



Manage S3 audit configurations

ONTAP 9.15.1 REST API reference

NetApp
September 11, 2024

Table of Contents

- Manage S3 audit configurations 1
 - Protocols audit svm.uuid object-store endpoint overview 1
 - Delete an S3 audit configuration 9
 - Retrieve an S3 audit configurations 12
 - Update an S3 audit configuration for an SVM 21
 - Create an S3 audit configuration 31

Manage S3 audit configurations

Protocols audit svm.uuid object-store endpoint overview

Overview

S3 events auditing is a security measure that enables you to track and log certain S3 events on storage virtual machines (SVMs). You can track potential security problems and provides evidence of any security breaches.

Examples

Creating an S3 audit entry with log rotation size and log retention count

To create an S3 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/{svm.uuid}/object-store/

# The call:
curl -X POST "https://<mgmt-ip>/api/protocols/audit/ec650e97-156e-11e9-
abcb-005056bbd0bf/object-store?return_records=true" -H "accept:
application/json" -H "Content-Type: application/json" -d "{ \"enabled\":
true, \"events\": { \"data\": false, \"management\": false}, \"log\": {
\"format\": \"json\", \"retention\": { \"count\": 10 }, \"rotation\": {
\"size\": 2048000 }}, \"log_path\": \"/\"}"

# The response:
{
  "records": [
    {
      "svm": {
        "uuid": "ec650e97-156e-11e9-abcb-005056bbd0bf",
        "name": "vs1"
      },
      "enabled": true,
      "events": {
        "data": false,
        "management": false
      },
      "log": {
        "format": "json",
        "rotation": {
          "size": 2048000
        },
        "retention": {
          "count": 10,
          "duration": "0s"
        }
      },
      "log_path": "/"
    }
  ],
  "num_records": 1
}
```

Creating an S3 audit entry with log rotation schedule and log retention duration

To create an S3 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/{svm.uuid}/object-store/

# The call:
curl -X POST "https://<mgmt-ip>/api/protocols/audit/a8d64674-13fc-11e9-87b1-005056a7ae7e/object-store?return_records=true" -H "accept: application/json" -H "Content-Type: application/json" -d "{ \"enabled\": false, \"events\": { \"data\": true, \"management\": true }, \"log\": { \"format\": \"json\", \"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\": \"/\"/>
# The response:
{
  "records": [
    {
      "svm": {
        "uuid": "a8d64674-13fc-11e9-87b1-005056a7ae7e",
        "name": "vs3"
      },
      "enabled": true,
      "events": {
        "data": true,
        "management": true
      },
      "log": {
        "format": "json",
        "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": "/"
}
],
"num_records": 1
}

```

Retrieving an S3 audit configuration for all SVMs in the cluster

```

# The API:
GET /api/protocols/audit/{svm.uuid}/object-store/

# The call:
curl -X GET "https://<mgmt-ip>/api/protocols/audit/*/object-store?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": {
    "data": false,
    "management": false
  },
  "log": {
    "format": "json",
    "rotation": {
      "size": 2048000
    },
    "retention": {
      "count": 10,
      "duration": "0s"
    }
  },
  "log_path": "/"
},
{
  "svm": {
    "uuid": "a8d64674-13fc-11e9-87b1-005056a7ae7e",
    "name": "vs3"
  },
  "enabled": true,
  "events": {
    "data": true,
    "management": true
  },
  "log": {
    "format": "json",
    "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": "/"  
}  
],  
"num_records": 2  
}
```

Retrieving specific entries with event list as data and management event for an SVM

The configuration returned is identified by the events in the list of S3 audit configurations of an SVM.

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

# The call:
curl -X GET "https://<mgmt-ip>/api/protocols/audit/*/object-
store?events.data=true&events.management=true&return_records=true&return_t
imeout=15" -H "accept: application/json"

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

Retrieving a specific S3 audit configuration of an SVM

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

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

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

# The response:
{
  "svm": {
    "uuid": "ec650e97-156e-11e9-abcb-005056bbd0bf",
    "name": "vs1"
  },
  "enabled": true,
  "events": {
    "data": false,
    "management": false
  },
  "log": {
    "format": "json",
    "rotation": {
      "size": 2048000
    },
    "retention": {
      "count": 10,
      "duration": "0s"
    }
  },
  "log_path": "/"
}
```

Updating a specific S3 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}/object-store/

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

Deleting a specific S3 audit configuration of an SVM

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

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

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

Delete an S3 audit configuration

```
DELETE /protocols/audit/{svm.uuid}/object-store
```

Introduced In: 9.10

Deletes an S3 audit configuration.

Related ONTAP commands

- `vserver object-store-server audit disable`
- `vserver object-store-server audit delete`

Learn more

- [DOC /protocols/audit/{svm.uuid}/object-store](#)

Parameters

| Name | Type | In | Required | Description |
|----------------|---------|-------|----------|--|
| force | boolean | query | False | Indicates whether a force deletion of the audit configuration is enabled. |
| return_timeout | integer | query | False | <p>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.</p> <ul style="list-style-type: none"> • Default value: 1 • Max value: 120 • Min value: 0 |
| svm.uuid | string | path | True | UUID of the SVM to which this object belongs. |

Response

```
Status: 200, Ok
```

Response

Status: 202, Accepted

Error

Status: Default

ONTAP Error Response Codes

| Error Code | Description |
|------------|---|
| 140902420 | Failed to delete audit configuration for the SVM. |
| 140902421 | Failed to delete audit configuration for the SVM because audit is enabled for the SVM. |
| 140902422 | Failed to delete audit configuration for the SVM because final consolidation is in progress. Wait a few minutes, and try the operation again. |

Also see the table of common errors in the [Response body](#) overview section of this documentation.

| Name | Type | Description |
|-------|--------------------------------|-------------|
| error | returned_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 |

returned_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 an S3 audit configurations

GET /protocols/audit/{svm.uuid}/object-store

Introduced In: 9.10

Retrieves S3 audit configurations.

Related ONTAP commands

- `vserver object-store-server audit show`

Learn more

- [DOC /protocols/audit/{svm.uuid}/object-store](#)

Parameters

| Name | Type | In | Required | Description |
|----------|--------|-------|----------|--------------------|
| svm.name | string | query | False | Filter by svm.name |

| Name | Type | In | Required | Description |
|--------------------------------|---------|-------|----------|---|
| enabled | boolean | query | False | Filter by enabled |
| events.management | boolean | query | False | Filter by events.management |
| events.data | boolean | query | False | Filter by events.data |
| log.rotation.size | integer | query | False | Filter by log.rotation.size |
| log.rotation.schedule.minutes | integer | query | False | Filter by log.rotation.schedule.minutes <ul style="list-style-type: none"> • Max value: 59 • Min value: 0 |
| log.rotation.schedule.days | integer | query | False | Filter by log.rotation.schedule.days <ul style="list-style-type: none"> • Max value: 31 • Min value: 1 |
| log.rotation.schedule.months | integer | query | False | Filter by log.rotation.schedule.months <ul style="list-style-type: none"> • Max value: 12 • Min value: 1 |
| log.rotation.schedule.hours | integer | query | False | Filter by log.rotation.schedule.hours <ul style="list-style-type: none"> • Max value: 23 • Min value: 0 |
| log.rotation.schedule.weekdays | integer | query | False | Filter by log.rotation.schedule.weekdays <ul style="list-style-type: none"> • Max value: 6 • Min value: 0 |
| log.format | string | query | False | Filter by log.format |

| Name | Type | In | Required | Description |
|------------------------|---------------|-------|----------|---|
| log.retention.count | integer | query | False | Filter by log.retention.count |
| log.retention.duration | string | query | False | Filter by log.retention.duration |
| log_path | string | query | False | Filter by log_path |
| svm.uuid | string | path | True | UUID of the SVM to which this object belongs. |
| 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. <ul style="list-style-type: none"> • Default value: 1 |
| 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. <ul style="list-style-type: none"> • Max value: 120 • Min value: 0 • Default value: 1 |

| Name | Type | In | Required | Description |
|----------|---------------|-------|----------|---|
| order_by | array[string] | query | False | Order results by specified fields and optional [asc |

Response

Status: 200, Ok

| Name | Type | Description |
|----------|------------------------|--|
| enabled | boolean | Specifies whether or not auditing is enabled on the SVM. |
| events | events | |
| log | s3_log | |
| log_path | string | The audit log destination path where consolidated audit logs are stored. |
| svm | svm | SVM, applies only to SVM-scoped objects. |

Example response

```
{
  "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 | returned_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 |
|------------|---------|-------------------|
| data | boolean | Data events |
| management | boolean | 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". |
| 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. |

| Name | Type | Description |
|----------|----------------|---|
| 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. |

s3_log

| Name | Type | Description |
|--------|------------------------|-------------|
| _links | _links | |

| Name | Type | Description |
|-----------|---------------------------|---|
| format | string | Format in which the logs are generated by the consolidation process. Possible values are: <ul style="list-style-type: none"> • json - ONTAP-specific Json log format. <ul style="list-style-type: none"> ◦ Default value: 1 ◦ enum: ["json"] ◦ Introduced in: 9.10 ◦ x-nullable: true |
| 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

SVM, applies only to SVM-scoped objects.

| Name | Type | Description |
|------------------------|------------------------|---|
| _links | _links | |
| name | string | The name of the SVM. This field cannot be specified in a PATCH method. |
| uuid | string | The unique identifier of the SVM. This field cannot be specified in a PATCH method. |

error_arguments

| Name | Type | Description |
|---------|--------|------------------|
| code | string | Argument code |
| message | string | Message argument |

returned_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 an S3 audit configuration for an SVM

PATCH /protocols/audit/{svm.uuid}/object-store

Introduced In: 9.10

Updates an S3 audit configuration for an SVM.

Important notes

- `events` - Not specifying either data or management is equivalent to setting it to false.

Related ONTAP commands

- `vserver object-store-server audit modify`

Learn more

- [DOC /protocols/audit/{svm.uuid}/object-store](#)

Parameters

| Name | Type | In | Required | Description |
|----------------|---------|-------|----------|--|
| return_timeout | integer | query | False | <p>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.</p> <ul style="list-style-type: none"> • Default value: 1 • Max value: 120 • 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 | |
| log | s3_log | |

| Name | Type | Description |
|----------|--------|--|
| log_path | string | The audit log destination path where consolidated audit logs are stored. |
| svm | svm | SVM, applies only to SVM-scoped objects. |

Example request

```
{
  "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"
  }
}
```

Response

Status: 200, Ok

Response

Status: 202, Accepted

Error

Status: Default

ONTAP Error Response Codes

| Error Code | Description |
|------------|--|
| 140902401 | Failed to create an audit configuration for the SVM. |
| 140902402 | Audit configuration is already present. |
| 140902402 | Audit configuration is already enabled. |
| 140902403 | Failed to create staging volume. |
| 140902415 | Failed to modify an audit configuration because no audit configuration exists for SVM. |
| 140902416 | Failed to modify audit configuration for SVM. |
| 140902422 | Final consolidation is in progress, audit delete failed. |
| 140902423 | Failed to delete the audit configuration for the SVM. |
| 140902425 | Audit configuration is not available for disabling. |
| 140902430 | Audit configuration is not available for enabling. |
| 140902431 | Audit enable failed, audit configuration already enabled for the SVM. |
| 140902432 | Final consolidation is in progress, audit enable failed. |
| 140902445 | Audit disable failed, audit configuration does not exist for the SVM. |
| 140902446 | Audit configuration is already disabled. |
| 140902446 | Audit disable failed, audit configuration does not exist for the SVM. |
| 140902456 | The specified log_path does not exist. |
| 140902457 | The log_path must be a directory. |

| Error Code | Description |
|------------|--|
| 140902458 | The log_path must be a canonical path in the SVM's namespace. |
| 140902459 | The log_path cannot be empty. |
| 140902460 | Rotate size must be greater than or equal to 1024 KB. |
| 140902461 | The destination path must not contain a symbolic link. |
| 140902470 | The log_path exceeds a maximum supported length of characters. |
| 140902471 | The log_path contains an unsupported read-only (DP/LS) volume. |
| 140902472 | The log_path is not a valid destination for the SVM. |
| 140902474 | The log_path contains an unsupported Snaplock volume. |
| 140902478 | The log_path validation failed. |
| 140902478 | The log_path cannot be accessed for validation. |
| 140902479 | No other fields can be specified when "enabled" is specified. |
| 140902490 | Audit configuration is absent for rotate. |
| 140902491 | Failed to rotate audit log. |
| 140902492 | Cannot rotate audit log, auditing is not enabled for this SVM. |

Also see the table of common errors in the [Response body](#) overview section of this documentation. ONTAP Error Response Codes

| Error Code | Description |
|------------|--------------------------------|
| 9699340 | SVM UUID lookup failed |
| 9699407 | Additional fields are provided |

| Name | Type | Description |
|-------|--------------------------------|-------------|
| error | returned_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 |
|------------|---------|-------------------|
| data | boolean | Data events |
| management | boolean | 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". |
| 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. |

| Name | Type | Description |
|----------|----------------|---|
| 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. |

s3_log

| Name | Type | Description |
|--------|------------------------|-------------|
| _links | _links | |

| Name | Type | Description |
|-----------|---------------------------|---|
| format | string | Format in which the logs are generated by the consolidation process. Possible values are: <ul style="list-style-type: none"> • json - ONTAP-specific Json log format. <ul style="list-style-type: none"> ◦ Default value: 1 ◦ enum: ["json"] ◦ Introduced in: 9.10 ◦ x-nullable: true |
| 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

SVM, applies only to SVM-scoped objects.

| Name | Type | Description |
|------------------------|------------------------|---|
| _links | _links | |
| name | string | The name of the SVM. This field cannot be specified in a PATCH method. |
| uuid | string | The unique identifier of the SVM. This field cannot be specified in a PATCH method. |

s3_audit

Auditing for NAS events is a security measure that enables you to track and log certain S3 events on SVMs.

| Name | Type | Description |
|----------|------------------------|--|
| enabled | boolean | Specifies whether or not auditing is enabled on the SVM. |
| events | events | |
| log | s3_log | |
| log_path | string | The audit log destination path where consolidated audit logs are stored. |
| svm | svm | SVM, applies only to SVM-scoped objects. |

error_arguments

| Name | Type | Description |
|---------|--------|------------------|
| code | string | Argument code |
| message | string | Message argument |

returned_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. |

Create an S3 audit configuration

POST /protocols/audit/{svm.uuid}/object-store

Introduced In: 9.10

Creates an S3 audit configuration.

Required properties

- `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.data` - *true*
- `events.management` - *false*
- `log.format` - *json*
- `log.retention.count` - *0*
- `log.retention.duration` - *PT0S*
- `log.rotation.size` - *100MB*
- `log.rotation.now` - *false*

Related ONTAP commands

- `vserver object-store-server audit create`
- `vserver object-store-server audit enable`

Learn more

- [DOC /protocols/audit/{svm.uuid}/object-store](#)

Parameters

| Name | Type | In | Required | Description |
|----------------|---------|-------|----------|--|
| return_timeout | integer | query | False | <p>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.</p> <ul style="list-style-type: none"> • Default value: 1 • Max value: 120 • 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 | |
| log | s3_log | |

| Name | Type | Description |
|----------|--------|--|
| log_path | string | The audit log destination path where consolidated audit logs are stored. |
| svm | svm | SVM, applies only to SVM-scoped objects. |

Example request

```
{
  "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"
  }
}
```

Response

Status: 202, Accepted

| Name | Type | Description |
|-------------|-----------------------------------|-------------------|
| _links | _links | |
| num_records | integer | Number of records |
| records | array[s3_audit] | |

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "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"
  }
]
}

```

Headers

| Name | Description | Type |
|----------|---|--------|
| Location | Useful for tracking the resource location | string |

Response

Status: 201, Created

Error

Status: Default

ONTAP Error Response Codes

| Error Code | Description |
|------------|--|
| 140902401 | Failed to create an audit configuration for the SVM. |
| 140902402 | Audit configuration is already present. |
| 140902402 | Audit configuration is already enabled. |
| 140902403 | Failed to create staging volume. |
| 140902415 | Failed to modify an audit configuration because no audit configuration exists for the SVM. |
| 140902416 | Failed to modify audit configuration for SVM. |
| 140902422 | Final consolidation is in progress, audit delete failed. |
| 140902423 | Failed to delete the audit configuration for the SVM. |
| 140902425 | Audit configuration is not available for disabling. |

| Error Code | Description |
|------------|---|
| 140902430 | Audit configuration is not available for enabling. |
| 140902431 | Audit enable failed, audit configuration already enabled for the SVM. |
| 140902432 | Final consolidation is in progress, audit enable failed. |
| 140902445 | Audit disable failed, audit configuration does not exist for the SVM. |
| 140902446 | Audit disable failed, audit configuration does not exist for the SVM. |
| 140902447 | Audit disable failed. |
| 140902456 | The specified log_path does not exist. |
| 140902457 | The log_path must be a directory. |
| 140902458 | The log_path must be a canonical path in the SVM's namespace. |
| 140902459 | The log_path cannot be empty. |
| 140902460 | Rotate size must be greater than or equal to 1024 KB. |
| 140902461 | The destination path must not contain a symbolic link. |
| 140902470 | The log_path exceeds a maximum supported length of characters. |
| 140902471 | The log_path contains an unsupported read-only (DP/LS) volume. |
| 140902472 | The log_path is not a valid destination for the SVM. |
| 140902474 | The log_path contains an unsupported Snaplock volume. |
| 140902478 | The log_path validation failed. |
| 140902478 | The log_path cannot be accessed for validation. |
| 140902490 | Audit configuration is absent for rotate. |
| 140902491 | Failed to rotate audit log. |
| 140902492 | Cannot rotate audit log, auditing is not enabled for this SVM. |

Also see the table of common errors in the [Response body](#) overview section of this documentation. ONTAP Error Response Codes

| Error Code | Description |
|------------|--------------------------------|
| 9699340 | SVM UUID lookup failed |
| 9699407 | Additional fields are provided |

| Name | Type | Description |
|-------|--------------------------------|-------------|
| error | returned_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 |
|------------|---------|-------------------|
| data | boolean | Data events |
| management | boolean | 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". |
| 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. |

| Name | Type | Description |
|----------|----------------|---|
| 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. |

s3_log

| Name | Type | Description |
|--------|------------------------|-------------|
| _links | _links | |

| Name | Type | Description |
|-----------|---------------------------|---|
| format | string | Format in which the logs are generated by the consolidation process. Possible values are: <ul style="list-style-type: none"> • json - ONTAP-specific Json log format. <ul style="list-style-type: none"> ◦ Default value: 1 ◦ enum: ["json"] ◦ Introduced in: 9.10 ◦ x-nullable: true |
| 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

SVM, applies only to SVM-scoped objects.

| Name | Type | Description |
|------------------------|------------------------|---|
| _links | _links | |
| name | string | The name of the SVM. This field cannot be specified in a PATCH method. |
| uuid | string | The unique identifier of the SVM. This field cannot be specified in a PATCH method. |

s3_audit

Auditing for NAS events is a security measure that enables you to track and log certain S3 events on SVMs.

| Name | Type | Description |
|----------|------------------------|--|
| enabled | boolean | Specifies whether or not auditing is enabled on the SVM. |
| events | events | |
| log | s3_log | |
| log_path | string | The audit log destination path where consolidated audit logs are stored. |
| svm | svm | SVM, applies only to SVM-scoped objects. |

[_links](#)

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

error_arguments

| Name | Type | Description |
|---------|--------|------------------|
| code | string | Argument code |
| message | string | Message argument |

returned_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.