# Manage NAS audit configurations

## REST API reference

NetApp
September 12, 2025

This PDF was generated from https://docs.netapp.com/us-en/ontap-restapi-9101/protocols_audit_endpoint_overview.html on September 12, 2025. Always check docs.netapp.com for the latest.

# Table of Contents


Manage NAS audit configurations . . . 1
- Protocols audit endpoint overview . . . 1
  - Overview . . . 1
  - Examples . . . 1
- Retrieve audit configurations . . . 9
  - Related ONTAP commands . . . 9
  - Learn more . . . 9
  - Parameters . . . 9
  - Response . . . 12
  - Error . . . 14
  - Definitions . . . 14
- Create an audit configuration . . . 19
  - Required properties . . . 19
  - Default property values . . . 19
  - Related ONTAP commands . . . 19
  - Learn more . . . 20
  - Parameters . . . 20
  - Request Body . . . 20
  - Response . . . 22
  - Error . . . 24
  - Definitions . . . 25
- Delete an audit configuration . . . 29
  - Related ONTAP commands . . . 29
  - Learn more . . . 29
  - Parameters . . . 30
  - Response . . . 30
  - Error . . . 31
  - Definitions . . . 32
- Retrieve the audit configuration for an SVM . . . 32
  - Related ONTAP commands . . . 32
  - Learn more . . . 32
  - Parameters . . . 32
  - Response . . . 33
  - Error . . . 35
  - Definitions . . . 35
- Update the audit configuration for an SVM . . . 39
  - Related ONTAP commands . . . 39
  - Learn more . . . 39
  - Parameters . . . 39
  - Request Body . . . 40
  - Response . . . 42
  - Error . . . 42
  - Definitions . . . 43

# Manage NAS audit configurations

## Protocols audit endpoint overview

### Overview

Auditing for NAS events is a security measure that enables you to track and log certain CIFS and NFS events on storage virtual machines (SVMs). This helps you track potential security problems and provides evidence of any security breaches.

### Examples

#### Creating an audit entry with log rotation size and log retention count

To create an audit entry with log rotation size and log retention count, use the following API. Note the *return_records=true* query parameter is used to obtain the newly created entry in the response.

```
# The API:
POST /api/protocols/audit/

# The call:
curl -X POST "https://<mgmt-ip>/api/protocols/audit" -H "accept:
application/json" -H "Content-Type: application/json" -d "{ \"enabled\":
true, \"events\": { \"authorization_policy\": false, \"cap_staging\":
false, \"cifs_logon_logoff\": true, \"file_operations\": true,
\"file_share\": false, \"security_group\": false, \"user_account\": false
}, \"guarantee\": true, \"log\": { \"format\": \"evtx\", \"retention\": {
\"count\": 10 }, \"rotation\": { \"size\": 2048000 }}, \"log_path\":
\"/\", \"svm\": { \"name\": \"vs1\", \"uuid\": \"ec650e97-156e-11e9-abcb-
005056bbd0bf\" }}"

# The response:
{
"records": [
  {
    "svm": {
      "uuid": "ec650e97-156e-11e9-abcb-005056bbd0bf",
      "name": "vs1"
    },
    "enabled": true,
    "events": {
      "authorization_policy": false,
      "cap_staging": false,
```

```
      "cifs_logon_logoff": true,
      "file_operations": true,
      "file_share": false,
      "security_group": false,
      "user_account": false
    },
    "log": {
      "format": "evtx",
      "rotation": {
        "size": 2048000
      },
      "retention": {
        "count": 10,
        "duration": "0s"
      }
    },
    "log_path": "/",
    "guarantee": true
  }
],
"num_records": 1
}
```

#### Creating an audit entry with log rotation schedule and log retention duration

To create an audit entry with log rotation schedule and log retention duration, use the following API. Note that the *return_records=true* query parameter is used to obtain the newly created entry in the response.

```
# The API:
POST /api/protocols/audit/

# The call:
curl -X POST "https://<mgmt-ip>/api/protocols/audit" -H "accept:
application/json" -H "Content-Type: application/json" -d "{ \"enabled\":
false, \"events\": { \"authorization_policy\": false, \"cap_staging\":
false, \"cifs_logon_logoff\": true, \"file_operations\": true,
\"file_share\": false, \"security_group\": false, \"user_account\": false
}, \"guarantee\": true, \"log\": { \"format\": \"xml\", \"retention\": {
\"duration\": \"P4DT12H30M5S\" }, \"rotation\": { \"schedule\": {
\"days\": [1, 5, 10, 15], \"hours\": [0, 1, 6, 12, 18, 23], \"minutes\":
[10, 15, 30, 45, 59], \"months\": [0], \"weekdays\": [0, 2, 5] } } },
\"log_path\": \"/\", \"svm\": { \"name\": \"vs3\", \"uuid\": \"a8d64674-
13fc-11e9-87b1-005056a7ae7e\" }}"
```

```
# The response:
{
"records": [
  {
    "svm": {
      "uuid": "a8d64674-13fc-11e9-87b1-005056a7ae7e",
      "name": "vs3"
    },
    "enabled": true,
    "events": {
      "authorization_policy": false,
      "cap_staging": false,
      "cifs_logon_logoff": true,
      "file_operations": true,
      "file_share": false,
      "security_group": false,
      "user_account": false
    },
    "log": {
      "format": "xml",
      "rotation": {
        "schedule": {
          "minutes": [
            10,
            15,
            30,
            45,
            59
          ],
          "hours": [
            0,
            1,
            6,
            12,
            18,
            23
          ],
          "weekdays": [
            0,
            2,
            5
          ],
          "days": [
            1,
            5,
```

```
            10,
            15
          ],
          "months": [
            0
          ]
        }
      },
      "retention": {
        "count": 0,
        "duration": "P4DT12H30M5S"
      }
    },
    "log_path": "/",
    "guarantee": true
  }
],
"num_records": 1
}
```

#### Retrieving an audit configuration for all SVMs in the cluster

```
# The API:
GET /api/protocols/audit/

# The call:
curl -X GET "https://<mgmt-
ip>/api/protocols/audit?fields=*&return_records=true&return_timeout=15" -H
"accept: application/json"

# The response:
{
"records": [
  {
    "svm": {
      "uuid": "ec650e97-156e-11e9-abcb-005056bbd0bf",
      "name": "vs1"
    },
    "enabled": true,
    "events": {
      "authorization_policy": false,
      "cap_staging": false,
```

```
      "cifs_logon_logoff": true,
      "file_operations": true,
      "file_share": false,
      "security_group": false,
      "user_account": false
    },
    "log": {
      "format": "evtx",
      "rotation": {
        "size": 2048000
      },
      "retention": {
        "count": 10,
        "duration": "0s"
      }
    },
    "log_path": "/",
    "guarantee": true
  },
  {
    "svm": {
      "uuid": "a8d64674-13fc-11e9-87b1-005056a7ae7e",
      "name": "vs3"
    },
    "enabled": true,
    "events": {
      "authorization_policy": false,
      "cap_staging": false,
      "cifs_logon_logoff": true,
      "file_operations": true,
      "file_share": false,
      "security_group": false,
      "user_account": false
    },
    "log": {
      "format": "xml",
      "rotation": {
        "schedule": {
          "minutes": [
            10,
            15,
            30,
            45,
            59
          ],
          "hours": [
```

```
            0,
            1,
            6,
            12,
            18,
            23
          ],
          "weekdays": [
            0,
            2,
            5
          ],
          "days": [
            1,
            5,
            10,
            15
          ],
          "months": [
            0
          ]
        }
      },
      "retention": {
        "count": 0,
        "duration": "P4DT12H30M5S"
      }
    },
    "log_path": "/",
    "guarantee": true
  }
],
"num_records": 2
}
```


**Retrieving specific entries with event list as cifs-logon-logoff, file-ops = true for an SVM**

The configuration returned is identified by the events in the list of audit configurations for an SVM.

```
# The API:
GET /api/protocols/audit/

# The call:
curl -X GET "https://<mgmt-
ip>/api/protocols/audit?events.file_operations=true&events.cifs_logon_logo
ff=true&return_records=true&return_timeout=15" -H "accept:
application/json"

# The response:
{
"records": [
  {
    "svm": {
      "uuid": "ec650e97-156e-11e9-abcb-005056bbd0bf",
      "name": "vs1"
    },
    "events": {
      "cifs_logon_logoff": true,
      "file_operations": true
    }
  },
  {
    "svm": {
      "uuid": "a8d64674-13fc-11e9-87b1-005056a7ae7e",
      "name": "vs3"
    },
    "events": {
      "cifs_logon_logoff": true,
      "file_operations": true
    }
  }
],
"num_records": 2
}
```

#### Retrieving a specific audit configuration for an SVM

The configuration returned is identified by the UUID of its SVM.

```
# The API:
GET /api/protocols/audit/{svm.uuid}

# The call:
curl -X GET "https://<mgmt-ip>/api/protocols/audit/ec650e97-156e-11e9-
abcb-005056bbd0bf" -H "accept: application/json"

# The response:
{
"svm": {
  "uuid": "ec650e97-156e-11e9-abcb-005056bbd0bf",
  "name": "vs1"
},
"enabled": true,
"events": {
  "authorization_policy": false,
  "cap_staging": false,
  "cifs_logon_logoff": true,
  "file_operations": true,
  "file_share" : false,
  "security_group": false,
  "user_account": false
},
"log": {
  "format": "evtx",
  "rotation": {
    "size": 2048000
  },
  "retention": {
    "count": 10,
    "duration": "0s"
  }
},
"log_path": "/",
"guarantee": true
}
```

#### Updating a specific audit configuration of an SVM

The configuration is identified by the UUID of its SVM and the provided information is updated.

```
# The API:
PATCH /api/protocols/audit/{svm.uuid}

# The call:
curl -X PATCH "https://<mgmt-ip>/api/protocols/audit/ec650e97-156e-11e9-
abcb-005056bbd0bf" -H "accept: application/json" -H "Content-Type:
application/json" -d "{ \"enabled\": false}"
```

#### Deleting a specific audit configuration for an SVM

The entry to be deleted is identified by the UUID of its SVM.

```
# The API:
DELETE /api/protocols/audit/{svm.uuid}

# The call:
curl -X DELETE "https://<mgmt-ip>/api/protocols/audit/ec650e97-156e-11e9-
abcb-005056bbd0bf?force=true" -H "accept: application/json"
```

# Retrieve audit configurations

GET `/protocols/audit`

**Introduced In:** 9.6

Retrieves audit configurations.

## Related ONTAP commands

- `vserver audit show`

## Learn more

- DOC /protocols/audit

## Parameters

| Name | Type | In | Required | Description |
|---|---|---|---|---|
| guarantee | boolean | query | False | Filter by guarantee<br>• Introduced in: 9.10 |

| Name | Type | In | Required | Description |
|---|---|---|---|---|
| log_path | string | query | False | Filter by log_path |
| enabled | boolean | query | False | Filter by enabled |
| log.format | string | query | False | Filter by log.format |
| log.retention.count | integer | query | False | Filter by log.retention.count |
| log.retention.duration | string | query | False | Filter by log.retention.duration |
| log.rotation.schedule.months | integer | query | False | Filter by log.rotation.schedule.months |
| log.rotation.schedule.days | integer | query | False | Filter by log.rotation.schedule.days |
| log.rotation.schedule.hours | integer | query | False | Filter by log.rotation.schedule.hours |
| log.rotation.schedule.minutes | integer | query | False | Filter by log.rotation.schedule.minutes |
| log.rotation.schedule.weekdays | integer | query | False | Filter by log.rotation.schedule.weekdays |
| log.rotation.size | integer | query | False | Filter by log.rotation.size |
| svm.uuid | string | query | False | Filter by svm.uuid |
| svm.name | string | query | False | Filter by svm.name |
| events.authorization_policy | boolean | query | False | Filter by events.authorization_policy |

| Name | Type | In | Required | Description |
|---|---|---|---|---|
| events.cifs_logon_logoff | boolean | query | False | Filter by events.cifs_logon_logoff |
| events.user_account | boolean | query | False | Filter by events.user_account |
| events.cap_staging | boolean | query | False | Filter by events.cap_staging |
| events.security_group | boolean | query | False | Filter by events.security_group |
| events.file_operations | boolean | query | False | Filter by events.file_operations |
| events.file_share | boolean | query | False | Filter by events.file_share |
| fields | array[string] | query | False | Specify the fields to return. |
| max_records | integer | query | False | Limit the number of records returned. |
| return_records | boolean | query | False | The default is true for GET calls. When set to false, only the number of records is returned.<br>• Default value: 1 |

| Name | Type | In | Required | Description |
|---|---|---|---|---|
| return_timeout | integer | query | False | 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.<br>• Default value: 1<br>• Max value: 120<br>• Min value: 0 |
| order_by | array[string] | query | False | Order results by specified fields and optional [asc |

## Response

```
Status: 200, Ok
```

| Name | Type | Description |
|---|---|---|
| _links | _links | |
| num_records | integer | Number of records |
| records | array[audit] | |

**Example response**


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": [
    {
      "guarantee": "",
      "log": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "format": "string",
        "retention": {
          "duration": "P4DT12H30M5S"
        },
        "rotation": {
          "schedule": {
            "days": [
              "integer"
            ],
            "hours": [
              "integer"
            ],
            "minutes": [
              "integer"
            ],
            "months": [
              "integer"
            ],
            "weekdays": [
              "integer"
            ]
          }
        }
      },
      "log_path": "string",
      "svm": {
```

```
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      }
    }
  ]
}
```


## 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 | |

events

| Name | Type | Description |
|---|---|---|
| authorization_policy | boolean | Authorization policy change events |
| cap_staging | boolean | Central access policy staging events |
| cifs_logon_logoff | boolean | CIFS logon and logoff events |
| file_operations | boolean | File operation events |
| file_share | boolean | File share category events |
| security_group | boolean | Local security group management events |
| user_account | boolean | Local user account management events |

_links

| Name | Type | Description |
|---|---|---|
| self | href | |

retention

| Name | Type | Description |
|---|---|---|
| count | integer | Determines how many audit log files to retain before rotating the oldest log file out. This is mutually exclusive with duration. |
| duration | string | Specifies an ISO-8601 format date and time to retain the audit log file. The audit log files are deleted once they reach the specified date/time. This is mutually exclusive with count. |

audit_schedule

Rotates the audit logs based on a schedule by using the time-based rotation parameters in any combination. The rotation schedule is calculated by using all the time-related values.

| Name | Type | Description |
|---|---|---|
| days | array[integer] | Specifies the day of the month schedule to rotate audit log. Leave empty for all. |
| hours | array[integer] | Specifies the hourly schedule to rotate audit log. Leave empty for all. |
| minutes | array[integer] | Specifies the minutes schedule to rotate the audit log. |
| months | array[integer] | Specifies the months schedule to rotate audit log. Leave empty for all. |
| weekdays | array[integer] | Specifies the weekdays schedule to rotate audit log. Leave empty for all. |

rotation

Audit event log files are rotated when they reach a configured threshold log size or are on a configured schedule. When an event log file is rotated, the scheduled consolidation task first renames the active converted file to a time-stamped archive file, and then creates a new active converted event log file.

| Name | Type | Description |
|---|---|---|
| now | boolean | Manually rotates the audit logs. Optional in PATCH only. Not available in POST. |
| schedule | audit_schedule | Rotates the audit logs based on a schedule by using the time-based rotation parameters in any combination. The rotation schedule is calculated by using all the time-related values. |
| size | integer | Rotates logs based on log size in bytes. |

log

| Name | Type | Description |
|---|---|---|
| _links | _links | |
| format | string | The format in which the logs are generated by consolidation process. Possible values are:<br>• xml - Data ONTAP-specific XML log format<br>• evtx - Microsoft Windows EVTX log format<br>◦ Default value: 1<br>◦ enum: ["xml", "evtx"]<br>◦ Introduced in: 9.6 |
| retention | retention | |
| rotation | rotation | Audit event log files are rotated when they reach a configured threshold log size or are on a configured schedule. When an event log file is rotated, the scheduled consolidation task first renames the active converted file to a time-stamped archive file, and then creates a new active converted event log file. |

svm

| Name | Type | Description |
|---|---|---|
| _links | _links | |
| name | string | The name of the SVM. |
| uuid | string | The unique identifier of the SVM. |

audit

Auditing for NAS events is a security measure that enables you to track and log certain CIFS and NFS events on SVMs.

| Name | Type | Description |
|---|---|---|
| enabled | boolean | Specifies whether or not auditing is enabled on the SVM. |
| events | events | |
| guarantee | boolean | Indicates whether there is a strict Guarantee of Auditing |
| log | log | |
| log_path | string | The audit log destination path where consolidated audit logs are stored. |
| svm | svm | |

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 |

| Name | Type | Description |
|---|---|---|
| target | string | The target parameter that caused the error. |

# Create an audit configuration

POST `/protocols/audit`

**Introduced In:** 9.6

Creates an audit configuration.

## Required properties

- `svm.uuid` or `svm.name` - Existing SVM to which audit configuration is to be created.
- `log_path` - Path in the owning SVM namespace that is used to store audit logs.

## Default property values

If not specified in POST, the following default property values are assigned:

- `enabled` - *true*
- `events.authorization_policy` - *false*
- `events.cap_staging` - *false*
- `events.file_share` - *false*
- `events.security_group` - *false*
- `events.user_account` - *false*
- `events.cifs_logon_logoff` - *true*
- `events.file_operations` - *true*
- `log.format` - *evtx*
- `log.retention.count` - *0*
- `log.retention.duration` - *PT0S*
- `log.rotation.size` - *100MB*
- `log.rotation.now` - *false*
- `guarantee` - *true*

## Related ONTAP commands

- `vserver audit create`
- `vserver audit enable`

## Learn more

- DOC /protocols/audit

## Parameters

| Name | Type | In | Required | Description |
|---|---|---|---|---|
| return_timeout | integer | query | False | The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.<br>• Default value: 1<br>• Max value: 120<br>• Min value: 0 |
| return_records | boolean | query | False | The default is false. If set to true, the records are returned.<br>• Default value: |

## Request Body

| Name | Type | Description |
| --- | --- | --- |
| enabled | boolean | Specifies whether or not auditing is enabled on the SVM. |
| events | events | |
| guarantee | boolean | Indicates whether there is a strict Guarantee of Auditing |
| log | log | |
| log_path | string | The audit log destination path where consolidated audit logs are stored. |
| svm | svm | |

**Example request**

```
{
  "guarantee": "",
  "log": {
    "format": "string",
    "retention": {
      "duration": "P4DT12H30M5S"
    },
    "rotation": {
      "schedule": {
        "days": [
          "integer"
        ],
        "hours": [
          "integer"
        ],
        "minutes": [
          "integer"
        ],
        "months": [
          "integer"
        ],
        "weekdays": [
          "integer"
        ]
      }
    }
  },
  "log_path": "string",
  "svm": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```

## Response

```
Status: 202, Accepted
```

| Name | Type | Description |
|---|---|---|
| num_records | integer | Number of records |

| Name | Type | Description |
| --- | --- | --- |
| records | array[audit] | |

**Example response**


```
{
  "records": [
    {
      "guarantee": "",
      "log": {
        "format": "string",
        "retention": {
          "duration": "P4DT12H30M5S"
        },
        "rotation": {
          "schedule": {
            "days": [
              "integer"
            ],
            "hours": [
              "integer"
            ],
            "minutes": [
              "integer"
            ],
            "months": [
              "integer"
            ],
            "weekdays": [
              "integer"
            ]
          }
        }
      },
      "log_path": "string",
      "svm": {
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      }
    }
  ]
}
```

## Error

```
Status: Default
```

ONTAP Error Response Codes

| Error Code | Description |
|---|---|
| 262196 | Log_rotation_now is not an allowed operation |
| 2621462 | The specified SVM does not exist |
| 9699330 | An audit configuration already exists |
| 9699337 | Audit system internal update is in progress, audit configuration create failed |
| 9699340 | SVM UUID lookup failed |
| 9699358 | Audit configuration is absent for enabling |
| 9699359 | Audit configuration is already enabled |
| 9699360 | Final consolidation is in progress, audit enable failed |
| 9699365 | Enabling of audit configuration failed |
| 9699370 | Auditing was successfully configured, however audit configuration could not be enabled |
| 9699384 | The specified log_path does not exist |
| 9699385 | The log_path must be a directory |
| 9699386 | The log_path must be a canonical path in the SVMs namespace |
| 9699387 | The log_path cannot be empty |
| 9699388 | Rotate size must be greater than or equal to 1024 KB |
| 9699389 | The log_path must not contain a symbolic link |
| 9699398 | The log_path exceeds a maximum supported length of characters |
| 9699399 | The log_path contains an unsupported read-only (DP/LS) volume |
| 9699400 | The specified log_path is not a valid destination for SVM |
| 9699402 | The log_path contains an unsupported snaplock volume |
| 9699403 | The log_path cannot be accessed for validation |
| 9699406 | The log_path validation failed |
| 9699409 | Failed to enable multiproto.audit.evtxlog.support support capability |

| Error Code | Description |
| --- | --- |
| 9699428 | All nodes need to run ONTAP 8.3.0 release to audit CIFS logon-logoff events |
| 9699429 | Failed to enable multiproto.audit.cifslogonlogoff.support support capability |
| 9699431 | All nodes need to run ONTAP 8.3.0 release to audit CAP staging events |
| 9699432 | Failed to enable multiproto.audit.capstaging.support support capability |

## Definitions

**See Definitions**

events

| Name | Type | Description |
|---|---|---|
| authorization_policy | boolean | Authorization policy change events |
| cap_staging | boolean | Central access policy staging events |
| cifs_logon_logoff | boolean | CIFS logon and logoff events |
| file_operations | boolean | File operation events |
| file_share | boolean | File share category events |
| security_group | boolean | Local security group management events |
| user_account | boolean | Local user account management events |

href

| Name | Type | Description |
|---|---|---|
| href | string | |

_links

retention

| Name | Type | Description |
|---|---|---|
| count | integer | Determines how many audit log files to retain before rotating the oldest log file out. This is mutually exclusive with duration. |
| duration | string | Specifies an ISO-8601 format date and time to retain the audit log file. The audit log files are deleted once they reach the specified date/time. This is mutually exclusive with count. |

audit_schedule

Rotates the audit logs based on a schedule by using the time-based rotation parameters in any combination. The rotation schedule is calculated by using all the time-related values.

| Name | Type | Description |
|---|---|---|
| days | array[integer] | Specifies the day of the month schedule to rotate audit log. Leave empty for all. |
| hours | array[integer] | Specifies the hourly schedule to rotate audit log. Leave empty for all. |
| minutes | array[integer] | Specifies the minutes schedule to rotate the audit log. |
| months | array[integer] | Specifies the months schedule to rotate audit log. Leave empty for all. |
| weekdays | array[integer] | Specifies the weekdays schedule to rotate audit log. Leave empty for all. |

rotation

Audit event log files are rotated when they reach a configured threshold log size or are on a configured schedule. When an event log file is rotated, the scheduled consolidation task first renames the active converted file to a time-stamped archive file, and then creates a new active converted event log file.

| Name | Type | Description |
|---|---|---|
| now | boolean | Manually rotates the audit logs. Optional in PATCH only. Not available in POST. |
| schedule | audit_schedule | Rotates the audit logs based on a schedule by using the time-based rotation parameters in any combination. The rotation schedule is calculated by using all the time-related values. |
| size | integer | Rotates logs based on log size in bytes. |

log

| Name | Type | Description |
|---|---|---|
| format | string | The format in which the logs are generated by consolidation process. Possible values are:<br>• xml - Data ONTAP-specific XML log format<br>• evtx - Microsoft Windows EVTX log format<br>◦ Default value: 1<br>◦ enum: ["xml", "evtx"]<br>◦ Introduced in: 9.6 |
| retention | retention | |
| rotation | rotation | Audit event log files are rotated when they reach a configured threshold log size or are on a configured schedule. When an event log file is rotated, the scheduled consolidation task first renames the active converted file to a time-stamped archive file, and then creates a new active converted event log file. |

svm

| Name | Type | Description |
|---|---|---|
| name | string | The name of the SVM. |
| uuid | string | The unique identifier of the SVM. |

audit

Auditing for NAS events is a security measure that enables you to track and log certain CIFS and NFS events on SVMs.

| Name | Type | Description |
|---|---|---|
| enabled | boolean | Specifies whether or not auditing is enabled on the SVM. |
| events | events | |
| guarantee | boolean | Indicates whether there is a strict Guarantee of Auditing |

| Name | Type | Description |
|---|---|---|
| log | log | |
| log_path | string | The audit log destination path where consolidated audit logs are stored. |
| svm | svm | |

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. |

# Delete an audit configuration

DELETE `/protocols/audit/{svm.uuid}`

**Introduced In:** 9.6

Deletes an audit configuration.

## Related ONTAP commands

- `vserver audit disable`
- `vserver audit delete`

## Learn more

- DOC /protocols/audit

## Parameters

| Name | Type | In | Required | Description |
|---|---|---|---|---|
| force | boolean | query | False | Indicates to force delete audit configuration.<br>• Introduced in: 9.10 |
| return_timeout | integer | query | False | The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.<br>• Default value: 1<br>• Max value: 120<br>• Min value: 0 |
| svm.uuid | string | path | True | UUID of the SVM to which this object belongs. |

## Response

```
Status: 202, Accepted
```

## Error

```
Status: Default
```

ONTAP Error Response Codes

| Error Code | Description |
|---|---|
| 9699349 | Auditing should be disabled before deleting the audit configuration |
| 9699350 | Audit configuration cannot be deleted, final consolidation is in progress |
| 9699410 | Failed to disable multiproto.audit.evtxlog.support support capability |
| 9699430 | Failed to disable multiproto.audit.cifslogonlogoff.support support capability |
| 9699433 | Failed to disable multiproto.audit.capstaging.support support capability |

| 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

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. |

# Retrieve the audit configuration for an SVM

GET `/protocols/audit/{svm.uuid}`

**Introduced In:** 9.6

Retrieves an audit configuration for an SVM.

## Related ONTAP commands

- `vserver audit show`

## Learn more

- DOC /protocols/audit

## Parameters

| Name | Type | In | Required | Description |
|---|---|---|---|---|
| svm.uuid | string | path | True | UUID of the SVM to which this object belongs. |
| fields | array[string] | query | False | Specify the fields to return. |

## Response

```
Status: 200, Ok
```

| Name | Type | Description |
|---|---|---|
| enabled | boolean | Specifies whether or not auditing is enabled on the SVM. |
| events | events | |
| guarantee | boolean | Indicates whether there is a strict Guarantee of Auditing |
| log | log | |
| log_path | string | The audit log destination path where consolidated audit logs are stored. |
| svm | svm | |

**Example response**


```
{
  "guarantee": "",
  "log": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "format": "string",
    "retention": {
      "duration": "P4DT12H30M5S"
    },
    "rotation": {
      "schedule": {
        "days": [
          "integer"
        ],
        "hours": [
          "integer"
        ],
        "minutes": [
          "integer"
        ],
        "months": [
          "integer"
        ],
        "weekdays": [
          "integer"
        ]
      }
    }
  },
  "log_path": "string",
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```

## 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**

events

| Name | Type | Description |
|---|---|---|
| authorization_policy | boolean | Authorization policy change events |
| cap_staging | boolean | Central access policy staging events |
| cifs_logon_logoff | boolean | CIFS logon and logoff events |
| file_operations | boolean | File operation events |
| file_share | boolean | File share category events |
| security_group | boolean | Local security group management events |
| user_account | boolean | Local user account management events |

href

| Name | Type | Description |
|---|---|---|
| href | string | |

_links

| Name | Type | Description |
|---|---|---|
| self | href | |

retention

| Name | Type | Description |
|---|---|---|
| count | integer | Determines how many audit log files to retain before rotating the oldest log file out. This is mutually exclusive with duration. |

| Name | Type | Description |
| --- | --- | --- |
| duration | string | Specifies an ISO-8601 format date and time to retain the audit log file. The audit log files are deleted once they reach the specified date/time. This is mutually exclusive with count. |

audit_schedule

Rotates the audit logs based on a schedule by using the time-based rotation parameters in any combination. The rotation schedule is calculated by using all the time-related values.

| Name | Type | Description |
| --- | --- | --- |
| days | array[integer] | Specifies the day of the month schedule to rotate audit log. Leave empty for all. |
| hours | array[integer] | Specifies the hourly schedule to rotate audit log. Leave empty for all. |
| minutes | array[integer] | Specifies the minutes schedule to rotate the audit log. |
| months | array[integer] | Specifies the months schedule to rotate audit log. Leave empty for all. |
| weekdays | array[integer] | Specifies the weekdays schedule to rotate audit log. Leave empty for all. |

rotation

Audit event log files are rotated when they reach a configured threshold log size or are on a configured schedule. When an event log file is rotated, the scheduled consolidation task first renames the active converted file to a time-stamped archive file, and then creates a new active converted event log file.

| Name | Type | Description |
| --- | --- | --- |
| now | boolean | Manually rotates the audit logs. Optional in PATCH only. Not available in POST. |

| Name | Type | Description |
|---|---|---|
| schedule | audit_schedule | Rotates the audit logs based on a schedule by using the time-based rotation parameters in any combination. The rotation schedule is calculated by using all the time-related values. |
| size | integer | Rotates logs based on log size in bytes. |

log

| Name | Type | Description |
|---|---|---|
| _links | _links | |
| format | string | The format in which the logs are generated by consolidation process. Possible values are:<br>• xml - Data ONTAP-specific XML log format<br>• evtx - Microsoft Windows EVTX log format<br>◦ Default value: 1<br>◦ enum: ["xml", "evtx"]<br>◦ Introduced in: 9.6 |
| retention | retention | |
| rotation | rotation | Audit event log files are rotated when they reach a configured threshold log size or are on a configured schedule. When an event log file is rotated, the scheduled consolidation task first renames the active converted file to a time-stamped archive file, and then creates a new active converted event log file. |

svm

| Name | Type | Description |
|---|---|---|
| _links | _links | |
| name | string | The name of the SVM. |

| Name | Type | Description |
|---|---|---|
| uuid | string | The unique identifier of the SVM. |

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. |

# Update the audit configuration for an SVM

PATCH `/protocols/audit/{svm.uuid}`

**Introduced In:** 9.6

Updates an audit configuration for an SVM.

## Related ONTAP commands

- `vserver audit modify`

## Learn more

- DOC /protocols/audit

## Parameters

| Name | Type | In | Required | Description |
|---|---|---|---|---|
| return_timeout | integer | query | False | The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.<br>• Default value: 1<br>• Max value: 120<br>• Min value: 0 |
| svm.uuid | string | path | True | UUID of the SVM to which this object belongs. |

## Request Body

| Name | Type | Description |
|---|---|---|
| enabled | boolean | Specifies whether or not auditing is enabled on the SVM. |
| events | events | |
| guarantee | boolean | Indicates whether there is a strict Guarantee of Auditing |

| Name | Type | Description |
| --- | --- | --- |
| log | log | |
| log_path | string | The audit log destination path where consolidated audit logs are stored. |
| svm | svm | |

**Example request**

```
{
  "guarantee": "",
  "log": {
    "format": "string",
    "retention": {
      "duration": "P4DT12H30M5S"
    },
    "rotation": {
      "schedule": {
        "days": [
          "integer"
        ],
        "hours": [
          "integer"
        ],
        "minutes": [
          "integer"
        ],
        "months": [
          "integer"
        ],
        "weekdays": [
          "integer"
        ]
      }
    }
  },
  "log_path": "string",
  "svm": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```

## Response

```
Status: 202, Accepted
```

## Error

```
Status: Default
```

ONTAP Error Response Codes

| Error Code | Description |
|---|---|
| 9699340 | SVM UUID lookup failed |
| 9699343 | Audit configuration is absent for modification |
| 9699358 | Audit configuration is absent for enabling |
| 9699359 | Audit configuration is already enabled |
| 9699360 | Final consolidation is in progress, audit enable failed |
| 9699365 | Enabling of audit configuration failed |
| 9699373 | Audit configuration is absent for disabling |
| 9699374 | Audit configuration is already disabled |
| 9699375 | Disabling of audit configuration failed |
| 9699384 | The specified log_path does not exist |
| 9699385 | The log_path must be a directory |
| 9699386 | The log_path must be a canonical path in the SVMs namespace |
| 9699387 | The log_path cannot be empty |
| 9699388 | Rotate size must be greater than or equal to 1024 KB |
| 9699389 | The log_path must not contain a symbolic link |
| 9699398 | The log_path exceeds a maximum supported length of characters |
| 9699399 | The log_path contains an unsupported read-only (DP/LS) volume |
| 9699400 | The specified log_path is not a valid destination for SVM |
| 9699402 | The log_path contains an unsupported snaplock volume |
| 9699403 | The log_path cannot be accessed for validation |
| 9699406 | The log_path validation failed |

| Error Code | Description |
| --- | --- |
| 9699407 | Additional fields are provided |
| 9699409 | Failed to enable multiproto.audit.evtxlog.support support capability |
| 9699410 | Failed to disable multiproto.audit.evtxlog.support support capability |
| 9699418 | Audit configuration is absent for rotate |
| 9699419 | Failed to rotate audit log |
| 9699420 | Cannot rotate audit log, auditing is not enabled for this SVM |
| 9699428 | All nodes need to run ONTAP 8.3.0 release to audit CIFS logon-logoff events |
| 9699429 | Failed to enable multiproto.audit.cifslogonlogoff.support support capability |
| 9699430 | Failed to disable multiproto.audit.cifslogonlogoff.support support capability |
| 9699431 | All nodes need to run ONTAP 8.3.0 release to audit CAP staging events |
| 9699432 | Failed to enable multiproto.audit.capstaging.support support capability |
| 9699433 | Failed to disable multiproto.audit.capstaging.support support capability |

## Definitions

**See Definitions**

events

| Name | Type | Description |
|---|---|---|
| authorization_policy | boolean | Authorization policy change events |
| cap_staging | boolean | Central access policy staging events |
| cifs_logon_logoff | boolean | CIFS logon and logoff events |
| file_operations | boolean | File operation events |
| file_share | boolean | File share category events |
| security_group | boolean | Local security group management events |
| user_account | boolean | Local user account management events |

href

| Name | Type | Description |
|---|---|---|
| href | string | |

_links

retention

| Name | Type | Description |
|---|---|---|
| count | integer | Determines how many audit log files to retain before rotating the oldest log file out. This is mutually exclusive with duration. |
| duration | string | Specifies an ISO-8601 format date and time to retain the audit log file. The audit log files are deleted once they reach the specified date/time. This is mutually exclusive with count. |

audit_schedule

Rotates the audit logs based on a schedule by using the time-based rotation parameters in any combination. The rotation schedule is calculated by using all the time-related values.

| Name | Type | Description |
|---|---|---|
| days | array[integer] | Specifies the day of the month schedule to rotate audit log. Leave empty for all. |
| hours | array[integer] | Specifies the hourly schedule to rotate audit log. Leave empty for all. |
| minutes | array[integer] | Specifies the minutes schedule to rotate the audit log. |
| months | array[integer] | Specifies the months schedule to rotate audit log. Leave empty for all. |
| weekdays | array[integer] | Specifies the weekdays schedule to rotate audit log. Leave empty for all. |

rotation

Audit event log files are rotated when they reach a configured threshold log size or are on a configured schedule. When an event log file is rotated, the scheduled consolidation task first renames the active converted file to a time-stamped archive file, and then creates a new active converted event log file.

| Name | Type | Description |
|---|---|---|
| now | boolean | Manually rotates the audit logs. Optional in PATCH only. Not available in POST. |
| schedule | audit_schedule | Rotates the audit logs based on a schedule by using the time-based rotation parameters in any combination. The rotation schedule is calculated by using all the time-related values. |
| size | integer | Rotates logs based on log size in bytes. |

log

| Name | Type | Description |
|---|---|---|
| format | string | The format in which the logs are generated by consolidation process. Possible values are:<br>• xml - Data ONTAP-specific XML log format<br>• evtx - Microsoft Windows EVTX log format<br>◦ Default value: 1<br>◦ enum: ["xml", "evtx"]<br>◦ Introduced in: 9.6 |
| retention | retention | |
| rotation | rotation | Audit event log files are rotated when they reach a configured threshold log size or are on a configured schedule. When an event log file is rotated, the scheduled consolidation task first renames the active converted file to a time-stamped archive file, and then creates a new active converted event log file. |

svm

| Name | Type | Description |
|---|---|---|
| name | string | The name of the SVM. |
| uuid | string | The unique identifier of the SVM. |

audit

Auditing for NAS events is a security measure that enables you to track and log certain CIFS and NFS events on SVMs.

| Name | Type | Description |
|---|---|---|
| enabled | boolean | Specifies whether or not auditing is enabled on the SVM. |
| events | events | |
| guarantee | boolean | Indicates whether there is a strict Guarantee of Auditing |

| Name | Type | Description |
| --- | --- | --- |
| log | log | |
| log_path | string | The audit log destination path where consolidated audit logs are stored. |
| svm | svm | |

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 © 2025 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.