監査できる**SMB**イベント

ONTAP 9

NetApp
February 12, 2026

目次

監査できるSMBイベント

ONTAPが監査して結果を解釈できるSMBイベントについて学習します

ONTAPは、ファイルおよびフォルダのアクセス イベント、ログオンおよびログオフ イベント、集約型アクセス ポリシーのステージング イベントなどのSMBイベントを監査できます。どのようなアクセス イベントを監査できるか理解しておくと、イベント ログの結果を解釈するときに役立ちます。

次の追加の SMB イベントを監査できます：

イベント ID（EVT/EVTX）	イベント	概要	カテゴリ
4670	オブジェクト権限の変更	オブジェクト アクセス：権限が変更されました。	ファイル アクセス
4907	オブジェクトの監査設定の変更	オブジェクト アクセス：監査設定が変更されました。	ファイル アクセス
4913	オブジェクトの集約型アクセス ポリシーの変更	オブジェクト アクセス：CAP が変更されました。	ファイル アクセス

ONTAP 9.0以降では、次のSMBイベントを監査できます。

イベント ID（EVT/EVTX）	イベント	概要	カテゴリ
540/4624	アカウントがログオンに成功	ログオン/ログオフ：ネットワーク（SMB）ログオン。	ログオンおよびログオフ
529/4625	アカウントがログオンに失敗	ログオン/ログオフ：ユーザー名が不明であるか、パスワードが間違っています。	ログオンおよびログオフ
530/4625	アカウントがログオンに失敗	ログオン/ログオフ：アカウントのログオン時間の制限。	ログオンおよびログオフ
531/4625	アカウントがログオンに失敗	LOGON/LOGOFF：アカウントは現在無効です。	ログオンおよびログオフ
532/4625	アカウントがログオンに失敗	ログオン/ログオフ：ユーザー アカウントの有効期限が切れています。	ログオンおよびログオフ

533/4625	アカウントがログオンに失敗	ログオン/ログオフ：ユーザーはこのコンピューターにログオンできません。	ログオンおよびログオフ
534/4625	アカウントがログオンに失敗	ログオン/ログオフ：ここではユーザーにログオン タイプが許可されていません。	ログオンおよびログオフ
535/4625	アカウントがログオンに失敗	ログオン/ログオフ：ユーザーのパスワードの有効期限が切れています。	ログオンおよびログオフ
537/4625	アカウントがログオンに失敗	LOGON/LOGOFF：上記以外の理由によりログオンに失敗しました。	ログオンおよびログオフ
539/4625	アカウントがログオンに失敗	ログオン/ログオフ：アカウントがロックアウトされています。	ログオンおよびログオフ
538/4634	アカウントがログオフ	ログオン/ログオフ：ローカルまたはネットワーク ユーザーのログオフ。	ログオンおよびログオフ
560/4656	オブジェクトのオープン / オブジェクトの作成	オブジェクト アクセス：オブジェクト（ファイルまたはディレクトリ）が開いています。	ファイル アクセス
563/4659	削除するためのオブジェクトのオープン	オブジェクト アクセス：削除の意図を持ってオブジェクト（ファイルまたはディレクトリ）へのハンドルが要求されました。	ファイル アクセス
564/4660	オブジェクトの削除	オブジェクト アクセス：オブジェクト（ファイルまたはディレクトリ）の削除。Windows クライアントがオブジェクト（ファイルまたはディレクトリ）を削除しようとしたときに、ONTAP はこのイベントを生成します。	ファイル アクセス

567/4663	オブジェクトの読み取り / オブジェクトの書き込み / オブジェクトの属性の取得 / オブジェクトの属性の設定	オブジェクト アクセス：オブジェクト アクセスの試行（読み取り、書き込み、属性の取得、属性の設定）。 注: このイベントでは、ONTAPはオブジェクトに対する最初のSMB読み取り操作と最初のSMB書き込み操作（成功または失敗）のみを監査します。これにより、単一のクライアントがオブジェクトを開き、同じオブジェクトに対して多数の読み取りまたは書き込み操作を連続して実行した場合に、ONTAPが過剰なログエントリを作成することを回避できます。	ファイル アクセス
NA / 4664	ハード リンク	オブジェクト アクセス：ハード リンクを作成しようとしました。	ファイル アクセス
NA / 4818	提案された集約型アクセス ポリシーで現在の集約型アクセス ポリシーと同じアクセス権限が許可されない	オブジェクト アクセス：Central Access Policy のステージング。	ファイル アクセス
NA / NA Data ONTAP イベントID 9999	オブジェクトの名前変更	オブジェクトアクセス：オブジェクト名が変更されました。これはONTAPイベントです。現在、Windowsでは単一のイベントとしてはサポートされていません。	ファイル アクセス
NA / NA Data ONTAP イベントID 9998	オブジェクトのリンク解除	オブジェクト アクセス：オブジェクトのリンクが解除されました。これは ONTAP イベントです。現在、Windows では単一のイベントとしてはサポートされていません。	ファイル アクセス

イベント**4656**に関する補足情報

監査 `XML`イベントの `HandleID`タグには、アクセスされたオブジェクト（ファイルまたはディレクトリ）のハンドルが含まれます。EVTX 4656イベントの `HandleID`タグには、オープンイベントが新しいオブジェクトの作成用か、既存のオブジェクトを開く用かによって異なる情報が含まれます。

- オープン イベントが新しいオブジェクト（ファイルまたはディレクトリ）を作成するためのオープン要求である場合、監査 XML イベント内の `HandleID`タグには空の `HandleID`が表示されます（例：`<Data Name="HandleID">00000000000000;00;00000000;00000000</Data>`）。

`HandleID`は空です。これは、OPEN（新しいオブジェクトを作成するための）要求が、実際のオブジェクト作成が発生する前、およびハンドルが存在する前に監査されるためです。同じオブジェクトに対する後続の監査イベントには、
`HandleID`タグ内に正しいオブジェクトハンドルがあります。

- オープン イベントが既存のオブジェクトを開くためのオープン要求である場合、監査イベントには、そのオブジェクトの割り当てられたハンドルが HandleID`タグ内に含まれます（例： `<Data Name="HandleID">00000000000401;00;000000ea;00123ed4</Data>）。

ONTAP監査対象オブジェクトへの完全パスを決定する

監査レコードの `<ObjectName>`タグに出力されるオブジェクトパスには、ボリューム名（括弧内）と、そのボリュームのルートからの相対パスが含まれます。ジャンクションパスを含む監査対象オブジェクトの完全パスを特定するには、いくつかの手順を実行する必要があります。

手順

1. 監査イベントの `<ObjectName>`タグを調べて、ボリューム名と監査対象オブジェクトへの相対パスを決定します。

   この例では、ボリューム名は「data1」で、ファイルへの相対パスは /dir1/file.txt：

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

2. 前の手順で決定したボリューム名を使用して、監査対象オブジェクトを含むボリュームのジャンクションパスを決定します：

   この例では、ボリューム名は「data1」であり、監査対象オブジェクトを含むボリュームのジャンクション パスは /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. `<ObjectName>`タグで見つかった相対パスをボリュームのジャンクション パスに追加して、監査対象オブジェクトへの完全パスを決定します。

   この例では、ボリュームのジャンクション パスは次のとおりです：

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

ONTAPのシンボリックリンクとハードリンクの監査について学ぶ

シンボリックリンクとハードリンクを監査する際には、留意すべき特定の考慮事項があります。

監査レコードには、監査対象オブジェクトに関する情報（ `ObjectName`タグで識別される監査対象オブジェクトへのパスを含む）が含まれます。シンボリックリンクとハードリンクのパスが `ObjectName`タグにどのように記録されるかを知っておく必要があります。

シンボリック リンク

シンボリックリンクとは、ターゲットと呼ばれる宛先オブジェクトの位置へのポインタを含む、独立したinodeを持つファイルです。シンボリックリンクを介してオブジェクトにアクセスする場合、ONTAPはシンボリックリンクを自動的に解釈し、ボリューム内のターゲットオブジェクトへの実際の標準的なプロトコル非依存パスをたどります。

以下の出力例には、2つのシンボリックリンクがあり、どちらも `target.txt`という名前のファイルを指しています。シンボリックリンクの1つは相対シンボリックリンクで、もう1つは絶対シンボリックリンクです。どちらかのシンボリックリンクが監査対象の場合、監査イベントの `ObjectName`タグにはファイル `target.txt`へのパスが含まれます。

```
[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
```

ハードリンク

ハードリンクとは、ファイルシステム上の既存のファイルに名前を関連付けるディレクトリエントリです。ハードリンクは、元のファイルのinode位置を指します。ONTAPはシンボリックリンクを解釈するのと同様に、ハードリンクを解釈し、ボリューム内のターゲットオブジェクトへの実際の正規パスをたどります。ハードリンクオブジェクトへのアクセスが監査される場合、監査イベントはハードリンクパスではなく、`ObjectName`タグにこの絶対正規パスを記録します。

ONTAP による代替 NTFS データストリームの監査について学ぶ

NTFS代替データ ストリームがあるファイルを監査する際には、注意が必要ないくつかの考慮事項があります。

監査対象オブジェクトの場所は、 `ObjectName`タグ（パス）と `HandleID`タグ（ハンドル）という2つのタグを使用してイベントレコードに記録されます。ログに記録されているストリーム要求を正しく識別するには、ONTAP が NTFS 代替データストリームについて以下のフィールドに何を記録するかを把握しておく必要があります：

- EVTX ID：4656 イベント（監査イベントのオープンと作成）
  - 代替データ ストリームのパスは `ObjectName`タグに記録されます。
  - 代替データ ストリームのハンドルが `HandleID` タグに記録されます。
- EVTX ID: 4663 イベント（読み取り、書き込み、getattr などのその他のすべての監査イベント）
  - 代替データ ストリームではなく、ベース ファイルのパスが `ObjectName`タグに記録されます。
  - 代替データ ストリームのハンドルが `HandleID` タグに記録されます。

例

次の例は、 `HandleID`タグを使用して代替データストリームのEVTX ID: 4663イベントを識別する方法を示しています。読み取り監査イベントに記録された `ObjectName`タグ（パス）はベースファイルパスを指していますが、 `HandleID`タグを使用することで、イベントが代替データストリームの監査レコードであることを識別できます。

ストリームファイル名は `base_file_name:stream_name`という形式になります。この例では、 `dir1`ディレクトリには以下のパスを持つ代替データストリームを持つベースファイルが含まれています：

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

次のイベント例の出力は省略されており、イベントの一部の出力タグは表示されていません。

EVTX ID 4656（オープン監査イベント）の場合、代替データ ストリームの監査レコード出力には、 `ObjectName`タグに代替データ ストリーム名が記録されます：

```
- <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（読み取り監査イベント）の場合、同じ代替データストリームの監査レコード出力では、

`ObjectName`タグに基本ファイル名が記録されます。ただし、`HandleID`タグ内のハンドルは代替データストリームのハンドルであり、このイベントを代替データストリームと関連付けるために使用できます：

```
- <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>
```