Manage audit logging for management activities

ONTAP 9

NetApp
May 12, 2022

Table of Contents

Manage audit logging for management activities

How ONTAP implements audit logging

Management activities recorded in the audit log are included in standard AutoSupport reports, and certain logging activities are included in EMS messages. You can also forward the audit log to destinations that you specify, and you can display audit log files by using the CLI or a web browser.

Beginning with ONTAP 9.11.1, you can display audit log contents using System Manager.

ONTAP logs management activities that are performed on the cluster, for example, what request was issued, the user who triggered the request, the user's access method, and the time of the request.

The management activities can be one of the following types:

- SET requests, which typically apply to non-display commands or operations
  - These requests are issued when you run a `create`, `modify`, or `delete` command, for instance.
  - Set requests are logged by default.
- GET requests, which retrieve information and display it in the management interface
  - These requests are issued when you run a `show` command, for instance.
  - GET requests are not logged by default, but you can control whether GET requests sent from the ONTAP CLI (`-cliget`) or from the ONTAP APIs (`-ontapiget`) are logged in the file.

ONTAP records management activities in the `/mroot/etc/log/mlog/audit.log` file of a node. Commands from the three shells for CLI commands—the clustershell, the nodeshell, and the non-interactive systemshell (interactive systemshell commands are not logged)--as well as API commands are logged here. Audit logs include timestamps to show whether all nodes in a cluster are time synchronized.

The `audit.log` file is sent by the AutoSupport tool to the specified recipients. You can also forward the content securely to external destinations that you specify; for example, a Splunk or a syslog server.

The `audit.log` file is rotated daily. The rotation also occurs when it reaches 100 MB in size, and the previous 48 copies are preserved (with a maximum total of 49 files). When the audit file performs its daily rotation, no EMS message is generated. If the audit file rotates because its file size limit is exceeded, an EMS message is generated.

Changes to audit logging in ONTAP 9

Beginning with ONTAP 9, the `command-history.log` file is replaced by `audit.log`, and the `mgwd.log` file no longer contains audit information. If you are upgrading to ONTAP 9, you should review any scripts or tools that refer to the legacy files and their contents.

After upgrade to ONTAP 9, existing `command-history.log` files are preserved. They are rotated out (deleted) as new `audit.log` files are rotated in (created).

Tools and scripts that check the `command-history.log` file might continue to work, because a soft link from

`command-history.log` to `audit.log` is created at upgrade. However, tools and scripts that check the `mgwd.log` file will fail, because that file no longer contains audit information.

In addition, audit logs in ONTAP 9 and later no longer include the following entries because they are not considered useful and cause unnecessary logging activity:

- Internal commands run by ONTAP (that is, where username=root)
- Command aliases (separately from the command they point to)

Beginning with ONTAP 9, you can transmit the audit logs securely to external destinations using the TCP and TLS protocols.

Display audit log contents

You can display the contents of the cluster's `/mroot/etc/log/mlog/audit.log` files by using the ONTAP CLI, System Manager, or a web browser.

The cluster's log file entries include the following:

Time
The log entry timestamp.

Application
The application used to connect to the cluster. Examples of possible values are `internal`, `console`, `ssh`, `http`, `ontapi`, `snmp`, `rsh`, `telnet`, and `service-processor`.

User
The username of the remote user.

State
The current state of the audit request, which could be `success`, `pending`, or `error`.

Message
An optional field that might contain error or additional information about the status of a command.

Session ID
The session ID on which the request is received. Each SSH *session* is assigned a session ID, while each HTTP, ONTAPI, or SNMP *request* is assigned a unique session ID.

Storage VM
The SVM through which the user connected.

Scope
Displays `svm` when the request is on a data storage VM; otherwise displays `cluster`.

Command ID
The ID for each command received on a CLI session. This enables you to correlate a request and response. ZAPI, HTTP, and SNMP requests do not have command IDs.

You can display the cluster's log entries from the ONTAP CLI, from a web browser, and beginning with ONTAP 9.11.1, from System Manager.

System Manager

- To display the inventory, select **Events & Jobs > Audit Logs**.
  Each column has controls to filter, sort, search, show, and inventory categories. The inventory details can be downloaded as an Excel workbook.
- To set filters, click the **Filter** button on the upper right side, then select the desired fields.
  You can also view all the commands executed in the session in which a failure occurred by clicking on the Session ID link.

CLI

To display audit entries merged from multiple nodes in the cluster, enter:
`security audit log show` *`[parameters]`*

You can use the `security audit log show` command to display audit entries for individual nodes or merged from multiple nodes in the cluster. You can also display the content of the `/mroot/etc/log/mlog` directory on a single node by using a web browser. See the man page for details.

Web browser

You can display the content of the `/mroot/etc/log/mlog` directory on a single node by using a web browser. Learn about how to access a node's log, core dump, and MIB files by using a web browser.

Manage audit GET request settings

While SET requests are logged by default, GET requests are not. However, you can control whether GET requests sent from ONTAP HTML (`-httpget`), the ONTAP CLI (`-cliget`), or from the ONTAP APIs (`-ontapiget`) are logged in the file.

You can modify audit logging settings from the ONTAP CLI, and beginning with ONTAP 9.11.1, from System Manager.

System Manager

1. Select **Events & Jobs > Audit Logs**.
2. Click ⚙ in the upper-right corner, then choose the requests to add or remove.

CLI

- To specify that GET requests from the ONTAP CLI or APIs should be recorded in the audit log (the audit.log file), in addition to default set requests, enter:
  `security audit modify [-cliget {on|off}][-httpget {on|off}][-ontapiget {on|off}]`
- To display the current settings, enter:
  `security audit show`

See the man pages for details.

Manage audit log destinations

You can forward the audit log to a maximum of 10 destinations. For example, you can forward the log to a Splunk or syslog server for monitoring, analysis, or backup purposes.

About this task

To configure forwarding, you must provide the IP address of the syslog or Splunk host, its port number, a transmission protocol, and the syslog facility to use for the forwarded logs. Learn about syslog facilities.

You can select one of the following transmission values:

UDP Unencrypted

User Datagram Protocol with no security (default)

TCP Unencrypted

Transmission Control Protocol with no security

TCP Encrypted

Transmission Control Protocol with Transport Layer Security (TLS)
A **Verify server** option is available when the TCP Encrypted protocol is selected.

You can forward audit logs from the ONTAP CLI, and beginning with ONTAP 9.11.1, from System Manager.

System Manager

- To display audit log destinations, select **Cluster >Settings**.
  A count of log destinations is shown in the **Notification Management tile**. Click ⋮ to show details.
- To add, modify, or delete audit log destinations, select **Events & Jobs > Audit Logs**, then click **Manage Audit Destinations** in the upper right of the screen.
  Click + Add, or click ⋮ in the **Host Address** column to edit or delete entries.

CLI

1. For each destination that you want to forward the audit log to, specify the destination IP address or host name and any security options.

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 514 -protocol tcp-encrypted -facility user
```

   - If the `cluster log-forwarding create` command cannot ping the destination host to verify connectivity, the command fails with an error. Although not recommended, using the `-force` parameter with the command bypasses the connectivity verification.
   - When you set the `-verify-server` parameter to `true`, the identity of the log forwarding destination is verified by validating its certificate. You can set the value to `true` only when you select the `tcp-encrypted` value in the `-protocol` field.

2. Verify that the destination records are correct by using the `cluster log-forwarding show` command.

```
cluster1::> cluster log-forwarding show

                                              Verify Syslog
Destination Host          Port   Protocol        Server Facility
------------------------- ------ --------        ------ --------
192.168.123.96            514    udp-unencrypted false  user
192.168.123.98            514    tcp-encrypted   true   user
2 entries were displayed.
```

See the man pages for details.