



security audit commands

ONTAP 9.13.1 commands

NetApp

February 12, 2024

Table of Contents

- security audit commands 1
 - security audit modify 1
 - security audit show 1
 - security audit log show 2

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. Each ssh/console session is assigned a unique session ID. Each ZAPI/HTTP/SNMP request is assigned a unique 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 vs1
vs1                      Success -
```

```

"Fri Jul 17 11:37:33 2020" node1 ssh 10.60.250.79 volume create
voll 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
voll -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

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.