감사할 수 있는 **SMB** 이벤트입니다
ONTAP 9

NetApp
February 12, 2026

목차

감사할 수 있는 **SMB** 이벤트입니다

ONTAP에서 결과를 해석하기 위해 감사할 수 있는 **SMB** 이벤트에 대해 알아보십시오

ONTAP는 특정 파일 및 폴더 액세스 이벤트, 특정 로그온 및 로그오프 이벤트, 중앙 액세스 정책 스테이징 이벤트를 비롯한 특정 SMB 이벤트를 감사할 수 있습니다. 감사할 수 있는 액세스 이벤트를 알면 이벤트 로그의 결과를 해석할 때 도움이 됩니다.

다음과 같은 추가 SMB 이벤트를 감사할 수 있습니다.

이벤트 ID(EVT/evtx)	이벤트	설명	범주
4670)을 참조하십시오	개체 권한이 변경되었습니다	객체 액세스: 권한이 변경되었습니다.	파일 액세스
4907	개체 감사 설정이 변경되었습니다	개체 액세스: 감사 설정이 변경되었습니다.	파일 액세스
4913	객체 중앙 액세스 정책이 변경되었습니다	개체 액세스: 캡이 변경되었습니다.	파일 액세스

다음 SMB 이벤트는 ONTAP 9.0 이상에서 감사할 수 있습니다.

이벤트 ID(EVT/evtx)	이벤트	설명	범주
540/4624	계정이 성공적으로 로그온되었습니다	로그온/로그오프: 네트워크(SMB) 로그온.	로그온 및 로그오프
529/4625	계정 로그온에 실패했습니다	로그온/로그오프: 알 수 없는 사용자 이름 또는 잘못된 암호입니다.	로그온 및 로그오프
530/4625	계정 로그온에 실패했습니다	로그온/로그오프: 계정 로그온 시간 제한.	로그온 및 로그오프
531/4625	계정 로그온에 실패했습니다	로그온/로그오프: 계정이 현재 비활성화되었습니다.	로그온 및 로그오프
532/4625	계정 로그온에 실패했습니다	로그온/로그오프: 사용자 계정이 만료되었습니다.	로그온 및 로그오프
533/4625	계정 로그온에 실패했습니다	로그온/로그오프: 사용자가 이 컴퓨터에 로그온할 수 없습니다.	로그온 및 로그오프

534/4625	계정 로그온에 실패했습니다	로그온/로그오프: 여기에 로그온 유형이 부여되지 않았습니다.	로그온 및 로그오프
535/4625	계정 로그온에 실패했습니다	로그온/로그오프: 사용자 암호가 만료되었습니다.	로그온 및 로그오프
537/4625	계정 로그온에 실패했습니다	로그온/로그오프: 위의 이유 이외의 이유로 로그온하지 못했습니다.	로그온 및 로그오프
539/4625	계정 로그온에 실패했습니다	로그온/로그오프: 계정이 잠겼습니다.	로그온 및 로그오프
538/4634	계정이 로그오프되었습니다	로그온/로그오프: 로컬 또는 네트워크 사용자 로그오프.	로그온 및 로그오프
560/4656)을 참조하십시오	객체 열기/객체 생성	오브젝트 액세스: 오브젝트(파일 또는 디렉토리)가 열려 있습니다.	파일 액세스
563/4659	삭제 의도에 따라 개체를 엽니다	오브젝트 액세스: 오브젝트(파일 또는 디렉토리)에 대한 핸들이 삭제 의향과 함께 요청되었습니다.	파일 액세스
564/4660	개체 삭제	오브젝트 액세스: 오브젝트 삭제(파일 또는 디렉토리). ONTAP는 Windows 클라이언트가 개체(파일 또는 디렉터리)를 삭제하려고 할 때 이 이벤트를 생성합니다.	파일 액세스
567/4663	개체 읽기/개체 쓰기/개체 속성 가져오기/개체 특성 설정	오브젝트 액세스: 오브젝트 액세스 시도(읽기, 쓰기, get 속성, set 속성) • 참고: * 이 이벤트의 경우 ONTAP는 개체에 대한 첫 번째 SMB 읽기 및 첫 번째 SMB 쓰기 작업(성공 또는 실패)만 감사합니다. 이렇게 하면 단일 클라이언트가 개체를 열고 동일한 개체에 대해 여러 번의 연속 읽기 또는 쓰기 작업을 수행할 때 ONTAP에서 과도한 로그 항목을 만들지 못하게 됩니다.	파일 액세스
해당 없음/4664	하드 링크	개체 액세스: 하드 링크를 만들려고 했습니다.	파일 액세스
해당 없음/4818	제안된 중앙 액세스 정책은 현재 중앙 액세스 정책과 동일한 액세스 권한을 부여하지 않습니다	객체 액세스: 중앙 액세스 정책 스테이징.	파일 액세스

NA/NA Data ONTAP 이벤트 ID 9999	개체 이름 바꾸기	오브젝트 액세스: 오브젝트 이름 바꾸기. ONTAP 이벤트입니다. 현재 Windows에서 단일 이벤트로 지원되지 않습니다.	파일 액세스
NA/NA Data ONTAP 이벤트 ID 9998	개체 연결 끊기	개체 액세스: 개체 연결 해제됨. ONTAP 이벤트입니다. 현재 Windows에서 단일 이벤트로 지원되지 않습니다.	파일 액세스

이벤트 **4656**에 대한 추가 정보

감사 XML 이벤트의 HandleID 태그에는 액세스한 개체(파일 또는 디렉터리)의 핸들이 들어 있습니다. evtx 4656 이벤트에 대한 "HandleID" 태그는 open 이벤트가 새 개체를 만들거나 기존 개체를 여는 데 사용되는지 여부에 따라 다른 정보를 포함합니다.

- Open event가 Open request로 새로운 object(file or directory)를 생성하려는 경우 Audit XML event의 HandleID 태그는 빈 HandleID를 표시합니다(예: "<Data Name="HandleID">00000000000000;00;00000000;00000000</Data>").

  실제 개체 생성이 발생하기 전과 핸들이 있기 전에 열려 있는(새 개체 만들기) 요청을 감사하기 때문에 "HandleID"가 비어 있습니다. 같은 개체에 대한 후속 감사 이벤트에는 'HandleID' 태그에 올바른 객체 핸들이 있습니다.

- open event가 기존 object를 열기 위한 open 요청인 경우 audit event는 'HandleID' 태그(예: "<Data Name="HandleID">0000000401;00;000000ea;00123ed4</Data>")에서 해당 object의 할당된 handle을 갖게 됩니다.

ONTAP 감사 객체에 대한 전체 경로를 결정합니다

감사 레코드에 대한 "<ObjectName>" 태그에 인쇄된 객체 경로에는 볼륨의 이름(괄호 안에 표시)과 포함하는 볼륨의 루트에서의 상대 경로가 포함됩니다. 연결 경로를 포함하여 감사된 개체의 전체 경로를 결정하려면 특정 단계를 수행해야 합니다.

단계

1. 감사 이벤트의 "<ObjectName>" 태그를 확인하여 감사된 개체에 대한 볼륨 이름 및 상대 경로를 확인합니다.

   이 예에서 볼륨 이름은 "data1"이고 파일의 상대 경로는 "/dir1/file.txt"입니다.

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

2. 이전 단계에서 확인한 볼륨 이름을 사용하여 감사된 개체가 포함된 볼륨의 연결 경로를 결정합니다.

   이 예에서 볼륨 이름은 "data1"이고 감사 대상 객체가 포함된 볼륨의 연결 경로는 "/data/data1"입니다.

   '볼륨 표시-접합-볼륨 데이터1'

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

3. 볼륨의 접합 경로에 "<ObjectName>" 태그에 있는 상대 경로를 추가하여 감사된 개체의 전체 경로를 확인합니다.

   이 예에서 볼륨의 접합 경로는 다음과 같습니다.

   '/data/data1/dir1/file.text'

교집합 및 하드 링크에 대한 ONTAP 감사에 대해 알아봅니다

symlink 및 hard link를 감사할 때는 몇 가지 고려 사항을 염두에 두어야 합니다.

감사 레코드에는 "ObjectName" 태그에서 식별되는 감사 객체의 경로를 비롯하여 감사 중인 객체에 대한 정보가 포함되어 있습니다. symlink와 hard link의 path가 ObjectName 태그에 기록되는 방식을 알고 있어야 합니다.

Symlink

Symlink는 대상 오브젝트의 위치에 대한 포인터가 포함된 별도의 inode가 있는 파일이며, 대상이라고 합니다. symlink를 통해 개체에 액세스할 때 ONTAP는 자동으로 symlink를 해석하고 볼륨의 대상 개체에 대한 실제 정규 프로토콜 무관 경로를 따릅니다.

다음 예제 출력에는 둘 다 target.txt라는 파일을 가리키는 두 개의 symlink가 있습니다. 심볼 링크 중 하나는 상대 symlink로, 다른 하나는 절대 symlink입니다. symlink 중 하나가 감사되는 경우 audit event의 ObjectName 태그에 "target.txt" 파일의 경로가 포함됩니다.

```
[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
```

하드 링크

하드 링크는 파일 시스템의 기존 파일과 이름을 연결하는 디렉토리 항목입니다. 하드 링크는 원본 파일의 inode 위치를 가리킵니다. ONTAP에서 symlink를 해석하는 방법과 마찬가지로 ONTAP는 하드 링크를 해석하고 볼륨의 대상 개체에 대한 실제 정규 경로를 따릅니다. 하드 링크 개체에 대한 액세스가 감사되면 감사 이벤트는 하드 링크 경로가 아닌 ObjectName 태그에 이 절대 정규 경로를 기록합니다.

대체 **NTFS** 데이터 스트림의 **ONTAP** 감사에 대해 알아봅니다

NTFS 대체 데이터 스트림을 사용하여 파일을 감사할 때 고려해야 할 몇 가지 사항이 있습니다.

감사대상 개체의 위치는 이벤트 레코드에 ObjectName 태그(경로)와 HandleID 태그(핸들)라는 두 개의 태그를 사용하여 기록됩니다. 기록되는 스트림 요청을 제대로 식별하려면 NTFS 대체 데이터 스트림에 대한 다음 필드의 ONTAP 레코드를 알고 있어야 합니다.

- evtx ID: 4656 이벤트(감사 이벤트 열기 및 만들기)
  - 대체 데이터 스트림의 경로는 ObjectName 태그에 기록됩니다.
  - 대체 데이터 스트림의 핸들은 HandleID 태그에 기록됩니다.
- evtx ID: 4663 이벤트(읽기, 쓰기, GetAttr 등과 같은 기타 모든 감사 이벤트)
  - 대체 데이터 스트림이 아닌 기본 파일의 경로는 ObjectName 태그에 기록됩니다.
  - 대체 데이터 스트림의 핸들은 HandleID 태그에 기록됩니다.

예

다음 예제에서는 "HandleID" 태그를 사용하여 대체 데이터 스트림에 대한 evtx ID: 4663 이벤트를 식별하는 방법을 보여 줍니다. READ AUDIT 이벤트에 기록된 ObjectName 태그(경로)가 기본 파일 경로에 있더라도 HandleID 태그를 사용하여 대체 데이터 스트림에 대한 감사 레코드로 이벤트를 식별할 수 있습니다.

스트림 파일 이름은 base_file_name:stream_name 형식으로 지정됩니다. 이 예제에서 dIR1 디렉토리에는 다음 경로를 가진 대체 데이터 스트림이 있는 기본 파일이 포함되어 있습니다.

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

다음 이벤트 예제의 출력은 표시된 대로 잘립니다. 출력에 해당 이벤트에 사용할 수 있는 출력 태그가 모두 표시되지 않습니다.

evtx ID 4656(열린 감사 이벤트)의 경우 대체 데이터 스트림에 대한 감사 레코드 출력은 "ObjectName" 태그에 대체 데이터 스트림 이름을 기록합니다.

```
- <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>
```

evtx ID 4663(감사 이벤트 읽기)의 경우 동일한 대체 데이터 스트림에 대한 감사 레코드 출력은 "ObjectName" 태그에 기본 파일 이름을 기록합니다. 그러나 "HandleID" 태그의 핸들은 대체 데이터 스트림의 핸들로, 이 이벤트를 대체 데이터 스트림과 연관시키는 데 사용할 수 있습니다.

```
- <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>
```