カンサテキル**SMB**イヘント
ONTAP 9

NetApp
December 20, 2024

目次

カンサテキル**SMB**イヘント

カンサテキル**SMB**イヘントノカイヨウ

ONTAPでは、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、特定のSMBイベントを監査できます。どのアクセスイベントを監査できるかを把握しておくと、イベントログの結果を解釈するときに役立ちます。

ONTAP 9 .2以降では、さらに次のSMBイベントを監査できます。

イベント ID （ EVT / EVTX ）	イベント	説明	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	オブジェクトへのアクセス： CAP が変更された。	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	説明	カテゴリ
540/4624	アカウントが正常にログオンしました	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しました	ログオン / ログオフ：ユーザ名が不明またはパスワードが無効です。	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しました	ログオン / ログオフ：アカウントログオンの時間制限です。	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しました	ログオン / ログオフ：アカウントは現在無効になっています。	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しました	ログオン / ログオフ：ユーザ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しました	ログオン / ログオフ：ユーザはこのコンピュータ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しました	ログオン / ログオフ：ユーザはログオンを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しました	ログオン / ログオフ：ユーザのパスワードが期限切れです。	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しました	ログオン / ログオフ：上記以外の理由でログオンが失敗しました。	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しました	ログオン / ログオフ：アカウントのロックアウト。	ログオンおよびログオフ
538/4634	アカウントがログオフされました	ログオン / ログオフ：ローカルまたはネットワークユーザのログオフ。	ログオンおよびログオフ
560/4656	オブジェクトを開く/オブジェクトを作成	オブジェクトへのアクセス：オブジェクト（ファイルまたはディレクトリ）が開きます。	ファイルアクセス
563/4659	削除するためのオブジェクトを開く	オブジェクトへのアクセス：削除するためにオブジェクト（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	オブジェクトへのアクセス：オブジェクト（ファイルまたはディレクトリ）を削除します。ONTAP は、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	オブジェクトへのアクセス：オブジェクトへのアクセスの試み（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 SMB 書き込み操作（の成功または失敗）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連続して多数の読み取りまたは書き込み処理を実行しても、ONTAPが過剰なログエントリを作成するのを防ぐことができます。	ファイルアクセス

NA / 4664	ハードリンク	オブジェクトへのアクセス：ハードリンクの作成が試行されました。	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付与されない	オブジェクトへのアクセス：集約型アクセスポリシーのステージング。	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	オブジェクトへのアクセス：オブジェクトの名前変更。これはONTAPイベントです。Windowsでは現在、単一イベントとして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	オブジェクトへのアクセス：オブジェクトのリンクが解除される。これはONTAPイベントです。Windowsでは現在、単一イベントとしてサポートされていません。	ファイルアクセス

イベント**4656**に関する追加情報

`HandleID`監査イベントのタグ
`XML`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ています。 `HandleID`EVTX
4656イベントのタグには、オープンイベントが新しいオブジェクトを作成するためのものか、既存のオブジェクトを開くためのものかによって、異なる情報が含まれます。

- open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イベントのタグには HandleID`空（例： `<Data Name="HandleID">00000000000000;00;00000000;00000000</Data>）が表示されます HandleID。

  が HandleID`空になっているのは、（新しいオブジェクトを作成するための）OPEN要求が、実際のオブジェクトの作成が行われる前、およびハンドルが存在する前に監査されるためです。同じオブジェクトの後続の監査対象イベントは、タグ内に適切なオブジェクトハンドルを持ちます `HandleID。

- open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タグに含まれ HandleID`ます（例： `<Data Name="HandleID">00000000000401;00;000000ea;00123ed4</Data>）。

監査対象オブジェクトへの完全なパスを特定する

監査レコードのタグに出力されたオブジェクトパス`<ObjectName>`には、ボリュームの名前（かっこ内）と、ボリュームを含むボリュームのルートからの相対パスが表示さ

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決定する場合には、実行する必要がある特定の手順があります。

手順

1. 監査イベントのタグを確認して、ボリューム名と監査対象オブジェクトへの相対パスを確認します `<ObjectName>`。

   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です `/dir1/file.txt`。

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

2. 前の手順で確認したボリューム名を使用して、監査対象オブジェクトが含まれているボリュームのジャンクションパスを確認します。

   この例では、ボリューム名は「data1」で、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です。 `/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. タグ内の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 `<ObjectName>`。

   この例では、ボリュームのジャンクションパスは次のようになります。

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

シンボリックリンクおよびハードリンクを監査する際の考慮事項

シンボリックリンクおよびハードリンクを監査する場合は、一定の考慮事項に注意する必要があります。

監査レコードには、タグで識別される監査対象オブジェクトのパスなど、監査対象オブジェクトに関する情報が含まれます。 `ObjectName`シンボリックリンクおよびハードリンクのパスがタグにどのように記録されるかを確認しておく必要があります `ObjectName`。

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デスティネーションオブジェクトの場所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際、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、プロトコ

ルに依存しない本来のパスに従います。

次の出力例には、2つのシンボリックリンクがあり、どちらもという名前のファイルを指して `target.txt`います。一方のシンボリックリンクは相対シンボリックリンクであり、他方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された場合、 `ObjectName`監査イベントのタグにファイルへのパスが含まれ `target.txt`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 の場所を指しています。ONTAP ONTAP は、シンボリックリンクの解釈方法と同様に、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本来のパスに従います。ハードリンクオブジェクトへのアクセスが監査されると、監査イベントはハードリンクパスではなく、この正規の絶対パスをタグに記録します `ObjectName`。

代替NTFSデータストリームを監査する際の考慮事項

NTFS代替データストリームを含むファイルを監査する場合は、一定の考慮事項に注意する必要があります。

監査対象のオブジェクトの場所は、タグ（パス）とタグ（ハンドル）の `HandleID`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 `ObjectName`。ログに記録されているストリーム要求を適切に識別するには、NTFS代替データストリームの次のフィールドにONTAPが記録するものに注意する必要があります。

- EVTX ID ： 4656 のイベント（オープンおよび作成の監査イベント）
  - 代替データストリームのパスはタグに記録され `ObjectName`ます。
  - 代替データストリームのハンドルはタグに記録され `HandleID`ます。
- EVTX ID ： 4663 のイベント（読み取り、書き込み、属性の取得など、その他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タグに記録され `ObjectName`ます。
  - 代替データストリームのハンドルはタグに記録され `HandleID`ます。

例

次の例は、タグを使用して代替データストリームのEVTX ID：4663イベントを特定する方法を示してい `HandleID`ます。 `ObjectName`読み取り監査イベントで記録されたタグ（パス）はベースファイルパスに対するものですが、 `HandleID`タグを使用すると、代替データストリームの監査レコードとしてイベントを識別できます。

ストリームファイル名はの形式になり `base_file_name:stream_name`ます。この例では、 `dir1`次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ディレクトリに含まれています。

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

次のイベント例の出力は、示されているように省略されています。出力には、イベントで使用可能なすべての出力タグが表示されるわけではありません。

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では、代替データストリーム名がタグに記録され `ObjectName`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、ベースファイル名がタグに記録され `ObjectName`ます。ただし、タグ内のハンドルは `HandleID`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>
```

著作権に関する情報

商標に関する情報