



Management von Audit-Konfigurationen

ONTAP 9

NetApp
March 24, 2023

Inhaltsverzeichnis

- Management von Audit-Konfigurationen 1
 - Drehen Sie die Überwachungsprotokolle manuell 1
 - Aktivieren und Deaktivieren der Prüfung auf SVMs 1
 - Zeigt Informationen zu Überwachungskonfigurationen an 2
 - Befehle zum Ändern von Überwachungskonfigurationen 4
 - Löschen einer Überwachungskonfiguration 5
 - Was ist der Prozess beim Zurückkehren 5

Management von Audit-Konfigurationen

Drehen Sie die Überwachungsprotokolle manuell

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

Schritt

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

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

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

Aktivieren und Deaktivieren der Prüfung auf SVMs

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

Was Sie benötigen

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

Über diese Aufgabe

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

Schritte

1. Führen Sie den entsprechenden Befehl aus:

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

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

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

Beispiele

Das folgende Beispiel ermöglicht das Auditing von SVM vs1:

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

cluster1::> vserver audit show -vserver vs1

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

Im folgenden Beispiel wird das Auditing von SVM vs1 deaktiviert:

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

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

Zeigt Informationen zu Überwachungskonfigurationen an

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

Überwachungskonfiguration aktiviert ist.

Über diese Aufgabe

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

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

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

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

Schritt

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

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

Beispiele

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

```
cluster1::> vservers audit show

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

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

```


cluster1::> vserver audit show -instance

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

```

Befehle zum Ändern von Überwachungskonfigurationen

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

Ihr Ziel ist	Befehl
Ändern Sie den Protokollzielpfad	<code>vserver audit modify</code> Mit dem <code>-destination</code> Parameter
Ändern Sie die Kategorie der zu prüfenden Ereignisse	<code>vserver audit modify</code> Mit dem <code>-events</code> Parameter  Zur Prüfung von Staging von zentralen Zugriffsrichtlinien muss die SMB-Serveroption Dynamic Access Control (DAC) auf der Storage Virtual Machine (SVM) aktiviert sein.
Ändern Sie das Protokollformat	<code>vserver audit modify</code> Mit dem <code>-format</code> Parameter
Aktivieren von automatischen Speichern basierend auf der internen Protokolldateigröße	<code>vserver audit modify</code> Mit dem <code>-rotate-size</code> Parameter

Durch Aktivieren der automatischen Einsparung auf Basis eines Zeitintervalls	<code>vserver audit modify</code> Mit dem <code>-rotate-schedule-month</code> , <code>-rotate-schedule-dayofweek</code> , <code>-rotate-schedule-day</code> , <code>-rotate-schedule-hour</code> , und <code>-rotate-schedule-minute</code> Parameter
Festlegen der maximalen Anzahl von gespeicherten Protokolldateien	<code>vserver audit modify</code> Mit dem <code>-rotate-limit</code> Parameter

Löschen einer Überwachungskonfiguration

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

Schritte

1. Deaktivieren der Überwachungskonfiguration:

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

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

2. Löschen Sie die Überwachungskonfiguration:

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

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

Was ist der Prozess beim Zurückkehren

Wenn Sie den Cluster zurücksetzen möchten, sollten Sie auf den ONTAP für den Umkehrprozess achten, wenn es im Cluster Audit-fähige Storage Virtual Machines (SVMs) gibt. Sie müssen bestimmte Aktionen durchführen, bevor Sie den Wechsel rückgängig machen.

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

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

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtlich geschützten Urhebers 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, BEISPIELHAFT 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 IRGENDWEISE 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.