



View administrative audit logs

ONTAP 9.13.1 REST API reference

NetApp
August 29, 2024

Table of Contents

- View administrative audit logs 1
- Security audit messages endpoint overview 1
- Retrieve the administrative audit log viewer 2

View administrative audit logs

Security audit messages endpoint overview

Overview

These APIs return audit log records. The GET requests retrieves all audit log records. An audit log record contains information such as timestamp, node name, index and so on.

Example

Retrieving audit log records

The following example shows the audit log records.

```
# The API:
/api/security/audit/messages

# The call:
curl -X GET "https://<cluster-ip>/api/security/audit/messages"

# The response:
{
  "records": [
    {
      "timestamp": "2019-03-08T11:03:32-05:00",
      "node": {
        "name": "node1",
        "uuid": "bc9af9da-41bb-11e9-a3db-005056bb27cf",
        "_links": {
          "self": {
            "href": "/api/cluster/nodes/bc9af9da-41bb-11e9-a3db-005056bb27cf"
          }
        }
      },
      "index": 4294967299,
      "application": "http",
      "location": "172.21.16.89",
      "user": "admin",
      "input": "GET /api/security/audit/destinations/",
      "state": "pending",
      "scope": "cluster"
    }
  ],
  "num_records": 1,
  "_links": {
    "self": {
      "href": "/api/security/audit/messages"
    }
  }
}
```

Retrieve the administrative audit log viewer

GET /security/audit/messages

Introduced In: 9.6

Retrieves the administrative audit log viewer.

Parameters

Name	Type	In	Required	Description
command_id	string	query	False	Filter by command_id
application	string	query	False	Filter by application
state	string	query	False	Filter by state
node.uuid	string	query	False	Filter by node.uuid
node.name	string	query	False	Filter by node.name
session_id	string	query	False	Filter by session_id
timestamp	string	query	False	Filter by timestamp
user	string	query	False	Filter by user
scope	string	query	False	Filter by scope
location	string	query	False	Filter by location
index	integer	query	False	Filter by index
svm.name	string	query	False	Filter by svm.name
message	string	query	False	Filter by message
input	string	query	False	Filter by input
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.

Name	Type	In	Required	Description
return_timeout	integer	query	False	<p>The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached.</p> <ul style="list-style-type: none"> • Default value: 1 • Max value: 120 • Min value: 0
return_records	boolean	query	False	<p>The default is true for GET calls. When set to false, only the number of records is returned.</p> <ul style="list-style-type: none"> • Default value: 1
order_by	array[string]	query	False	<p>Order results by specified fields and optional [asc</p>

Response

Status: 200, Ok

Name	Type	Description
_links	_links	
num_records	integer	Number of records
records	array[security_audit_log]	

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "application": "string",
      "command_id": "string",
      "index": 0,
      "input": "string",
      "location": "string",
      "message": "string",
      "node": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "node1",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      },
      "scope": "string",
      "session_id": "string",
      "state": "string",
      "svm": {
        "name": "string"
      },
      "timestamp": "string",
      "user": "string"
    }
  ]
}
```

Error

Status: Default, Error

Name	Type	Description
error	error	

Example error

```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

node

Node where the audit message resides.

Name	Type	Description
_links	_links	
name	string	
uuid	string	

svm

This is the SVM through which the user connected.

Name	Type	Description
name	string	

security_audit_log

Name	Type	Description
_links	_links	
application	string	This identifies the "application" by which the request was processed.

Name	Type	Description
command_id	string	This is the command ID for this request. Each command received on a CLI session is assigned a command ID. This enables you to correlate a request and response.
index	integer	Internal index for accessing records with same time/node. This is a 64 bit unsigned value.
input	string	The request.
location	string	This identifies the location of the remote user. This is an IP address or "console".
message	string	This is an optional field that might contain "error" or "additional information" about the status of a command.
node	node	Node where the audit message resides.
scope	string	Set to "svm" when the request is on a data SVM; otherwise set to "cluster".
session_id	string	This is the session ID on which the request is received. Each SSH session is assigned a session ID. Each http/ontapi/snmp request is assigned a unique session ID.
state	string	State of of this request.
svm	svm	This is the SVM through which the user connected.
timestamp	string	Log entry timestamp. Valid in URL
user	string	Username of the remote user.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

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.