可审核的 SMB 事件

ONTAP 9

NetApp
February 12, 2026

目录

可审核的 SMB 事件

了解ONTAP可以审核以解释结果的SMB事件

ONTAP 可以审核某些 SMB 事件，包括某些文件和文件夹访问事件，某些登录和注销事件以及中央访问策略暂存事件。了解可以审核哪些访问事件有助于解释事件日志中的结果。

可以审核以下附加 SMB 事件：

事件 ID （ EVT/EVTX ）	事件	Description	类别
4670	对象权限已更改	对象访问：权限已更改。	文件访问
4907年	对象审核设置已更改	对象访问：审核设置已更改。	文件访问
4913.	对象中央访问策略已更改	对象访问： CAP 已更改。	文件访问

可以在 ONTAP 9.0 及更高版本中审核以下 SMB 事件：

事件 ID （ EVT/EVTX ）	事件	Description	类别
540/4624.	已成功登录帐户	登录/注销：网络(SMB)登录。	登录和注销
529/4625.	帐户无法登录	logon/logoff ： 用户名未知或密码错误。	登录和注销
530/4625	帐户无法登录	logon/logoff ： 帐户登录时间限制。	登录和注销
531/4625.	帐户无法登录	logon/logoff ： 帐户当前已禁用。	登录和注销
532/4625.	帐户无法登录	登录 / 注销：用户帐户已过期。	登录和注销
533/4625.	帐户无法登录	logon/logoff ： 用户无法登录到此计算机。	登录和注销
534/4625.	帐户无法登录	logon/logoff ： 此处未授予用户登录类型。	登录和注销
535/4625.	帐户无法登录	登录 / 注销：用户密码已过期。	登录和注销
5374625.	帐户无法登录	logon/logoff ： 由于上述原因，登录失败。	登录和注销

539/4625.	帐户无法登录	logon/logoff ： 帐户已锁定。	登录和注销
534/4634	已注销帐户	登录 / 注销：本地或网络用户注销。	登录和注销
560/4656	打开对象 / 创建对象	对象访问：打开对象（文件或目录）。	文件访问
563/4659.	打开要删除的对象	对象访问：已请求对对象（文件或目录）的句柄，其目的是删除。	文件访问
564/4660	删除对象	对象访问：删除对象（文件或目录）。当 Windows 客户端尝试删除对象（文件或目录）时， ONTAP 会生成此事件。	文件访问
567/463.	读取对象 / 写入对象 / 获取对象属性 / 设置对象属性	对象访问：对象访问尝试（读取，写入，获取属性，设置属性）。 • 注意： * 对于此事件， ONTAP 仅审核对象的第一个 SMB 读取和第一个 SMB 写入操作（成功或失败）。这样，当一个客户端打开一个对象并对同一个对象执行多次连续读写操作时， ONTAP 就不会创建过多的日志条目。	文件访问
NA/4664	硬链接	对象访问：尝试创建硬链接。	文件访问
NA/4818	建议的中央访问策略不会授予与当前中央访问策略相同的访问权限	对象访问：中央访问策略暂存。	文件访问
不适用 Data ONTAP 事件 ID 9999	重命名对象	对象访问：对象已重命名。这是一个 ONTAP 事件。目前， Windows 不支持将其作为单个事件。	文件访问
不适用/不适用Data ONTAP事件ID 9998	取消对象链接	对象访问：对象未链接。这是一个 ONTAP 事件。目前， Windows 不支持将其作为单个事件。	文件访问

追加信息关于事件 **4656**

。 `HandleID` 标记 `XML` event包含所访问对象(文件或目录)的句柄。。 `HandleID` 根据打开的事件是用于创建新对象还是用于打开现有对象、evtx 4656事件的标记包含不同的信息：

- 如果打开事件是创建新对象(文件或目录)的打开请求、则 `HandleID` 审核XML事件中的标记显示为空 `HandleID` (例如： `<Data Name="HandleID">00000000000000;00;00000000;00000000</Data>` ）。

。 HandleID 为空、因为在实际创建对象之前和句柄存在之前、系统会审核打开(用于创建新对象)请求。同一对象的后续审核事件在中具有正确的对象句柄 HandleID 标记。

- 如果此打开事件是打开现有对象的OPEN请求、则此审核事件将在中为该对象分配句柄 HandleID 标记(例如： <Data Name="HandleID">00000000000401;00;000000ea;00123ed4</Data> ）。

确定ONTAP审核对象的完整路径

打印在中的对象路径 <ObjectName> 审核记录的标记包含卷的名称(用圆括号括起)以及从所属卷的根目录开始的相对路径。如果要确定已审核对象的完整路径，包括接合路径，则必须执行某些步骤。

步骤

1. 通过查看来确定卷名称以及经过审核的对象的相对路径 <ObjectName> 审核事件中的标记。

   在此示例中、卷名称为`data1`、文件的相对路径为 /dir1/file.txt：

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

2. 使用上一步中确定的卷名称，确定包含已审核对象的卷的接合路径：

   在此示例中、卷名称为`data1`、包含已审核对象的卷的接合路径为 /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. 通过附加中的相对路径来确定经过审核的对象的完整路径 <ObjectName> 标记到卷的接合路径。

   在此示例中，卷的接合路径为：

   /data/data1/dir1/file.text

了解ONTAP对符号链接和硬链接的审核

审核符号链接和硬链接时，必须牢记某些注意事项。

审核记录包含有关要审核的对象的信息、包括中标识的已审核对象的路径 ObjectName 标记。您应了解符号链接和硬链接的路径如何记录在中 ObjectName 标记。

符号链接

符号链接是一个具有单独索引节点的文件，其中包含指向目标对象（称为目标）位置的指针。通过符号链接访问对象时， ONTAP 会自动解释符号链接，并遵循卷中目标对象的实际不受规范协议限制的路径。

在以下示例输出中、有两个符号链接、它们都指向一个名为的文件 `target.txt`。其中一个符号链接是相对符号链接，一个符号链接是绝对符号链接。如果审核了其中任何一个符号链接、则 `ObjectName` 审核事件中的标记包含文件的路径 `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
```

硬链接

硬链接是指将名称与文件系统上的现有文件关联的目录条目。硬链接指向原始文件的索引节点位置。与 ONTAP 解释符号链接的方式类似， ONTAP 解释硬链接并遵循卷中目标对象的实际规范路径。审核对硬链接对象的访问时、审核事件会在中记录此绝对规范路径 `ObjectName` 标记、而不是硬链接路径。

了解ONTAP对备用NTFS数据流的审核

在使用 NTFS 备用数据流审核文件时，必须牢记某些注意事项。

要审核的对象的位置会使用两个标记(即)记录在事件记录中 `ObjectName` 标记(路径)和 `HandleID` 标记(手柄)。要正确识别正在记录的流请求，您必须了解 NTFS 备用数据流的以下字段中的 ONTAP 记录：

- evtx ID： 4656 个事件（打开和创建审核事件）
  - 备用数据流的路径将记录在中 `ObjectName` 标记。
  - 备用数据流的句柄记录在中 `HandleID` 标记。
- evtx ID： 4663 个事件（所有其他审核事件，例如读取，写入， getattr 等）
  - 基础文件的路径(而不是备用数据流)会记录在中 `ObjectName` 标记。
  - 备用数据流的句柄记录在中 `HandleID` 标记。

示例

以下示例说明了如何使用确定备用数据流的evtx ID：4663个事件 `HandleID` 标记。即使 `ObjectName` 读取审核事件中记录的标记(路径)指向基本文件路径、即 `HandleID` 标记可用于将事件标识为备用数据流的审核记录。

流文件名采用以下格式 `base_file_name:stream_name`。在此示例中、将显示 `dir1` 目录包含一个基础文件、其中包含一个备用数据流、其路径如下：

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

以下事件示例中的输出将被截断，如图所示；输出不会显示事件的所有可用输出标记。

对于evtx ID 4656 (打开审核事件)、备用数据流的审核记录输出将在中记录备用数据流名称 `ObjectName` 标记：

```
- <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>
```

对于evtx ID 4663 (读取审核事件)、同一备用数据流的审核记录输出将在中记录基本文件名 `ObjectName` 标记；但是、中的句柄 `HandleID` 标记是备用数据流的句柄、可用于将此事件与备用数据流相关联：

```
- <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>
```