Événements SMB pouvant être audités

ONTAP 9

NetApp
September 12, 2024

Sommaire

Événements SMB pouvant être audités

Événements SMB pouvant être audités

ONTAP peut auditer certains événements SMB, notamment certains événements d'accès aux fichiers et aux dossiers, certains événements de connexion et de déconnexion, et des événements d'activation des règles d'accès central. Savoir quels événements d'accès peuvent être audités est utile pour interpréter les résultats des journaux d'événements.

Les événements SMB supplémentaires suivants peuvent être audités dans ONTAP 9.2 et versions ultérieures :

ID D'ÉVÉNEMENT (EVT/EVTX)	Événement	Description	Catégorie
4670	Les autorisations d'objet ont été modifiées	ACCÈS AUX OBJETS : autorisations modifiées.	Accès aux fichiers
4907	Les paramètres d'audit d'objet ont été modifiés	ACCÈS À L'OBJET : paramètres d'audit modifiés.	Accès aux fichiers
4913	La stratégie d'accès à Object Central a été modifiée	ACCÈS À L'OBJET : BOUCHON MODIFIÉ.	Accès aux fichiers

Les événements SMB suivants peuvent être audités dans ONTAP 9.0 et versions ultérieures :

ID D'ÉVÉNEMENT (EVT/EVTX)	Événement	Description	Catégorie
540/4624	Un compte a été connecté avec succès	CONNEXION/DÉCONNEXION : connexion réseau (SMB).	Connexion et déconnexion
529/4625	Impossible de se connecter à un compte	CONNEXION/DÉCONNEXION : nom d'utilisateur inconnu ou mot de passe incorrect.	Connexion et déconnexion
530/4625	Impossible de se connecter à un compte	OUVERTURE/FERMETURE de SESSION : restriction de l'heure de connexion au compte.	Connexion et déconnexion
531/4625	Impossible de se connecter à un compte	CONNEXION/DÉCONNEXION : compte actuellement désactivé.	Connexion et déconnexion
532/4625	Impossible de se connecter à un compte	OUVERTURE/FERMETURE DE SESSION : le compte utilisateur a expiré.	Connexion et déconnexion

533/4625	Impossible de se connecter à un compte	OUVERTURE/FERMETURE DE SESSION : l'utilisateur ne peut pas se connecter à cet ordinateur.	Connexion et déconnexion
534/4625	Impossible de se connecter à un compte	OUVERTURE DE SESSION/DÉCONNEXION : l'utilisateur n'a pas accordé de type de connexion ici.	Connexion et déconnexion
535/4625	Impossible de se connecter à un compte	OUVERTURE/FERMETURE DE SESSION : le mot de passe de l'utilisateur a expiré.	Connexion et déconnexion
537/4625	Impossible de se connecter à un compte	OUVERTURE/FERMETURE de SESSION : la connexion a échoué pour des raisons autres que ci-dessus.	Connexion et déconnexion
539/4625	Impossible de se connecter à un compte	OUVERTURE DE SESSION/DÉCONNEXION : compte verrouillé.	Connexion et déconnexion
538/4634	Un compte a été déconnecté	OUVERTURE/FERMETURE DE SESSION : déconnexion de l'utilisateur local ou réseau.	Connexion et déconnexion
560/4656	Ouvrir objet/Créer objet	ACCÈS EN MODE OBJET : objet (fichier ou répertoire) ouvert.	Accès aux fichiers
563/4659	Ouvrez l'objet avec l'intention de supprimer	ACCÈS AUX OBJETS : un descripteur d'objet (fichier ou répertoire) a été demandé avec l'intention de supprimer.	Accès aux fichiers
564/4660	Supprimer l'objet	ACCÈS OBJET : supprimer l'objet (fichier ou répertoire). ONTAP génère cet événement lorsqu'un client Windows tente de supprimer l'objet (fichier ou répertoire).	Accès aux fichiers

567/4663	Lire objet/Ecrire objet/obtenir attributs d'objet/définir attributs d'objet	ACCÈS AUX OBJETS : tentative d'accès aux objets (lecture, écriture, obtenir l'attribut, définir l'attribut). **Remarque :** pour cet événement, ONTAP vérifie uniquement la première opération de lecture SMB et la première opération d'écriture SMB (succès ou échec) sur un objet. Cela empêche ONTAP de créer un nombre excessif d'entrées de journal lorsqu'un seul client ouvre un objet et effectue de nombreuses opérations de lecture ou d'écriture successives sur le même objet.	Accès aux fichiers
NA/4664	Lien dur	ACCÈS À L'OBJET : tentative de création d'un lien dur.	Accès aux fichiers
NA/4818	La politique d'accès central proposée n'accorde pas les mêmes autorisations d'accès que la politique d'accès central actuelle	ACCÈS AUX OBJETS : transfert de la stratégie d'accès central.	Accès aux fichiers
Na/NA - ID d'événement Data ONTAP 9999	Renommer l'objet	ACCÈS OBJET : objet renommé. Il s'agit d'un événement ONTAP. Windows ne prend actuellement pas en charge cet événement en tant qu'événement unique.	Accès aux fichiers
Na/NA Data ONTAP ID d'événement 9998	Dissocier l'objet	ACCÈS AUX OBJETS : objet non lié. Il s'agit d'un événement ONTAP. Windows ne prend actuellement pas en charge cet événement en tant qu'événement unique.	Accès aux fichiers

Informations supplémentaires sur l'événement 4656

Le `HandleID` dans l'audit `XML` event contient le descripteur de l'objet (fichier ou répertoire) accédé. Le `HandleID` La balise de l'événement EVTX 4656 contient des informations différentes selon que l'événement ouvert permet de créer un nouvel objet ou d'ouvrir un objet existant :

- Si l'événement ouvert est une demande ouverte pour créer un nouvel objet (fichier ou répertoire), le `HandleID` La balise dans l'événement XML d'audit affiche un vide `HandleID` (par exemple : `<Data Name="HandleID">00000000000000;00;00000000;00000000</Data>`).

  Le `HandleID` Est vide car la demande OUVERTE (pour la création d'un nouvel objet) est auditée avant la création réelle de l'objet et avant qu'un descripteur n'existe. Les événements audités suivants pour le même objet ont le bon descripteur d'objet dans le `HandleID` balise :

- Si l'événement ouvert est une demande ouverte d'ouverture d'un objet existant, l'événement d'audit aura le descripteur affecté à cet objet dans le `HandleID` balise (par exemple : `<Data Name="HandleID">00000000000401;00;000000ea;00123ed4</Data>`).

Déterminez le chemin complet de l'objet vérifié

Le chemin d'accès de l'objet imprimé dans `<ObjectName>` la balise d'un enregistrement d'audit contient le nom du volume (entre parenthèses) et le chemin relatif de la racine du volume contenant. Si vous voulez déterminer le chemin complet de l'objet vérifié, y compris le chemin de jonction, il y a certaines étapes que vous devez suivre.

Étapes

1. Déterminez ce que correspond le nom du volume et le chemin relatif de l'objet vérifié en consultant le `<ObjectName>` balise dans l'événement d'audit.

   Dans cet exemple, le nom du volume est "data1" et le chemin relatif vers le fichier est `/dir1/file.txt`:

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

2. En utilisant le nom du volume déterminé à l'étape précédente, déterminez ce qu'est la Junction path du volume contenant l'objet vérifié :

   Dans cet exemple, le nom du volume est "data1" et le chemin de jonction du volume contenant l'objet vérifié est `/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. Déterminez le chemin d'accès complet à l'objet vérifié en ajoutant le chemin d'accès relatif trouvé dans le `<ObjectName>` marquez la junction path du volume.

   Dans cet exemple la Junction path du volume :

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

Considérations relatives à l'audit des liens symlinks et des liens matériels

Il y a certaines considérations que vous devez garder à l'esprit lors de l'audit des liens symlinks et des liens matériels.

Un enregistrement d'audit contient des informations sur l'objet en cours d'audit, y compris le chemin d'accès à

l'objet vérifié, qui est identifié dans le `ObjectName` balise : Vous devez savoir comment les chemins pour les liens symlinks et les liens rigides sont enregistrés dans le `ObjectName` balise :

Symlinks

Un symlink est un fichier avec un inode séparé qui contient un pointeur vers l'emplacement d'un objet de destination, appelé cible. Lors de l'accès à un objet via une symlink, ONTAP interprète automatiquement la symlink et suit le chemin canonique réel de protocole indépendant vers l'objet cible dans le volume.

Dans l'exemple de sortie suivant, il y a deux symlinks, tous deux pointant vers un fichier nommé `target.txt`. Un des symlinks est un symlink relatif et un est un symlink absolu. Si l'un des symlinks est vérifié, le `ObjectName` la balise de l'événement d'audit contient le chemin d'accès au fichier `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
```

Liens matériels

Un lien dur est une entrée de répertoire qui associe un nom à un fichier existant sur un système de fichiers. Le lien matériel pointe vers l'emplacement d'inode du fichier d'origine. De la même manière que ONTAP interprète les symlinks, ONTAP interprète le lien rigide et suit le chemin canonique réel vers l'objet cible dans le volume. Lorsque l'accès à un objet de lien rigide est vérifié, l'événement d'audit enregistre ce chemin canonique absolu dans l' `ObjectName` marquez plutôt que le chemin du lien dur.

Points à prendre en compte lors de l'audit des autres flux de données NTFS

Vous devez garder à l'esprit certaines considérations lors de l'audit des fichiers avec les autres flux de données NTFS.

L'emplacement d'un objet vérifié est enregistré dans un enregistrement d'événement à l'aide de deux balises, le `ObjectName` tag (le chemin) et le `HandleID` étiquette (la poignée). Pour identifier correctement les demandes de flux en cours de journalisation, vous devez connaître les enregistrements ONTAP dans ces champs pour les flux de données alternatifs NTFS :

- EVTX ID : 4656 événements (ouvrir et créer des événements d'audit)
  - Le chemin du flux de données secondaire est enregistré dans le `ObjectName` balise :
  - La poignée du flux de données alternatif est enregistrée dans le `HandleID` balise :
- EVTX ID : 4663 événements (tous les autres événements d'audit, tels que lecture, écriture, getattr, etc.)
  - Le chemin du fichier de base, et non le flux de données secondaire, est enregistré dans le `ObjectName` balise :
  - La poignée du flux de données alternatif est enregistrée dans le `HandleID` balise :

Exemple

L'exemple suivant illustre comment identifier EVTX ID : 4663 événements pour d'autres flux de données à l'aide de l' `HandleID` balise : Même si le `ObjectName` la balise (chemin) enregistrée dans l'événement d'audit de lecture correspond au chemin du fichier de base, le `HandleID` la balise peut être utilisée pour identifier l'événement comme enregistrement d'audit pour le flux de données secondaire.

Les noms des fichiers de flux prennent le format `base_file_name:stream_name`. Dans cet exemple, le `dir1` le répertoire contient un fichier de base avec un autre flux de données ayant les chemins suivants :

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

> La sortie dans l'exemple d'événement suivant est tronquée comme indiqué ; la sortie n'affiche pas toutes les balises de sortie disponibles pour les événements.

Pour un EVTX ID 4656 (événement d'audit ouvert), la sortie de l'enregistrement d'audit du flux de données secondaire enregistre le nom du flux de données alternatif dans le `ObjectName` tag :

```
- <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>
```

Pour un EVTX ID 4663 (lecture d'événement d'audit), la sortie de l'enregistrement d'audit du même flux de données alternatif enregistre le nom du fichier de base dans le `ObjectName` marquez, cependant, la poignée dans le `HandleID` tag est la poignée du flux de données alternatif et peut être utilisé pour mettre en corrélation cet événement avec l'autre flux de données :

```
- <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>
```