Audit S3 events

ONTAP 9

NetApp
May 27, 2022

Table of Contents

Audit S3 events . . . 1
- Audit S3 events . . . 1
- Plan an S3 auditing configuration . . . 2
- Create and enable an S3 auditing configuration . . . 4
- Select buckets for S3 auditing . . . 6
- Modify an S3 auditing configuration . . . 7
- Show S3 auditing configurations . . . 7

Audit S3 events

Audit S3 events

Beginning with ONTAP 9.10.1, you can audit data and management events in ONTAP S3 environments. S3 audit functionality is similar to existing NAS auditing capabilities, and S3 and NAS auditing can coexist in a cluster.

When you create and enable an S3 auditing configuration on an SVM, S3 events are recorded in a log file. The you can specify the following events to be logged:

- Object access (data) events

  GetObject, PutObject, and DeleteObject

- Management events

  PutBucket and DeleteBucket

The log format is JavaScript Object Notation (JSON).

The combined limit for S3 and NFS auditing configurations is 50 SVMs per cluster.

The following license bundle is required: * Core Bundle, for ONTAP S3 protocol and storage

For more information, see How the ONTAP auditing process works.

Guaranteed auditing

By default, S3 and NAS auditing is guaranteed. ONTAP guarantees that all auditable bucket access events are recorded, even if a node is unavailable. A requested bucket operation cannot be completed until the audit record for that operation is saved to the staging volume on persistent storage. If audit records cannot be committed in the staging files, either because of insufficient space or because of other issues, client operations are denied.

Space requirements for auditing

In the ONTAP auditing system, audit records are initially stored in binary staging files on individual nodes. Periodically, they are consolidated and converted to user-readable event logs, which are stored in the audit event log directory for the SVM.

The staging files are stored in a dedicated staging volume, which is created by ONTAP when the auditing configuration is created. There is one staging volume per aggregate.

You must plan for sufficient available space in the auditing configuration:

- For the staging volumes in aggregates that contain audited buckets.
- For the volume containing the directory where converted event logs are stored.

You can control the number of event logs, and hence the available space in the volume, using one of two methods when creating the S3 auditing configuration:

- A numerical limit; the `-rotate-limit` parameter controls the minimum number of audit files that must be preserved.
- A time limit; the `-retention-duration` parameter controls the maximum period that files can be preserved.

In both parameters, once that configured is exceeded, older audit files can be deleted to make room for newer ones. For both parameters, the value is 0, indicating that all files must be maintained. In order to ensure sufficient space, it is therefore a best practice to set one of the parameters to a non-zero value.

Because of guaranteed auditing, if the space available for audit data runs out before the rotation limit, newer audit data cannot be created, resulting in failure to clients accessing data. Therefore, the choice of this value and of the space allocated to auditing must be chosen carefully, and you must respond to warnings about available space from the auditing system.

For more information, see Basic auditing concepts.

Plan an S3 auditing configuration

You must specify a number of parameters for the S3 auditing configuration or accept the defaults. In particular, you should consider which log rotation parameters will help ensure adequate free space.

See the **`vserver object-store-server audit create`** man page for syntax details.

General parameters

There are two required parameters that you must specify when you create the auditing configuration. There are also three optional parameters that you can specify.

Type of information	Option	Required
SVM name Name of the SVM on which to create the auditing configuration. The SVM must already exist and be enabled for S3.	`-verserver` *`svm_name`*	Yes
Log destination path Specifies where the converted audit logs are stored. The path must already exist on the SVM. The path can be up to 864 characters in length and must have read-write permissions. If the path is not valid, the audit configuration command fails.	`-destination` *`text`*	Yes

Type of information	Option	Required
Categories of events to audit The following event categories can be audited: * data GetObject, PutObject, and DeleteObject events * management PutBucket and DeleteBucket events The default is to audit data events only.	`-events {data|management}, …`	No

You can enter one of the following parameters to control the number of audit log files. If no value is entered, all log files are retained.

Type of information	Option	Required
Log files rotation limit Determines how many audit log files to retain before rotating the oldest log file out. For example, if you enter a value of 5, the last five log files are retained. A value of 0 indicates that all the log files are retained. The default value is 0.	`-rotate-limit` *integer*	No
Log files duration limit Determines how long a log file can be retained before being deleted. For example, if you enter a value of 5d0h0m, logs more than 5 days old are deleted. A value of 0 indicates that all the log files are retained. The default value is 0.	`-retention duration` *integer_time*	No

Parameters for audit log rotation

You can rotate audit logs based on size or schedule. The default is to rotate audit logs based on size.

Rotate logs based on log size

If you want to use the default log rotation method and the default log size, you do not need to configure any specific parameters for log rotation. The default log size is 100 MB.

If you do not want to use the default log size, you can configure the `-rotate-size` parameter to specify a custom log size.

If you want to reset the rotation based on a log size alone, use the following command to unset the `-rotate -schedule-minute` parameter:

```
vserver audit modify -vserver svm_name -destination / -rotate-schedule-minute -
```

Rotate logs based on a schedule

If you choose to rotate the audit logs based on a schedule, you can schedule log rotation by using the time-based rotation parameters in any combination.

- If you use time-based rotation, the `-rotate-schedule-minute` parameter is mandatory.
- All other time-based rotation parameters are optional.
  - `-rotate-schedule-month`
  - `-rotate-schedule-dayofweek`
  - `-rotate-schedule-day`
  - `-rotate-schedule-hour`
- The rotation schedule is calculated by using all the time-related values. For example, if you specify only the `-rotate-schedule-minute` parameter, the audit log files are rotated based on the minutes specified on all days of the week, during all hours on all months of the year.
- If you specify only one or two time-based rotation parameters (for example, `-rotate-schedule-month` and `-rotate-schedule-minutes`), the log files are rotated based on the minute values that you specified on all days of the week, during all hours, but only during the specified months.

  For example, you can specify that the audit log is to be rotated during the months January, March, and August on all Mondays, Wednesdays, and Saturdays at 10:30 a.m.

- If you specify values for both `-rotate-schedule-dayofweek` and `-rotate-schedule-day`, they are considered independently.

  For example, if you specify `-rotate-schedule-dayofweek` as Friday and `-rotate-schedule-day` as 13, then the audit logs would be rotated on every Friday and on the 13th day of the specified month, not just on every Friday the 13th.

- If you want to reset the rotation based on a schedule alone, use the following command to unset the `-rotate-size parameter`:

  ```
  vserver audit modify -vserver svm_name -destination / -rotate-size -
  ```

Rotate logs based on log size and schedule

You can choose to rotate the log files based on log size and a schedule by setting both the -rotate-size parameter and the time-based rotation parameters in any combination. For example: if `-rotate-size` is set to 10 MB and `-rotate-schedule-minute` is set to 15, the log files rotate when the log file size reaches 10 MB or on the 15th minute of every hour (whichever event occurs first).

Create and enable an S3 auditing configuration

To implement S3 auditing, you first create a persistent object store auditing configuration on an S3-enabled SVM, then enable the configuration.

What you'll need

- An S3-enabled SVM.
- Sufficient space for staging volumes in the aggregate.

About this task

An auditing configuration is required for each SVM that contains S3 buckets that you wish to audit. You can enable S3 auditing on new or existing S3 servers. Auditing configurations persist in an S3 environment until removed by the **vserver object-store-server audit delete** command.

The S3 auditing configuration applies to all buckets in the SVM that you select for auditing. An audit-enabled SVM can contain audited and un-audited buckets.

It is recommended that you configure S3 auditing for automatic log rotation, determined by log size or a schedule. If you don't configure automatic log rotation, all log files are retained by default. You can also rotate S3 log files manually using the **vserver object-store-server audit rotate-log** command.

If the SVM is an SVM disaster recovery source, the destination path cannot be on the root volume.

Procedure

1. Create the auditing configuration to rotate audit logs based on log size or a schedule.

If you want to rotate audit logs by…	Enter…
Log size	`vserver object-store-server audit create -vserver` *svm_name* `-destination` *path* `[[-events] {data|management}, …] {[-rotate-limit` *integer*`] | [-retention-duration [`*integer_d*`][_`*integer_h*`][_`*integer_m*`][_`*integers*`]]} [-rotate-size {`*integer*`[KB|MB|GB|TB|PB]}]`
A schedule	`vserver object-store-server audit create -vserver` *svm_name* `-destination path [[-events] {data|management}, …] {[-rotate-limit` *integer*`] | [-retention-duration [`*integerd*`][`*integerh*`] [`*integerm*`][`*integers*`]] } [-rotate-schedule-month` *chron_month*`] [-rotate-schedule-dayofweek` *chron_dayofweek*`] [-rotate-schedule-day` *chron_dayofmonth*`] [-rotate-schedule-hour` *chron_hour*`] -rotate-schedule-minute` *chron_minute* The `-rotate-schedule-minute` parameter is required if you are configuring time-based audit log rotation.

2. Enable S3 auditing:

   `vserver object-store-server audit enable -vserver` *svm_name*

Examples

The following example creates an auditing configuration that audits all S3 events (the default) using size-based rotation. The logs are stored in the /audit_log directory. The log file size limit is 200 MB. The logs are rotated when they reach 200 MB in size.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -rotate
-size 200MB
```

The following example creates an auditing configuration that audits all S3 events (the default) using size-based rotation. The log file size limit is 100 MB (the default), and the logs are retained for 5 days before being deleted.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -retention
-duration 5d0h0m
```

The following example creates an auditing configuration that audits S3 management events, and central access policy staging events using time-based rotation. The audit logs are rotated monthly, at 12:30 p.m. on all days of the week. The log rotation limit is 5.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -events
management -rotate-schedule-month all -rotate-schedule-dayofweek all -rotate
-schedule-hour 12 -rotate-schedule-minute 30 -rotate-limit 5
```

Select buckets for S3 auditing

You must specify which buckets to audit in an audit-enabled SVM.

What you'll need

- An SVM enabled for S3 auditing.

About this task

S3 auditing configurations are enabled on a per-SVM basis, but you must select the buckets in SVMS that are enabled for audit. If you add buckets to the SVM and you want the new buckets to be audited, you must select them with this procedure. You can also have non-audited buckets in an SVM enabled for S3 auditing.

Auditing configurations persist for buckets until removed by the `vserver object-store-server audit object-select delete` command.

Procedure

Select a bucket for S3 auditing:

```
vserver object-store-server audit event-selector create -vserver svm_name -bucket
bucket_name [[-access] {read-only|write-only|all}] [[-permission] {allow-
only|deny-only|all}]
```

- `-access` - specifies the type of event access to be audited: `read-only`, `write-only` or `all` (default is `all`).
- `-permission` - specifies the type of event permission to be audited: `allow-only`, `deny-only` or `all` (default is `all`).

Example

The following example creates a bucket auditing configuration that only logs allowed events with read-only access:

```
cluster1::> vserver object-store-server audit event-selector create -vserver vs1
-bucket test-bucket -access read-only -permission allow-only
```

Modify an S3 auditing configuration

You can modify the auditing parameters of individual buckets or the auditing configuration of all buckets selected for audit in the SVM.

Table 1. Procedure

If you want to modify the audit configuration for…	Enter…
Individual buckets	`vserver object-store-server audit event-selector modify -vserver` *`svm_name`* `[-bucket` *`bucket_name`*`] [`*`parameters to modify`*`]`
All buckets in the SVM	`vserver object-store-server audit modify -vserver` *`svm_name`* `[`*`parameters to modify`*`]`

Examples

The following example modifies an individual bucket auditing configuration to audit only write-only access events:

```
cluster1::> vserver object-store-server audit event-selector modify
-vserver vs1 -bucket test-bucket -access write-only
```

The following example modifies the auditing configuration of all buckets in the SVM to change the log size limit to 10MB and to retain 3 log files before rotating.

```
cluster1::> vserver object-store-server audit modify -vserver vs1 -rotate
-size 10MB -rotate-limit 3
```

Show S3 auditing configurations

After completing the auditing configuration, you can verify that auditing is configured properly and is enabled. You can also display information about all object store auditing configurations in the cluster.

About this task

You can display information about bucket and SVM auditing configurations.

- Buckets – use the `vserver object-store-server audit event-selector show` command

  Without any parameters, the command displays the following information about buckets in all SVMs in the cluster with object store auditing configurations:

  - SVM name
  - Bucket name
  - Access and permission values

- SVMs – use the `vserver object-store-server audit show` command

  Without any parameters, the command displays the following information about all SVMs in the cluster with object store auditing configurations:

  - SVM name
  - Audit state
  - Target directory

You can specify the `-fields` parameter to specify which audit configuration information to display.

Procedure

Show information about S3 auditing configurations:

If you want to modify the configuration for…	Enter…
Buckets	`vserver object-store-server audit event-selector show [-vserver` *`svm_name`*`] [`*`parameters`*`]`
SVMs	`vserver object-store-server audit show [-vserver` *`svm_name`*`] [`*`parameters`*`]`

Examples

The following example displays information for a single bucket:

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1 -bucket test-bucket
     Vserver     Bucket     Access          Permission
     ----------- ---------- --------------- ----------
     vs1         bucket1    read-only       allow-only
```

The following example displays information for all buckets on an SVM:

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1

     Vserver           :vs1
     Bucket            :test-bucket
     Access            :all
     Permission        :all
```

The following example displays the name, audit state, event types, log format, and target directory for all SVMs.

```
cluster1::> vserver object-store-server audit show

Vserver     State  Event Types Log Format Target Directory
----------- ------ ----------- ---------- --------------------
vs1         false  data        json       /audit_log
```

The following example displays the SVM names and details about the audit log for all SVMs.

```
cluster1::> vserver object-store-server audit show -log-save-details

                 Rotation                              Rotation
      Vserver    File Size Rotation Schedule           Limit
      ---------- --------- ------------------------- --------
      vs1        100MB     -                         0
```

The following example displays in list form all audit configuration information about all SVMs.

```
cluster1::> vserver object-store-server audit show -instance

                           Vserver: vs1
                  Auditing state: true
             Log Destination Path: /audit_log
       Categories of Events to Audit: data
                        Log Format: json
              Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
         Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
                 Rotation Schedules: -
           Log Files Rotation Limit: 0
                 Log Retention Time: 0s
```