



# Eventos SMB que podem ser auditados

ONTAP 9

NetApp  
January 17, 2025

# Índice

- Eventos SMB que podem ser auditados ..... 1
  - Visão geral de eventos SMB que podem ser auditados ..... 1
  - Determine qual é o caminho completo para o objeto auditado ..... 3
  - Considerações ao auditar links simbólicos e links duros ..... 4
  - Considerações ao auditar fluxos de dados NTFS alternativos ..... 5

# Eventos SMB que podem ser auditados

## Visão geral de eventos SMB que podem ser auditados

O ONTAP pode auditar determinados eventos SMB, incluindo determinados eventos de acesso a arquivos e pastas, determinados eventos de logon e logoff e eventos de preparação de políticas de acesso central. Saber quais eventos de acesso podem ser auditados é útil ao interpretar os resultados dos logs de eventos.

Os seguintes eventos SMB adicionais podem ser auditados no ONTAP 9.2 e posteriores:

ID DO EVENTO (EVT/EVTX)	Evento	Descrição	Categoria
4670	As permissões do objeto foram alteradas	ACESSO A OBJETO: Permissões alteradas.	Acesso a ficheiros
4907	As definições de auditoria de objetos foram alteradas	ACESSO A OBJETO: Definições de auditoria alteradas.	Acesso a ficheiros
4913	A Política de Acesso Central Objeto foi alterada	ACESSO A OBJETO: CAP ALTERADO.	Acesso a ficheiros

Os seguintes eventos SMB podem ser auditados no ONTAP 9.0 e posteriores:

ID DO EVENTO (EVT/EVTX)	Evento	Descrição	Categoria
540/4624	Uma conta foi iniciada com êxito	Logon/LOGOFF: Logon em rede (SMB).	Início de sessão e fim de sessão
529/4625	Não foi possível iniciar sessão numa conta	Logon/LOGOFF: Nome de usuário desconhecido ou senha ruim.	Início de sessão e fim de sessão
530/4625	Não foi possível iniciar sessão numa conta	Logon/LOGOFF: Restrição de tempo de logon da conta.	Início de sessão e fim de sessão
531/4625	Não foi possível iniciar sessão numa conta	Logon/LOGOFF: Conta atualmente desativada.	Início de sessão e fim de sessão
532/4625	Não foi possível iniciar sessão numa conta	Logon/LOGOFF: A conta de usuário expirou.	Início de sessão e fim de sessão
533/4625	Não foi possível iniciar sessão numa conta	Logon/LOGOFF: O usuário não pode fazer logon neste computador.	Início de sessão e fim de sessão

534/4625	Não foi possível iniciar sessão numa conta	Logon/LOGOFF: O usuário não recebeu o tipo de logon aqui.	Início de sessão e fim de sessão
535/4625	Não foi possível iniciar sessão numa conta	Logon/LOGOFF: A senha do usuário expirou.	Início de sessão e fim de sessão
537/4625	Não foi possível iniciar sessão numa conta	Logon/LOGOFF: O logon falhou por motivos diferentes dos acima.	Início de sessão e fim de sessão
539/4625	Não foi possível iniciar sessão numa conta	Logon/LOGOFF: Conta bloqueada.	Início de sessão e fim de sessão
538/4634	Uma conta foi encerrada	Logon/LOGOFF: LOGOFF de usuário local ou de rede.	Início de sessão e fim de sessão
560/4656	Abrir Objeto/criar Objeto	ACESSO A OBJETO: Objeto (arquivo ou diretório) aberto.	Acesso a ficheiros
563/4659	Abra Objeto com a intenção de Excluir	ACESSO A OBJETO: Um identificador para um objeto (arquivo ou diretório) foi solicitado com o intent to Delete.	Acesso a ficheiros
564/4660	Eliminar Objeto	ACESSO A OBJETO: Excluir Objeto (arquivo ou diretório). O ONTAP gera esse evento quando um cliente Windows tenta excluir o objeto (arquivo ou diretório).	Acesso a ficheiros
567/4663	Ler Objeto/escrever Objeto/obter atributos Objeto/Definir atributos Objeto	ACESSO A OBJETO: Tentativa de acesso a objeto (ler, escrever, obter atributo, definir atributo).  <b>Observação:</b> para este evento, o ONTAP audita apenas a primeira operação de leitura e gravação SMB (sucesso ou falha) em um objeto. Isso impede que o ONTAP crie entradas de log excessivas quando um único cliente abre um objeto e executa muitas operações de leitura ou gravação sucessivas no mesmo objeto.	Acesso a ficheiros
NA/4664	Link físico	ACESSO A OBJETOS: Foi feita uma tentativa de criar um link físico.	Acesso a ficheiros

NA/4818	A política de acesso central proposta não concede as mesmas permissões de acesso que a política de acesso central atual	ACESSO A OBJETOS: Central Access Policy Staging.	Acesso a ficheiros
ID do evento Data ONTAP NA/na 9999	Mudar o nome do objeto	ACESSO A OBJETO: Objeto renomeado. Este é um evento da ONTAP. Atualmente, não é suportado pelo Windows como um único evento.	Acesso a ficheiros
ID do evento Data ONTAP NA/na 9998	Desvincular Objeto	ACESSO A OBJETO: Objeto não vinculado. Este é um evento da ONTAP. Atualmente, não é suportado pelo Windows como um único evento.	Acesso a ficheiros

## Informações adicionais sobre o evento 4656

A `HandleID` tag no evento de auditoria XML contém o identificador do objeto (arquivo ou diretório) acessado. A `HandleID` tag para o evento EVT\_X 4656 contém informações diferentes, dependendo se o evento aberto é para criar um novo objeto ou para abrir um objeto existente:

- Se o evento aberto for uma solicitação aberta para criar um novo objeto (arquivo ou diretório), a `HandleID` tag no evento XML de auditoria mostrará um vazio `HandleID` (por exemplo: `<Data Name="HandleID">0000000000000000;00;00000000;00000000</Data>` ).

O `HandleID` está vazio porque a SOLICITAÇÃO ABERTA (para criar um novo objeto) é auditada antes da criação real do objeto acontecer e antes de existir um identificador. Eventos auditados subsequentes para o mesmo objeto têm o identificador de objeto certo na `HandleID` tag.

- Se o evento aberto for uma solicitação aberta para abrir um objeto existente, o evento de auditoria terá o identificador atribuído desse objeto na `HandleID` tag (por exemplo: `<Data Name="HandleID">000000000000401;00;000000ea;00123ed4</Data>` ).

## Determine qual é o caminho completo para o objeto auditado

O caminho do objeto impresso na `<ObjectName>` tag para um Registro de auditoria contém o nome do volume (entre parênteses) e o caminho relativo da raiz do volume que contém. Se você quiser determinar o caminho completo do objeto auditado, incluindo o caminho de junção, há certas etapas que você deve seguir.

### Passos

1. Determine qual é o nome do volume e o caminho relativo para o objeto auditado olhando para a `<ObjectName>` tag no evento de auditoria.

Neste exemplo, o nome do volume é "ATA1" e o caminho relativo para o arquivo é `/dir1/file.txt`:

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

2. Usando o nome do volume determinado na etapa anterior, determine qual é o caminho de junção para o volume que contém o objeto auditado:

Neste exemplo, o nome do volume é "ATA1" e o caminho de junção para o volume que contém o objeto auditado é `/data/data1`:

```
volume show -junction -volume data1
```

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

3. Determine o caminho completo para o objeto auditado anexando o caminho relativo encontrado na `<ObjectName>` tag para o caminho de junção para o volume.

Neste exemplo, o caminho de junção para o volume:

```
/data/data1/dir1/file.txt
```

## Considerações ao auditar links simbólicos e links duros

Há certas considerações que você deve ter em mente ao auditar links simbólicos e links duros.

Um Registro de auditoria contém informações sobre o objeto que está sendo auditado, incluindo o caminho para o objeto auditado, que é identificado na `ObjectName` tag. Você deve estar ciente de como caminhos para links simbólicos e links rígidos são gravados na `ObjectName` tag.

### Links simbólicos

Um link simbólico é um arquivo com um inode separado que contém um ponteiro para a localização de um objeto de destino, conhecido como alvo. Ao acessar um objeto por meio de um link simbólico, o ONTAP interpreta automaticamente o link simbólico e segue o caminho agnóstico do protocolo canônico real para o objeto de destino no volume.

Na saída de exemplo a seguir, há dois links simbólicos, ambos apontando para um arquivo `target.txt` chamado . Um dos links simbólicos é um link simbólico relativo e um é um link simbólico absoluto. Se qualquer um dos links simbólicos for auditado, a `ObjectName` tag no evento de auditoria conterà o caminho para o arquivo `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
```

## Links físicos

Um link físico é uma entrada de diretório que associa um nome a um arquivo existente em um sistema de arquivos. O link físico aponta para a localização do inode do arquivo original. Semelhante a como o ONTAP interpreta links simbólicos, o ONTAP interpreta o link físico e segue o caminho canônico real para o objeto alvo no volume. Quando o acesso a um objeto de link físico é auditado, o evento de auditoria Registra esse caminho canônico absoluto na `ObjectName` tag em vez do caminho do link físico.

## Considerações ao auditar fluxos de dados NTFS alternativos

Há certas considerações que você deve ter em mente ao auditar arquivos com fluxos de dados alternativos NTFS.

A localização de um objeto que está sendo auditado é registrada em um Registro de evento usando duas tags, a `ObjectName` tag (o caminho) e a `HandleID` tag (o identificador). Para identificar corretamente quais solicitações de fluxo estão sendo registradas, você deve estar ciente de quais Registros do ONTAP nesses campos para fluxos de dados alternativos do NTFS:

- ID EVT: 4656 eventos (abrir e criar eventos de auditoria)
  - O caminho do fluxo de dados alternativo é gravado na `ObjectName` tag.
  - O identificador do fluxo de dados alternativo é gravado na `HandleID` tag.
- ID EVT: 4663 eventos (todos os outros eventos de auditoria, como leitura, escrita, `getattr`, e assim por diante)
  - O caminho do arquivo base, não o fluxo de dados alternativo, é gravado na `ObjectName` tag.
  - O identificador do fluxo de dados alternativo é gravado na `HandleID` tag.

### Exemplo

O exemplo a seguir ilustra como identificar o ID EVT: 4663 eventos para fluxos de dados alternativos usando a `HandleID` tag. Mesmo que a `ObjectName` tag (caminho) registrada no evento de auditoria de leitura seja para o caminho do arquivo base, a `HandleID` tag pode ser usada para identificar o evento como um Registro de auditoria para o fluxo de dados alternativo.

Os nomes dos arquivos de stream assumem o formulário `base_file_name:stream_name`. Neste exemplo, o `dir1` diretório contém um arquivo base com um fluxo de dados alternativo com os seguintes caminhos:

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



A saída no exemplo de evento a seguir é truncada como indicado; a saída não exibe todas as tags de saída disponíveis para os eventos.

Para um EVT X ID 4656 (evento de auditoria aberto), a saída do Registro de auditoria para o fluxo de dados alternativo Registra o nome do fluxo de dados alternativo na `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>
```

Para um EVT X ID 4663 (evento de auditoria de leitura), a saída do Registro de auditoria para o mesmo fluxo de dados alternativo Registra o nome do arquivo base na `ObjectName` tag; no entanto, o identificador na `HandleID` tag é o identificador do fluxo de dados alternativo e pode ser usado para correlacionar esse evento com o fluxo de dados 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>
```

## Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

## Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.