



Audit-Protokollierung

ONTAP 9

NetApp
April 24, 2024

Inhalt

- Audit-Protokollierung 1
 - So implementiert ONTAP Audit-Protokollierung..... 1
 - Änderungen an der Auditprotokollierung in ONTAP 9 1
 - Zeigt den Inhalt des Prüfprotokolls an 2
 - Verwalten DER Einstellungen für AUDITANFRAGE 3
 - Verwalten von Zielen für Überwachungsprotokolle 4

Audit-Protokollierung

So implementiert ONTAP Audit-Protokollierung

Die im Audit-Protokoll aufgezeichneten Managementaktivitäten sind Teil der AutoSupport-Standardberichte und bestimmte Protokollierungsaktivitäten werden in EMS-Nachrichten erfasst. Sie können das Auditprotokoll auch an die von Ihnen angegebenen Ziele weiterleiten und Audit-Log-Dateien über die 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.

ONTAP protokolliert Managementaktivitäten, die auf dem Cluster ausgeführt werden, beispielsweise eine Anfrage, den Benutzer, der die Anforderung ausgelöst hat, die Zugriffsmethode des Benutzers und die Zeit der Anfrage.

Die Management-Aktivitäten können eine der folgenden Arten sein:

- **LEGEN** Sie Anforderungen FEST, die in der Regel für Befehle oder Vorgänge ohne Anzeige gelten
 - Diese Anfragen werden ausgegeben, wenn Sie ein ausführen `create`, `modify`, Oder `delete` Befehl zum Beispiel.
 - Festgelegte Anforderungen werden standardmäßig protokolliert.
- **ABRUFEN** von Anforderungen, die Informationen abrufen und in der Managementoberfläche anzeigen
 - Diese Anfragen werden ausgegeben, wenn Sie ein ausführen `show` Befehl zum Beispiel.
 - GET Requests werden nicht standardmäßig protokolliert, Sie können jedoch kontrollieren, ob GET Requests from the ONTAP CLI gesendet WERDEN (`-cliget`), aus der ONTAP API (`-ontapiget`), oder von der REST API (`-httpget`) Sind in der Datei protokolliert.

ONTAP zeichnet die Managementaktivitäten in auf `/mroot/etc/log/mlog/audit.log` Datei eines Node. Befehle aus den drei Shells für CLI-Befehle - die clustershell, die nodeshell, und die nicht-interaktive Systemshell (interaktive Systemshell-Befehle werden nicht protokolliert)- sowie API-Befehle werden hier protokolliert. In den Audit-Protokollen werden Zeitstempel verwendet, um anzuzeigen, ob alle Nodes in einem Cluster Zeit synchronisiert sind.

Der `audit.log` Die 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.

Der `audit.log` Die 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.

Änderungen an der Auditprotokollierung in ONTAP 9

Ab ONTAP 9 beginnt der `command-history.log` Datei wird durch ersetzt `audit.log`,

Und das `mgwd.log` Die 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 ist vorhanden `command-history.log` Dateien bleiben erhalten. Sie werden als neu ausgedreht (gelöscht) `audit.log` Dateien werden in gedreht (erstellt).

Tools und Skripte, die den prüfen `command-history.log` Die Datei wird möglicherweise weiterhin verwendet, da ein Soft-Link von verwendet wird `command-history.log` Bis `audit.log` Wird beim Upgrade erstellt. Jedoch Tools und Skripte, die prüfen, die `mgwd.log` Die Datei schlägt 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.

Zeigt den Inhalt des Prüfprotokolls an

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

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.

Bundesland

Der aktuelle Status des Audit-Antrags. Dies kann der Fall sein `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

Anzeigen `svm` Wenn sich die Anforderung auf einer Storage-VM befindet, wird anderenfalls 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 die von mehreren Knoten im Cluster zusammengeführten Auditeinträge anzuzeigen, geben Sie: + ein `security audit log show [parameters]`

Sie können das verwenden `security audit log show` Befehl zum Anzeigen von Auditeinträgen für einzelne Nodes oder, die von mehreren Nodes im Cluster zusammengeführt wurden. Sie können auch den Inhalt des anzeigen `/mroot/etc/log/mlog` Verzeichnis auf einem einzelnen Knoten mit einem Webbrowser. Details finden Sie auf der man-Seite.

Webbrowser


Sie können den Inhalt des anzeigen `/mroot/etc/log/mlog` Verzeichnis auf einem einzelnen Knoten mit einem Webbrowser. ["Erfahren Sie, wie Sie auf einen Knoten Protokoll zugreifen, Core Dump, und MIB-Dateien mit einem Web-Browser"](#).

Verwalten DER Einstellungen für AUDITANFRAGE

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

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 Auf  Wählen Sie in der rechten oberen Ecke die Anforderungen aus, die hinzugefügt oder entfernt werden sollen.

CLI

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

Weitere Informationen finden Sie auf den man-Pages.

Verwalten von Zielen für Überwachungsprotokolle

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

Für die Konfiguration der Weiterleitung müssen Sie die IP-Adresse des Syslog- oder Splunk-Hosts, seine Portnummer, ein Übertragungsprotokoll sowie die Syslog-Einrichtung für die weitergeleiteten Protokolle angeben. "[Hier erfahren Sie mehr über Syslog-Funktionen](#)".

Sie können 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.

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 Auf **:** 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 **+ Add**, Oder klicken Sie auf **:** In der Spalte **Host Address** können Sie Einträge bearbeiten oder 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 514 -protocol tcp-encrypted -facility user
```

- Wenn der `cluster log-forwarding create` Der Befehl kann den Ziel-Host nicht pingen, um die Verbindung zu überprüfen. Der Befehl schlägt mit einem Fehler fehl. Obwohl nicht empfohlen, verwenden Sie die `-force` Parameter mit dem Befehl umgeht die Konnektivitätsprüfung.
 - Wenn Sie die einstellen `-verify-server` Parameter an `true`, Die Identität des Protokollweiterleitungsziels wird durch die Validierung seines Zertifikats überprüft. Sie können den Wert auf einstellen `true` Nur wenn Sie das auswählen `tcp-encrypted` Wert im `-protocol` Feld.
2. Überprüfen Sie, ob die Zieldatensätze korrekt sind, indem Sie die verwenden `cluster log-forwarding show` Befehl.

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

Destination Host	Port	Protocol	Verify Server	Syslog Facility
192.168.123.96	514	udp-unencrypted	false	user
192.168.123.98	514	tcp-encrypted	true	user

2 entries were displayed.

Weitere Informationen finden Sie auf den man-Pages.

Copyright-Informationen

Copyright © 2024 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, BEISPIELHAFT 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 IRGEND EINER 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.