Erstellen einer Datei- und Verzeichnisüberwachungskonfiguration auf SVMs

ONTAP 9

NetApp
September 09, 2026

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

Inhalt

Erstellen einer Datei- und Verzeichnisüberwachungskonfiguration auf SVMs 1
Erstellung der Datei- und Verzeichnisüberwachungskonfiguration auf ONTAP SVMs 1
Die Überwachung auf ONTAP SVMs wird nach dem Einrichten der Überwachungskonfiguration aktiviert. . . 3
Die ONTAP Revisionsprotokoll-Konfiguration überprüfen 3

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."

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.