Audit-Protokollierung

ONTAP 9

NetApp
January 08, 2026

Inhalt

Audit-Protokollierung

Erfahren Sie mehr über die Implementierung von ONTAP Audit-Protokollierung

Die im Audit-Protokoll aufgezeichneten Verwaltungsaktivitäten sind in den Standardberichten von AutoSupport enthalten, und bestimmte Protokollierungsaktivitäten sind in EMS-Nachrichten enthalten. Sie können das Audit-Protokoll auch an von Ihnen angegebene Ziele weiterleiten und Audit-Protokolldateien über die ONTAP -CLI oder einen Webbrowser anzeigen.

Ab ONTAP 9.11.1 können Sie den Inhalt des Revisionsprotokolls mithilfe von System Manager anzeigen.

Ab ONTAP 9.12.1 bietet ONTAP Manipulationswarnungen für Prüfprotokolle. ONTAP führt einen täglichen Hintergrundjob aus, um auf Manipulation von audit.log Dateien zu überprüfen und sendet eine EMS-Warnung, wenn Protokolldateien gefunden werden, die geändert oder manipuliert wurden.

Beginnend mit ONTAP 9.17.1 und mit ONTAP 9.16.1 P4 und späteren 9.16.1 Patch-Releases, "Remote-Verwaltungsaktivitäten, die von einem Peering-Cluster mithilfe von Cluster-übergreifenden Operationen initiiert werden, können ebenfalls protokolliert werden" . Diese Aktivitäten umfassen benutzergesteuerte und interne Vorgänge, die aus einem anderen Cluster stammen.

In ONTAP protokollierte Verwaltungsaktivitäten

ONTAP protokolliert Verwaltungsaktivitäten, die auf einem Cluster ausgeführt werden, z. B. welche Anfrage gestellt wurde, welcher Benutzer die Anfrage ausgelöst hat, die Zugriffsmethode des Benutzers und den Zeitpunkt der Anfrage.

Es gibt folgende Arten von Managementaktivitäten:

- **SET-Anfragen**:
  - Diese Anforderungen beziehen sich normalerweise auf Befehle oder Vorgänge, die keine Anzeigevorgänge sind.
  - Diese Anforderungen werden ausgegeben, wenn Sie `create` `modify` `delete` beispielsweise einen, , oder -Befehl ausführen.
  - SET-Anfragen werden standardmäßig protokolliert.
- **GET-Anfragen**:
  - Diese Anfragen rufen Informationen ab und zeigen sie in der Verwaltungsschnittstelle an.
  - Diese Anforderungen werden ausgegeben, wenn Sie `show` beispielsweise einen Befehl ausführen.
  - GET-Anfragen werden standardmäßig nicht protokolliert, Sie können jedoch steuern, ob GET-Anfragen, die von der ONTAP CLI gesendet werden, (`-cliget`), aus der ONTAP API (`-ontapiget`) oder über die ONTAP REST API (`-httpget`) werden in der Datei protokolliert.

Aufzeichnung und Rotation von Überwachungsprotokollen

ONTAP Records Management-Aktivitäten in der `/mroot/etc/log/mlog/audit.log` Datei eines Knotens. Befehle der drei Shells für CLI-Befehle (Cluster-Shell, Nodeshell und nicht-interaktive Systemshell) sowie API-Befehle werden hier protokolliert. Interaktive Systemshell-Befehle werden nicht protokolliert. Audit-Protokolle enthalten Zeitstempel, um zu zeigen, ob alle Knoten in einem Cluster synchronisiert sind.

Die `audit.log` Datei wird vom AutoSupport-Tool an die angegebenen Empfänger gesendet. Sie können den Inhalt auch sicher an angegebene externe Ziele weiterleiten, z. B. an einen Splunk oder Syslog-Server.

Die `audit.log` Datei wird täglich gedreht. Die Rotation tritt auch auf, wenn sie 100 MB groß erreicht, und die vorherigen 48 Kopien erhalten bleiben (mit maximal 49 Dateien). Wenn die Audit-Datei ihre tägliche Rotation durchführt, wird keine EMS-Nachricht erzeugt. Wenn die Überwachungsdatei sich dreht, weil ihre Dateigröße überschritten wird, wird eine EMS-Nachricht generiert.

Wenn Sie die GET-Überwachung aktivieren, sollten Sie die Protokollweiterleitung konfigurieren, um Datenverluste durch schnelle Protokollrotation zu vermeiden. Weitere Informationen finden Sie im folgenden Knowledge Base-Artikel: "Aktivieren der Weiterleitung von Überwachungsprotokollen" .

Erfahren Sie mehr über Änderungen an der ONTAP-Audit-Protokollierung

Beginnend mit ONTAP 9 `command-history.log` wird die Datei durch `audit.log`, ersetzt und die `mgwd.log` Datei enthält keine Audit-Informationen mehr. Wenn Sie ein Upgrade auf ONTAP 9 durchführen, sollten Sie alle Skripte oder Tools lesen, die sich auf die vorhandenen Dateien und deren Inhalte beziehen.

Nach dem Upgrade auf ONTAP 9 `command-history.log` bleiben vorhandene Dateien erhalten. Sie werden gedreht (gelöscht), wenn neue `audit.log` Dateien in gedreht (erstellt) werden.

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

Darüber hinaus enthalten Audit-Protokolle in ONTAP 9 und höher nicht mehr die folgenden Einträge, da sie nicht als nützlich betrachtet werden und unnötige Protokollierungsaktivitäten verursachen:

- Interne Befehle, die von ONTAP ausgeführt werden (d. h., Benutzername=Root)
- Befehlsaliasen (getrennt vom Befehl, auf den sie verweisen)

Ab ONTAP 9 können Sie die Prüfprotokolle sicher mit den Protokollen TCP und TLS an externe Ziele übertragen.

Anzeigen des Inhalts des ONTAP-Überwachungsprotokolls

Sie können den Inhalt der Cluster- `/mroot/etc/log/mlog/audit.log`Dateien mit der ONTAP CLI, mit System Manager oder mit einem Webbrowser anzeigen.

Die Protokolldateieinträge des Clusters umfassen Folgendes:

Zeit
: Zeitstempel der Protokolleingabe.

Applikation
: Die Anwendung, die zum Herstellen einer Verbindung zum 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 Prüfungsanforderung, der sein könnte `success`, , `pending` oder `error`.

Nachricht

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

Sitzungs-ID

Die Sitzungs-ID, für die die Anforderung eingeht. Jeder SSH_Session_ wird eine Session-ID zugewiesen, während jedem HTTP, ONTAPI oder SNMP *Request* eine eindeutige Session-ID zugewiesen wird.

Storage-VM

Der SVM, über die der Benutzer verbunden ist.

Umfang

Zeigt an `svm`, wenn sich die Anforderung auf einer Datenspeicher-VM befindet; andernfalls wird angezeigt `cluster`.

Command ID

Die ID für jeden Befehl, der in einer CLI-Sitzung empfangen wurde. So können Sie Anfragen und Antworten korrelieren. ZAPI-, HTTP- und SNMP-Anforderungen verfügen nicht über Befehl-IDs.

Sie können die Protokolleinträge des Clusters aus der ONTAP CLI, aus einem Webbrowser und beginnend mit ONTAP 9.11.1, von System Manager anzeigen.

System Manager

- Um den Bestand anzuzeigen, wählen Sie **Events & Jobs > Audit Logs**. + jede Spalte verfügt über Steuerelemente zum Filtern, Sortieren, Suchen, Anzeigen und Inventar Kategorien. Die Bestandsdetails können als Excel-Arbeitsmappe heruntergeladen werden.
- Um Filter einzustellen, klicken Sie oben rechts auf die Schaltfläche **Filter** und wählen Sie dann die gewünschten Felder aus. + Sie können auch alle Befehle anzeigen, die in der Sitzung ausgeführt wurden, in der ein Fehler aufgetreten ist, indem Sie auf den Link Session-ID klicken.

CLI

Um Überwachungseinträge anzuzeigen, die aus mehreren Knoten im Cluster zusammengeführt wurden, geben Sie Folgendes ein:
`security audit log show <[parameters]>`

Mit dem `security audit log show` Befehl können Sie Überwachungseinträge für einzelne Nodes anzeigen oder aus mehreren Nodes im Cluster zusammengeführt werden. Sie können den Inhalt des `/mroot/etc/log/mlog` Verzeichnisses auch mit einem Webbrowser auf einem einzelnen Knoten anzeigen. Erfahren Sie mehr über `security audit log show` in der "ONTAP-Befehlsreferenz".

Webbrowser

Sie können den Inhalt des `/mroot/etc/log/mlog` Verzeichnisses mit einem Webbrowser auf einem einzelnen Knoten anzeigen. "Hier erfahren Sie, wie Sie mit einem Webbrowser auf die Protokoll-, Core Dump- und MIB-Dateien eines Node zugreifen".

Managen der Einstellungen für ONTAP Audit GET-Anforderungen

Während FESTGELEGTE Anforderungen standardmäßig protokolliert werden, sind GET-Anforderungen nicht. Sie können jedoch steuern, ob GET Requests(`-httpget`, die von ONTAP HTML), der ONTAP-CLI (`-cliget`) oder von den ONTAP-APIs (`-ontapiget`) gesendet werden, in der Datei protokolliert werden.

Sie können die Einstellungen für die Protokollierung von Audits über die ONTAP-CLI ändern, und beginnend mit ONTAP 9.11.1, in System Manager.

System Manager

1. Wählen Sie **Events & Jobs > Audit Logs** Aus.
2. Klicken Sie oben rechts auf , und wählen Sie dann die Anforderungen aus, die Sie hinzufügen oder entfernen möchten.

CLI

- Um festzulegen, dass GET-Anforderungen von der ONTAP-CLI oder -APIs im Audit-Protokoll (der Datei audit.log) aufgezeichnet werden sollen, geben Sie zusätzlich zu den Standardanforderungen für Set Folgendes ein:
  `security audit modify [-cliget {on|off}][-httpget {on|off}][-ontapiget {on|off}]`
- Um die aktuellen Einstellungen anzuzeigen, geben Sie Folgendes ein:
  `security audit show`

Erfahren Sie mehr über `security audit show` in der "ONTAP-Befehlsreferenz".

Aktivieren Sie ONTAP Cross-Cluster-Audits

Ab ONTAP 9.17.1 und ab ONTAP 9.16.1 P4 sowie späteren Patch-Versionen 9.16.1 können Sie in ONTAP Cluster-übergreifendes Auditing aktivieren, um von einem Peering-Cluster initiierte Vorgänge zu protokollieren. Dieses Remote-Auditing ist besonders wertvoll in Umgebungen, in denen mehrere ONTAP Cluster interagieren, da es die Nachvollziehbarkeit und Verantwortlichkeit von Remote-Aktionen ermöglicht.

Die clusterübergreifende Überwachung kann zwischen benutzerinitiierten GET- (Lesen) oder SET- (Erstellen/Ändern/Entfernen) Operationen unterscheiden. Standardmäßig werden nur benutzerinitiierte SET-Operationen auf Zielclustern überwacht. Jede Anfrage, die Daten liest, wie z. B. eine GET- oder `show` Befehl in der CLI wird standardmäßig nicht geprüft, unabhängig davon, ob die Anforderung clusterübergreifend ist.

Bevor Sie beginnen

- Sie müssen `advanced` Ebenenberechtigungen
- Der Cluster muss mit einem anderen Cluster 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 Audit-Protokollierung nur auf Knoten mit der aktualisierten Version. Es wird empfohlen, alle Knoten auf eine unterstützte Version zu aktualisieren, um ein konsistentes Audit-Verhalten zu gewährleisten.

Aktivieren oder Deaktivieren der clusterübergreifenden Überwachung

Schritte

1. Aktivieren (oder deaktivieren) Sie die Cluster-übergreifende Überwachung auf dem Cluster, indem Sie die `cluster-peer` Parameter auf `on` oder `off` :

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

2. Bestätigen Sie, dass die Cluster-Peer-Einstellung aktiviert oder deaktiviert ist, indem Sie den aktuellen Überwachungsstatus prüfen:

```
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 "Aktivieren Sie CLI, HTTP, ONTAPI GET-Auditing" In einem Peering-Cluster aktivieren Sie auch die Überwachung clusterübergreifender, benutzerinitiierter GET-Anfragen. In früheren ONTAP Versionen bezog sich die GET-Überwachung nur auf Anfragen in einem lokalen Cluster. Mit ONTAP 9.17.1 aktivieren Sie die GET-Überwachung mit dem `cluster-peer` Option eingestellt auf `on` , sowohl lokale Cluster- als auch clusterübergreifende Anforderungen werden geprüft.

ONTAP-Audit-Protokoll-Ziele verwalten

Sie können das Audit-Protokoll an maximal 10 Ziele weiterleiten. Sie können das Protokoll beispielsweise an einen Splunk oder Syslog-Server für Monitoring-, Analyse- und Backup-Zwecke weiterleiten.

Über diese Aufgabe

Um die Weiterleitung zu konfigurieren, müssen Sie die IP-Adresse des Syslog- oder Splunk-Hosts, seine Portnummer, ein Übertragungsprotokoll und die Syslog-Funktion angeben, die für die weitergeleiteten

Protokolle verwendet werden soll. "Hier erfahren Sie mehr über Syslog-Funktionen".

Mit dem `-protocol` Parameter können Sie einen der folgenden Übertragungswerte auswählen:

UDP unverschlüsselt
: User Datagram Protocol ohne Sicherheit (Standard)

TCP unverschlüsselt
: Übertragungsprotokoll ohne Sicherheit

TCP verschlüsselt
: Transmission Control Protocol mit Transport Layer Security (TLS) + A **Verify Server** Option ist verfügbar, wenn das TCP verschlüsselte Protokoll ausgewählt ist.

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

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

Legacy-NetApp
: Eine Variation des RFC-3164 Syslog-Formats (Format: <PRIVAL> TIMESTAMP HOSTNAME: MSG)

rfc-5424
: Syslog-Format gemäß RFC-5424 (Format: <PRIVAL> SION ZEITSTEMPEL HOSTNAME: MSG)

Sie können die Prüfprotokolle von der ONTAP CLI, und beginnend mit ONTAP 9.11.1, von System Manager weiterleiten.

System Manager

- Um die Ziele des Prüfprotokolls anzuzeigen, wählen Sie **Cluster >Einstellungen**. + die Anzahl der Protokollziele wird in der Kachel **Benachrichtigungsmanagement** angezeigt. Klicken Sie hier, ⋮ um Details anzuzeigen.
- Um Ziele für das Auditprotokoll hinzuzufügen, zu ändern oder zu löschen, wählen Sie **Events & Jobs > Audit Logs** und klicken Sie dann rechts oben auf dem Bildschirm auf **Audit-Ziele verwalten**. + Klicken Sie auf + Add , oder klicken Sie ⋮ in die Spalte **Host-Adresse**, um Einträge zu bearbeiten oder zu löschen.

CLI

1. Geben Sie für jedes Ziel, an das Sie das Prüfprotokoll weiterleiten möchten, die Ziel-IP-Adresse oder den Host-Namen und alle Sicherheitsoptionen an.

```
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 keinen Ping-Befehl an den Ziel-Host senden kann, um die Konnektivität zu überprüfen, schlägt der Befehl mit einem Fehler fehl. Obwohl nicht empfohlen, wird `-force` die Konnektivitätsprüfung mit dem Parameter mit dem Befehl umgangen.
   - Wenn Sie den `-verify-server` Parameter auf setzen `true`, wird die Identität des Protokollweiterleitungsziels durch Validierung des Zertifikats überprüft. Sie können den Wert `true` nur einstellen, wenn Sie den `tcp-encrypted` Wert im `-protocol` Feld auswählen.

2. Überprüfen Sie mit dem `cluster log-forwarding show` Befehl, 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 wird angezeigt"
- "Erstellung von Cluster-Protokollweiterleitungsfunktion"