Funktionsweise von Audits

ONTAP 9

NetApp
September 09, 2026

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

Inhalt

Funktionsweise von Audits . . . 1
- Die grundlegenden ONTAP Audit-Konzepte . . . 1
- Informationen zur Funktionsweise des ONTAP-Auditprozesses . . . 1
  - Prozess, wenn die Protokollierung auf einer SVM aktiviert ist . . . 2
  - Zusammenführung der Ereignisprotokolle . . . 2
  - Garantierte Prüfung . . . 2
  - Konsolidierungsprozess, wenn ein Node nicht verfügbar ist . . . 3
  - Ereignisprotokollrotation . . . 3
  - Prozess, wenn die Protokollierung auf der SVM deaktiviert ist . . . 3

Funktionsweise von Audits

Die grundlegenden ONTAP Audit-Konzepte

Für das Verständnis der Prüfung in ONTAP ist es hilfreich, einige grundlegende Prüfungskonzepte zu kennen.

- **Staging-Dateien**

  Die temporären Binärdateien auf den einzelnen Knoten, in denen die Revisionsprotokolle vor der Konsolidierung und Konvertierung gespeichert werden. Staging-Dateien befinden sich in Staging-Volumes.

- **Staging-Volume**

  Ein dediziertes Volume, das von ONTAP zum Speichern von Staging-Dateien erstellt wird. Pro Aggregat existiert ein Staging-Volume. Alle für die Revisionsprotokollierung aktivierten Storage Virtual Machines (SVMs) nutzen gemeinsam ein Staging-Volume, um Revisionsprotokolle des Dateizugriffs für die Datenvolumes des jeweiligen Aggregats zu speichern. Die Revisionsprotokolle jeder SVM werden in einem separaten Verzeichnis innerhalb des Staging-Volumes gespeichert.

  Clusteradministratoren können Informationen über Staging-Volumes einsehen, aber die meisten anderen Volume-Operationen sind nicht zulässig. Nur ONTAP kann Staging-Volumes erstellen. ONTAP weist Staging-Volumes automatisch einen Namen zu. Alle Staging-Volume-Namen beginnen mit `MDV_aud_` gefolgt von der UUID des Aggregats, das dieses Staging-Volume enthält (zum Beispiel: `MDV_aud_1d0131843d4811e296fc123478563412`).

- **System-Volumes**

  Ein FlexVol volume, das spezielle Metadaten enthält, wie beispielsweise Metadaten für Revisionsprotokolle von Dateidiensten. Die Admin-SVM besitzt Systemvolumes, die im gesamten Cluster sichtbar sind. Staging-Volumes sind eine Art von Systemvolume.

- **Konsolidierungsaufgabe**

  Eine Aufgabe, die erstellt wird, wenn die Überwachung aktiviert ist. Diese lang laufende Aufgabe auf jedem SVM übernimmt die Überwachungsdatensätze aus den Staging-Dateien der Mitgliedsknoten des SVM. Diese Aufgabe führt die Überwachungsdatensätze in chronologisch sortierter Reihenfolge zusammen und konvertiert sie dann in ein benutzerlesbares Ereignisprotokollformat, das in der Überwachungskonfiguration festgelegt ist – entweder das EVTX- oder das XML-Dateiformat. Die konvertierten Ereignisprotokolle werden im Verzeichnis für Überwachungsereignisprotokolle gespeichert, das in der SVM-Überwachungskonfiguration angegeben ist.

Informationen zur Funktionsweise des ONTAP-Auditprozesses

Der ONTAP Auditing-Prozess unterscheidet sich vom Microsoft Auditing-Prozess. Vor der Konfiguration des Auditing empfiehlt es sich, die Funktionsweise des ONTAP Auditing-Prozesses zu verstehen.

Audit-Protokolle werden zunächst in binären Staging-Dateien auf den einzelnen Nodes gespeichert. Wenn die Auditierung für eine SVM aktiviert ist, verwaltet jeder Mitgliedsnode Staging-Dateien für diese SVM. Periodisch

werden sie konsolidiert und in benutzerlesbare Ereignisprotokolle umgewandelt, die im Verzeichnis für Revisionsprotokolle des SVM gespeichert werden.

Prozess, wenn die Protokollierung auf einer SVM aktiviert ist

Auditing kann nur auf SVMs aktiviert werden. Wenn der Storage-Administrator Auditing auf der SVM aktiviert, prüft das Auditing-Subsystem, ob Staging-Volumes vorhanden sind. Für jedes Aggregat, das Daten-Volumes enthält, die der SVM gehören, muss ein Staging-Volume existieren. Das Auditing-Subsystem erstellt alle benötigten Staging-Volumes, falls diese nicht vorhanden sind.

Das Überwachungssubsystem führt außerdem weitere vorbereitende Aufgaben aus, bevor die Überwachung aktiviert wird:

- Das Überwachungssubsystem überprüft, ob der Pfad zum Protokollverzeichnis verfügbar ist und keine Symlinks enthält.

  Das Protokollverzeichnis muss bereits als Pfad im Namespace der SVM vorhanden sein. Es wird empfohlen, ein neues Volume oder einen neuen Qtree für die Revisionsprotokolldateien zu erstellen. Das Auditing-Subsystem weist keinen Standardspeicherort für Protokolldateien zu. Wenn der in der Auditing-Konfiguration angegebene Protokollverzeichnispfad kein gültiger Pfad ist, schlägt die Erstellung der Auditing-Konfiguration mit dem `The specified path "/path" does not exist in the namespace belonging to Vserver "Vserver_name"` Fehler fehl.

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

- Die Protokollierung plant die Konsolidierungsaufgabe.

  Nachdem diese Aufgabe eingeplant wurde, ist die Überwachung aktiviert. Die SVM-Überwachungskonfiguration und die Protokolldateien bleiben auch nach einem Neustart oder wenn die NFS- oder SMB-Server gestoppt oder neu gestartet werden, erhalten.

Zusammenführung der Ereignisprotokolle

Die Protokollkonsolidierung ist eine geplante Aufgabe, die regelmäßig ausgeführt wird, bis die Überwachung deaktiviert ist. Wenn die Überwachung deaktiviert ist, überprüft die Konsolidierungsaufgabe, ob alle verbleibenden Protokolle konsolidiert sind.

Garantierte Prüfung

Standardmäßig ist die Protokollierung gewährleistet. ONTAP garantiert, dass alle protokollierbaren Dateizugriffsereignisse (wie durch die konfigurierte Zugriffssteuerungsliste festgelegt) aufgezeichnet werden, selbst wenn ein Node nicht verfügbar ist. Ein angeforderter Dateivorgang kann erst abgeschlossen werden, wenn der Protokolleintrag für diesen Vorgang im Staging-Volume auf dem persistenten Speicher gespeichert wurde. Können Protokolleinträge nicht in den Staging-Dateien auf der Festplatte gespeichert werden, entweder aufgrund von unzureichendem Speicherplatz oder anderen Problemen, werden Clientvorgänge abgelehnt.

> Ein Administrator oder ein Benutzer mit privilegiertem Zugriff kann die Protokollierung von Dateizugriffen umgehen, indem NetApp Manageability SDK oder REST-APIs verwendet werden. Ob Dateizugriffe mithilfe von NetApp Manageability SDK oder REST-APIs erfolgt sind, lässt sich durch Überprüfung der in der `audit.log` Datei gespeicherten Befehlshistorie feststellen.
>
> Weitere Informationen zu Revisionsprotokollen des Befehlsverlaufs finden sich im Abschnitt „Protokollierung verwalten für Managementaktivitäten“ in "Systemadministration".

Konsolidierungsprozess, wenn ein Node nicht verfügbar ist

Wenn ein Knoten, der Volumes enthält, die zu einer SVM mit aktivierter Überwachung gehören, nicht verfügbar ist, hängt das Verhalten der Überwachungskonsolidierungsaufgabe davon ab, ob der Storage-Failover-Partner (SFO-Partner) des Knotens (oder der HA-Partner im Falle eines Zwei-Node-Cluster) verfügbar ist:

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

  Wenn ein Knoten nicht erreichbar ist, konsolidiert der Konsolidierungsvorgang die Revisionsprotokolle der anderen verfügbaren Knoten dieser SVM. Zur Kennzeichnung, dass die Konsolidierung nicht abgeschlossen ist, fügt der Vorgang dem Dateinamen der konsolidierten Datei das Suffix `.partial` hinzu.

- Sobald der nicht verfügbare Knoten wieder verfügbar ist, werden die Revisionsprotokolle dieses Knotens mit den Revisionsprotokollen der anderen Knoten zu diesem Zeitpunkt zusammengeführt.
- Alle Revisionsprotokolle werden aufbewahrt.

Ereignisprotokollrotation

Die Revisionsprotokolldateien werden rotiert, wenn sie eine konfigurierte Schwellenwertgröße erreichen oder nach einem festgelegten Zeitplan. Wenn eine Revisionsprotokolldatei rotiert wird, benennt der geplante Konsolidierungsvorgang zunächst die aktive konvertierte Datei in eine mit einem Zeitstempel versehene Archivdatei um und erstellt anschließend eine neue aktive konvertierte Revisionsprotokolldatei.

Prozess, wenn die Protokollierung auf der SVM deaktiviert ist

Wenn die Überwachung auf der SVM deaktiviert ist, wird die Konsolidierungsaufgabe ein letztes Mal ausgeführt. Alle ausstehenden, aufgezeichneten Revisionsprotokolle werden in einem für Benutzer lesbaren Format protokolliert. Vorhandene Ereignisprotokolle im Ereignisprotokollverzeichnis werden bei Deaktivierung der Überwachung auf der SVM nicht gelöscht und stehen weiterhin zur Ansicht zur Verfügung.

Nachdem alle vorhandenen Staging-Dateien für diese SVM konsolidiert wurden, wird die Konsolidierungsaufgabe aus dem Zeitplan entfernt. Das Deaktivieren der Auditing-Konfiguration für die SVM entfernt die Auditing-Konfiguration nicht. Ein Storage-Administrator kann die Auditing-Funktion jederzeit wieder aktivieren.

Der Auditing-Konsolidierungsauftrag, der bei aktivierter Auditing-Funktion erstellt wird, überwacht die Konsolidierungsaufgabe und erstellt sie neu, falls die Konsolidierungsaufgabe aufgrund eines Fehlers beendet wird. Benutzer können den Auditing-Konsolidierungsauftrag nicht löschen.

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.