監査できる SMB イベント

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/ontap/nas-audit/smb-events-audit-concept.html on April 24, 2024. Always check docs.netapp.com for the latest.

目次

監査できる SMB イベント 1
監査できる SMB イベントの概要 1
監査対象オブジェクトへの完全なパスを決定します 4
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 5
代替 NTFS データストリームを監査する際の考慮事項 5

監査できる SMB イベント

監査できる SMB イベントの概要

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。

ONTAP 9.2 以降では、次の SMB イベントが監査対象として追加されました。

イベント ID （ EVT / EVTX ）	イベント	説明	カテゴリ
4670	オブジェクト権限が変更されました	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が変更されました	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が変更されました	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	アカウントがログオンに成功しました	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.	削除するために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	オブジェクトを削除します	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）の削除を試みると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、 1 つのクライアントが、あるオブジェクトを開き、そのオブジェクトに対して連続的に多数の読み取りまたは書き込みを行っても、 ONTAP が余計にログエントリを書き込むことがなくなります。	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は、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ません	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	オブジェクト名を変更します	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` 監査でタグを付けます `XML` イベントには、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。。 `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は、 `HandleID` 監査XMLイベントのタグに空が表示されます `HandleID` （例： `<Data Name="HandleID">00000000000000;00;00000000;00000000</Data>` ）。

。 HandleID が空の理由は、（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、で適切なオブジェクトハンドルを持ちます HandleID タグ。

- 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、でそのオブジェクトの割り当てられたハンドルが割り当てられます HandleID タグ（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決定します

に出力されたオブジェクトパス <ObjectName> 監査レコードのタグには、ボリュームの名前（かっこ内）と、その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. を参照して、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> 監査イベントのタグ。

   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」、監査対象オブジェクトが含まれる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. で見つかった相対パスを追加して、監査対象オブジェクトへの完全パスを決定します <ObjectName> ボリュームのジャンクションパスにタグを付けます。

   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、で識別される監査対象オブジェクトへのパスなど、監査対象オブジェクトに関する情報が含まれます `ObjectName` タグ。シンボリックリンクおよびハードリンクのパスが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` タグ。

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います `target.txt`。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は、が実行されます `ObjectName` 監査イベントのタグにファイルへのパスが含まれています `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
```

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、監査イベントはこの正規の絶対パスをに記録します `ObjectName` ハードリンクパスではなくタグを付けます。

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持つ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、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` タグ（パス）および `HandleID` タグ（ハンドル）。ログに記録され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でこれらのフィールドに記録される ONTAP レコードを把握しておく必要があります。

- 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に記録されます `ObjectName` タグ。
  - 代替データストリームのハンドルはに記録されます `HandleID` タグ。
- 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に記録されます `ObjectName` タグ。
  - 代替データストリームのハンドルはに記録されます `HandleID` タグ。

例

次の例は、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ます `HandleID` タグ。にもかかわらず `ObjectName` 読み取り監査イベントで記録されるタグ（パス）は、ベースファイルパスであるへのパスです `HandleID` タグを使用すると、イベントを代替データストリームの監査レコードとして識別できます。

ストリームファイル名はの形式になります `base_file_name:stream_name`。この例では、を使用しています `dir1` ディレクトリには、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ご覧のように省略されています。この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てい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に代替データストリーム名が記録されます `ObjectName` タグ：

```
- <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にベースファイル名が記録されます `ObjectName` タグ。ただし、のハンドル `HandleID` タグ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>
```

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。