NetApp

Audit NAS events on SVMs

ONTAP 9

NetApp
September 15, 2022

Table of Contents

Audit NAS events on SVMs

Audit NAS events on SVMs overview

Auditing for NAS events is a security measure that enables you to track and log certain SMB and NFS events on storage virtual machines (SVMs). This helps you track potential security problems and provides evidence of any security breaches. You can also stage and audit Active Directory central access policies to see what the result of implementing them would be.

SMB events

You can audit the following events:

- SMB file and folder access events

  You can audit SMB file and folder access events on objects stored on FlexVol volumes belonging to the auditing-enabled SVMs.

- SMB logon and logoff events

  You can audit SMB logon and logoff events for SMB servers on SVMs.

- Central access policy staging events

  You can audit the effective access of objects on SMB servers using permissions applied through proposed central access policies. Auditing through the staging of central access policies enables you to see what the effects are of central access policies before they are deployed.

  Auditing of central access policy staging is set up using Active Directory GPOs; however, the SVM auditing configuration must be configured to audit central access policy staging events.

  Although you can enable central access policy staging in the auditing configuration without enabling Dynamic Access Control on the SMB server, central access policy staging events are generated only if Dynamic Access Control is enabled. Dynamic Access Control is enabled through a SMB server option. It is not enabled by default.

NFS events

You can audit file and directory NFSv4 access events on objects stored on SVMs.

How auditing works

Basic auditing concepts

To understand auditing in ONTAP, you should be aware of some basic auditing concepts.

- **Staging files**

  The intermediate binary files on individual nodes where audit records are stored prior to consolidation and

conversion. Staging files are contained in staging volumes.

- **Staging volume**

  A dedicated volume created by ONTAP to store staging files. There is one staging volume per aggregate. Staging volumes are shared by all audit-enabled storage virtual machines (SVMs) to store audit records of data access for data volumes in that particular aggregate. Each SVM's audit records are stored in a separate directory within the staging volume.

  Cluster administrators can view information about staging volumes, but most other volume operations are not permitted. Only ONTAP can create staging volumes. ONTAP automatically assigns a name to staging volumes. All staging volume names begin with `MDV_aud_` followed by the UUID of the aggregate containing that staging volume (for example: `MDV_aud_1d0131843d4811e296fc123478563412.`)

- **System volumes**

  A FlexVol volume that contains special metadata, such as metadata for file services audit logs. The admin SVM owns system volumes, which are visible across the cluster. Staging volumes are a type of system volume.

- **Consolidation task**

  A task that gets created when auditing is enabled. This long-running task on each SVM takes the audit records from staging files across the member nodes of the SVM. This task merges the audit records in sorted chronological order, and then converts them to a user-readable event log format specified in the auditing configuration—either the EVTX or XML file format. The converted event logs are stored in the audit event log directory that is specified in the SVM auditing configuration.

How the ONTAP auditing process works

The ONTAP auditing process is different from the Microsoft auditing process. Before you configure auditing, you should understand how the ONTAP auditing process works.

Audit records are initially stored in binary staging files on individual nodes. If auditing is enabled on an SVM, every member node maintains staging files for that SVM. Periodically, they are consolidated and converted to user-readable event logs, which are stored in the audit event log directory for the SVM.

Process when auditing is enabled on an SVM

Auditing can only be enabled on SVMs. When the storage administrator enables auditing on the SVM, the auditing subsystem checks whether staging volumes are present. A staging volume must exist for each aggregate that contains data volumes owned by the SVM. The auditing subsystem creates any needed staging volumes if they do not exist.

The auditing subsystem also completes other prerequisite tasks before auditing is enabled:

- The auditing subsystem verifies that the log directory path is available and does not contain symlinks.

  The log directory must already exist as a path within the SVM's namespace. It is recommended to create a new volume or qtree to hold the audit log files. The auditing subsystem does not assign a default log file location. If the log directory path specified in the auditing configuration is not a valid path, auditing configuration creation fails with the `The specified path "/path" does not exist in the namespace belonging to Vserver "Vserver_name"` error.

Configuration creation fails if the directory exists but contains symlinks.

- Auditing schedules the consolidation task.

  After this task is scheduled, auditing is enabled. The SVM auditing configuration and the log files persist across a reboot or if the NFS or SMB servers are stopped or restarted.

Event log consolidation

Log consolidation is a scheduled task that runs on a routine basis until auditing is disabled. When auditing is disabled, the consolidation task verifies that all of the remaining logs are consolidated.

Guaranteed auditing

By default, auditing is guaranteed. ONTAP guarantees that all auditable file access events (as specified by configured audit policy ACLs) are recorded, even if a node is unavailable. A requested file 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 to the disk in the staging files, either because of insufficient space or because of other issues, client operations are denied.

> (i) An administrator, or account user with privilege level access, can bypass the file audit logging operation by using NetApp Manageability SDK or REST APIs. You can determine if any file actions have been taken using NetApp Manageability SDK or REST APIs by reviewing the command history logs stored in the `audit.log` file.
>
> For more information about command history audit logs, see the "Managing audit logging for management activities" section in System administration.

Consolidation process when a node is unavailable

If a node containing volumes belonging to an SVM with auditing enabled is unavailable, the behavior of the auditing consolidation task depends on whether the node's storage failover (SFO) partner (or the HA partner in the case of a two-node cluster) is available:

- If the staging volume is available through the SFO partner, the staging volumes last reported from the node are scanned, and consolidation proceeds normally.

- If the SFO partner is not available, the task creates a partial log file.

  When a node is not reachable, the consolidation task consolidates the audit records from the other available nodes of that SVM. To identify that it is not complete, the task adds the suffix `.partial` to the consolidated file name.

- After the unavailable node is available, the audit records in that node are consolidated with the audit records from the other nodes at that time.

- All audit records are preserved.

Event log rotation

Audit event log files are rotated when they reach a configured threshold log size or 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.

Process when auditing is disabled on the SVM

When auditing is disabled on the SVM, the consolidation task is triggered one final time. All outstanding, recorded audit records are logged in a user-readable format. Existing event logs stored in the event log directory are not deleted when auditing is disabled on the SVM and are available for viewing.

After all existing staging files for that SVM are consolidated, the consolidation task is removed from the schedule. Disabling the auditing configuration for the SVM does not remove the auditing configuration. A storage administrator can reenable auditing at any time.

The auditing consolidation job, which gets created when auditing is enabled, monitors the consolidation task and re-creates it if the consolidation task exits because of an error. Previously, users could delete the auditing consolidation job by using job manager commands such as `job delete`. Users are no longer allowed to delete the auditing consolidation job.

Auditing requirements and considerations

Before you configure and enable auditing on your storage virtual machine (SVM), you need to be aware of certain requirements and considerations.

- The maximum number of auditing-enabled SVMs supported in a cluster is 50.
- Auditing is not tied to SMB or NFS licensing.

  You can configure and enable auditing even if SMB and NFS licenses are not installed on the cluster.

- NFS auditing supports security ACEs (type U).
- For NFS auditing, there is no mapping between mode bits and auditing ACEs.

  When converting ACLs to mode bits, auditing ACEs are skipped. When converting mode bits to ACLs, auditing ACEs are not generated.

- The directory specified in the auditing configuration must exist.

  If it does not exist, the command to create the auditing configuration fails.

- The directory specified in the auditing configuration must meet the following requirements:

  ◦ The directory must not contain symbolic links.

    If the directory specified in the auditing configuration contains symbolic links, the command to create the auditing configuration fails.

  ◦ You must specify the directory by using an absolute path.

    You should not specify a relative path, for example, `/vs1/../`.

- Auditing is dependent on having available space in the staging volumes.

  You must be aware of and have a plan for ensuring that there is sufficient space for the staging volumes in aggregates that contain audited volumes.

- Auditing is dependent on having available space in the volume containing the directory where converted event logs are stored.

You must be aware of and have a plan for ensuring that there is sufficient space in the volumes used to store event logs. You can specify the number of event logs to retain in the auditing directory by using the `-rotate-limit` parameter when creating an auditing configuration, which can help to ensure that there is enough available space for the event logs in the volume.

- Although you can enable central access policy staging in the auditing configuration without enabling Dynamic Access Control on the SMB server, Dynamic Access Control must be enabled to generate central access policy staging events.

  Dynamic Access Control is not enabled by default.

Aggregate space considerations when enabling auditing

When an auditing configuration is created and auditing is enabled on at least one storage virtual machine (SVM) in the cluster, the auditing subsystem creates staging volumes on all existing aggregates and on all new aggregates that are created. You need to be aware of certain aggregate space considerations when you enable auditing on the cluster.

Staging volume creation might fail due to non-availability of space in an aggregate. This might happen if you create an auditing configuration and existing aggregates do not have enough space to contain the staging volume.

You should ensure that there is enough space on existing aggregates for the staging volumes before enabling auditing on an SVM.

Limitations for the size of audit records on staging files

The size of an audit record on a staging file cannot be greater than 32 KB.

When large audit records can occur

Large audit records might occur during management auditing in one of the following scenarios:

- Adding or deleting users to or from groups with a large number of users.
- Adding or deleting a file-share access control list (ACL) on a file-share with a large number of file-share users.
- Other scenarios.

Disable management auditing to avoid this issue. To do this, modify the audit configuration and remove the following from the list of audit event types:

- file-share
- user-account
- security-group
- authorization-policy-change

  After removal, they will not be audited by the file services auditing subsystem.

The effects of audit records that are too large

- If the size of an audit record is too large (over 32 KB), the audit record is not created and the auditing subsystem generates an event management system (EMS) message similar to the following:

  ```
  File Services Auditing subsystem failed the operation or truncated an audit
  record because it was greater than max_audit_record_size value. Vserver
  UUID=%s, event_id=%u, size=%u
  ```

  If auditing is guaranteed, the file operation fails because its audit record cannot be created.

- If the size of the audit record is more than 9,999 bytes, the same EMS message as above is displayed. A partial audit record is created with the larger key value missing.

- If the audit record exceeds 2,000 characters, the following error message shows instead of the actual value:

  ```
  The value of this field was too long to display.
  ```

What the supported audit event log formats are

Supported file formats for the converted audit event logs are `EVTX` and `XML` file formats.

You can specify the type of file format when you create the auditing configuration. By default, ONTAP converts the binary logs to the `EVTX` file format.

View audit event logs

You can use audit event logs to determine whether you have adequate file security and whether there have been improper file and folder access attempts. You can view and process audit event logs saved in the `EVTX` or `XML` file formats.

- `EVTX` file format

  You can open the converted `EVTX` audit event logs as saved files using Microsoft Event Viewer.

  There are two options that you can use when viewing event logs using Event Viewer:

  ○ General view

    Information that is common to all events is displayed for the event record. In this version of ONTAP, the event-specific data for the event record is not displayed. You can use the detailed view to display event-specific data.

  ○ Detailed view

    A friendly view and an XML view are available. The friendly view and the XML view display both the information that is common to all events and the event-specific data for the event record.

- `XML` file format

  You can view and process `XML` audit event logs on third-party applications that support the `XML` file format.

XML viewing tools can be used to view the audit logs provided you have the XML schema and information about definitions for the XML fields. For more information about the XML schema and definitions, see the ONTAP Auditing Schema Reference.

How active audit logs are viewed using Event Viewer

If the audit consolidation process is running on the cluster, the consolidation process appends new records to the active audit log file for audit-enabled storage virtual machines (SVMs). This active audit log can be accessed and opened over an SMB share in Microsoft Event Viewer.

In addition to viewing existing audit records, Event Viewer has a refresh option that enables you to refresh the content in the console window. Whether the newly appended logs are viewable in Event Viewer depends on whether oplocks are enabled on the share used to access the active audit log.

Oplocks setting on the share	Behavior
Enabled	Event Viewer opens the log that contains events written to it up to that point in time. The refresh operation does not refresh the log with new events appended by the consolidation process.
Disabled	Event Viewer opens the log that contains events written to it up to that point in time. The refresh operation refreshes the log with new events appended by the consolidation process.

> ⓘ This information is applicable only for `EVTX` event logs. `XML` event logs can be viewed through SMB in a browser or through NFS using any XML editor or viewer.

SMB events that can be audited

SMB events that can be audited overview

ONTAP can audit certain SMB events, including certain file and folder access events, certain logon and logoff events, and central access policy staging events. Knowing which access events can be audited is helpful when interpreting results from the event logs.

The following additional SMB events can be audited in ONTAP 9.2 and later:

Event ID (EVT/EVTX)	Event	Description	Category
4670	Object permissions were changed	OBJECT ACCESS: Permissions changed.	File Access
4907	Object auditing settings were changed	OBJECT ACCESS: Audit settings changed.	File Access
4913	Object Central Access Policy was changed	OBJECT ACCESS: CAP changed.	File Access

The following SMB events can be audited in ONTAP 9.0 and later:

Event ID (EVT/EVTX)	Event	Description	Category
540/4624	An account was successfully logged on	LOGON/LOGOFF: Network (SMB) logon.	Logon and Logoff
529/4625	An account failed to log on	LOGON/LOGOFF: Unknown user name or bad password.	Logon and Logoff
530/4625	An account failed to log on	LOGON/LOGOFF: Account logon time restriction.	Logon and Logoff
531/4625	An account failed to log on	LOGON/LOGOFF: Account currently disabled.	Logon and Logoff
532/4625	An account failed to log on	LOGON/LOGOFF: User account has expired.	Logon and Logoff
533/4625	An account failed to log on	LOGON/LOGOFF: User cannot log on to this computer.	Logon and Logoff
534/4625	An account failed to log on	LOGON/LOGOFF: User not granted logon type here.	Logon and Logoff
535/4625	An account failed to log on	LOGON/LOGOFF: User's password has expired.	Logon and Logoff
537/4625	An account failed to log on	LOGON/LOGOFF: Logon failed for reasons other than above.	Logon and Logoff
539/4625	An account failed to log on	LOGON/LOGOFF: Account locked out.	Logon and Logoff
538/4634	An account was logged off	LOGON/LOGOFF: Local or network user logoff.	Logon and Logoff
560/4656	Open Object/Create Object	OBJECT ACCESS: Object (file or directory) open.	File Access
563/4659	Open Object with the Intent to Delete	OBJECT ACCESS: A handle to an object (file or directory) was requested with the Intent to Delete.	File Access

564/4660	Delete Object	OBJECT ACCESS: Delete Object (file or directory). ONTAP generates this event when a Windows client attempts to delete the object (file or directory).	File Access
567/4663	Read Object/Write Object/Get Object Attributes/Set Object Attributes	OBJECT ACCESS: Object access attempt (read, write, get attribute, set attribute). **Note:** For this event, ONTAP audits only the first SMB read and first SMB write operation (success or failure) on an object. This prevents ONTAP from creating excessive log entries when a single client opens an object and performs many successive read or write operations to the same object.	File Access
NA/4664	Hard link	OBJECT ACCESS: An attempt was made to create a hard link.	File Access
NA/4818	Proposed central access policy does not grant the same access permissions as the current central access policy	OBJECT ACCESS: Central Access Policy Staging.	File Access
NA/NA Data ONTAP Event ID 9999	Rename Object	OBJECT ACCESS: Object renamed. This is an ONTAP event. It is not currently supported by Windows as a single event.	File Access
NA/NA Data ONTAP Event ID 9998	Unlink Object	OBJECT ACCESS: Object unlinked. This is an ONTAP event. It is not currently supported by Windows as a single event.	File Access

Additional information about Event 4656

The `HandleID` tag in the audit `XML` event contains the handle of the object (file or directory) accessed. The `HandleID` tag for the EVTX 4656 event contains different information depending on whether the open event is for creating a new object or for opening an existing object:

- If the open event is an open request to create a new object (file or directory), the `HandleID` tag in the audit XML event shows an empty `HandleID` (for example: `<Data Name="HandleID">00000000000000;00;00000000;00000000</Data>`).

  The `HandleID` is empty because the OPEN (for creating a new object) request gets audited before the actual object creation happens and before a handle exists. Subsequent audited events for the same object

have the right object handle in the `HandleID` tag.

- If the open event is an open request to open an existing object, the audit event will have the assigned handle of that object in the `HandleID` tag (for example: `<Data Name="HandleID">00000000000401;00;000000ea;00123ed4</Data>`).

Determine what the complete path to the audited object is

The object path printed in the `<ObjectName>` tag for an audit record contains the name of the volume (in parentheses) and the relative path from the root of the containing volume. If you want to determine the complete path of the audited object, including the junction path, there are certain steps you must take.

Steps

1. Determine what the volume name and relative path to audited object is by looking at the `<ObjectName>` tag in the audit event.

   In this example, the volume name is "data1" and the relative path to the file is `/dir1/file.txt`:

   `<Data Name="ObjectName"> (data1);/dir1/file.txt </Data>`

2. Using the volume name determined in the previous step, determine what the junction path is for the volume containing the audited object:

   In this example, the volume name is "data1" and the junction path for the volume containing the audited object is `/data/data1`:

   `volume show -junction -volume data1`

   ```
                                    Junction                      Junction
    Vserver    Volume        Language Active    Junction Path     Path Source
    --------- ------------ -------- --------  ----------------- -----------
    vs1        data1         en_US.UTF-8
                                      true     /data/data1       RW_volume
   ```

3. Determine the full path to the audited object by appending the relative path found in the `<ObjectName>` tag to the junction path for the volume.

   In this example, the junction path for the volume:

   `/data/data1/dir1/file.text`

Considerations when auditing symlinks and hard links

There are certain considerations you must keep in mind when auditing symlinks and hard links.

An audit record contains information about the object being audited including the path to the audited object, which is identified in the `ObjectName` tag. You should be aware of how paths for symlinks and hard links are

recorded in the `ObjectName` tag.

Symlinks

A symlink is a file with a separate inode that contains a pointer to the location of a destination object, known as the target. When accessing an object through a symlink, ONTAP automatically interprets the symlink and follows the actual canonical protocol agnostic path to the target object in the volume.

In the following example output, there are two symlinks, both pointing to a file named `target.txt`. One of the symlinks is a relative symlink and one is an absolute symlink. If either of the symlinks are audited, the `ObjectName` tag in the audit event contains the path to the file `target.txt`:

```
[root@host1 audit]# ls -l
total 0
lrwxrwxrwx 1 user1 group1 37 Apr  2 10:09 softlink_fullpath.txt ->
/data/audit/target.txt
lrwxrwxrwx 1 user1 group1 10 Apr  2 09:54 softlink.txt -> target.txt
-rwxrwxrwx 1 user1 group1 16 Apr  2 10:05 target.txt
```

Hard links

A hard link is a directory entry that associates a name with an existing file on a file system. The hard link points to the inode location of the original file. Similar to how ONTAP interprets symlinks, ONTAP interprets the hard link and follows the actual canonical path to the target object in the volume. When access to a hard link object is audited, the audit event records this absolute canonical path in the `ObjectName` tag rather than the hard link path.

Considerations when auditing alternate NTFS data streams

There are certain considerations you must keep in mind when auditing files with NTFS alternate data streams.

The location of an object being audited is recorded in an event record using two tags, the `ObjectName` tag (the path) and the `HandleID` tag (the handle). To properly identify which stream requests are being logged, you must be aware of what ONTAP records in these fields for NTFS alternate data streams:

- EVTX ID: 4656 events (open and create audit events)
  - The path of the alternate data stream is recorded in the `ObjectName` tag.
  - The handle of the alternate data stream is recorded in the `HandleID` tag.
- EVTX ID: 4663 events (all other audit events, such as read, write, getattr, and so on)
  - The path of the base file, not the alternate data stream, is recorded in the `ObjectName` tag.
  - The handle of the alternate data stream is recorded in the `HandleID` tag.

Example

The following example illustrates how to identify EVTX ID: 4663 events for alternate data streams using the `HandleID` tag. Even though the `ObjectName` tag (path) recorded in the read audit event is to the base file path, the `HandleID` tag can be used to identify the event as an audit record for the alternate data stream.

Stream file names take the form `base_file_name:stream_name`. In this example, the `dir1` directory contains a base file with an alternate data stream having the following paths:

```
/dir1/file1.txt
/dir1/file1.txt:stream1
```

ⓘ The output in the following event example is truncated as indicated; the output does not display all of the available output tags for the events.

For an EVTX ID 4656 (open audit event), the audit record output for the alternate data stream records the alternate data stream name in the `ObjectName` tag:

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4656</EventID>
  <EventName>Open Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt:stream1</Data\>
**
  [...]
  </EventData>
  </Event>
- <Event>
```

For an EVTX ID 4663 (read audit event), the audit record output for the same alternate data stream records the base file name in the `ObjectName` tag; however, the handle in the `HandleID` tag is the alternative data stream's handle and can be used to correlate this event with the alternative data stream:

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4663</EventID>
  <EventName>Read Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt</Data\> **
  [...]
  </EventData>
  </Event>
- <Event>
```

NFS file and directory access events that can be audited

ONTAP can audit certain NFS file and directory access events. Knowing what access events can be audited is helpful when interpreting results from the converted audit event logs.

You can audit the following NFS file and directory access events:

- READ
- OPEN
- CLOSE
- READDIR
- WRITE
- SETATTR
- CREATE
- LINK
- OPENATTR
- REMOVE
- GETATTR
- VERIFY
- NVERIFY
- RENAME

To reliably audit NFS RENAME events, you should set audit ACEs on directories instead of files because file permissions are not checked for a RENAME operation if the directory permissions are sufficient.

Plan the auditing configuration

Before you configure auditing on storage virtual machines (SVMs), you must understand which configuration options are available and plan the values that you want to set for each option. This information can help you configure the auditing configuration that meets your business needs.

There are certain configuration parameters that are common to all auditing configurations.

Additionally, there are certain parameters that you can use to specify which methods are used when rotating the consolidated and converted audit logs. You can specify one of the three following methods when you configure auditing:

- Rotate logs based on log size

    This is the default method used to rotate logs.

- Rotate logs based on a schedule
- Rotate logs based on log size and schedule (whichever event occurs first)

> (i) At least one of the methods for log rotation should always be set.

Parameters common to all auditing configurations

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	Include	Your values
SVM name Name of the SVM on which to create the auditing configuration. The SVM must already exist.	`-vserver vserver_name`	Yes	Yes	

| *Log destination path*

Specifies the directory where the converted audit logs are stored, typically a dedicated volume or qtree. The path must already exist in the SVM namespace.

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.

If the SVM is an SVM disaster recovery source, the log destination path cannot be on the root volume. This is because root volume content is not replicated to the disaster recovery destination.

You cannot use a FlexCache volume as a log destination (ONTAP 9.7 and later). | `-destination text` | Yes | Yes | 15 |

Categories of events to audit Specifies the categories of events to audit. The following event categories can be audited: • File access events (both SMB and NFSv4) • SMB logon and logoff events • Central access policy staging events Central access policy staging events are a new advanced auditing event available beginning with Windows 2012 Active Directory domains. Central access policy staging events log information about changes to central access policies configured in Active Directory. • File share category events • Audit policy change events • Local user account management events • Security group management events • Authorization policy change events The default is to audit file access and SMB logon and logoff events. **Note:** Before you can specify `cap-staging` as an event category, a SMB server must exist on the SVM. Although you can enable central access policy staging in the auditing configuration without enabling Dynamic Access Control on the SMB server, central access policy staging events are generated only if Dynamic Access Control is enabled. Dynamic Access Control is enabled through a SMB server option. It is not enabled by default.	`-events {file-ops|cifs-logon-logoff|cap-staging|file-share |audit-policy-change |user-account|security-group|authorization-policy-change}`	No		
Log file output format Determines the output format of the audit logs. The output format can be either ONTAP-specific `XML` or Microsoft Windows `EVTX` log format. By default, the output format is `EVTX`.	`-format {xml|evtx}`	No		

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		

Parameters used for determining when to rotate audit event logs

Rotate logs based on log size

The default is to rotate audit logs based on size.

- The default log size is 100 MB

- 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.

- If you want to rotate the audit logs based on a log size alone, use the following command to unset the `-rotate-schedule-minute` parameter: `vserver audit modify -vserver vs0 -destination / -rotate-schedule-minute -`

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

Type of information	Option	Required	Include	Your values
Log file size limit Determines the audit log file size limit.	`-rotate-size { integer[KB|MB|GB|TB|PB]}`	No		

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.

- 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 rotate the audit logs based on a schedule alone, use the following command to unset the `-rotate-size` parameter: `vserver audit modify -vserver vs0 -destination / -rotate -size -`

You can use the following list of available auditing parameters to determine what values to use for configuring a schedule for audit event log rotations:

Type of information	Option	Required	Include	Your values
Log rotation schedule: Month Determines the monthly schedule for rotating audit logs. Valid values are `January` through `December`, and `all`. For example, you can specify that the audit log is to be rotated during the months January, March, and August.	`-rotate-schedule-month` `chron_month`	No		

Log rotation schedule: Day of week
 	
Determines the daily (day of week) schedule for rotating audit logs.
 	
Valid values are `Sunday` through `Saturday`, and `all`. For example, you can specify that the audit log is to be rotated on Tuesdays and Fridays, or during all the days of a week.
	`-rotate-schedule`
	`-dayofweek`
	`chron_dayofweek`
		No		

Log rotation schedule: Day Determines the day of the month schedule for rotating the audit log. Valid values range from `1` through `31`. For example, you can specify that the audit log is to be rotated on the 10th and 20th days of a month, or all days of a month.	`-rotate-schedule-day` `chron_dayofmonth`	No		

Log rotation schedule: Hour Determines the hourly schedule for rotating the audit log. Valid values range from `0` (midnight) to `23` (11:00 p.m.). Specifying `all` rotates the audit logs every hour. For example, you can specify that the audit log is to be rotated at 6 (6 a.m.) and 18 (6 p.m.).	`-rotate-schedule-hour chron_hour`	No		
Log rotation schedule: Minute Determines the minute schedule for rotating the audit log. Valid values range from `0` to `59`. For example, you can specify that the audit log is to be rotated at the 30th minute.	`-rotate-schedule-minute chron_minute`	Yes, if configuring schedule-based log rotation; otherwise, no.		

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 a file and directory auditing configuration on SVMs

Create the auditing configuration

Creating a file and directory auditing configuration on your storage virtual machine (SVM) includes understanding the available configuration options, planning the configuration, and then configuring and enabling the configuration. You can then display information about the auditing configuration to confirm that the resultant configuration is the desired configuration.

Before you can begin auditing file and directory events, you must create an auditing configuration on the storage virtual machine (SVM).

Before you begin

If you plan on creating an auditing configuration for central access policy staging, a SMB server must exist on the SVM.

- Although you can enable central access policy staging in the auditing configuration without enabling Dynamic Access Control on the SMB server, central access policy staging events are generated only if Dynamic Access Control is enabled.

  Dynamic Access Control is enabled through a SMB server option. It is not enabled by default.

- If the arguments of a field in a command is invalid, for example, invalid entries for fields, duplicate entries, and non-existent entries, then the command fails before the audit phase.

  Such failures do not generate an audit record.

About this task

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

Step

1. Using the information in the planning worksheet, 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 audit create -vserver vserver_name -destination path -events [{file-ops|cifs-logon-logoff|cap-staging|file-share|audit-policy-change|user-account|security-group|authorization-policy-change}] [-format {xml|evtx}] [-rotate-limit integer] [-rotate-size {integer[KB|MB|GB|TB|PB]}]`
A schedule	`vserver audit create -vserver vserver_name -destination path -events [{file-ops|cifs-logon-logoff|cap-staging}] [-format {xml|evtx}] [-rotate-limit integer] [-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.

Examples

The following example creates an auditing configuration that audits file operations and SMB logon and logoff events (the default) using size-based rotation. The log format is EVTX (the default). 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 file operations and SMB logon and logoff events (the default) using size-based rotation. The log format is `EVTX` (the default). The log file size limit is `100 MB` (the default), and the log rotation limit is `5`:

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-limit 5
```

The following example creates an auditing configuration that audits file operations, CIFS logon and logoff events, and central access policy staging events using time-based rotation. The log format is `EVTX` (the default). 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 file-ops,cifs-logon-logoff,file-share,audit-policy-change,user-
account,security-group,authorization-policy-change,cap-staging -rotate
-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour
12 -rotate-schedule-minute 30 -rotate-limit 5
```

Enable auditing on the SVM

After you finish setting up the auditing configuration, you must enable auditing on the storage virtual machine (SVM).

What you'll need
The SVM audit configuration must already exist.

About this task
When an SVM disaster recovery ID discard configuration is first started (after the SnapMirror initialization is complete) and the SVM has an auditing configuration, ONTAP automatically disables the auditing configuration. Auditing is disabled on the read-only SVM to prevent the staging volumes from filling up. You can enable auditing only after the SnapMirror relationship is broken and the SVM is read-write.

Step
1. Enable auditing on the SVM:

   ```
   vserver audit enable -vserver vserver_name
   ```

   ```
   vserver audit enable -vserver vs1
   ```

Verify the auditing configuration

After completing the auditing configuration, you should verify that auditing is configured properly and is enabled.

Steps
1. Verify the auditing configuration:

   ```
   vserver audit show -instance -vserver vserver_name
   ```

The following command displays in list form all auditing configuration information for storage virtual machine (SVM) vs1:

```
vserver audit show -instance -vserver vs1
```

```
                          Vserver: vs1
                  Auditing state: true
             Log Destination Path: /audit_log
        Categories of Events to Audit: file-ops
                      Log Format: evtx
               Log File Size Limit: 200MB
        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
```

Configure file and folder audit policies

Configure file and folder audit policies

Implementing auditing on file and folder access events is a two-step process. First, you must create and enable an auditing configuration on storage virtual machines (SVMs). Second, you must configure audit policies on the files and folders that you want to monitor. You can configure audit policies to monitor both successful and failed access attempts.

You can configure both SMB and NFS audit policies. SMB and NFS audit policies have different configuration requirements and audit capabilities.

If the appropriate audit policies are configured, ONTAP monitors SMB and NFS access events as specified in the audit policies only if the SMB or NFS servers are running.

Configure audit policies on NTFS security-style files and directories

Before you can audit file and directory operations, you must configure audit policies on the files and directories for which you want to collect audit information. This is in addition to setting up and enabling the audit configuration. You can configure NTFS audit policies by using the Windows Security tab or by using the ONTAP CLI.

Configuring NTFS audit policies using the Windows Security tab

You can configure NTFS audit policies on files and directories by using the **Windows Security** tab in the Windows Properties window. This is the same method used when

configuring audit policies on data residing on a Windows client, which enables you to use the same GUI interface that you are accustomed to using.

What you'll need

Auditing must be configured on the storage virtual machine (SVM) that contains the data to which you are applying system access control lists (SACLs).

About this task

Configuring NTFS audit policies is done by adding entries to NTFS SACLs that are associated with an NTFS security descriptor. The security descriptor is then applied to NTFS files and directories. These tasks are automatically handled by the Windows GUI. The security descriptor can contain discretionary access control lists (DACLs) for applying file and folder access permissions, SACLs for file and folder auditing, or both SACLs and DACLs.

To set NTFS audit policies using the Windows Security tab, complete the following steps on a Windows host:

Steps

1. From the **Tools** menu in Windows Explorer, select **Map network drive**.

2. Complete the **Map Network Drive** box:

    a. Select a **Drive** letter.

    b. In the **Folder** box, type the SMB server name that contains the share, holding the data you want to audit and the name of the share.

    You can specify the IP address of the data interface for the SMB server instead of the SMB server name.

    If your SMB server name is "SMB_SERVER" and your share is named "share1", you should enter `\\SMB_SERVER\share1`.

    c. Click **Finish**.

    The drive you selected is mounted and ready with the Windows Explorer window displaying files and folders contained within the share.

3. Select the file or directory for which you want to enable auditing access.

4. Right-click the file or directory, and then select **Properties**.

5. Select the **Security** tab.

6. Click **Advanced**.

7. Select the **Auditing** tab.

8. Perform the desired actions:

If you want to….	Do the following
Set up auditing for a new user or group	a. Click **Add**. b. In the Enter the object name to select box, type the name of the user or group that you want to add. c. Click **OK**.

Remove auditing from a user or group	a. In the Enter the object name to select box, select the user or group that you want to remove. b. Click **Remove**. c. Click **OK**. d. Skip the rest of this procedure.
Change auditing for a user or group	a. In the Enter the object name to select box, select the user or group that you want to change. b. Click **Edit**. c. Click **OK**.

If you are setting up auditing on a user or group or changing auditing on an existing user or group, the Auditing Entry for <object> box opens.

9. In the **Apply to** box, select how you want to apply this auditing entry.

You can select one of the following:

- **This folder, subfolders and files**
- **This folder and subfolders**
- **This folder only**
- **This folder and files**
- **Subfolders and files only**
- **Subfolders only**
- **Files only** If you are setting up auditing on a single file, the **Apply to** box is not active. The **Apply to** box setting defaults to **This object only**.

> (i) Because auditing takes SVM resources, select only the minimal level that provides the auditing events that meet your security requirements.

10. In the **Access** box, select what you want audited and whether you want to audit successful events, failure events, or both.

- To audit successful events, select the Success box.
- To audit failure events, select the Failure box.

Select only the actions that you need to monitor to meet your security requirements. For more information about these auditable events, see your Windows documentation. You can audit the following events:

- **Full control**
- **Traverse folder / execute file**
- **List folder / read data**
- **Read attributes**
- **Read extended attributes**
- **Create files / write data**

- ◦ **Create folders / append data**
- ◦ **Write attributes**
- ◦ **Write extended attributes**
- ◦ **Delete subfolders and files**
- ◦ **Delete**
- ◦ **Read permissions**
- ◦ **Change permissions**
- ◦ **Take ownership**

11. If you do not want the auditing setting to propagate to subsequent files and folders of the original container, select the **Apply these auditing entries to objects and/or containers within this container only** box.

12. Click **Apply**.

13. After you finish adding, removing, or editing auditing entries, click **OK**.

    The Auditing Entry for <object> box closes.

14. In the **Auditing** box, select the inheritance settings for this folder.

    Select only the minimal level that provides the auditing events that meet your security requirements. You can choose one of the following:

    - ◦ Select the Include inheritable auditing entries from this object's parent box.
    - ◦ Select the Replace all existing inheritable auditing entries on all descendants with inheritable auditing entries from this object box.
    - ◦ Select both boxes.
    - ◦ Select neither box. If you are setting SACLs on a single file, the Replace all existing inheritable auditing entries on all descendants with inheritable auditing entries from this object box is not present in the Auditing box.

15. Click **OK**.

    The Auditing box closes.

Configure NTFS audit policies using the ONTAP CLI

You can configure audit policies on files and folders using the ONTAP CLI. This enables you to configure NTFS audit policies without needing to connect to the data using an SMB share on a Windows client.

You can configure NTFS audit policies by using the `vserver security file-directory` command family.

You can only configure NTFS SACLs using the CLI. Configuring NFSv4 SACLs is not supported with this ONTAP command family. See the man pages for more information about using these commands to configure and add NTFS SACLs to files and folders.

Configure auditing for UNIX security style files and directories

You configure auditing for UNIX security style files and directories by adding audit ACEs to NFSv4.x ACLs. This allows you to monitor certain NFS file and directory access events

for security purposes.

About this task

For NFSv4.x, both discretionary and system ACEs are stored in the same ACL. They are not stored in separate DACLs and SACLs. Therefore, you must exercise caution when adding audit ACEs to an existing ACL to avoid overwriting and losing an existing ACL. The order in which you add the audit ACEs to an existing ACL does not matter.

Steps

1. Retrieve the existing ACL for the file or directory by using the `nfs4_getfacl` or equivalent command.

   For more information about manipulating ACLs, see the man pages of your NFS client.

2. Append the desired audit ACEs.

3. Apply the updated ACL to the file or directory by using the `nfs4_setfacl` or equivalent command.

Display information about audit policies applied to files and directories

Display information about audit policies using the Windows Security tab

You can display information about audit policies that have been applied to files and directories by using the Security tab in the Windows Properties window. This is the same method used for data residing on a Windows server, which enables customers to use the same GUI interface that they are accustomed to using.

About this task

Displaying information about audit policies applied to files and directories enables you to verify that you have the appropriate system access control lists (SACLs) set on specified files and folders.

To display information about SACLs that have been applied to NTFS files and folders, complete the following steps on a Windows host.

Steps

1. From the **Tools** menu in Windows Explorer, select **Map network drive**.

2. Complete the **Map Network Drive** dialog box:

   a. Select a **Drive** letter.

   b. In the **Folder** box, type the IP address or SMB server name of the storage virtual machine (SVM) containing the share that holds both the data you would like to audit and the name of the share.

   If your SMB server name is "SMB_SERVER" and your share is named "share1", you should enter `\\SMB_SERVER\share1`.

   > ⓘ You can specify the IP address of the data interface for the SMB server instead of the SMB server name.

   c. Click **Finish**.

   The drive you selected is mounted and ready with the Windows Explorer window displaying files and

folders contained within the share.

3. Select the file or directory for which you display auditing information.

4. Right-click on the file or directory, and select **Properties**.

5. Select the **Security** tab.

6. Click **Advanced**.

7. Select the **Auditing** tab.

8. Click **Continue**.

   The Auditing box opens. The **Auditing entries** box displays a summary of users and groups that have SACLs applied to them.

9. In the **Auditing entries** box select the user or group whose SACL entries you want displayed.

10. Click **Edit**.

    The Auditing entry for <object> box opens.

11. In the **Access** box, view the current SACLs that are applied to the selected object.

12. Click **Cancel** to close the **Auditing entry for <object>** box.

13. Click **Cancel** to close the **Auditing** box.

Display information about NTFS audit policies on FlexVol volumes using the CLI

You can display information about NTFS audit policies on FlexVol volumes, including what the security styles and effective security styles are, what permissions are applied, and information about system access control lists. You can use the information to validate your security configuration or to troubleshoot auditing issues.

About this task

Displaying information about audit policies applied to files and directories enables you to verify that you have the appropriate system access control lists (SACLs) set on specified files and folders.

You must provide the name of the storage virtual machine (SVM) and the path to the files or folders whose audit information you want to display. You can display the output in summary form or as a detailed list.

- NTFS security-style volumes and qtrees use only NTFS system access control lists (SACLs) for audit policies.

- Files and folders in a mixed security-style volume with NTFS effective security can have NTFS audit policies applied to them.

  Mixed security-style volumes and qtrees can contain some files and directories that use UNIX file permissions, either mode bits or NFSv4 ACLs, and some files and directories that use NTFS file permissions.

- The top level of a mixed security-style volume can have either UNIX or NTFS effective security and might or might not contain NTFS SACLs.

- Because Storage-Level Access Guard security can be configured on a mixed security-style volume or qtree even if the effective security style of the volume root or qtree is UNIX, the output for a volume or qtree path where Storage-Level Access Guard is configured might display both regular file and folder NFSv4

SACLs and Storage-Level Access Guard NTFS SACLs.

- If the path that is entered in the command is to data with NTFS effective security, the output also displays information about Dynamic Access Control ACEs if Dynamic Access Control is configured for the given file or directory path.

- When displaying security information about files and folders with NTFS effective security, UNIX-related output fields contain display-only UNIX file permission information.

  NTFS security-style files and folders use only NTFS file permissions and Windows users and groups when determining file access rights.

- ACL output is displayed only for files and folders with NTFS or NFSv4 security.

  This field is empty for files and folders using UNIX security that have only mode bit permissions applied (no NFSv4 ACLs).

- The owner and group output fields in the ACL output apply only in the case of NTFS security descriptors.

Step

1. Display file and directory audit policy settings with the desired level of detail:

If you want to display information…	Enter the following command…
In summary form	`vserver security file-directory show -vserver vserver_name -path path`
As a detailed list	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Examples

The following example displays the audit policy information for the path `/corp` in SVM vs1. The path has NTFS effective security. The NTFS security descriptor contains both a SUCCESS and a SUCCESS/FAIL SACL entry.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                    Vserver: vs1
                  File Path: /corp
          File Inode Number: 357
             Security Style: ntfs
            Effective Style: ntfs
             DOS Attributes: 10
    DOS Attributes in Text: ----D---
     Expanded Dos Attributes: -
               Unix User Id: 0
              Unix Group Id: 0
             Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8014
                             Owner:DOMAIN\Administrator
                             Group:BUILTIN\Administrators
                             SACL - ACEs
                                ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                                SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                             DACL - ACEs
                                ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                                ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                                ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                                ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

The following example displays the audit policy information for the path `/datavol1` in SVM vs1. The path contains both regular file and folder SACLs and Storage-Level Access Guard SACLs.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                  Vserver: vs1
                File Path: /datavol1
         File Inode Number: 77
           Security Style: ntfs
          Effective Style: ntfs
           DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
             Unix User Id: 0
            Unix Group Id: 0
           Unix Mode Bits: 777
  Unix Mode Bits in Text: rwxrwxrwx
                     ACLs: NTFS Security Descriptor
                           Control:0xaa14
                           Owner:BUILTIN\Administrators
                           Group:BUILTIN\Administrators
                           SACL - ACEs
                             AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                           DACL - ACEs
                             ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                             ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                           Storage-Level Access Guard security
                           SACL (Applies to Directories):
                             AUDIT-EXAMPLE\Domain Users-0x120089-FA
                             AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           DACL (Applies to Directories):
                             ALLOW-EXAMPLE\Domain Users-0x120089
                             ALLOW-EXAMPLE\engineering-0x1f01ff
                             ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                           SACL (Applies to Files):
                             AUDIT-EXAMPLE\Domain Users-0x120089-FA
                             AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           DACL (Applies to Files):
                             ALLOW-EXAMPLE\Domain Users-0x120089
                             ALLOW-EXAMPLE\engineering-0x1f01ff
                             ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Ways to display information about file security and audit policies

You can use the wildcard character (*) to display information about file security and audit
policies of all files and directories under a given path or a root volume.

The wildcard character (*) can be used as the last subcomponent of a given directory path below which you want to display information of all files and directories.

If you want to display information of a particular file or directory named as "*", then you need to provide the complete path inside double quotes (" ").

Example

The following command with the wildcard character displays the information about all files and directories below the path `/1/` of SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                      Vserver: vs1
                    File Path: /1/1
               Security Style: mixed
              Effective Style: ntfs
               DOS Attributes: 10
       DOS Attributes in Text: ----D---
       Expanded Dos Attributes: -
                 Unix User Id: 0
                Unix Group Id: 0
               Unix Mode Bits: 777
       Unix Mode Bits in Text: rwxrwxrwx
                         ACLs: NTFS Security Descriptor
                               Control:0x8514
                               Owner:BUILTIN\Administrators
                               Group:BUILTIN\Administrators
                               DACL - ACEs
                               ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                      Vserver: vs1
                    File Path: /1/1/abc
               Security Style: mixed
              Effective Style: ntfs
               DOS Attributes: 10
       DOS Attributes in Text: ----D---
       Expanded Dos Attributes: -
                 Unix User Id: 0
                Unix Group Id: 0
               Unix Mode Bits: 777
       Unix Mode Bits in Text: rwxrwxrwx
                         ACLs: NTFS Security Descriptor
                               Control:0x8404
                               Owner:BUILTIN\Administrators
                               Group:BUILTIN\Administrators
                               DACL - ACEs
                               ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

The following command displays the information of a file named as "*" under the path `/vol1/a` of SVM vs1. The path is enclosed within double quotes (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                  Vserver: vs1
                File Path: "/vol1/a/*"
           Security Style: mixed
          Effective Style: unix
            DOS Attributes: 10
   DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
            Unix User Id: 1002
           Unix Group Id: 65533
           Unix Mode Bits: 755
   Unix Mode Bits in Text: rwxr-xr-x
                      ACLs: NFSV4 Security Descriptor
                            Control:0x8014
                            SACL - ACEs
                                AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                            DACL - ACEs
                                ALLOW-EVERYONE@-0x1f00a9-FI|DI
                                ALLOW-OWNER@-0x1f01ff-FI|DI
                                ALLOW-GROUP@-0x1200a9-IG
```

CLI change events that can be audited

CLI change events that can be audited overview

ONTAP can audit certain CLI change events, including certain SMB-share events, certain audit policy events, certain local security group events, local user group events, and authorization policy events. Understanding which change events can be audited is helpful when interpreting results from the event logs.

You can manage storage virtual machine (SVM) auditing CLI change events by manually rotating the audit logs, enabling or disabling auditing, displaying information about auditing change events, modifying auditing change events, and deleting auditing change events.

As an administrator, if you execute any command to change configuration related to the SMB-share, local user-group, local security-group, authorization-policy, and audit-policy events, a record generates and the corresponding event gets audited:

Auditing Category	Events	Event IDs	Run this command…

Mhost Auditing	policy-change	[4719] Audit configuration changed	`vserver audit disable|enable|modify`
	file-share	[5142] Network share was added	`vserver cifs share create`
		[5143] Network share was modified	`vserver cifs share modify vserver cifs share create|modify|delete vserver cifs share add|remove`
		[5144] Network share deleted	`vserver cifs share delete`

Auditing

		Rename	`and-groups local-user rename`
	security-group	[4731] Local Security Group created	`vserver cifs users-and-groups local-group create` `vserver services name-service unix-group create`
		[4734] Local Security Group deleted	`vserver cifs users-and-groups local-group delete` `vserver services name-service unix-group delete`
		[4735] Local Security Group Modified	`vserver cifs users-and-groups local-group rename|modify` `vserver services name-service unix-group modify`
		[4732] User added to Local Group	`vserver cifs users-and-groups local-group add-members` `vserver services name-service unix-group adduser`
		[4733] User Removed from Local Group	`vserver cifs users-and-groups local-group remove-members` `vserver services name-service unix-group deluser`
	authorization-policy-change	[4704] User Rights Assigned	`vserver cifs users-and-groups privilege add-privilege`
		[4705] User Rights Removed	`vserver cifs users-and-groups privilege remove-privilege|reset-privilege`

Manage file-share event

When a file-share event is configured for a storage virtual machine (SVM) and an audit is enabled, audit events are generated. The file-share events are generated when the SMB network share is modified using `vserver cifs share` related commands.

The file-share events with the event-ids 5142, 5143, and 5144 are generated when a SMB network share is added, modified, or deleted for the SVM. The SMB network share configuration is modified using the `cifs share access control create|modify|delete` commands.

The following example displays a file-share event with the ID 5143 is generated, when a share object called 'audit_dest' is created:

```
netapp-clus1::*> cifs share create -share-name audit_dest -path
/audit_dest
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 5142
   EventName Share Object Added
   ...
   ...
  ShareName audit_dest
  SharePath /audit_dest
  ShareProperties oplocks;browsable;changenotify;show-previous-versions;
  SD O:BAG:S-1-5-21-2447422786-1297661003-4197201688-513D:(A;;FA;;;WD)
```

Manage audit-policy-change event

When an audit-policy-change event is configured for a storage virtual machine (SVM) and an audit is enabled, audit events are generated. The audit-policy-change events are generated when an audit policy is modified using `vserver audit` related commands.

The audit-policy-change event with the event-id 4719 is generated whenever an audit policy is disabled, enabled, or modified and helps to identify when a user attempts to disable auditing to cover the tracks. It is configured by default and requires diagnostic privilege to disable.

The following example displays an audit-policy change event with the ID 4719 generated, when an audit is disabled:

```
netapp-clus1::*> vserver audit disable -vserver vserver_1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4719
   EventName Audit Disabled
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
```

Manage user-account event

When a user-account event is configured for a storage virtual machine (SVM) and an audit is enabled, audit events are generated.

The user-account events with event-ids 4720, 4722, 4724, 4725, 4726, 4738, and 4781 are generated when a local SMB or NFS user is created or deleted from the system, local user account is enabled, disabled or modified, and local SMB user password is reset or changed. The user-account events are generated when a user account is modified using `vserver cifs users-and-groups <local user>` and `vserver services name-service <unix user>` commands.

The following example displays a user account event with the ID 4720 generated, when a local SMB user is created:

```
netapp-clus1::*> vserver cifs users-and-groups local-user create -user
-name testuser -is-account-disabled false -vserver vserver_1
Enter the password:
Confirm the password:

- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4720
   EventName Local Cifs User Created
   ...
   ...
  TargetUserName testuser
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1003
  TargetType CIFS
  DisplayName testuser
  PasswordLastSet 1472662216
  AccountExpires NO
  PrimaryGroupId 513
  UserAccountControl %%0200
  SidHistory ~
  PrivilegeList ~
```

The following example displays a user account event with the ID 4781 generated, when the local SMB user created in the preceding example is renamed:

```
 netapp-clus1::*> vserver cifs users-and-groups local-user rename -user
-name testuser -new-user-name testuser1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4781
   EventName Local Cifs User Renamed
   ...
   ...
  OldTargetUserName testuser
  NewTargetUserName testuser1
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1000
  TargetType CIFS
  SidHistory ~
  PrivilegeList ~
```

Manage security-group event

When a security-group event is configured for a storage virtual machine (SVM) and an audit is enabled, audit events are generated.

The security-group events with event-ids 4731, 4732, 4733, 4734, and 4735 are generated when a local SMB or NFS group is created or deleted from the system, and local user is added or removed from the group. The security-group-events are generated when a user account is modified using `vserver cifs users-and-groups <local-group>` and `vserver services name-service <unix-group>` commands.

The following example displays a security group event with the ID 4731 generated, when a local UNIX security group is created:

```
netapp-clus1::*> vserver services name-service unix-group create -name
testunixgroup -id 20
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4731
   EventName Local Unix Security Group Created
    ...
    ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
  TargetUserName testunixgroup
  TargetDomainName
  TargetGid 20
  TargetType NFS
  PrivilegeList ~
  GidHistory ~
```

Manage authorization-policy-change event

When authorization-policy-change event is configured for a storage virtual machine
(SVM) and an audit is enabled, audit events are generated.

The authorization-policy-change events with the event-ids 4704 and 4705 are generated whenever the
authorization rights are granted or revoked for an SMB user and SMB group. The authorization-policy-change
events are generated when the authorization rights are assigned or revoked using `vserver cifs users-
and-groups privilege` related commands.

The following example displays an authorization policy event with the ID 4704 generated, when the
authorization rights for a SMB user group are assigned:

```
netapp-clus1::*> vserver cifs users-and-groups privilege add-privilege
-user-or-group-name testcifslocalgroup -privileges *
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4704
   EventName User Right Assigned
   ...
   ...
  TargetUserOrGroupName testcifslocalgroup
  TargetUserOrGroupDomainName NETAPP-CLUS1
  TargetUserOrGroupSid S-1-5-21-2447422786-1297661003-4197201688-1004;
  PrivilegeList
SeTcbPrivilege;SeBackupPrivilege;SeRestorePrivilege;SeTakeOwnershipPrivile
ge;SeSecurityPrivilege;SeChangeNotifyPrivilege;
  TargetType CIFS
```

Manage auditing configurations

Manually rotate the audit event logs

Before you can view the audit event logs, the logs must be converted to user-readable formats. If you want to view the event logs for a specific storage virtual machine (SVM) before ONTAP automatically rotates the log, you can manually rotate the audit event logs on an SVM.

Step

1. Rotate the audit event logs by using the `vserver audit rotate-log` command.

   ```
   vserver audit rotate-log -vserver vs1
   ```

   The audit event log is saved in the SVM audit event log directory with the format specified by the auditing configuration (`XML` or `EVTX`), and can be viewed by using the appropriate application.

Enable and disable auditing on SVMs

You can enable or disable auditing on storage virtual machines (SVMs). You might want to temporarily stop file and directory auditing by disabling auditing. You can enable auditing at any time (if an auditing configuration exists).

What you'll need

Before you can enable auditing on the SVM, the SVM's auditing configuration must already exist.

About this task

Disabling auditing does not delete the auditing configuration.

Steps

1. Perform the appropriate command:

If you want auditing to be…	Enter the command…
Enabled	`vserver audit enable -vserver vserver_name`
Disabled	`vserver audit disable -vserver vserver_name`

2. Verify that auditing is in the desired state:

   `vserver audit show -vserver vserver_name`

Examples

The following example enables auditing for SVM vs1:

```
cluster1::> vserver audit enable -vserver vs1

cluster1::> vserver audit show -vserver vs1

                          Vserver: vs1
                  Auditing state: true
            Log Destination Path: /audit_log
      Categories of Events to Audit: file-ops, cifs-logon-logoff
                      Log Format: evtx
             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: 10
```

The following example disables auditing for SVM vs1:

```
cluster1::> vserver audit disable -vserver vs1

                              Vserver: vs1
                      Auditing state: false
                Log Destination Path: /audit_log
          Categories of Events to Audit: file-ops, cifs-logon-logoff
                           Log Format: evtx
                  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: 10
```

Display information about auditing configurations

You can display information about auditing configurations. The information can help you determine whether the configuration is what you want in place for each SVM. The displayed information also enables you to verify whether an auditing configuration is enabled.

About this task

You can display detailed information about auditing configurations on all SVMs or you can customize what information is displayed in the output by specifying optional parameters. If you do not specify any of the optional parameters, the following is displayed:

- SVM name to which the auditing configuration applies
- The audit state, which can be `true` or `false`

  If the audit state is `true`, auditing is enabled. If the audit state is `false`, auditing is disabled.

- The categories of events to audit
- The audit log format
- The target directory where the auditing subsystem stores consolidated and converted audit logs

Step

1. Display information about the auditing configuration by using the `vserver audit show` command.

   For more information about using the command, see the man pages.

Examples

The following example displays a summary of the auditing configuration for all SVMs:

```
cluster1::> vserver audit show

 Vserver      State   Event Types  Log Format  Target Directory
 -----------  ------  -----------  ----------  --------------------
 vs1          false   file-ops     evtx        /audit_log
```

The following example displays, in list form, all auditing configuration information for all SVMs:

```
cluster1::> vserver audit show -instance

                              Vserver: vs1
                       Auditing state: true
                 Log Destination Path: /audit_log
          Categories of Events to Audit: file-ops
                           Log Format: evtx
                    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
```

Commands for modifying auditing configurations

If you want to change an auditing setting, you can modify the current configuration at any time, including modifying the log path destination and log format, modifying the categories of events to audit, how to automatically save log files, and specify the maximum number of log files to save.

If you want to…	Use this command…
Modify the log destination path	`vserver audit modify` with the `-destination` parameter
Modify the category of events to audit	`vserver audit modify` with the `-events` parameter ⓘ To audit central access policy staging events, the Dynamic Access Control (DAC) SMB server option must be enabled on the storage virtual machine (SVM).

Modify the log format	`vserver audit modify` with the `-format` parameter
Enabling automatic saves based on internal log file size	`vserver audit modify` with the `-rotate-size` parameter
Enabling automatic saves based on a time interval	`vserver audit modify` with the `-rotate-schedule-month`, `-rotate-schedule-dayofweek`, `-rotate-schedule-day`, `-rotate-schedule-hour`, and `-rotate-schedule-minute` parameters
Specifying the maximum number of saved log files	`vserver audit modify` with the `-rotate-limit` parameter

Delete an auditing configuration

In you no longer want to audit file and directory events on the storage virtual machine (SVM) and do not want to maintain an auditing configuration on the SVM, you can delete the auditing configuration.

Steps

1. Disable the auditing configuration:

   `vserver audit disable -vserver vserver_name`

   `vserver audit disable -vserver vs1`

2. Delete the auditing configuration:

   `vserver audit delete -vserver vserver_name`

   `vserver audit delete -vserver vs1`

What the process is when reverting

If you plan to revert the cluster, you should be aware of the revert process ONTAP follows when there are auditing-enabled storage virtual machines (SVMs) in the cluster. You must take certain actions before reverting.

Reverting to a version of ONTAP that does not support the auditing of SMB logon and logoff events and central access policy staging events

Support for auditing of SMB logon and logoff events and for central access policy staging events starts with clustered Data ONTAP 8.3. If you are reverting to a version of ONTAP that does not support these event types and you have auditing configurations that monitor these event types, you must change the auditing configuration for those audit-enabled SVMs before reverting. You must modify the configuration so that only file-op events are audited.

Troubleshoot auditing and staging volume space issues

Issues can arise when there is insufficient space on either the staging volumes or on the volume containing the audit event logs. If there is insufficient space, new audit records cannot be created, which prevents clients from accessing data, and access requests fail. You should know how to troubleshoot and resolve these volume space issues.

Troubleshoot space issues related to the event log volumes

If volumes containing event log files run out of space, auditing cannot convert log records into log files. This results in client access failures. You must know how to troubleshoot space issues related to event log volumes.

- storage virtual machine (SVM) and cluster administrators can determine whether there is insufficient volume space by displaying information about volume and aggregate usage and configuration.
- If there is insufficient space in the volumes containing event logs, SVM and cluster administrators can resolve the space issues by either removing some of the event log files or by increasing the size of the volume.

> (i) If the aggregate that contains the event log volume is full, then the size of the aggregate must be increased before you can increase the size of the volume. Only a cluster administrator can increase the size of an aggregate.

- The destination path for the event log files can be changed to a directory on another volume by modifying the auditing configuration.

> (i) Data access is denied in the following cases:
>
> - If the destination directory is deleted.
> - If the file limit on a volume, which hosts the destination directory, reaches to its maximum level.

For more information about how to view information about volumes and increasing volume size, see the Logical storage management

For more information about how to view information about aggregates and managing aggregates, see Disks and aggregates management.

Troubleshoot space issues related to the staging volumes

If any of the volumes containing staging files for your storage virtual machine (SVM) runs out of space, auditing cannot write log records into staging files. This results in client access failures. To troubleshoot this issue, you need to determine whether any of the staging volumes used in the SVM are full by displaying information about volume usage.

If the volume containing the consolidated event log files has sufficient space but there are still client access failures due to insufficient space, then the staging volumes might be out of space. The SVM administrator must contact you to determine whether the staging volumes that contain staging files for the SVM have insufficient space. The auditing subsystem generates an EMS event if auditing events cannot be generated due to insufficient space in a staging volume. The following message is displayed: `No space left on device`. Only you can view information about staging volumes; SVM administrators cannot.

All staging volume names begin with `MDV_aud_` followed by the UUID of the aggregate containing that staging volume. The following example shows four system volumes on the admin SVM, which were automatically created when a file services auditing configuration was created for a data SVM in the cluster:

```
cluster1::> volume show -vserver cluster1
Vserver    Volume        Aggregate     State      Type       Size   Available
Used%
---------  ------------  ------------  ---------- ---- ---------- ----------
-----
cluster1   MDV_aud_1d0131843d4811e296fc123478563412
                         aggr0         online     RW         2GB     1.90GB
5%
cluster1   MDV_aud_8be27f813d7311e296fc123478563412
                         root_vs0      online     RW         2GB     1.90GB
5%
cluster1   MDV_aud_9dc4ad503d7311e296fc123478563412
                         aggr1         online     RW         2GB     1.90GB
5%
cluster1   MDV_aud_a4b887ac3d7311e296fc123478563412
                         aggr2         online     RW         2GB     1.90GB
5%
4 entries were displayed.
```

If there is insufficient space in the staging volumes, you can resolve the space issues by increasing the size of the volume.

ⓘ If the aggregate that contains the staging volume is full, then the size of the aggregate must be increased before you can increase the size of the volume. Only you can increase the size of an aggregate; SVM administrators cannot.

If one or more aggregates have an available space of less than 2 GB, the SVM audit creation fails. When the SVM audit creation fails, the staging volumes that were created are deleted.

Related information

ONTAP concepts Logical storage management Disks and aggregates management