Eventi SMB che possono essere verificati

ONTAP 9

NetApp
April 24, 2024

Sommario

Eventi SMB che possono essere verificati

Panoramica degli eventi SMB che è possibile verificare

ONTAP può controllare alcuni eventi SMB, inclusi determinati eventi di accesso a file e cartelle, determinati eventi di accesso e disconnessione ed eventi di staging dei criteri di accesso centrale. Sapere quali eventi di accesso è possibile verificare è utile quando si interpretano i risultati dei registri eventi.

I seguenti eventi SMB aggiuntivi possono essere verificati in ONTAP 9.2 e versioni successive:

ID EVENTO (EVT/EVTX)	Evento	Descrizione	Categoria
4670	Le autorizzazioni degli oggetti sono state modificate	OBJECT ACCESS (ACCESSO A OGGETTI): Autorizzazioni modificate.	Accesso al file
4907	Le impostazioni di controllo degli oggetti sono state modificate	OBJECT ACCESS (ACCESSO A OGGETTI): Impostazioni di controllo modificate.	Accesso al file
4913	La policy di accesso di Object Central è stata modificata	ACCESSO A OGGETTI: CAP MODIFICATO.	Accesso al file

I seguenti eventi SMB possono essere verificati in ONTAP 9.0 e versioni successive:

ID EVENTO (EVT/EVTX)	Evento	Descrizione	Categoria
540/4624	Un account è stato collegato correttamente	LOGON/LOGOFF: Accesso alla rete (SMB).	Accesso e disconnessione
529/4625	Impossibile accedere a un account	LOGON/LOGOFF: Nome utente sconosciuto o password errata.	Accesso e disconnessione
530/4625	Impossibile accedere a un account	LOGON/LOGOFF: Limite di tempo per l’accesso all’account.	Accesso e disconnessione
531/4625	Impossibile accedere a un account	LOGON/LOGOFF: Account attualmente disattivato.	Accesso e disconnessione
532/4625	Impossibile accedere a un account	LOGON/LOGOFF: L’account utente è scaduto.	Accesso e disconnessione

533/4625	Impossibile accedere a un account	LOGON/LOGOFF (ACCESSO/DISCONNESSIONE): L'utente non può accedere al computer.	Accesso e disconnessione
534/4625	Impossibile accedere a un account	LOGON/LOGOFF: L'utente non ha concesso il tipo di accesso qui.	Accesso e disconnessione
535/4625	Impossibile accedere a un account	LOGON/LOGOFF: La password dell'utente è scaduta.	Accesso e disconnessione
537/4625	Impossibile accedere a un account	LOGON/LOGOFF: Accesso non riuscito per motivi diversi da quelli sopra indicati.	Accesso e disconnessione
539/4625	Impossibile accedere a un account	LOGON/LOGOFF: Account bloccato.	Accesso e disconnessione
538/4634	Un account è stato disconnesso	LOGON/LOGOFF: Disconnessione dell'utente locale o di rete.	Accesso e disconnessione
560/4656	Apri oggetto/Crea oggetto	ACCESSO A OGGETTI: Oggetto (file o directory) aperto.	Accesso al file
563/4659	Aprire l'oggetto con l'intento di eliminare	ACCESSO A OGGETTI: È stato richiesto un handle a un oggetto (file o directory) con l'intento di eliminare.	Accesso al file
564/4660	Elimina oggetto	OBJECT ACCESS (ACCESSO A OGGETTI): Elimina oggetto (file o directory). ONTAP genera questo evento quando un client Windows tenta di eliminare l'oggetto (file o directory).	Accesso al file
567/4663	Read Object/Write Object/Get Object Attributes/Set Object Attributes	ACCESSO A OGGETTI: Tentativo di accesso a oggetti (lettura, scrittura, attributo get, attributo set). **Nota:** per questo evento, ONTAP controlla solo la prima operazione di lettura SMB e la prima operazione di scrittura SMB (successo o errore) su un oggetto. Ciò impedisce a ONTAP di creare voci di registro eccessive quando un singolo client apre un oggetto ed esegue molte operazioni di lettura o scrittura successive sullo stesso oggetto.	Accesso al file

NA/4664	Collegamento rigido	OBJECT ACCESS (ACCESSO A OGGETTI): Tentativo di creazione di un hard link.	Accesso al file
NA/4818	Il criterio di accesso centrale proposto non concede le stesse autorizzazioni di accesso del criterio di accesso centrale corrente	ACCESSO A OGGETTI: Gestione temporanea dei criteri di accesso centrale.	Accesso al file
ID evento Data ONTAP NA/NA 9999	Rinominare l'oggetto	ACCESSO AGLI OGGETTI: Oggetto rinominato. Si tratta di un evento ONTAP. Attualmente non è supportato da Windows come singolo evento.	Accesso al file
ID evento Data ONTAP NA/NA 9998	Scollegare l'oggetto	ACCESSO A OGGETTI: Oggetto non collegato. Si tratta di un evento ONTAP. Attualmente non è supportato da Windows come singolo evento.	Accesso al file

Ulteriori informazioni sull'evento 4656

Il `HandleID` tag nell'audit `XML` l'evento contiene l'handle dell'oggetto (file o directory) a cui si accede. Il `HandleID` Tag per L'evento EVTX 4656 contiene informazioni diverse a seconda che l'evento aperto sia per la creazione di un nuovo oggetto o per l'apertura di un oggetto esistente:

- Se l'evento open è una richiesta di apertura per creare un nuovo oggetto (file o directory), il `HandleID` Il tag nell'evento XML di audit mostra un valore vuoto `HandleID` (ad esempio: `<Data Name="HandleID">00000000000000;00;00000000;00000000</Data>`).

  Il `HandleID` È vuoto perché la richiesta DI APERTURA (per la creazione di un nuovo oggetto) viene controllata prima che avvenga la creazione effettiva dell'oggetto e prima che esista un handle. Gli eventi controllati successivi per lo stesso oggetto hanno il giusto handle di oggetto in `HandleID` tag.

- Se l'evento open è una richiesta aperta per aprire un oggetto esistente, l'evento di audit avrà l'handle assegnato di tale oggetto in `HandleID` tag (ad esempio: `<Data Name="HandleID">00000000000401;00;000000ea;00123ed4</Data>`).

Determinare il percorso completo dell'oggetto verificato

Il percorso dell'oggetto stampato in `<ObjectName>` il tag per un record di audit contiene il nome del volume (tra parentesi) e il percorso relativo dalla directory principale del volume contenente. Se si desidera determinare il percorso completo dell'oggetto sottoposto a audit, incluso il percorso di giunzione, è necessario eseguire alcuni passaggi.

Fasi

1. Determinare il nome del volume e il relativo percorso dell'oggetto sottoposto a controllo osservando il `<ObjectName>` tag nell'evento di audit.

   In questo esempio, il nome del volume è "data1" e il percorso relativo al file è `/dir1/file.txt`:

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

2. Utilizzando il nome del volume determinato nella fase precedente, determinare il percorso di giunzione per il volume contenente l'oggetto verificato:

   In questo esempio, il nome del volume è "data1" e il percorso di giunzione per il volume contenente l'oggetto sottoposto a audit è `/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. Determinare il percorso completo dell'oggetto verificato aggiungendo il percorso relativo trovato in `<ObjectName>` contrassegnare il percorso di giunzione per il volume.

   In questo esempio, il percorso di giunzione per il volume:

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

Considerazioni per il controllo di collegamenti simbolici e hard link

Ci sono alcune considerazioni da tenere a mente quando si esegue il controllo dei collegamenti simbolici e dei collegamenti rigidi.

Un record di audit contiene informazioni sull'oggetto sottoposto a audit, incluso il percorso dell'oggetto sottoposto a audit, identificato in `ObjectName` tag. È necessario conoscere come vengono registrati i percorsi per i collegamenti simbolici e gli hard link in `ObjectName` tag.

Link simbolici

Un collegamento simbolico è un file con un inode separato che contiene un puntatore alla posizione di un oggetto di destinazione, noto come destinazione. Quando si accede a un oggetto tramite un collegamento simbolico, ONTAP interpreta automaticamente il collegamento simbolico e segue il percorso indipendente dal protocollo canonico effettivo verso l'oggetto di destinazione nel volume.

Nell'output dell'esempio seguente, sono presenti due collegamenti simbolici, entrambi rivolti a un file denominato `target.txt`. Uno dei link simbolici è un link simbolico relativo e uno è un link simbolico assoluto. Se uno dei collegamenti simbolici viene controllato, il `ObjectName` tag nell'evento di audit contiene il percorso

del 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
```

Collegamenti hardware

Un hard link è una voce di directory che associa un nome a un file esistente su un file system. L'hard link punta alla posizione inode del file originale. Analogamente a quanto ONTAP interpreta i collegamenti simbolici, ONTAP interpreta il collegamento rigido e segue il percorso canonico effettivo dell'oggetto di destinazione nel volume. Quando viene verificato l'accesso a un oggetto hard link, l'evento di audit registra questo percorso canonico assoluto in `ObjectName` piuttosto che il percorso hard link.

Considerazioni per il controllo di flussi di dati NTFS alternativi

È necessario tenere presente alcune considerazioni durante il controllo dei file con flussi di dati alternativi NTFS.

La posizione di un oggetto sottoposto a audit viene registrata in un record di evento utilizzando due tag, l' `ObjectName` tag (il percorso) e il `HandleID` tag (l'impugnatura). Per identificare correttamente le richieste di flusso registrate, è necessario conoscere i record ONTAP presenti in questi campi per i flussi di dati alternativi NTFS:

- ID EVTX: 4656 eventi (aprire e creare eventi di audit)
  - Il percorso del flusso di dati alternativo viene registrato in `ObjectName` tag.
  - L'handle del flusso di dati alternativo viene registrato in `HandleID` tag.
- ID EVTX: 4663 eventi (tutti gli altri eventi di audit, come lettura, scrittura, getattr e così via)
  - Il percorso del file di base, non del flusso di dati alternativo, viene registrato in `ObjectName` tag.
  - L'handle del flusso di dati alternativo viene registrato in `HandleID` tag.

Esempio

Nell'esempio seguente viene illustrato come identificare L'ID EVTX: 4663 eventi per flussi di dati alternativi che utilizzano `HandleID` tag. Anche se il `ObjectName` il tag (percorso) registrato nell'evento di controllo in lettura si trova nel percorso del file di base, il `HandleID` il tag può essere utilizzato per identificare l'evento come record di audit per il flusso di dati alternativo.

I nomi dei file di streaming hanno la forma `base_file_name:stream_name`. In questo esempio, il `dir1` la directory contiene un file di base con un flusso di dati alternativo con i seguenti percorsi:

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

> L'output nel seguente esempio di evento viene troncato come indicato; l'output non visualizza tutti i tag di output disponibili per gli eventi.

Per un ID EVTX 4656 (evento di audit aperto), l'output del record di audit per il flusso di dati alternativo registra il nome del flusso di dati alternativo in `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>
```

Per un ID EVTX 4663 (evento di audit in lettura), l'output del record di audit per lo stesso flusso di dati alternativo registra il nome del file di base in `ObjectName` tag; tuttavia, l'handle in `HandleID` tag è l'handle alternativo del flusso di dati e può essere utilizzato per correlare questo evento con il flusso di dati 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>
```