ONTAP Auditing Schema Reference

Birendra Prasad Gupta
December 2020

Abstract

This document describes the events generated by the NetApp® ONTAP® NAS native auditing solution for NFS and SMB/CIFS. ONTAP auditing currently supports XML and EVTX format.

TABLE OF CONTENTS

LIST OF TABLES

Introduction

This document describes the various events and their contents that are generated by the NetApp ONTAP NAS native auditing solution for NFS and SMB/CIFS. ONTAP Auditing currently supports XML and EVTX format. The schema consists of the following sections:

- **Base section (described in section 1):** The event information in this section is common to all events, including information about the system that generated the event and details such as version of the template, event name, and so on. This section is tagged with `<system> </system>`.
- **Event data section (described in section 2 through section 10):** These sections are specific to the events and provide event-specific details. These events are tagged with `<EventData> </EventData>`.

1. Base Section

This section of the event schema contains event information that is common to all events. It is tagged with `<system> </system>`.

1.1. Provider Name

Name of the provider subsystem that provides (generates) the event. In this example, the name **NetApp-Security-Auditing** indicates the subsystem within ONTAP that provides these events.

1.2. GUID

GUID is a Globally Unique Identifier for the provider name mentioned above.

1.3. EventID

Event ID is an identification number to identify an event. These are standard event IDs defined by Microsoft. This can be used in conjunction with the Event name to identify a security event.

1.4. Event Name

Represents the exact event and thus provides additional detail for a particular Event ID. There are cases, where a single event ID is mapped to multiple event names.

For example, event ID 4656 (A Handle to an object was requested), there could be two possible values for the event names:

- Open object
- Create object

1.5. Version

Defines the version of the event template (Event Schema format) as defined by Microsoft. It consists of `<base_version_num>.<event_version_number>`.

Currently Base version is 101 and event `version_num` depends on the specific event. If we add new events or add new fields in a particular event, expect version to be bumped up for that specific event.

1.6. Source

Describes the source protocol for the event. ONTAP supports different access protocols; therefore, this fields describes which protocol generated this event.

Most common Values:

- SMB/CIFS
- NFSv3
- NFSv4

Currently ONTAP supports file-operations auditing only for these protocols. This could change if other protocols (such as HTTP, Cloud protocols, etc.) are supported in the future.

1.7. Level

Defines the severity level of the event. It is always 0.

1.8. opcode

Defines operations performed by various components that generated this event. It is currently not used and always zero.

1.9. Keywords

Classify events; it supports two values:

- Audit Success > 0x8020000000000000
- Audit Failure > 0x8010000000000000

1.10. Result

Defines the type of Audit Event. It is the same as the Keyword field above. It can have two values:

- For success Sacls > Audit Success
- For Failure Sacls > Audit Failure

  Note: Audit Failure here means that the operation was denied.

1.11. TimeCreated SystemTime

Provides the time when this event was generated in the system. It is the system time represented in `<YYYY-MM-DDThh:mm:ss.s)Z`, which provides date, time, and time zone information. A trailing `Z` means UTC time zone.

1.12. Channel

Defines the category this event belongs to. A channel is a sink that collects events. Consumers of the events can subscribe to one or more channels they are interested in.

Currently we support only one channel: Security.

1.13. Computer

Describes the Name of the system generating the events. It consists of `<cluster_name>/<SVM name>`.

1.14. Computer UUID

UUID identifier for the system generating the events. It consists of `<cluster_uuid>/<svm uuid>`.

2. Common Event Data Section

This section contains a set of fields common to all file system events, as described below. Most of the events contains these common fields and some event specific fields.

2.1. SubjectIP

Describes the IP address of the client that initiated the event. The format of the address depends on the IP version (IPv4/IPv6).

2.2. SubjectHostName

Contains the hostname of the client that initiated the event.

2.3. SubjectUnix

Describes the UNIX credentials of the user. The UNIX user is identified by:

- UID: UID of the UNIX user
- GID: Gid of the UNIX user
- Local: Indicates if the user is a local user configured in ONTAP system or a Domain user

2.4. SubjectUserSid

Indicates the user's Windows SID. User Mapping in ONTAP defines the mapping of Unix Users with Windows users and vice versa for multi-protocol access. The UNIX Name (and its UID/GID) and the corresponding SID is thus mapped by the user mapping facility in ONTAP systems.

2.5. SubjectUserisLocal

Describes whether the user is a locally configured user on ONTAP or a domain user

2.6. SubjectDomainName

Indicates the Domain Name to which the user belongs. In the case of a Local user, it contains SMB/CIFS server Name.

2.7. SubjectUserName

Provides the username of the user.

2.8. ObjectServer

This value defaults to Security.

2.9. ObjectType

Indicates the type of Object being accessed. For example, File for a file Object, Directory for Directory objects. Possible values for this field include:

- File
- Directory
- Symbolic Link
- Stream

  Note: The value "Unknown" is set if the object is not of any of the four types mentioned above.

2.10.HandleId

Uniquely identifies an object in the file system. It consists of:

```
<volume_identifier>;00;<file_identifier>;;<file_identifier_extended>
```

It can be used to corelate different events on the same object. This identifies only the object and is not associated with a session or a user. The field `file_identifier_extended` is just the extension of the file Identifier, it is not related to file extension in anyway.

2.11.ObjectName

Specifies the name of the object being accessed. It contains the full path of the object relative to the volume.

For example:

```
<data Name="ObjectName">(Vol1);/dir1/file.txt </data>
```

3. Event: file-ops

3.1. 4656: An Attempt Was Made to Open an Object

Generated when an object is opened or created. Accordingly, this event ID is mapped to two events:

- Open object
- Create object

3.1.1. Open Object

Generated when an existing object is opened. It contains all fields defined in section 2, "Common Event Data Section" and the following specific fields:

3.1.1.1. AccessList

List of rights that specifies requested or granted access to an object. It is represented in schema value format given in Table 1. This will contain one or more Schema value depending on the Access Mask.

3.1.1.2. Access Mask

Mask of list of rights that specifies requested or granted access to an object. The mask value in the event is a combination of access Mask represented in decimal format. For example, if access requested is Read Data, Write Data, and Append Data, the mask value is a logical or operation of corresponding mask values, 0x1 | 0x2 | 0x4 = 7.

3.1.1.3. DesiredAccess

The specific permissions requested on this object in textual form. A combination of the Access List, Access Mask, and Desired Access fields are provided in Table 1.

Table 1) Access list.

Access	Access Mask	Schema Value
Read Data or List Directory	0x1	%%4416
Write Data or Add File	0x2	%%4417
Append Data OR Add Subdirectory	0x4	%%4418

Access	Access Mask	Schema Value
Read Extended Attributes	0x8	%%4419
Write Extended Attributes	0x10	%%4420
Execute/Traverse	0x20	%%4421
Delete Child	0x40	%%4422
Read Attributes	0x80	%%4423
Write Attributes	0x100	%%4424
Delete	0x200	%%1537
Read ACL	0x2000	%%1538
Write ACL	0x4000	%%1539
Write Owner	0x8000	%%1540
Synchronize	0x10000	%%1541

For a detailed description of these accesses, see: Event 4656(S, F): A handle to an object was requested.

3.1.1.4. Attributes

Describes internal flags that were part of the SMB request. Indicates the intent of the SMB request. Contains one or combination of these values:

- **Set Attributes.** Attributes were specified as part of the request.
- **Create.** This is an attempt to create as well as open the object.
- **Fail if Exists.** The operation will fail if the object exists.
- **Open a Directory.** Open a directory.
- **Open a Nondirectory.** Open a nondirectory.

3.1.2. Create Object

Generated when a new object is created. It contains all common fields mentioned above in section 2, “Common Event Data Section” and the following specific fields:

3.1.2.1. Attributes

Describes internal flags that were part of the SMB request. Indicates the intent of the SMB request.

Contains one or combination of these values:

- **Set Attributes.** Attributes were specified as part of the request.
- **Streams.** Indicates the object being created is a stream.
- **Guarded.** If this attribute is set, create for an existing object would fail. Otherwise old object will be replaced. If the size attribute is set to zero in an unguarded create, then an existing object will be truncated

3.2. 4663: An Attempt Was Made to Access an Object

Indicates that an attempt to access a file system object was made. This event is mapped to the following operations identified in the Event Name field:

- Read object
- Write object
- Get object attributes

- Set object attributes
- Read directory

All the above events contain a set of common event data fields mentioned in section 2, “Common Event Data Section” and some of the specific fields for each event described below:

3.2.1. Read Object

Indicates that an attempt was made to read the contents of a file system object.

3.2.1.1. Read offset

Specifies the byte offset of the file from where the data must be read.

3.2.1.2. Read Count

Specifies the number of bytes must be read from the file.

3.2.2. Write Object

Indicates that an attempt was made to write some contents to a file system object.

3.2.2.1. Write Offset

Specifies the byte offset of the file at which the data must be written.

3.2.2.2. Write Count

Specifies the number of bytes must be written to the file.

3.2.3. Get Object Attributes

Indicates that an attempt was made to retrieve attributes from a file system object (GETATTR). It contains the following fields apart from the common fields mentioned in section 2, “Common Event Data Section.”

3.2.3.1. Information Requested

A detailed list of the information that the client has requested. It can contain one or more of the following:

- File type
- File size
- Available space
- Created time
- Last accessed time
- Last modified time
- Last backed up time
- UNIX mode
- UNIX owner
- UNIX group
- SMB/CIFS ACL
- NFSv4 ACL
- Basic attributes (also known as the DOS attributes)
- Version and state of antivirus
- Allocation size

- Delete on last close

3.2.4. Set Object Attributes

Indicates that an attempt was made to set attributes on a file system object (SETATTR). It contains the following field apart from the common fields mentioned in section 2, “Common Event Data Section.”

3.2.4.1. Information Set

A detailed list of the information that the client has requested. Contains the same list as in Get Object Attributes Event mentioned in section 3.2.3.1, “Information Requested.”

3.2.5. Read Directory

Indicates that an attempt was made to read the contents of a directory (READDIR). It contains the following field apart from the common fields mentioned in section 2, “Common Event Data Section.”

3.2.5.1. SearchPattern

The pattern specified by the client that will be used to determine whether objects in the directory are returned in the result set.

3.2.5.2. SearchFilter

Restricts the search to objects that match these attributes:

- Read Only
- Hidden
- System
- Volume ID
- Directory
- Archive

3.2.5.3. Information Requested

Same as section 3.2.3.1, “Information Requested.”

3.3. 4659: A Handle to an Object Was Requested with the Intent to Delete

Generated when an SMB client opens a file system object with delete intent (DOC bit set in `SMB_OPEN`).

All fields of this event are same as 4656 OPEN events as described in section 3.1.1, “Open Object.”

3.4. 4660: An Attempt Was Made to Delete a File System Object

Generated when a client tries to delete a file system object. Contains all common fields for event Data as described in section 2, “Common Event Data Section” and the following field:

3.4.1. Information Set

A detailed list of the information that the client has requested. This may contain one or more values from the list mentioned in section 3.2.3.1, “Information Requested.”

3.5. 4658: An Attempt Was Made to Close the Object

Generated when a client tries to close the object. The object could be a file system, kernel, or registry object, or a file system object on removable storage or a device. It contains all common fields for event data, as described in section 2, “Common Event Data Section.”

3.6. 4664: An Attempt Was Made to Create a Hardlink

Generated when a hard link was successfully created. It contains all common fields for event data as described in section 2, “Common Event Data Section” and the following fields:

3.6.1. FileName

Contains the name of the file for which the link is created.

3.6.2. LinkName

Describes the name of the link that was created for the object.

3.7. 9998: An Attempt Was Made to Unlink an Object

Generated when an object is unlinked. It contains all common fields for event Data as described in section 2, “Common Event Data Section” and the following fields:

3.7.1. DirHandleID

Contains the directory object handle value.

3.7.2. FileName

Describes the name of the file object that was unlinked.

3.8. 9999: An Attempt Was Made to Rename a File System Object

Generated when an attempt is made to rename a file system object. It contains the following fields:

3.8.1. SubjectIP

Describes the IP address of the client that initiated the event. The format of the address depends on the IP version (IPv4/IPv6).

3.8.2. SubjectHostName

Contains hostname of the client that initiated the event.

3.8.3. SubjectUnix

Describes the UNIX credentials of the user. The UNIX user is identified by:

- UID: UID of the UNIX user
- GID: Gid of the UNIX user
- Local: Indicates if the user is a local user configured in ONTAP or a domain user.

3.8.4. SubjectUserSid

Indicates the user’s Windows SID. User mapping in ONTAP defines mapping of UNIX users with Windows users and vice versa for multiprotocol access. Therefore, the UNIX name (and its UID/GID) and the corresponding SID are mapped by the user mapping facility in ONTAP.

3.8.5. SubjectUserisLocal

Describes whether the user is a locally configured user on ONTAP or a domain user.

3.8.6. SubjectDomainName

Indicates the domain name to which the user belongs. In the case of a local user, it contains the SMB/CIFS server name.

3.8.7. SubjectUserName

Provides the username of the user.

3.8.8. OldDirHandle

The HandleID of the source directory. HandleID uniquely identifies a file system object in a cluster.

3.8.9. NewDirHandle

The HandleID of the destination directory. HandleID uniquely identifies a file system object in a cluster.

3.8.10. OldPath

Contains the path, from the root of the volume, to the source of the file system object renamed. This might not be the same path that the client used to attempt the operation.

3.8.11. NewPath

Contains the path from the root of the file system to the target location of this object.

3.8.12. Attributes

A list of attributes that (if set) affects the rename operation. It can contain the following:

3.8.12.1. Replace Existing

If specified, the rename will attempt to overwrite the target location if it already exists.

3.9. 4670: Permissions on an Object Were Changed

Generated when the permissions for an object are changed. It contains the following specific fields along with Common Data Event fields described in section 2, “Common Event Data Section.”

3.9.1. OldSD

The old security descriptor the object had before permission was changed. This is a Unicode string represented in Security Descriptor Definition Language (SDDL) format.

3.9.2. NewSD

New Security Descriptor for the object after permission change event. Comparing the two SD, one can determine what changed for the object. This is a Unicode string represented in SDDL format. SDDL is a standard format defined by Microsoft for storing and transporting information in a Security Descriptor. Details of this format can be found in Microsoft documentation online.

4. Event: cifs-logon-logoff

4.1. 4624: An Account Was Successfully Logged On

Generated when a logon session is created on destination machine. This event comes during SESSION_SETUP_ANDX SMB request. It contains the following fields in its Event Data section:

4.1.1. IP Address

Describes the IP address of the client that initiates the logon session. The format of the address depends on the IP version (IPv4/IPv6).

4.1.2. IP Port

Specifies the client-side port from which the session is initiated. IP Port and IP address can be used together to identify the client session with a 4625 event (Log Off) to identify the duration of the session.

4.1.3. TargetUserSID

Specifies the SID of the user who initiated this logon attempt.

4.1.4. TargetUserName

Username of the user that initiated the logon attempt. This field along with SID can identify a user uniquely.

4.1.5. TargetIsUserLocal

Indicates if the user is a local user (locally configured in ONTAP) or a domain user. If this field is true, the Domain Name to which this user belongs to is indicated by TargetDomainName.

4.1.6. TargetDomainName

Contains the fully qualified domain name of the user that attempted logon.

4.1.7. AuthenticationPackageName

Specifies the Authentication method that is used to authenticate the TargetUser for the logon attempt. It can contain any of the following values:

- NTLM_V1
- NTLM_V2
- KRB5
- ANON

4.1.8. LogonType

Specifies the type of logon that was performed. Logon type can be used to monitor suspicious activities by users who are not authorized to use a particular logon type. Table 2 contains the list of possible values for this field.

Table 2) Possible values for logon type.

Logon Type	Description
2	Interactive
3	Network

Logon Type	Description
4	Batch
5	Service
7	Unlock
8	NetworkCleartext
9	NewCredentials
10	RemoteInteractive
11	CachedInteractive

Details on these options can be found at Microsoft Documentation of this event

Note: ONTAP supports only the Network (3) logon type.

4.2. 4634: An Account Was Logged Off

Generated when a logon session was terminated. It is generated due to LOGOFF_ANDX SMB request. Fields contained in this event is same as Logon event except AuthenticationPackageName. A Logon/logoff session for a given user can thus be identified by the pair of IP address and IP port. Logon/Logoff are important events to monitor access to secure Share or folder.

4.3. 4625: An Account Failed to Log On

Generated when a logon attempt was failed. It contains the following specific fields along with Common Data Event fields described in SDDL in section 2, “Common Event Data Section” and the following fields:

4.3.1. Status

Contains the status code information of the reason why logon failed.

4.3.2. FailureReasonString

Contains the textual explanation of Status field value. This following are the reasons for logon failure:

- The specified account's password has expired
- Unknown username or bad password
- Account currently disabled
- The specified user account has expired
- No such user account
- No logon servers available to service the logon
- Insufficient system resources
- The requested operation was unsuccessful
- Username is correct but the password is wrong
- User is currently locked out
- User tried to logon outside his day of week or time of day restrictions
- Workstation restriction
- Clocks between DC and other computer too far out of sync
- The user has not been granted the requested logon type at this machine
- Evidently a bug in Windows and not a risk
- Unknown error

4.3.3. FailureReason

Contains the failure reason error code.

5. Event: file-share

5.1. 5142: A CIFS Share Was Created

The file-share event Share Object Added is generated when a SMB/CIFS network share is added. It contains the following specific fields along with Common Data Event fields described in section 2, “Common Event Data Section” and the following fields:

5.1.1. ShareName

Specifies the name of the added share object.

5.1.2. SharePath

Specifies the full system (NTFS) path for the added share object.

5.1.3. ShareProperties

Provides the properties of the share.

5.2. 5143: A CIFS Share Was Modified

The file-share event Share Object Modified is generated when a SMB/CIFS network share is modified. It contains the following specific fields along with Common Data Event fields described in section 2, “Common Event Data Section” and the following fields:

5.2.1. ShareName

Specifies the name of the modified share object.

5.2.2. OldSharePath

Provides the full system (NTFS) old path for the added share object.

5.2.3. NewSharePath

Provides the full system (NTFS) path for the added share object that is modified.

5.2.4. OldShareProperties

Provides the properties before any modifications for the share.

5.2.5. NewShareProperties

Provides the properties that were added/modified for the share.

5.2.6. OldMaxUsers

Specifies the old hexadecimal value of the Limit the Number of Simultaneous Users To field.

5.2.7. NewMaxUsers

Specifies the new hexadecimal value of the Limit the Number of Simultaneous Users To field.

5.2.8. OldSD

This filed contains the old SDDL value for network share security descriptor.

5.2.9. NewSD

This filed contains the new SDDL value for network share security descriptor.

5.3. 5144: A CIFS Share Was Deleted

The file-share event Share Object Deleted is generated when a SMB/CIFS network share is deleted. It contains the following specific fields along with Common Data Event fields described in section 2, “Common Event Data Section” and the following fields:

5.3.1. ShareName

Specifies the name of the removed share object.

5.3.2. SharePath

Specifies the full system (NTFS) path for the removed share object.

5.3.3. ShareProperties

Provides the properties of the share.

5.3.4. SD

Specifies the SDDL value for network share security descriptor.

6. Event: user-account

6.1. 4720: A Local User Was Created

This user-account event is generated when a local SMB/CIFS or UNIX user is created. Contains all common fields for event Data as described in section 2, “Common Event Data Section” and the following fields:

6.1.1. TargetSID

Specifies the SID of the created SMB/CIFS or UNIX user.

6.1.2. TargetUserName

Specifies the name of the SMB/CIFS or UNIX user account that was created.

6.1.3. TargetType

Indicates the type (SMB/CIFS or NFS) of user.

6.1.4. TargetDomainName

Contains the domain name of created SMB/CIFS or UNIX user. In case of Local user, it contains SMB/CIFS server Name.

6.1.5. PasswordLastSet

Specifies the last time the account's password was modified.

6.1.6. DisplayName

Specifies the Display name of the of the new SMB/CIFS or UNIX user.

6.1.7. AccountExpires

Indicates the date when the account expires. This parameter contains the value of accountExpires attribute of new user object.

6.1.8. PrimaryGroupId

Specifies the Relative Identifier (RID) of user's object primary group.

6.1.9. UserAccountControl

This field shows the list of changes in userAccountControl attribute.

6.1.10. SidHistory

Contains previous SIDs used for the object if the object was moved from another domain. Whenever an object is moved from one domain to another, a new SID is created and becomes the objectSID. The previous SID is added to the sIDHistory property.

6.1.11. PrivilegeList

Specifies the list of user privileges that were used during the operation, for example, SeBackupPrivilege. This parameter might not be captured in the event, and in that case appears as "~".

6.2. 4722: A Local User Was Enabled

This user-account event is generated when a local SMB/CIFS user is enabled. Contains all common fields for event Data as described in section 2, "Common Event Data Section" and the following fields:

6.2.1. TargetSID

Specifies the SID of the SMB/CIFS user that was enabled.

6.2.2. TargetUserName

Specifies the name of the user that was enabled.

6.2.3. TargetType

Indicates the type of user.

6.2.4. TargetDomainName

Contains domain name of the user that was enabled. In case of local user, it contains SMB/CIFS server name.

6.3. 4725: A Local User Was Disabled

This user account event is generated when a local SMB/CIFS user is disabled. Contains all common fields for event data as described in section 2, "Common Event Data Section" and the following fields:

6.3.1. TargetSID

Specifies the SID of the SMB/CIFS user that was disabled.

6.3.2. TargetUserName

Specifies the name of the user that was disabled.

6.3.3. TargetType

Indicates the type of user.

6.3.4. TargetDomainName

Contains domain name of the user that was disabled. In case of local user, it contains SMB/CIFS server name.

6.4. 4726: A Local User Was Deleted

This user account event is generated when a local SMB/CIFS or UNIX user is deleted. Contains all common fields for event data as described in section 2, “Common Event Data Section” and the following fields:

6.4.1. TargetSID

Specifies the SID of the SMB/CIFS or UNIX user that was deleted.

6.4.2. TargetUserName

Specifies the name of the user that was deleted.

6.4.3. TargetType

Indicates the type (SMB/CIFS/NFS) of user.

6.4.4. TargetDomainName

Contains domain name of the user that was deleted. In case of local user, it contains SMB/CIFS server name.

6.5. 4724: A Local User Password Reset

This user account event is generated when a local SMB/CIFS user password reset. Contains all common fields for event data, as described in section 2, “Common Event Data Section” and the following fields:

6.5.1. TargetSID

Specifies the SID of the user for which password reset was requested.

6.5.2. TargetUserName

Specifies the name of the user for which password reset was requested.

6.5.3. TargetType

Indicates the type of user.

6.5.4. TargetDomainName

Contains the domain name. In the case of a local user, it contains SMB/CIFS server name.

6.6. 4738: A Local User Is Changed

The user account event is generated when a local SMB/CIFS or UNIX user is changed. Contains all common fields for event data, as described in section 2, “Common Event Data Section” and the following fields:

6.6.1. TargetSID

Specifies the SID of the SMB/CIFS or UNIX user that was changed.

6.6.2. TargetUserName

Specifies the name of the SMB/CIFS or UNIX user that was changed.

6.6.3. TargetType

Indicates the type (SMB/CIFS or NFS) of the user.

6.6.4. TargetDomainName

Contains the domain name of the user that was changed. In the case of a local user, it contains SMB/CIFS server name.

6.7. 4781: A Local User Is Renamed

This user account event is generated when a local SMB/CIFS user is renamed. Contains all common fields for event data, as described in section 2, “Common Event Data Section” and the following fields:

6.7.1. TargetSID

Specifies the SID of the SMB/CIFS user that was renamed.

6.7.2. TargetUserName

Specifies the name of the SMB/CIFS user that was renamed.

6.7.3. TargetType

Indicates the type of user.

6.7.4. TargetDomainName

Contains domain name of the user that was renamed. In case of local user, it contains SMB/CIFS server name.

6.7.5. OldTargetUserName

Contains the old name of target user.

6.7.6. NewTargetUserName

Contains the new name of target user.

7. Event: audit-policy-change

7.1. 4719: Audit Policy Disabled/Enabled

The audit policy change event Audit Disabled/Audit Enabled is generated when audit policy is enabled or disabled. Contains all common fields for event data, as described in section 2, “Common Event Data Section” and the fields also described in this section.

7.2. 4719: Audit Policy Is Changed

The audit policy change event Audit Policy Changed is generated when the audit policy is changed. Contains all common fields for event data, as described in section 2, “Common Event Data Section” and the following fields:

7.2.1. OldDestinationPath

Specifies the old destination path of the audit configuration.

7.2.2. NewDestinationPath

Specifies the new destination path of the audit configuration.

7.2.3. OldRotateLimit

Specifies the old rotate changes of the audit.

7.2.4. NewRotateLimit

Specifies the newer rotate changes of the audit.

7.2.5. OldLogFormat

Specifies the log format of the log file if changed.

7.2.6. NewLogFormat

Specifies the newer log format of the log file if changed.

7.2.7. AuditGuarantee

Specifies the Audit Guarantee is Unchanged or Changed.

7.2.8. OldSD

Contains the old SDDL value for the object.

7.2.9. NewSD

Contains the new SDDL value for the object.

7.3. 4907: Audit Settings on the Object Were Changed

The Auditing Settings Changed event is generated when an audit setting on an object is changed. Contains all common fields for event data, as described in section 2, “Common Event Data Section” and the following fields:

7.3.1. ObjectServer

This field has Security value for this event.

7.3.2. ObjectType

The type of an object that was accessed during the operation.

7.3.3. HandleID

A hexadecimal value of a handle to Object Name. This field can help you correlate this event with other events that might contain the same Handle ID.

7.3.4. ObjectName

Describes the full path and name of the object for which the SACL was modified.

7.3.5. OldSD

Contains the old SDDL value for the object.

7.3.6. NewSD

Contains the new SDDL value for the object.

7.4. 4913: Central Access Policy on the Object Was Changed

This Central Access Policy Changed event is generated when a Central Access Policy on a file system object is changed. Contains all common fields for event data, as described in in section 2, “Common Event Data Section” and the following fields:

7.4.1. OldSD

Contains the Original Security Descriptor, the SDDL value for the old Central Policy ID.

7.4.2. NewSD

Contains the New Security Descriptor, the SDDL value for the new Central Policy ID.

8. Event: authorization-policy-change

8.1. 4704: Authorization Policy is Assigned

The authorization policy change event User Right Assigned is generated whenever the authorization rights are granted for a SMB/CIFS user and group. Contains all common fields for event data, as described in in section 2, “Common Event Data Section” and the fields also described in this section.

8.1.1. TargetType

Specifies the type of the target user.

8.1.2. PrivilegeList

Specifies the list of user privileges that were used during the operation; for example, SeBackupPrivilege. This parameter might not be captured in the event; in that case, it appears as “~”.

The parameter PrivilegeList options supported by ONTAP are listed in Table 3.

Table 3) PrivilegeList parameter options.

Privilege Name	Description
`SeTcbPrivilege`	Act as part of the operating system
`SeBackupPrivilege`	Back up files and directories, overriding any ACLs
`SeRestorePrivilege`	Restore files and directories, overriding any ACLs
`SeTakeOwnershipPrivilege`	Take ownership of files or other objects
`SeSecurityPrivilege`	This includes viewing, dumping, and clearing the security log.
`SeChangeNotifyPrivilege`	Bypass traverse checking Users with this privilege are not required to have traverse (x) permissions to traverse folders, symlinks, or junctions.

8.1.3. TargetUserOrGroupName

Contains the user/group name where the privileges were assigned.

8.1.4. TargetUserOrGroupDomainName

Contains the Domain name to which the user/group belongs to.

8.1.5. TargetUserOrGroupSid

Contains the SID of User/Group for which the privileges were assigned.

8.2. 4705: Authorization Policy is Removed

The authorization policy change event User Right Removed is generated whenever the authorization rights are granted for a SMB/CIFS user and group. Contains all common fields for event data, as described in section 2, “Common Event Data Section” and the following fields:

8.2.1. TargetType

Specifies the type of the target user.

8.2.2. PrivilegeList

Specifies the list of user privileges that were used during the operation; for example, SeBackupPrivilege. This parameter might not be captured in the event, and in that case appears as “~”.

The parameter PrivilegeList options supported by ONTAP are described in the section 8.1.2, “PrivilegeList.”

8.2.3. TargetUserOrGroupName

Contains the user/group name where the privileges were removed.

8.2.4. TargetUserOrGroupDomainName

Contains the Domain name to which the user/group belongs to.

8.2.5. TargetUserOrGroupSid

Contains the SID of User/Group for which the privileges were removed.

9. Event: security-group

9.1. 4731: Local Security Group Created

The security group event is generated when a local SMB/CIFS or UNIX group is created. It contains all common fields for event data, as described in section 2, “Common Event Data Section” and the following fields:

9.1.1. TargetSID

Specifies the SID of the created group.

9.1.2. TargetUserName

Specifies the name of the group that was created.

9.1.3. TargetType

Indicates the type (SMB/CIFS or NFS) of group.

9.1.4. TargetDomainName

Contains the domain or computer name of the created group.

9.1.5. SidHistory

Contains previous SIDs used for the object if the object was moved from another domain. Whenever an object is moved from one domain to another, a new SID is created and becomes the objectSID. The previous SID is added to the SIDHistory property.

9.1.6. PrivilegeList

Specifies the list of user privileges that were used during the operation, for example, SeBackupPrivilege. This parameter might not be captured in the event, and in that case appears as “~”.

The parameter ‘PrivilegeList’ options supported by ONTAP are described in the section 8.1.2, “PrivilegeList.”.

9.2. 4732: Local User Added to Security Group

The security group event is generated when a member is added to SMB/CIFS or UNIX group. Contains all common fields for event data, as described in section 2, “Common Event Data Section” and the following fields:

9.2.1. TargetSID

Specifies the SID of the group to which the new member was added.

9.2.2. TargetUserName

Specifies the name of the group to which the new member was added.

9.2.3. TargetType

Indicates the type (SMB/CIFS or NFS) of the group.

9.2.4. TargetDomainName

Contains domain or computer name of the group to which the new member was added.

9.2.5. PrivilegeList

Specifies the list of user privileges that were used during the operation, for example, SeBackupPrivilege. This parameter might not be captured in the event, and in that case appears as “~”.

The parameter PrivilegeList options supported by ONTAP are described in the section 8.1.2, “PrivilegeList.”

9.2.6. MemberName

Specifies the name of the user that is added to the group.

9.2.7. MemberSid

Contains the info about the SID of the user that was added to the group.

9.3. 4733: Local User Removed from Security Group

The security group event is generated when a member is removed from the SMB/CIFS or UNIX group. Contains all common fields for event data, as described in section 2, “Common Event Data Section” and the following fields:

9.3.1. TargetSID

Specifies the SID of the SMB/CIFS or UNIX user that was removed from group.

9.3.2. TargetUserName

Specifies the name of the group from which the member was removed.

9.3.3. TargetType

Indicates the type (SMB/CIFS or NFS) of group.

9.3.4. TargetDomainName

Contains the domain or computer name of the group from which the member was removed.

9.3.5. PrivilegeList

Specifies the list of user privileges that were used during the operation, for example, SeBackupPrivilege. This parameter might not be captured in the event, and in that case appears as “~”.

The parameter PrivilegeList options supported by ONTAP are described in the section 8.1.2, “PrivilegeList.”

9.3.6. MemberName

Specifies the name of the user that was removed from the group.

9.3.7. MemberSid

Contains the info about the SID of the user that was removed from the group.

9.4. 4734: Local Security Group Removed

The security-group event is generated when a local SMB/CIFS or UNIX group is removed. This event contains the following fields:

9.4.1. TargetSID

Specifies the SID of the deleted group.

9.4.2. TargetUserName

Specifies the name of the group that was deleted.

9.4.3. TargetType

Indicates the type (SMB/CIFS/NFS) of group.

9.4.4. TargetDomainName

Contains the domain or computer name of the deleted group.

9.4.5. SidHistory

Contains previous SIDs used for the object if the object was moved from another domain. Whenever an object is moved from one domain to another, a new SID is created and becomes the objectSID. The previous SID is added to the sIDHistory property.

9.4.6. PrivilegeList

Specifies the list of user privileges that were used during the operation, for example, SeBackupPrivilege. This parameter might not be captured in the event, and in that case appears as “~”.

The parameter PrivilegeList options supported by ONTAP are described in the section 8.1.2, “PrivilegeList.”

9.5. 4735: Local Security Group Changed

The security group event is generated when a local SMB/CIFS or UNIX group was changed. Contains all common fields for event data, as described in section 2, “Common Event Data Section” and the following fields:

9.5.1. TargetSID

Specifies the SID of the changed group.

9.5.2. TargetUserName

Specifies the name of the group that was changed.

9.5.3. TargetType

Indicates the type of group.

9.5.4. TargetDomainName

Contains domain or computer name of the changed group.

9.5.5. GidHistory

Contains previous GIDs used for the object. The previous GIDs were added to the gIDHistory property.

9.5.6. PrivilegeList

Specifies the list of user privileges that were used during the operation; for example, SeBackupPrivilege. This parameter might not be captured in the event, and in that case appears as “~”.

The parameter PrivilegeList options supported by ONTAP are described in the section 8.1.2, “PrivilegeList.”

10.Event: cap-staging

10.1.4818: Central Access Policy Staging

Central access policies (CAP) for files enable organizations to centrally deploy and manage authorization policies that include conditional expressions using user groups, user claims, device claims, and resource properties.

For example, for accessing high business impact data, a user needs to be a full-time employee and only have access to the data from a managed device. Central access policies are defined in Active Directory and distributed to file servers via the GPO mechanism.

This Central Access Policy Staging event contains all common fields for event data, as described in section 2, “Common Event Data Section” and the following fields:

10.1.1. ObjectServer

This field has security value for this event.

10.1.2. ObjectType

The type of an object that was accessed during the operation. Always File for this event.

10.1.3. HandleID

A hexadecimal value of a handle to Object Name. This field can help you correlate this event with other events that might contain the same Handle ID.

10.1.4. ObjectName

Describes the name of the object that was accessed.

10.1.5. AccessReason

This field has the list of access check results for Current Access Policy.

11.Where to Find Additional Information

- ONTAP 9 SMB/CIFS and NFS Auditing and Security Tracing Guide
  Auditing NAS events on SVMs
- Clustered Data ONTAP CIFS Auditing Quick Start Guide (Data ONTAP 8.x)
- Native Auditing Event Schema for ONTAP 8.2.1

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

NetApp