



SMB-Ereignisse, die geprüft werden können

ONTAP 9

NetApp
February 12, 2026

Inhalt

- SMB-Ereignisse, die geprüft werden können 1
 - Informieren Sie sich über SMB-Ereignisse, die ONTAP prüfen kann, um die Ergebnisse zu interpretieren . . 1
 - Weitere Informationen zu Event 4656 3
 - Bestimmen Sie den vollständigen Pfad zum überwachten ONTAP-Objekt 4
 - Erfahren Sie mehr über ONTAP Auditing von Symlinks und Hard Links 5
 - Symlinks 5
 - Feste Verbindungen 5
 - Erfahren Sie mehr über das ONTAP-Auditing von alternativen NTFS-Datenströmen 5

SMB-Ereignisse, die geprüft werden können

Informieren Sie sich über SMB-Ereignisse, die ONTAP prüfen kann, um die Ergebnisse zu interpretieren

ONTAP kann bestimmte SMB-Ereignisse überprüfen, einschließlich bestimmter Datei- und Ordnerzugriffsereignisse, bestimmter Anmelde- und Abmeldungsereignisse sowie zentrale Staging von Zugriffsrichtlinien. Das Wissen, welche Zugriffsereignisse auditiert werden können, ist hilfreich bei der Interpretation der Ergebnisse aus den Ereignisprotokollen.

Die folgenden zusätzlichen SMB-Ereignisse können überwacht werden:

EREIGNIS-ID (EVT/EVTX)	Ereignis	Beschreibung	Kategorie
4670	Objektberechtigungen wurden geändert	OBJEKTZUGRIFF: Berechtigungen geändert.	Dateizugriff
4907	Objektaudits-Einstellungen wurden geändert	OBJEKTZUGRIFF: Audit-Einstellungen geändert.	Dateizugriff
4913	Objektzugriffsrichtlinie wurde geändert	OBJEKTZUGRIFF: KAPPE GEÄNDERT.	Dateizugriff

Die folgenden SMB Ereignisse können im ONTAP 9.0 und höher geprüft werden:

EREIGNIS-ID (EVT/EVTX)	Ereignis	Beschreibung	Kategorie
540/4624	Ein Konto wurde erfolgreich angemeldet	ANMELDUNG/ABMELDUNG: Netzwerk (SMB)-Anmeldung	Anmeldung und Anmeldung
529/4625	Ein Konto konnte sich nicht anmelden	ANMELDUNG/ABMELDUNG: Unbekannter Benutzername oder schlechtes Passwort.	Anmeldung und Anmeldung
530/4625	Ein Konto konnte sich nicht anmelden	ANMELDUNG/ABMELDUNG: Einschränkung der Anmeldezeit des Kontos.	Anmeldung und Anmeldung
531/4625	Ein Konto konnte sich nicht anmelden	ANMELDUNG/ABMELDUNG: Konto derzeit deaktiviert.	Anmeldung und Anmeldung
532/4625	Ein Konto konnte sich nicht anmelden	ANMELDUNG/ABMELDEN: Benutzerkonto abgelaufen.	Anmeldung und Anmeldung

533/4625	Ein Konto konnte sich nicht anmelden	ANMELDUNG/ABMELDUNG: Benutzer kann sich nicht bei diesem Computer anmelden.	Anmeldung und Anmeldung
534/4625	Ein Konto konnte sich nicht anmelden	ANMELDUNG/ABMELDUNG: Der Benutzer hat hier keinen Logon-Typ erhalten.	Anmeldung und Anmeldung
535/4625	Ein Konto konnte sich nicht anmelden	ANMELDUNG/ABMELDUNG: Das Kennwort des Benutzers ist abgelaufen.	Anmeldung und Anmeldung
537/4625	Ein Konto konnte sich nicht anmelden	ANMELDUNG/ABMELDUNG: Anmeldung aus anderen als den oben genannten Gründen fehlgeschlagen.	Anmeldung und Anmeldung
539/4625	Ein Konto konnte sich nicht anmelden	ANMELDUNG/ABMELDUNG: Konto gesperrt.	Anmeldung und Anmeldung
538/4634	Ein Konto wurde abgemeldet	ANMELDUNG/ABMELDUNG: Lokale oder Netzwerk-Benutzer abmelden.	Anmeldung und Anmeldung
560/4656	Objekt Öffnen/Objekt Erstellen	OBJEKTZUGRIFF: Objekt (Datei oder Verzeichnis) geöffnet.	Dateizugriff
563/4659	Objekt öffnen mit dem zu löschenden Ziel	OBJEKTZUGRIFF: Ein Handle zu einem Objekt (Datei oder Verzeichnis) wurde mit dem Ziel zum Löschen angefordert.	Dateizugriff
564/4660	Objekt Löschen	OBJEKTZUGRIFF: Objekt löschen (Datei oder Verzeichnis). ONTAP generiert dieses Ereignis, wenn ein Windows-Client versucht, das Objekt (Datei oder Verzeichnis) zu löschen.	Dateizugriff

567/4663	Objekt Lesen/Objekt Schreiben/Objekt-Attribute Abrufen/Objekt-Attribute Festlegen	OBJEKTZUGRIFF: Objektzugriffsversuch (Lesen, Schreiben, get attribut, set attribut). Hinweis: bei diesem Event prüft ONTAP nur den ersten SMB-Lesevorgang und den ersten SMB-Schreibvorgang (Erfolg oder Fehler) auf einem Objekt. Dadurch wird verhindert, dass ONTAP übermäßige Protokolleinträge erstellt, wenn ein einzelner Client ein Objekt öffnet und viele aufeinanderfolgende Lese- oder Schreibvorgänge an demselben Objekt durchführt.	Dateizugriff
NA/4664	Harter Link	OBJEKTZUGRIFF: Es wurde versucht, eine harte Verbindung zu erstellen.	Dateizugriff
NA/4818	Die vorgeschlagene zentrale Zugangsrichtlinie gewährt nicht dieselben Zugriffsberechtigungen wie die aktuelle zentrale Zugangsrichtlinie	OBJEKTZUGRIFF: Zentrale Zugriffsrichtlinien-Staging.	Dateizugriff
NA/NA Data ONTAP Ereignis-ID 9999	Objekt Umbenennen	OBJEKTZUGRIFF: Objekt umbenannt. Dies ist ein ONTAP-Event. Derzeit wird es von Windows nicht als einzelnes Ereignis unterstützt.	Dateizugriff
NA/NA Data ONTAP Ereignis-ID 9998	Verknüpfung Des Objekts Aufheben	OBJEKTZUGRIFF: Objekt wird nicht verknüpft. Dies ist ein ONTAP-Event. Derzeit wird es von Windows nicht als einzelnes Ereignis unterstützt.	Dateizugriff

Weitere Informationen zu Event 4656

Das `HandleID` Tag im Überwachungsereignis XML enthält das Handle des Objekts (Datei oder Verzeichnis), auf das zugegriffen wird. Das `HandleID` Tag für das EVT-X 4656-Ereignis enthält unterschiedliche Informationen, je nachdem, ob das offene Ereignis zum Erstellen eines neuen Objekts oder zum Öffnen eines vorhandenen Objekts dient:

- Wenn das offene Ereignis eine offene Anforderung ist, ein neues Objekt (Datei oder Verzeichnis) zu erstellen, `HandleID` zeigt das Tag im XML-Audit-Ereignis ein leeres `HandleID` (z.B.: `<Data Name="HandleID">0000000000000000;00;00000000;00000000</Data>`) An.

Der `HandleID` ist leer, da die OFFENE (zum Erstellen eines neuen Objekts) Anforderung vor der eigentlichen Objekterstellung und vor dem Vorhandensein eines Handles geprüft wird. Nachfolgende

überwachte Ereignisse für dasselbe Objekt haben das richtige Objekthandle im HandleID Tag.

- Wenn das offene Ereignis eine offene Anforderung zum Öffnen eines vorhandenen Objekts ist, hat das Audit-Ereignis das zugewiesene Handle dieses Objekts im HandleID Tag (z.B.: <Data Name="HandleID">000000000000401;00;000000ea;00123ed4</Data>).

Bestimmen Sie den vollständigen Pfad zum überwachten ONTAP-Objekt

Der im <ObjectName> Tag für einen Audit-Datensatz gedruckte Objektpfad enthält den Namen des Volumes (in Klammern) und den relativen Pfad vom Stammverzeichnis des enthaltenen Volumes. Wenn Sie den vollständigen Pfad des geprüften Objekts einschließlich des Verbindungspfades bestimmen möchten, müssen Sie bestimmte Schritte durchführen.

Schritte

1. Ermitteln Sie den Namen des Volumes und den relativen Pfad zum überwachten Objekt, indem Sie das <ObjectName> Tag im Überwachungsereignis betrachten.

In diesem Beispiel ist der Datenträgername "data1" und der relative Pfad zur Datei lautet /dir1/file.txt:

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

2. Anhand des im vorherigen Schritt festgelegten Volume-Namens bestimmen Sie, was der Verbindungspfad für das Volume ist, das das geprüfte Objekt enthält:

In diesem Beispiel lautet der Volumename „data1“ und der Verbindungspfad für das Volume, das das überwachte Objekt enthält, lautet /data/data1:

```
volume show -junction -volume data1
```

Vserver	Volume	Junction		Junction Path	Junction Path Source
		Language	Active		
vs1	data1	en_US.UTF-8	true	/data/data1	RW_volume

3. Bestimmen Sie den vollständigen Pfad zum geprüften Objekt, indem Sie den relativen Pfad <ObjectName>, der im Tag gefunden wurde, an den Verbindungspfad für das Volume anhängen.

In diesem Beispiel ist der Verbindungspfad für das Volume:

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

Erfahren Sie mehr über ONTAP Auditing von Symlinks und Hard Links

Es gibt bestimmte Überlegungen, die Sie bei der Prüfung von Symlinks und harten Links beachten müssen.

Ein Audit-Datensatz enthält Informationen über das zu überwachende Objekt, einschließlich des Pfads zum überwachten Objekt, der im `ObjectName` Tag identifiziert wird. Sie sollten wissen, wie Pfade für Symlinks und harte Links im `ObjectName` Tag aufgezeichnet werden.

Symlinks

Ein Symlink ist eine Datei mit einer separaten Inode, die einen Zeiger auf den Speicherort eines Zielobjekts enthält, das als Ziel bezeichnet wird. Beim Zugriff auf ein Objekt über einen Symlink interpretiert ONTAP automatisch den Symlink und folgt dem tatsächlichen kanonischen protokollunabhängigen Pfad zum Zielobjekt im Volume.

In der folgenden Beispielausgabe gibt es zwei Symlinks, die beide auf eine Datei mit dem Namen `target.txt` verweisen. Einer der Symlinks ist ein relativer Symlink und einer ist ein absolutes Symlink. Wenn einer der Symlinks auditiert ist, `ObjectName` enthält das Tag im Audit-Ereignis den Pfad zur Datei `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
```

Feste Verbindungen

Eine harte Verbindung ist ein Verzeichniseintrag, der einen Namen mit einer vorhandenen Datei auf einem Dateisystem verknüpft. Die harte Verbindung verweist auf den Inode-Speicherort der Originaldatei. Ähnlich wie ONTAP Symlinks interpretiert, interpretiert ONTAP die harte Verbindung und folgt dem eigentlichen kanonischen Pfad zum Zielobjekt im Volume. Wenn der Zugriff auf ein hartes Link-Objekt überwacht wird, zeichnet das Audit-Ereignis diesen absoluten kanonischen Pfad im `ObjectName` Tag statt im Pfad für die harte Verknüpfung auf.

Erfahren Sie mehr über das ONTAP-Auditing von alternativen NTFS-Datenströmen

Beim Auditing von Dateien mit alternativen NTFS-Datenströmen müssen Sie bestimmte Überlegungen beachten.

Die Position eines zu überwachenden Objekts wird in einem Ereignisdatensatz mit zwei Tags, dem `ObjectName` Tag (dem Pfad) und dem `HandleID` Tag (dem Handle) aufgezeichnet. Um die zu protokollierenden Stream-Anforderungen richtig zu ermitteln, müssen Sie sich bewusst sein, welche ONTAP-Datensätze in diesen Feldern für NTFS-alternative Datenströme enthalten sind:

- EVTX-ID: 4656 Ereignisse (Öffnen und Erstellen von Audit-Ereignissen)
 - Der Pfad des alternativen Datenstroms wird im `ObjectName` Tag aufgezeichnet.
 - Das Handle des alternativen Datenstroms wird im `HandleID` Tag aufgezeichnet.
- EVTX-ID: 4663 Ereignisse (alle anderen Audit-Ereignisse, wie Lesen, Schreiben, getattr usw.)
 - Der Pfad der Basisdatei, nicht der alternative Datenstrom, wird im `ObjectName` Tag aufgezeichnet.
 - Das Handle des alternativen Datenstroms wird im `HandleID` Tag aufgezeichnet.

Beispiel

Das folgende Beispiel zeigt, wie man EVTX ID identifiziert: 4663 Ereignisse für alternative Datenströme mit dem `HandleID` Tag. Obwohl das `ObjectName` im Ereignis „Leseprüfung“ aufgezeichnete Tag (Pfad) auf den Pfad der Basisdatei zutrifft, `HandleID` kann das Tag verwendet werden, um das Ereignis als Überwachungsdatensatz für den alternativen Datenstrom zu identifizieren.

Stream-Dateinamen nehmen das Formular `base_file_name:stream_name`. In diesem Beispiel `dir1` enthält das Verzeichnis eine Basisdatei mit einem alternativen Datenstrom, der die folgenden Pfade hat:

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



Die Ausgabe im folgenden Ereignisbeispiel wird wie angegeben abgeschnitten; in der Ausgabe werden nicht alle verfügbaren Ausgabetags für die Ereignisse angezeigt.

Bei einer EVTX-ID 4656 (offenes Audit-Ereignis) zeichnet die Ausgabe des Audit-Datensatzes für den alternativen Datenstrom den alternativen Datenstromnamen im `ObjectName` Tag auf:

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4656</EventID>
  <EventName>Open Object</EventName>
  [...]
</System>
- <EventData>
  [...]
  **<Data Name="ObjectType">Stream</Data>
  <Data Name="HandleID">000000000000401;00;000001e4;00176767</Data>
  <Data Name="ObjectName">\(data1\);/dir1/file1.txt:stream1</Data>
  **
  [...]
</EventData>
</Event>
- <Event>
```

Bei einer EVTX-ID 4663 (Leseaudit-Ereignis) zeichnet die Ausgabe des Audit-Datensatzes für denselben

alternativen Datenstrom den Basisdateinamen im `ObjectName` Tag auf. Der `Handle` im `HandleID` Tag ist jedoch der `Handle` des alternativen Datenstroms und kann verwendet werden, um dieses Ereignis mit dem alternativen Datenstrom zu korrelieren:

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4663</EventID>
  <EventName>Read Object</EventName>
  [...]
</System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>000000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt</Data\> **
  [...]
</EventData>
</Event>
- <Event>
```

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.