Funktionsweise des Audits

ONTAP 9

NetApp
March 22, 2023

Inhaltsverzeichnis

Funktionsweise des Audits

Grundlegende Prüfungskonzepte

Um das Auditing in ONTAP zu verstehen, sollten Sie einige grundlegende Prüfungskonzepte kennen.

- **Staging-Dateien**

  Die zwischenliegenden Binärdateien auf einzelnen Knoten, in denen Audit-Datensätze vor der Konsolidierung und Konvertierung gespeichert werden. Staging-Dateien sind in Staging-Volumes enthalten.

- **Staging Volumen**

  Ein von ONTAP erstelltes dediziertes Volume zum Speichern von Staging-Dateien. Es gibt ein Staging-Volume pro Aggregat. Staging Volumes werden von allen revisionssichere Storage Virtual Machines (SVMs) gemeinsam genutzt, um Audit-Datensätze des Datenzugriffs für Daten-Volumes im jeweiligen Aggregat zu speichern. Die Audit-Datensätze jeder SVM werden in einem separaten Verzeichnis innerhalb des Staging-Volume gespeichert.

  Cluster-Administratoren können Informationen über Staging Volumes anzeigen, die meisten anderen Volume-Vorgänge sind jedoch nicht zulässig. Nur ONTAP kann Staging-Volumes erstellen. ONTAP weist Staging-Volumes automatisch einen Namen zu. Alle Staging-Volume-Namen beginnen mit `MDV_aud_` Anschließend die UUID des Aggregats, welches das Staging-Volume enthält (z. B.: `MDV_aud_1d0131843d4811e296fc123478563412`.)

- **System-Volumes**

  Ein FlexVol Volume mit speziellen Metadaten, wie z. B. Metadaten für Audit-Protokolle für Fileservices. Die Admin-SVM ist Eigentümer von System-Volumes, die im Cluster sichtbar sind. Staging Volumes sind eine Art System-Volume.

- * Konsolidierungsaufgabe*

  Eine Aufgabe, die bei aktivierter Prüfung erstellt wird. Diese langwierige Aufgabe auf jeder SVM nimmt die Audit-Datensätze aus Staging-Dateien über die Mitglied-Nodes der SVM auf. Mit dieser Aufgabe werden die Audit-Datensätze in einer sortierten chronologischen Reihenfolge zusammengeführt und dann in ein benutzerlesbares Ereignisprotokollformat konvertiert, das in der Überwachungskonfiguration angegeben ist – entweder das EVTX- oder das XML-Dateiformat. Die umgerechneten Ereignisprotokolle werden im Verzeichnis für Revisionsereignisse gespeichert, das in der SVM-Audit-Konfiguration angegeben ist.

Funktionsweise des ONTAP-Prüfprozesses

Der ONTAP-Audit-Prozess unterscheidet sich vom Microsoft-Audit-Prozess. Bevor Sie die Prüfung konfigurieren, sollten Sie verstehen, wie der ONTAP-Audit-Prozess funktioniert.

Auditdatensätze werden zunächst in binären Staging-Dateien auf einzelnen Knoten gespeichert. Wenn das Auditing auf einer SVM aktiviert ist, behält jeder Member-Node Staging-Dateien für diese SVM bei. Sie werden in regelmäßigen Abständen konsolidiert und in benutzerlesbare Ereignisprotokolle umgewandelt, die im

Verzeichnis der Auditereignisse für die SVM gespeichert sind.

Prozess, bei dem die Prüfung auf einer SVM aktiviert ist

Auditing kann nur auf SVMs aktiviert werden. Wenn der Storage-Administrator das Auditing für die SVM ermöglicht, überprüft das Auditing-Subsystem, ob Staging-Volumes vorhanden sind. Für jedes Aggregat, das Daten-Volumes der SVM enthält, muss ein Staging-Volume vorhanden sein. Das Audit-Subsystem erstellt alle erforderlichen Staging-Volumes, wenn sie nicht vorhanden sind.

Das Revisions-Subsystem schließt auch andere erforderliche Aufgaben ab, bevor die Prüfung aktiviert wird:

- Das Audit-Subsystem überprüft, ob der Protokollverzeichnis-Pfad verfügbar ist und keine Symlinks enthält.

  Das Logverzeichnis muss bereits als Pfad innerhalb des Namespace der SVM vorhanden sein. Es wird empfohlen, ein neues Volume oder einen neuen qtree zu erstellen, um die Audit-Log-Dateien zu speichern. Das Audit-Subsystem weist keinen Standardspeicherort für Protokolldateien zu. Wenn der in der Überwachungskonfiguration angegebene Protokollverzeichnis-Pfad kein gültiger Pfad ist, schlägt die Erstellung der Überwachungskonfiguration mit dem fehl `The specified path "/path" does not exist in the namespace belonging to Vserver "Vserver_name"` Fehler.

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

- Auditing plant die Konsolidierungsaufgabe.

  Nach der Planung dieser Aufgabe wird die Prüfung aktiviert. Die SVM-Überwachungskonfiguration und die Protokolldateien bleiben bei einem Neustart erhalten oder wenn die NFS- oder SMB-Server angehalten oder neu gestartet werden.

Konsolidierung von Ereignisprotokolls

Die Protokollkonsolidierung ist eine geplante Aufgabe, die auf routinemäßiger Basis ausgeführt wird, bis die Prüfung deaktiviert ist. Bei deaktiviertem Auditing überprüft der Konsolidierungsauftrag, ob alle übrigen Protokolle konsolidiert werden.

Garantierte Audits

Standardmäßig ist Auditing garantiert. ONTAP garantiert, dass alle prüffähigen Dateizugriffsereignisse (wie durch konfigurierte Audit-Policy-ACLs festgelegt) aufgezeichnet werden, selbst wenn ein Knoten nicht verfügbar ist. Ein angeforderter Dateivorgang kann erst abgeschlossen werden, wenn der Prüfdatensatz für diesen Vorgang im Staging-Volume auf einem persistenten Speicher gespeichert wird. Wenn Audit-Datensätze nicht auf der Festplatte in den Staging-Dateien gespeichert werden können, entweder aufgrund von mangelhaftdem Speicherplatz oder aufgrund anderer Probleme, werden Client-Vorgänge verweigert.

Ein Administrator oder Account-Benutzer mit Zugriff auf die Berechtigungsebene kann die Dateiauditprotokollierung mithilfe des NetApp Manageability SDK oder REST-APIs umgehen. Sie können ermitteln, ob Dateiaktionen mit NetApp Manageability SDK oder REST-APIs ausgeführt wurden, indem Sie die in den gespeicherten Befehlsprotokollen überprüfen `audit.log` Datei:

Weitere Informationen zu Audit-Protokollen zum Befehlsprotokoll finden Sie im Abschnitt „Managen der Audit-Protokollierung für Verwaltungsaktivitäten“ in "Systemadministration".

Konsolidierungsprozess, wenn ein Node nicht verfügbar ist

Wenn ein Node mit Volumes, die zu einer SVM mit aktivierter Prüfung gehören, nicht verfügbar ist, hängt das Verhalten der Überwachungskonsolidierungsaufgabe davon ab, ob der Storage Failover (SFO)-Partner (oder der HA-Partner im Fall eines Clusters mit zwei Nodes) verfügbar ist:

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

  Wenn ein Knoten nicht erreichbar ist, konsolidiert der Konsolidierungsauftrag die Audit-Datensätze von den anderen verfügbaren Nodes dieser SVM. Um festzustellen, dass er nicht vollständig ist, fügt die Aufgabe das Suffix hinzu `.partial` Zum konsolidierten Dateinamen.

- Nachdem der nicht verfügbare Knoten verfügbar ist, werden die Audit-Datensätze in diesem Knoten zu diesem Zeitpunkt mit den Audit-Datensätzen der anderen Knoten konsolidiert.
- Alle Audit-Datensätze werden erhalten bleiben.

Drehung des Ereignisprotokolls

Audit-Ereignisprotokolldateien werden gedreht, wenn sie eine konfigurierte Größe des Schwellenwertprotokolls oder einen konfigurierten Zeitplan erreichen. Wenn eine Ereignis-Log-Datei gedreht wird, benennt der geplante Konsolidierungsvorgang zunächst die in eine zeitgestempelte Archivdatei konvertierte aktive Datei und erstellt dann eine neue aktive, konvertierte Ereignis-Log-Datei.

Prozess bei deaktiviertem Auditing auf der SVM

Wenn die Prüfung auf der SVM deaktiviert ist, wird die Konsolidierungsaufgabe ein letztes Mal ausgelöst. Alle ausstehenden, aufgezeichneten Audit-Datensätze werden in einem vom Benutzer lesbaren Format protokolliert. Vorhandene Ereignisprotokolle, die im Verzeichnis für das Ereignisprotokoll gespeichert sind, werden nicht gelöscht, wenn die Prüfung auf der SVM deaktiviert ist und zur Anzeige zur Verfügung stehen.

Nachdem alle bestehenden Staging-Dateien für diese SVM konsolidiert wurden, wird die Aufgabe der Konsolidierung aus dem Zeitplan entfernt. Durch Deaktivieren der Überwachungskonfiguration für die SVM wird die Überwachungskonfiguration nicht entfernt. Ein Storage-Administrator kann das Auditing jederzeit neu aktivieren.

Der beim Auditing erstellte Konsolidierungsauftrag überwacht die Konsolidierungsaufgabe und erstellt sie neu, wenn die Konsolidierungsaufgabe aufgrund eines Fehlers beendet wird. Bisher konnten Benutzer den Überwachungskonsolidierungsauftrag mithilfe von Job-Manager-Befehlen wie löschen `job delete`. Benutzer dürfen den Konsolidierungsauftrag für Audits nicht mehr löschen.