可稽核的SMB事件

ONTAP 9

NetApp
April 24, 2024

目錄

可稽核的SMB事件

可稽核的SMB事件總覽

可稽核特定的SMB事件、包括特定檔案和資料夾存取事件、特定登入和登出事件、以及集中存取原則暫存事件。ONTAP瞭解哪些存取事件可以稽核、有助於解讀事件記錄的結果。

下列額外的SMB事件可在ONTAP 下列版本中進行稽核：

事件ID（EVT/evtx）	活動	說明	類別
4670	物件權限已變更	物件存取：權限已變更。	檔案存取
4907	物件稽核設定已變更	物件存取：稽核設定已變更。	檔案存取
4913.	物件中心存取原則已變更	物件存取：CAP已變更。	檔案存取

下列SMB事件ONTAP 可在下列版本中透過下列功能進行稽核：

事件ID（EVT/evtx）	活動	說明	類別
540/4624	帳戶已成功登入	登入/登出：網路（SMB）登入。	登入與登出
598/4625	帳戶無法登入	登入/登出：不明的使用者名稱或錯誤的密碼。	登入與登出
530/4625	帳戶無法登入	登入/登出：帳戶登入時間限制。	登入與登出
531/4625	帳戶無法登入	登入/登出：帳戶目前已停用。	登入與登出
532/4625	帳戶無法登入	登入/登出：使用者帳戶已過期。	登入與登出
533/4625	帳戶無法登入	登入/登出：使用者無法登入此電腦。	登入與登出
534/4625	帳戶無法登入	登入/登出：使用者未在此授予登入類型。	登入與登出
535/4625	帳戶無法登入	登入/登出：使用者密碼已過期。	登入與登出
537-4625	帳戶無法登入	登入/登出：登入失敗的原因並非上述原因。	登入與登出
5310/4625	帳戶無法登入	登入/登出：帳戶已鎖定。	登入與登出

538/4634	帳戶已登出	登入/登出：本機或網路使用者登出。	登入與登出
560/ 4656	開啟物件/建立物件	物件存取：物件（檔案或目錄）開啟。	檔案存取
563/4659	開啟要刪除的物件	物件存取：要求物件（檔案或目錄）的控點、目的是刪除。	檔案存取
564/4660	刪除物件	物件存取：刪除物件（檔案或目錄）。當Windows用戶端嘗試刪除物件（檔案或目錄）時、會產生此事件。ONTAP	檔案存取
567/4663	讀取物件/寫入物件/取得物件屬性/設定物件屬性	物件存取：物件存取嘗試（讀取、寫入、取得屬性、設定屬性）。 附註： ONTAP 針對此活動、僅針對物件上的第一個SMB讀取和第一個SMB寫入作業（成功或失敗）進行不稽核。這可防止ONTAP 在單一用戶端開啟物件並對同一個物件執行多次連續的讀取或寫入作業時、造成過多的記錄項目。	檔案存取
NA/4664	硬式連結	物件存取：嘗試建立硬式連結。	檔案存取
NA/4818	建議的集中存取原則並未授予與目前集中存取原則相同的存取權限	物件存取：集中存取原則Staging。	檔案存取
NA/ NA Data ONTAP 不適用事件ID 9999	重新命名物件	物件存取：物件已重新命名。這是一個不確定的事件。ONTAPWindows目前不支援將它當成單一事件。	檔案存取
NA/ NA Data ONTAP 不景事件ID 9998	取消連結物件	物件存取：物件未連結。這是一個不確定的事件。ONTAPWindows目前不支援將它當成單一事件。	檔案存取

活動**4656**的其他相關資訊

。 `HandleID` 稽核中的標記 `XML` 事件包含所存取物件（檔案或目錄）的處理方式。。 `HandleID` evtx 4656 事件的標記包含不同的資訊、取決於開啟的事件是用於建立新物件或開啟現有物件：

- 如果開啟的事件是建立新物件（檔案或目錄）的開放式要求、則 `HandleID` 稽核 XML 事件中的標記顯示為空白 `HandleID` （例如： `<Data Name="HandleID">00000000000000;00;00000000;00000000</Data>` ）。
  - `HandleID` 為空白、因為在實際物件建立之前和處理代碼存在之前、會先稽核開啟（用於建立新物件）的

要求。相同物件的後續稽核事件在中具有適當的物件控點 `HandleID` 標記。

- 如果開啟的事件是開啟現有物件的開放式要求、則稽核事件會在中指派該物件的處理代碼 `HandleID` 標記（例如： `<Data Name="HandleID">00000000000401;00;000000ea;00123ed4</Data>` ）。

判斷稽核物件的完整路徑

列印在中的物件路徑 `<ObjectName>` 稽核記錄的標記包含磁碟區名稱（以括弧括住）、以及包含磁碟區根目錄的相對路徑。如果您想要判斷稽核物件的完整路徑（包括交會路徑）、您必須採取某些步驟。

步驟

1. 請查看、判斷哪些磁碟區名稱和受稽核物件的相對路徑 `<ObjectName>` 稽核事件中的標記。

   在此範例中、磁碟區名稱為「 data1 」、檔案的相對路徑為 `/dir1/file.txt`：

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

2. 使用上一步驟所決定的磁碟區名稱、判斷包含稽核物件之磁碟區的交會路徑：

   在此範例中、磁碟區名稱為「 data1 」、而包含稽核物件之磁碟區的交會路徑為 `/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. 附加在中找到的相對路徑、以決定稽核物件的完整路徑 `<ObjectName>` 標記為磁碟區的交會路徑。

   在此範例中、磁碟區的交會路徑為：

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

稽核symlink和硬式連結時的考量

稽核symlink和硬式連結時、必須謹記某些考量事項。

稽核記錄包含所稽核物件的相關資訊、包括中所識別的已稽核物件路徑 `ObjectName` 標記。您應該瞭解 symlinks 和硬式連結的路徑如何記錄在中 `ObjectName` 標記。

symlinks

symlink是一個具有獨立inode的檔案、其中包含指向目的地物件（稱為目標）位置的指標。透過symlink存取物

件時ONTAP 、流通會自動解譯symlink、並遵循實際規範的非規範傳輸協定路徑、前往磁碟區中的目標物件。

在下列範例輸出中、有兩個 symlink 、兩者都指向一個名為的檔案 `target.txt`。其中一個symlink是相對symlink、一個是絕對symlink。如果稽核其中任一符號連結、則為 `ObjectName` 稽核事件中的標記包含檔案路徑 `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
```

硬式連結

硬式連結是指將名稱與檔案系統上現有檔案相關聯的目錄項目。硬式連結指向原始檔案的inode位置。如同用什麼方式解譯symlinks、它會解譯硬式連結、並遵循實際規範路徑前往Volume中的目標物件。ONTAP ONTAP稽核硬式連結物件的存取時、稽核事件會在中記錄這條絕對規範路徑 `ObjectName` 標記而非硬連結路徑。

稽核替代NTFS資料流時的考量事項

在使用NTFS替代資料流稽核檔案時、您必須謹記某些考量事項。

要稽核的物件位置會使用兩個標籤（即）記錄在事件記錄中 `ObjectName` 標記（路徑）和 `HandleID` 標記（控點）。若要正確識別正在記錄的串流要求、您必須知道ONTAP 這些欄位中有哪些資料流是NTFS替代資料串流的佐證記錄：

- evtxID：4656個事件（開啟並建立稽核事件）
  - 替代資料串流的路徑會記錄在中 `ObjectName` 標記。
  - 替代資料串流的處理方式會記錄在中 `HandleID` 標記。
- evtxID：4663個事件（所有其他稽核事件、例如讀取、寫入、getattr等）
  - 基礎檔案的路徑、而非替代資料串流、會記錄在中 `ObjectName` 標記。
  - 替代資料串流的處理方式會記錄在中 `HandleID` 標記。

範例

下列範例說明如何使用識別 evtx ID ： 4663 個事件以用於替代資料串流 `HandleID` 標記。即使是 `ObjectName` 在讀取稽核事件中記錄的標記（路徑）位於基礎檔案路徑 `HandleID` 標記可用於將事件識別為替代資料串流的稽核記錄。

串流檔案名稱採用格式 `base_file_name:stream_name`。在此範例中 `dir1` 目錄包含基礎檔案、具有下列路徑的替代資料串流：

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

下列事件範例中的輸出會如所示被刪減；輸出不會顯示事件的所有可用輸出標記。

對於 evtx ID 4656 （開放式稽核事件）、替代資料串流的稽核記錄輸出會在中記錄替代資料串流名稱 `ObjectName` 標記：

```
- <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>
```

對於 evtx ID 4663 （讀取稽核事件）、相同替代資料串流的稽核記錄輸出會在中記錄基礎檔案名稱 `ObjectName` 標記；不過、中的控點 `HandleID` 標記是替代資料串流的處理方式、可用於將此事件與替代資料串流建立關聯：

```
- <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>
```