NAS-Ereignisse auf SVMs überwachen

ONTAP 9

NetApp
September 09, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/nas-audit/index.html on September 09, 2026. Always check docs.netapp.com for the latest.

Inhalt

NAS-Ereignisse auf SVMs überwachen . . . 1
Informationen zur Überwachung des Dateizugriffs mit ONTAP für die Protokolle SMB und NFS . . . 1
NAS-Ereignisse auf SVMs überwachen . . . 1
Funktionsweise von Audits . . . 2
Die grundlegenden ONTAP Audit-Konzepte . . . 2
Informationen zur Funktionsweise des ONTAP-Auditprozesses . . . 3
Voraussetzungen für ONTAP Prüfung . . . 4
Überlegungen zum Aggregatspeicherplatz bei der Aktivierung der Überwachung . . . 6
Beschränkungen der Größe von Staging-Dateien für ONTAP Revisionsprotokolle . . . 6
Wann große Revisionsprotokolle auftreten können . . . 6
Die Auswirkungen von zu großen Revisionsprotokollen . . . 6
Informationen zu den unterstützten Formaten für ONTAP Audit-Ereignisprotokolle . . . 7
ONTAP Revisionsprotokolle für Ereignisse anzeigen und verarbeiten . . . 7
Wie aktive Revisionsprotokolle mit der Ereignisanzeige angezeigt werden . . . 8
SMB-Ereignisse, die geprüft werden können . . . 8
Informationen zu SMB-Ereignissen, die ONTAP prüfen kann, um die Ergebnisse zu interpretieren . . . 8
Den vollständigen Pfad zum ONTAP Revisionsobjekt bestimmen . . . 11
Informationen zur ONTAP-Prüfung von symbolischen Links und Hardlinks . . . 11
Informationen zur ONTAP-Protokollierung alternativer NTFS-Datenströme . . . 12
Informationen zur ONTAP Überwachung von NFS-Datei- und Verzeichniszugriffsereignissen . . . 14
Die Überwachungskonfiguration auf ONTAP SVMs planen . . . 14
Parameter, die allen Audit-Konfigurationen gemeinsam sind . . . 15
Parameter zur Bestimmung des Rotationszeitpunkts von Revisionsprotokollen für Ereignisse . . . 19
Erstellen einer Datei- und Verzeichnisüberwachungskonfiguration auf SVMs . . . 22
Erstellung der Datei- und Verzeichnisüberwachungskonfiguration auf ONTAP SVMs . . . 22
Die Überwachung auf ONTAP SVMs wird nach dem Einrichten der Überwachungskonfiguration aktiviert. . . . 24
Die ONTAP Revisionsprotokoll-Konfiguration überprüfen . . . 24
Datei- und Ordnerüberwachungsrichtlinien konfigurieren . . . 25
Audit-Konfiguration auf ONTAP SVMs aktivieren und Audit-Richtlinien für Dateien und Ordner konfigurieren . . . 25
ONTAP Revisionsrichtlinien für NTFS Security-Style-Dateien und -Verzeichnisse konfigurieren . . . 26
ONTAP Revisionsprotokoll für Dateien und Verzeichnisse im UNIX-Sicherheitsstil konfigurieren . . . 29
Informationen zu den auf Dateien und Verzeichnisse angewendeten Revisionsrichtlinien . . . 29
Informationen zu den ONTAP-Revisionsrichtlinien sind über die Registerkarte „Windows-Sicherheit“ einsehbar. . . . 30
Informationen zu NTFS-Audit-Richtlinien auf ONTAP FlexVol Volumes . . . 31
Platzhalterzeichen können verwendet werden, um Informationen zu ONTAP Dateisicherheits- und Revisionsprotokollrichtlinien anzuzeigen. . . . 34
CLI-Änderungsereignisse, die geprüft werden können . . . 35
Informationen zu ONTAP CLI-Änderungsereignissen, die protokolliert werden können . . . 35
ONTAP Dateifreigabeereignisse verwalten . . . 37
ONTAP-Ereignisse zur Änderung der Audit-Richtlinie verwalten . . . 38

Benutzerkonto-ONTAP-Ereignisse verwalten . . . 38
Verwaltung von ONTAP Sicherheitsgruppen-Ereignissen . . . 40
ONTAP-Ereignisse zur Änderung der Autorisierungsrichtlinie verwalten . . . 41
Überwachungskonfigurationen verwalten . . . 41
Die Audit-Ereignisprotokolle manuell rotieren, um bestimmte ONTAP SVM-Ereignisprotokolle anzuzeigen . . . 41
Überwachung auf ONTAP SVMs aktivieren oder deaktivieren . . . 42
Informationen zu ONTAP Audit-Konfigurationen . . . 43
ONTAP Befehle zum Ändern von Audit-Konfigurationen . . . 44
Löschen einer Revisionskonfiguration auf einer ONTAP SVM . . . 45
Die Auswirkungen der Rücksetzung eines geprüften ONTAP Clusters . . . 45
Probleme mit ONTAP Auditing und Staging Volume Speicherplatz beheben . . . 46
Beheben von Speicherplatzproblemen im Zusammenhang mit den Ereignisprotokollvolumes . . . 46
Behebung von Speicherplatzproblemen im Zusammenhang mit den Staging Volumes . . . 47

NAS-Ereignisse auf SVMs überwachen

Informationen zur Überwachung des Dateizugriffs mit ONTAP für die Protokolle SMB und NFS

Die für die SMB- und NFS-Protokolle verfügbaren Funktionen zur Dateizugriffsüberwachung mit ONTAP, wie etwa die native Überwachung und die Verwaltung von Dateirichtlinien mit FPolicy, können genutzt werden.

Die Überwachung von SMB- und NFS-Dateizugriffen ist unter den folgenden Umständen zu konzipieren und zu implementieren:

- Der grundlegende SMB- und NFS-Protokoll-Dateizugriff wurde konfiguriert.
- Es besteht der Wunsch, eine Überwachungskonfiguration mit einer der folgenden Methoden zu erstellen und zu verwalten:
  - Native ONTAP Funktionalität
  - Externe FPolicy Server

NAS-Ereignisse auf SVMs überwachen

Die Überwachung von NAS-Ereignissen ist eine Sicherheitsmaßnahme, mit der bestimmte SMB- und NFS-Ereignisse auf Storage Virtual Machines (SVMs) nachverfolgt und protokolliert werden können. Dies unterstützt die Nachverfolgung potenzieller Sicherheitsprobleme und liefert Nachweise für etwaige Sicherheitsverletzungen. Es besteht außerdem die Möglichkeit, Active Directory Central Access Policies zu testen und zu überwachen, um das Ergebnis ihrer Implementierung zu sehen.

SMB-Ereignisse

Die folgenden Ereignisse können geprüft werden:

- SMB-Datei- und Ordnerzugriffsereignisse

  Sie können SMB-Datei- und Ordnerzugriffsereignisse für Objekte prüfen, die auf FlexVol Volumes gespeichert sind, die zu den für die Prüfung aktivierten SVMs gehören.

- SMB-Anmelde- und Abmeldeereignisse

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

- Staging-Ereignisse für zentrale Zugriffsrichtlinien

  Sie können den effektiven Zugriff von Objekten auf SMB-Servern mithilfe von Berechtigungen prüfen, die durch vorgeschlagene zentrale Zugriffsrichtlinien angewendet werden. Die Überprüfung durch das Staging zentraler Zugriffsrichtlinien ermöglicht es, die Auswirkungen zentraler Zugriffsrichtlinien zu erkennen, bevor sie bereitgestellt werden.

  Die Überwachung der zentralen Zugriffsrichtlinien-Staging erfolgt mithilfe von Active Directory GPOs, jedoch muss die SVM-Überwachungskonfiguration so eingerichtet werden, dass Ereignisse des zentralen Zugriffsrichtlinien-Staging protokolliert werden.

  Obwohl die zentrale Zugriffsrichtlinienbereitstellung in der Überwachungskonfiguration aktiviert werden

kann, ohne dass Dynamic Access Control auf dem SMB-Server aktiviert ist, werden Ereignisse zur zentralen Zugriffsrichtlinienbereitstellung nur generiert, wenn Dynamic Access Control aktiviert ist. Dynamic Access Control wird über eine SMB-Serveroption aktiviert. Standardmäßig ist sie nicht aktiviert.

NFS-Ereignisse

Datei- und Verzeichnisereignisse können durch die Nutzung von NFSv4-ACLs auf Objekten, die auf SVMs gespeichert sind, geprüft werden.

Funktionsweise von Audits

Die grundlegenden ONTAP Audit-Konzepte

Für das Verständnis der Prüfung in ONTAP ist es hilfreich, einige grundlegende Prüfungskonzepte zu kennen.

- **Staging-Dateien**

  Die temporären Binärdateien auf den einzelnen Knoten, in denen die Revisionsprotokolle vor der Konsolidierung und Konvertierung gespeichert werden. Staging-Dateien befinden sich in Staging-Volumes.

- **Staging-Volume**

  Ein dediziertes Volume, das von ONTAP zum Speichern von Staging-Dateien erstellt wird. Pro Aggregat existiert ein Staging-Volume. Alle für die Revisionsprotokollierung aktivierten Storage Virtual Machines (SVMs) nutzen gemeinsam ein Staging-Volume, um Revisionsprotokolle des Dateizugriffs für die Datenvolumes des jeweiligen Aggregats zu speichern. Die Revisionsprotokolle jeder SVM werden in einem separaten Verzeichnis innerhalb des Staging-Volumes gespeichert.

  Clusteradministratoren können Informationen über Staging-Volumes einsehen, aber die meisten anderen Volume-Operationen sind nicht zulässig. Nur ONTAP kann Staging-Volumes erstellen. ONTAP weist Staging-Volumes automatisch einen Namen zu. Alle Staging-Volume-Namen beginnen mit `MDV_aud_` gefolgt von der UUID des Aggregats, das dieses Staging-Volume enthält (zum Beispiel: `MDV_aud_1d0131843d4811e296fc123478563412`).

- **System-Volumes**

  Ein FlexVol volume, das spezielle Metadaten enthält, wie beispielsweise Metadaten für Revisionsprotokolle von Dateidiensten. Die Admin-SVM besitzt Systemvolumes, die im gesamten Cluster sichtbar sind. Staging-Volumes sind eine Art von Systemvolume.

- **Konsolidierungsaufgabe**

  Eine Aufgabe, die erstellt wird, wenn die Überwachung aktiviert ist. Diese lang laufende Aufgabe auf jedem SVM übernimmt die Überwachungsdatensätze aus den Staging-Dateien der Mitgliedsknoten des SVM. Diese Aufgabe führt die Überwachungsdatensätze in chronologisch sortierter Reihenfolge zusammen und konvertiert sie dann in ein benutzerlesbares Ereignisprotokollformat, das in der Überwachungskonfiguration festgelegt ist – entweder das EVTX- oder das XML-Dateiformat. Die konvertierten Ereignisprotokolle werden im Verzeichnis für Überwachungsereignisprotokolle gespeichert, das in der SVM-Überwachungskonfiguration angegeben ist.

Informationen zur Funktionsweise des ONTAP-Auditprozesses

Der ONTAP Auditing-Prozess unterscheidet sich vom Microsoft Auditing-Prozess. Vor der Konfiguration des Auditing empfiehlt es sich, die Funktionsweise des ONTAP Auditing-Prozesses zu verstehen.

Audit-Protokolle werden zunächst in binären Staging-Dateien auf den einzelnen Nodes gespeichert. Wenn die Auditierung für eine SVM aktiviert ist, verwaltet jeder Mitgliedsnode Staging-Dateien für diese SVM. Periodisch werden sie konsolidiert und in benutzerlesbare Ereignisprotokolle umgewandelt, die im Verzeichnis für Revisionsprotokolle des SVM gespeichert werden.

Prozess, wenn die Protokollierung auf einer SVM aktiviert ist

Auditing kann nur auf SVMs aktiviert werden. Wenn der Storage-Administrator Auditing auf der SVM aktiviert, prüft das Auditing-Subsystem, ob Staging-Volumes vorhanden sind. Für jedes Aggregat, das Daten-Volumes enthält, die der SVM gehören, muss ein Staging-Volume existieren. Das Auditing-Subsystem erstellt alle benötigten Staging-Volumes, falls diese nicht vorhanden sind.

Das Überwachungssubsystem führt außerdem weitere vorbereitende Aufgaben aus, bevor die Überwachung aktiviert wird:

- Das Überwachungssubsystem überprüft, ob der Pfad zum Protokollverzeichnis verfügbar ist und keine Symlinks enthält.

  Das Protokollverzeichnis muss bereits als Pfad im Namespace der SVM vorhanden sein. Es wird empfohlen, ein neues Volume oder einen neuen Qtree für die Revisionsprotokolldateien zu erstellen. Das Auditing-Subsystem weist keinen Standardspeicherort für Protokolldateien zu. Wenn der in der Auditing-Konfiguration angegebene Protokollverzeichnispfad kein gültiger Pfad ist, schlägt die Erstellung der Auditing-Konfiguration mit dem `The specified path "/path" does not exist in the namespace belonging to Vserver "Vserver_name"` Fehler fehl.

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

- Die Protokollierung plant die Konsolidierungsaufgabe.

  Nachdem diese Aufgabe eingeplant wurde, ist die Überwachung aktiviert. Die SVM-Überwachungskonfiguration und die Protokolldateien bleiben auch nach einem Neustart oder wenn die NFS- oder SMB-Server gestoppt oder neu gestartet werden, erhalten.

Zusammenführung der Ereignisprotokolle

Die Protokollkonsolidierung ist eine geplante Aufgabe, die regelmäßig ausgeführt wird, bis die Überwachung deaktiviert ist. Wenn die Überwachung deaktiviert ist, überprüft die Konsolidierungsaufgabe, ob alle verbleibenden Protokolle konsolidiert sind.

Garantierte Prüfung

Standardmäßig ist die Protokollierung gewährleistet. ONTAP garantiert, dass alle protokollierbaren Dateizugriffsereignisse (wie durch die konfigurierte Zugriffssteuerungsliste festgelegt) aufgezeichnet werden, selbst wenn ein Node nicht verfügbar ist. Ein angeforderter Dateivorgang kann erst abgeschlossen werden, wenn der Protokolleintrag für diesen Vorgang im Staging-Volume auf dem persistenten Speicher gespeichert wurde. Können Protokolleinträge nicht in den Staging-Dateien auf der Festplatte gespeichert werden, entweder aufgrund von unzureichendem Speicherplatz oder anderen Problemen, werden Clientvorgänge abgelehnt.

Ein Administrator oder ein Benutzer mit privilegiertem Zugriff kann die Protokollierung von Dateizugriffen umgehen, indem NetApp Manageability SDK oder REST-APIs verwendet werden. Ob Dateizugriffe mithilfe von NetApp Manageability SDK oder REST-APIs erfolgt sind, lässt sich durch Überprüfung der in der `audit.log` Datei gespeicherten Befehlshistorie feststellen.

Weitere Informationen zu Revisionsprotokollen des Befehlsverlaufs finden sich im Abschnitt „Protokollierung verwalten für Managementaktivitäten“ in "Systemadministration".

Konsolidierungsprozess, wenn ein Node nicht verfügbar ist

Wenn ein Knoten, der Volumes enthält, die zu einer SVM mit aktivierter Überwachung gehören, nicht verfügbar ist, hängt das Verhalten der Überwachungskonsolidierungsaufgabe davon ab, ob der Storage-Failover-Partner (SFO-Partner) des Knotens (oder der HA-Partner im Falle eines Zwei-Node-Cluster) verfügbar ist:

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

  Wenn ein Knoten nicht erreichbar ist, konsolidiert der Konsolidierungsvorgang die Revisionsprotokolle der anderen verfügbaren Knoten dieser SVM. Zur Kennzeichnung, dass die Konsolidierung nicht abgeschlossen ist, fügt der Vorgang dem Dateinamen der konsolidierten Datei das Suffix `.partial` hinzu.

- Sobald der nicht verfügbare Knoten wieder verfügbar ist, werden die Revisionsprotokolle dieses Knotens mit den Revisionsprotokollen der anderen Knoten zu diesem Zeitpunkt zusammengeführt.
- Alle Revisionsprotokolle werden aufbewahrt.

Ereignisprotokollrotation

Die Revisionsprotokolldateien werden rotiert, wenn sie eine konfigurierte Schwellenwertgröße erreichen oder nach einem festgelegten Zeitplan. Wenn eine Revisionsprotokolldatei rotiert wird, benennt der geplante Konsolidierungsvorgang zunächst die aktive konvertierte Datei in eine mit einem Zeitstempel versehene Archivdatei um und erstellt anschließend eine neue aktive konvertierte Revisionsprotokolldatei.

Prozess, wenn die Protokollierung auf der SVM deaktiviert ist

Wenn die Überwachung auf der SVM deaktiviert ist, wird die Konsolidierungsaufgabe ein letztes Mal ausgeführt. Alle ausstehenden, aufgezeichneten Revisionsprotokolle werden in einem für Benutzer lesbaren Format protokolliert. Vorhandene Ereignisprotokolle im Ereignisprotokollverzeichnis werden bei Deaktivierung der Überwachung auf der SVM nicht gelöscht und stehen weiterhin zur Ansicht zur Verfügung.

Nachdem alle vorhandenen Staging-Dateien für diese SVM konsolidiert wurden, wird die Konsolidierungsaufgabe aus dem Zeitplan entfernt. Das Deaktivieren der Auditing-Konfiguration für die SVM entfernt die Auditing-Konfiguration nicht. Ein Storage-Administrator kann die Auditing-Funktion jederzeit wieder aktivieren.

Der Auditing-Konsolidierungsauftrag, der bei aktivierter Auditing-Funktion erstellt wird, überwacht die Konsolidierungsaufgabe und erstellt sie neu, falls die Konsolidierungsaufgabe aufgrund eines Fehlers beendet wird. Benutzer können den Auditing-Konsolidierungsauftrag nicht löschen.

Voraussetzungen für ONTAP Prüfung

Bevor Sie die Überwachung auf Ihrer Storage Virtual Machine (SVM) konfigurieren und

aktivieren, sind bestimmte Anforderungen und Überlegungen zu berücksichtigen.

- Das kombinierte Limit für NFS- und S3-Audit-aktivierte SVMs hängt von Ihrer ONTAP-Version ab:

ONTAP Version	Maximal
9.8 und früher	50
9.9.1 und später	400

- Die Prüfung ist nicht an SMB- oder NFS-Lizenzierung gebunden.

  Sie können die Überwachung auch dann konfigurieren und aktivieren, wenn keine SMB- und NFS-Lizenzen auf dem Cluster installiert sind.

- NFS Auditing unterstützt Security-ACEs (Typ U).
- Für die NFS-Überwachung gibt es keine Zuordnung zwischen Modusbits und Überwachungs-ACEs.

  Bei der Umwandlung von ACLs in Modusbits werden Audit-ACEs übersprungen. Bei der Umwandlung von Modusbits in ACLs werden keine Audit-ACEs generiert.

- Das in der Überwachungskonfiguration angegebene Verzeichnis muss existieren.

  Wenn die Konfiguration nicht existiert, schlägt der Befehl zum Erstellen der Auditing-Konfiguration fehl.

- Das in der Audit-Konfiguration angegebene Verzeichnis muss die folgenden Anforderungen erfüllen:
  - Das Verzeichnis darf keine symbolischen Links enthalten.

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

  - Das Verzeichnis ist mit einem absoluten Pfad anzugeben.

    Es sollte kein relativer Pfad angegeben werden, zum Beispiel `/vs1/../`.

- Auditing ist davon abhängig, dass in den Staging-Volumes verfügbarer Speicherplatz vorhanden ist.

  Es ist wichtig, sich darüber im Klaren zu sein und einen Plan zu haben, um sicherzustellen, dass in Aggregaten, die geprüfte Volumes enthalten, ausreichend Platz für die Staging-Volumes vorhanden ist.

- Die Überwachung ist davon abhängig, dass im Volume, das das Verzeichnis enthält, in dem die konvertierten Ereignisprotokolle gespeichert werden, ausreichend Speicherplatz verfügbar ist.

  Es ist erforderlich, sich darüber im Klaren zu sein und einen Plan zu haben, um sicherzustellen, dass in den für die Speicherung von Ereignisprotokollen verwendeten Volumes ausreichend Speicherplatz vorhanden ist. Die Anzahl der im Auditing-Verzeichnis aufzubewahrenden Ereignisprotokolle kann beim Erstellen einer Auditing-Konfiguration mit dem `-rotate-limit` Parameter festgelegt werden, was dazu beiträgt, dass im Volume genügend Speicherplatz für die Ereignisprotokolle zur Verfügung steht.

- Obwohl die zentrale Bereitstellung von Zugriffsrichtlinien in der Überwachungskonfiguration aktiviert werden kann, ohne Dynamic Access Control auf dem SMB-Server zu aktivieren, muss Dynamic Access Control aktiviert sein, um zentrale Bereitstellungsereignisse für Zugriffsrichtlinien zu generieren.

  Die dynamische Zugriffskontrolle ist nicht standardmäßig aktiviert.

Überlegungen zum Aggregatspeicherplatz bei der Aktivierung der Überwachung

Wenn eine Überwachungskonfiguration erstellt wird und die Überwachung auf mindestens einer Storage Virtual Machine (SVM) im Cluster aktiviert ist, erstellt das Überwachungssubsystem Staging-Volumes auf allen vorhandenen Aggregaten und auf allen neuen Aggregaten, die erstellt werden. Bestimmte Überlegungen zum Aggregatspeicherplatz sind zu beachten, wenn die Überwachung im Cluster aktiviert wird.

Die Erstellung des Staging-Volumes kann aufgrund von nicht verfügbarem Speicherplatz in einem Aggregat fehlschlagen. Dies kann vorkommen, wenn eine Auditing-Konfiguration erstellt wird und die vorhandenen Aggregate nicht über genügend Speicherplatz für das Staging-Volume verfügen.

Es ist sicherzustellen, dass auf den vorhandenen Aggregaten genügend Speicherplatz für die Staging-Volumes vorhanden ist, bevor die Auditierung auf einer SVM aktiviert wird.

Beschränkungen der Größe von Staging-Dateien für ONTAP Revisionsprotokolle

Die Größe eines Revisionsprotokolls in einer Staging-Datei darf 32 KB nicht überschreiten.

Wann große Revisionsprotokolle auftreten können

Umfangreiche Revisionsprotokolle können während der Management-Protokollierung in einem der folgenden Szenarien auftreten:

- Hinzufügen oder Entfernen von Benutzern zu oder aus Gruppen mit einer großen Anzahl von Benutzern.
- Hinzufügen oder Löschen einer Zugriffssteuerungsliste (ACL) auf einer Dateifreigabe mit einer großen Anzahl von Dateifreigabebenutzern.
- Andere Szenarien.

Die Management-Protokollierung sollte deaktiviert werden, um dieses Problem zu vermeiden. Hierzu ist die Audit-Konfiguration zu ändern und Folgendes aus der Liste der Audit-Ereignistypen zu entfernen:

- Dateifreigabe
- Benutzerkonto
- Sicherheitsgruppe
- Änderung der Autorisierungsrichtlinie

  Nach der Entfernung werden sie nicht mehr vom Dateidienst-Audit-Subsystem geprüft.

Die Auswirkungen von zu großen Revisionsprotokollen

- Ist die Größe eines Prüfdatensatzes zu groß (über 32 KB), wird der Prüfdatensatz nicht erstellt und das Prüfsubsystem generiert eine Meldung des Ereignisverwaltungssystems (EMS), die in etwa wie folgt aussieht:

  ```
  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 Protokollierung garantiert ist, schlägt der Dateivorgang fehl, weil der zugehörige Revisionsprotokolleintrag nicht erstellt werden kann.

- Ist der Prüfdatensatz größer als 9.999 Byte, wird dieselbe EMS-Meldung wie oben angezeigt. Es wird ein Teilprüfdatensatz erstellt, bei dem der größere Schlüsselwert fehlt.
- Wenn der Prüfdatensatz mehr als 2.000 Zeichen umfasst, wird anstelle des tatsächlichen Werts die folgende Fehlermeldung angezeigt:

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

Informationen zu den unterstützten Formaten für ONTAP Audit-Ereignisprotokolle

Unterstützte Dateiformate für die konvertierten Audit-Ereignisprotokolle sind `EVTX` und `XML` Dateiformate.

Beim Erstellen der Audit-Konfiguration kann der Typ des Dateiformats festgelegt werden. Standardmäßig konvertiert ONTAP die Binärprotokolle in das `EVTX` Dateiformat.

ONTAP Revisionsprotokolle für Ereignisse anzeigen und verarbeiten

Mithilfe von Revisionsprotokollen für Ereignisse kann festgestellt werden, ob die Dateisicherheit ausreichend ist und ob unberechtigte Zugriffsversuche auf Dateien und Ordner erfolgt sind. Revisionsprotokolle für Ereignisse, die im `EVTX`- oder `XML` -Dateiformat gespeichert sind, können angezeigt und verarbeitet werden.

- `EVTX` Dateiformat

  Sie können die konvertierten `EVTX`Revisionsprotokolle als gespeicherte Dateien mit Microsoft Event Viewer öffnen.

  Es gibt zwei Optionen, die Sie beim Anzeigen von Ereignisprotokollen mit der Ereignisanzeige verwenden können:

  - Gesamtansicht

    Für den Ereignisdatensatz werden Informationen angezeigt, die für alle Ereignisse gelten. In dieser Version von ONTAP werden die ereignisspezifischen Daten für den Ereignisdatensatz nicht angezeigt. In der Detailansicht lassen sich ereignisspezifische Daten anzeigen.

  - Detailansicht

    Es stehen eine benutzerfreundliche Ansicht und eine XML-Ansicht zur Verfügung. Die benutzerfreundliche Ansicht und die XML-Ansicht zeigen sowohl die für alle Ereignisse gemeinsamen Informationen als auch die ereignisspezifischen Daten des Ereignisdatensatzes an.

- `XML` Dateiformat

  Sie können Audit-Ereignisprotokolle `XML` in Drittanbieteranwendungen anzeigen und verarbeiten, die das

`XML` Dateiformat unterstützen. XML-Anzeigetools können verwendet werden, um die Audit-Protokolle anzuzeigen, sofern Sie über das XML-Schema und Informationen zu den Definitionen der XML-Felder verfügen. Weitere Informationen zum XML-Schema und zu den Definitionen finden Sie in der "ONTAP Revisionsprotokoll-Schema-Referenz".

Wie aktive Revisionsprotokolle mit der Ereignisanzeige angezeigt werden

Wenn der Revisionsprotokoll-Konsolidierungsprozess auf dem Cluster ausgeführt wird, fügt der Konsolidierungsprozess neue Einträge an die aktive Revisionsprotokolldatei für audit-aktivierte Storage Virtual Machines (SVMs) an. Auf dieses aktive Revisionsprotokoll kann über eine SMB-Freigabe in der Microsoft Event Viewer zugegriffen und es geöffnet werden.

Zusätzlich zur Anzeige vorhandener Revisionsprotokolle bietet die Ereignisanzeige eine Aktualisierungsoption, mit der der Inhalt im Konsolenfenster aktualisiert werden kann. Ob die neu hinzugefügten Protokolle in der Ereignisanzeige sichtbar sind, hängt davon ab, ob Oplocks für die Freigabe aktiviert sind, die für den Zugriff auf das aktive Revisionsprotokoll verwendet wird.

Oplocks Einstellung für die Freigabe	Verhalten
Aktiviert	Die Ereignisanzeige öffnet das Protokoll, das die bis zu diesem Zeitpunkt gespeicherten Ereignisse enthält. Der Aktualisierungsvorgang aktualisiert das Protokoll nicht mit neuen Ereignissen, die vom Konsolidierungsprozess hinzugefügt wurden.
Deaktiviert	Die Ereignisanzeige öffnet das Protokoll, das die bis zu diesem Zeitpunkt gespeicherten Ereignisse enthält. Der Aktualisierungsvorgang aktualisiert das Protokoll mit den vom Konsolidierungsprozess hinzugefügten neuen Ereignissen.

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

Informationen zu SMB-Ereignissen, die ONTAP prüfen kann, um die Ergebnisse zu interpretieren

ONTAP kann bestimmte SMB-Ereignisse protokollieren, darunter bestimmte Datei- und Ordnerzugriffsereignisse, bestimmte An- und Abmeldevorgänge sowie Ereignisse der zentralen Zugriffsrichtlinienbereitstellung. Zu wissen, welche Zugriffsereignisse protokolliert werden können, ist hilfreich bei der Interpretation der Ergebnisse aus den Ereignisprotokollen.

Die folgenden zusätzlichen SMB-Ereignisse können geprüft werden:

Ereignis-ID (EVT/EVTX)	Ereignis	Beschreibung	Kategorie
4670	Die Objektberechtigungen wurden geändert	OBJEKTZUGRIFF: Berechtigungen geändert.	Dateizugriff

4907	Die Einstellungen für die Objektüberwachung wurden geändert	OBJEKTZUGRIFF: Überwachungseinstellungen geändert.	Dateizugriff
4913	Die Central Access Policy für Objekte wurde geändert	OBJEKTZUGRIFF: CAP geändert.	Dateizugriff

Die folgenden SMB-Ereignisse können in ONTAP 9.0 und höher protokolliert werden:

Ereignis-ID (EVT/EVTX)	Ereignis	Beschreibung	Kategorie
540/4624	Ein Konto wurde erfolgreich angemeldet	ANMELDUNG/ABMELDUNG: Netzwerkanmeldung (SMB).	An- und Abmelden
529/4625	Ein Konto konnte nicht angemeldet werden	AN-/ABMELDEN: Unbekannter Benutzername oder falsches Passwort.	An- und Abmelden
530/4625	Ein Konto konnte nicht angemeldet werden	AN- UND ABMELDEN: Zeitliche Beschränkung für die Kontoanmeldung.	An- und Abmelden
531/4625	Ein Konto konnte nicht angemeldet werden	AN-/ABMELDEN: Konto ist derzeit deaktiviert.	An- und Abmelden
532/4625	Ein Konto konnte nicht angemeldet werden	AN-/ABMELDEN: Das Benutzerkonto ist abgelaufen.	An- und Abmelden
533/4625	Ein Konto konnte nicht angemeldet werden	AN-/ABMELDEN: Der Benutzer kann sich an diesem Computer nicht anmelden.	An- und Abmelden
534/4625	Ein Konto konnte nicht angemeldet werden	AN-/ABMELDEN: Dem Benutzer wurde hier kein Anmeldetyp gewährt.	An- und Abmelden
535/4625	Ein Konto konnte nicht angemeldet werden	AN-/ABMELDEN: Das Passwort des Benutzers ist abgelaufen.	An- und Abmelden
537/4625	Ein Konto konnte nicht angemeldet werden	ANMELDEN/ABMELDEN: Die Anmeldung ist aus anderen als den oben genannten Gründen fehlgeschlagen.	An- und Abmelden
539/4625	Ein Konto konnte nicht angemeldet werden	AN-/ABMELDEN: Konto gesperrt.	An- und Abmelden
538/4634	Ein Konto wurde abgemeldet	ANMELDUNG/LOGOFF: Lokale oder Netzwerkbenutzerabmeldung.	An- und Abmelden
560/4656	Objekt öffnen/Objekt erstellen	OBJEKTZUGRIFF: Objekt (Datei oder Verzeichnis) geöffnet.	Dateizugriff
563/4659	Objekt mit der Absicht zu löschen öffnen	OBJEKTZUGRIFF: Ein Handle zu einem Objekt (Datei oder Verzeichnis) wurde mit der Absicht zum Löschen angefordert.	Dateizugriff

564/4660	Objekt löschen	OBJEKTZUGRIFF: Objekt (Datei oder Verzeichnis) löschen. ONTAP generiert dieses Ereignis, wenn ein Windows-Client versucht, das Objekt (Datei oder Verzeichnis) zu löschen.	Dateizugriff
567/4663	Objekt lesen/Objekt schreiben/Objektattribute abrufen/Objektattribute festlegen	OBJEKTZUGRIFF: Zugriffsversuch auf ein Objekt (Lesen, Schreiben, Attribut abrufen, Attribut setzen). **Hinweis:** Für dieses Ereignis protokolliert ONTAP nur den ersten SMB-Lese- und den ersten SMB-Schreibvorgang (erfolgreich oder fehlgeschlagen) eines Objekts. Dies verhindert, dass ONTAP übermäßig viele Protokolleinträge erzeugt, wenn ein einzelner Client ein Objekt öffnet und viele aufeinanderfolgende Lese- oder Schreibvorgänge für dasselbe Objekt durchführt.	Dateizugriff
NA/4664	Hardlink	OBJEKTZUGRIFF: Es wurde versucht, einen Hardlink zu erstellen.	Dateizugriff
NA/4818	Die vorgeschlagene zentrale Zugriffsrichtlinie gewährt nicht dieselben Zugriffsberechtigungen wie die aktuelle zentrale Zugriffsrichtlinie	OBJEKTZUGRIFF: Zentrale Zugriffsrichtlinien-Staging.	Dateizugriff
NA/NA Data ONTAP Event-ID 9999	Objekt umbenennen	OBJEKTZUGRIFF: Objekt umbenannt. Dies ist ein ONTAP Ereignis. Es wird derzeit von Windows nicht als einzelnes Ereignis unterstützt.	Dateizugriff
NA/NA Data ONTAP Event-ID 9998	Objektverknüpfung aufheben	OBJEKTZUGRIFF: Objekt nicht verknüpft. Dies ist ein ONTAP Ereignis. Es wird derzeit von Windows nicht als einzelnes Ereignis unterstützt.	Dateizugriff

Weitere Informationen zu Ereignis 4656

Das `HandleID` Tag im Audit `XML` Ereignis enthält den Handle des Objekts (Datei oder Verzeichnis), auf das zugegriffen wurde. Das `HandleID` Tag für das EVTX 4656 Ereignis enthält unterschiedliche Informationen, abhängig davon, ob das Öffnungsereignis das Erstellen eines neuen Objekts oder das Öffnen eines vorhandenen Objekts betrifft:

- Wenn das Öffnungsereignis eine Öffnungsanforderung zum Erstellen eines neuen Objekts (Datei oder Verzeichnis) ist, zeigt das `HandleID` Tag im Audit-XML-Ereignis ein leeres `HandleID` an (zum Beispiel: `<Data Name="HandleID">00000000000000;00;00000000;00000000</Data>`).

  Das `HandleID` ist leer, da die OPEN-Anfrage (zum Erstellen eines neuen Objekts) protokolliert wird, bevor

das Objekt tatsächlich erstellt wird und bevor ein Handle existiert. Nachfolgende protokollierte Ereignisse für dasselbe Objekt enthalten das korrekte Objekthandle im `HandleID` Tag.

- Wenn es sich bei dem Öffnungsereignis um eine Anfrage zum Öffnen eines bestehenden Objekts handelt, enthält das Audit-Ereignis den zugewiesenen Handle dieses Objekts im `HandleID`-Tag (zum Beispiel: `<Data Name="HandleID">00000000000401;00;000000ea;00123ed4</Data>`).

Den vollständigen Pfad zum ONTAP Revisionsobjekt bestimmen

Der im `<ObjectName>`-Tag eines Revisionsprotokolls ausgegebene Objektpfad enthält den Namen des Volumes (in Klammern) und den relativen Pfad vom Stammverzeichnis des enthaltenen Volumes. Um den vollständigen Pfad des geprüften Objekts einschließlich des Verbindungspfads zu bestimmen, sind bestimmte Schritte erforderlich.

Schritte

1. Der Datenträgername und der relative Pfad zum überwachten Objekt lassen sich anhand des `<ObjectName>`-Tags im Überwachungsereignis bestimmen.

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

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

2. Anhand des im vorherigen Schritt ermittelten Volume-Namens lässt sich ermitteln, welcher Verbindungspfad für das Volume mit dem überwachten Objekt besteht:

   In diesem Beispiel lautet der Volumenname “data1” und der Verbindungspfad für das Volumen, das das überwachte Objekt enthält, ist `/data/data1`:

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

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

3. Der vollständige Pfad zum überwachten Objekt ergibt sich, indem der im `<ObjectName>`-Tag gefundene relative Pfad an den Verbindungspfad für das Volume angehängt wird.

   In diesem Beispiel ist der Verbindungspfad für das Volumen:

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

Informationen zur ONTAP-Prüfung von symbolischen Links und Hardlinks

Bei der Überprüfung von Symlinks und Hardlinks sind bestimmte Aspekte zu berücksichtigen.

Ein Prüfprotokoll enthält Informationen über das geprüfte Objekt, einschließlich des Pfads zu dem geprüften Objekt, der im `ObjectName` Tag angegeben ist. Es ist zu beachten, wie Pfade für symbolische Links und Hardlinks im `ObjectName` Tag erfasst werden.

Symlinks

Ein symbolischer Link ist eine Datei mit einem separaten Inode, der einen Zeiger auf den Speicherort eines Zielobjekts, des sogenannten Targets, enthält. Beim Zugriff auf ein Objekt über einen symbolischen Link interpretiert ONTAP diesen automatisch und folgt dem tatsächlichen kanonischen, protokollunabhängigen Pfad zum Zielobjekt im Volume.

Im folgenden Beispielausgabe gibt es zwei Symlinks, die beide auf eine Datei mit dem Namen `target.txt` zeigen. Einer der Symlinks ist ein relativer Symlink und einer ist ein absoluter Symlink. Wenn einer der Symlinks geprüft wird, enthält das `ObjectName`-Tag im Revisionsereignis 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
```

Harte Links

Ein Hardlink ist ein Verzeichniseintrag, der einen Namen mit einer vorhandenen Datei im Dateisystem verknüpft. Der Hardlink verweist auf den Inode-Standort der Originaldatei. Ähnlich wie ONTAP symbolische Links interpretiert, interpretiert ONTAP auch den Hardlink und folgt dem tatsächlichen kanonischen Pfad zum Zielobjekt im Volume. Wenn der Zugriff auf ein Hardlink-Objekt protokolliert wird, zeichnet das Protokollereignis diesen absoluten kanonischen Pfad im `ObjectName` Tag auf, anstatt des Hardlink-Pfads.

Informationen zur ONTAP-Protokollierung alternativer NTFS-Datenströme

Bei der Überprüfung von Dateien mit alternativen NTFS-Datenströmen sind bestimmte Aspekte zu berücksichtigen.

Der Speicherort eines überwachten Objekts wird in einem Ereignisdatensatz mithilfe zweier Tags protokolliert, dem `ObjectName` Tag (dem Pfad) und dem `HandleID` Tag (dem Handle). Für die korrekte Identifizierung der protokollierten Stream-Anforderungen ist es erforderlich, zu wissen, welche Daten ONTAP in diesen Feldern für NTFS-Alternate Data Streams erfasst.

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

Beispiel

Das folgende Beispiel veranschaulicht, wie Ereignisse mit der EVTX-ID 4663 für alternative Datenströme mithilfe des `HandleID` Tags identifiziert werden. Auch wenn der im Lese-Revisionsprotokoll-Ereignis aufgezeichnete `ObjectName` Tag (Pfad) auf den Basisdateipfad verweist, kann der `HandleID` Tag verwendet werden, um das Ereignis als Revisionsprotokolleintrag für den alternativen Datenstrom zu identifizieren.

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

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

Die Ausgabe im folgenden Ereignisbeispiel ist wie angegeben gekürzt; die Ausgabe zeigt nicht alle verfügbaren Ausgabetags für die Ereignisse an.

Für eine EVTX-ID 4656 (offenes Revisionsereignis) gibt der Revisionsdatensatz für den alternativen Datenstrom den Namen des alternativen Datenstroms im `ObjectName`-Tag aus:

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4656</EventID>
  <EventName>Open Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt:stream1</Data\>
**
  [...]
  </EventData>
  </Event>
- <Event>
```

Bei einer EVTX-ID 4663 (Lese-Audit-Ereignis) gibt die Audit-Datensatzausgabe für denselben alternativen Datenstrom den Basisdateinamen im `ObjectName` Tag aus; der Handle im `HandleID` Tag ist jedoch der Handle des alternativen Datenstroms und kann zur Korrelation dieses Ereignisses mit dem alternativen Datenstrom verwendet werden:

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4663</EventID>
  <EventName>Read Object</EventName>
```

```
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt</Data\> **
  [...]
  </EventData>
  </Event>
- <Event>
```

Informationen zur ONTAP Überwachung von NFS-Datei- und Verzeichniszugriffsereignissen

ONTAP kann bestimmte NFS-Datei- und Verzeichniszugriffsereignisse protokollieren. Es ist hilfreich zu wissen, welche Zugriffsereignisse protokolliert werden können, wenn die Ergebnisse der konvertierten Audit-Ereignisprotokolle interpretiert werden.

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

- LESEN
- OFFEN
- SCHLIESSEN
- READDIR
- SCHREIBEN
- SETATTR
- ERSTELLEN
- Link
- OPENATTR
- ENTFERNEN
- GETATTR
- VERIFIZIEREN
- NVERIFY
- UMBENENNEN

Um NFS RENAME-Ereignisse zuverlässig zu protokollieren, sollten Überwachungs-ACEs auf Verzeichnisse anstatt auf Dateien festgelegt werden, da die Dateiberechtigungen bei einer RENAME-Operation nicht überprüft werden, wenn die Verzeichnisberechtigungen ausreichend sind.

Die Überwachungskonfiguration auf ONTAP SVMs planen

Bevor Sie die Überwachung auf Storage Virtual Machines (SVMs) konfigurieren, ist es

erforderlich, die verfügbaren Konfigurationsoptionen zu verstehen und die Werte zu planen, die für jede Option festgelegt werden sollen. Diese Informationen können dabei unterstützen, die Überwachungskonfiguration so zu gestalten, dass sie den geschäftlichen Anforderungen entspricht.

Es gibt bestimmte Konfigurationsparameter, die allen Audit-Konfigurationen gemeinsam sind.

Darüber hinaus gibt es bestimmte Parameter, mit denen Sie festlegen können, welche Methoden beim Rotieren der konsolidierten und konvertierten Audit-Logs verwendet werden. Bei der Konfiguration der Überwachung kann eine der folgenden drei Methoden festgelegt werden:

- Protokolle basierend auf der Protokollgröße rotieren

  Dies ist die Standardmethode zum Rotieren von Protokolldateien.

- Protokolle gemäß einem Zeitplan rotieren
- Protokolldateien werden basierend auf der Protokolldateigröße und dem Zeitplan rotiert (je nachdem, welches Ereignis zuerst eintritt).

Mindestens eine der Methoden zur Logrotation muss immer eingestellt sein.

Parameter, die allen Audit-Konfigurationen gemeinsam sind

Beim Erstellen der Audit-Konfiguration müssen zwei obligatorische Parameter angegeben werden. Es gibt außerdem drei optionale Parameter, die angegeben werden können:

Art der Information	Option	Erforderlich	Enthalten	Ihre Werte
SVM Name Name der SVM, auf der die Revisionsprotokoll-Konfiguration erstellt werden soll. Die SVM muss bereits existieren.	`-vserver vserver_name`	Ja	Ja	

Protokollzielpfad Gibt das Verzeichnis an, in dem die konvertierten Audit-Logs gespeichert werden, typischerweise ein dediziertes Volume oder ein qtree. Der Pfad muss bereits im SVM-Namensraum vorhanden sein. Der Pfad darf maximal 864 Zeichen lang sein und muss über Lese-/Schreibberechtigung verfügen. Ist der Pfad ungültig, schlägt der Revisionsdatei-Konfigurationsbefehl fehl. Wenn es sich bei der SVM um eine SVM Disaster Recovery-Quelle handelt, darf der Protokollzielpfad nicht auf dem Root-Volume liegen. Dies ist darauf zurückzuführen, dass der Inhalt des Root-Volumes nicht auf das Disaster Recovery-Ziel repliziert wird. Es kann kein FlexCache Volume als Protokollziel verwendet werden (ONTAP 9.7 und höher).	`-destination text`	Ja	Ja	

Kategorien von zu prüfenden Ereignissen Legt die Kategorien der zu prüfenden Ereignisse fest. Die folgenden Ereigniskategorien können im Revisionsprotokoll erfasst werden: • Dateizugriffsereignisse (sowohl SMB als auch NFSv4) • SMB-Anmelde- und Abmeldeereignisse • Staging-Ereignisse für zentrale Zugriffsrichtlinien Zentrale Zugriffsrichtlinien-Staging-Ereignisse sind ab Windows 2012 Active Directory Domains verfügbar. • Asynchrones Löschen • Ereignisse der Kategorie „Dateifreigabe“ • Ereignisse bei Änderungen der Prüfungsrichtlinie • Lokale Benutzerkontenverwaltungsereignisse • Sicherheitsgruppen-Managementereignisse • Ereignisse bei Änderungen der Autorisierungsrichtlinie Standardmäßig werden der Dateizugriff und SMB-Anmelde- sowie Abmeldeereignisse protokolliert. **Hinweis:** Bevor Sie `cap-staging` als Ereigniskategorie angeben können, muss auf der SVM ein SMB-Server vorhanden sein. Obwohl die zentrale Zugriffsrichtlinienbereitstellung in der Überwachungskonfiguration aktiviert werden kann, ohne dass Dynamic Access Control auf dem SMB-Server aktiviert ist, werden Ereignisse zur zentralen Zugriffsrichtlinienbereitstellung nur generiert, wenn Dynamic Access Control aktiviert ist. Dynamic Access Control wird über eine SMB-Serveroption aktiviert. Standardmäßig ist sie nicht aktiviert.	`-events {file-ops`	`cifs-logon-logoff`	`cap-staging`	`file-share`

`audit-policy-change`	`user-account`	`security-group`	`authorization-policy-change`	`async-delete}`
Nein			*Ausgabeformat der Protokolldatei* Legt das Ausgabeformat der Revisionsprotokolle fest. Das Ausgabeformat kann entweder ONTAP-spezifisch `XML` oder Microsoft Windows `EVTX` Protokollformat sein. Standardmäßig ist das Ausgabeformat `EVTX`.	`-format {xml`

`evtx}`	Nein			*Rotationslimit für Protokolldateien* Legt fest, wie viele Revisionsprotokoll-Logdateien aufbewahrt werden, bevor die älteste Logdatei entfernt wird. Wenn beispielsweise der Wert `5` eingegeben wird, werden die letzten fünf Logdateien aufbewahrt. Ein Wert von `0` zeigt an, dass alle Protokolldateien beibehalten werden. Der Standardwert ist 0.

Parameter zur Bestimmung des Rotationszeitpunkts von Revisionsprotokollen für Ereignisse

Protokolle basierend auf der Protokollgröße rotieren

Standardmäßig werden Revisionsprotokolle basierend auf Größe rotiert.

- Die Standard-Protokollgröße beträgt 100 MB
- Wenn Sie die Standardmethode für die Protokollrotation und die Standardprotokollgröße verwenden, ist keine spezifische Konfiguration von Parametern für die Protokollrotation erforderlich.
- Wenn die Revisionsprotokolle ausschließlich basierend auf der Protokollgröße rotiert werden sollen, kann der folgende Befehl verwendet werden, um den `-rotate-schedule-minute`Parameter zu deaktivieren: `vserver audit modify -vserver vs0 -destination / -rotate -schedule-minute -`

Wenn Sie nicht die Standardprotokollgröße verwenden möchten, kann der `-rotate-size` Parameter so konfiguriert werden, dass eine benutzerdefinierte Protokollgröße festgelegt wird:

Art der Information	Option	Erforderlich	Enthalten	Ihre Werte
Beschränkung der Protokolldateigröße Legt das Größenlimit der Revisionsprotokolldatei fest.	`-rotate-size` {`integer`[KB	MB	GB	TB

Protokolle gemäß einem Zeitplan rotieren

Wenn Sie sich dafür entscheiden, die Revisionsprotokolle nach einem Zeitplan zu rotieren, kann die Protokollrotation mithilfe der zeitbasierten Rotationsparameter in beliebiger Kombination geplant werden.

- Bei Verwendung einer zeitbasierten Rotation ist der `-rotate-schedule-minute` Parameter obligatorisch.
- Alle anderen zeitbasierten Rotationsparameter sind optional.
- Der Rotationsplan wird anhand aller zeitbezogenen Werte berechnet.

  Wenn nur der `-rotate-schedule-minute` Parameter angegeben wird, werden die Revisionsprotokoll-Dateien an allen Wochentagen, zu allen Stunden und in allen Monaten des Jahres entsprechend der angegebenen Minuten rotiert.

- Wenn Sie nur einen oder zwei zeitbasierten Rotationsparameter angeben (zum Beispiel `-rotate -schedule-month` und `-rotate-schedule-minutes`), erfolgt die Rotation der Protokolldateien an allen Wochentagen und zu allen Stunden auf Grundlage der angegebenen Minutenwerte, jedoch nur während der festgelegten Monate.

  Beispielsweise kann festgelegt werden, dass das Revisionsprotokoll in den Monaten Januar, März und August jeweils montags, mittwochs und samstags um 10:30 Uhr rotiert wird.

- Wenn Sie Werte für sowohl `-rotate-schedule-dayofweek` als auch `-rotate-schedule-day` angeben, werden diese unabhängig voneinander betrachtet.

  Wenn beispielsweise `-rotate-schedule-dayofweek` als Freitag und `-rotate-schedule-day` als 13 angegeben werden, werden die Revisionsprotokolle an jedem Freitag und am 13. Tag des angegebenen Monats rotiert, nicht nur an jedem Freitag, der auf den 13. fällt.

- Wenn die Revisionsprotokolle ausschließlich nach einem Zeitplan rotiert werden sollen, kann der folgende Befehl verwendet werden, um den `-rotate-size` Parameter zu deaktivieren: `vserver audit modify -vserver vs0 -destination / -rotate-size -`

Die folgende Liste der verfügbaren Überwachungsparameter bietet eine Übersicht über die Werte, die für die

Konfiguration eines Zeitplans für die Rotation des Revisionsprotokolls verwendet werden können:

Art der Information	Option	Erforderlich	Enthalten	Ihre Werte
Protokollrotationsplan: Monat Bestimmt den monatlichen Zeitplan für die Rotation der Revisionsprotokolle. Gültige Werte sind `January` bis `December` und `all`. Zum Beispiel kann angegeben werden, dass das Revisionsprotokoll in den Monaten Januar, März und August rotiert wird.	`-rotate-schedule-month chron_month`	Nein		
Rotationsplan für das Protokoll: Wochentag Legt den täglichen (Wochentag) Zeitplan für die Rotation der Revisionsprotokolle fest. Gültige Werte sind `Sunday` bis `Saturday` und `all`. Beispielsweise kann angegeben werden, dass das Revisionsprotokoll dienstags und freitags oder an allen Tagen einer Woche rotiert wird.	`-rotate-schedule -dayofweek chron_dayofweek`	Nein		
Rotationsplan für das Protokoll: Tag Legt den Tag des Monats fest, an dem das Revisionsprotokoll rotiert wird. Gültige Werte reichen von `1` bis `31`. Beispielsweise kann angegeben werden, dass das Revisionsprotokoll am 10. und 20. Tag eines Monats oder an allen Tagen eines Monats rotiert wird.	`-rotate-schedule-day chron_dayofmonth`	Nein		
Rotationsplan für das Protokoll: Stunde Bestimmt den stündlichen Zeitplan für die Rotation des Revisionsprotokolls. Gültige Werte liegen zwischen `0` (Mitternacht) und `23` (23:00 Uhr). Die Angabe von `all` bewirkt, dass die Revisionsprotokolle stündlich rotiert werden. Beispielsweise kann angegeben werden, dass das Revisionsprotokoll um 6 (6:00 Uhr) und 18 (18:00 Uhr) rotiert wird.	`-rotate-schedule-hour chron_hour`	Nein		

Protokollrotationsplan: Minute Legt den Minutenplan für die Rotation des Revisionsprotokolls fest. Gültige Werte reichen von `0` bis `59`. Beispielsweise kann angegeben werden, dass das Revisionsprotokoll zur 30. Minute rotiert wird.	`-rotate-schedule-minute chron_minute`	Ja, wenn die zeitplanbasierte Protokollrotation konfiguriert wird; andernfalls nein.		

Protokolle basierend auf Protokollgröße und Zeitplan rotieren

Sie können die Rotation der Protokolldateien anhand der Protokolldateigröße und eines Zeitplans steuern, indem sowohl der `-rotate-size` Parameter als auch die zeitbasierten Rotationsparameter in beliebiger Kombination gesetzt werden. Beispielsweise: Wenn `-rotate-size` auf 10 MB und `-rotate-schedule -minute` auf 15 gesetzt ist, werden die Protokolldateien rotiert, sobald die Protokolldateigröße 10 MB erreicht oder in der 15. Minute jeder Stunde (je nachdem, welches Ereignis zuerst eintritt).

Erstellen einer Datei- und Verzeichnisüberwachungskonfiguration auf SVMs

Erstellung der Datei- und Verzeichnisüberwachungskonfiguration auf ONTAP SVMs

Das Erstellen einer Datei- und Verzeichnis-Revisionsprotokollierungskonfiguration auf Ihrer Storage Virtual Machine (SVM) umfasst das Verständnis der verfügbaren Konfigurationsoptionen, die Planung der Konfiguration sowie das Konfigurieren und Aktivieren der Konfiguration. Anschließend lassen sich Informationen zur Revisionsprotokollierungskonfiguration anzeigen, um zu bestätigen, dass die resultierende Konfiguration der gewünschten Konfiguration entspricht.

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

Bevor Sie beginnen

Wenn eine Revisionsprotokoll-Konfiguration für das Staging zentraler Zugriffsrichtlinien erstellt werden soll, muss auf der SVM ein SMB-Server vorhanden sein.

- Obwohl die zentrale Zugriffsrichtlinienbereitstellung in der Überwachungskonfiguration aktiviert werden kann, ohne dass Dynamic Access Control auf dem SMB-Server aktiviert ist, werden Ereignisse zur zentralen Zugriffsrichtlinienbereitstellung nur generiert, wenn Dynamic Access Control aktiviert ist.

  Dynamic Access Control wird über eine SMB-Serveroption aktiviert. Standardmäßig ist sie nicht aktiviert.

- Sind die Argumente eines Feldes in einem Befehl ungültig, zum Beispiel ungültige Einträge für Felder, doppelte Einträge oder nicht vorhandene Einträge, schlägt der Befehl vor der Revisionsphase fehl.

  Solche Fehler erzeugen keinen Revisionsprotokolleintrag.

Über diese Aufgabe

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

Schritt

1. Anhand der Informationen im Planungsarbeitsblatt wird die Revisionsprotokoll-Konfiguration erstellt, um Revisionsprotokolle basierend auf der Protokollgröße oder einem Zeitplan zu rotieren:

Wenn Sie die Revisionsprotokolle rotieren möchten…	Eingeben…
Loggröße	`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]}]`
Ein Zeitplan	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging}] [-format {xml

Beispiele

Das folgende Beispiel erstellt eine Revisionsprotokollkonfiguration, die Dateizugriffe sowie SMB-An- und Abmeldeereignisse (die Standardeinstellung) mithilfe größenbasierter Rotation protokolliert. Das Protokollformat ist `EVTX` (Standard). Die Protokolle werden im `/audit_log` Verzeichnis gespeichert. Die maximale Protokolldateigröße beträgt `200 MB`. Die Protokolle werden rotiert, sobald sie eine Größe von 200 MB erreichen.

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

Das folgende Beispiel erstellt eine Revisionsprotokollkonfiguration, die Dateizugriffe sowie SMB-An- und Abmeldeereignisse (die Standardeinstellung) mithilfe größenbasierter Rotation protokolliert. Das Protokollformat ist `EVTX` (Standard). Die Protokolle werden im `/cifs_event_logs` Verzeichnis gespeichert. Die maximale Protokolldateigröße beträgt `100 MB` (die Standardeinstellung), und die maximale Protokollrotation beträgt `5`:

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

Das folgende Beispiel erstellt eine Revisionsprotokollierungskonfiguration, die Dateizugriffe, CIFS-An- und

Abmeldeereignisse sowie Ereignisse der zentralen Zugriffsrichtlinien-Staging mittels zeitbasierter Rotation protokolliert. Das Protokollformat ist `EVTX` (Standard). Die Audit-Protokolle werden monatlich um 12:30 Uhr an allen Wochentagen rotiert. Das Limit für die Protokollrotation beträgt `5`:

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-events file-ops,cifs-logon-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

- "Die Überwachung auf der SVM aktivieren."
- "Überprüfung der Audit-Konfiguration"

Die Überwachung auf ONTAP SVMs wird nach dem Einrichten der Überwachungskonfiguration aktiviert.

Nachdem die Überwachungskonfiguration abgeschlossen ist, muss die Überwachung auf der Storage Virtual Machine (SVM) aktiviert werden.

Bevor Sie beginnen

Die SVM Audit-Konfiguration muss bereits vorhanden sein.

Über diese Aufgabe

Wenn eine SVM Disaster Recovery ID Discard-Konfiguration zum ersten Mal gestartet wird (nach Abschluss der SnapMirror-Initialisierung) und die SVM über eine Auditing-Konfiguration verfügt, deaktiviert ONTAP die Auditing-Konfiguration automatisch. Auditing ist auf der schreibgeschützten SVM deaktiviert, um ein Überlaufen der Staging-Volumes zu verhindern. Auditing kann erst wieder aktiviert werden, nachdem die SnapMirror Beziehung aufgehoben und die SVM schreibbar ist.

Schritte

1. Audit auf der SVM aktivieren:

   ```
   vserver audit enable -vserver vserver_name

   vserver audit enable -vserver vs1
   ```

Verwandte Informationen

- "Die Überwachungskonfiguration erstellen"
- "Überprüfung der Audit-Konfiguration"

Die ONTAP Revisionsprotokoll-Konfiguration überprüfen

Nach Abschluss der Revisionsprotokollkonfiguration sollte überprüft werden, ob das Revisionsprotokoll ordnungsgemäß konfiguriert und aktiviert ist.

Schritte

1. Überprüfen der Audit-Konfiguration:

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

Der folgende Befehl zeigt in Listenform alle Revisionsprotokoll-Konfigurationsinformationen für die Storage Virtual Machine (SVM) vs1 an:

```
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

- "Die Überwachungskonfiguration erstellen"
- "Die Überwachung auf der SVM aktivieren."

Datei- und Ordnerüberwachungsrichtlinien konfigurieren

Audit-Konfiguration auf ONTAP SVMs aktivieren und Audit-Richtlinien für Dateien und Ordner konfigurieren

Die Implementierung der Überwachung von Datei- und Ordnerzugriffsereignissen ist ein zweistufiger Prozess. Zunächst muss eine Revisionsprotokollierungskonfiguration auf Storage Virtual Machines (SVMs) erstellt und aktiviert werden. Anschließend müssen Revisionsprotokollierungsrichtlinien für die Dateien und Ordner konfiguriert werden, die überwacht werden sollen. Revisionsprotokollierungsrichtlinien können so konfiguriert werden, dass sowohl erfolgreiche als auch fehlgeschlagene Zugriffsversuche überwacht werden.

Sie können sowohl SMB- als auch NFS-Revisionsrichtlinien konfigurieren. SMB- und NFS-Revisionsrichtlinien haben unterschiedliche Konfigurationsanforderungen und Revisionsfunktionen.

Wenn die entsprechenden Revisionsrichtlinien konfiguriert sind, überwacht ONTAP SMB- und NFS-Zugriffsereignisse gemäß den Vorgaben in den Revisionsrichtlinien nur, wenn die SMB- oder NFS-Server ausgeführt werden.

ONTAP Revisionsrichtlinien für NTFS Security-Style-Dateien und -Verzeichnisse konfigurieren

Bevor Sie Revisionsdatei- und Verzeichnisvorgänge überwachen können, müssen Sie Revisionsrichtlinien für die Dateien und Verzeichnisse konfigurieren, für die Sie Revisionsinformationen erfassen möchten. Dies ist zusätzlich zur Einrichtung und Aktivierung der Revisionskonfiguration erforderlich. NTFS-Revisionsrichtlinien können über die Registerkarte „Windows-Sicherheit“ oder über die ONTAP CLI konfiguriert werden.

Konfiguration von NTFS-Revisionsrichtlinien über die Registerkarte „Windows-Sicherheit“

Sie können NTFS-Überwachungsrichtlinien für Dateien und Verzeichnisse über die Registerkarte **Windows-Sicherheit** im Fenster „Windows-Eigenschaften“ konfigurieren. Dies entspricht der Methode, die auch bei der Konfiguration von Überwachungsrichtlinien für Daten auf einem Windows-Client verwendet wird, wodurch die gewohnte grafische Benutzeroberfläche genutzt werden kann.

Bevor Sie beginnen

Die Überwachung muss auf der Storage Virtual Machine (SVM) konfiguriert werden, die die Daten enthält, auf die Sie Systemzugriffskontrolllisten (SACLs) anwenden.

Über diese Aufgabe

Die Konfiguration von NTFS-Überwachungsrichtlinien erfolgt durch Hinzufügen von Einträgen zu NTFS-SACLs, die einem NTFS-Sicherheitsdeskriptor zugeordnet sind. Der Sicherheitsdeskriptor wird anschließend auf NTFS-Dateien und Verzeichnisse angewendet. Diese Aufgaben werden automatisch von der Windows-Benutzeroberfläche übernommen. Der Sicherheitsdeskriptor kann diskretionäre Zugriffskontrolllisten (DACLs) zur Anwendung von Datei- und Ordnerzugriffsberechtigungen, SACLs für Datei- und Ordnerüberwachung oder sowohl SACLs als auch DACLs enthalten.

Um NTFS-Überwachungsrichtlinien mithilfe der Registerkarte Windows-Sicherheit auf einem Windows-Host festzulegen, sind die folgenden Schritte erforderlich:

Schritte

1. Im Menü **Extras** des Windows Explorers **Netzlaufwerk verbinden** auswählen.
2. Das Feld **Netzlaufwerk verbinden** ausfüllen:

   a. Einen Laufwerksbuchstaben auswählen.

   b. Im Feld **Ordner** ist der Name des SMB-Servers anzugeben, der die Freigabe mit den zu prüfenden Daten sowie den Namen der Freigabe enthält.

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

      Wenn Ihr SMB-Servername “SMB_SERVER” ist und Ihre Freigabe “share1” heißt, sollte `\\SMB_SERVER\share1` eingegeben werden.

   c. Klicken Sie auf **Finish**.

   Das von Ihnen ausgewählte Laufwerk ist eingebunden und einsatzbereit, wobei das Windows Explorer-Fenster die in der Freigabe enthaltenen Dateien und Ordner anzeigt.

3. Wählen Sie die Datei oder das Verzeichnis aus, für das Sie den Revisionszugriff aktivieren möchten.

4. Klicken Sie mit der rechten Maustaste auf die Datei oder das Verzeichnis und wählen Sie dann **Eigenschaften**.
5. Die Registerkarte **Sicherheit** auswählen.
6. Auf **Erweitert** klicken.
7. Die Registerkarte **Überwachung** auswählen.
8. Führen Sie die gewünschten Aktionen aus:

Wenn Sie möchten….	Folgendes ist durchzuführen
Überwachung für einen neuen Benutzer oder eine neue Gruppe einrichten	a. Klicken Sie auf **Add**. b. Im Feld „Geben Sie den Namen des auszuwählenden Objekts ein“ den Namen des Benutzers oder der Gruppe eingeben, die hinzugefügt werden soll. c. Klicken Sie auf **OK**.
Auditing für einen Benutzer oder eine Gruppe entfernen	a. Im Feld „Geben Sie den Namen des auszuwählenden Objekts ein“ den Benutzer oder die Gruppe auswählen, die entfernt werden soll. b. Klicken Sie auf **Entfernen**. c. Klicken Sie auf **OK**. d. Der Rest dieses Vorgangs kann übersprungen werden.
Änderungsüberwachung für einen Benutzer oder eine Gruppe	a. Im Feld „Geben Sie den Objektnamen ein, um ihn auszuwählen“ wird der Benutzer oder die Gruppe ausgewählt, die geändert werden soll. b. Klicken Sie auf **Bearbeiten**. c. Klicken Sie auf **OK**.

Wenn die Überwachung für einen Benutzer oder eine Gruppe eingerichtet oder die Überwachung für einen bestehenden Benutzer oder eine bestehende Gruppe geändert wird, öffnet sich das Feld „Überwachungseintrag für <object>“.

9. Im Feld **Anwenden auf** kann ausgewählt werden, wie dieser Revisionsdatensatz angewendet werden soll.

   Sie können eine der folgenden Optionen auswählen:

   - **Dieser Ordner, Unterordner und Dateien**
   - **Dieser Ordner und Unterordner**
   - **Nur dieser Ordner**
   - **Dieser Ordner und Dateien**
   - **Nur Unterordner und Dateien**
   - **Nur Unterordner**
   - **Nur Dateien** Wenn Sie das Revisionsprotokoll für eine einzelne Datei einrichten, ist das Feld **Anwenden auf** nicht aktiv. Die Einstellung für das Feld **Anwenden auf** ist standardmäßig auf **Nur dieses Objekt** gesetzt.

   

   Da das Revisionsprotokoll SVM-Ressourcen beansprucht, sollte nur das minimale Niveau ausgewählt werden, das die Revisionsprotokoll-Ereignisse bereitstellt, die den

Sicherheitsanforderungen entsprechen.

10. Im Feld **Zugriff** kann ausgewählt werden, was protokolliert werden soll und ob erfolgreiche Ereignisse, Fehlerereignisse oder beides protokolliert werden.
    - Zum Prüfen erfolgreicher Ereignisse das Kontrollkästchen „Erfolg“ auswählen.
    - Fehlerereignisse werden protokolliert, wenn das Kontrollkästchen „Fehler“ ausgewählt ist.

      Es sollten nur die Aktionen überwacht werden, die zur Erfüllung der Sicherheitsanforderungen erforderlich sind. Weitere Informationen zu diesen überwachbaren Ereignissen enthält die Windows-Dokumentation. Die folgenden Ereignisse können geprüft werden:

    - **Volle Kontrolle**
    - **Ordner durchsuchen / Datei ausführen**
    - **Ordner auflisten / Daten lesen**
    - **Attribute lesen**
    - **Erweiterte Attribute lesen**
    - **Dateien erstellen / Daten schreiben**
    - **Ordner erstellen / Daten anhängen**
    - **Attribute schreiben**
    - **Erweiterte Attribute schreiben**
    - **Unterordner und Dateien löschen**
    - **Löschen**
    - **Leseberechtigungen**
    - **Berechtigungen ändern**
    - **Verantwortung übernehmen**
11. Wenn die Revisionsprotokoll-Einstellung nicht auf nachfolgende Dateien und Ordner des ursprünglichen Containers übertragen werden soll, ist das Kontrollkästchen **Diese Revisionsprotokolleinträge nur auf Objekte und/oder Container innerhalb dieses Containers anwenden** auszuwählen.
12. Auf **Anwenden** klicken.
13. Nachdem das Hinzufügen, Entfernen oder Bearbeiten von Revisionsprotokolleinträgen abgeschlossen ist, auf **OK** klicken.

    Der Prüfeintrag für <object> wird geschlossen.

14. Im Feld **Überwachung** können die Vererbungseinstellungen für diesen Ordner ausgewählt werden.

    Wählen Sie nur die minimale Stufe aus, die die für Ihre Sicherheitsanforderungen erforderlichen Revisionsereignisse bereitstellt. Es stehen die folgenden Optionen zur Auswahl:

    - Das Kontrollkästchen „Vererbbare Überwachungseinträge vom übergeordneten Objekt einbeziehen“ auswählen.
    - Das Kontrollkästchen „Alle vorhandenen vererbbaren Überwachungseinträge auf allen Nachfolgern durch vererbbare Überwachungseinträge aus diesem Objekt ersetzen“ auswählen.
    - Wählen Sie beide Kästchen aus.
    - Keines der Kästchen wird ausgewählt. Wenn SACLs für eine einzelne Datei festgelegt werden, ist das

Kontrollkästchen „Alle vorhandenen vererbbaren Überwachungseinträge auf allen Nachfolgern durch vererbbare Überwachungseinträge von diesem Objekt ersetzen“ im Bereich „Überwachung“ nicht vorhanden.

15. Klicken Sie auf **OK**.

    Das Prüfungsfenster wird geschlossen.

NTFS-Revisionsrichtlinien mithilfe der ONTAP CLI konfigurieren

Sie können Überwachungsrichtlinien für Dateien und Ordner mithilfe der ONTAP CLI konfigurieren. Dies ermöglicht die Konfiguration von NTFS-Überwachungsrichtlinien, ohne eine Verbindung zu den Daten über eine SMB-Freigabe auf einem Windows-Client herstellen zu müssen.

NTFS-Revisionsrichtlinien lassen sich mithilfe der `vserver security file-directory` Befehlssuite konfigurieren.

NTFS-SACLs können ausschließlich über die Befehlszeilenschnittstelle (CLI) konfiguriert werden. Die Konfiguration von NFSv4-SACLs wird mit dieser ONTAP Befehlsfamilie nicht unterstützt. Weitere Informationen zur Verwendung dieser Befehle zum Konfigurieren und Hinzufügen von NTFS-SACLs zu Dateien und Ordnern befinden sich in der "ONTAP-Befehlsreferenz".

ONTAP Revisionsprotokoll für Dateien und Verzeichnisse im UNIX-Sicherheitsstil konfigurieren

Sie konfigurieren die Überwachung für Dateien und Verzeichnisse im UNIX-Sicherheitsstil, indem Sie Überwachungs-ACEs zu den NFSv4.x-ACLs hinzufügen. Dies ermöglicht die Überwachung bestimmter NFS-Datei- und Verzeichniszugriffsereignisse zu Sicherheitszwecken.

Über diese Aufgabe

Bei NFSv4.x werden sowohl optionale als auch System-ACEs in derselben ACL gespeichert. Sie werden nicht in separaten DACLs und SACLs gespeichert. Daher ist beim Hinzufügen von Audit-ACEs zu einer bestehenden ACL Vorsicht geboten, um ein Überschreiben und den Verlust einer bestehenden ACL zu vermeiden. Die Reihenfolge, in der Audit-ACEs zu einer bestehenden ACL hinzugefügt werden, ist unerheblich.

Schritte

1. Die vorhandene ACL für die Datei oder das Verzeichnis wird mit dem `nfs4_getfacl` oder einem entsprechenden Befehl abgerufen.

   Weitere Informationen zur Manipulation von ACLs finden Sie in der "ONTAP-Befehlsreferenz".

2. Die gewünschten Audit-ACEs anhängen.
3. Die aktualisierte ACL wird auf die Datei oder das Verzeichnis mit dem `nfs4_setfacl` oder einem entsprechenden Befehl angewendet.

Informationen zu den auf Dateien und Verzeichnisse angewendeten Revisionsrichtlinien

Informationen zu den ONTAP-Revisionsrichtlinien sind über die Registerkarte „Windows-Sicherheit“ einsehbar.

Informationen zu den auf Dateien und Verzeichnisse angewendeten Revisionsrichtlinien werden über die Registerkarte „Sicherheit“ im Eigenschaftenfenster von Windows angezeigt. Dies ist die gleiche Methode wie für Daten auf einem Windows Server, wodurch Kunden die gewohnte GUI-Oberfläche nutzen können.

Über diese Aufgabe

Die Anzeige von Informationen über auf Dateien und Verzeichnisse angewendete Revisionsrichtlinien ermöglicht die Überprüfung, ob die entsprechenden Systemzugriffskontrolllisten (SACLs) für bestimmte Dateien und Ordner festgelegt sind.

Informationen über SACLs, die auf NTFS-Dateien und Ordner angewendet wurden, lassen sich auf einem Windows-Host wie folgt anzeigen.

Schritte

1. Im Menü **Extras** des Windows Explorers **Netzlaufwerk verbinden** auswählen.
2. Das Dialogfeld **Netzlaufwerk verbinden** ausfüllen:
   a. Einen Laufwerksbuchstaben auswählen.
   b. Im Feld **Ordner** ist die IP-Adresse oder der SMB-Servername der Storage Virtual Machine (SVM) anzugeben, die die Freigabe enthält, welche sowohl die zu prüfenden Daten als auch den Namen der Freigabe enthält.

      Wenn Ihr SMB-Servername “SMB_SERVER” ist und Ihre Freigabe “share1” heißt, sollte `\\SMB_SERVER\share1` eingegeben werden.

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

   c. Klicken Sie auf **Finish**.

   Das von Ihnen ausgewählte Laufwerk ist eingebunden und einsatzbereit, wobei das Windows Explorer-Fenster die in der Freigabe enthaltenen Dateien und Ordner anzeigt.
3. Wählen Sie die Datei oder das Verzeichnis aus, für das Überwachungsinformationen angezeigt werden.
4. Mit der rechten Maustaste auf die Datei oder das Verzeichnis klicken und **Eigenschaften** auswählen.
5. Die Registerkarte **Sicherheit** auswählen.
6. Auf **Erweitert** klicken.
7. Die Registerkarte **Überwachung** auswählen.
8. Klicken Sie auf **Weiter**.

   Das Überwachungsfenster öffnet sich. Im Fenster **Überwachungseinträge** wird eine Zusammenfassung der Benutzer und Gruppen angezeigt, denen SACLs zugewiesen sind.
9. Im Feld **Überwachungseinträge** den Benutzer oder die Gruppe auswählen, deren SACL-Einträge angezeigt werden sollen.
10. Klicken Sie auf **Bearbeiten**.

Der Auditing-Eintrag für <object> wird geöffnet.

11. Im Feld **Zugriff** werden die aktuell auf das ausgewählte Objekt angewendeten SACLs angezeigt.
12. Klicken Sie auf **Abbrechen**, um das Feld **Überwachungseintrag für <object>** zu schließen.
13. Mit **Abbrechen** wird das Fenster **Überwachung** geschlossen.

Informationen zu NTFS-Audit-Richtlinien auf ONTAP FlexVol Volumes

Sie können Informationen zu NTFS-Überwachungsrichtlinien auf FlexVol Volumes anzeigen, einschließlich der Sicherheitsstile und effektiven Sicherheitsstile, der angewendeten Berechtigungen sowie Informationen zu Systemzugriffskontrolllisten. Diese Informationen dienen zur Validierung der Sicherheitskonfiguration oder zur Fehlerbehebung bei Überwachungsproblemen.

Über diese Aufgabe

Die Anzeige von Informationen über auf Dateien und Verzeichnisse angewendete Revisionsrichtlinien ermöglicht die Überprüfung, ob die entsprechenden Systemzugriffskontrolllisten (SACLs) 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 Sie anzeigen möchten. Die Ausgabe kann in zusammengefasster Form oder als detaillierte Liste angezeigt werden.

- NTFS Security-Style Volumes und Qtrees verwenden ausschließlich NTFS-Systemzugriffskontrolllisten (SACLs) für Audit-Richtlinien.
- Auf Dateien und Ordner in einem Volume mit gemischtem Sicherheitsstil und effektiver NTFS-Sicherheit können NTFS-Überwachungsrichtlinien angewendet werden.

  Volumes und Qtrees mit gemischtem Security-Style können einige Dateien und Verzeichnisse enthalten, die UNIX-Dateiberechtigungen verwenden, entweder Modusbits oder NFSv4-ACLs, und einige Dateien und Verzeichnisse, die NTFS-Dateiberechtigungen verwenden.

- Die oberste Ebene eines Volumes mit gemischtem Sicherheitsstil kann entweder UNIX- oder NTFS-effektive Sicherheit aufweisen und kann NTFS-SACLs enthalten oder auch nicht.
- Da die Storage-Level Access Guard Sicherheit auch auf einem Volume oder Qtree mit gemischtem Sicherheitsstil konfiguriert werden kann, selbst wenn der effektive Sicherheitsstil des Volume-Root oder Qtree UNIX ist, kann die Ausgabe für einen Volume- oder Qtree-Pfad, auf dem Storage-Level Access Guard konfiguriert ist, sowohl reguläre Datei- und Ordner-NFSv4-SACLs als auch Storage-Level Access Guard NTFS-SACLs anzeigen.
- Wenn der im Befehl eingegebene Pfad zu Daten mit NTFS effektiver Sicherheit führt, werden in der Ausgabe auch Informationen über Dynamic Access Control ACEs angezeigt, sofern Dynamic Access Control für den angegebenen Datei- oder Verzeichnispfad konfiguriert ist.
- Bei der Anzeige von Sicherheitsinformationen zu Dateien und Ordnern mit NTFS effektiver Sicherheit enthalten die UNIX-bezogenen Ausgabefelder nur Anzeigeinformationen zu UNIX-Dateiberechtigungen.

  Dateien und Ordner im NTFS-Sicherheitsstil verwenden ausschließlich NTFS-Dateiberechtigungen sowie Windows-Benutzer und -Gruppen zur Bestimmung der Dateizugriffsrechte.

- 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 und bei denen nur Modus-Bit-

Berechtigungen angewendet werden (keine NFSv4 ACLs).

- Die Ausgabefelder „Besitzer“ und „Gruppe“ in der ACL-Ausgabe gelten nur im Fall von NTFS-Sicherheitsdeskriptoren.

Schritt

1. Anzeige der Überwachungsrichtlinieneinstellungen für Dateien und Verzeichnisse mit dem gewünschten Detaillierungsgrad:

Wenn Informationen angezeigt werden sollen…	Führen Sie den folgenden Befehl aus…
Zusammengefasst	`vserver security file-directory show -vserver vserver_name -path path`
Als detaillierte Liste	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Beispiele

Das folgende Beispiel zeigt die Informationen zur Überwachungsrichtlinie für den Pfad `/corp` in SVM vs1. Der Pfad verfügt über effektive NTFS-Sicherheit. Der NTFS-Sicherheitsdeskriptor enthält sowohl einen SUCCESS- als auch einen SUCCESS/FAIL-SACL-Eintrag.

```
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
```

Das folgende Beispiel zeigt die Informationen zur Überwachungsrichtlinie für den Pfad `/datavol1` in SVM vs1. Der Pfad enthält sowohl reguläre Datei- und Ordner-SACLs als auch Storage-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
```

Platzhalterzeichen können verwendet werden, um Informationen zu ONTAP Dateisicherheits- und Revisionsprotokollrichtlinien anzuzeigen.

Sie können das Platzhalterzeichen (*) verwenden, um Informationen über die Dateisicherheit und die Revisionsprotokollrichtlinien aller Dateien und Verzeichnisse unter einem bestimmten Pfad oder einem Stammvolume anzuzeigen.

Das Platzhalterzeichen (*) kann als letzter Bestandteil eines angegebenen Verzeichnispfads verwendet werden, unterhalb dessen Informationen zu allen Dateien und Verzeichnissen angezeigt werden.

Wenn Informationen zu einer bestimmten Datei oder einem Verzeichnis mit dem Namen "*" angezeigt werden sollen, ist der vollständige Pfad in doppelten Anführungszeichen (" ") anzugeben.

Beispiel

Der folgende Befehl mit dem Platzhalterzeichen zeigt die Informationen zu allen Dateien und Verzeichnissen unterhalb des Pfads `/1/` von SVM vs1 an:

```
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)
```

Der folgende Befehl zeigt die Informationen einer Datei mit dem Namen "*" unter dem Pfad `/vol1/a` von SVM vs1 an. Der Pfad ist in doppelte Anführungszeichen (" ") eingeschlossen.

```
cluster::> vserver security file-directory show -vserver 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
```

CLI-Änderungsereignisse, die geprüft werden können

Informationen zu ONTAP CLI-Änderungsereignissen, die protokolliert werden können

ONTAP kann bestimmte CLI-Änderungsereignisse protokollieren, darunter bestimmte SMB-Freigabeereignisse, bestimmte Überwachungsrichtlinienereignisse, bestimmte lokale Sicherheitsgruppenereignisse, lokale Nutzergruppe-Ereignisse und Autorisierungsrichtlinienereignisse. Das Verständnis darüber, welche Änderungsereignisse protokolliert werden können, ist hilfreich bei der Interpretation der Ergebnisse aus den Ereignisprotokollen.

Sie können CLI-Änderungsereignisse der Storage Virtual Machine (SVM) verwalten, indem Sie die Audit-Protokolle manuell rotieren, die Auditierung aktivieren oder deaktivieren, Informationen zu Auditierungsänderungsereignissen anzeigen, Auditierungsänderungsereignisse ändern und Auditierungsänderungsereignisse löschen.

Wenn als Administrator ein Befehl ausgeführt wird, der die Konfiguration im Zusammenhang mit SMB-Share, lokaler Nutzergruppe, lokaler Sicherheitsgruppe, Authorization-Policy und Audit-Policy Ereignissen ändert, wird ein Datensatz generiert und das entsprechende Ereignis protokolliert:

Prüfungskategorie	Veranstaltungen	Ereignis-IDs	Führen Sie diesen Befehl aus…
Mhost Auditing	Richtlinienänderung	[4719] Die Audit-Konfiguration wurde 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 Nutzer 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 Passworts des lokalen Benutzers
`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
`vserver cifs users-and-groups local-group rename`	modify` `vserver services name-service unix-group modify`	[4732] Benutzer zur lokalen Gruppe hinzugefügt	`vserver cifs users-and-groups local-group add-members vserver services name-service unix-group adduser`
[4733] Benutzer aus lokaler Gruppe entfernt	`vserver cifs users-and-groups local-group remove-members vserver services name-service unix-group deluser`	Änderung der Autorisierungsrichtlinie	[4704] Zugewiesene Benutzerrechte
`vserver cifs users-and-groups privilege add-privilege`	[4705] Benutzerrechte entfernt	`vserver cifs users-and-groups privilege remove-privilege`	reset-privilege`

Verwandte Informationen

- "vserver"

ONTAP Dateifreigabeereignisse verwalten

Wenn für eine Storage Virtual Machine (SVM) ein Dateifreigabeereignis konfiguriert und eine Überwachung aktiviert ist, werden Überwachungsereignisse generiert. Die Dateifreigabeereignisse werden generiert, wenn die SMB-Netzwerkfreigabe mit `vserver cifs share` verwandten Befehlen geändert wird.

Die Dateifreigabeereignisse mit den Ereignis-IDs 5142, 5143 und 5144 werden generiert, wenn eine SMB-Netzwerkfreigabe für die SVM hinzugefügt, geändert oder gelöscht wird. Die SMB-Netzwerkfreigabekonfiguration wird mit den `cifs share access control create|modify|delete` Befehlen geändert.

Das folgende Beispiel zeigt ein Dateifreigabeereignis mit der ID 5143, das generiert wird, wenn ein Freigabeobjekt 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)
```

ONTAP-Ereignisse zur Änderung der Audit-Richtlinie verwalten

Wenn für eine Storage Virtual Machine (SVM) ein Ereignis zur Änderung der Audit-Policy konfiguriert und das Auditing aktiviert ist, werden Audit-Ereignisse generiert. Die Audit-Policy-Change-Ereignisse werden generiert, wenn eine Audit-Policy mithilfe `vserver audit` verwandter Befehle geändert wird.

Das Ereignis „audit-policy-change“ mit der Ereignis-ID 4719 wird immer dann generiert, wenn eine Überwachungsrichtlinie deaktiviert, aktiviert oder geändert wird und hilft dabei, zu erkennen, wenn ein Benutzer versucht, die Überwachung zu deaktivieren, um Spuren zu verwischen. Es ist standardmäßig konfiguriert und erfordert Diagnoseberechtigung zum Deaktivieren.

Das folgende Beispiel zeigt ein Ereignis zur Änderung der Revisionsrichtlinie mit der ID 4719, das generiert wird, wenn eine Überwachung 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
```

Benutzerkonto-ONTAP-Ereignisse verwalten

Wenn ein Benutzerkontoereignis für eine Storage Virtual Machine (SVM) konfiguriert ist und eine Überwachung aktiviert ist, werden Überwachungsereignisse generiert.

Die Benutzerkontoereignisse mit den Ereignis-IDs 4720, 4722, 4724, 4725, 4726, 4738 und 4781 werden generiert, wenn ein lokaler SMB- oder NFS-Benutzer im System erstellt oder gelöscht wird, ein lokales

Benutzerkonto aktiviert, deaktiviert oder geändert wird oder das Passwort eines lokalen SMB-Benutzers zurückgesetzt oder geändert wird. Die Benutzerkontoereignisse werden generiert, wenn ein Benutzerkonto mithilfe von `vserver cifs users-and-groups <local user>` und `vserver services name-service <unix user>` Befehlen geändert wird.

Das folgende Beispiel zeigt ein Benutzerkontoereignis mit der ID 4720, das generiert wird, wenn ein lokaler SMB-Benutzer erstellt wird:

```
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 ~
```

Das folgende Beispiel zeigt ein Benutzerkontoereignis mit der ID 4781, das generiert wurde, als der im vorhergehenden Beispiel erstellte lokale SMB-Benutzer umbenannt wurde:

```
 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 ~
```

Verwaltung von ONTAP Sicherheitsgruppen-Ereignissen

Wenn ein Sicherheitsgruppenereignis für eine Storage Virtual Machine (SVM) konfiguriert ist und eine Überwachung aktiviert ist, werden Überwachungsereignisse generiert.

Die Sicherheitsgruppenereignisse mit den Ereignis-IDs 4731, 4732, 4733, 4734 und 4735 werden generiert, wenn eine lokale SMB- oder NFS-Gruppe auf dem System erstellt oder gelöscht wird und ein lokaler Benutzer der Gruppe hinzugefügt oder daraus entfernt wird. Die Sicherheitsgruppenereignisse werden generiert, wenn ein Benutzerkonto mit `vserver cifs users-and-groups <local-group>`- und `vserver services name-service <unix-group>`-Befehlen geändert wird.

Das folgende Beispiel zeigt ein Sicherheitsgruppenereignis mit der ID 4731, das beim Erstellen einer lokalen UNIX-Sicherheitsgruppe generiert 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 ~
```

ONTAP-Ereignisse zur Änderung der Autorisierungsrichtlinie verwalten

Wenn das Ereignis zur Änderung der Autorisierungsrichtlinie für eine Storage Virtual Machine (SVM) konfiguriert ist und eine Revisionsfunktion aktiviert ist, werden Revisionsereignisse generiert.

Die Ereignisse vom Typ „Autorisierungsrichtlinienänderung“ mit den Ereignis-IDs 4704 und 4705 werden immer dann generiert, wenn einem SMB-Benutzer oder einer SMB-Gruppe Autorisierungsrechte erteilt oder entzogen werden. Die Ereignisse vom Typ „Autorisierungsrichtlinienänderung“ werden generiert, wenn die Autorisierungsrechte mithilfe von `vserver cifs users-and-groups privilege` zugehörigen Befehlen zugewiesen oder entzogen werden.

Das folgende Beispiel zeigt ein Autorisierungsrichtlinienereignis mit der ID 4704, das generiert wurde, als die Autorisierungsrechte für eine SMB-Benutzergruppe zugewiesen wurden:

```
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
```

Überwachungskonfigurationen verwalten

Die Audit-Ereignisprotokolle manuell rotieren, um bestimmte ONTAP SVM-Ereignisprotokolle anzuzeigen

Bevor Sie die Audit-Ereignisprotokolle anzeigen können, müssen diese in ein benutzerlesbares Format konvertiert werden. Wenn die Ereignisprotokolle einer bestimmten Storage Virtual Machine (SVM) vor der automatischen Protokollrotation durch ONTAP angezeigt werden sollen, ist eine manuelle Rotation der Audit-Ereignisprotokolle auf dieser SVM möglich.

Schritt

1. Die Audit-Ereignisprotokolle werden mit dem `vserver audit rotate-log` Befehl rotiert.

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

Das Audit-Ereignisprotokoll wird im SVM-Audit-Ereignisprotokollverzeichnis im durch die Audit-Konfiguration festgelegten Format gespeichert (`XML` oder `EVTX` und kann mit der entsprechenden Anwendung angezeigt werden.

Überwachung auf ONTAP SVMs aktivieren oder deaktivieren

Sie können die Überwachung auf Storage Virtual Machines (SVMs) aktivieren oder deaktivieren. Die Überwachung von Dateien und Verzeichnissen kann vorübergehend durch Deaktivieren der Überwachung gestoppt werden. Die Überwachung kann jederzeit wieder aktiviert werden (sofern eine Überwachungskonfiguration vorhanden ist).

Bevor Sie beginnen

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

"Die Überwachungskonfiguration erstellen"

Über diese Aufgabe

Das Deaktivieren der Überwachung löscht die Überwachungskonfiguration nicht.

Schritte

1. Den entsprechenden Befehl ausführen:

Wenn eine Überprüfung erfolgen soll…	Geben Sie den Befehl ein…
Aktiviert	`vserver audit enable -vserver vserver_name`
Deaktiviert	`vserver audit disable -vserver vserver_name`

2. Es sollte sichergestellt werden, dass sich die Überwachung im gewünschten Zustand befindet:

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

Beispiele

Das folgende Beispiel ermöglicht die Überwachung für 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
```

Das folgende Beispiel deaktiviert die Überwachung für SVM vs1:

```
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
```

Informationen zu ONTAP Audit-Konfigurationen

Sie können Informationen zu Revisionskonfigurationen anzeigen. Die Informationen können dabei helfen festzustellen, ob die Konfiguration für jede SVM wie gewünscht eingerichtet ist. Die angezeigten Informationen ermöglichen zudem die Überprüfung, ob eine Revisionskonfiguration aktiviert ist.

Über diese Aufgabe

Sie können detaillierte Informationen zu den Audit-Konfigurationen aller SVMs anzeigen oder die angezeigten Informationen durch Angabe optionaler Parameter anpassen. Wenn Sie keinen der optionalen Parameter angeben, wird Folgendes angezeigt:

- SVM-Name, auf den die Auditing-Konfiguration angewendet wird
- Der Revisionsstatus, der `true` oder `false` sein kann

  Wenn der Revisionsstatus `true` ist, ist die Revision aktiviert. Wenn der Revisionsstatus `false` ist, ist die Revision deaktiviert.

- Die Kategorien der zu prüfenden Ereignisse
- Das Revisionsprotokoll-Format

- Das Zielverzeichnis, in dem das Überwachungssubsystem konsolidierte und konvertierte Revisionsprotokolle speichert

Schritt

1. Informationen zur Audit-Konfiguration werden mit dem `vserver audit show` Befehl angezeigt.

   Weitere Informationen zu `vserver audit show` finden sich in der "ONTAP-Befehlsreferenz".

Beispiele

Das folgende Beispiel zeigt eine Zusammenfassung der Revisionskonfiguration für alle SVMs:

```
cluster1::> vserver audit show

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

Das folgende Beispiel zeigt in Listenform alle Revisionskonfigurationsinformationen für alle SVMs:

```
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
```

ONTAP Befehle zum Ändern von Audit-Konfigurationen

Wenn eine Revisions-Einstellung geändert werden soll, kann die aktuelle Konfiguration jederzeit angepasst werden, einschließlich der Änderung des Protokollpfad-Ziels und des Protokollformats, der Kategorien der zu prüfenden Ereignisse, der automatischen Speicherung von Protokolldateien sowie der Angabe der maximalen Anzahl an zu speichernden Protokolldateien.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…

Pfad des Protokollziels ändern	`vserver audit modify` mit dem `-destination` Parameter
Die Kategorie der zu prüfenden Ereignisse anpassen	`vserver audit modify` mit dem `-events` Parameter Um Ereignisse der zentralen Zugriffsrichtlinienbereitstellung zu prüfen, muss die Dynamic Access Control (DAC) SMB-Serveroption auf der Storage Virtual Machine (SVM) aktiviert sein.
Das Protokollformat anpassen	`vserver audit modify` mit dem `-format` Parameter
Automatisches Speichern basierend auf der Größe der internen Protokolldatei aktivieren	`vserver audit modify` mit dem `-rotate-size` Parameter
Automatisches Speichern basierend auf einem Zeitintervall aktivieren	`vserver audit modify` mit den `-rotate -schedule-month`, `-rotate-schedule -dayofweek`, `-rotate-schedule-day`, `-rotate -schedule-hour` und `-rotate-schedule -minute` Parametern
Festlegen der maximalen Anzahl gespeicherter Protokolldateien	`vserver audit modify` mit dem `-rotate-limit` Parameter

Löschen einer Revisionskonfiguration auf einer ONTAP SVM

Wenn Sie keine Revisionsdatei- und Verzeichnisereignisse mehr auf der Storage Virtual Machine (SVM) protokollieren und keine Revisionskonfiguration auf der SVM aufrechterhalten möchten, kann die Revisionskonfiguration gelöscht werden.

Schritte

1. Die Revisionskonfiguration deaktivieren:

```
vserver audit disable -vserver vserver_name

vserver audit disable -vserver vs1
```

2. Die Revisionskonfiguration löschen:

```
vserver audit delete -vserver vserver_name

vserver audit delete -vserver vs1
```

Die Auswirkungen der Rücksetzung eines geprüften ONTAP Clusters

Wenn Sie planen, den Cluster zurückzusetzen, sollten Sie sich über den Rücksetzungsprozess informieren, den ONTAP befolgt, wenn im Cluster Storage Virtual Machines (SVMs) mit aktivierter Überwachung vorhanden sind. Bestimmte Maßnahmen sind vor der Rücksetzung erforderlich.

Die Rückkehr zu einer Version von ONTAP, die die Überwachung von SMB-An- und Abmeldeereignissen sowie von Ereignissen der zentralen Zugriffsrichtlinienbereitstellung nicht unterstützt

Die Unterstützung für die Überwachung von SMB-An- und Abmeldeereignissen sowie von Ereignissen der zentralen Zugriffsrichtlinienbereitstellung beginnt mit clustered Data ONTAP 8.3. Wenn auf eine Version von ONTAP zurückgesetzt wird, die diese Ereignistypen nicht unterstützt, und Überwachungskonfigurationen vorhanden sind, die diese Ereignistypen überwachen, muss die Überwachungskonfiguration für die entsprechenden SVMs mit aktivierter Überwachung vor dem Zurücksetzen geändert werden. Die Konfiguration muss so angepasst werden, dass nur Dateivorgänge überwacht werden.

Probleme mit ONTAP Auditing und Staging Volume Speicherplatz beheben

Probleme können auftreten, wenn auf den Staging-Volumes oder dem Volume mit den Audit-Ereignisprotokollen nicht genügend Speicherplatz vorhanden ist. Wenn nicht genügend Speicherplatz vorhanden ist, können keine neuen Audit-Einträge erstellt werden. Wenn die Audit-Garantie aktiviert ist, kann dies den Datenzugriff von Clients verhindern und zu Fehlern bei Zugriffsanfragen führen. Es ist wichtig, die Vorgehensweise zur Fehlerbehebung und Lösung dieser Speicherplatzprobleme bei Volumes zu kennen.

Dieses Verhalten tritt auf, wenn die Audit-Garantie aktiviert ist. Weitere Informationen finden Sie unter "Garantierte Prüfung".

Beheben von Speicherplatzproblemen im Zusammenhang mit den Ereignisprotokollvolumes

Wenn Volumes mit Ereignisprotokolldateien keinen Speicherplatz mehr haben, kann die Überwachung keine Protokolleinträge in Protokolldateien umwandeln. Wenn die Audit-Garantie aktiviert ist, führt dies zu Fehlern beim Clientzugriff. Es ist erforderlich, die Vorgehensweise zur Fehlerbehebung bei Speicherplatzproblemen im Zusammenhang mit Ereignisprotokoll-Volumes zu kennen.

- Administratoren von Storage Virtual Machines (SVM) und Clustern können feststellen, ob nicht genügend Volume-Speicherplatz vorhanden ist, indem Informationen über die Nutzung und Konfiguration von Volumes und Aggregaten angezeigt werden.
- Wenn in den Volumes, die die Ereignisprotokolle enthalten, nicht genügend Speicherplatz vorhanden ist, können SVM- und Clusteradministratoren das Speicherplatzproblem beheben, indem sie entweder einige der Ereignisprotokolldateien entfernen oder die Größe des Volumes erhöhen.

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

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

  Der Datenzugriff wird in folgenden Fällen verweigert:

  - Das Zielverzeichnis wurde gelöscht.

- Das Dateilimit auf einem Volume, das das Zielverzeichnis hostet, erreicht sein maximales Niveau.

Weitere Informationen zu:

- "Informationen zu Volumes anzeigen und die Volumegröße erhöhen".
- "Informationen zu Aggregaten anzeigen und Aggregate verwalten".

Behebung von Speicherplatzproblemen im Zusammenhang mit den Staging Volumes

Wenn auf einem der Volumes, die Staging-Dateien für Ihre Storage Virtual Machine (SVM) enthalten, der Speicherplatz ausgeht, kann die Überwachung keine Protokolleinträge in die Staging-Dateien schreiben. Bei aktivierter Überwachungsgarantie führt dies zu Fehlern beim Clientzugriff. Zur Fehlerbehebung bei diesem Problem ist zu ermitteln, ob eines der in der SVM verwendeten Staging-Volumes voll ist, indem Informationen zur Volume-Nutzung angezeigt werden.

Wenn das Volume mit den konsolidierten Ereignisprotokolldateien über ausreichend Speicherplatz verfügt, aber weiterhin Clientzugriffsfehler aufgrund von unzureichendem Speicherplatz auftreten, könnten die Staging-Volumes keinen freien Speicherplatz mehr haben. Der SVM-Administrator muss sich an Sie wenden, um festzustellen, ob die Staging-Volumes, die Staging-Dateien für die SVM enthalten, über unzureichenden Speicherplatz verfügen. Das Auditing-Subsystem generiert ein EMS-Ereignis, wenn Auditing-Ereignisse aufgrund von unzureichendem Speicherplatz in einem Staging-Volume nicht generiert werden können. Die folgende Meldung wird angezeigt: `No space left on device`. Nur Sie können Informationen zu Staging-Volumes anzeigen; SVM-Administratoren können dies nicht.

Alle Namen von Staging-Volumes beginnen mit `MDV_aud_` gefolgt von der UUID des Aggregats, das dieses Staging-Volume enthält. Das folgende Beispiel zeigt vier System-Volumes auf der Admin-SVM, die automatisch erstellt wurden, als eine Dateidienst-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 in den Staging-Volumes nicht genügend Speicherplatz vorhanden ist, lässt sich das Speicherplatzproblem durch Erhöhen der Volume-Größe beheben.

> Wenn das Aggregat, das das Staging-Volume enthält, voll ist, muss die Größe des Aggregats erhöht werden, bevor die Größe des Volumes erhöht werden kann. Nur Sie können die Größe eines Aggregats erhöhen; SVM-Administratoren können dies nicht.

Wenn ein oder mehrere Aggregate weniger als 2GB (in ONTAP 9.14.1 und früher) oder 5GB (ab ONTAP 9.15.1) verfügbaren Speicherplatz haben, schlägt die SVM Audit-Erstellung fehl. Wenn die SVM Audit-Erstellung fehlschlägt, werden die erstellten Staging Volumes gelöscht.

Copyright-Informationen

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

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

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