Eventos SMB que se pueden auditar

ONTAP 9

NetApp
February 12, 2026

Tabla de contenidos

Eventos SMB que se pueden auditar

Obtenga más información sobre los eventos de bloque de mensajes del servidor que ONTAP puede auditar para interpretar los resultados

ONTAP puede auditar determinados eventos SMB, incluidos determinados eventos de acceso a archivos y carpetas, determinados eventos de inicio y cierre de sesión y eventos de configuración de directivas de acceso central. Saber qué eventos de acceso se pueden auditar es útil cuando se interpretan los resultados de los registros de eventos.

Se pueden auditar los siguientes eventos SMB adicionales:

ID DE EVENTO (EVT/EVTX)	Evento	Descripción	Categoría
4670	Se han cambiado los permisos de objeto	ACCESO A OBJETOS: Se han cambiado los permisos.	Acceso a archivos
4907	Se ha cambiado la configuración de auditoría de objetos	ACCESO A OBJETOS: Se ha cambiado la configuración de auditoría.	Acceso a archivos
4913	Se ha cambiado la política de acceso central de objetos	ACCESO A OBJETOS: SE HA CAMBIADO LA TAPA.	Acceso a archivos

Los siguientes eventos del bloque de mensajes del servidor pueden auditarse en ONTAP 9.0 y versiones posteriores:

ID DE EVENTO (EVT/EVTX)	Evento	Descripción	Categoría
540/4624	Una cuenta se ha conectado correctamente	INICIO de SESIÓN/CIERRE DE SESIÓN: Inicio de sesión en la red (SMB).	Inicio de sesión y cierre sesión
529/4625	No se pudo iniciar sesión en una cuenta	INICIO de SESIÓN/CIERRE DE SESIÓN: Nombre de usuario desconocido o contraseña incorrecta.	Inicio de sesión y cierre sesión
530/4625	No se pudo iniciar sesión en una cuenta	INICIO de SESIÓN/CIERRE DE SESIÓN: Restricción del tiempo de inicio de sesión de la cuenta.	Inicio de sesión y cierre sesión

531/4625	No se pudo iniciar sesión en una cuenta	INICIO de SESIÓN/CIERRE DE SESIÓN: Cuenta desactivada actualmente.	Inicio de sesión y cierre sesión
532/4625	No se pudo iniciar sesión en una cuenta	INICIO de SESIÓN/CIERRE DE SESIÓN: La cuenta de usuario ha caducado.	Inicio de sesión y cierre sesión
533/4625	No se pudo iniciar sesión en una cuenta	INICIO de SESIÓN/CIERRE DE SESIÓN: El usuario no puede iniciar sesión en este equipo.	Inicio de sesión y cierre sesión
534/4625	No se pudo iniciar sesión en una cuenta	INICIO de SESIÓN/CIERRE DE SESIÓN: El usuario no ha concedido el tipo de inicio de sesión aquí.	Inicio de sesión y cierre sesión
535/4625	No se pudo iniciar sesión en una cuenta	INICIO de SESIÓN/CIERRE DE SESIÓN: La contraseña del usuario ha caducado.	Inicio de sesión y cierre sesión
537/4625	No se pudo iniciar sesión en una cuenta	INICIO de SESIÓN/CIERRE DE SESIÓN: Error de inicio de sesión por motivos distintos a los anteriores.	Inicio de sesión y cierre sesión
539/4625	No se pudo iniciar sesión en una cuenta	INICIO de SESIÓN/CIERRE DE SESIÓN: Cuenta bloqueada.	Inicio de sesión y cierre sesión
538/4634	Se ha cerrado una cuenta	INICIO de SESIÓN/CIERRE DE SESIÓN: Cierre de sesión del usuario local o de la red.	Inicio de sesión y cierre sesión
560/4656	Abra objeto/Crear objeto	ACCESO A OBJETOS: Objeto (archivo o directorio) abierto.	Acceso a archivos
563/4659	Abrir objeto con la intención de eliminar	ACCESO A OBJETOS: Se ha solicitado un controlador a un objeto (archivo o directorio) con el propósito de eliminar.	Acceso a archivos
564/4660	Eliminar objeto	ACCESO A OBJETOS: Eliminar objeto (archivo o directorio). ONTAP genera este evento cuando un cliente de Windows intenta eliminar el objeto (archivo o directorio).	Acceso a archivos

567/4663	Leer objeto/escribir objeto/obtener atributos de objeto/establecer atributos de objeto	ACCESO A OBJETOS: Intento de acceso al objeto (lectura, escritura, Get Attribute, set attribute). **Nota:** para este evento, ONTAP sólo audita la primera operación de lectura y escritura de SMB (éxito o fallo) en un objeto. Esto impide que ONTAP cree demasiadas entradas de registro cuando un único cliente abre un objeto y realiza muchas operaciones de lectura o escritura sucesivas al mismo objeto.	Acceso a archivos
NA/4664 PULG	Vínculo rígido	ACCESO A OBJETOS: Se ha intentado crear un vínculo rígido.	Acceso a archivos
NA/4818 PULG	La directiva de acceso central propuesta no concede los mismos permisos de acceso que la directiva de acceso central actual	ACCESO A OBJETOS: Configuración de la directiva de acceso central.	Acceso a archivos
ID Evento Data ONTAP NA/NA 9999	Cambiar nombre de objeto	ACCESO A OBJETOS: Objeto cambiado de nombre. Este es un evento de ONTAP. Actualmente no es compatible con Windows como un único evento.	Acceso a archivos
ID Evento Data ONTAP NA/NA 9998	Desvincular objeto	ACCESO A OBJETOS: Objeto no vinculado. Este es un evento de ONTAP. Actualmente no es compatible con Windows como un único evento.	Acceso a archivos

Información adicional sobre el evento 4656

La `HandleID` etiqueta del `XML` evento de auditoría contiene el manejador del objeto (archivo o directorio) al que se accede. La `HandleID` etiqueta para el evento EVTX 4656 contiene información diferente dependiendo de si el evento abierto es para crear un nuevo objeto o para abrir un objeto existente:

- Si el evento abierto es una solicitud abierta para crear un nuevo objeto (archivo o directorio), la `HandleID` etiqueta del evento XML de auditoría muestra un valor vacío `HandleID` (por ejemplo `<Data Name="HandleID">00000000000000;00;00000000;00000000</Data>`:).

  El `HandleID` está vacío porque la solicitud OPEN (para crear un nuevo objeto) se audita antes de que se cree el objeto real y antes de que exista un manejador. Los eventos auditados posteriores para el mismo objeto tienen el manejador de objeto correcto en la `HandleID` etiqueta.

- Si el evento abierto es una solicitud abierta para abrir un objeto existente, el evento de auditoría tendrá el

manejador asignado de ese objeto en la `HandleID` etiqueta (por ejemplo `<Data Name="HandleID">00000000000401;00;000000ea;00123ed4</Data>`:).

Determine la ruta de acceso completa al objeto auditado ONTAP

La ruta de objeto impresa en la `<ObjectName>` etiqueta de un registro de auditoría contiene el nombre del volumen (en paréntesis) y la ruta relativa de la raíz del volumen que lo contiene. Si desea determinar la ruta completa del objeto auditado, incluida la ruta de unión, hay algunos pasos que debe seguir.

Pasos

1. Para determinar el nombre del volumen y la ruta relativa al objeto auditado, observe la `<ObjectName>` etiqueta en el evento de auditoría.

   En este ejemplo, el nombre del volumen es «ata1» y la ruta relativa al archivo es `/dir1/file.txt`:

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

2. Con el nombre del volumen determinado en el paso anterior, determine cuál es la ruta de unión para el volumen que contiene el objeto auditado:

   En este ejemplo, el nombre del volumen es «ata1» y la ruta de unión para el volumen que contiene el objeto auditado es `/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. Para determinar la ruta completa al objeto auditado, anexa `<ObjectName>` la ruta relativa que se encuentra en la etiqueta a la ruta de unión del volumen.

   En este ejemplo, la ruta de unión para el volumen:

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

Obtenga más información sobre la auditoría ONTAP de enlaces simbólicos y enlaces duros

Hay ciertas consideraciones que usted debe tener en cuenta al auditar enlaces simbólicos y vínculos duros.

Un registro de auditoría contiene información sobre el objeto que se está auditando, incluida la ruta de acceso

al objeto auditado, que se identifica en la `ObjectName` etiqueta. Debe tener en cuenta cómo se registran en la `ObjectName` etiqueta las rutas de los enlaces simbólicos y los enlaces físicos.

Enlaces simbólicos

Un symlink es un archivo con un inodo independiente que contiene un puntero a la ubicación de un objeto de destino, conocido como el destino. Al acceder a un objeto mediante un enlace simbólico, ONTAP interpreta automáticamente el enlace simbólico y sigue la ruta real independiente del protocolo canónico al objeto de destino del volumen.

En la siguiente salida de ejemplo, hay dos enlaces simbólicos, ambos apuntando a un archivo llamado `target.txt`. Uno de los enlaces simbólicos es un enlace simbólico relativo y uno es un enlace absoluto. Si se audita cualquiera de los enlaces simbólicos, la `ObjectName` etiqueta del evento de auditoría contiene la ruta de acceso al archivo `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
```

Vínculos duros

Un vínculo rígido es una entrada de directorio que asocia un nombre a un archivo existente en un sistema de archivos. El enlace rígido apunta a la ubicación del inodo del archivo original. De forma similar a cómo ONTAP interpreta los enlaces simbólicos, ONTAP interpreta el vínculo duro y sigue la ruta canónica real al objeto de destino del volumen. Cuando se audita el acceso a un objeto de enlace físico, el evento de auditoría registra esta ruta canónica absoluta en la `ObjectName` etiqueta en lugar de la ruta de enlace duro.

Obtenga más información sobre la auditoría ONTAP de flujos de datos NTFS alternativos

Hay ciertas consideraciones que debe tener en cuenta al auditar archivos con flujos de datos alternativos NTFS.

La ubicación de un objeto que se va a auditar se registra en un registro de evento mediante dos etiquetas, la `ObjectName` etiqueta (la ruta) y la `HandleID` etiqueta (el identificador). Para identificar correctamente qué solicitudes de flujo se están registrando, debe tener en cuenta qué registros de ONTAP hay en estos campos para flujos de datos alternativos NTFS:

- ID DE EVTX: 4656 eventos (abrir y crear eventos de auditoría)
  - La ruta del flujo de datos alternativo se registra en la `ObjectName` etiqueta.
  - El manejador del flujo de datos alternativo se registra en la `HandleID` etiqueta.
- ID DE EVTX: 4663 eventos (el resto de eventos de auditoría, como leído, Write, getattr, etc.)
  - La ruta del archivo base, no la corriente de datos alternativa, se registra en la `ObjectName` etiqueta.

- El manejador del flujo de datos alternativo se registra en la `HandleID` etiqueta.

Ejemplo

El siguiente ejemplo ilustra cómo identificar eventos de EVTX ID: 4663 para flujos de datos alternativos usando la `HandleID` etiqueta. Aunque la `ObjectName` etiqueta (ruta de acceso) registrada en el evento de auditoría de lectura sea la ruta de acceso del archivo base, la `HandleID` etiqueta se puede utilizar para identificar el evento como un registro de auditoría para el flujo de datos alternativo.

Los nombres de archivo de flujo toman el formato `base_file_name:stream_name`. En este ejemplo, el `dir1` directorio contiene un archivo base con un flujo de datos alternativo que tiene las siguientes rutas:

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

El resultado del ejemplo de evento siguiente se truncará como se indica; la salida no muestra todas las etiquetas de salida disponibles para los eventos.

Para un EVTX ID 4656 (evento de auditoría abierto), la salida del registro de auditoría para el flujo de datos alternativo registra el nombre del flujo de datos alternativo en la `ObjectName` etiqueta:

```
- <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>
```

Para un EVTX ID 4663 (evento de auditoría de lectura), la salida del registro de auditoría para el mismo flujo de datos alternativo registra el nombre del archivo base en la `ObjectName` etiqueta; sin embargo, el identificador de la `HandleID` etiqueta es el identificador del flujo de datos alternativo y se puede utilizar para correlacionar este evento con el flujo de datos alternativo:

```
- <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>
```