLN969175) on the Online Support site.

Before you begin troubleshooting, confirm that you can connect through either another subnet or pool, or that you have physical access to the cluster.

**Configure screen logging through SSH**

We recommend that you configure screen logging to log all session input and output during your troubleshooting session. This log file can be shared with Isilon Technical Support, if you require assistance at any point during troubleshooting.

1. Open an SSH connection to the cluster and log in by using the root account.

   **Note:** If the cluster is in compliance mode, use the compadmin account to log in. All compadmin commands must be preceded by the sudo prefix.

2. Change the directory to `/ifs/data/Isilon_Support` by running the following command:
   ```
   cd /ifs/data/Isilon_Support
   ```

3. Run the following command to capture all input and output from the session:
   ```
   screen -L
   ```
   This will create a file named `screenlog.0` that will be appended to during your session.

4. Perform troubleshooting.
OneFS protocol auditing overview

Overview
This troubleshooting guide covers protocol auditing only. For issues with configuration change auditing, contact Isilon Technical Support.

You can audit protocol activity on an Isilon cluster. All audit data is stored and protected in the cluster file system. These internally stored events are translated into events that can be forwarded through the Common Events Enabler (CEE) to a third-party auditing application.

In OneFS 8.0 and later, you can audit SMB, NFS, and HDFS protocol activity.

In OneFS 7.2.x, you can audit SMB and NFS protocol activity.

Protocol auditing must be configured on a per-access-zone basis. The audit events are logged on the node on which the client initiated the activity. The events are stored in binary log files located in subdirectories of the /ifs/.ifsvar/audit/logs directory. There is one subdirectory for each node in the cluster.

When audited events are logged, the CEE forwarder service (isi_audit_kee) forwards the events to CEE using an HTTP PUT operation. CEE forwards the events to a configured third-party application, such as Varonis.

For more information, see the OneFS Web Administration Guide or the OneFS CLI Administration Guide for your version of OneFS.
Start troubleshooting

**Introduction**
Start troubleshooting here. If you need help understanding the flowchart conventions that are used in this guide, see Appendix B: How to use this flowchart.

Start

If you have not done so already, log in to the cluster and configure screen logging through SSH, as described on page 3.

Are you experiencing STATUS_TIMEOUT errors?

Yes -> Go to Page 15

No

Run the following command to confirm that protocol auditing is enabled, that the relevant access zones are being audited, and that the CEE server URI is correct:

**OneFS 8.0 and later**

isi audit settings global view

**OneFS 7.2**

isi audit settings view

See Appendix C for example output.

Go to Page 6
Check for valid URI and hostnames

You could have arrived here from:

- Page 5 – Start troubleshooting

```
Does the output show that protocol auditing is enabled for the relevant access zones and that the CEE server URI and Hostname are correct?  
```

```
Enable protocol auditing and update the CEE server URI and Hostname, as needed.  
```

```
Is the issue resolved?  
```

```
End troubleshooting  
```

```Page 7```

---

6 - Dell EMC Isilon Customer Troubleshooting Guide: Troubleshooting Protocol Auditing Issues on Your Isilon Cluster

For links to all Isilon customer troubleshooting guides, visit the OneFS Customer Troubleshooting Guides Info Hub.

Confirm which events are configured for auditing

You could have arrived here from:
- Page 6 - Check for valid URI and hostnames
- Page 16 - Configure events for auditing

Run the appropriate command to confirm that the expected events are configured to be audited and the list of events that are configured to be forwarded to syslog where <access zone> is the name of the access zone you want to check:

OneFS 8.0 and later
isi audit settings view --zone=<access zone>

OneFS 7.2
isi zone zones view --zone=<access zone>

See Appendix E for example output.

Note
The Syslog Audit Events field lists the event types that are configured to be forwarded to syslog.

Example output
cluster-1# isi_for_array -s date
cluster-1: Tue Sep 17 09:32:08 PDT 2019
cluster-2: Tue Sep 17 09:32:08 PDT 2019
cluster-3: Tue Sep 17 09:32:08 PDT 2019

Do the Audit Failure and Audit Success fields display a complete list of the events you want to audit, and does the Syslog Audit Events field contain the complete list of the events that you want forwarded to syslog?

Yes

Run the following command to get the current timestamp on the cluster:
isi_for_array -s date

No

Go to Page 16

Go to Page 8
Check for delays in sending events

Run the following command:

```bash
isi_for_array -sX isi_audit_progress -t protocol CEE_FWD
```

The output looks similar to the following:

```
cluster-2# isi_for_array -sX isi_audit_progress -t protocol CEE_FWD
cluster-1: Last consumed event time: '2019-09-13 16:15:48'
cluster-1: Last logged event time: '2019-09-13 16:15:48'
```

**Note**

NANON nodes are not expected to send audit events.

The `isi_audit_progress` output fields indicate the following:

- **Last consumed event time** - this is the timestamp of the last event that was sent to the CEE server
- **Last logged event time** - this is the timestamp of the last auditable event in `isi_audit_d`

For the **Last consumed event time** to increase we need to send the event to the CEE server, which will then forward the event to the endpoint. The CEE server will receive an acknowledgment back if transmission to the end point was successful. Upon successful transmission, the CEE server will send an acknowledgment to the Isilon cluster. Until that acknowledgment is received, the timestamp will not increase.

Go to Page 9
Using the output from the previous two steps, check the following two things to determine whether the Isilon cluster is experiencing a delay in sending audit events to the CEE server:

- The date and time posted for both the Last consumed and the Last logged events should be within 24 hours of each other. If the last logged event time is more than 24 hours later than the last consumed event time, then there is a delay.
- The last logged event time should always be within a few seconds of the current timestamp on the cluster. If the last logged event time is more than a few seconds after the current timestamp on the cluster, then there is a delay.

Is there a delay in sending audit events to the CEE server?  

If the answer is No, then go to Page 10. If the answer is Yes, then:

Is this delay the issue you are trying to resolve?  

If the answer is Yes, then go to Page 17. If the answer is No, then go to Page 10.
Check the timestamp of recent events

You could have arrived here from:
- Page 9 – Check for delays in sending events (2)

Example output
- cluster-1: isi_for_array -s date
  cluster-1: Tue Sep 17 09:32:08 PDT 2019
- cluster-2: Tue Sep 17 09:32:08 PDT 2019
- cluster-3: Tue Sep 17 09:32:08 PDT 2019

Run the following command to get the current time on the cluster:

```
si_for_array -s date
```

To gather the last five minutes of events on this node, run the following command:

```
isi_audit_viewer -t protocol -s "$(date -v-5M +%Y-%m-%d %H:%M:%S)" -e "$(date +%Y-%m-%d %H:%M:%S)"
```

The output should show five minutes of events per node, unless there is not an event to report, or if the node has been configured not to log events. In that case, the output will simply report done.

See Appendix D for example output.

For each node that is reporting events, check the timestamp of the most recent event and compare it to the current timestamp on the cluster. The timestamp should be within a few minutes of the cluster timestamp.

All of the cluster nodes that are reporting events are capturing the events and logging them in the Audit database.

For each node that is reporting events, is the timestamp of the most recent event within a few minutes of the cluster timestamp?

- Yes
- No

Some or all of the cluster nodes are not capturing events and logging them in the audit database.

Go to Page 11

Go to Page 13
Confirm that nodes are forwarding events to the CEE server

You could have arrived here from:

- Page 10 – Check the timestamp of recent events

Perform the following steps to confirm that the cluster is forwarding events to the CEE server. Choose the commands for your version of OneFS.

1. Enable debug logging for the isi_audit_cee.log on all nodes by running:
   
   **OneFS 8.0.x and later**
   isi_for_array '/usr/likewise/bin/lwsm set-log-level isi_audit_cee - trace'

   **OneFS 7.2 - 8.0.0.x**
   isi_for_array 'pkill -SIGUSR1 isi_audit_cee'

2. Wait five minutes.

3. Disable debug logging for the isi_audit_cee.log on all nodes by running:

   **OneFS 8.0.x and later**
   isi_for_array '/usr/likewise/bin/lwsm set-log-level isi_audit_cee - warning'

   **OneFS 7.2 - 8.0.0.x**
   isi_for_array 'pkill -SIGUSR1 isi_audit_cee'

4. Run the following command to see the first five most recent events in /var/log/isi_audit_cee.log for each node:

   **OneFS 8.0.x and later**
   isi_for_array 'grep EventsDelivered /var/log/isi_audit_cee.log | tail -n5'

   Verify if the EventsDelivered value has increased. **If the number remains the same, then proceed to the No path: Some or all of the cluster nodes are unable to forward the events to the CEE server.** See Appendix F, Example 1 for example output.

   **OneFS 7.2 - 8.0.0.x**
   isi_for_array 'cat /var/log/isi_audit_cee.log | tail -n5'

   Each event should contain DEBUG: Got event, and also DEBUG: deliver_event: Routing event to <IP address of CEE server>.

   See Appendix F, Example 2 for example output.
Confirm that your third-party auditing application is receiving events

You could have arrived here from:

- Page 11 – Confirm that nodes are forwarding events to the CEE server

---

**Page 12**

Do the events look correct as described in step 4 for each event, on each node in the cluster?

- **No**
  - Note the page number that you are currently on. Upload log files and contact Isilon Technical Support, as instructed in Appendix A.

- **Yes**
  - All of the cluster nodes are forwarding events to the CEE server.

---

Is your third-party auditing application receiving events from the CEE server?

- **Yes**
  - End troubleshooting

- **No**
  - The OneFS auditing system is performing correctly. Contact the vendor of your third-party auditing application for assistance with troubleshooting the issue.

---

12 - Dell EMC Isilon Customer Troubleshooting Guide: Troubleshooting Protocol Auditing Issues on Your Isilon Cluster

For links to all Isilon customer troubleshooting guides, visit the [OneFS Customer Troubleshooting Guides Info Hub](https://www.dell.com/support/home/us/en/19/onefs-customer-troubleshooting-guides-info-hub).

Increase the logging level for the audit driver

- Page 10 – Check the timestamp of recent events
- Page 13 – Remove the audit log files

### Increase the logging level for the audit driver (flt_audit) to the debug level.

**OneFS 8.0 and later**
- SMB: `/usr/likewise/bin/lwsm set-log-level lwio flt_audit debug`
- NFS: `/usr/likewise/bin/lwsm set-log-level nfs flt_audit_nfs debug`
- HDFS: `/usr/likewise/bin/lwsm set-log-level hdfs flt_audit_hdfs debug`

**OneFS 7.2.1**
- `/usr/likewise/bin/lwsm set-log-level flt_audit flt_audit debug`

Connect to a node in the cluster over a protocol you are auditing and perform a task that should be audited. For example, if you are auditing create and close events performed by SMB clients, connect to a node over SMB and create and then close a file within an audited access zone.

### CAUTION!

You must reset the logging level to `warning`, increasing the logging level causes OneFS to log more messages in the log files and might lead to the creation of additional log files. Over time, the additional log files could fill the `/var` partition. In addition, the `/var` partition is stored on a node's boot drives and excessive logging could adversely affect the wear life of those drives.

### Reset the logging level for the audit driver to the default level.

**OneFS 8.0 and later**
- SMB: `/usr/likewise/bin/lwsm set-log-level lwio flt_audit warning`
- NFS: `/usr/likewise/bin/lwsm set-log-level nfs flt_audit_nfs warning`
- HDFS: `/usr/likewise/bin/lwsm set-log-level hdfs flt_audit_hdfs warning`

**OneFS 7.2.1**
- `/usr/likewise/bin/lwsm set-log-level flt_audit flt_audit warning`
Check the lwiod.log file

Check the lwiod.log file on the node you performed the audited task on to confirm whether the event was logged.

1. Connect over SSH to the node on which you previously performed an audited task, and log in as root.
2. Run the following command to view the last five DEBUG message logged in the lwiod.log file:

```
cat /var/log/lwiod.log | grep DEBUG | tail -n5
```

If the event was logged, the command output will contain messages similar to the following example. In the example below, the zone in which the event occurred is System, the type of event that occurred was a close event, and the file that was closed was README.txt.

```
2014-12-09T20:38:51-05:00 <30.7s> isi-7111b-1(id1) lwio[2002]: [f1t_audit] DEBUG: 0x805c039b0:log_event(): audit_worker.cpp:537: deque'd: ("zoneID":1, "zoneName": "System", "eventType": "close", "isDirectory":false,"clientIPAddr":"178.178.178.221", "fileName":"/ifs/README.txt","userSID":"S-1-22-0","bytesRead":0,"bytesWritten":0, "numberOfReads":0,"numberOfWrites":0, "ntStatus":0,"handle":"0000000005ca4118")
```

Were the events logged and does the output contain the expected information?

- **Yes** → End troubleshooting
- **No** → Note the page number that you are currently on. Upload log files and contact Isilon Technical Support, as instructed in Appendix A.
STATUS_TIMEOUT errors

You could have arrived here from:
• Page 5 - Start troubleshooting

Go to
Isilon Audit reports STATUS_TIMEOUT errors, article 540170

Did this article resolve the issue?

Yes → End troubleshooting

No

Note the page number that you are currently on. Upload log files and contact Isilon Technical Support, as instructed in Appendix A.
Configure events for auditing

You could have arrived here from:

- Page 7 – Confirm which events are configured for auditing

Is this the first time you have visited this page?

- No → Upload log files and contact Isilon Technical Support, as instructed in Appendix A.
- Yes → Refer to the "Supported event types" section of the "Auditing" chapter in the OneFS CLI Administration Guide for your version of OneFS.

This section of the guide lists the events that can be audited and provides information about which protocols support specific events.

Note
The Syslog Audit Events field lists the event types that are configured to be forwarded to syslog.

Refer to the "Auditing Commands" section of the OneFS CLI Administration Guide for your version of OneFS for the commands to add and remove Audit Failure, Audit Success, and Syslog Audit events. These events cannot be added globally. They must be added to each access zone that is being audited.

Run the isi audit settings modify command with the appropriate parameters to configure OneFS to audit the desired events for the relevant access zones.

Go to Page 7
Audit performance and servers

OneFS 8.0 and later
isi audit settings global view

OneFS 7.2.1
isi audit settings view

Which version of OneFS is the cluster on?

OneFS 8.0.1 and later

Later versions of OneFS offer improved CEE performance. An upgrade is suggested.

End troubleshooting

8.0.0 and earlier

How many audit servers are configured?

Less than 1 per node

1 per node

Note the page number that you are currently on. Upload log files and contact Isilon Technical Support, as instructed in Appendix A.

Example output

Output for OneFS 8.0 and later
cluster-1# isi audit settings global view
Protocol Auditing Enabled: Yes
Audited Zones: System, zoneA
CEE Server URIs: http://example.com:12228/cee
    Hostname: mycluster
Config Auditing Enabled: Yes
Config Syslog Enabled: Yes

Output for OneFS 7.2.1
cluster-1# isi audit settings view
Protocol Auditing Enabled: No
Audited Zones: System
CEE Server URIs: http://10.2.2.2:12228/cee
    Hostname: 10.1.1.1
Config Auditing Enabled: No
Config Syslog Enabled: Yes

Best practice is to have one CEE server per node.

See the "Delivering protocol audit events to multiple CEE servers" section of the OneFS Web Administration Guide for your version of OneFS.
Appendix A: If you need further assistance

Contact Isilon Technical Support
If you need to contact Isilon Technical Support during troubleshooting, reference the page or step that you need help with. This information and the log file will help Isilon Technical Support staff resolve your case more quickly.

Upload node log files and the screen log file to Isilon Technical Support
1. When troubleshooting is complete, type exit to end your screen session.
2. Gather and upload the node log set and include the SSH screen log file by using the command appropriate for your method of uploading files. If you are not sure which method to use, use FTP.
   
   **ESRS:**
   isi_gather_info --esrs --local-only -f /ifs/data/Isilon_Support/screenlog.0

   **FTP:**
   isi_gather_info --ftp --local-only -f /ifs/data/Isilon_Support/screenlog.0

   **HTTP:**
   isi_gather_info --http --local-only -f /ifs/data/Isilon_Support/screenlog.0

   **SupportIQ:**
   Copy and paste the following command.
   
   **Note:** When you copy and paste the command into the command-line interface, it will appear on multiple lines (exactly as it appears on the page), but when you press Enter, the command will run as it should.

   isi_gather_info --local-only -f /ifs/data/Isilon_Support/screenlog.0 --noupload \ --symlink /var/crash/SupportIQ/upload/ftp

3. If you receive a message that the upload was unsuccessful, refer to article 304567 for directions on how to upload files over FTP.
Appendix B: How to use this flowchart

Introduction
Describes what the section helps you to accomplish.

You could have arrived here from:
• Page 5 - Start troubleshooting

Directional arrows indicate the path through the process flow.

Yes  Process step
     
Optiona process step

End point

No  Process step with command:
    command xyz
     
Go to Page #

Decision diamond

Note
Provides context and additional information. Sometimes a note is linked to a process step with a colored dot.

CAUTION!
Caution boxes warn that a particular step needs to be performed with great care, to prevent serious consequences.

Document Shape
Calls out supporting documentation for a process step. When possible, these shapes contain links to the reference document. Sometimes linked to a process step with a colored dot.
Appendix C: Example output

Notes
In the examples below, the output provides the following information about the configuration of protocol auditing on the Isilon cluster:

- Protocol auditing is enabled.
- Zone-A and Zone-X are configured for protocol auditing.
- The CEE server URI is http://ceeserver.com:12228/cee.
- The Hostname is myCluster.

OneFS 8.0 and later example output
cluster-1# isi audit settings global view
Protocol Auditing Enabled: Yes
Audited Zones: Zone-A, Zone-X
CEE Server URIs: http://ceeserver.com:12228/cee
Hostname: myCluster
Config Auditing Enabled: No
Config Syslog Enabled: No

OneFS 7.2 example output
cluster-1# isi audit settings view
Protocol Auditing Enabled: Yes
Audited Zones: Zone-A, Zone-X
CEE Server URIs: http://ceeserver.com:12228/cee
Hostname: myCluster
Config Auditing Enabled: No
Config Syslog Enabled: No
Example output

Cluster-1e is1_audit_viewer -t protocol -s "$\{date -v-5M +'%Y-%m-%d %H:%M:%S'\}" -e "$\{date +'%Y-%m-%d %H:%M:%S'\}"
[0] Tue May 12 15:41:10 2020
{"id":"88034f86-9488-11ea-9b22-005056a47069","timestamp":1589312470660307,"payloadType":"c41a642-c139-4c7a-be58-93680bc20b41","payload":{"protocol":"NFS","zoneID":1,"zoneName":"System","eventType":"create","createResult":"OPENED","isDirectory":true,"desiredAccess":0,"clientIPAddr":"10.12.13.14","createDisposition":1,"userSID":"S-1-22-1-0","userID":0,"fileName":"\ifs\datatest","ntStatus":0,"fsId":1,"inode":4298769124}}
[1] Tue May 12 15:41:10 2020
{"id":"880e6505-9488-11ea-9b22-005056a47069","timestamp":1589312470732943,"payloadType":"c41a642-c139-4c7a-be58-93680bc20b41","payload":{"protocol":"NFS","zoneID":1,"zoneName":"System","eventType":"close","isDirectory":true,"clientIPAddr":"10.12.13.14","fileName":"\ifs\datatest","userSID":"S-1-22-1-0","userID":0,"bytesRead":0,"bytesWritten":0,"numberOfReads":0,"numberOfWrites":0,"ntStatus":0,"fsId":1,"inode":4298769124}}
{"id":"880e9cc2-9488-11ea-9b22-005056a47069","timestamp":158931247074387,"payloadType":"c41a642-c139-4c7a-be58-93680bc20b41","payload":{"protocol":"NFS","zoneID":1,"zoneName":"System","eventType":"create","isDirectory":false,"clientIPAddr":"10.12.13.14","createDisposition":1,"userSID":"S-1-22-1-0","userID":0,"fileName":"\ifs\datatest","ntStatus":0,"fsId":1,"inode":4298769124}}
{"id":"88511dcd-9488-11ea-9b22-005056a47069","timestamp":1589312470750791,"payloadType":"c41a642-c139-4c7a-be58-93680bc20b41","payload":{"protocol":"NFS","zoneID":1,"zoneName":"System","eventType":"create","isDirectory":false,"clientIPAddr":10.12.13.14,"createDisposition":1,"userSID":"S-1-22-1-0","userID":0,"bytesRead":0,"bytesWritten":0,"numberOfReads":0,"numberOfWrites":0,"ntStatus":0,"fsId":1,"inode":4298769124}}
{"id":"881366a6-9488-11ea-9b22-005056a47069","timestamp":158931247075874,"payloadType":"c41a642-c139-4c7a-be58-93680bc20b41","payload":{"protocol":"NFS","zoneID":1,"zoneName":"System","eventType":"create","isDirectory":false,"clientIPAddr":10.12.13.14,"createDisposition":1,"userSID":"S-1-22-1-0","userID":0,"bytesRead":0,"bytesWritten":0,"numberOfReads":0,"numberOfWrites":0,"ntStatus":0,"fsId":1,"inode":4298769124}}
{"id":"880ed1e2-9488-11ea-9b22-005056a47069","timestamp":1589312470735725,"payloadType":"c41a642-c139-4c7a-be58-93680bc20b41","payload":{"protocol":"NFS","zoneID":1,"zoneName":"System","eventType":"create","isDirectory":false,"desiredAccess":262272,"clientIPAddr":"10.12.13.14","createDisposition":3,"userSID":"S-1-22-1-0","userID":0,"fileName":\ifs\datatest\tesso","ntStatus":3221225599,"fsId":1,"partialPath":"tesso","rootInode":4298769124}}
{"id":"890475eb-9488-11ea-9b22-005056a47069","timestamp":1589312472345558,"payloadType":"c41a642-c139-4c7a-be58-93680bc20b41","payload":{"protocol":"NFS","zoneID":1,"zoneName":"System","eventType":"create","isDirectory":false,"desiredAccess":262272,"clientIPAddr":"10.12.13.14","createDisposition":3,"userSID":"S-1-22-1-0","userID":0,"fileName":\ifs\datatest\tesso","ntStatus":3221225599,"fsId":1,"partialPath":"tesso","rootInode":4298769124}}
Appendix E: Example output

You could have arrived here from:

- Page 7 - Confirm which events are configured for auditing

Notes

- The following examples show the list of events that are enabled for auditing in the Zone-A access zone.
- The Audit Success and Audit Failure fields contain the list of events that are configured to be audited.
- The Syslog Audit Events field contains the list of events that are configured to be forwarded to Syslog if Syslog forwarding is enabled.

For the complete list of events that can be enabled for auditing, see the OneFS Web Administration Guide or the OneFS CLI Administration Guide for the version of OneFS that is installed on your cluster.

OneFS 8.0 and later example output

```
cluster-1# isi audit settings view --zone=Zone-A
Audit Failure: create, delete, rename, set_security, close
Audit Success: close, create, delete, logoff, logon, read, rename, set_security
Syslog Audit Events: create, delete, rename, set_security
Syslog Forwarding Enabled: No
```

OneFS 7.2 example output

```
cluster-1# isi zone zones view --zone=Zone-A
Name: System
Path: /ifs
Cache Size: 9.54M
Map Untrusted:
Auth Providers: lsad-local-provider:System
NetBIOS Name: All Auth Providers: No
User Mapping Rules: -
Home Directory Umask: 0077
Skeleton Directory: /usr/share/skel
Audit Success: close, create, delete, logon, read, rename, set_security
Audit Failure: create, delete, rename, set_security, close
HDFS Authentication: all
HDFS Root Directory: /ifs
WebHDFS Enabled: Yes
HDFS Ambari Server:
HDFS Ambari Namenode:
HDFS Odp Version: Syslog Forwarding Enabled: No
Syslog Audit Events: create, delete, rename, set_security
Zone ID: 1
```
Appendix F: Example output

You could have arrived here from:

- Page 11 - Confirm that nodes are forwarding events to the CEE server

Example 1 - OneFS 8.0 and later

```
cluster-1: 2018-05-02T15:30:38-04:00 <30.7> cluster-1 isi_audit_cee[48017]: [audit-cee-ipc]
TRACE:0x800742510:lmsg_peer_assoc_session_log_message():lmsg/src/peer-log.c:136:
{session:43dd2377dfe8432f-5a961879e7a3c320} >> 5595) call res AUDIT_CEE_TAG_EXPORT_TOTAL_RES:
{EventsDelivered = 318 } <<<<<<
```

Example 2 - OneFS 7.2

```
2019-12-09 13:12:37 isi-7111b-1 isi_audit_cee[59207][0x800d0200]: DEBUG: Got event
"id":"f486de84-7fce-11e4-99c6-005056a16fbc","timestamp":148148757042760,"payloadType":
"c41a642-c139-4c7a-be58-936b80b202b1","payload":
{"zoneID":1,"zoneName":"System","eventType":
"create","createResult":"OPENED","isDirectory":true,"desiredAccess":1048706,"clientIPAddr":
"178.178.178.221","createDisposition":1,"userSID":"S-1-22-1-0","fileName":"\ifs\home","ntStatus":0,
"handle":"0000000005ca4028"}
```