Erstellen einer Datei- und Verzeichnisüberprüfung auf SVMs

ONTAP 9

NetApp
February 12, 2026

Inhalt

Erstellen einer Datei- und Verzeichnisüberprüfung auf SVMs

Konfiguration von Datei- und Verzeichnisprüfungen auf ONTAP SVMs erstellen

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

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

Bevor Sie beginnen

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

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

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

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

  Solche Fehler erzeugen keinen Audit-Datensatz.

Über diese Aufgabe

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

Schritt

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

Wenn Sie die Prüfprotokolle drehen möchten, um…	Eingeben…
Protokollgröße	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging

file-share	authorization-policy-change
user-account	security-group
authorization-policy-change}] [-format {xml	evtx}] [-rotate-limit integer] [-rotate-size {integer[KB
MB	GB
TB	PB]}]`
Einen Zeitplan	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging}] [-format {xml

Beispiele

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

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

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

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

Im folgenden Beispiel wird eine Audit-Konfiguration erstellt, die Dateivorgänge, CIFS-Anmelde- und -Abmeldungsereignisse und zentrale Zugriffs- und Staging-Ereignisse anhand zeitbasierter Rotation prüft. Das Protokollformat ist `EVTX` (Standard). Die Prüfprotokolle werden monatlich um 12:30 Uhr an allen Wochentagen gedreht. Die Log-Rotationsgrenze ist `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

- "Prüfung auf SVM aktivieren"
- "Überprüfen Sie die Überwachungskonfiguration"

Aktivieren Sie Auditing für ONTAP SVMs nach Einrichtung der Überwachungskonfiguration

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

Bevor Sie beginnen

Die SVM-Audit-Konfiguration muss bereits vorhanden sein.

Über diese Aufgabe

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

Schritte

1. Prüfung auf der SVM aktivieren:

   ```
   vserver audit enable -vserver vserver_name

   vserver audit enable -vserver vs1
   ```

Verwandte Informationen

- "Erstellen Sie die Überwachungskonfiguration"
- "Überprüfen Sie die Überwachungskonfiguration"

Überprüfen Sie die ONTAP-Überwachungskonfiguration

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

Schritte

1. Überprüfen Sie die Überwachungskonfiguration:

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

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

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

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

Verwandte Informationen

- "Erstellen Sie die Überwachungskonfiguration"
- "Prüfung auf SVM aktivieren"