security audit commands

ONTAP 9.12.1 commands

NetApp
December 14, 2022

Table of Contents

security audit commands

security audit modify

Set administrative audit logging settings

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `security audit modify` command modifies the following audit-logging settings for the management interface:

- Whether get requests for the CLI are audited
- Whether get requests for the Data ONTAP API (ONTAPI) are audited

Parameters

`[-cliget {on|off}]` - Enable Auditing of CLI Get Operations

This specifies whether get requests for the CLI are audited. The default setting is *`off`* .

`[-httpget {on|off}]` - Enable Auditing of HTTP Get Operations

This specifies whether get requests for the web (HTTP) interface are audited. The default setting is *`off`* .

`[-ontapiget {on|off}]` - Enable Auditing of Data ONTAP API Get Operations

This specifies whether get requests for the Data ONTAP API (ONTAPI) interface are audited. The default setting is *`off`* .

Examples

The following example turns off auditing of get requests for the CLI interface:

```
cluster1::> security audit modify -cliget off
```

security audit show

Show administrative audit logging settings

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `security audit show` command displays the following audit-logging settings for the management interface:

- Whether get requests for the CLI are audited
- Whether get requests for the web (HTTP) interface are audited

- Whether get requests for the Data ONTAP API (ONTAPI) are audited

Audit log entries are written to the 'audit' log, viewable via the 'security audit log show' command.

Examples

The following example displays the audit-logging settings for the management interface:

```
cluster1::> security audit show
               Auditing State for
    Operation Get Requests
    --------- ------------------
          CLI off
         HTTP off
       ONTAPI off
```

security audit log show

Display audit entries merged from multiple nodes in the cluster

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `security audit log show` command displays cluster-wide audit log messages. Messages from each node are interleaved in chronological order.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-detail]

This display option shows the individual fields of the audit record.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-timestamp <Date>] - Log Entry Timestamp

Selects the entries that match the specified input for timestamp. This will be in a human-readable format <day> <month> <day of month> <hour>:<min>:<sec> <year> in the local timezone.

[-node {<nodename>|local}] - Node

Selects the entries that match the specified input for node.

[-entry <text>] - Log Message Entry

Selects the entries that match the specified input for entry.

[-session-id <text>] - Session ID

This is the "session id" for this audit record. Eash ssh/console session is assigned a unique session ID. Eash ZAPI/HTTP/SNMP request is assigned a uniqueue session ID

[-command-id <text>] - Command ID

This is useful with ssh/console sessions. Each command in a session is assigned a unique command ID. Each ZAPI/HTTP/SNMP request does not have a command ID.

[-application <text>] - Protocol

This is the application used to connect to the cluster. Possible values include the following: internal, console, ssh, http, ontapi, snmp, rsh, telnet, service-processor

[-location <text>] - Remote user location

The remote IP address or remote access point.

[-vserver <text>] - Vserver name

Storage Virtual Machine name

[-username <text>] - Username

Username

[-input <text>] - Command being executed

The operation being attempted

[-state {Pending|Success|Error}] - State of this audit request

State of this request

[-message <text>] - Additional information and/or error message

Additional information which may be error or informative message.

Examples

The following example displays specific fields based on a custom query:

```
cluster1::> security audit log show -fields application, location, state,
input, message -location 10.60.* -state Error|Success -input v*|st*
-timestamp >"Jul 10 12:00:00 2020"
timestamp                  node  application location     input
state   message
-------------------------- ----- ----------- ------------
---------------------------------------- ------- -------
"Fri Jul 17 11:32:44 2020" node1 ssh         10.60.250.79 storage
aggregate create test -diskcount 5 Success -
"Fri Jul 17 11:36:47 2020" node1 ssh         10.60.250.79 vserver create
vs1                         Success -
```

```
"Fri Jul 17 11:37:33 2020" node1 ssh         10.60.250.79 volume create
vol1                          Error   One of the following parameters is
required: -aggregate, -aggr-list, -auto-provision-as
"Fri Jul 17 11:38:08 2020" node1 ssh         10.60.250.79 volume create
vol1 -aggregate test          Success -
Some more examples for -timestamp usage:
cluster1::> security audit log show -timestamp "Mon Jan 03 18:37:05 2022"
Time                        Node          Audit Message
--------------------------  ------------  ----------------------
Mon Jan 03 18:37:05 2022  node1
                                          [kern_audit:info:988] mlogd:
started

cluster1::> security audit log show -timestamp Mon Jan 03 *
Time                        Node          Audit Message
--------------------------  ------------  ----------------------
Mon Jan 03 18:37:05 2022  node1
                                          [kern_audit:info:988] mlogd:
started
Mon Jan 03 18:37:06 2022  node2
                                          [kern_audit:info:988] mlogd:
started
Mon Jan 03 18:41:25 2022  node1
                                          [kern_audit:info:977] mlogd:
started
Mon Jan 03 18:41:25 2022  node2
                                          [kern_audit:info:977] mlogd:
started

cluster1::> security audit log show -timestamp Mon Jan 03 18:37*
Time                        Node          Audit Message
--------------------------  ------------  ----------------------
Mon Jan 03 18:37:05 2022  node1
                                          [kern_audit:info:988] mlogd:
started
Mon Jan 03 18:37:06 2022  node2
                                          [kern_audit:info:988] mlogd:
started
2 entries were displayed.
```

Copyright information

Trademark information