Revisionsprotokollierung

ONTAP 9

NetApp
September 09, 2026

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

Inhalt

Revisionsprotokollierung . . . 1
- Informationen zur Implementierung der ONTAP Revisionsprotokollierung . . . 1
- Informationen zu Änderungen an der ONTAP Protokollierung . . . 2
- Anzeigen des Inhalts des ONTAP Revisionsprotokolls . . . 2
- Einstellungen für ONTAP Revisionsprotokoll-GET-Anfragen verwalten . . . 4
- ONTAP Cluster-übergreifende Audits aktivieren . . . 4
  - Clusterübergreifende Protokollierung aktivieren oder deaktivieren . . . 5
  - Auswirkungen der Aktivierung der GET-Überwachung . . . 5
- ONTAP Revisionsprotokollziele verwalten . . . 5

Revisionsprotokollierung

Informationen zur Implementierung der ONTAP Revisionsprotokollierung

Managementaktivitäten, die im Revisionsprotokoll erfasst werden, sind in Standard-AutoSupport-Berichten enthalten, und bestimmte Protokollierungsaktivitäten sind in EMS-Meldungen enthalten. Das Revisionsprotokoll kann auch an von Ihnen festgelegte Ziele weitergeleitet werden, und Revisionsprotokolldateien lassen sich über die ONTAP CLI oder einen Webbrowser anzeigen.

Ab ONTAP 9.11.1 lässt sich der Inhalt des Revisionsprotokolls mit System Manager anzeigen.

Ab ONTAP 9.12.1 stellt ONTAP Manipulationswarnungen für Revisionsprotokolle bereit. ONTAP führt täglich einen Hintergrundprozess aus, um Manipulationen an audit.log-Dateien zu überprüfen und sendet eine EMS-Warnung, wenn veränderte oder manipulierte Protokolldateien gefunden werden.

Beginnend mit ONTAP 9.17.1 und mit ONTAP 9.16.1 P4 sowie späteren Patch-Releases der Version 9.16.1 "Auch Fernverwaltungsaktivitäten, die von einem verbundenen Cluster mittels clusterübergreifender Operationen initiiert werden, können protokolliert werden.". Diese Aktivitäten umfassen benutzergesteuerte und interne Vorgänge, die von einem anderen Cluster ausgehen.

In ONTAP protokollierte Managementaktivitäten

ONTAP protokolliert Managementaktivitäten, die auf einem Cluster durchgeführt werden, wie zum Beispiel welche Anfrage gestellt wurde, welcher Benutzer die Anfrage ausgelöst hat, welche Zugriffsmethode der Benutzer verwendet hat und zu welchem Zeitpunkt die Anfrage gestellt wurde.

Managementaktivitäten können zu einer der folgenden Typen gehören:

- **SET-Anfragen**:
  - Diese Anfragen beziehen sich typischerweise auf Befehle oder Operationen ohne Anzeige.
  - Diese Anfragen werden beispielsweise gestellt, wenn Sie einen `create`, `modify` oder `delete`-Befehl ausführen.
  - SET-Anfragen werden standardmäßig protokolliert.
- **GET-Anfragen**:
  - Diese Anfragen rufen Informationen ab und zeigen sie in der Managementoberfläche an.
  - Diese Anfragen werden gestellt, wenn Sie beispielsweise einen `show` Befehl ausführen.
  - GET-Anfragen werden standardmäßig nicht protokolliert, aber es kann gesteuert werden, ob GET-Anfragen, die von der ONTAP CLI (`-cliget`), von der ONTAP API (`-ontapiget`) oder von der ONTAP REST API (`-httpget`) gesendet werden, in der Datei protokolliert werden.

Aufzeichnung und Rotation des Revisionsprotokolls

ONTAP protokolliert Verwaltungsaktivitäten in der `/mroot/etc/log/mlog/audit.log` Datei eines Knotens. Befehle aus den drei Shells für CLI-Befehle: der Clustershell, der Nodeshell und der nicht-interaktiven Systemshell sowie API-Befehle werden hier protokolliert. Interaktive Systemshell-Befehle werden nicht protokolliert. Revisionsprotokolle enthalten Zeitstempel, die anzeigen, ob alle Knoten in einem Cluster synchronisiert sind.

Die `audit.log` Datei wird vom AutoSupport Tool an die angegebenen Empfänger gesendet. Der Inhalt kann auch sicher an von Ihnen festgelegte externe Ziele weitergeleitet werden, beispielsweise an einen Splunk oder einen syslog Server.

Die `audit.log` Datei wird täglich rotiert. Die Rotation erfolgt auch, wenn sie 100 MB groß ist, und die vorherigen 48 Kopien bleiben erhalten (mit maximal insgesamt 49 Dateien). Wenn die Revisionsdatei ihre tägliche Rotation durchführt, wird keine EMS-Meldung generiert. Wenn die Revisionsdatei rotiert wird, weil die Dateigrößenbeschränkung überschritten wird, wird eine EMS-Meldung generiert.

Beim Aktivieren der GET-Überwachung empfiehlt es sich, die Protokollweiterleitung zu konfigurieren, um Datenverlust durch schnelle Protokollrotation zu vermeiden. Weitere Informationen enthält der folgende Knowledge Base Artikel: "Aktivieren der Weiterleitung des Revisionsprotokolls".

Informationen zu Änderungen an der ONTAP Protokollierung

Ab ONTAP 9 wird die `command-history.log` Datei durch `audit.log` ersetzt, und die `mgwd.log` Datei enthält keine Audit-Informationen mehr. Bei einem Upgrade auf ONTAP 9 empfiehlt sich eine Überprüfung aller Skripte und Tools, die auf die alten Dateien und deren Inhalte verweisen.

Nach dem Upgrade auf ONTAP 9 werden bestehende `command-history.log` Dateien beibehalten. Sie werden entfernt (gelöscht), wenn neue `audit.log` Dateien hinzugefügt (erstellt) werden.

Tools und Skripte, die die `command-history.log` Datei überprüfen, könnten weiterhin funktionieren, da beim Upgrade ein Softlink von `command-history.log` zu `audit.log` erstellt wird. Allerdings schlagen Tools und Skripte, die die `mgwd.log` Datei überprüfen, fehl, da diese Datei keine Audit-Informationen mehr enthält.

Darüber hinaus enthalten die Audit-Logs in ONTAP 9 und späteren Versionen die folgenden Einträge nicht mehr, da diese als nicht nützlich erachtet werden und unnötige Protokollierung verursachen:

- Interne Befehle, die von ONTAP ausgeführt werden (d. h. wenn Benutzername=root)
- Befehlsaliase (getrennt von dem Befehl, auf den sie verweisen)

Ab ONTAP 9 ist es möglich, die Audit-Logs sicher über die TCP- und TLS-Protokolle an externe Ziele zu übertragen.

Anzeigen des Inhalts des ONTAP Revisionsprotokolls

Sie können den Inhalt der `/mroot/etc/log/mlog/audit.log`Clusterdateien mithilfe der ONTAP CLI, des System Manager oder eines Webbrowsers anzeigen.

Die Logdateieinträge des Clusters umfassen Folgendes:

Zeit

Der Zeitstempel des Logeintrags.

Anwendung

Die Anwendung, die zur Verbindung mit dem Cluster verwendet wird. Beispiele für mögliche Werte sind `internal`, `console`, `ssh`, `http`, `ontapi`, `snmp`, `rsh`, `telnet` und `service-processor`.

Benutzer

Der Benutzername des Remote-Benutzers.

Status

Der aktuelle Status der Prüfungsanfrage, der `success`, `pending` oder `error` sein könnte.

Nachricht

Ein optionales Feld, das Fehlermeldungen oder zusätzliche Informationen zum Status eines Befehls enthalten kann.

Session ID

Die Session ID, unter der die Anfrage empfangen wird. Jeder SSH-Session wird eine Session ID zugewiesen, während jeder HTTP-, ONTAPI- oder SNMP-Request eine eindeutige Session ID zugewiesen wird.

Speicher-VM

Die SVM, über die der Benutzer verbunden ist.

Umfang

Zeigt `svm` an, wenn die Anfrage auf einer Data Storage-VM erfolgt, andernfalls wird `cluster` angezeigt.

Befehls-ID

Die ID jedes in einer CLI-Sitzung empfangenen Befehls. Dies ermöglicht die Zuordnung von Anfrage und Antwort. ZAPI, HTTP und SNMP-Anfragen verfügen nicht über Befehls-IDs.

Die Protokolleinträge des Clusters lassen sich über die ONTAP CLI, einen Webbrowser und ab ONTAP 9.11.1 auch über den System Manager anzeigen.

System Manager

- Zur Anzeige des Bestands wird **Events & Jobs > Revisionsprotokolle** ausgewählt. Jede Spalte verfügt über Steuerelemente zum Filtern, Sortieren, Suchen, Anzeigen und für Bestandskategorien. Die Bestandsdetails können als Excel-Arbeitsmappe heruntergeladen werden.
- Um Filter festzulegen, auf die Schaltfläche **Filter** oben rechts klicken und anschließend die gewünschten Felder auswählen. + Es besteht außerdem die Möglichkeit, alle Befehle anzuzeigen, die in der Session ausgeführt wurden, in der ein Fehler aufgetreten ist, indem auf den Session ID Link geklickt wird.

CLI

Um zusammengeführte Revisionsprotokolleinträge von mehreren Knoten im Cluster anzuzeigen, Folgendes eingeben:
`security audit log show <[parameters]>`

Der `security audit log show`Befehl kann verwendet werden, um Revisionsprotokoll-Einträge für einzelne Knoten oder zusammengeführt von mehreren Knoten im Cluster anzuzeigen. Der Inhalt des `/mroot/etc/log/mlog`Verzeichnisses auf einem einzelnen Knoten kann auch mit einem Webbrowser angezeigt werden. Weitere Informationen zu `security audit log show` finden sich in der "ONTAP-Befehlsreferenz".

Webbrowser

Der Inhalt des `/mroot/etc/log/mlog`-Verzeichnisses auf einem einzelnen Knoten lässt sich mit einem Webbrowser anzeigen. "Informationen darüber, wie auf die Protokoll-, Core-Dump- und MIB-Dateien eines Knotens mithilfe eines Webbrowsers zugegriffen werden kann".

Einstellungen für ONTAP Revisionsprotokoll-GET-Anfragen verwalten

SET-Anfragen werden standardmäßig protokolliert und können nicht deaktiviert werden, GET-Anfragen hingegen nicht. Sie können jedoch steuern, ob GET-Anfragen, die von ONTAP HTML (`-httpget`), der ONTAP CLI (`-cliget`) oder von den ONTAP APIs (`-ontapiget`) gesendet werden, in der Datei protokolliert werden.

Die Einstellungen für die Revisionsprotokollierung können über die ONTAP CLI und ab ONTAP 9.11.1 auch über den System Manager geändert werden.

System Manager

1. **Events & Jobs > Revisionsprotokolle** auswählen.
2. Oben rechts auf klicken und anschließend die Anfragen zum Hinzufügen oder Entfernen auswählen.

CLI

- Um anzugeben, dass GET-Anfragen von der ONTAP CLI oder den APIs zusätzlich zu den standardmäßig festgelegten Anfragen im Revisionsprotokoll (der Datei audit.log) protokolliert werden, Folgendes eingeben:
  `security audit modify [-cliget {on|off}][-httpget {on|off}][-ontapiget {on|off}]`
- Um die aktuellen Einstellungen anzuzeigen, folgenden Befehl eingeben:
  `security audit show`

Weitere Informationen zu `security audit show` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Cluster-übergreifende Audits aktivieren

Ab ONTAP 9.17.1 sowie ab ONTAP 9.16.1 P4 und späteren Patch-Releases der Version 9.16.1 kann in ONTAP die clusterübergreifende Revisionsprotokollierung aktiviert werden, um Vorgänge zu protokollieren, die von einem verbundenen Cluster initiiert werden. Diese Remote-Revisionsprotokollierung ist besonders in Umgebungen wertvoll, in denen mehrere ONTAP Cluster miteinander interagieren, da sie die Nachvollziehbarkeit und Verantwortlichkeit von Remote-Aktionen ermöglicht.

Die clusterübergreifende Überwachung kann zwischen benutzerinitiierten GET- (Lese-) oder SET-Operationen (Erstellen/Ändern/Löschen) unterscheiden. Standardmäßig werden nur benutzerinitiierte SET-Operationen auf den Zielclustern überwacht. Jede Anfrage, die Daten liest, wie eine GET- oder `show`-Anfrage in der Befehlszeile, wird standardmäßig nicht überwacht, unabhängig davon, ob die Anfrage clusterübergreifend ist.

Bevor Sie beginnen

- Sie müssen über `advanced`-Berechtigungen verfügen
- Der Cluster muss mit einem anderen Cluster per Peering verbunden sein, und auf beiden Clustern muss ONTAP 9.16.1 P4 oder höher ausgeführt werden.

> In Umgebungen, in denen einige, aber nicht alle Knoten auf ONTAP 9.16.1 P4 oder höher aktualisiert wurden, erfolgt die Revisionsprotokollierung nur auf Knoten, auf denen die aktualisierte Version ausgeführt wird. Es wird empfohlen, alle Knoten auf eine unterstützte Version zu aktualisieren, um ein einheitliches Revisionsprotokollierungsverhalten zu gewährleisten.

Clusterübergreifende Protokollierung aktivieren oder deaktivieren

Schritte

1. Die clusterübergreifende Protokollierung auf dem Cluster kann aktiviert oder deaktiviert werden, indem der `cluster-peer` Parameter auf `on` oder `off` gesetzt wird:

```
security audit modify -cluster-peer {on|off}
```

2. Bestätigen Sie anhand des aktuellen Revisionsprotokoll-Status, ob die Cluster-Peer-Einstellung aktiviert oder deaktiviert ist:

```
security audit show
```

Antwort:

```
    Audit Setting State
    ------------- -----
         CLI GET: off
        HTTP GET: off
      ONTAPI GET: off
    Cluster Peer: on
```

Auswirkungen der Aktivierung der GET-Überwachung

Ab ONTAP 9.17.1, wenn Sie "CLI-, HTTP- und ONTAPI-GET-Revisionsprotokollierung aktivieren" auf einem Peering-Cluster aktivieren, wird auch die Protokollierung von clusterübergreifenden, benutzerinitiierten GET-Anfragen ermöglicht. In früheren ONTAP Versionen galt die GET-Protokollierung nur für Anfragen auf einem lokalen Cluster. Mit ONTAP 9.17.1, wenn die GET-Protokollierung mit der Option `cluster-peer` auf `on` aktiviert wird, werden sowohl lokale als auch clusterübergreifende Anfragen protokolliert.

ONTAP Revisionsprotokollziele verwalten

Sie können das Revisionsprotokoll an maximal 10 Ziele weiterleiten. Beispielsweise kann das Log zu Überwachungs-, Analyse- oder Sicherungszwecken an einen Splunk oder

syslog Server weitergeleitet werden.

Über diese Aufgabe

Um die Weiterleitung zu konfigurieren, sind die IP-Adresse des Syslog- oder Splunk-Hosts, dessen Portnummer, ein Übertragungsprotokoll und die Syslog-Einrichtung anzugeben, die für die weitergeleiteten Protokolle verwendet wird "Informationen zu Syslog-Facilities".

Es kann einer der folgenden Übertragungswerte mit dem `-protocol` Parameter ausgewählt werden:

UDP unverschlüsselt
: Benutzerdatagrammprotokoll ohne Sicherheit (Standard)

TCP unverschlüsselt
: Transmission Control Protocol ohne Sicherheit

TCP verschlüsselt
: Transmission Control Protocol mit Transport Layer Security (TLS) + Eine Option **Verify server** ist verfügbar, wenn das TCP Encrypted-Protokoll ausgewählt ist.

Der Standardport ist 514 für UDP und 6514 für TCP, aber Sie können jeden beliebigen Port festlegen, der den Anforderungen Ihres Netzwerks entspricht.

Sie können mit dem `-message-format` Befehl eines der folgenden Nachrichtenformate auswählen:

legacy-netapp
: Eine Variante des RFC-3164 Syslog-Formats (Format: <PRIVAL>TIMESTAMP HOSTNAME: MSG)

rfc-5424
: Syslog-Format gemäß RFC-5424 (Format: <PRIVAL>VERSION TIMESTAMP HOSTNAME: MSG)

Sie können Revisionsprotokolle von der ONTAP CLI und ab ONTAP 9.11.1 auch vom System Manager weiterleiten.

System Manager

- Zur Anzeige der Ziele des Revisionsprotokolls **Cluster > Einstellungen** auswählen. + Die Anzahl der Protokollziele wird in der **Kachel Benachrichtigungsverwaltung** angezeigt. ⋮ auswählen, um Details anzuzeigen.
- Um Revisionsprotokollziele hinzuzufügen, zu ändern oder zu löschen, **Ereignisse & Aufträge > Revisionsprotokolle** auswählen und dann oben rechts auf **Revisionsprotokollziele verwalten** klicken. + + Add anklicken oder ⋮ in der Spalte **Hostadresse**, um Einträge zu bearbeiten oder zu löschen.

CLI

1. Für jedes Ziel, an das das Revisionsprotokoll weitergeleitet werden soll, sind die Ziel-IP-Adresse oder der Hostname sowie alle Sicherheitsoptionen anzugeben.

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user
```

```
cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 6514 -protocol tcp-encrypted -facility user
```

- Wenn der `cluster log-forwarding create`Befehl den Zielhost nicht anpingen kann, um die Konnektivität zu überprüfen, schlägt der Befehl mit einem Fehler fehl. Obwohl dies nicht empfohlen wird, umgeht die Verwendung des `-force`Parameters mit dem Befehl die Überprüfung der Konnektivität.
- Wenn Sie den Parameter `-verify-server` auf `true` festlegen, wird die Identität des Ziels für die Protokollweiterleitung durch die Validierung seines Zertifikats überprüft. Sie können den Wert nur dann auf `true` festlegen, wenn Sie den Wert `tcp-encrypted` im Feld `-protocol` auswählen.

2. Es kann mithilfe des `cluster log-forwarding show` Befehls überprüft werden, ob die Zieldatensätze korrekt sind.

```
cluster1::> cluster log-forwarding show

                                                 Verify Syslog
Destination Host          Port   Protocol        Server Facility
------------------------- ------ --------        ------ --------
192.168.123.96            514    udp-unencrypted false  user
192.168.123.98            6514   tcp-encrypted   true   user
2 entries were displayed.
```

Verwandte Informationen

- "Cluster Log-Forwarding anzeigen"
- "cluster log-forwarding create"

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.