Manage audit logging for management activities

ONTAP 9

NetApp
February 22, 2022

Table of Contents

Manage audit logging for management activities . . . 1
Changes to audit logging in ONTAP 9 . . . 1
How ONTAP implements audit logging . . . 1
Forward the audit log to a destination . . . 2
Commands for managing audit settings for management activities . . . 3

Manage audit logging for management activities

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.

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.

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 use the `security audit modify` command to 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.

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.

Forward the audit log to a destination

You can forward the audit log to a maximum of 10 destinations that you specify by using the `cluster log-forwarding create` command. For example, you can forward the log to a Splunk or syslog server for monitoring, analysis, or backup purposes.

About this task

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.

You can configure transmission security options when forwarding log files:

- Protocols for sending messages to the destination

  You can select one of the following `-protocol` 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)
- Verification of destination server identity

  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.

Steps

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
```

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.
```

Related information

ONTAP 9 commands

Commands for managing audit settings for management activities

You use the `security audit` commands to manage which management activities are logged in the `audit.log` file. You use the `cluster log-forwarding` commands to manage destinations for forwarding the audit log to.

If you want to…	Use this command…
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	`security audit modify`
Display the settings of the audit log	`security audit show`
Display audit entries merged from multiple nodes in the cluster	`security audit log show`
Specify a forwarding destination for the audit log and security measures for its transmission	`cluster log-forwarding create`
Modify a destination for the audit log	`cluster log-forwarding modify`

If you want to…	Use this command…
Delete a destination for the audit log	`cluster log-forwarding delete`
Show the configured destinations for the audit log	`cluster log-forwarding show`

Related information

ONTAP 9 commands