Management von Audit-Konfigurationen

ONTAP 9

NetApp
March 24, 2023

Inhaltsverzeichnis

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	`vserver audit enable -vserver vserver_name`
Deaktiviert	`vserver audit disable -vserver vserver_name`

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

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

Beispiele

Das folgende Beispiel ermöglicht das Auditing von SVM vs1:

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

cluster1::> vserver audit show -vserver vs1

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

Im folgenden Beispiel wird das Auditing von SVM vs1 deaktiviert:

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

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

Zeigt Informationen zu Überwachungskonfigurationen an

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

Überwachungskonfiguration aktiviert ist.

Über diese Aufgabe

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

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

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

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

Schritt

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

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

Beispiele

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

```
cluster1::> vserver audit show

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

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

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

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

Befehle zum Ändern von Überwachungskonfigurationen

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

Ihr Ziel ist	Befehl
Ändern Sie den Protokollzielpfad	`vserver audit modify` Mit dem `-destination` Parameter
Ändern Sie die Kategorie der zu prüfenden Ereignisse	`vserver audit modify` Mit dem `-events` 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	`vserver audit modify` Mit dem `-format` Parameter
Aktivieren von automatischen Speichern basierend auf der internen Protokolldateigröße	`vserver audit modify` Mit dem `-rotate-size` Parameter

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