



# **Prüfung von NAS-Ereignissen auf SVMs**

## **ONTAP 9**

NetApp  
September 12, 2024

# Inhalt

|  |    |
|--|----|
| Prüfung von NAS-Ereignissen auf SVMs .....   | 1  |
| SMB- und NFS-Auditing und Sicherheits-Tracing .....  | 1  |
| Funktionsweise des Audits .....  | 2  |
| Anforderungen und Überlegungen des Audits .....  | 5  |
| Einschränkungen für die Größe von Prüfdatensätzen für Staging-Dateien .....                  | 6  |
| Die unterstützten Audit-Ereignisprotokollformate .....                                       | 7  |
| Anzeigen von Audit-Ereignisprotokollen .....   | 7  |
| SMB-Ereignisse, die geprüft werden können .....  | 8  |
| Es können NFS-Datei- und Verzeichniszugriffe geprüft werden .....                            | 15 |
| Planen der Überwachungskonfiguration .....   | 16 |
| Erstellen einer Datei- und Verzeichnisüberprüfung auf SVMs .....                             | 23 |
| Audit-Richtlinien für Dateien und Ordner konfigurieren .....                                 | 26 |
| Informationen über auf Dateien und Verzeichnisse angewandte Audit-Richtlinien anzeigen ..... | 30 |
| Änderungseignisse in der CLI, die geprüft werden können .....                                | 37 |
| Management von Audit-Konfigurationen .....   | 44 |
| Fehlerbehebung bei Problemen mit Auditing und Staging von Volume-Speicherplatz .....         | 49 |

# Prüfung von NAS-Ereignissen auf SVMs

## SMB- und NFS-Auditing und Sicherheits-Tracing

Zudem können die mit ONTAP verfügbaren Auditing-Funktionen für Dateizugriffe über SMB und NFS verwendet werden, beispielsweise von nativen Audits und Dateirichtlinien-Management über FPolicy.

Unter den folgenden Umständen sollten Audits für SMB- und NFS-Dateizugriffe entworfen und implementiert werden:

- Der grundlegende Dateizugriff über SMB und NFS wurde konfiguriert.
- Sie möchten eine Überwachungskonfiguration mit einer der folgenden Methoden erstellen und verwalten:
  - Native ONTAP Funktionalität
  - Externe FPolicy Server

## Prüfung von NAS-Ereignissen auf SVMs

Das Auditing von NAS-Ereignissen ist eine Sicherheitsmaßnahme, mit der Sie bestimmte SMB- und NFS-Ereignisse auf Storage Virtual Machines (SVMs) nachverfolgen und protokollieren können. So können Sie potenzielle Sicherheitsprobleme verfolgen und Sicherheitsverletzungen nachweisen. Außerdem können Sie zentrale Active Directory-Zugriffsrichtlinien erstellen und prüfen, um zu sehen, welche Ergebnisse diese implementieren würden.

### SMB-Ereignisse

Sie können die folgenden Ereignisse prüfen:

- SMB-Datei- und Ordnerzugriff

SMB-Datei- und Ordnerzugriffe auf Objekte prüfen, die in FlexVol Volumes gespeichert sind, die zu prüfenden SVMs gehören.

- SMB-Anmeldung und -Abmeldung

Sie können SMB-Anmeldeereignisse und Abmeldeereignisse für SMB-Server auf SVMs prüfen.

- Staging von zentralen Zugriffsrichtlinien

Sie können den effektiven Zugriff auf Objekte auf SMB-Servern anhand von Berechtigungen überprüfen, die anhand vorgeschlagener, zentraler Zugriffsrichtlinien angewendet werden. Das Auditing durch die Durchführung von zentralen Zugriffsrichtlinien ermöglicht es Ihnen, die Auswirkungen zentraler Zugriffsrichtlinien zu sehen, bevor sie bereitgestellt werden.

Das Auditing von zentralen Zugriffsrichtlinien-Staging wird über Active Directory GPOs eingerichtet. Die SVM-Auditing-Konfiguration muss jedoch für das Auditing von Staging von zentralen Zugriffsrichtlinien konfiguriert werden.

Obwohl Sie die zentrale Zugriffsrichtlinien-Staging in der Überwachungskonfiguration aktivieren können, ohne die dynamische Zugriffskontrolle auf dem SMB-Server zu aktivieren, werden zentrale Zugriffsrichtlinien-Staging-Ereignisse nur erzeugt, wenn Dynamic Access Control aktiviert ist. Die

dynamische Zugriffskontrolle wird über eine SMB-Serveroption aktiviert. Sie ist standardmäßig nicht aktiviert.

## NFS-Ereignisse

Sie können Datei- und Verzeichnisereignisse prüfen, indem Sie die NFSv4-ACL auf Objekten verwenden, die auf SVMs gespeichert sind.

# Funktionsweise des Audits

## Grundlegende Prüfungskonzepte

Um das Auditing in ONTAP zu verstehen, sollten Sie einige grundlegende Prüfungskonzepte kennen.

- **Staging-Dateien**

Die zwischenliegenden Binärdateien auf einzelnen Knoten, in denen Audit-Datensätze vor der Konsolidierung und Konvertierung gespeichert werden. Staging-Dateien sind in Staging-Volumes enthalten.

- **Staging Volumen**

Ein von ONTAP erstelltes dediziertes Volume zum Speichern von Staging-Dateien. Es gibt ein Staging-Volume pro Aggregat. Staging Volumes werden von allen revisionssichere Storage Virtual Machines (SVMs) gemeinsam genutzt, um Audit-Datensätze des Datenzugriffs für Daten-Volumes im jeweiligen Aggregat zu speichern. Die Audit-Datensätze jeder SVM werden in einem separaten Verzeichnis innerhalb des Staging-Volume gespeichert.

Cluster-Administratoren können Informationen über Staging Volumes anzeigen, die meisten anderen Volume-Vorgänge sind jedoch nicht zulässig. Nur ONTAP kann Staging-Volumes erstellen. ONTAP weist Staging-Volumes automatisch einen Namen zu. Alle Staging-Volume-Namen beginnen mit MDV\_aud\_ Anschließend die UUID des Aggregats, welches das Staging-Volume enthält (z. B.: MDV\_aud\_1d0131843d4811e296fc123478563412.)

- **System-Volumes**

Ein FlexVol Volume mit speziellen Metadaten, wie z. B. Metadaten für Audit-Protokolle für Fileservices. Die Admin-SVM ist Eigentümer von System-Volumes, die im Cluster sichtbar sind. Staging Volumes sind eine Art System-Volume.

- **\* Konsolidierungsaufgabe\***

Eine Aufgabe, die bei aktivierter Prüfung erstellt wird. Diese langwierige Aufgabe auf jeder SVM nimmt die Audit-Datensätze aus Staging-Dateien über die Mitglied-Nodes der SVM auf. Mit dieser Aufgabe werden die Audit-Datensätze in einer sortierten chronologischen Reihenfolge zusammengeführt und dann in ein benutzerlesbares Ereignisprotokollformat konvertiert, das in der Überwachungskonfiguration angegeben ist – entweder das EVT- oder das XML-Dateiformat. Die umgerechneten Ereignisprotokolle werden im Verzeichnis für Revisionsereignisse gespeichert, das in der SVM-Audit-Konfiguration angegeben ist.

## Funktionsweise des ONTAP-Prüfprozesses

Der ONTAP-Audit-Prozess unterscheidet sich vom Microsoft-Audit-Prozess. Bevor Sie die Prüfung konfigurieren, sollten Sie verstehen, wie der ONTAP-Audit-Prozess funktioniert.

Auditdatensätze werden zunächst in binären Staging-Dateien auf einzelnen Knoten gespeichert. Wenn das Auditing auf einer SVM aktiviert ist, behält jeder Member-Node Staging-Dateien für diese SVM bei. Sie werden in regelmäßigen Abständen konsolidiert und in benutzerlesbare Ereignisprotokolle umgewandelt, die im Verzeichnis der Auditereignisse für die SVM gespeichert sind.

### Prozess, bei dem die Prüfung auf einer SVM aktiviert ist

Auditing kann nur auf SVMs aktiviert werden. Wenn der Storage-Administrator das Auditing für die SVM ermöglicht, überprüft das Auditing-Subsystem, ob Staging-Volumes vorhanden sind. Für jedes Aggregat, das Daten-Volumes der SVM enthält, muss ein Staging-Volume vorhanden sein. Das Audit-Subsystem erstellt alle erforderlichen Staging-Volumes, wenn sie nicht vorhanden sind.

Das Revisions-Subsystem schließt auch andere erforderliche Aufgaben ab, bevor die Prüfung aktiviert wird:

- Das Audit-Subsystem überprüft, ob der Protokollverzeichnis-Pfad verfügbar ist und keine Symlinks enthält.

Das Logverzeichnis muss bereits als Pfad innerhalb des Namespace der SVM vorhanden sein. Es wird empfohlen, ein neues Volume oder einen neuen qtree zu erstellen, um die Audit-Log-Dateien zu speichern. Das Audit-Subsystem weist keinen Standardspeicherort für Protokolldateien zu. Wenn der in der Überwachungskonfiguration angegebene Protokollverzeichnis-Pfad kein gültiger Pfad ist, schlägt die Erstellung der Überwachungskonfiguration mit dem fehl `The specified path "/path" does not exist in the namespace belonging to Vserver "Vserver_name"` Fehler.

Die Konfigurationserstellung schlägt fehl, wenn das Verzeichnis existiert, aber Symlinks enthält.

- Auditing plant die Konsolidierungsaufgabe.

Nach der Planung dieser Aufgabe wird die Prüfung aktiviert. Die SVM-Überwachungskonfiguration und die Protokolldateien bleiben bei einem Neustart erhalten oder wenn die NFS- oder SMB-Server angehalten oder neu gestartet werden.

### Konsolidierung von Ereignisprotokolls

Die Protokollkonsolidierung ist eine geplante Aufgabe, die auf routinemäßiger Basis ausgeführt wird, bis die Prüfung deaktiviert ist. Bei deaktiviertem Auditing überprüft der Konsolidierungsauftrag, ob alle übrigen Protokolle konsolidiert werden.

### Garantierte Audits

Standardmäßig ist Auditing garantiert. ONTAP garantiert, dass alle prüffähigen Dateizugriffsereignisse (wie durch konfigurierte Audit-Policy-ACLs festgelegt) aufgezeichnet werden, selbst wenn ein Knoten nicht verfügbar ist. Ein angeforderter Dateivorgang kann erst abgeschlossen werden, wenn der Prüfdatensatz für diesen Vorgang im Staging-Volume auf einem persistenten Speicher gespeichert wird. Wenn Audit-Datensätze nicht auf der Festplatte in den Staging-Dateien gespeichert werden können, entweder aufgrund von mangelhaftem Speicherplatz oder aufgrund anderer Probleme, werden Client-Vorgänge verweigert.



Ein Administrator oder Account-Benutzer mit Zugriff auf die Berechtigungsebene kann die Dateiauditprotokollierung mithilfe des NetApp Manageability SDK oder REST-APIs umgehen. Sie können ermitteln, ob Dateiaktionen mit NetApp Manageability SDK oder REST-APIs ausgeführt wurden, indem Sie die in den gespeicherten Befehlsprotokollen überprüfen `audit.log` Datei:

Weitere Informationen zu Audit-Protokollen zum Befehlsprotokoll finden Sie im Abschnitt „Managen der Audit-Protokollierung für Verwaltungsaktivitäten“ in ["Systemadministration"](#).

### Konsolidierungsprozess, wenn ein Node nicht verfügbar ist

Wenn ein Node mit Volumes, die zu einer SVM mit aktivierter Prüfung gehören, nicht verfügbar ist, hängt das Verhalten der Überwachungskonsolidierungsaufgabe davon ab, ob der Storage Failover (SFO)-Partner (oder der HA-Partner im Fall eines Clusters mit zwei Nodes) verfügbar ist:

- Wenn das Staging-Volume über den SFO-Partner verfügbar ist, werden die zuletzt vom Node gemeldeten Staging-Volumes gescannt und die Konsolidierung wird normal durchgeführt.
- Wenn der SFO-Partner nicht verfügbar ist, erstellt die Aufgabe eine partielle Protokolldatei.

Wenn ein Knoten nicht erreichbar ist, konsolidiert der Konsolidierungsauftrag die Audit-Datensätze von den anderen verfügbaren Nodes dieser SVM. Um festzustellen, dass er nicht vollständig ist, fügt die Aufgabe das Suffix hinzu `.partial` Zum konsolidierten Dateinamen.

- Nachdem der nicht verfügbare Knoten verfügbar ist, werden die Audit-Datensätze in diesem Knoten zu diesem Zeitpunkt mit den Audit-Datensätzen der anderen Knoten konsolidiert.
- Alle Audit-Datensätze werden erhalten bleiben.

### Drehung des Ereignisprotokolls

Audit-Ereignisprotokolldateien werden gedreht, wenn sie eine konfigurierte Größe des Schwellenwertprotokolls oder einen konfigurierten Zeitplan erreichen. Wenn eine Ereignis-Log-Datei gedreht wird, benennt der geplante Konsolidierungsvorgang zunächst die in eine zeitgestempelte Archivdatei konvertierte aktive Datei und erstellt dann eine neue aktive, konvertierte Ereignis-Log-Datei.

### Prozess bei deaktiviertem Auditing auf der SVM

Wenn die Prüfung auf der SVM deaktiviert ist, wird die Konsolidierungsaufgabe ein letztes Mal ausgelöst. Alle ausstehenden, aufgezeichneten Audit-Datensätze werden in einem vom Benutzer lesbaren Format protokolliert. Vorhandene Ereignisprotokolle, die im Verzeichnis für das Ereignisprotokoll gespeichert sind, werden nicht gelöscht, wenn die Prüfung auf der SVM deaktiviert ist und zur Anzeige zur Verfügung stehen.

Nachdem alle bestehenden Staging-Dateien für diese SVM konsolidiert wurden, wird die Aufgabe der Konsolidierung aus dem Zeitplan entfernt. Durch Deaktivieren der Überwachungskonfiguration für die SVM wird die Überwachungskonfiguration nicht entfernt. Ein Storage-Administrator kann das Auditing jederzeit neu aktivieren.

Der beim Auditing erstellte Konsolidierungsauftrag überwacht die Konsolidierungsaufgabe und erstellt sie neu, wenn die Konsolidierungsaufgabe aufgrund eines Fehlers beendet wird. Benutzer können den Überwachungskonsolidierungsauftrag nicht löschen.

# Anforderungen und Überlegungen des Audits

Bevor Sie das Auditing über eine Storage Virtual Machine (SVM) konfigurieren und aktivieren, müssen Sie bestimmte Anforderungen und Überlegungen beachten.

- Die maximale Anzahl der unterstützten SVMs mit Auditing-Aktivierung hängt von Ihrer Version von ONTAP ab:

| ONTAP-Version   | Maximal |
|-----------------|---------|
| 9.8 und früher  | 50      |
| 9.9.1 und höher | 400     |

- Das Auditing ist nicht an SMB- oder NFS-Lizenzen gebunden.

Auch wenn SMB- und NFS-Lizenzen nicht auf dem Cluster installiert sind, können Sie das Auditing konfigurieren und aktivieren.

- NFS-Prüfung unterstützt Sicherheitsvorkehrungen (Typ U).
- Für NFS-Prüfung gibt es keine Zuordnung zwischen Modus-Bits und Audit-Aces.

Beim Konvertieren von ACLs in Mode-Bits werden die Auditierung von Aces übersprungen. Beim Konvertieren von Modusbits zu ACLs werden keine Auditierungsaces generiert.

- Das in der Überwachungskonfiguration angegebene Verzeichnis muss vorhanden sein.

Wenn sie nicht vorhanden ist, schlägt der Befehl zum Erstellen der Überwachungskonfiguration fehl.

- Das in der Überwachungskonfiguration angegebene Verzeichnis muss die folgenden Anforderungen erfüllen:

- Das Verzeichnis darf keine symbolischen Links enthalten.

Wenn das in der Überwachungskonfiguration angegebene Verzeichnis symbolische Links enthält, schlägt der Befehl zum Erstellen der Überwachungskonfiguration fehl.

- Sie müssen das Verzeichnis über einen absoluten Pfad angeben.

Sie sollten keinen relativen Pfad angeben, z. B. `/vs1/././`.

- Die Prüfung hängt davon ab, dass in den Staging-Volumes Platz zur Verfügung steht.

Sie müssen einen Plan kennen und sicherstellen, dass ausreichend Platz für die Staging-Volumes in Aggregaten mit auditierten Volumes vorhanden ist.

- Die Prüfung hängt davon ab, dass im Volume genügend Speicherplatz verfügbar ist, der das Verzeichnis enthält, in dem konvertierte Ereignisprotokolle gespeichert werden.

Sie müssen sich bewusst sein und einen Plan erstellen, um sicherzustellen, dass in den Volumes ausreichend Speicherplatz für die Speicherung von Ereignisprotokollen vorhanden ist. Sie können die Anzahl der Ereignisprotokolle angeben, die im Überwachungsverzeichnis aufbewahrt werden sollen, indem Sie die verwenden `-rotate-limit` Parameter beim Erstellen einer Überwachungskonfiguration, der dabei helfen kann, sicherzustellen, dass genügend Speicherplatz für die Ereignisprotokolle im Volume vorhanden ist.

- Obwohl Sie die zentrale Zugriffsrichtlinien-Staging in der Überwachungskonfiguration aktivieren können, ohne Dynamic Access Control auf dem SMB-Server zu aktivieren, muss Dynamic Access Control aktiviert sein, um zentrale Zugriffs-Policy-Staging-Ereignisse zu generieren.

Die dynamische Zugriffskontrolle ist standardmäßig nicht aktiviert.

## Überlegungen zu Aggregatspeicherplatz bei Aktivierung von Auditing

Wenn eine Audit-Konfiguration erstellt und Auditing auf mindestens einer Storage Virtual Machine (SVM) im Cluster aktiviert wird, erstellt das Audit-Subsystem Staging-Volumes auf allen bestehenden Aggregaten und auf allen neu erstellten Aggregaten. Wenn Sie das Auditing auf dem Cluster aktivieren, müssen Sie bestimmte Überlegungen zu Aggregatspeicherplatz beachten.

Die Erstellung von Staging-Volumes kann aufgrund der nicht verfügbaren Speicherkapazität in einem Aggregat fehlschlagen. Dies kann passieren, wenn Sie eine Audit-Konfiguration erstellen und vorhandene Aggregate nicht über genügend Platz verfügen, um das Staging-Volume zu enthalten.

Sie sollten sicherstellen, dass auf vorhandenen Aggregaten für die Staging-Volumes genügend Speicherplatz vorhanden ist, bevor das Auditing auf einer SVM aktiviert wird.

## Einschränkungen für die Größe von Prüfdatensätzen für Staging-Dateien

Die Größe eines Audit-Datensatzes für eine Staging-Datei darf nicht größer als 32 KB sein.

### Wenn große Audit-Datensätze auftreten können

Bei der Prüfung der Verwaltung können große Audit-Datensätze in einem der folgenden Szenarien auftreten:

- Benutzer zu oder aus Gruppen mit einer großen Anzahl von Benutzern hinzufügen oder löschen.
- Hinzufügen oder Löschen einer Zugriffssteuerungsliste für Dateifreigabe (File-share Access Control List, ACL) auf einer Dateifreigabe mit einer großen Anzahl von Benutzern für die Dateifreigabe
- Andere Szenarien.

Deaktivieren Sie die Managementprüfung, um dieses Problem zu vermeiden. Ändern Sie dazu die Audit-Konfiguration, und entfernen Sie Folgendes aus der Liste der Audit-Ereignistypen:

- Dateifreigabe
- Benutzerkonto
- Sicherheitsgruppe
- Änderung der Autorisierungsrichtlinie

Nach dem Entfernen werden diese vom Audit-Subsystem für Fileservices nicht geprüft.

### Die Auswirkungen von zu großen Audit-Datensätzen

- Wenn die Größe eines Audit-Datensatzes zu groß ist (über 32 KB), wird der Audit-Datensatz nicht erstellt und das Audit-Subsystem erzeugt eine EMS-Meldung (Event Management System), die der folgenden



ähnelt:

```
File Services Auditing subsystem failed the operation or truncated an audit
record because it was greater than max_audit_record_size value. Vserver
UUID=%s, event_id=%u, size=%u
```

Wenn die Prüfung gewährleistet ist, schlägt der Dateivorgang fehl, da sein Audit-Datensatz nicht erstellt werden kann.

- Wenn die Größe des Audit-Datensatzes mehr als 9,999 Byte beträgt, wird die gleiche EMS-Meldung wie oben angezeigt. Ein partieller Prüfdatensatz wird erstellt, wobei der größere Schlüsselwert fehlt.
- Wenn der Prüfdatensatz 2,000 Zeichen überschreitet, wird anstelle des tatsächlichen Werts die folgende Fehlermeldung angezeigt:

```
The value of this field was too long to display.
```

## Die unterstützten Audit-Ereignisprotokollformate

Unterstützte Dateiformate für die umgerechneten Audit-Ereignisprotokolle sind **EVTX** Und **XML** Dateiformate.

Sie können den Dateityp angeben, wenn Sie die Überwachungskonfiguration erstellen. Standardmäßig konvertiert ONTAP die Binärprotokolle in das **EVTX** Dateiformat.

## Anzeigen von Audit-Ereignisprotokollen

Mithilfe von Audit-Ereignisprotokollen können Sie feststellen, ob Sie über eine ausreichende Dateisicherheit verfügen und ob es keine falschen Datei- und Ordnerzugriffsversuche gab. Sie können die in gespeicherten Audit-Ereignisprotokolle anzeigen und verarbeiten **EVTX** Oder **XML** Dateiformate.

- **EVTX** Dateiformat

Sie können die konvertierte öffnen **EVTX** Ereignisprotokolle als gespeicherte Dateien mit Microsoft Event Viewer prüfen.

Es gibt zwei Optionen, die Sie für die Anzeige von Ereignisprotokollen mit der Ereignisanzeige verwenden können:

- **Allgemeine Ansicht**

Für den Ereignisdatensatz werden Informationen angezeigt, die für alle Ereignisse gemeinsam sind. In dieser ONTAP-Version werden die ereignisspezifischen Daten für den Ereignisdatensatz nicht angezeigt. Mithilfe der detaillierten Ansicht können ereignisspezifische Daten angezeigt werden.

- **Detailansicht**

Eine freundliche Aussicht und eine XML-Ansicht stehen zur Verfügung. Die freundliche Ansicht und die XML-Ansicht zeigen sowohl die Informationen, die für alle Ereignisse gemeinsam sind, als auch die ereignisspezifischen Daten für den Ereignisdatensatz.

- XML Dateiformat

Sie können anzeigen und verarbeiten XML Prüfung von Ereignisprotokollen für Anwendungen von Drittanbietern, die den unterstützen XML Dateiformat. XML-Anzeigewerkzeuge können verwendet werden, um die Überwachungsprotokolle anzuzeigen, vorausgesetzt, Sie haben das XML-Schema und Informationen zu Definitionen für die XML-Felder. Weitere Informationen zum XML-Schema und zu Definitionen finden Sie im ["ONTAP-Überwachungsschema – Referenz"](#).

## Wie aktive Prüfprotokolle mit der Ereignisanzeige angezeigt werden

Wenn der Audit-Konsolidierungsprozess auf dem Cluster ausgeführt wird, fügt der Konsolidierungsprozess neue Datensätze an die aktive Audit-Log-Datei für revisionssichere Storage Virtual Machines (SVMs) an. Auf dieses aktive Prüfprotokoll kann über eine SMB-Freigabe in Microsoft Event Viewer zugegriffen und geöffnet werden.

Neben der Anzeige vorhandener Überwachungsdatensätze verfügt die Ereignisanzeige über eine Aktualisierungsoption, mit der Sie den Inhalt im Konsolenfenster aktualisieren können. Ob die neu angefügten Protokolle in der Ereignisanzeige angezeigt werden, hängt davon ab, ob Oplocks auf der Freigabe aktiviert sind, die zum Zugriff auf das aktive Audit-Protokoll verwendet wird.

| Oplocks-Einstellung auf dem Share | Verhalten  |
|-----------------------------------|--|
| Aktiviert                         | Event Viewer öffnet das Protokoll, das Ereignisse enthält, die bis zu diesem Zeitpunkt geschrieben wurden. Beim Aktualisierungsvorgang wird das Protokoll nicht mit neuen Ereignissen aktualisiert, die durch den Konsolidierungsvorgang angehängt sind. |
| Deaktiviert                       | Event Viewer öffnet das Protokoll, das Ereignisse enthält, die bis zu diesem Zeitpunkt geschrieben wurden. Beim Aktualisierungsvorgang wird das Protokoll mit neuen Ereignissen aktualisiert, die durch den Konsolidierungsprozess angefügt werden.      |



Diese Informationen gelten nur für EVTX Ereignisprotokolle XML Ereignisprotokolle können über SMB in einem Browser oder über NFS mit einem beliebigen XML-Editor oder Viewer angezeigt werden.

## SMB-Ereignisse, die geprüft werden können

### SMB-Ereignisse, die geprüft werden können, Übersicht

ONTAP kann bestimmte SMB-Ereignisse überprüfen, einschließlich bestimmter Datei- und Ordnerzugriffsereignisse, bestimmter Anmelde- und Abmeldungereignisse 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 im ONTAP 9.2 und höher geprüft werden:

| EREIGNIS-ID<br>(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<br>(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 | <p>OBJEKTZUGRIFF: Objektzugriffsversuch (Lesen, Schreiben, get attribut, set attribut).</p> <p><b>Hinweis:</b> 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.</p> | 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 Zugriffsrichtlinie | 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

Der `HandleID` Kennzeichnung im Audit XML Event enthält den Handle des Objekts (Datei oder Verzeichnis), auf das zugegriffen wird. Der `HandleID` Das Tag für das Ereignis EVT 4656 enthält unterschiedliche Informationen, je nachdem, ob das offene Ereignis zum Erstellen eines neuen Objekts oder zum Öffnen eines vorhandenen Objekts ist:

- Wenn das offene Ereignis eine offene Anforderung ist, ein neues Objekt (Datei oder Verzeichnis) zu erstellen, wird das angezeigt `HandleID` Das Tag im XML-Ereignis „Audit“ ist leer `HandleID` (Beispiel: `<Data Name="HandleID">0000000000000000;00;00000000;00000000</Data>` ).

Der `HandleID` Ist leer, weil die OFFENE (zum Erstellen eines neuen Objekts) Anforderung geprüft wird, bevor die tatsächliche Objekterstellung stattfindet und bevor ein Handle vorhanden ist. Nachfolgende geprüfte Ereignisse für dasselbe Objekt haben den richtigen Objektgriff im `HandleID` Tag:

- Wenn das offene Ereignis eine offene Anfrage zum Öffnen eines vorhandenen Objekts ist, wird dem Audit-Ereignis das zugewiesene Handle dieses Objekts im zugewiesenen `HandleID` Tag (zum Beispiel: `<Data Name="HandleID">000000000000401;00;000000ea;00123ed4</Data>` ).

### Legen Sie fest, welcher Pfad zum geprüften Objekt vollständig ist

Der im gedruckte Objektpfad `<ObjectName>` Das Tag für einen Prüfdatensatz enthält den Namen des Volumens (in Klammern) und den relativen Pfad aus der Root des enthaltenden Volumens. Wenn Sie den vollständigen Pfad des geprüften Objekts einschließlich des Verbindungspfades bestimmen möchten, müssen Sie bestimmte Schritte durchführen.

#### Schritte

1. Ermitteln Sie den Volume-Namen und den relativen Pfad zum geprüften Objekt, indem Sie sich das ansehen `<ObjectName>` Kennzeichnung im Audit-Ereignis.

In diesem Beispiel lautet der Volume-Name „data1“ und der relative Pfad zur Datei `/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 Volume-Name „data1“ und der Verbindungspfad für das Volume mit dem geprüften Objekt 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 im gefundenen relativen Pfad anhängen <ObjectName> Markieren Sie den Verbindungspfad für das Volume.

In diesem Beispiel ist der Verbindungspfad für das Volume:

```
/data/data1/dir1/file.txt
```

## Überlegungen beim 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 prüfende Objekt einschließlich des Pfads zum geprüften Objekt, das im identifiziert wird `ObjectName` Tag: Sie sollten sich bewusst sein, wie Pfade für Symlinks und harte Links in aufgezeichnet werden `ObjectName` Tag:

### 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 verweisen `target.txt`. Einer der Symlinks ist ein relativer Symlink und einer ist ein absolutes Symlink. Wenn eines der Symlinks geprüft wird, wird das angezeigt `ObjectName` Das Tag im Überwachungsereignis enthält 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 Objekt mit harter Verbindung geprüft wird, zeichnet das Ereignis Audit diesen absoluten kanonischen Pfad im auf `ObjectName` Markieren Sie anstelle des Pfads der harten Verbindung.

## Überlegungen beim Prüfen alternativer NTFS-Datenströme

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

Der Speicherort eines zu auditierenden Objekts wird in einem Ereignisdatensatz mit zwei Tags, dem, aufgezeichnet `ObjectName` Tag (der Pfad) und der `HandleID` Kennzeichen (Griff). 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 aufgezeichnet `ObjectName` Tag:
  - Das Handle des alternativen Datenstroms wird im aufgezeichnet `HandleID` Tag:
- EVTX-ID: 4663 Ereignisse (alle anderen Audit-Ereignisse, wie Lesen, Schreiben, getattr usw.)
  - Der Pfad der Basisdatei, nicht der alternative Datenstrom, wird im aufgezeichnet `ObjectName` Tag:
  - Das Handle des alternativen Datenstroms wird im aufgezeichnet `HandleID` Tag:

## Beispiel

Das folgende Beispiel zeigt, wie die EVTX-ID identifiziert werden kann: 4663 Ereignisse für alternative Datenströme mit dem `HandleID` Tag: Obwohl das `ObjectName` Das Tag (Pfad), das im Ereignis „Audit lesen“ aufgezeichnet wurde, befindet sich in dem Pfad der Basisdatei, dem `HandleID` Mit dem Tag kann das Ereignis als Prüfdatensatz für den alternativen Datenstrom identifiziert werden.

Stream-Dateinamen nehmen das Formular ein `base_file_name:stream_name`. In diesem Beispiel ist der `dir1` Das Verzeichnis enthält eine Basisdatei mit einem alternativen Datenstrom mit folgenden Pfaden:

```
/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 (Open Audit Event) zeichnet der Audit-Datensatz-Ausgang für den alternativen Datenstrom den alternativen Namen des Datenstroms in auf `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">000000000000401;00;000001e4;00176767</Data>
  <Data Name="ObjectName">\(data1\);/dir1/file1.txt:stream1</Data>
  **
  [...]
</EventData>
</Event>
- <Event>
```

Bei einer EVTX-ID 4663 (Ereignis „Audit lesen“) zeichnet die Ausgabe des Prüfdatensätzen für denselben alternativen Datenstrom den Namen der Basisdatei in der auf `ObjectName` Markieren Sie jedoch den Griff im `HandleID` Das Tag ist der Griff 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>

```

## Es können NFS-Datei- und Verzeichniszugriffe geprüft werden

ONTAP kann bestimmte NFS-Datei- und Verzeichniszugriffe prüfen. Das Wissen, welche Zugriffsereignisse auditiert werden können, ist hilfreich bei der Interpretation der Ergebnisse aus den umgerechneten Audit-Ereignisprotokollen.

Sie können die folgenden NFS-Datei- und Verzeichniszugriffsereignisse prüfen:

- LESEN
- OFFEN
- SCHLIESSEN
- LESDIR
- SCHREIBEN
- SETATTR
- ERSTELLEN
- VERLINKEN
- OPENATTR
- ENTFERNEN
- GETATTR
- VERIFIZIEREN
- NVERIFY
- UMBENENNEN

Um NFS-UMBENENNUNGSEREIGNISSE zuverlässig zu prüfen, sollten Sie Überwachungsaces auf

Verzeichnissen statt auf Dateien festlegen, da Dateiberechtigungen nicht auf EINEN UMBENENNUNGSVORGANG überprüft werden, wenn die Verzeichnisberechtigungen ausreichen.

## Planen der Überwachungskonfiguration

Bevor Sie das Auditing auf Storage Virtual Machines (SVMs) konfigurieren, müssen Sie wissen, welche Konfigurationsoptionen verfügbar sind, und die Werte planen, die Sie für die einzelnen Optionen festlegen möchten. Diese Informationen können Ihnen dabei helfen, die Prüfungskonfiguration zu konfigurieren, die Ihren geschäftlichen Anforderungen entspricht.

Es gibt bestimmte Konfigurationsparameter, die allen Überwachungskonfigurationen gemeinsam sind.

Darüber hinaus gibt es bestimmte Parameter, mit denen Sie angeben können, welche Methoden beim Drehen der konsolidierten und konvertierten Prüfprotokolle verwendet werden. Sie können eine der drei folgenden Methoden angeben, wenn Sie die Prüfung konfigurieren:

- Drehen Sie Protokolle basierend auf der Protokollgröße

Dies ist die Standardmethode, mit der Protokolle gedreht werden.

- Protokolle nach einem Zeitplan drehen
- Protokolle nach Protokollgröße und Zeitplan rotieren (je nachdem, welches Ereignis zuerst eintritt)



Mindestens eine der Methoden für die Protokollrotation sollte immer eingestellt werden.

## Gemeinsame Parameter für alle Überwachungskonfigurationen

Es gibt zwei erforderliche Parameter, die Sie beim Erstellen der Überwachungskonfiguration angeben müssen. Sie können außerdem drei optionale Parameter angeben:

| Informationstyp   | Option                             | Erforderlich | Einschließlich | Ihre Werte |
|---|------------------------------------|--------------|----------------|------------|
| <b>SVM Name</b><br><br>Name der SVM, auf der die Audit-Konfiguration erstellt werden soll. Die SVM muss bereits vorhanden sein. | <code>-vserver vserver_name</code> | Ja.          | Ja.            |            |

|   |                   |     |     |  |
|---|-------------------|-----|-----|--|
| <p><i>Zielpfad protokollieren</i></p> <p>Gibt das Verzeichnis an, in dem umgerechnete Audit-Protokolle gespeichert werden, in der Regel ein dediziertes Volume oder qtree. Der Pfad muss im SVM-Namespace bereits vorhanden sein.</p> <p>Der Pfad kann bis zu 864 Zeichen lang sein und muss über Lese-/Schreibberechtigungen verfügen.</p> <p>Wenn der Pfad nicht gültig ist, schlägt der Befehl für die Prüfungskonfiguration fehl.</p> <p>Wenn die SVM eine Disaster-Recovery-Quelle für SVM ist, kann sich der Protokollzielpfad nicht auf dem Root-Volume befinden. Das liegt daran, dass der Root-Volume-Inhalt nicht zum Disaster-Recovery-Ziel repliziert wird.</p> <p>Sie können ein FlexCache-Volume nicht als Protokollziel verwenden (ONTAP 9.7 und höher).</p> | -destination text | Ja. | Ja. |  |
|---|-------------------|-----|-----|--|

|  |                   |                       |                              |                |
|--|-------------------|-----------------------|------------------------------|----------------|
| <p><b>Kategorien von Ereignissen zur Prüfung</b></p> <p>Gibt die Kategorien von zu prüfenden Ereignissen an. Folgende Ereigniskategorien können geprüft werden:</p> <ul style="list-style-type: none"> <li>• Dateizugriff (SMB und NFSv4)</li> <li>• SMB-Anmeldung und -Abmeldung</li> <li>• Staging von zentralen Zugriffsrichtlinien</li> </ul> <p>Die Staging-Ereignisse für zentrale Zugriffsrichtlinien sind ab Windows 2012 Active Directory-Domänen verfügbar.</p> <ul style="list-style-type: none"> <li>• Ereignisse in der Kategorie Dateifreigabe</li> <li>• Änderungsereignisse für die Überwachungsrichtlinien</li> <li>• Lokale Benutzerkontenverwaltungsereignisse</li> <li>• Ereignisse für das Management von Sicherheitsgruppen</li> <li>• Änderungsereignisse für die Autorisierungsrichtlinie</li> </ul> <p>Der Standardwert ist der Dateizugriff sowie das SMB-Anmelde- und -Abmeldungs-Ereignis.</p> <p><b>Hinweis:</b> bevor Sie angeben können cap-staging Als Ereigniskategorie muss auf der SVM ein SMB-Server vorhanden sein. Obwohl Sie die zentrale Zugriffsrichtlinien-Staging in der Überwachungskonfiguration aktivieren können, ohne die dynamische Zugriffskontrolle auf dem SMB-Server zu aktivieren, werden zentrale Zugriffsrichtlinien-Staging-Ereignisse nur erzeugt, wenn Dynamic Access Control aktiviert ist. Die dynamische Zugriffskontrolle wird über eine SMB-Serveroption aktiviert. Sie ist standardmäßig nicht aktiviert.</p> | -events {file-ops | cifs-logon-<br>logoff | cap-<br>staging              | file-<br>share |
| audit-policy-change  | user-account      | security-group        | authorization-policy-change} | Nein           |

|  |  |   |                 |       |
|--|--|---|-----------------|-------|
|  |  | <p>Ausgabef<br/>ormat<br/><i>Log-Datei</i></p> <p>Legt das<br/>Ausgabef<br/>ormat der<br/>Prüfproto<br/>kolle fest.<br/>Das<br/>Ausgabef<br/>ormat<br/>kann<br/>entweder<br/>ONTAP-<br/>spezifisc<br/>h sein<br/>XML Oder<br/>Microsoft<br/>Windows<br/>EVTX<br/>Protokollf<br/>ormat:<br/>Standard<br/>mäßig<br/>lautet das<br/>Ausgabef<br/>ormat<br/>EVTX.</p> | -format<br>{xml | evtx} |
|--|--|---|-----------------|-------|

|      |  |  |   |                                       |
|------|--|--|---|---------------------------------------|
| Nein |  |  | <p><b>Log-Dateien Rotationsgrenze</b></p> <p>Legt fest, wie viele Audit-Log-Dateien gespeichert werden sollen, bevor die älteste Protokoll datei ausgedreht wird. Wenn Sie beispielsweise einen Wert von eingeben 5, Die letzten fünf Log-Dateien werden beibehalten.</p> <p>Der Wert von 0 Zeigt an, dass alle Protokoll dateien aufbewahrt werden. Der Standard wert ist 0.</p> | <p>-rotate<br/>-limit<br/>integer</p> |
|------|--|--|---|---------------------------------------|

## Parameter, die zur Bestimmung des Drehungswahres von Audit-Ereignisprotokollen verwendet werden

### Protokolle auf Basis der Protokollgröße drehen

Standardmäßig werden Auditprotokolle auf der Grundlage der Größe gedreht.

- Die Standard-Protokollgröße beträgt 100 MB
- Wenn Sie die Standard-Protokollrotation-Methode und die Standard-Protokollgröße verwenden möchten, müssen Sie keine spezifischen Parameter für die Protokollrotation konfigurieren.
- Wenn Sie die Prüfprotokolle allein auf Grundlage einer Protokollgröße drehen möchten, können Sie mit dem folgenden Befehl die Einstellung aufheben `-rotate-schedule-minute` Parameter: `vserver audit modify -vserver vs0 -destination / -rotate-schedule-minute -`

Wenn Sie die Standardprotokollgröße nicht verwenden möchten, können Sie das konfigurieren `-rotate-size` Parameter zur Angabe einer benutzerdefinierten Protokollgröße:

| Informationstyp   | Option  | Erforderlich | Einschließlich | Ihre Werte |
|---|---|--------------|----------------|------------|
| <i>Größe der Protokolldatei</i><br><br>Bestimmt die Größenbeschränkung der Prüfprotokoll-Datei. | <code>-rotate-size {integer[KB MB/GB/TB/PB]}</code> | Nein         |                |            |

### Protokolle nach Zeitplan drehen

Wenn Sie die Prüfprotokolle nach einem Zeitplan drehen möchten, können Sie die Protokollrotation mithilfe der zeitbasierten Rotationsparameter in beliebiger Kombination planen.

- Wenn Sie zeitbasierte Rotation verwenden, wird das angezeigt `-rotate-schedule-minute` Parameter muss angegeben werden.
- Alle anderen zeitbasierten Rotationsparameter sind optional.
- Der Rotationsplan wird unter Verwendung aller zeitbezogenen Werte berechnet.

Wenn Sie beispielsweise nur die angeben `-rotate-schedule-minute` Parameter, die Audit-Log-Dateien werden auf der Grundlage der Minuten gedreht, die an allen Wochentagen, während aller Stunden an allen Monaten des Jahres angegeben sind.

- Wenn Sie nur einen oder zwei zeitbasierte Rotationsparameter angeben (z. B. `-rotate-schedule-month` Und `-rotate-schedule-minutes`), die Log-Dateien werden basierend auf den Minutenwerten, die Sie an allen Wochentagen, während aller Stunden, aber nur während der angegebenen Monate angegeben.

Sie können z. B. angeben, dass das Audit-Protokoll in den Monaten Januar, März und August alle Montag, Mittwoch und Samstag um 10:30 Uhr gedreht werden soll

- Wenn Sie Werte für beide angeben `-rotate-schedule-dayofweek` Und `-rotate-schedule-day`, Sie werden unabhängig betrachtet.

Beispiel: Wenn Sie angeben `-rotate-schedule-dayofweek` Als Freitag und `-rotate-schedule-day` Als 13, dann werden die Audit-Protokolle an jedem Freitag und am 13. Tag des angegebenen Monats gedreht werden, nicht nur an jedem Freitag der 13...

- Wenn Sie die Prüfprotokolle nur nach einem Zeitplan drehen möchten, können Sie mit dem folgenden Befehl die Einstellung aufheben `-rotate-size` Parameter: `vserver audit modify -vserver vs0 -destination / -rotate-size -`

Anhand der folgenden Liste verfügbarer Überwachungsparameter können Sie bestimmen, welche Werte für die Konfiguration eines Zeitplans für die Rotation des Ereignisprotokolls verwendet werden sollen:

| Informationstyp   | Option   | Erforderlich | Einschließlich | Ihre Werte |
|---|--|--------------|----------------|------------|
| <p><b>Drehplan Log: Monat</b></p> <p>Legt den monatlichen Zeitplan für rotierende Prüfprotokolle fest.</p> <p>Gültige Werte sind <code>January</code> Bis <code>December</code>, und <code>all</code>. Sie können z. B. angeben, dass das Prüfprotokoll in den Monaten Januar, März und August gedreht werden soll.</p>                               | <code>-rotate-schedule-month</code><br><code>chron_month</code>                          | Nein         |                |            |
| <p><b>Drehplan Log: Wochentag</b></p> <p>Legt den täglichen Zeitplan (Wochentag) für rotierende Prüfprotokolle fest.</p> <p>Gültige Werte sind <code>Sunday</code> Bis <code>Saturday</code>, und <code>all</code>. Sie können z. B. angeben, dass das Audit-Protokoll dienstags und freitags oder an allen Wochentagen gedreht werden soll.</p>      | <code>-rotate-schedule</code><br><code>-dayofweek</code><br><code>chron_dayofweek</code> | Nein         |                |            |
| <p><b>Drehplan Log: Tag</b></p> <p>Bestimmt den Tag des Monatsplans für das Drehen des Prüfprotokolls.</p> <p>Gültige Werte reichen von 1 Bis 31. Sie können z. B. angeben, dass das Audit-Protokoll an den 10. Und 20. Tagen eines Monats oder an allen Tagen eines Monats gedreht werden soll.</p>  | <code>-rotate-schedule-day</code><br><code>chron_dayofmonth</code>                       | Nein         |                |            |
| <p><b>Drehplan Log: Stunde</b></p> <p>Legt den Stundenplan für das Drehen des Prüfprotokolls fest.</p> <p>Gültige Werte reichen von 0 (Mitternacht) bis 23 (11:00 Uhr). Angeben <code>all</code> Dreht die Prüfprotokolle jede Stunde. Sie können beispielsweise angeben, dass das Prüfprotokoll um 6 (6 Uhr) und 18 (6 Uhr) gedreht werden soll.</p> | <code>-rotate-schedule-hour</code><br><code>chron_hour</code>                            | Nein         |                |            |



|   |   |   |  |  |
|---|---|---|--|--|
| <p><b>Drehplan Log: Minute</b></p> <p>Legt den Minutenplan für das Drehen des Prüfprotokolls fest.</p> <p>Gültige Werte reichen von 0 Bis 59. Sie können z. B. angeben, dass das Prüfprotokoll in der 30. Minute gedreht werden soll.</p> | <p><code>-rotate-schedule-minute</code><br/><code>chron_minute</code></p> | <p>Ja, wenn Sie eine planbasierte Protokollrotation konfigurieren, andernfalls Nein</p> |  |  |
|---|---|---|--|--|

### Rundprotokolle basierend auf Loggröße und Zeitplan drehen

Sie können wählen, ob Sie die Protokolldateien basierend auf der Protokollgröße und einem Zeitplan drehen möchten, indem Sie die beiden festlegen `-rotate-size` Parameter und die zeitbasierten Rotationsparameter in beliebiger Kombination. Beispiel: Wenn `-rotate-size` Ist auf 10 MB und eingestellt `-rotate-schedule-minute` Ist auf 15 gesetzt, drehen sich die Protokolldateien, wenn die Protokolldateigröße 10 MB oder in der 15. Minute jeder Stunde (je nachdem, welches Ereignis zuerst eintritt) erreicht.

## Erstellen einer Datei- und Verzeichnisüberprüfung auf SVMs

### Erstellen Sie die Überwachungskonfiguration

Das Erstellen einer Datei- und Verzeichnisüberwachung auf Ihrer Storage Virtual Machine (SVM) umfasst die Analyse der verfügbaren Konfigurationsoptionen, die Planung der Konfiguration und die Konfiguration sowie die Aktivierung der Konfiguration. Sie können dann Informationen zur Überwachungskonfiguration anzeigen, um zu bestätigen, dass die resultierende Konfiguration die gewünschte Konfiguration ist.

Bevor Sie mit dem Auditing von Datei- und Verzeichnisereignissen beginnen können, müssen Sie eine Auditing-Konfiguration auf der Storage Virtual Machine (SVM) erstellen.

#### Bevor Sie beginnen

Wenn Sie eine Auditing-Konfiguration für zentrale Zugriffsrichtlinien-Staging erstellen möchten, muss auf der SVM ein SMB-Server vorhanden sein.



- Obwohl Sie die zentrale Zugriffsrichtlinien-Staging in der Überwachungskonfiguration aktivieren können, ohne die dynamische Zugriffskontrolle auf dem SMB-Server zu aktivieren, werden zentrale Zugriffsrichtlinien-Staging-Ereignisse nur erzeugt, wenn Dynamic Access Control aktiviert ist.

Die dynamische Zugriffskontrolle wird über eine SMB-Serveroption aktiviert. Sie ist standardmäßig nicht aktiviert.

- Wenn die Argumente eines Feldes in einem Befehl ungültig sind, z. B. ungültige Einträge für Felder, doppelte Einträge und nicht vorhandene Einträge, dann schlägt der Befehl vor der Audit-Phase fehl.

Solche Fehler erzeugen keinen Audit-Datensatz.

## Über diese Aufgabe

Wenn die SVM eine SVM Disaster-Recovery-Quelle ist, kann sich der Zielpfad nicht auf dem Root-Volume befinden.

## Schritt

1. Erstellen Sie mithilfe der Informationen im Planungsarbeitsblatt die Überwachungskonfiguration, um Prüfprotokolle auf der Grundlage der Protokollgröße oder eines Zeitplans zu drehen:

|   |  |
|---|--|
| Wenn Sie die Prüfprotokolle drehen möchten, um... | Eingeben...  |
| Protokollgröße                                    | `vserver audit create -vserver vserver_name -destination path -events [{file-ops |
| cifs-logon-logoff                                 | cap-staging  |
| file-share  | authorization-policy-change  |
| user-account                                      | security-group   |
| authorization-policy-change}] [-format {xml       | evtx}] [-rotate-limit integer] [-rotate-size {integer[KB                         |
| MB  | GB   |
| TB  | PB]]]`   |
| Einen Zeitplan                                    | `vserver audit create -vserver vserver_name -destination path -events [{file-ops |
| cifs-logon-logoff                                 | cap-staging}] [-format {xml  |

## Beispiele

Im folgenden Beispiel wird eine Überwachungskonfiguration erstellt, die Dateivorgänge und SMB-Anmelde- und -Abmeldungseignisse (Standard) anhand der größenbasierten Rotation prüft. Das Protokollformat lautet EVTX (Standardeinstellung). Die Protokolle werden im gespeichert `/audit_log` Verzeichnis. Die maximale Größe der Protokolldatei ist 200 MB. Die Protokolle werden gedreht, wenn sie eine Größe von 200 MB erreichen:

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log  
-rotate-size 200MB
```

Im folgenden Beispiel wird eine Überwachungskonfiguration erstellt, die Dateivorgänge und SMB-Anmelde- und -Abmeldungseignisse (Standard) anhand der größenbasierten Rotation prüft. Das Protokollformat lautet EVTX (Standardeinstellung). Die Protokolle werden im gespeichert `/cifs_event_logs` Verzeichnis. Die maximale Größe der Protokolldatei ist 100 MB (Die Standardeinstellung), und die Protokollrotationsgrenze ist 5:

```
cluster1::> vserver audit create -vserver vs1 -destination  
/cifs_event_logs -rotate-limit 5
```

Im folgenden Beispiel wird eine Audit-Konfiguration erstellt, die Dateivorgänge, CIFS-Anmelde- und -Abmeldungsereignisse und zentrale Zugriffs- und Staging-Ereignisse anhand zeitbasierter Rotation prüft. Das Protokollformat lautet EVT<sub>X</sub> (Standardeinstellung). Die Prüfprotokolle werden monatlich um 12:30 Uhr gedreht. An allen Wochentagen. Die Protokollrotationsgrenze ist 5:

```
cluster1::> vservers audit create -vservers vs1 -destination /audit_log
-events file-ops,cifs-login-logoff,file-share,audit-policy-change,user-
account,security-group,authorization-policy-change,cap-staging -rotate
-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour
12 -rotate-schedule-minute 30 -rotate-limit 5
```

#### Verwandte Informationen

- ["Prüfung auf SVM aktivieren"](#)
- ["Überprüfen Sie die Überwachungskonfiguration"](#)

## Prüfung auf SVM aktivieren

Nachdem Sie die Auditing-Konfiguration abgeschlossen haben, müssen Sie das Auditing auf der Storage Virtual Machine (SVM) aktivieren.

#### Bevor Sie beginnen

Die SVM-Audit-Konfiguration muss bereits vorhanden sein.

#### Über diese Aufgabe

Wenn die SVM-Konfiguration für Disaster-Recovery-ID-verwerfen (nach Abschluss der SnapMirror-Initialisierung) und eine Audit-Konfiguration vorhanden ist, deaktiviert ONTAP die Prüfungskonfiguration automatisch. Die Prüfung wird auf der schreibgeschützten SVM deaktiviert, um zu verhindern, dass die Staging-Volumes gefüllt werden. Sie können das Auditing nur aktivieren, wenn die SnapMirror Beziehung beschädigt ist und die SVM Lese-/Schreibzugriff ist.

#### Schritte

1. Prüfung auf der SVM aktivieren:

```
vservers audit enable -vservers vservers_name
```

```
vservers audit enable -vservers vs1
```

#### Verwandte Informationen

- ["Erstellen Sie die Überwachungskonfiguration"](#)
- ["Überprüfen Sie die Überwachungskonfiguration"](#)

## Überprüfen Sie die Überwachungskonfiguration

Nach Abschluss der Überwachungskonfiguration sollten Sie überprüfen, ob die Prüfung ordnungsgemäß konfiguriert und aktiviert ist.

#### Schritte

## 1. Überprüfen Sie die Überwachungskonfiguration:

```
vserver audit show -instance -vserver vserver_name
```

Mit dem folgenden Befehl werden alle Audit-Konfigurationsinformationen für Storage Virtual Machine (SVM) vs1 in Listenform angezeigt:

```
vserver audit show -instance -vserver vs1
```

```
Vserver: vs1
Auditing state: true
Log Destination Path: /audit_log
Categories of Events to Audit: file-ops
Log Format: evtX
Log File Size Limit: 200MB
Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
Log Rotation Schedule: Day: -
Log Rotation Schedule: Hour: -
Log Rotation Schedule: Minute: -
Rotation Schedules: -
Log Files Rotation Limit: 0
```

### Verwandte Informationen

- ["Erstellen Sie die Überwachungskonfiguration"](#)
- ["Prüfung auf SVM aktivieren"](#)

## Audit-Richtlinien für Dateien und Ordner konfigurieren

### Audit-Richtlinien für Dateien und Ordner konfigurieren

Die Implementierung der Prüfung von Datei- und Ordnerzugriffsereignissen ist ein zweistufiger Prozess. Zunächst müssen Sie eine Audit-Konfiguration auf Storage Virtual Machines (SVMs) erstellen und aktivieren. Zweitens müssen Sie die Audit-Richtlinien für die Dateien und Ordner konfigurieren, die Sie überwachen möchten. Sie können Audit-Richtlinien konfigurieren, um sowohl erfolgreiche als auch fehlgeschlagene Zugriffsversuche zu überwachen.

Sie können sowohl SMB- als auch NFS-Audit-Richtlinien konfigurieren. Audit-Richtlinien für SMB und NFS gelten für unterschiedliche Konfigurationsanforderungen und Audit-Funktionen.

Wenn die entsprechenden Audit-Richtlinien konfiguriert sind, überwacht ONTAP die SMB- und NFS-Zugriffsereignisse wie in den Audit-Richtlinien festgelegt, nur wenn SMB- oder NFS-Server ausgeführt werden.

## Konfigurieren Sie die Audit-Richtlinien für Dateien und Verzeichnisse im NTFS-Sicherheitsstil

Bevor Sie Vorgänge in Dateien und Verzeichnissen prüfen können, müssen Sie die Überwachungsrichtlinien für die Dateien und Verzeichnisse konfigurieren, für die Sie Audit-Informationen erfassen möchten. Dies ist zusätzlich zur Einrichtung und Aktivierung der Audit-Konfiguration. Sie können NTFS-Audit-Richtlinien über die Registerkarte Windows-Sicherheit oder über die ONTAP-CLI konfigurieren.

### Konfigurieren von NTFS-Audit-Richtlinien über die Registerkarte Windows-Sicherheit

Sie können NTFS-Audit-Richtlinien für Dateien und Verzeichnisse über die Registerkarte **Windows Security** im Fenster Windows-Eigenschaften konfigurieren. Dies ist die gleiche Methode, die bei der Konfiguration von Audit-Richtlinien für Daten auf einem Windows-Client verwendet wird. Auf diese Weise können Sie die gleiche GUI-Schnittstelle verwenden, die Sie gewohnt sind.

#### Bevor Sie beginnen

Das Auditing muss auf der Storage Virtual Machine (SVM) konfiguriert werden, die die Daten enthält, auf die Sie Systemzugriffssteuerungslisten (SACLs) anwenden.

#### Über diese Aufgabe

Das Konfigurieren von NTFS-Audit-Richtlinien erfolgt durch Hinzufügen von Einträgen zu NTFS-SACLs, die mit einem NTFS-Sicherheitsdeskriptor verknüpft sind. Der Sicherheitsdeskriptor wird dann auf NTFS-Dateien und -Verzeichnisse angewendet. Diese Aufgaben werden automatisch von der Windows GUI übernommen. Der Sicherheitsdeskriptor kann Discretionary Access Control Lists (DACLS) zum Anwenden von Datei- und Ordnerzugriffsberechtigungen, SACLs für Datei- und Ordnerprüfung oder SACLs und DACLS enthalten.

Führen Sie die folgenden Schritte auf einem Windows-Host aus, um NTFS-Audit-Richtlinien über die Registerkarte Windows-Sicherheit festzulegen:

#### Schritte

1. Wählen Sie im Menü **Tools** im Windows Explorer die Option **Netzwerklaufwerk zuordnen** aus.
2. Füllen Sie die Box \* Map Network Drive\* aus:
  - a. Wählen Sie einen **Drive**-Buchstaben aus.
  - b. Geben Sie im Feld **Ordner** den SMB-Servernamen ein, der die Freigabe enthält und die zu prüfenden Daten sowie den Namen der Freigabe enthält.

Sie können anstelle des SMB-Servernamens die IP-Adresse der Datenschnittstelle für den SMB-Server angeben.

Wenn der Name Ihres SMB-Servers „SMB\_SERVER“ lautet und Ihre Freigabe den Namen „share1“ hat, sollten Sie eingeben \\SMB\_SERVER\share1.

- c. Klicken Sie Auf **Fertig Stellen**.

Das ausgewählte Laufwerk ist mit dem Windows Explorer-Fenster verbunden und bereit, in dem die Dateien und Ordner in der Freigabe angezeigt werden.

3. Wählen Sie die Datei oder das Verzeichnis aus, für die Sie den Audit-Zugriff aktivieren möchten.
4. Klicken Sie mit der rechten Maustaste auf die Datei oder das Verzeichnis, und wählen Sie dann **Eigenschaften** aus.

5. Wählen Sie die Registerkarte **Sicherheit**.
6. Klicken Sie Auf **Erweitert**.
7. Wählen Sie die Registerkarte **Revision** aus.
8. Führen Sie die gewünschten Aktionen aus:

| Wenn Sie... wollen  | Gehen Sie wie folgt vor   |
|---|---|
| Einrichten der Prüfung für einen neuen Benutzer oder eine neue Gruppe | <ol style="list-style-type: none"> <li>a. Klicken Sie Auf <b>Hinzufügen</b>.</li> <li>b. Geben Sie in das Feld Objektnamen eingeben, um auszuwählen, den Namen des Benutzers oder der Gruppe ein, den Sie hinzufügen möchten.</li> <li>c. Klicken Sie auf <b>OK</b>.</li> </ol>                         |
| Audit von einem Benutzer oder einer Gruppe entfernen                  | <ol style="list-style-type: none"> <li>a. Wählen Sie im Feld Objektnamen eingeben den Benutzer oder die Gruppe aus, die Sie entfernen möchten.</li> <li>b. Klicken Sie Auf <b>Entfernen</b>.</li> <li>c. Klicken Sie auf <b>OK</b>.</li> <li>d. Überspringen Sie den Rest dieses Verfahrens.</li> </ol> |
| Ändern Sie die Prüfung für einen Benutzer oder eine Gruppe            | <ol style="list-style-type: none"> <li>a. Wählen Sie im Feld Objektnamen eingeben den Benutzer oder die Gruppe aus, die Sie ändern möchten.</li> <li>b. Klicken Sie Auf <b>Bearbeiten</b>.</li> <li>c. Klicken Sie auf <b>OK</b>.</li> </ol>  |

Wenn Sie eine Prüfung für einen Benutzer oder eine Gruppe einrichten oder die Prüfung für einen vorhandenen Benutzer oder eine vorhandene Gruppe ändern, wird das Feld Überwachungseintrag für <Object> geöffnet.

9. Wählen Sie im Feld **Apply to** aus, wie Sie diesen Prüfungseintrag anwenden möchten.

Sie können eine der folgenden Optionen auswählen:

- **Dieser Ordner, Unterordner und Dateien**
- **Dieser Ordner und Unterordner**
- **Nur dieser Ordner**
- **Dieser Ordner und die Dateien**
- **Nur Unterordner und Dateien**
- **Nur Unterordner**
- **Nur Dateien** Wenn Sie eine Prüfung auf eine einzelne Datei einrichten, ist die Box **Apply to** nicht aktiv. Die Einstellung **auf** anwenden ist standardmäßig auf **nur dieses Objekt** eingestellt.



Da durch das Auditing SVM-Ressourcen belegt werden, wählen Sie nur die minimale Stufe aus, die die Auditing-Ereignisse erfüllt, die Ihre Sicherheitsanforderungen erfüllen.

10. Wählen Sie im Feld **Zugriff** aus, was geprüft werden soll und ob erfolgreiche Ereignisse, Fehlereignisse oder beides geprüft werden sollen.

- Wenn erfolgreiche Ereignisse geprüft werden sollen, wählen Sie das Feld Erfolg aus.
- Um Fehlerereignisse zu überwachen, wählen Sie das Feld Fehler aus.

Wählen Sie nur die Aktionen aus, die Sie überwachen müssen, um Ihre Sicherheitsanforderungen zu erfüllen. Weitere Informationen zu diesen prüffähigen Ereignissen finden Sie in Ihrer Windows-Dokumentation. Sie können die folgenden Ereignisse prüfen:

- **Volle Kontrolle**
- **Traverse Ordner / Datei ausführen**
- **Ordner auflisten / Daten lesen**
- **Attribute lesen**
- **Erweiterte Attribute lesen**
- **Dateien erstellen / Daten schreiben**
- **Ordner erstellen / Daten anhängen**
- **Attribute schreiben**
- **Erweiterte Attribute schreiben**
- **Löschen von Unterordnern und Dateien**
- **Löschen**
- **Berechtigungen lesen**
- **Berechtigungen ändern**
- **Besitzrechte übernehmen**

11. Wenn Sie nicht möchten, dass sich die Überwachungseinstellung auf nachfolgende Dateien und Ordner des ursprünglichen Containers verbreitet, wählen Sie die Option **Diese Überwachungseinträge auf Objekte und/oder Container innerhalb dieses Containers only** anwenden aus.
12. Klicken Sie Auf **Anwenden**.
13. Klicken Sie nach dem Hinzufügen, Entfernen oder Bearbeiten von Prüfungseinträgen auf **OK**.

Das Feld Überwachungseintrag für <Object> wird geschlossen.

14. Wählen Sie im Feld **Revision** die Vererbungseinstellungen für diesen Ordner aus.

Wählen Sie nur die minimale Stufe aus, die die Überwachungsereignisse enthält, die Ihren Sicherheitsanforderungen entsprechen. Sie können eine der folgenden Optionen auswählen:

- Wählen Sie aus dem übergeordneten Feld dieses Objekts die Option vererbbare Überwachungseinträge einschließen aus.
- Wählen Sie das Kontrollkästchen Alle bestehenden vererbbsen Überwachungseinträge für alle abhängigen Elemente durch vererbbsen Prüfeinträge aus diesem Objekt ersetzen aus.
- Wählen Sie beide Felder aus.
- Wählen Sie keine der Kontrollkästchen aus. Wenn Sie SACLs auf eine einzelne Datei setzen, ist das Ersetzen aller vorhandenen vererbbsen Überwachungseinträge auf allen Nachkommen durch vererbbsen Prüfeinträge aus diesem Objektfeld nicht im Feld Auditing vorhanden.

15. Klicken Sie auf **OK**.

Das Feld Auditing wird geschlossen.

## Konfigurieren Sie die NTFS-Audit-Richtlinien mithilfe der ONTAP-CLI

Über die ONTAP-Befehlszeilenschnittstelle können Sie die Audit-Richtlinien für Dateien und Ordner konfigurieren. So können Sie NTFS-Audit-Richtlinien konfigurieren, ohne dass eine Verbindung zu den Daten über eine SMB-Freigabe auf einem Windows-Client hergestellt werden muss.

Sie können NTFS-Audit-Richtlinien mit konfigurieren `vserver security file-directory` Befehlsfamilie.

Sie können NTFS SACLs nur mit der CLI konfigurieren. Das Konfigurieren von NFSv4 SACLs wird von dieser ONTAP-Befehlsfamilie nicht unterstützt. Weitere Informationen über die Verwendung dieser Befehle zum Konfigurieren und Hinzufügen von NTFS-SACLs zu Dateien und Ordnern finden Sie auf den man-Pages.

## Konfigurieren Sie Auditing für Dateien und Verzeichnisse im UNIX-Sicherheitsstil

Sie konfigurieren Audit für Dateien und Verzeichnisse im UNIX-Sicherheitsstil durch Hinzufügen von Audit ACLs zu NFSv4.x ACLs. So können Sie bestimmte NFS-Datei- und Verzeichniszugriffe zu Sicherheitszwecken überwachen.

### Über diese Aufgabe

Für NFSv4.x sind Ermessenswert- und SystemAsse in derselben ACL gespeichert. Sie werden nicht in separaten DACLs und SACLs gespeichert. Daher müssen Sie beim Hinzufügen von Audit Aces zu einer vorhandenen ACL Vorsicht walten lassen, um zu vermeiden, dass eine vorhandene ACL überschrieben und verloren geht. Die Reihenfolge, in der Sie die Audit Aces zu einer bestehenden ACL hinzufügen, ist nicht von Bedeutung.

### Schritte

1. Rufen Sie die vorhandene ACL für die Datei oder das Verzeichnis mithilfe von `ab nfs4_getfacl` Oder gleichwertiger Befehl.

Weitere Informationen zum Bearbeiten von ACLs finden Sie in den man-Pages des NFS-Clients.

2. Fügen Sie die gewünschten Audit Aces hinzu.
3. Wenden Sie die aktualisierte ACL mithilfe des auf die Datei oder das Verzeichnis an `nfs4_setfacl` Oder gleichwertiger Befehl.

## Informationen über auf Dateien und Verzeichnisse angewandte Audit-Richtlinien anzeigen

### Zeigen Sie Informationen über Überwachungsrichtlinien mithilfe der Registerkarte Windows-Sicherheit an

Sie können Informationen zu Audit-Richtlinien anzeigen, die auf Dateien und Verzeichnisse angewendet wurden, indem Sie die Registerkarte Sicherheit im Fenster Windows-Eigenschaften verwenden. Das ist dieselbe Methode für Daten auf einem Windows Server, mit der Kunden dieselbe Benutzeroberfläche nutzen können, die sie bereits kennen.

### Über diese Aufgabe

Durch das Anzeigen von Informationen über Überwachungsrichtlinien, die auf Dateien und Verzeichnisse angewendet werden, können Sie überprüfen, ob die entsprechenden SACLs (System Access Control Lists) für



bestimmte Dateien und Ordner festgelegt sind.

Führen Sie die folgenden Schritte auf einem Windows-Host aus, um Informationen über SACLs anzuzeigen, die auf NTFS-Dateien und -Ordner angewendet wurden.

### Schritte

1. Wählen Sie im Menü **Tools** im Windows Explorer die Option **Netzwerklaufwerk zuordnen** aus.
2. Füllen Sie das Dialogfeld **Map Network Drive** aus:
  - a. Wählen Sie einen **Drive**-Buchstaben aus.
  - b. Geben Sie im Feld **Ordner** die IP-Adresse oder den Namen des SMB-Servers der virtuellen Speichermaschine (SVM) ein, die den Share enthält, der sowohl die zu prüfenden Daten als auch den Namen der Freigabe enthält.

Wenn der Name Ihres SMB-Servers „SMB\_SERVER“ lautet und Ihre Freigabe den Namen „share1“ hat, sollten Sie eingeben \\SMB\_SERVER\share1.



Sie können anstelle des SMB-Servernamens die IP-Adresse der Datenschnittstelle für den SMB-Server angeben.

- c. Klicken Sie Auf **Fertig Stellen**.

Das ausgewählte Laufwerk ist mit dem Windows Explorer-Fenster verbunden und bereit, in dem die Dateien und Ordner in der Freigabe angezeigt werden.

3. Wählen Sie die Datei oder das Verzeichnis aus, für das Sie Audit-Informationen anzeigen.
4. Klicken Sie mit der rechten Maustaste auf die Datei oder das Verzeichnis, und wählen Sie **Eigenschaften**.
5. Wählen Sie die Registerkarte **Sicherheit**.
6. Klicken Sie Auf **Erweitert**.
7. Wählen Sie die Registerkarte **Revision** aus.
8. Klicken Sie Auf **Weiter**.

Das Feld Auditing wird geöffnet. Das Feld \* Revisionseinträge\* zeigt eine Zusammenfassung von Benutzern und Gruppen an, deren SACLs auf sie angewendet wurden.

9. Wählen Sie im Feld \* Überwachungseinträge\* den Benutzer oder die Gruppe aus, deren SACL-Einträge angezeigt werden sollen.
10. Klicken Sie Auf **Bearbeiten**.

Der Überwachungseintrag für <object> wird geöffnet.

11. Zeigen Sie im Feld **Zugriff** die aktuellen SACLs an, die auf das ausgewählte Objekt angewendet werden.
12. Klicken Sie auf **Abbrechen**, um das Feld **Prüfeintrag für <Object>** zu schließen.
13. Klicken Sie auf **Abbrechen**, um das Feld **Revision** zu schließen.

### Zeigt Informationen zu NTFS-Audit-Richtlinien auf FlexVol-Volumes mithilfe der CLI an

Sie können Informationen zu NTFS-Audit-Richtlinien auf FlexVol Volumes anzeigen,

einschließlich der Sicherheitsstile und effektiven Sicherheitsstile, der angewandten Berechtigungen und Informationen zu Zugriffssteuerungslisten des Systems. Sie können die Informationen zur Überprüfung der Sicherheitskonfiguration oder zur Fehlerbehebung bei Audit-Problemen verwenden.

### Über diese Aufgabe

Durch das Anzeigen von Informationen über Überwachungsrichtlinien, die auf Dateien und Verzeichnisse angewendet werden, können Sie überprüfen, ob die entsprechenden SACLs (System Access Control Lists) für bestimmte Dateien und Ordner festgelegt sind.

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Dateien oder Ordnern angeben, deren Audit-Informationen angezeigt werden sollen. Sie können die Ausgabe als Übersichtsformular oder als detaillierte Liste anzeigen.

- Bei NTFS-Volumes und qtrees werden für Audit-Richtlinien nur NTFS-Systemzugriffssteuerungslisten (SACLs) verwendet.
- Dateien und Ordner in einem gemischten Security-Stil-Volume mit NTFS effektive Sicherheit können NTFS-Audit-Richtlinien auf sie angewendet werden.

Gemischte sicherheitsrelevante Volumes und qtrees können einige Dateien und Verzeichnisse enthalten, die UNIX-Dateiberechtigungen verwenden, entweder Modus-Bits oder NFSv4-ACLs und einige Dateien und Verzeichnisse, die NTFS-Dateiberechtigungen verwenden.

- Die oberste Ebene eines gemischten Security-Volumes kann entweder UNIX oder NTFS effektive Sicherheit haben und möglicherweise NTFS SACLs enthalten.
- Da die Sicherheit des Storage-Level Access Guard auf einem Volume oder qtree mit gemischtem Sicherheitsstil konfiguriert werden kann, selbst wenn der effektive Sicherheitsstil des Volume Root oder qtree UNIX ist, Die Ausgabe für einen Volume- oder qtree-Pfad, wo Storage-Level Access Guard konfiguriert ist, zeigt möglicherweise sowohl normale Datei als auch Ordner NFSv4 SACLs und Storage-Level Access Guard NTFS SACLs an.
- Wenn der im Befehl eingegebene Pfad zu Daten mit NTFS-effektiver Sicherheit besteht, zeigt die Ausgabe auch Informationen über Dynamic Access Control Aces an, wenn Dynamic Access Control für den angegebenen Datei- oder Verzeichnispfad konfiguriert ist.
- Wenn Sicherheitsinformationen über Dateien und Ordner mit NTFS-effektiver Sicherheit angezeigt werden, enthalten UNIX-bezogene Ausgabefelder nur Informationen über die Berechtigung von UNIX-Dateien.

NTFS-Dateien und -Ordner verwenden bei der Ermittlung der Zugriffsrechte auf Dateien nur NTFS-Dateiberechtigungen und Windows-Benutzer und -Gruppen.

- Die ACL-Ausgabe wird nur für Dateien und Ordner mit NTFS- oder NFSv4-Sicherheit angezeigt.

Dieses Feld ist leer für Dateien und Ordner, die UNIX-Sicherheit verwenden, die nur Modus-Bit-Berechtigungen angewendet haben (keine NFSv4 ACLs).

- Die Felder „Eigentümer“ und „Gruppenausgabe“ in der ACL-Ausgabe gelten nur bei NTFS-Sicherheitsdeskriptoren.

### Schritt

1. Anzeige von Datei- und Verzeichnisaudits-Einstellungen mit der gewünschten Detailebene:

|                           |                                       |
|---------------------------|---------------------------------------|
| Informationen anzeigen... | Geben Sie den folgenden Befehl ein... |
|---------------------------|---------------------------------------|

|                            |  |
|----------------------------|--|
| In zusammengefassener Form | <code>vserver security file-directory show -vserver vserver_name -path path</code>                   |
| Als detaillierte Liste     | <code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code> |

## Beispiele

Im folgenden Beispiel werden die Informationen zu den Überwachungsrichtlinien für den Pfad angezeigt /corp in SVM vs1. Der Pfad verfügt über NTFS effektive Sicherheit. Der NTFS-Sicherheitsdeskriptor enthält sowohl einen ERFOLG als auch einen SACL-Eintrag FÜR ERFOLG/FEHLER.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
      Vserver: vs1
      File Path: /corp
      File Inode Number: 357
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8014
            Owner:DOMAIN\Administrator
            Group:BUILTIN\Administrators
            SACL - ACEs
                  ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                  SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
            DACL - ACEs
                  ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                  ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                  ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                  ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

Im folgenden Beispiel werden die Informationen zu den Überwachungsrichtlinien für den Pfad angezeigt /datavol1 in SVM vs1. Der Pfad enthält sowohl normale Datei- als auch Ordner-SACLs und Speicher-Level Access Guard SACLs.

```

cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

      Vserver: vs1
      File Path: /datavol1
      File Inode Number: 77
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0xaa14
            Owner: BUILTIN\Administrators
            Group: BUILTIN\Administrators
            SACL - ACEs
                  AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
            DACL - ACEs
                  ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                  ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

      Storage-Level Access Guard security
      SACL (Applies to Directories):
            AUDIT-EXAMPLE\Domain Users-0x120089-FA
            AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Directories):
            ALLOW-EXAMPLE\Domain Users-0x120089
            ALLOW-EXAMPLE\engineering-0x1f01ff
            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
      SACL (Applies to Files):
            AUDIT-EXAMPLE\Domain Users-0x120089-FA
            AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Files):
            ALLOW-EXAMPLE\Domain Users-0x120089
            ALLOW-EXAMPLE\engineering-0x1f01ff
            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

## **Möglichkeiten zum Anzeigen von Informationen über Dateisicherheitsrichtlinien und Audit-Richtlinien**

Mithilfe des Platzhalterzeichens (\*) können Sie Informationen über Dateisicherheit und

Audit-Richtlinien aller Dateien und Verzeichnisse unter einem bestimmten Pfad oder einem Root-Volume anzeigen.

Das Platzhalterzeichen (\*) kann als letzte Unterkomponente eines bestimmten Verzeichnispfades verwendet werden, unter dem Sie Informationen zu allen Dateien und Verzeichnissen anzeigen möchten.

Wenn Sie Informationen zu einer bestimmten Datei oder einem Verzeichnis mit dem Namen „\*“ anzeigen möchten, müssen Sie den vollständigen Pfad innerhalb doppelter Anführungszeichen („ “) angeben.

### **Beispiel**

Mit dem folgenden Befehl mit dem Platzhalterzeichen werden die Informationen über alle Dateien und Verzeichnisse unter dem Pfad angezeigt / 1 / Von SVM vs1:

```

cluster::> vserver security file-directory show -vserver vs1 -path /1/*

      Vserver: vs1
      File Path: /1/1
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8514
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

      Vserver: vs1
      File Path: /1/1/abc
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8404
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

```

Mit dem folgenden Befehl werden Informationen zu einer Datei mit dem Namen „\*\*“ unter dem Pfad angezeigt /vol1/a Von SVM vs1. Der Pfad ist in doppelte Anführungszeichen eingeschlossen (" ").

```
cluster::> vservers security file-directory show -vservers vs1 -path  
"/vol1/a/*"
```

```
      Vserver: vs1  
      File Path: "/vol1/a/*"  
      Security Style: mixed  
      Effective Style: unix  
      DOS Attributes: 10  
      DOS Attributes in Text: ----D---  
      Expanded Dos Attributes: -  
      Unix User Id: 1002  
      Unix Group Id: 65533  
      Unix Mode Bits: 755  
      Unix Mode Bits in Text: rwxr-xr-x  
      ACLs: NFSV4 Security Descriptor  
      Control:0x8014  
      SACL - ACEs  
      AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA  
      DACL - ACEs  
      ALLOW-EVERYONE@-0x1f00a9-FI|DI  
      ALLOW-OWNER@-0x1f01ff-FI|DI  
      ALLOW-GROUP@-0x1200a9-IG
```

## Änderungsereignisse in der CLI, die geprüft werden können

### Änderungsereignisse in der CLI, die geprüft werden können, Übersicht

ONTAP kann bestimmte CLI-Änderungsereignisse prüfen, darunter bestimmte SMB-Share-Ereignisse, bestimmte Audit-Richtlinienereignisse, bestimmte lokale Ereignisse von Sicherheitsgruppen, Ereignisse lokaler Benutzergruppen und Autorisierungsrichtlinien. Das Verständnis, welche Änderungsereignisse überprüft werden können, ist hilfreich bei der Interpretation der Ergebnisse aus den Ereignisprotokollen.

Sie können die Ereignisse, die auf einer Storage Virtual Machine (SVM) stattfinden, verwalten, indem Sie die Überwachungsprotokolle manuell drehen, die Prüfung aktivieren oder deaktivieren, Informationen über das Auditing von Änderungsereignissen anzeigen, Änderungsereignisse für das Auditing ändern und Änderungsereignisse für das Auditing löschen.

Wenn Sie als Administrator einen beliebigen Befehl zum Ändern der Konfiguration in Bezug auf SMB-Share, lokale Benutzergruppe, lokale Sicherheitsgruppe, Autorisierungsrichtlinie und Ereignis für Prüfrichtlinien ausführen, ein Datensatz erzeugt und das entsprechende Ereignis wird auditiert:

| Kategorie „Audits“ | Veranstaltungen | Ereignis-IDs | Führen Sie diesen Befehl aus... |
|--------------------|-----------------|--------------|---------------------------------|
|--------------------|-----------------|--------------|---------------------------------|

|  |  |  |  |
|--|--|--|--|
| Mhost Auditing   | Richtlinienänderung  | [4719] Audit-Konfiguration geändert  | `vserver audit disable   |
| enable   | modify`  | Dateifreigabe  | [5142] Netzwerkfreigabe wurde hinzugefügt  |
| vserver cifs share create  | [5143] Netzwerkfreigabe wurde geändert   | vserver cifs share modify `vserver cifs share create   | modify   |
| delete` `vserver cifs share add  | remove`  | [5144] Netzwerkfreigabe gelöscht   | vserver cifs share delete  |
| Prüfung  | Benutzerkonto  | [4720] lokaler Benutzer erstellt   | vserver cifs users-and-groups local-user create vserver services name-service unix-user create |
| [4722] lokaler Benutzer aktiviert  | `vserver cifs users-and-groups local-user create   | modify`  | [4724] Zurücksetzen des lokalen Benutzerpassworts  |
| vserver cifs users-and-groups local-user set-password  | [4725] lokaler Benutzer deaktiviert  | `vserver cifs users-and-groups local-user create   | modify`  |
| [4726] lokaler Benutzer gelöscht   | vserver cifs users-and-groups local-user delete vserver services name-service unix-user delete | [4738] Lokale Benutzeränderung   | vserver cifs users-and-groups local-user modify vserver services name-service unix-user modify |
| [4781] lokaler Benutzer umbenennen   | vserver cifs users-and-groups local-user rename  | Sicherheitsgruppe  | [4731] Lokale Sicherheitsgruppe erstellt   |
| vserver cifs users-and-groups local-group create vserver services name-service unix-group create | [4734] Lokale Sicherheitsgruppe gelöscht   | vserver cifs users-and-groups local-group delete vserver services name-service unix-group delete | [4735] Lokale Sicherheitsgruppe Geändert   |



|  |  |  |   |
|--|--|--|---|
| <code>`vserver cifs users-and-groups local-group rename</code>     | <code>modify` vserver services name-service unix-group modify</code>   | [4732] Benutzer zur lokalen Gruppe hinzugefügt                         | <code>vserver cifs users-and-groups local-group add-members vserver services name-service unix-group adduser</code> |
| [4733] Benutzer aus der lokalen Gruppe entfernt                    | <code>vserver cifs users-and-groups local-group remove-members vserver services name-service unix-group deluser</code> | Änderung der Autorisierungsrichtlinie                                  | [4704] Benutzerrechte Zugewiesen  |
| <code>vserver cifs users-and-groups privilege add-privilege</code> | [4705] Benutzerrechte Entfernt   | <code>`vserver cifs users-and-groups privilege remove-privilege</code> | <code>reset-privilege`</code>   |

## Dateifreigabe-Ereignisse verwalten

Wenn ein Dateifreigabe-Ereignis für eine Storage Virtual Machine (SVM) konfiguriert ist und ein Audit aktiviert ist, werden Audit-Ereignisse generiert. Die Dateifreigabe-Ereignisse werden generiert, wenn die SMB-Netzwerkfreigabe mit geändert wird `vserver cifs share` Ähnliche Befehle.

Die Dateifreigabe-Ereignisse mit den Ereignis-ids 5142, 5143 und 5144 werden generiert, wenn eine SMB-Netzwerkfreigabe für die SVM hinzugefügt, geändert oder gelöscht wird. Die Konfiguration der SMB-Netzwerkfreigabe wird mithilfe des geändert `cifs share access control create|modify|delete` Befehle.

Im folgenden Beispiel wird ein Dateifreigabe-Ereignis mit der ID 5143 erzeugt, wenn ein Freigabetobjekt namens 'Audit\_dest' erstellt wird:

```

netapp-clus1::*> cifs share create -share-name audit_dest -path
/audit_dest
- System
  - Provider
    [ Name]   NetApp-Security-Auditing
    [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
    EventID  5142
    EventName Share Object Added
    ...
    ...
    ShareName audit_dest
    SharePath /audit_dest
    ShareProperties oplocks;browsable;changenotify;show-previous-versions;
    SD O:BAG:S-1-5-21-2447422786-1297661003-4197201688-513D:(A;;;FA;;;WD)

```

## Management von Änderungs- und Audit-Richtlinien

Wenn ein Ereignis für die Änderung von Audit-Richtlinien für eine Storage Virtual Machine (SVM) konfiguriert und ein Audit aktiviert ist, werden Audit-Ereignisse generiert. Die Ereignisse der Revisionspolitik-Änderung werden generiert, wenn eine Audit-Richtlinie mit geändert wird `vserver audit` Ähnliche Befehle.

Das Ereignis „Audit-Policy-change“ mit der Ereignis Event-id 4719 wird immer dann generiert, wenn eine Audit-Richtlinie deaktiviert, aktiviert oder geändert wird. Außerdem wird festgestellt, wann ein Benutzer versucht, die Prüfung für die Tracks zu deaktivieren. Er ist standardmäßig konfiguriert und erfordert zum Deaktivieren Diagnoseberechtigung.

Im folgenden Beispiel wird ein Änderungsereignis für die Audit-Richtlinie mit der generierten ID 4719 angezeigt, wenn ein Audit deaktiviert ist:

```

netapp-clus1::*> vserver audit disable -vserver vserver_1
- System
  - Provider
    [ Name]   NetApp-Security-Auditing
    [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
    EventID  4719
    EventName Audit Disabled
    ...
    ...
    SubjectUserName admin
    SubjectUserSid 65533-1001
    SubjectDomainName ~
    SubjectIP console
    SubjectPort

```

## Verwalten von Benutzerkontenereignis

Wenn ein Benutzerkontenereignis für eine Storage Virtual Machine (SVM) konfiguriert ist und ein Audit aktiviert ist, werden Audit-Ereignisse generiert.

Ereignisse des Benutzerkontos mit Event-ids 4720, 4722, 4724, 4725, 4726 4738 und 4781 werden generiert, wenn ein lokaler SMB- oder NFS-Benutzer aus dem System erstellt oder gelöscht wird, ein lokales Benutzerkonto ist aktiviert, deaktiviert oder geändert und das lokale SMB-Benutzerpasswort wird zurückgesetzt oder geändert. Die Benutzerkontoereignisse werden generiert, wenn ein Benutzerkonto mit `vserver cifs users-and-groups <local user>` Und `vserver services name-service <unix user>` Befehle.

Im folgenden Beispiel wird ein Benutzerkontoereignis mit der ID 4720 angezeigt, das beim Erstellen eines lokalen SMB-Benutzers generiert wurde:

```
netapp-clus1::*> vserver cifs users-and-groups local-user create -user
-name testuser -is-account-disabled false -vserver vserver_1
Enter the password:
Confirm the password:

- System
- Provider
  [ Name]   NetApp-Security-Auditing
  [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
  EventID  4720
  EventName Local Cifs User Created
  ...
  ...
  TargetUserName testuser
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1003
  TargetType CIFS
  DisplayName testuser
  PasswordLastSet 1472662216
  AccountExpires NO
  PrimaryGroupId 513
  UserAccountControl %%0200
  SidHistory ~
  PrivilegeList ~
```

Im folgenden Beispiel wird ein Benutzerkontoereignis mit der anhand der ID 4781 erstellten ID angezeigt, wenn der im vorhergehenden Beispiel erstellte lokale SMB-Benutzer umbenannt wird:

```

netapp-clus1::*> vserver cifs users-and-groups local-user rename -user
-name testuser -new-user-name testuser1
- System
- Provider
  [ Name]   NetApp-Security-Auditing
  [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
  EventID  4781
  EventName Local Cifs User Renamed
  ...
  ...
  OldTargetUserName testuser
  NewTargetUserName testuser1
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1000
  TargetType CIFS
  SidHistory ~
  PrivilegeList ~

```

## Verwalten von Sicherheitsereignisereignis

Wenn ein Sicherheitsereignis für eine Storage Virtual Machine (SVM) konfiguriert ist und ein Audit aktiviert ist, werden Audit-Ereignisse generiert.

Die Ereignisse der Sicherheitsgruppe mit Ereignis-ids 4731, 4732, 4733, 4734 und 4735 werden generiert, wenn eine lokale SMB- oder NFS-Gruppe aus dem System erstellt oder gelöscht wird und der lokale Benutzer aus der Gruppe hinzugefügt oder entfernt wird. Die Ereignisse der Sicherheitsgruppe werden generiert, wenn ein Benutzerkonto mit geändert wird `vserver cifs users-and-groups <local-group>` Und `vserver services name-service <unix-group>` Befehle.

Im folgenden Beispiel wird ein Ereignis der Sicherheitsgruppe mit der generierten ID 4731 angezeigt, wenn eine lokale UNIX-Sicherheitsgruppe erstellt wird:

```

netapp-clus1::*> vserver services name-service unix-group create -name
testunixgroup -id 20
- System
- Provider
  [ Name]   NetApp-Security-Auditing
  [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
  EventID  4731
  EventName Local Unix Security Group Created
  ...
  ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
  TargetUserName testunixgroup
  TargetDomainName
  TargetGid 20
  TargetType NFS
  PrivilegeList ~
  GidHistory ~

```

## Management von Berechtigungs- und Richtlinienänderungen

Wenn ein Ereignis zur Änderung von Autorisierungsrichtlinien für eine Storage Virtual Machine (SVM) konfiguriert ist und ein Audit aktiviert ist, werden Audit-Ereignisse generiert.

Die Ereignisse mit den Ereignis-ids 4704 und 4705 werden generiert, sobald die Autorisierungsrechte für einen SMB-Benutzer und eine SMB-Gruppe erteilt oder widerrufen werden. Die Ereignisse zur Änderung der Autorisierungsrichtlinie werden generiert, wenn die Autorisierungsrechte mit zugewiesen oder widerrufen werden `vserver cifs users-and-groups privilege` Ähnliche Befehle.

Im folgenden Beispiel wird ein Ereignis für die Autorisierungsrichtlinie mit der generierten ID 4704 angezeigt, wenn die Autorisierungsrechte für eine SMB-Benutzergruppe zugewiesen sind:

```

netapp-clus1::*> vserver cifs users-and-groups privilege add-privilege
-user-or-group-name testcifslocalgroup -privileges *
- System
- Provider
  [ Name]   NetApp-Security-Auditing
  [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
  EventID   4704
  EventName User Right Assigned
  ...
  ...
  TargetUserOrGroupName testcifslocalgroup
  TargetUserOrGroupDomainName NETAPP-CLUS1
  TargetUserOrGroupSid S-1-5-21-2447422786-1297661003-4197201688-1004;
  PrivilegeList
  SeTcbPrivilege;SeBackupPrivilege;SeRestorePrivilege;SeTakeOwnershipPrivile
ge;SeSecurityPrivilege;SeChangeNotifyPrivilege;
  TargetType CIFS

```

## Management von Audit-Konfigurationen

### Drehen Sie die Überwachungsprotokolle manuell

Bevor Sie die Protokolle der Audit-Ereignisse anzeigen können, müssen die Protokolle in benutzerlesbare Formate konvertiert werden. Wenn Sie die Ereignisprotokolle für eine bestimmte Storage Virtual Machine (SVM) anzeigen möchten, bevor ONTAP das Protokoll automatisch rotiert, können Sie die Überwachungsprotokolle auf einer SVM manuell drehen.

#### Schritt

1. Drehen Sie die Überwachungsprotokolle mit dem `vserver audit rotate-log` Befehl.

```
vserver audit rotate-log -vserver vs1
```

Das Revisionsprotokoll wird im SVM-Audit-Ereignisprotokoll mit dem von der Audit-Konfiguration angegebenen Format gespeichert (XML Oder EVT), und kann mit der entsprechenden Anwendung angezeigt werden.

### Aktivieren und Deaktivieren der Prüfung auf SVMs

Sie können die Überprüfung auf Storage Virtual Machines (SVMs) aktivieren oder deaktivieren. Möglicherweise möchten Sie die Datei- und Verzeichnisüberprüfung vorübergehend beenden, indem Sie die Prüfung deaktivieren. Sie können die Prüfung jederzeit aktivieren (falls eine Überwachungskonfiguration vorhanden ist).

#### Was Sie benötigen

Bevor Sie Auditing auf der SVM aktivieren können, muss die Auditing-Konfiguration der SVM bereits vorhanden sein.

### "Erstellen Sie die Überwachungskonfiguration"

#### Über diese Aufgabe

Durch Deaktivieren der Prüfung wird die Konfiguration der Prüfung nicht gelöscht.

#### Schritte

1. Führen Sie den entsprechenden Befehl aus:

| Wenn Prüfung ausgeführt werden soll... | Geben Sie den Befehl ein...                              |
|--|--|
| Aktiviert                              | <code>vserver audit enable -vserver vserver_name</code>  |
| Deaktiviert                            | <code>vserver audit disable -vserver vserver_name</code> |

2. Überprüfen Sie, ob die Prüfung den gewünschten Status hat:

```
vserver audit show -vserver vserver_name
```

#### Beispiele

Das folgende Beispiel ermöglicht das Auditing von SVM vs1:

```
cluster1::> vserver audit enable -vserver vs1

cluster1::> vserver audit show -vserver vs1

                Vserver: vs1
            Auditing state: true
      Log Destination Path: /audit_log
Categories of Events to Audit: file-ops, cifs-logon-logoff
                Log Format: evtX
            Log File Size Limit: 100MB
    Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
        Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
    Log Rotation Schedule: Minute: -
            Rotation Schedules: -
        Log Files Rotation Limit: 10
```

Im folgenden Beispiel wird das Auditing von SVM vs1 deaktiviert:

```
cluster1::> vserver audit disable -vserver vs1
```

```

                Vserver: vs1
            Auditing state: false
        Log Destination Path: /audit_log
Categories of Events to Audit: file-ops, cifs-logon-logoff
                Log Format: evtX
            Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
            Log Rotation Schedule: Day: -
            Log Rotation Schedule: Hour: -
        Log Rotation Schedule: Minute: -
                Rotation Schedules: -
            Log Files Rotation Limit: 10
```

## Zeigt Informationen zu Überwachungskonfigurationen an

Sie können Informationen zu Überwachungskonfigurationen anzeigen. Diese Informationen unterstützen Sie bei der Ermittlung der gewünschten Konfiguration für die jeweilige SVM. Mit den angezeigten Informationen können Sie auch überprüfen, ob eine Überwachungskonfiguration aktiviert ist.

### Über diese Aufgabe

Sie können ausführliche Informationen zum Auditing von Konfigurationen auf allen SVMs anzeigen oder Sie können durch Angabe optionaler Parameter anpassen, welche Informationen in der Ausgabe angezeigt werden. Wenn Sie keinen der optionalen Parameter angeben, wird Folgendes angezeigt:

- SVM-Name, auf den die Audit-Konfiguration zutrifft
- Der Prüfstatus, der sein kann `true` Oder `false`

Wenn der Prüfstatus lautet `true`, Prüfung ist aktiviert. Wenn der Prüfstatus lautet `false`, Prüfung ist deaktiviert.

- Die Kategorien der zu prüfenden Ereignisse
- Das Format des Prüfprotokolls
- Das Zielverzeichnis, in dem das Audit-Subsystem konsolidierte und konvertierte Audit-Protokolle speichert

### Schritt

1. Zeigen Sie Informationen über die Überwachungskonfiguration mithilfe des `an vserver audit show` Befehl.

Weitere Informationen zur Verwendung des Befehls finden Sie in den man-Pages.

### Beispiele

Im folgenden Beispiel wird eine Zusammenfassung der Audit-Konfiguration für alle SVMs angezeigt:



```
cluster1::> vserver audit show
```

| Vserver | State | Event Types | Log Format | Target Directory |
|---------|-------|-------------|------------|------------------|
| vs1     | false | file-ops    | evtx       | /audit_log       |

Im folgenden Beispiel werden alle Audit-Konfigurationsinformationen für alle SVMs in Listenform angezeigt:


```
cluster1::> vserver audit show -instance
```

```
                Vserver: vs1
            Auditing state: true
        Log Destination Path: /audit_log
Categories of Events to Audit: file-ops
            Log Format: evtx
        Log File Size Limit: 100MB
    Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
        Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
    Log Rotation Schedule: Minute: -
            Rotation Schedules: -
        Log Files Rotation Limit: 0
```

## Befehle zum Ändern von Überwachungskonfigurationen

Wenn Sie eine Überwachungseinstellung ändern möchten, können Sie die aktuelle Konfiguration jederzeit ändern, einschließlich der Änderung des Protokollpfadziels und des Protokollformats, der Änderung der Kategorien von zu prüfenden Ereignissen, der automatischen Speicherung von Protokolldateien und der maximalen Anzahl der zu speicherenden Protokolldateien.

| Ihr Ziel ist                     | Befehl  |
|----------------------------------|---|
| Ändern Sie den Protokollzielpfad | <code>vserver audit modify</code> Mit dem <code>-destination</code> Parameter |

|   |   |
|---|---|
| Ändern Sie die Kategorie der zu prüfenden Ereignisse                                  | vserver audit modify Mit dem <code>-events</code> Parameter<br><br><div>  <p>Zur Prüfung von Staging von zentralen Zugriffsrichtlinien muss die SMB-Serveroption Dynamic Access Control (DAC) auf der Storage Virtual Machine (SVM) aktiviert sein.</p> </div> |
| Ändern Sie das Protokollformat  | vserver audit modify Mit dem <code>-format</code> Parameter   |
| Aktivieren von automatischen Speichern basierend auf der internen Protokolldateigröße | vserver audit modify Mit dem <code>-rotate-size</code> Parameter  |
| Durch Aktivieren der automatischen Einsparung auf Basis eines Zeitintervalls          | vserver audit modify Mit dem <code>-rotate-schedule-month, -rotate-schedule-dayofweek, -rotate-schedule-day, -rotate-schedule-hour, und -rotate-schedule-minute</code> Parameter  |
| Festlegen der maximalen Anzahl von gespeicherten Protokolldateien                     | vserver audit modify Mit dem <code>-rotate-limit</code> Parameter   |

## Löschen einer Überwachungskonfiguration

Wenn Datei- und Verzeichnisereignisse für die Storage Virtual Machine (SVM) nicht mehr geprüft und keine Auditing-Konfiguration auf der SVM beibehalten werden soll, können Sie die Audit-Konfiguration löschen.

### Schritte

1. Deaktivieren der Überwachungskonfiguration:

```
vserver audit disable -vserver vserver_name
```

```
vserver audit disable -vserver vs1
```

2. Löschen Sie die Überwachungskonfiguration:

```
vserver audit delete -vserver vserver_name
```

```
vserver audit delete -vserver vs1
```

## Auswirkungen des Zurücks des Clusters benennen

Wenn Sie den Cluster zurücksetzen möchten, sollten Sie auf den ONTAP für den Umkehrprozess achten, wenn es im Cluster Audit-fähige Storage Virtual Machines

(SVMs) gibt. Sie müssen bestimmte Aktionen durchführen, bevor Sie den Wechsel rückgängig machen.

### **Zurücksetzen auf eine Version von ONTAP, die keine Unterstützung für das Auditing von SMB-Anmeldeereignissen und Abmeldungs-Ereignissen sowie von Staging-Ereignissen für zentrale Zugriffsrichtlinien bietet**

Clustered Data ONTAP 8.3 unterstützt das Auditing von SMB-Anmeldeereignissen und Abmeldung sowie von zentralen Zugriffs-Policy-Staging-Ereignissen. Wenn Sie zurück zu einer Version von ONTAP wechseln, die diese Ereignistypen nicht unterstützt, und Sie verfügen über Auditing-Konfigurationen, die diese Ereignistypen überwachen, müssen Sie vor dem Zurücksetzen die Prüfungskonfiguration für diese revisionssigemeinsam verwendeten SVMs ändern. Sie müssen die Konfiguration so ändern, dass nur Datei-op-Ereignisse überprüft werden.

## **Fehlerbehebung bei Problemen mit Auditing und Staging von Volume-Speicherplatz**

Probleme können auftreten, wenn entweder auf den Staging-Volumes oder auf dem Volume, das die Audit-Ereignisprotokolle enthält, nicht genügend Speicherplatz vorhanden ist. Wenn nicht genügend Speicherplatz vorhanden ist, können keine neuen Audit-Datensätze erstellt werden. Dies verhindert, dass Clients auf Daten zugreifen und Zugriffsanforderungen fehlschlagen. Sie sollten wissen, wie Sie diese Probleme mit Volume-Speicherplatz beheben und beheben.

### **Behebung von Platzproblemen im Zusammenhang mit den Ereignisprotokollvolumes**

Wenn Volumes mit Ereignisprotokolldateien nicht mehr genügend Speicherplatz haben, können Protokolldatensätze durch Auditing nicht in Protokolldateien konvertiert werden. Dies führt zu einem Ausfall des Client-Zugriffs. Sie müssen wissen, wie die Behebung von Platzproblemen im Zusammenhang mit Ereignisprotokollvolumen behoben wird.

- SVM (Storage Virtual Machine) und Cluster-Administratoren können feststellen, ob nicht genügend Volume-Speicherplatz vorhanden ist, indem Informationen zur Auslastung und Konfiguration von Volumes und Aggregaten angezeigt werden.
- Falls in den Volumes, die Ereignisprotokolle enthalten, nicht genügend Speicherplatz verfügbar ist, können SVM- und Cluster-Administratoren diese Platzprobleme beheben, indem sie einige der Ereignisprotokolldateien entfernen oder die Größe des Volume erhöhen.



Wenn das Aggregat, das das Ereignisprotokoll enthält, voll ist, muss die Größe des Aggregats erhöht werden, bevor Sie die Größe des Volumes erhöhen können. Nur ein Cluster-Administrator kann die Größe eines Aggregats erhöhen.

- Der Zielpfad für die Ereignisprotokolldateien kann durch Ändern der Überwachungskonfiguration in ein Verzeichnis auf einem anderen Volume geändert werden.



Der Datenzugriff wird in den folgenden Fällen verweigert:

- Das Zielverzeichnis wird gelöscht.
- Die Dateibegrenzung auf einem Volume, das das Zielverzeichnis hostet, erreicht seine maximale Ebene.

Weitere Informationen:

- ["So erhalten Sie Informationen zu Volumes und zur Vergrößerung des Volumes"](#).
- ["Anzeigen von Informationen zu Aggregaten und zum Managen von Aggregaten"](#).

## Behebung von Platzproblemen im Zusammenhang mit den Staging-Volumes

Sollte einer der Volumes, die Staging-Dateien für die SVM (Storage Virtual Machine) enthalten, nicht mehr genügend Speicherplatz haben, kann die Prüfung Protokolldatensätze nicht in Staging-Dateien schreiben. Dies führt zu einem Ausfall des Client-Zugriffs. Um dieses Problem zu beheben, müssen Sie ermitteln, ob die in der SVM verwendeten Staging-Volumes durch die Anzeige von Informationen zur Volume-Nutzung vollständig sind.

Wenn das Volume, das die konsolidierten Ereignisprotokolldateien enthält, genügend Speicherplatz hat, aber aufgrund eines unzureichenden Speicherplatzes beim Client-Zugriff weiterhin besteht, sind die Staging-Volumes möglicherweise nicht mehr genügend Platz. Der SVM-Administrator muss sich mit Ihnen in Verbindung setzen, um zu ermitteln, ob die Staging-Volumes, die Staging-Dateien für die SVM enthalten, über unzureichenden Speicherplatz verfügen. Das Audit-Subsystem generiert ein EMS-Ereignis, wenn Überwachungsereignisse nicht generiert werden können, weil der Speicherplatz in einem Staging-Volume nicht ausreicht. Die folgende Meldung wird angezeigt: `No space left on device`. Nur Informationen zu Staging Volumes können angezeigt werden. SVM-Administratoren können dies nicht.

Alle Staging-Volume-Namen beginnen mit `MDV_aud_`. Anschließend die UUID des Aggregats, das das Staging-Volume enthält. Das folgende Beispiel zeigt vier System-Volumes auf der Administrator-SVM, die automatisch erstellt wurden, wenn eine Fileservices-Auditing-Konfiguration für eine Daten-SVM im Cluster erstellt wurde:

```
cluster1::> volume show -vserver cluster1
```

| Vserver  | Volume                                   | Aggregate | State  | Type  | Size  | Available |
|----------|--|-----------|--------|-------|-------|-----------|
| Used%    |  |           |        |       |       |           |
| -----    | -----                                    | -----     | -----  | ----- | ----- | -----     |
| -----    |  |           |        |       |       |           |
| cluster1 | MDV_aud_1d0131843d4811e296fc123478563412 | aggr0     | online | RW    | 5GB   | 4.75GB    |
| 5%       |  |           |        |       |       |           |
| cluster1 | MDV_aud_8be27f813d7311e296fc123478563412 | root_vs0  | online | RW    | 5GB   | 4.75GB    |
| 5%       |  |           |        |       |       |           |
| cluster1 | MDV_aud_9dc4ad503d7311e296fc123478563412 | aggr1     | online | RW    | 5GB   | 4.75GB    |
| 5%       |  |           |        |       |       |           |
| cluster1 | MDV_aud_a4b887ac3d7311e296fc123478563412 | aggr2     | online | RW    | 5GB   | 4.75GB    |
| 5%       |  |           |        |       |       |           |

4 entries were displayed.

Wenn der Speicherplatz in den Staging-Volumes nicht ausreicht, können Sie die Platzprobleme beheben, indem Sie die Größe des Volumes erhöhen.



Ist das Aggregat, das das Staging-Volume enthält, voll, muss die Größe des Aggregats erhöht werden, bevor Sie die Volume-Größe erhöhen können. Nur Sie können die Größe eines Aggregats erhöhen, was SVM-Administratoren nicht können.

Wenn ein oder mehrere Aggregate einen verfügbaren Speicherplatz von weniger als 2 GB (ab ONTAP 9.14.1) bzw. 5 GB (ab ONTAP 9.15.1) aufweisen, schlägt die SVM-Audit-Erstellung fehl. Wenn die Erstellung der SVM-Audits fehlschlägt, werden die erstellten Staging-Volumes gelöscht.

## Copyright-Informationen

Copyright © 2024 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.